# **Module 1: Introduction to asset security – Giới thiệu về bảo mật tài sản**

|  |
| --- |
| You will be introduced to how organizations determine what assets to protect. You'll learn about the connection between managing risk and classifying assets by exploring the unique challenge of securing physical and digital assets. You'll also be introduced to the National Institute of Standards and Technology (NIST) framework standards, guidelines and best practices to manage cybersecurity risk. |

Bạn sẽ được giới thiệu cách các tổ chức xác định những tài sản cần bảo vệ. Bạn sẽ tìm hiểu về mối liên hệ giữa quản lý rủi ro và phân loại tài sản bằng cách khám phá thách thức đặc biệt trong việc bảo vệ tài sản vật chất và kỹ thuật số. Bạn cũng sẽ được giới thiệu về các tiêu chuẩn, hướng dẫn và phương pháp thực hành tốt nhất của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) để quản lý rủi ro an ninh mạng.

|  |
| --- |
| **Learning Objectives**   * Define threat, vulnerability, asset, and risk. * Explain security’s role in mitigating organizational risk. * Classify assets based on value. * Identify whether data is in use, in transit, or at rest. * Discuss the uses and benefits of the NIST Cybersecurity Framework. |

**Mục tiêu học tập**

* Xác định mối đe dọa, tính dễ bị tổn thương, tài sản và rủi ro.
* Giải thích vai trò của an ninh trong việc giảm thiểu rủi ro của tổ chức.
* Phân loại tài sản theo giá trị.
* Xác định xem dữ liệu đang được sử dụng, đang di chuyển hay đang ở trạng thái nghỉ.
* Thảo luận về việc sử dụng và lợi ích của Khung An ninh mạng NIST.

**1. Get started with the course – Bắt đầu với khóa học**

***1.1. Introduction to Course 5 – Giới thiệu khóa học 5***

|  |
| --- |
| What do you picture when you think about the security field? This might make you think of a dark room with people hunched over their computers. Maybe you picture a person in a lab carefully analyzing evidence. Or, maybe you imagine a guard standing watch in front of a building. The truth is, no matter what thoughts cross your mind, all of these examples are part of the wide world of security. |

Bạn hình dung điều gì khi nghĩ về lĩnh vực an ninh?Điều này có thể khiến bạn liên tưởng đến một căn phòng tối với mọi người đang cúi mình trước máy tính.Có thể bạn hình dung một người đang ở trong phòng thí nghiệm đang phân tích cẩn thận các bằng chứng.Hoặc, có thể bạn tưởng tượng một người bảo vệ đang đứng canh gác trước một tòa nhà.Sự thật là, bất kể suy nghĩ nào xuất hiện trong đầu bạn,tất cả những ví dụ này là một phần của thế giới bảo mật rộng lớn.

|  |
| --- |
| Hi, my name is Da'Queshia. I have worked as a security engineer for four years. I'm excited to be your instructor for this course and share some of my experience with you. At Google, I'm part of a diverse team of security professionals who all have different backgrounds and unique perspectives. For example, in my role, I work to secure Gmail. Part of my daily activities include developing new security features and fixing vulnerabilities in the application to make email safer for our users. |

Xin chào, tên tôi là Da'Queshia.Tôi đã làm kỹ sư an ninh được bốn năm.Tôi rất vui được trở thành người hướng dẫn của bạn cho khóa học này vàchia sẻ một số kinh nghiệm của tôi với bạn.Tại Google, tôi là thành viên của một nhóm chuyên gia bảo mật đa dạng, tất cả đều cónền tảng khác nhau và quan điểm độc đáo.Ví dụ: trong vai trò của mình, tôi làm việc để bảo mật Gmail.Một phần hoạt động hàng ngày của tôi bao gồm phát triển các tính năng bảo mật mới vàsửa các lỗ hổng trong ứng dụng để giúp email an toàn hơn cho người dùng.

|  |
| --- |
| Some members of my team began working in security after graduating from college. Many others found their way into the field after years of working in another industry. Security teams come in all different shapes and sizes. Each member of a team has a role to play. While our specific functions within the group differ, we all share the same objective: protecting valuable assets from harm. Accomplishing this mission involves a combination of people, processes, and tools. In this course, you'll learn about each of these in detail. |

Một số thành viên trong nhóm của tôi bắt đầu làm việc trong lĩnh vực an ninh sau khi tốt nghiệp đại học.Nhiều người khác đã tìm được con đường vào lĩnh vực này sau nhiều năm làm việc ở một nơi khác.ngành công nghiệp.Các đội an ninh có đủ hình dạng và kích cỡ khác nhau.Mỗi thành viên trong nhóm đều có một vai trò.Mặc dù chức năng cụ thể của chúng tôi trong nhóm có khác nhau,tất cả chúng ta đều có chung mục tiêu: bảo vệ tài sản có giá trị khỏi bị tổn hại.Hoàn thành sứ mệnh này đòi hỏi sự kết hợp của con người, quy trình,và các công cụ.Trong khóa học này, bạn sẽ tìm hiểu chi tiết về từng điều này.

|  |
| --- |
| First, you'll be introduced to the world of asset security. You'll learn about the variety of assets that organizations protect and how these factor into a company's overall approach to security. Then, you'll begin exploring the security systems and controls that teams use to proactively protect people and their information. All systems have weaknesses that can be improved upon. When those weaknesses are neglected or ignored, they can lead to serious problems. In this section of the course, you'll focus on common vulnerabilities in systems and the ways security teams stay ahead of potential problems. Finally, you'll learn about the threats to asset security. You'll also be introduced to the threat modeling process that security teams use to stay one step ahead of potential attacks. In this field, we try to do everything possible to avoid being put in a compromised position. By the end of this course, you'll have a clearer picture of the ways people, processes, and technology work together to protect all that's important. Throughout the course, you'll also get an idea of the exciting career opportunities available to you. |

Đầu tiên, bạn sẽ được giới thiệu về thế giới bảo mật tài sản.Bạn sẽ tìm hiểu về sự đa dạng của tài sản mà các tổ chức bảo vệ vànhững yếu tố này ảnh hưởng như thế nào đến cách tiếp cận tổng thể của công ty đối với vấn đề bảo mật.Sau đó, bạn sẽ bắt đầu khám phá các hệ thống bảo mật vàcác biện pháp kiểm soát mà các nhóm sử dụng để chủ động bảo vệ mọi người và thông tin của họ.Tất cả các hệ thống đều có điểm yếu có thể được cải thiện.Khi những điểm yếu đó bị bỏ qua hoặc bỏ qua, chúng có thể dẫn đến những vấn đề nghiêm trọng.Trong phần này của khóa học, bạn sẽ tập trung vào các lỗ hổng phổ biến trong hệ thốngvà cách các nhóm bảo mật đón đầu các vấn đề tiềm ẩn.Cuối cùng, bạn sẽ tìm hiểu về các mối đe dọa đối với an ninh tài sản.Bạn cũng sẽ được giới thiệu quy trình lập mô hình mối đe dọa mà các nhóm bảo mật sử dụngđể đi trước một bước trước các cuộc tấn công tiềm năng.Trong lĩnh vực này,chúng tôi cố gắng làm mọi thứ có thể để tránh bị đặt vào thế bị tổn hại.Khi kết thúc khóa học này, bạn sẽ có bức tranh rõ ràng hơn về cách mọi người,các quy trình và công nghệ phối hợp với nhau để bảo vệ tất cả những gì quan trọng.Trong suốt khóa học,bạn cũng sẽ biết được những cơ hội nghề nghiệp thú vị dành cho mình.

|  |
| --- |
| Security truly is an interdisciplinary field. Your background and perspective is an asset. Whether you're a recent college graduate or starting a new career path, the security field presents a wide range of possibilities. So what do you say? Are you ready to go on this journey with me? |

An ninh thực sự là một lĩnh vực liên ngành.Nền tảng và quan điểm của bạn là một tài sản.Cho dù bạn là sinh viên mới tốt nghiệp đại học hay đang bắt đầu một con đường sự nghiệp mới,lĩnh vực an ninh mang lại nhiều khả năng.Vậy bạn sẽ nói gì?Bạn đã sẵn sàng tham gia cuộc hành trình này cùng tôi chưa?

***1.2. Course 5 overview – Tổng quan về khóa 5***

|  |
| --- |
| **Course 5 overview** |

**Tổng quan về khóa 5**



|  |
| --- |
| Hello, and welcome to **Assets, Threats, and Vulnerabilities**, the fifth course in the Google Cybersecurity Certificate. You’re on an exciting journey! |

Xin chào và chào mừng bạn đến với **Tài sản, Mối đe dọa và Lỗ hổng** , khóa học thứ năm trong Chứng chỉ An ninh mạng của Google. Bạn đang trên một hành trình thú vị!

|  |
| --- |
| By the end of this course, you’ll build an understanding of the wide range of assets organizations must protect. You’ll explore many of the most common security controls used to protect valuable assets from risk. You’ll also discover the variety of ways assets are vulnerable to threats by adopting an attacker mindset. |

Khi kết thúc khóa học này, bạn sẽ nâng cao hiểu biết về nhiều loại tài sản mà tổ chức phải bảo vệ. Bạn sẽ khám phá nhiều biện pháp kiểm soát bảo mật phổ biến nhất được sử dụng để bảo vệ tài sản có giá trị khỏi rủi ro. Bạn cũng sẽ khám phá nhiều cách tài sản dễ bị đe dọa bằng cách áp dụng tư duy của kẻ tấn công.

|  |
| --- |
| **Certificate program progress** |

**Tiến độ chương trình chứng chỉ**

|  |
| --- |
| The Google Cybersecurity Certificate program has eight courses. **Assets, Threats, and Vulnerabilities** is the fifth course. |

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. **Tài sản, Mối đe dọa và Tính dễ bị tổn thương** là khóa học thứ năm.



|  |
| --- |
| 1. [**Foundations of Cybersecurity**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)— Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities. 2. [**Play It Safe: Manage Security Risks**](https://www.coursera.org/learn/manage-security-risks/home/week/1)— Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. 3. [**Connect and Protect: Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)— Gain an understanding of network-level vulnerabilities and how to secure networks. 4. [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)— Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL. 5. [**Assets, Threats, and Vulnerabilities**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)— *(current course)* Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities. 6. [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1)— Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents. 7. [**Automate Cybersecurity Tasks with Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)— Explore the Python programming language and write code to automate cybersecurity tasks. 8. [**Put It to Work: Prepare for Cybersecurity Jobs**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)— Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search. |

1. [**Nền tảng của an ninh mạng**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)— Khám phá nghề an ninh mạng, bao gồm các sự kiện quan trọng dẫn đến sự phát triển của lĩnh vực an ninh mạng và tầm quan trọng liên tục của nó đối với hoạt động của tổ chức. Tìm hiểu về vai trò và trách nhiệm an ninh mạng cấp cơ bản.
2. [**Chơi an toàn: Quản lý rủi ro bảo mật**](https://www.coursera.org/learn/manage-security-risks/home/week/1)— Xác định cách các chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh cũng như khám phá các công cụ an ninh mạng phổ biến.
3. [**Kết nối và bảo vệ: Mạng và an ninh mạng**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)- Hiểu biết về các lỗ hổng ở cấp độ mạng và cách bảo mật mạng.
4. [**Công cụ giao dịch: Linux và SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)- Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
5. [**Tài sản, mối đe dọa và lỗ hổng**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)— *(khóa học hiện tại)* Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.
6. [**Phát âm thanh báo động: Phát hiện và phản hồi**](https://www.coursera.org/learn/detection-and-response/home/week/1)— Hiểu vòng đời ứng phó sự cố và thực hành sử dụng các công cụ để phát hiện và ứng phó sự cố an ninh mạng.
7. [**Tự động hóa các tác vụ an ninh mạng với Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)— Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. [**Đưa nó vào hoạt động: Chuẩn bị cho công việc an ninh mạng**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)— Tìm hiểu về phân loại sự cố, trình báo và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

|  |
| --- |
| **Course 5 content** |

**Nội dung khóa 5**

|  |
| --- |
| Each course of this certificate program is broken into modules. You can complete courses at your own pace, but the module breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months. |

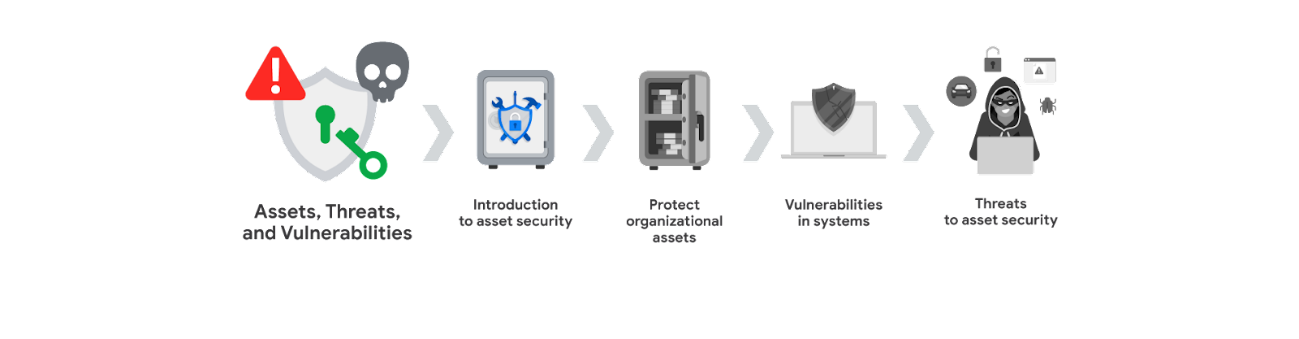
Mỗi khóa học của chương trình chứng chỉ này được chia thành các mô-đun. Bạn có thể hoàn thành các khóa học theo tốc độ của riêng mình nhưng phần phân tích mô-đun được thiết kế để giúp bạn hoàn thành toàn bộ Chứng chỉ an ninh mạng của Google trong khoảng sáu tháng.

|  |
| --- |
| What’s to come? Here’s a quick overview of the skills you’ll learn in each module of this course. |

Điều gì sẽ đến? Dưới đây là tổng quan nhanh về các kỹ năng bạn sẽ học trong mỗi mô-đun của khóa học này.

|  |
| --- |
| **Module 1: Introduction to asset security** |

**Học phần 1: Giới thiệu về bảo đảm tài sản**

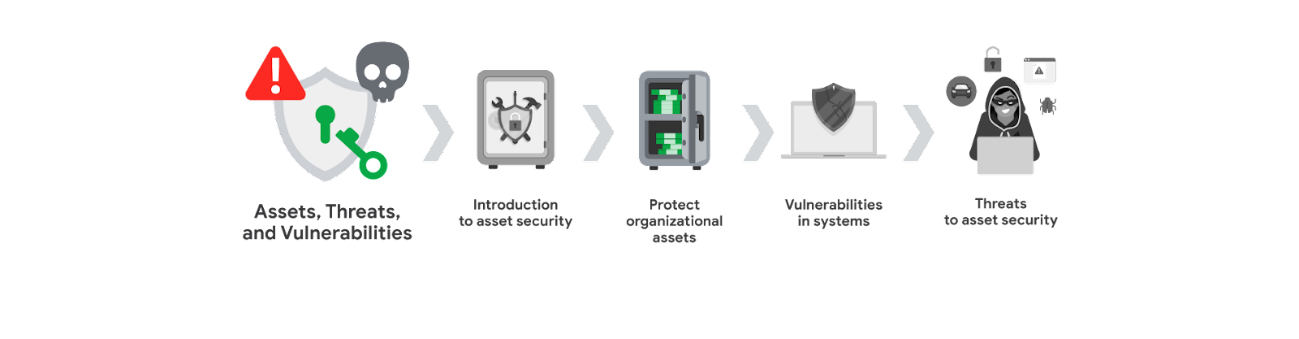


|  |
| --- |
| You will be introduced to how organizations determine what assets to protect. You'll learn about the connection between managing risk and classifying assets by exploring the unique challenge of securing physical and digital assets. You'll also be introduced to the National Institute of Standards and Technology (NIST) framework standards, guidelines, and best practices for managing cybersecurity risk. |

Bạn sẽ được giới thiệu cách các tổ chức xác định những tài sản cần bảo vệ. Bạn sẽ tìm hiểu về mối liên hệ giữa quản lý rủi ro và phân loại tài sản bằng cách khám phá thách thức đặc biệt trong việc bảo vệ tài sản vật chất và kỹ thuật số. Bạn cũng sẽ được giới thiệu về các tiêu chuẩn, hướng dẫn và phương pháp thực hành tốt nhất của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) để quản lý rủi ro an ninh mạng.

|  |
| --- |
| **Module 2: Protect organizational assets** |

**Mô-đun 2: Bảo vệ tài sản của tổ chức**

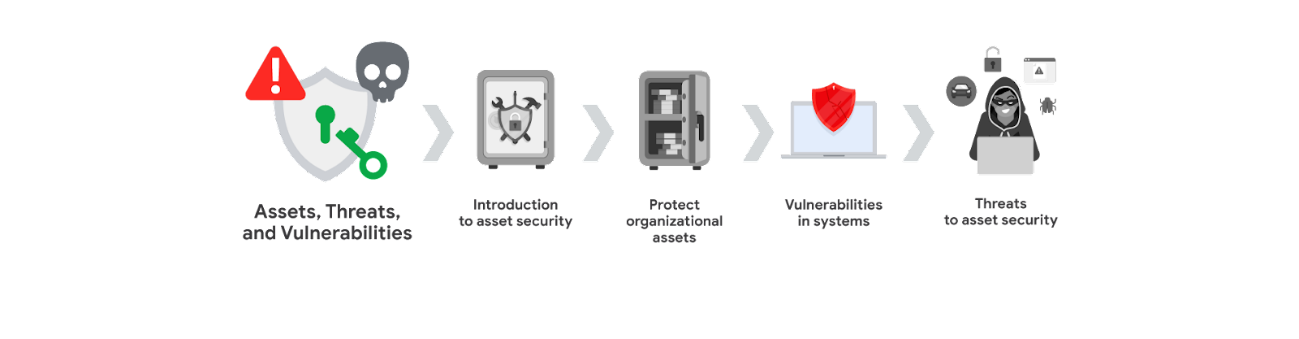


|  |
| --- |
| You will focus on security controls that protect organizational assets. You'll explore how privacy impacts asset security and understand the role that encryption plays in maintaining the privacy of digital assets. You'll also explore how authentication and authorization systems help verify a user’s identity. |

Bạn sẽ tập trung vào các biện pháp kiểm soát bảo mật để bảo vệ tài sản của tổ chức. Bạn sẽ khám phá quyền riêng tư tác động như thế nào đến bảo mật tài sản và hiểu vai trò của mã hóa trong việc duy trì quyền riêng tư của tài sản kỹ thuật số. Bạn cũng sẽ khám phá cách hệ thống xác thực và ủy quyền giúp xác minh danh tính người dùng.

|  |
| --- |
| **Module 3: Vulnerabilities in systems** |

**Mô-đun 3: Lỗ hổng trong hệ thống**

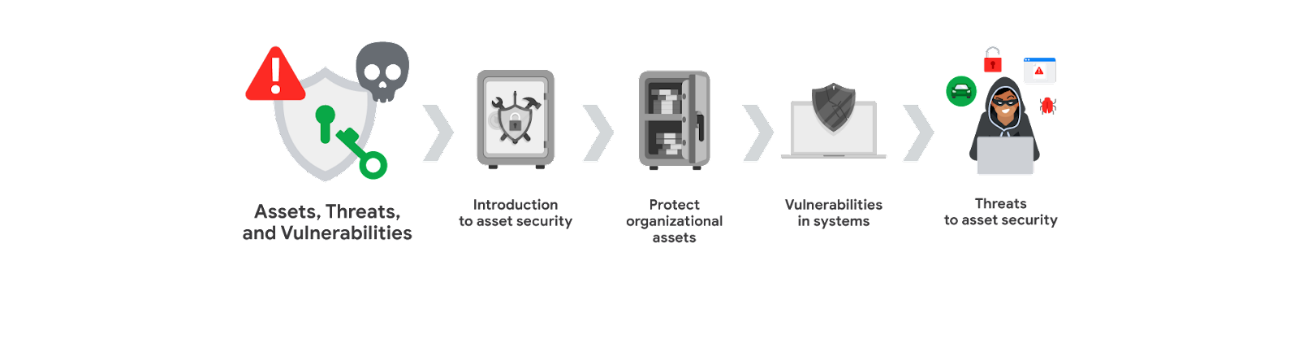


|  |
| --- |
| You will build an understanding of the vulnerability management process. You'll learn about common vulnerabilities and develop an attacker mindset by examining the ways vulnerabilities can become threats to asset security if they are exploited. |

Bạn sẽ xây dựng sự hiểu biết về quy trình quản lý lỗ hổng. Bạn sẽ tìm hiểu về các lỗ hổng phổ biến và phát triển tư duy của kẻ tấn công bằng cách kiểm tra cách các lỗ hổng có thể trở thành mối đe dọa đối với an ninh tài sản nếu chúng bị khai thác.

|  |
| --- |
| **Module 4: Threats to asset security** |

**Mô-đun 4: Các mối đe dọa đối với an ninh tài sản**



|  |
| --- |
| Finally, you will explore common types of threats to digital asset security. You'll also examine the tools and techniques used by cybercriminals to target assets. In addition, you'll be introduced to the threat modeling process and learn ways security professionals stay ahead of security breaches. |

Cuối cùng, bạn sẽ khám phá các loại mối đe dọa phổ biến đối với bảo mật tài sản kỹ thuật số. Bạn cũng sẽ kiểm tra các công cụ và kỹ thuật được tội phạm mạng sử dụng để nhắm mục tiêu vào tài sản. Ngoài ra, bạn sẽ được giới thiệu về quy trình lập mô hình mối đe dọa và tìm hiểu cách các chuyên gia bảo mật ngăn chặn các hành vi vi phạm bảo mật.

|  |
| --- |
| **What to expect** |

**Những gì mong đợi**

|  |
| --- |
| Each course offers many types of learning opportunities:   * **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories. * **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies. * **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the [discussion forums](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/discussions). * **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example. * **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course. * **In-video quizzes** help you check your comprehension as you progress through each video. * **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback. * **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score. |

Mỗi khóa học cung cấp nhiều loại cơ hội học tập:

* **Các video** do người hướng dẫn của Google hướng dẫn sẽ dạy các khái niệm mới, giới thiệu cách sử dụng các công cụ có liên quan, cung cấp hỗ trợ nghề nghiệp và cung cấp những câu chuyện cá nhân đầy cảm hứng.
* **Các bài đọc** được xây dựng dựa trên các chủ đề được thảo luận trong video, giới thiệu các khái niệm liên quan, chia sẻ các tài nguyên hữu ích và mô tả các nghiên cứu điển hình.
* **Lời nhắc thảo luận** khám phá các chủ đề khóa học để hiểu rõ hơn và cho phép bạn trò chuyện cũng như trao đổi ý tưởng với những người học khác trong khóa học.[diễn đàn thảo luận](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/discussions).
* **Các hoạt động tự đánh giá** và **phòng thí nghiệm** giúp bạn thực hành thực hành trong việc áp dụng các kỹ năng bạn đang học và cho phép bạn đánh giá bài làm của chính mình bằng cách so sánh nó với một ví dụ hoàn chỉnh.
* **Các plug-in tương tác** khuyến khích bạn thực hành các nhiệm vụ cụ thể và giúp bạn tích hợp kiến ​​thức bạn đã thu được trong khóa học.
* **Các câu đố trong video** giúp bạn kiểm tra mức độ hiểu của mình khi bạn xem qua từng video.
* **Các câu hỏi thực hành** cho phép bạn kiểm tra sự hiểu biết của mình về các khái niệm chính và cung cấp phản hồi có giá trị.
* **Các câu hỏi được chấm điểm** thể hiện sự hiểu biết của bạn về các khái niệm chính của khóa học. Bạn phải đạt 80% điểm trở lên trong mỗi bài kiểm tra được xếp loại để nhận được chứng chỉ và bạn có thể làm bài kiểm tra được xếp loại nhiều lần để đạt được điểm đậu.

|  |
| --- |
| **Tips for success** |

**Lời khuyên để thành công**

|  |
| --- |
| * It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge. * Participate in all learning opportunities to gain as much knowledge and experience as possible. * If something is confusing, don’t hesitate to replay a video, review a reading, or repeat a self-review activity. * Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the [**Resources**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/resources/4ypPt) tab. * When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review. * Understand and follow the [Coursera Code of Conduct](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?) to ensure that the learning community remains a welcoming, friendly, and supportive place for all members. |

* Chúng tôi đặc biệt khuyên bạn nên xem qua các mục trong mỗi bài học theo thứ tự chúng xuất hiện vì thông tin và khái niệm mới được xây dựng dựa trên kiến ​​thức trước đó.
* Tham gia vào tất cả các cơ hội học tập để có được càng nhiều kiến ​​thức và kinh nghiệm càng tốt.
* Nếu có điều gì đó khó hiểu, đừng ngần ngại phát lại video, xem lại bài đọc hoặc lặp lại hoạt động tự xem xét.
* Sử dụng các tài nguyên bổ sung được tham chiếu trong khóa học này. Chúng được thiết kế để hỗ trợ việc học của bạn. Bạn có thể tìm thấy tất cả các tài nguyên này trong[**Tài nguyên**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/resources/4ypPt)chuyển hướng.
* Khi bạn gặp các liên kết hữu ích trong khóa học này, hãy đánh dấu chúng để bạn có thể tham khảo thông tin sau này để nghiên cứu hoặc ôn tập.
* Hãy hiểu và làm theo[Quy tắc ứng xử của Coursera](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?)để đảm bảo rằng cộng đồng học tập vẫn là một nơi thân thiện, thân thiện và hỗ trợ cho tất cả các thành viên.

***1.3. Helpful resources and tips - Tài nguyên và lời khuyên hữu ích***

|  |
| --- |
| **Helpful resources and tips** |

**Tài nguyên và lời khuyên hữu ích**

|  |
| --- |
| As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera. |

Là người học, bạn có thể chọn hoàn thành một hoặc nhiều khóa học trong chương trình này. Tuy nhiên, để có được Chứng chỉ an ninh mạng của Google, bạn phải hoàn thành tất cả các khóa học. Bài đọc này mô tả những gì cần thiết để có được chứng chỉ và các phương pháp hay nhất để bạn có trải nghiệm học tập tốt trên Coursera.

|  |
| --- |
| **Obtain the Google Cybersecurity Certificate** |

**Nhận Chứng chỉ an ninh mạng của Google**

|  |
| --- |
| To receive your official Google Cybersecurity Certificate, you must:   * Pass all graded assignments in all 8 courses of the certificate program. Each graded assignment is part of a cumulative graded score for the course, and the passing grade for each course is 80%. |

Để nhận Chứng chỉ an ninh mạng chính thức của Google, bạn phải:

* Đạt tất cả các bài tập được chấm điểm trong tất cả 8 khóa học của chương trình cấp chứng chỉ. Mỗi bài tập được chấm điểm là một phần của điểm chấm điểm tích lũy cho khóa học và điểm đậu cho mỗi khóa học là 80%.

|  |
| --- |
| AND **one**of the following:   * Pay the [course certificate fee](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US), * Be approved for [Coursera Financial Aid](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US), **or** * Complete the certificate through an educational institution, employer, or agency that's sponsoring your participation. |

VÀ  **một** trong những điều sau đây:

* Tra[lệ phí cấp chứng chỉ khóa học](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US),
* Được chấp thuận cho[Hỗ trợ tài chính Coursera](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US),  **hoặc**
* Hoàn thành chứng chỉ thông qua tổ chức giáo dục, người sử dụng lao động hoặc cơ quan tài trợ cho sự tham gia của bạn

|  |
| --- |
| **Healthy habits for course completion** |

**Thói quen lành mạnh khi hoàn thành khóa học**

|  |
| --- |
| Here is a list of best practices that will help you complete the courses in the program in a timely manner: |

Dưới đây là danh sách các phương pháp hay nhất sẽ giúp bạn hoàn thành các khóa học trong chương trình một cách kịp thời:

|  |
| --- |
| * **Plan your time:** Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities. * **Work at your own pace:** Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead. * **Be curious:** If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs. * **Take notes:** Notes will help you remember important information in the future, especially as you’re preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics. * **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity. * **Chat (responsibly) with other learners:** If you have a question, chances are, you’re not alone. Use the [discussion forums](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/discussions) to ask for help from other learners taking this program. You can also visit Coursera’s [Global Online Community](https://coursera.community/). Other important things to know while learning with others can be found in the [Coursera Honor Code](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code) and [Code of Conduct](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct). * **Update your profile:** Consider [updating your profile](https://www.coursera.org/account/profile) on Coursera to include your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better. |

* **Lập kế hoạch thời gian của bạn:** Đặt thời gian học tập thường xuyên và tuân theo chúng mỗi tuần có thể giúp bạn biến việc học trở thành một phần thói quen của mình. Sử dụng lịch hoặc thời gian biểu để tạo lịch trình và liệt kê những việc bạn dự định làm mỗi ngày để đặt ra các mục tiêu có thể đạt được. Tìm một không gian cho phép bạn tập trung khi xem video, xem lại bài đọc và hoàn thành các hoạt động.
* **Làm việc theo tốc độ của riêng bạn:** Mọi người học theo cách khác nhau, vì vậy chương trình này được thiết kế để giúp bạn làm việc theo tốc độ của riêng mình. Mặc dù thời hạn được cá nhân hóa của bạn bắt đầu khi bạn đăng ký, nhưng hãy thoải mái chuyển qua chương trình với tốc độ phù hợp nhất với bạn. Không có hình phạt cho bài tập muộn; để có được chứng chỉ, tất cả những gì bạn phải làm là hoàn thành tất cả công việc. Bạn có thể gia hạn thời hạn của mình bất kỳ lúc nào bằng cách đi tới **Tổng quan** trong bảng điều hướng và chọn **Chuyển đổi phiên** . Nếu bạn đã bỏ lỡ thời hạn trước đó, hãy chọn **Đặt lại thời hạn của tôi** .
* **Hãy tò mò:** Nếu bạn tìm thấy một ý tưởng khiến bạn hứng thú, hãy hành động theo nó! Đặt câu hỏi, tìm kiếm thêm chi tiết trực tuyến, khám phá các liên kết mà bạn quan tâm và ghi chú những khám phá của bạn. Các bước bạn thực hiện để hỗ trợ quá trình học tập của mình sẽ nâng cao kiến ​​thức của bạn, tạo ra nhiều cơ hội hơn trong lĩnh vực có tốc độ tăng trưởng cao này và giúp bạn đủ điều kiện tìm việc làm.
* **Ghi chú:** Ghi chú sẽ giúp bạn ghi nhớ những thông tin quan trọng trong tương lai, đặc biệt khi bạn đang chuẩn bị bước vào một lĩnh vực công việc mới. Ngoài ra, ghi chép là một cách hiệu quả để tạo sự kết nối giữa các chủ đề và hiểu rõ hơn về các chủ đề đó.
* **Xem lại các mẫu:** Các mẫu là các bài tập đã hoàn thành đáp ứng đầy đủ các tiêu chí của hoạt động. Nhiều hoạt động trong chương trình này có mẫu để bạn xác thực công việc của mình hoặc kiểm tra lỗi. Mặc dù thường có nhiều cách để hoàn thành bài tập nhưng các ví dụ mẫu sẽ đưa ra hướng dẫn và nguồn cảm hứng về cách hoàn thành hoạt động.
* **Trò chuyện (có trách nhiệm) với những người học khác:** Nếu bạn có câu hỏi, rất có thể bạn không đơn độc. Sử dụng[diễn đàn thảo luận](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/discussions)để yêu cầu sự giúp đỡ từ những người học khác tham gia chương trình này. Bạn cũng có thể ghé thăm Coursera's[Cộng đồng trực tuyến toàn cầu](https://coursera.community/). Những điều quan trọng khác cần biết khi học cùng người khác có thể được tìm thấy trong[Mã danh dự Coursera](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code)Và[Quy tắc ứng xử](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct).
* **Cập nhật hồ sơ của bạn:** Hãy xem xét[cập nhật hồ sơ của bạn](https://www.coursera.org/account/profile)trên Coursera để đưa ảnh của bạn, mục tiêu nghề nghiệp, v.v. Khi những người học khác tìm thấy bạn trong các diễn đàn thảo luận, họ có thể nhấp vào tên của bạn để truy cập hồ sơ của bạn và hiểu rõ hơn về bạn.

|  |
| --- |
| **Documents, spreadsheets, presentations, and labs for course activities** |

**Tài liệu, bảng tính, bài thuyết trình và phòng thí nghiệm cho các hoạt động của khóa học**

|  |
| --- |
| To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources: |

Để hoàn thành một số hoạt động nhất định trong chương trình, bạn sẽ cần sử dụng tài liệu kỹ thuật số, bảng tính, bản trình bày và/hoặc phòng thí nghiệm. Các chuyên gia bảo mật sử dụng các công cụ phần mềm này để cộng tác trong nhóm và tổ chức của họ. Nếu bạn cần thêm thông tin về cách sử dụng một công cụ cụ thể, hãy tham khảo các tài nguyên sau:

|  |
| --- |
| * [Microsoft Word: Help and learning](https://support.microsoft.com/en-us/word): Microsoft Support page for Word * [Google Docs](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Help Center page for Google Docs * [Microsoft Excel: Help and learning](https://support.microsoft.com/en-us/excel): Microsoft Support page for Excel * [Google Sheets](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Help Center page for Google Sheets * [Microsoft PowerPoint: Help and learning](https://support.microsoft.com/en-us/powerpoint): Microsoft Support page for PowerPoint * [How to use Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Help Center page for Google Slides * [Common problems with labs](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Troubleshooting help for Qwiklabs activities |

* [Microsoft Word: Trợ giúp và học tập](https://support.microsoft.com/en-us/word): Trang hỗ trợ của Microsoft dành cho Word
* [Google Tài liệu](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Documents
* [Microsoft Excel: Trợ giúp và học tập](https://support.microsoft.com/en-us/excel): Trang hỗ trợ của Microsoft dành cho Excel
* [Google Trang tính](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Trang tính
* [Microsoft PowerPoint: Trợ giúp và học tập](https://support.microsoft.com/en-us/powerpoint): Trang hỗ trợ của Microsoft dành cho PowerPoint
* [Cách sử dụng Google Trang trình bày](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Trang Trung tâm trợ giúp dành cho Google Trang trình bày
* [Các vấn đề thường gặp với phòng thí nghiệm](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Trợ giúp khắc phục sự cố cho các hoạt động của Qwiklabs

|  |
| --- |
| **Module, course, and certificate glossaries** |

**Bảng thuật ngữ mô-đun, khóa học và chứng chỉ**

|  |
| --- |
| This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries: |

Chương trình này bao gồm rất nhiều thuật ngữ và khái niệm, một số trong đó bạn có thể đã biết và một số có thể xa lạ với bạn. Để xem lại các thuật ngữ và giúp bạn chuẩn bị cho các bài kiểm tra được chấm điểm, hãy tham khảo các bảng thuật ngữ sau:

|  |
| --- |
| * **Module glossaries**: At the end of each module’s content, you can review a glossary of terms from that module. Each module’s glossary builds upon the terms from the previous modules in that course. The module glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable. * **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course. * **Certificate glossary**: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future. |

* **Bảng thuật ngữ mô-đun** : Ở cuối nội dung của mỗi mô-đun, bạn có thể xem lại bảng chú giải thuật ngữ của mô-đun đó. Bảng thuật ngữ của mỗi mô-đun được xây dựng dựa trên các thuật ngữ từ các mô-đun trước đó trong khóa học đó. Bảng thuật ngữ mô-đun không thể tải xuống được; tuy nhiên, tất cả các thuật ngữ và định nghĩa đều có trong bảng thuật ngữ khóa học và chứng chỉ, có thể tải xuống được.
* **Bảng thuật ngữ khóa học** : Vào cuối mỗi khóa học, bạn có thể truy cập và tải xuống bảng chú giải thuật ngữ bao gồm tất cả các thuật ngữ trong khóa học đó.
* **Bảng chú giải thuật ngữ chứng chỉ** : Bảng chú giải chứng chỉ bao gồm tất cả các thuật ngữ trong toàn bộ chương trình chứng chỉ và là nguồn tài nguyên hữu ích mà bạn có thể tham khảo trong suốt chương trình hoặc bất kỳ lúc nào trong tương lai.

|  |
| --- |
| You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course’s [Resources](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/Xi7Ty/course-5-glossary) section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.   * [Cybersecurity Certificate glossary](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?usp=sharing&resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ) |

Bạn có thể truy cập và tải xuống bảng chú giải chứng chỉ và lưu chúng trên máy tính của mình. Bạn luôn có thể tìm thấy bảng chú giải thuật ngữ về khóa học và chứng chỉ thông qua trang của khóa học.[Tài nguyên](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/Xi7Ty/course-5-glossary)phần. Để truy cập **bảng chú giải Chứng chỉ An ninh mạng** , hãy nhấp vào liên kết bên dưới và chọn *Sử dụng Mẫu* .

* [Thuật ngữ chứng chỉ an ninh mạng](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?usp=sharing&resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ)

|  |
| --- |
| **Course feedback** |

**Phản hồi khóa học**

|  |
| --- |
| Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols. |

Việc cung cấp phản hồi về video, bài đọc và các tài liệu khác thật dễ dàng. Khi tài nguyên mở trong trình duyệt của bạn, bạn có thể tìm thấy các biểu tượng không thích và không thích.

|  |
| --- |
| * Click **thumbs-up** for materials that are helpful. * Click **thumbs-down** for materials that are not helpful. |

* Hãy **nhấp vào biểu tượng** thích để xem các tài liệu hữu ích.
* Hãy **nhấp vào nút không thích** đối với những tài liệu không hữu ích.

|  |
| --- |
| If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn’t visible to other learners. All feedback received helps to create even better certificate programs in the future. |

Nếu bạn muốn gắn cờ một vấn đề cụ thể cho một mục, hãy nhấp vào biểu tượng lá cờ, chọn một danh mục và nhập lời giải thích vào hộp văn bản. Phản hồi này sẽ được chuyển lại cho nhóm phát triển khóa học và những người học khác sẽ không nhìn thấy được. Tất cả phản hồi nhận được sẽ giúp tạo ra các chương trình chứng chỉ tốt hơn nữa trong tương lai.

|  |
| --- |
| For technical help, visit the [Learner Help Center](https://learner.coursera.help/hc/en-us). |

Để được trợ giúp kỹ thuật, hãy truy cập[Trung tâm trợ giúp người học](https://learner.coursera.help/hc/en-us).

***1.4. Da'Queshia: My path to cybersecurity - Da'Queshia: Con đường đến với an ninh mạng của tôi***

|  |
| --- |
| Hi. My name is Da'Queshia. I'm a security engineer. That basically means I work securing Google's products so users like you aren't vulnerable. Before I entered cybersecurity, I worked installing Internet. I also worked at a chip factory. I worked in fast food. I sold shoes at the mall. I did a lot of things before I made it here. A lot of what I learned in my past jobs I actually use every day. Some of it is my soft skills like time management, people skills, and communication. As a new cybersecurity analyst, it's important to be able to communicate, take feedback, and feel uncomfortable, not with the people around you, but with the problems you're trying to solve because sometimes it requires you to think outside of the box and be challenged. I would describe my job as a Google security guard because I work on the Gmail security team, it's my job to protect Gmail. Some of those threats are people who are sending you bad emails, who are trying to get your user credentials or get you to click on a phishing link. When it comes to vulnerabilities, some of those could be something like unsanitized input, which can lead to trouble. My typical work day starts like everyone else. I check my emails and then from there I go into my bug queue; it's essentially when people tell me there's a problem with one of our products. I start doing a little bit of research and then I like to explore the bug a little bit more. I like to figure out if this can break this, can it also break this, and if it can, what else can I do with it? Then from there, I look for a solution to make sure that I fix that hole and then any other holes that we might have in our security. Some of the things you learned about in this course is threat modeling, and that's something I use every day. Whenever I get a bug, it's part of my job to figure out the attack tree and what type of vectors we use to take advantage of vulnerabilities. No one is born knowing everything. I know that sounds really cliche or like super obvious, but it helps me because it helps put some perspective the time and effort that everyone has to put in in order to learn something new. So be patient with yourself. Don't let anyone discourage you from cybersecurity. Taking this course is one step closer to getting into your goal. Don't get discouraged now. Keep going. |

CHÀO. Tên tôi là Da'Queshia.Tôi là kỹ sư an ninh.Về cơ bản điều đó có nghĩa là tôi làm việc để bảo vệCác sản phẩm của Google nên những người dùng như bạn không dễ bị tổn thương.Trước khi tôi bước vào lĩnh vực an ninh mạng,Tôi đã làm việc cài đặt Internet.Tôi cũng từng làm việc tại một nhà máy sản xuất chip.Tôi đã làm việc trong lĩnh vực thức ăn nhanh.Tôi bán giày ở trung tâm thương mại.Tôi đã làm rất nhiều thứ trước khi đến đây.Rất nhiều điều tôi đã học được trong công việc trước đây của mìnhTôi thực sự sử dụng hàng ngày.Một phần là các kỹ năng mềm của tôi như quản lý thời gian,kỹ năng con người và giao tiếp.Là một nhà phân tích an ninh mạng mới,điều quan trọng là có khả năng giao tiếp, nhận phản hồi,và cảm thấy không thoải mái, không phải với những người xung quanh bạn,nhưng với những vấn đề bạn đang cố gắng giải quyếtgiải quyết vì đôi khi nóđòi hỏi bạn phải suy nghĩ bên ngoàichiếc hộp và được thử thách.Tôi sẽ mô tả công việc của mình như mộtNhân viên bảo vệ của Google vìTôi làm việc trong nhóm bảo mật Gmail,công việc của tôi là bảo vệ Gmail.Một số mối đe dọa đó lànhững người đang gửi cho bạn những email xấu,những người đang cố lấy thông tin đăng nhập người dùng của bạnhoặc khiến bạn nhấp vào liên kết lừa đảo.Khi nói đến các lỗ hổng,một số trong số đó có thể là một cái gì đónhư đầu vào không được vệ sinh,có thể dẫn đến rắc rối.Ngày làm việc điển hình của tôi bắt đầu như mọi người khác.Tôi kiểm tra email của mình vàsau đó từ đó tôi đi vào hàng đợi lỗi của mình;về cơ bản là khi mọi người nói với tôicó vấn đề với một trong các sản phẩm của chúng tôi.Tôi bắt đầu thực hiện một chút nghiên cứu và sau đóTôi thích khám phá lỗi hơn một chút.Tôi muốn tìm hiểu xem liệu điều này có thể phá vỡ được điều này không,nó cũng có thể phá vỡ cái này không,và nếu có thể, tôi có thể làm gì khác với nó?Rồi từ đó tôi tìmmột giải pháp để đảm bảo rằng tôi khắc phục đượccái lỗ đó và cái khácnhững lỗ hổng mà chúng ta có thể có trong bảo mật của mình.Một số điều bạn đã học được trongkhóa học này là mô hình mối đe dọa,và đó là thứ tôi sử dụng hàng ngày.Bất cứ khi nào tôi gặp lỗi, đó là một phần củacông việc của tôi là tìm ra cây tấn côngvà loại vectơ chúng tôi sử dụngđể lợi dụng các lỗ hổng.Không ai sinh ra đã biết tất cả mọi thứ.Tôi biết điều đó nghe có vẻ sáo rỗng hoặc siêu hiển nhiên,nhưng nó giúp tôi vì nó giúpđặt một số quan điểm thời gianvà nỗ lực mà mọi người phải làmđưa vào để học một cái gì đó mới.Vì vậy hãy kiên nhẫn với chính mình.Đừng để bất cứ ai ngăn cản bạn khỏi an ninh mạng.Tham gia khóa học này là một bướctiến gần hơn tới mục tiêu của bạn.Đừng nản lòng bây giờ. Tiếp tục đi.

***1.5. Connect with your classmates - Kết nối với các bạn cùng lớp của bạn***

**2. Introduction to assets – Giới thiệu về tài sản**

***2.1. Welcome to module 1 - Chào mừng đến với mô-đun 1***

|  |
| --- |
| We all depend on technology so much nowadays. Examples of this are all around us. Personal devices, like smartphones, help keep us in touch with friends and families across the globe. Wearable technologies help us achieve personal goals and be more productive. Businesses have also come to embrace technology in everyday life. From streamlining operations to automating processes, our world is more connected because of technology. |

Ngày nay tất cả chúng ta đều phụ thuộc vào công nghệ rất nhiều.Ví dụ về điều này ở xung quanh chúng ta.Các thiết bị cá nhân, như điện thoại thông minh, giúp chúng ta giữ liên lạc với bạn bè vàgia đình trên toàn cầu.Công nghệ thiết bị đeo giúp chúng ta đạt được mục tiêu cá nhân và làm việc hiệu quả hơn.Các doanh nghiệp cũng đã bắt đầu ứng dụng công nghệ vào cuộc sống hàng ngày.Từ việc hợp lý hóa các hoạt động đến tự động hóa các quy trình, thế giới của chúng ta ngày càng trở nên thú vị hơn.được kết nối nhờ công nghệ.

|  |
| --- |
| The more we rely on technology, the more information we share. As a result, an enormous amount of data is created every day. This huge surge in data creation presents unique challenges. As businesses become more reliant on technology, cybercriminals become more sophisticated in how they affect organizations. Data breaches are becoming increasingly serious due to all the sensitive data businesses are storing. One positive aspect of these challenges is a growing need for individuals like you! Security is a team effort. Unique perspectives, like yours, are an asset to any organization. A team filled with diverse backgrounds, cultures, and experiences is more likely to solve problems and be innovative. As breach after breach hits the headlines, it's clear that organizations need more professionals focused on security. Companies around the globe are working hard to keep up with the demands of a rapidly changing digital landscape. As the environment continues to transform, the more your personal experience is valuable. |

Chúng ta càng dựa vào công nghệ thì chúng ta càng chia sẻ nhiều thông tin hơn.Kết quả là, một lượng dữ liệu khổng lồ được tạo ra mỗi ngày.Sự đột biến lớn trong việc tạo ra dữ liệu này đặt ra những thách thức đặc biệt.Khi các doanh nghiệp ngày càng phụ thuộc nhiều hơn vào công nghệ,Tội phạm mạng trở nên tinh vi hơn trong cách chúng ảnh hưởng đến các tổ chức.Vi phạm dữ liệu ngày càng trở nên nghiêm trọng do tất cả các dữ liệu nhạy cảmdoanh nghiệp đang lưu trữ.Một khía cạnh tích cực của những thách thức này là nhu cầu ngày càng tăng đối với những cá nhân như bạn!An ninh là một nỗ lực của nhóm.Những quan điểm độc đáo, giống như quan điểm của bạn, là tài sản của bất kỳ tổ chức nào.Một nhóm có nền tảng, văn hóa và nền tảng đa dạngkinh nghiệm có nhiều khả năng giải quyết vấn đề và có tính sáng tạo hơn.Khi hết vi phạm này đến vi phạm khác được đưa lên mặt báo, rõ ràng là các tổ chứccần nhiều chuyên gia hơn tập trung vào bảo mật.Các công ty trên toàn cầu đang nỗ lực để đáp ứng nhu cầucủa bối cảnh kỹ thuật số đang thay đổi nhanh chóng.Khi môi trường tiếp tục biến đổi, trải nghiệm cá nhân của bạn càng có giá trị.

|  |
| --- |
| In this section, we'll start by exploring how assets, threats, and vulnerabilities factor into security plans. After that, we'll discuss the use of asset inventories in protecting the wide range of assets that companies have. Then, we'll consider the challenges in this rapidly changing digital world. And finally, you'll gain an understanding of the building blocks of a security plan: its policies, standards, and procedures. We'll examine the NIST Cybersecurity Framework that companies use to create security plans that protect their customers and their brands. I hope you're as excited to go on this journey into this world of security as I am. Now, let's get started! |

Trong phần này, chúng ta sẽ bắt đầu bằng cách khám phá các tài sản, mối đe dọa,và các yếu tố dễ bị tổn thương trong các kế hoạch bảo mật.Sau đó, chúng ta sẽ thảo luận về việc sử dụng hàng tồn kho tài sản trongbảo vệ nhiều loại tài sản mà công ty có.Sau đó, chúng ta sẽ xem xét những thách thức trong thế giới kỹ thuật số đang thay đổi nhanh chóng này.Và cuối cùng, bạn sẽ hiểu được các khối xây dựng của một kế hoạch bảo mật:chính sách, tiêu chuẩn và thủ tục của mình.Chúng ta sẽ xem xét Khung bảo mật không gian mạng NIST mà các công ty sử dụng đểtạo ra các kế hoạch bảo mật để bảo vệ khách hàng và thương hiệu của họ.Tôi hy vọng bạn cũng hào hứng tham gia cuộc hành trình vào thế giới an toàn nàynhư tôi.Bây giờ, hãy bắt đâù!

***2.2. The what, why, and how of asset security - Cái gì, tại sao và như thế nào về bảo đảm tài sản***

|  |
| --- |
| Painting a portrait. Perfecting a new basketball move. Playing a solo on guitar. They all share something in common. Can you guess what it is? If you thought "practice," you're absolutely correct! It takes time, dedication, and focus to improve these skills. The security profession is no different. Planning for the future is a core skill that you'll need to practice all the time in security. |

Vẽ một bức chân dung. Hoàn thiện một động tác bóng rổ mới.Chơi solo trên guitar. Tất cả họ đều có chung một điều gì đó.Bạn có đoán được nó là gì không?Nếu bạn nghĩ "thực hành" thì bạn hoàn toàn đúng!Cần có thời gian, sự cống hiến và sự tập trung để cải thiện những kỹ năng này.Nghề bảo vệ cũng không khác.Lập kế hoạch chotương lai là kỹ năng cốt lõi mà bạn sẽ cần phải thực hành mọi lúc trong lĩnh vực bảo mật.

|  |
| --- |
| We all deal with uncertainty by trying to solve problems before they arise. For example, if you're going on a trip, you might think about the length of the trip and how much to pack. Maybe you're traveling somewhere cold. You might bring coats and sweaters to help keep you warm. We all want to feel the security of knowing that there's a plan if something goes wrong. Businesses are no different. Just like you, organizations try their best to plan ahead by analyzing risk. |

Tất cả chúng ta đều đối mặt với sự không chắc chắn bằng cách cố gắng giải quyết vấn đề trước khi chúng phát sinh.Ví dụ: nếu bạn đang đi du lịch,bạn có thể nghĩ về độ dài của chuyến đi và số lượng hành lý cần mang theo.Có lẽ bạn đang đi du lịch ở một nơi nào đó lạnh giá. Bạn có thể mang theo áo khoác vàáo len giúp bạn giữ ấm.Tất cả chúng ta đều muốn cảm thấy an toàn khi biết rằng có một kế hoạch nếu có điều gì đóđi sai.Các doanh nghiệp cũng không khác. Giống như bạn,các tổ chức cố gắng hết sức để lập kế hoạch trước bằng cách phân tích rủi ro.

|  |
| --- |
| Security teams help companies by focusing on risk. In security, a risk is anything that can impact the confidentiality, integrity, or availability of an asset. Our primary focus as security practitioners is to maintain confidentiality, integrity, and availability, which are the three components of the CIA triad. The process of security risk planning is the first step toward protecting these cornerstones. Each organization has their own unique security plan based on the risk they face. Thankfully, you don't need to be familiar with every possible security plan to be a good security practitioner. All you really need to know are the basics of how these plans are put together. |

Đội ngũ bảo mật giúp đỡ các công ty bằng cách tập trung vào rủi ro.Trong bảo mật, rủi ro là bất cứ điều gì có thể ảnh hưởng đến tính bảo mật,tính toàn vẹn hoặc tính sẵn có của một tài sản.Trọng tâm chính của chúng tôi với tư cách là người thực hiện bảo mật là duy trìtính bảo mật, tính toàn vẹn và tính sẵn sàng,đó là ba thành phần của bộ ba CIA.Quá trình lập kế hoạch rủi ro bảo mật là bước đầu tiên hướng tới việc bảo vệ những rủi ro này.nền tảng.Mỗi tổ chức có kế hoạch bảo mật riêng dựa trên rủi ro mà họ gặp phải.Rất may, bạn không cần phải làm quen với mọi kế hoạch bảo mật có thể có.một người thực hành an ninh tốt.Tất cả những gì bạn thực sự cần biết là những điều cơ bản về cách kết hợp các kế hoạch này lại với nhau.

|  |
| --- |
| Security plans are based on the analysis of three elements: assets, threats, and vulnerabilities. Organizations measure security risk by analyzing how each can have an effect on confidentiality, integrity, and availability of their information and systems. Basically, they each represent the what, why, and how of security. Let's spend a little time exploring each of these in more detail. |

Kế hoạch bảo mật dựa trên việc phân tích ba yếu tố: tài sản,các mối đe dọa và điểm yếu.Các tổ chức đo lường rủi ro bảo mật bằng cách phân tích xem mỗi rủi ro có thể ảnh hưởng như thế nào đếntính bảo mật, tính toàn vẹn và tính sẵn có của thông tin của họ vàhệ thống.Về cơ bản, chúng đại diện cho cái gì, tại sao và như thế nào về bảo mật.Chúng ta hãy dành một chút thời gian để khám phá từng điều này một cách chi tiết hơn.

|  |
| --- |
| As you might imagine, an asset is an item perceived as having value to an organization. This often includes a wide range of things. Buildings, equipment, data, and people are all examples of assets that businesses want to protect. Let's examine this idea more by analyzing the assets of a home. Inside a home, there's a wide range of assets, like people and personal belongings. The outside structure of a home is made of assets too, like the walls, roof, windows, and doors. All of these assets have value, but they differ in how they might be protected. Someone might place a lower priority on protecting the outside walls than on the front door, for example. This is because a burglar is more likely to enter through the front door than a wall. That's why we have locks. With so many types of assets to think of, security plans need to prioritize resources. After all, no matter how large a security team is, it would be impossible to monitor every single asset at all hours of the day. |

Như bạn có thể tưởng tượng, tài sản là một vật phẩm được coi là có giá trị đối vớimột tổ chức.Điều này thường bao gồm nhiều thứ. Tòa nhà, thiết bị, dữ liệu,và con người đều là những ví dụ về tài sản mà doanh nghiệp muốn bảo vệ.Hãy xem xét ý tưởng này nhiều hơn bằng cách phân tích tài sản của một ngôi nhà.Bên trong một ngôi nhà có rất nhiều tài sản, như con người vàđồ dùng cá nhân.Cấu trúc bên ngoài của một ngôi nhà cũng được tạo thành từ các tài sản như tường, mái nhà,cửa sổ và cửa ra vào.Tất cả những tài sản này đều có giá trị nhưng chúng khác nhau về cách bảo vệ.Ai đó có thể đặt mức độ ưu tiên thấp hơn cho việc bảo vệ các bức tường bên ngoài so với việc bảo vệ các bức tường bên ngoài.cửa trước chẳng hạn.Điều này là do kẻ trộm có nhiều khả năng đi vào bằng cửa trước hơn làbức tường. Đó là lý do tại sao chúng ta có ổ khóa.Với rất nhiều loại tài sản để nghĩ đến,kế hoạch bảo mật cần ưu tiên các nguồn lực.Suy cho cùng, cho dù đội an ninh có lớn đến đâu,sẽ không thể giám sát từng tài sản vào tất cả các giờ trong ngày.

|  |
| --- |
| Security teams can prioritize their efforts based on threats. In security, a threat is any circumstance or event that can negatively impact assets. Much like assets, threats include a wide range of things. Going back to the example of a home, a threat can be a burglar who's trying to gain access. Burglars aren't the only type of threat that affect the security of windows and doors. What if either broke by accident? Strong winds can blow the door open during a bad storm. Or, kids playing with a ball nearby can accidentally damage a window. If any of these thoughts crossed your mind, great job! You're already demonstrating a security mindset. |

Các nhóm bảo mật có thể ưu tiên nỗ lực của họ dựa trên các mối đe dọa.Trong lĩnh vực bảo mật, mối đe dọa là bất kỳ tình huống hoặcsự kiện có thể tác động tiêu cực đến tài sản.Giống như tài sản, các mối đe dọa bao gồm rất nhiều thứ.Trở lại ví dụ về một ngôi nhà,mối đe dọa có thể là một tên trộm đang cố gắng truy cập.Kẻ trộm không phải là mối đe dọa duy nhất ảnh hưởng đến tính bảo mật của Windowsvà cửa ra vào.Điều gì sẽ xảy ra nếu một trong hai bị hỏng do tai nạn?Gió mạnh có thể thổi tung cửa khi có bão lớn.Hoặc trẻ em chơi bóng gần đó có thể vô tình làm hỏng cửa sổ.Nếu bất kỳ suy nghĩ nào trong số này xuất hiện trong đầu bạn, thì tuyệt vời!Bạn đã thể hiện tư duy bảo mật.

|  |
| --- |
| The final element of a security plan that we're going to cover are vulnerabilities. In security, a vulnerability is a weakness that can be exploited by a threat. A weak lock on a front door, for example, is a vulnerability that can be exploited by a burglar. And old, cracked wood is a different vulnerability on that same front door that can increase the chances of storm damage. In other words, think of vulnerabilities as flaws within an asset. Assets can have many different types of vulnerabilities that are an easy target for attackers. |

Yếu tố cuối cùng của kế hoạch bảo mật mà chúng tôi sắp đề cập đến là các lỗ hổng bảo mật.Trong bảo mật, lỗ hổng là điểm yếu có thể bị khai thác bởi mối đe dọa.Ví dụ, một ổ khóa yếu ở cửa trước,là một lỗ hổng có thể bị kẻ trộm khai thác.Và gỗ cũ, nứt nẻ là một lỗ hổng khác trên cùng cánh cửa trước đó.có thể làm tăng nguy cơ thiệt hại do bão.Nói cách khác, hãy coi các lỗ hổng như những sai sót trong một tài sản.Tài sản có thể có nhiều loại lỗ hổng khác nhau dễ dàng trở thành mục tiêucho những kẻ tấn công.

|  |
| --- |
| We'll explore different types of threats and vulnerabilities in greater detail later. For now, just understand that security teams need to account for a wide range of assets, threats, and vulnerabilities to effectively plan for the future. |

Chúng ta sẽ khám phá các loại mối đe dọa khác nhau vàcác lỗ hổng chi tiết hơn sau này.Hiện tại, chỉ cần hiểu rằng các nhóm bảo mật cần phải tính đến nhiều loạitài sản, mối đe dọa và điểm yếu để lập kế hoạch hiệu quả cho tương lai.

***2.3. Understand risks, threats, and vulnerabilities - Hiểu rủi ro, mối đe dọa và lỗ hổng***

|  |
| --- |
| **Understand risks, threats, and vulnerabilities** |

**Hiểu rủi ro, mối đe dọa và lỗ hổng**

|  |
| --- |
| When security events occur, you’ll need to work in close coordination with others to address the problem. Doing so quickly requires clear communication between you and your team to get the job done. |

Khi các sự kiện bảo mật xảy ra, bạn sẽ cần phải phối hợp chặt chẽ với những người khác để giải quyết vấn đề. Làm như vậy một cách nhanh chóng đòi hỏi phải có sự giao tiếp rõ ràng giữa bạn và nhóm của bạn để hoàn thành công việc.

|  |
| --- |
| Previously, you learned about three foundational security terms:   * **Risk**: Anything that can impact the confidentiality, integrity, or availability of an asset * **Threat**: Any circumstance or event that can negatively impact assets * **Vulnerability**: A weakness that can be exploited by a threat |

Trước đây, bạn đã tìm hiểu về ba thuật ngữ bảo mật cơ bản:

* **Rủi ro** : Bất cứ điều gì có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của tài sản
* **Mối đe dọa** : Bất kỳ tình huống hoặc sự kiện nào có thể tác động tiêu cực đến tài sản
* **Tính dễ bị tổn thương** : Điểm yếu có thể bị khai thác bởi mối đe dọa

|  |
| --- |
| These words tend to be used interchangeably in everyday life. But in security, they are used to describe very specific concepts when responding to and planning for security events. In this reading, you’ll identify what each term represents and how they are related. |

Những từ này có xu hướng được sử dụng thay thế cho nhau trong cuộc sống hàng ngày. Nhưng trong bảo mật, chúng được sử dụng để mô tả các khái niệm rất cụ thể khi phản hồi và lập kế hoạch cho các sự kiện bảo mật. Trong bài đọc này, bạn sẽ xác định được mỗi thuật ngữ đại diện cho điều gì và chúng có liên quan với nhau như thế nào.

|  |
| --- |
| **Security risk** |

**Rủi ro bảo mật**

|  |
| --- |
| Security plans are all about how an organization defines risk. However, this definition can vary widely by organization. As you may recall, a **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. Since organizations have particular assets that they value, they tend to differ in how they interpret and approach risk. |

Các kế hoạch bảo mật đều liên quan đến cách tổ chức xác định rủi ro. Tuy nhiên, định nghĩa này có thể khác nhau tùy theo tổ chức. Như bạn có thể nhớ lại, **rủi ro** là bất kỳ điều gì có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính khả dụng của tài sản. Vì các tổ chức có những tài sản cụ thể mà họ coi trọng nên họ có xu hướng khác nhau trong cách giải thích và tiếp cận rủi ro.

|  |
| --- |
| One way to interpret risk is to consider the potential effects that negative events can have on a business. Another way to present this idea is with this calculation: |

Một cách để giải thích rủi ro là xem xét những tác động tiềm tàng mà các sự kiện tiêu cực có thể gây ra đối với doanh nghiệp. Một cách khác để trình bày ý tưởng này là tính toán sau:

|  |
| --- |
| **Likelihood x Impact = Risk** |

**Khả năng xảy ra x Tác động = Rủi ro**

|  |
| --- |
| For example, you risk being late when you drive a car to work. This negative event is more likely to happen if you get a flat tire along the way. And the impact could be serious, like losing your job. All these factors influence how you approach commuting to work every day. The same is true for how businesses handle security risks. |

Ví dụ, bạn có nguy cơ bị trễ khi lái ô tô đi làm. Sự kiện tiêu cực này có nhiều khả năng xảy ra hơn nếu bạn bị xẹp lốp trên đường đi. Và tác động có thể nghiêm trọng, như mất việc. Tất cả những yếu tố này ảnh hưởng đến cách bạn tiếp cận việc đi làm hàng ngày. Điều này cũng đúng với cách doanh nghiệp xử lý rủi ro bảo mật.

|  |
| --- |
| In general, we calculate risk in this field to help:   * Prevent costly and disruptive events * Identify improvements that can be made to systems and processes * Determine which risks can be tolerated * Prioritize the critical assets that require attention |

Nói chung, chúng tôi tính toán rủi ro trong lĩnh vực này để giúp:

* Ngăn chặn các sự kiện tốn kém và gây rối
* Xác định những cải tiến có thể được thực hiện đối với hệ thống và quy trình
* Xác định những rủi ro nào có thể chấp nhận được
* Ưu tiên các tài sản quan trọng cần được chú ý

|  |
| --- |
| The business impact of a negative event will always depend on the asset and the situation. Your primary focus as a security professional will be to focus on the likelihood side of the equation by dealing with certain factors that increase the odds of a problem. |

Tác động kinh doanh của một sự kiện tiêu cực sẽ luôn phụ thuộc vào tài sản và tình hình. Trọng tâm chính của bạn với tư cách là một chuyên gia bảo mật sẽ là tập trung vào khía cạnh khả năng xảy ra của phương trình bằng cách xử lý các yếu tố nhất định làm tăng khả năng xảy ra sự cố.

|  |
| --- |
| **Risk factors** |

**Các yếu tố rủi ro**

|  |
| --- |
| As you’ll discover throughout this course, there are two broad risk factors that you’ll be concerned with in the field:   * Threats * Vulnerabilities |

Như bạn sẽ khám phá trong suốt khóa học này, có hai yếu tố rủi ro chung mà bạn sẽ quan tâm trong lĩnh vực này:

* Các mối đe dọa
* Lỗ hổng

|  |
| --- |
| The risk of an asset being harmed or damaged depends greatly on whether a threat takes advantage of vulnerabilities. |

Rủi ro tài sản bị tổn hại hoặc hư hỏng phụ thuộc rất lớn vào việc liệu mối đe dọa có lợi dụng các lỗ hổng hay không.

|  |
| --- |
| Let’s apply this to the risk of being late to work. A threat would be a nail puncturing your tire, since tires are vulnerable to running over sharp objects. In terms of security planning, you would want to reduce the likelihood of this risk by driving on a clean road. |

Hãy áp dụng điều này vào nguy cơ đi làm muộn. Một mối đe dọa sẽ là một chiếc đinh làm thủng lốp xe của bạn, vì lốp xe dễ bị va vào các vật sắc nhọn. Về mặt lập kế hoạch an ninh, bạn sẽ muốn giảm khả năng xảy ra rủi ro này bằng cách lái xe trên đường sạch sẽ.

|  |
| --- |
| **Categories of threat** |

**Các loại mối đe dọa**

|  |
| --- |
| **Threats** are circumstances or events that can negatively impact assets. There are many different types of threats. However, they are commonly categorized as two types: intentional and unintentional. |

**Mối đe dọa** là những tình huống hoặc sự kiện có thể tác động tiêu cực đến tài sản. Có nhiều loại mối đe dọa khác nhau. Tuy nhiên, chúng thường được phân thành hai loại: cố ý và vô ý.

|  |
| --- |
| For example, an *intentional* threat might be a malicious hacker who gains access to sensitive information by targeting a misconfigured application. An *unintentional* threat might be an employee who holds the door open for an unknown person and grants them access to a restricted area. Either one can cause an event that must be responded to. |

Ví dụ: một mối đe dọa *có chủ ý* có thể là một hacker độc hại có quyền truy cập vào thông tin nhạy cảm bằng cách nhắm mục tiêu vào một ứng dụng bị định cấu hình sai. Một mối đe dọa *vô ý* có thể là một nhân viên giữ cửa mở cho một người không xác định và cấp cho họ quyền vào khu vực hạn chế. Một trong hai có thể gây ra một sự kiện phải được phản hồi.

|  |
| --- |
| **Categories of vulnerability** |

**Các loại lỗ hổng**

|  |
| --- |
| **Vulnerabilities** are weaknesses that can be exploited by threats. There’s a wide range of vulnerabilities, but they can be grouped into two categories: technical and human. |

**Lỗ hổng** là điểm yếu có thể bị khai thác bởi các mối đe dọa. Có rất nhiều lỗ hổng, nhưng chúng có thể được nhóm thành hai loại: kỹ thuật và con người.

|  |
| --- |
| For example, a *technical* vulnerability can be misconfigured software that might give an unauthorized person access to important data. A *human* vulnerability can be a forgetful employee who loses their access card in a parking lot. Either one can lead to risk. |

Ví dụ: lỗ hổng *kỹ thuật* có thể là phần mềm bị định cấu hình sai có thể cấp cho người khác quyền truy cập trái phép vào dữ liệu quan trọng. Điểm yếu của con *người* có thể là một nhân viên hay quên làm mất thẻ ra vào trong bãi đậu xe. Một trong hai có thể dẫn đến rủi ro.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Risks, threats, and vulnerabilities have very specific meanings in security. Knowing the relationship between them can help you build a strong foundation as you grow essential skills and knowledge as a security analyst. This can help you gain credibility in the industry by demonstrating that you have working knowledge of the field. And it signals to your future colleagues that you’re a member of the global security community. |

Rủi ro, mối đe dọa và lỗ hổng có ý nghĩa rất cụ thể trong bảo mật. Biết được mối quan hệ giữa chúng có thể giúp bạn xây dựng nền tảng vững chắc khi bạn phát triển các kỹ năng và kiến ​​thức cần thiết với tư cách là một nhà phân tích bảo mật. Điều này có thể giúp bạn có được sự tín nhiệm trong ngành bằng cách chứng minh rằng bạn có kiến ​​thức làm việc về lĩnh vực này. Và nó báo hiệu cho các đồng nghiệp tương lai của bạn biết rằng bạn là thành viên của cộng đồng an ninh toàn cầu.

***2.4. Tri: Life in asset security - Tri: Cuộc sống an toàn về tài sản***

|  |
| --- |
| I'm Tri, a security engineer at Google. My department is Detection and Response. Let's see, what does my everyday look like? Well, of course I have the free lunch and coffee, which is nice. And then I finally get to my desk and I open up the SIEM to see what kind of exciting events are there for me to look into and what threats there could be out there for me to analyze. Also, I work on improving our analysis for detection of potential threats. So my security passion developed at a young age. I was a victim of a hack, believe it or not. After school every day at that time I would go home and play a computer game. One day I got home, I brought it up and it said, "Your CD key is in use by...", and then it gave some strange name there that I didn't recognize. At first I felt shocked. I had bought this game myself and somebody stole my CD key, but it did provide me this motivation to start to learn how to defend myself. For example, I learned about manual removal of malware, and that became one of my favorite topics. Also, for fun, I started doing some white hat hacker activity against some of my friends. Asset security is a very important field, and there's many varieties of assets that you could be looking into to protect. My favorite part is building the detections that actually have the potential to catch malicious behavior. In asset management security, you have the ability to accurately inventory all of the assets which include IP, user data, employee machines, and to make sure you have a security posture that's on par with what you need. There's always new technology coming on the scene, new hardware, and we are responsible for understanding what potential new threats are out there. Problem solving ability and creative thinking is important in cybersecurity because there's always complex problems, and people need to be able to think outside of the box, think creatively, and think holistically as they approach their solutions to mitigate risks. Cybersecurity is a noble occupation. Many things can happen. Many bad things can happen on the Internet, but we can be there to stand up against it and we can be there to do something about it. We can be there to protect our users, or family members, or friends. That responsibility is heavy. But also, of course, it's a very important mission. And I am proud to be within the security team. |

Tôi là Trí, kỹ sư bảo mật tại Google.Bộ phận của tôi là Phát hiện và Phản hồi.Để xem mỗi ngày của tôi diễn ra như thế nào?Tất nhiên là tôi có bữa trưa và cà phê miễn phí, thật tuyệt.Và cuối cùng tôi cũng đến bàn làm việc của mình và mở SIEM để xemcó những sự kiện thú vị nào để tôi xem xétvà những mối đe dọa nào có thể tồn tại ngoài kia để tôi phân tích.Ngoài ra, tôi còn nỗ lực cải thiện khả năng phân tích của mình để phát hiện các mối đe dọa tiềm ẩn.Vì vậy, niềm đam mê bảo mật của tôi đã phát triển từ khi còn trẻ.Tôi là nạn nhân của một vụ hack, tin hay không tùy bạn.Sau giờ học hàng ngày vào thời điểm đó tôi sẽ về nhà và chơi game trên máy tính.Một ngày nọ, tôi về nhà, tôi mang nó lên và nó nói: "Khóa CD của bạn đang được sử dụng bởi...",rồi nó đặt một cái tên lạ nào đó mà tôi không nhận ra.Lúc đầu tôi cảm thấy sốc.Tôi đã tự mua trò chơi này và ai đó đã lấy trộm CD key của tôi,nhưng nó đã mang lại cho tôi động lực để bắt đầu học cách tự vệ.Ví dụ: tôi đã tìm hiểu về cách loại bỏ phần mềm độc hại theo cách thủ công,và điều đó đã trở thành một trong những chủ đề yêu thích của tôi.Ngoài ra, để giải trí, tôi bắt đầu làm hacker mũ trắnghoạt động chống lại một số người bạn của tôi.Bảo đảm tài sản là một lĩnh vực rất quan trọng,và có nhiều loại tài sản mà bạn có thể xem xét để bảo vệ.Phần yêu thích của tôi là xây dựng các phát hiệnthực sự có khả năng phát hiện hành vi nguy hiểm.Trong bảo mật quản lý tài sản, bạn có khả năngđể kiểm kê chính xáctất cả các tài sản bao gồm IP, dữ liệu người dùng,máy móc của nhân viên và để đảm bảo bạn cómột trạng thái bảo mật ngang bằng với những gì bạn cần.Luôn có công nghệ mới xuất hiện, phần cứng mới,và chúng tôi có trách nhiệm tìm hiểu những mối đe dọa mới tiềm ẩn hiện có.Khả năng giải quyết vấn đề và tư duy sáng tạorất quan trọng trong an ninh mạng vì luôn có những vấn đề phức tạp,và mọi người cần có khả năng suy nghĩ sáng tạo,và suy nghĩ một cách tổng thể khi họ tiếp cậngiải pháp của họ để giảm thiểu rủi ro.An ninh mạng là một nghề cao quý.Nhiều điều có thể xảy ra.Nhiều điều tồi tệ có thể xảy ra trên Internet,nhưng chúng ta có thể ở đó để đứng lên chống lại nóvà chúng ta có thể ở đó để làm điều gì đó về nó.Chúng tôi có thể ở đó để bảo vệ người dùng, thành viên gia đình hoặc bạn bè của mình.Trách nhiệm đó thật nặng nề.Nhưng tất nhiên, đó cũng là một nhiệm vụ rất quan trọng.Và tôi tự hào được ở trong đội an ninh.

***2.5. Security starts with asset classification - Bảo mật bắt đầu bằng việc phân loại tài sản***

|  |
| --- |
| It can be really stressful when you have trouble finding something important. You're late to an appointment and can't find your keys! We all find ourselves in situations like these at one time or another. Believe it or not, organizations deal with the same kind of trouble. Take a few seconds to think of the number of important assets you have nearby. I'm thinking of my phone, wallet, and keys, for example. |

Nó có thể thực sự căng thẳngkhi bạn gặp khó khăn trong việc tìm kiếm thứ gì đó quan trọng.Bạn đến muộn cuộc hẹn và không thể tìm thấy chìa khóa của mình!Tất cả chúng ta đều thấy mình trongnhững tình huống như thế này lúc này hay lúc khác.Dù bạn có tin hay không, các tổ chứcđối phó với cùng một loại rắc rối.Hãy dành vài giây để nghĩ về số lượngtài sản quan trọng bạn có ở gần.Tôi đang nghĩ về điện thoại của mình,Ví và chìa khóa chẳng hạn.

|  |
| --- |
| Next, imagine that you've just joined a security team for a small online retailer. The company has been growing over the past few years, adding more and more customers. As a result, they're expanding their security department to protect the increasing numbers of assets they have. Let's say each of you are responsible for 10 assets. That's a lot of assets! Even in this small business setting, that's an incredible amount of things that need protecting. |

Tiếp theo, hãy tưởng tượng rằng bạn vừa tham giamột nhóm bảo mật cho một nhà bán lẻ trực tuyến nhỏ.Công ty đã phát triển trong vài năm qua,ngày càng có thêm nhiều khách hàng.Kết quả là họ đang mở rộng bộ phận an ninh của mìnhđể bảo vệ số lượng tài sản ngày càng tăng mà họ có.Giả sử mỗi bạn chịu trách nhiệm về 10 tài sản.Đó là rất nhiều tài sản!Ngay cả trong môi trường kinh doanh nhỏ này,đó là một số lượng đáng kinh ngạcnhững thứ cần bảo vệ.

|  |
| --- |
| A fundamental truth of security is you can only protect the things you account for. Asset management is the process of tracking assets and the risks that affects them. All security plans revolve around asset management. Recall that assets include any item perceived as having value to an organization. Equipment, data, and intellectual property are just a few of the wide range of assets businesses want to protect. A critical part of every organization's security plan is keeping track of its assets. |

Sự thật cơ bản về bảo mật là bạnchỉ có thể bảo vệ những thứ bạn chiếm giữ.Quản lý tài sản là quá trìnhtheo dõi tài sản và những rủi ro ảnh hưởng đến chúng.Tất cả các kế hoạch bảo mật đều xoay quanh việc quản lý tài sản.Hãy nhớ rằng tài sản bao gồmbất kỳ mục nào được coi là có giá trị đối với một tổ chức.Thiết bị, dữ liệu và sở hữu trí tuệ chỉ là mộtmột vài trong số rất nhiềutài sản mà doanh nghiệp muốn bảo vệ.Một phần quan trọng củakế hoạch bảo mật của mọi tổ chứcđang theo dõi tài sản của mình.

|  |
| --- |
| Asset management starts with having an asset inventory, a catalog of assets that need to be protected. This is a central part of protecting organizational assets. Without this record, organizations run the risk of losing track of all that's important to them. A good way to think of asset inventories is as a shepherd protecting sheep. Having an accurate count of the number of sheep help in a lot of ways. For example, it will be easier to allocate resources, like food, to take care of them. Another benefit of asset inventory might be that you'd get an alert if one of them goes missing. |

Quản lý tài sản bắt đầu bằng việc kiểm kê tài sản,danh mục tài sản cần được bảo vệ.Đây là phần trung tâmcủa việc bảo vệ tài sản của tổ chức.Nếu không có hồ sơ này, các tổ chức sẽ hoạt độngnguy cơ mất dấu tất cả những gì quan trọng đối với họ.Một cách tốt để nghĩ vềviệc kiểm kê tài sản giống như người chăn cừu bảo vệ đàn cừu.Có con số thống kê chính xác về số lượngcừu giúp đỡ bằng nhiều cách.Ví dụ, sẽ dễ dàng hơn đểphân bổ các nguồn lực, như thực phẩm, để chăm sóc chúng.Một lợi ích khác của việc kiểm kê tài sảncó thể bạn sẽ nhận được cảnh báonếu một trong số họ bị mất tích.

|  |
| --- |
| Once more, think of the important assets you have nearby. Just like me, you're probably able to rate them according to the level of importance. I would rank my wallet ahead of my shoes, for example. In security, this practice is known as asset classification. In general, asset classification is the practice of labeling assets based on the sensitivity and importance to an organization. Organizations label assets differently. Many of them follow a basic classification scheme: public, internal-only, confidential, and restricted. |

Một lần nữa hãy suy nghĩtrong số những tài sản quan trọng bạn có ở gần.Cũng giống như tôi, có lẽ bạn có thểđánh giá chúng theo mức độ quan trọng.Ví dụ, tôi sẽ xếp ví của mình lên trên giày.Trong lĩnh vực bảo mật, cách làm này làđược gọi là phân loại tài sản.Nhìn chung, việc phân loại tài sảnlà việc thực hành dán nhãntài sản dựa trên độ nhạyvà tầm quan trọng đối với một tổ chức.Các tổ chức dán nhãn tài sản khác nhau.Nhiều người trong số họ tuân theo sơ đồ phân loại cơ bản:công khai, chỉ dành cho nội bộ,bí mật và bị hạn chế.

|  |
| --- |
| Public assets can be shared with anyone. Internal-only can be shared with anyone in the organization but should not be shared outside of it. And confidential assets should only be accessed by those working on a specific project. Assets classified as restricted are typically highly sensitive and must be protected. Assets with this label are considered need-to-know. Examples include intellectual property and health or payment information. For example, a growing online retailer might mark internal emails about a new product as confidential because those working on the new product should know about it. They might also label the doors at their offices with the restricted sign to keep everyone out who doesn't have a specific reason to be in there. These are just a couple of everyday examples that you may be familiar with from your prior experience. |

Tài sản công có thể được chia sẻ với bất cứ ai.Chỉ có thể chia sẻ nội bộ với bất kỳ ai trongtổ chức nhưng không nên chia sẻ ra bên ngoài tổ chức đó.Và tài sản bí mật chỉ nên đượcđược truy cập bởi những người làm việc trên một dự án cụ thể.Tài sản được phân loại là bị hạn chếthường rất nhạy cảm và phải được bảo vệ.Nội dung có nhãn này được coi là nội dung cần biết.Ví dụ bao gồm sở hữu trí tuệvà thông tin sức khỏe hoặc thanh toán.Ví dụ: một nhà bán lẻ trực tuyến đang phát triểncó thể đánh dấu các email nội bộ vềmột sản phẩm mới được bảo mật vì những sản phẩm đólàm việc trên sản phẩm mới nên biết về nó.Họ cũng có thể dán nhãn cho các cánh cửa ởvăn phòng của họ có biển cấmđể giữ những người không làm vậy tránh xacó lý do cụ thể để vào đó.Đây chỉ là một vài ví dụ hàng ngày mà bạncó thể quen thuộc với kinh nghiệm trước đây của bạn.

|  |
| --- |
| For the most part, classification determines whether an asset can be disclosed, altered, or destroyed. Asset management is a continuous process, one that helps uncover unexpected gaps in security for potential risks. Keeping track of all that's important to a organization is an essential part of security planning. |

Phần lớn, việc phân loại quyết định liệumột tài sản có thể được tiết lộ, thay đổi hoặc tiêu hủy.Quản lý tài sản là một quá trình liên tục,một thứ giúp khám phánhững lỗ hổng bảo mật bất ngờ trước những rủi ro tiềm ẩn.Theo dõi tất cả những gì quan trọng đối vớimột tổ chức là một phần thiết yếu của kế hoạch an ninh.

***2.6. Common classification requirements - Yêu cầu phân loại chung***

|  |
| --- |
| **Common classification requirements** |

**Yêu cầu phân loại chung**

|  |
| --- |
| Asset management is the process of tracking assets and the risks that affect them. The idea behind this process is simple: you can only protect what you know you have. |

**Quản lý tài sản** là quá trình theo dõi tài sản và những rủi ro ảnh hưởng đến chúng. Ý tưởng đằng sau quá trình này rất đơn giản: bạn chỉ có thể bảo vệ những gì bạn biết mình có.

|  |
| --- |
| Previously, you learned that identifying, tracking, and classifying assets are all important parts of asset management. In this reading, you’ll learn more about the purpose and benefits of asset classification, including common classification levels. |

Trước đây, bạn đã biết rằng việc xác định, theo dõi và phân loại tài sản đều là những phần quan trọng của việc quản lý tài sản. Trong bài đọc này, bạn sẽ tìm hiểu thêm về mục đích và lợi ích của việc phân loại tài sản, bao gồm các cấp độ phân loại phổ biến.



|  |
| --- |
| **Why asset management matters** |

**Tại sao quản lý tài sản lại quan trọng**

|  |
| --- |
| Keeping assets safe requires a workable system that helps businesses operate smoothly. Setting these systems up requires having detailed knowledge of the assets in an environment. For example, a bank needs to have money available each day to serve its customers. Equipment, devices, and processes need to be in place to ensure that money is available and secure from unauthorized access. |

Việc giữ tài sản được an toàn đòi hỏi một hệ thống khả thi giúp doanh nghiệp vận hành trơn tru. Việc thiết lập các hệ thống này đòi hỏi phải có kiến ​​thức chi tiết về tài sản trong môi trường. Ví dụ, một ngân hàng cần có sẵn tiền mỗi ngày để phục vụ khách hàng. Cần phải có thiết bị, dụng cụ và quy trình để đảm bảo rằng tiền luôn sẵn có và an toàn khỏi sự truy cập trái phép.

|  |
| --- |
| Organizations protect a variety of different assets. Some examples might include:   * Digital assets such as customer data or financial records. * Information systems that process data, like networks or software. * Physical assets which can include facilities, equipment, or supplies. * Intangible assets such as brand reputation or intellectual property. |

Các tổ chức bảo vệ nhiều loại tài sản khác nhau. Một số ví dụ có thể bao gồm:

* Tài sản kỹ thuật số như dữ liệu khách hàng hoặc hồ sơ tài chính.
* Hệ thống thông tin xử lý dữ liệu, như mạng hoặc phần mềm.
* Tài sản vật chất có thể bao gồm cơ sở vật chất, thiết bị hoặc vật tư.
* Tài sản vô hình như danh tiếng thương hiệu hoặc tài sản trí tuệ.

|  |
| --- |
| Regardless of its type, every asset should be classified and accounted for. As you may recall, **asset classification** is the practice of labeling assets based on sensitivity and importance to an organization. Determining each of those two factors varies, but the sensitivity and importance of an asset typically requires knowing the following:   * What you have * Where it is * Who owns it, and * How important it is |

Bất kể loại tài sản nào, mọi tài sản đều phải được phân loại và hạch toán. Như bạn có thể nhớ lại, phân loại tài sản là phương pháp dán nhãn tài sản dựa trên mức độ nhạy cảm và tầm quan trọng đối với một tổ chức. Việc xác định từng yếu tố trong số hai yếu tố đó là khác nhau, nhưng độ nhạy và tầm quan trọng của tài sản thường đòi hỏi phải biết những điều sau:

* Bạn có gì
* Nó ở đâu
* Ai sở hữu nó và
* Nó quan trọng thế nào

|  |
| --- |
| An organization that classifies its assets does so based on these characteristics. Doing so helps them determine the sensitivity and value of an asset. |

Một tổ chức phân loại tài sản của mình dựa trên những đặc điểm này. Làm như vậy sẽ giúp họ xác định được độ nhạy cảm và giá trị của một tài sản.

|  |
| --- |
| **Common asset classifications** |

**Phân loại tài sản chung**

|  |
| --- |
| Asset classification helps organizations implement an effective risk management strategy. It also helps them prioritize security resources, reduce IT costs, and stay in compliance with legal regulations. |

Phân loại tài sản giúp tổ chức thực hiện chiến lược quản lý rủi ro hiệu quả. Nó cũng giúp họ ưu tiên các nguồn lực bảo mật, giảm chi phí CNTT và tuân thủ các quy định pháp luật.

|  |
| --- |
| The most common classification scheme is: restricted, confidential, internal-only, and public. |

Sơ đồ phân loại phổ biến nhất là: hạn chế, bí mật, chỉ nội bộ và công khai.

|  |
| --- |
| * **Restricted** is the highest level. This category is reserved for incredibly sensitive assets,  like need-to-know information. * **Confidential** refers to assets whose disclosure may lead to a significant negative impact on an organization. * **Internal-only** describes assets that are available to employees and business partners. * **Public** is the lowest level of classification. These assets have no negative consequences to the organization if they’re released. |

* **Hạn chế** là mức cao nhất. Danh mục này được dành riêng cho những nội dung cực kỳ nhạy cảm, như thông tin cần biết.
* **Bí mật** đề cập đến tài sản mà việc tiết lộ có thể dẫn đến tác động tiêu cực đáng kể đến tổ chức.
* **Chỉ nội bộ** mô tả các tài sản có sẵn cho nhân viên và đối tác kinh doanh.
* **Công khai** là cấp độ phân loại thấp nhất. Những tài sản này không gây hậu quả tiêu cực cho tổ chức nếu chúng được phát hành.

|  |
| --- |
| How this scheme is applied depends greatly on the characteristics of an asset. It might surprise you to learn that identifying an asset’s owner is sometimes the most complicated characteristic to determine. |

Việc áp dụng kế hoạch này như thế nào phụ thuộc rất lớn vào đặc điểm của tài sản. Bạn có thể ngạc nhiên khi biết rằng việc xác định chủ sở hữu tài sản đôi khi là đặc điểm phức tạp nhất cần xác định.

|  |
| --- |
| **Note:** Although many organizations adopt this classification scheme, there can be variability at the highest levels. For example, government organizations label their most sensitive assets as confidential instead of restricted. |

**Lưu ý:** Mặc dù nhiều tổ chức áp dụng sơ đồ phân loại này nhưng vẫn có thể có sự khác biệt ở cấp độ cao nhất. Ví dụ: các tổ chức chính phủ dán nhãn tài sản nhạy cảm nhất của họ là bí mật thay vì bị hạn chế.

|  |
| --- |
| **Challenges of classifying information** |

**Những thách thức của việc phân loại thông tin**

|  |
| --- |
| Identifying the owner of certain assets is straightforward, like the owner of a building. Other types of assets can be trickier to identify. This is especially true when it comes to information. |

Việc xác định chủ sở hữu của một số tài sản nhất định rất đơn giản, giống như chủ sở hữu của một tòa nhà. Các loại tài sản khác có thể khó xác định hơn. Điều này đặc biệt đúng khi nói đến thông tin.

|  |
| --- |
| For example, a business might issue a laptop to one of its employees to allow them to work remotely. You might assume the business is the asset owner in this situation. But, what if the employee uses the laptop for personal matters, like storing their photos? |

Ví dụ: một doanh nghiệp có thể cấp máy tính xách tay cho một nhân viên của mình để cho phép họ làm việc từ xa. Bạn có thể cho rằng doanh nghiệp là chủ sở hữu tài sản trong tình huống này. Tuy nhiên, điều gì sẽ xảy ra nếu nhân viên sử dụng máy tính xách tay cho các vấn đề cá nhân, như lưu trữ ảnh của họ?

|  |
| --- |
| Ownership is just one characteristic that makes classifying information a challenge. Another concern is that information can have multiple classification values at the same time. For example, consider a letter addressed to you in the mail. The letter contains some public information that’s okay to share, like your name. It also contains fairly confidential pieces of information that you’d rather only be available to certain people, like your address. You’ll learn more about how these challenges are addressed as you continue through the program. |

Quyền sở hữu chỉ là một đặc điểm khiến việc phân loại thông tin trở thành một thách thức. Một mối quan tâm khác là thông tin có thể có nhiều giá trị phân loại cùng một lúc. Ví dụ, hãy xem xét một lá thư gửi cho bạn qua đường bưu điện. Bức thư chứa một số thông tin công khai có thể chia sẻ, chẳng hạn như tên của bạn. Nó cũng chứa những thông tin khá bí mật mà bạn chỉ muốn cung cấp cho một số người nhất định, chẳng hạn như địa chỉ của bạn. Bạn sẽ tìm hiểu thêm về cách giải quyết những thách thức này khi tiếp tục tham gia chương trình.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Every business is different. Each business will have specific requirements to address when devising their security strategy. Knowing why and how businesses classify their assets is an important skill to have as a security professional. Information is one of the most important assets in the world. As a cybersecurity professional, you will be closely involved with protecting information from damage, disclosure, and misuse. Recognizing the challenges that businesses face classifying this type of asset is a key to helping them solve their security needs. |

Mỗi doanh nghiệp đều khác nhau. Mỗi doanh nghiệp sẽ có những yêu cầu cụ thể cần giải quyết khi xây dựng chiến lược bảo mật của mình. Biết lý do và cách thức các doanh nghiệp phân loại tài sản của mình là một kỹ năng quan trọng cần có với tư cách là một chuyên gia bảo mật. Thông tin là một trong những tài sản quan trọng nhất trên thế giới. Là một chuyên gia an ninh mạng, bạn sẽ tham gia chặt chẽ vào việc bảo vệ thông tin khỏi bị hư hại, tiết lộ và sử dụng sai mục đích. Nhận thức được những thách thức mà doanh nghiệp gặp phải trong việc phân loại loại tài sản này là chìa khóa giúp họ giải quyết nhu cầu bảo mật.

***2.7. Test your knowledge: Introduction to assets - Kiểm tra kiến ​​thức của bạn: Giới thiệu về tài sản***

***2.8. Activity: Classify the assets connected to a home network - Hoạt động: Phân loại các tài sản được kết nối với mạng gia đình***

|  |
| --- |
| **Activity Overview**  In this activity, you will classify assets connected to a home office network.  Asset management is a critical part of every organization's security plan. Remember that **asset management** is the process of tracking assets and the risks that affect them. Effective asset management starts with creating an **asset inventory**, or a catalog of assets that need to be protected. Then, it involves classifying assets based on their level of importance and sensitivity to risk.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ phân loại các tài sản được kết nối với mạng văn phòng tại nhà.

Quản lý tài sản là một phần quan trọng trong kế hoạch bảo mật của mọi tổ chức. Hãy nhớ rằng **quản lý tài sản** là quá trình theo dõi tài sản và những rủi ro ảnh hưởng đến chúng. Quản lý tài sản hiệu quả bắt đầu bằng việc tạo **bản kiểm kê tài sản** hoặc danh mục tài sản cần được bảo vệ. Sau đó, nó liên quan đến việc phân loại tài sản dựa trên mức độ quan trọng và độ nhạy cảm với rủi ro của chúng.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the following scenario. Then, complete the step-by-step instructions.  One of the most valuable assets in the world today is information. Most information is accessed over a network. There tend to be a variety of devices connected to a network and each is a potential entry point to other assets.  An inventory of network devices can be a useful asset management tool. An inventory can highlight sensitive assets that require extra protection. |

**Kịch bản**

Xem lại tình huống sau. Sau đó, hoàn thành các hướng dẫn từng bước.

Một trong những tài sản quý giá nhất trên thế giới ngày nay là thông tin. Hầu hết thông tin được truy cập qua mạng. Có xu hướng có nhiều loại thiết bị được kết nối với mạng và mỗi thiết bị đều là điểm truy cập tiềm năng vào các tài sản khác.

Việc kiểm kê các thiết bị mạng có thể là một công cụ quản lý tài sản hữu ích. Khoảng không quảng cáo có thể làm nổi bật những tài sản nhạy cảm cần được bảo vệ thêm.

|  |
| --- |
| You’re operating a small business from your home and must create an inventory of your network devices. This will help you determine which ones contain sensitive information that require extra protection. |

Bạn đang điều hành một doanh nghiệp nhỏ tại nhà và phải tạo một kho lưu trữ các thiết bị mạng của mình. Điều này sẽ giúp bạn xác định những thông tin nào chứa thông tin nhạy cảm cần được bảo vệ thêm.

|  |
| --- |
| To do this, you will start by identifying three devices that have access to your home network. This might include devices such as:   * Desktop or laptop computers * Smartphones * Smart home devices * Game consoles * Storage devices or servers * Video streaming devices |

Để thực hiện việc này, bạn sẽ bắt đầu bằng việc xác định ba thiết bị có quyền truy cập vào mạng gia đình của bạn. Điều này có thể bao gồm các thiết bị như:

* Máy tính để bàn hoặc máy tính xách tay
* Điện thoại thông minh
* Thiết bị nhà thông minh
* Trình điều khiển game
* Thiết bị lưu trữ hoặc máy chủ
* Thiết bị truyền phát video

|  |
| --- |
| Then, you’ll list important characteristics of each device such as its owner, location, and type. Finally, you will assign each device a level of sensitivity based on how important it is to protect. |

Sau đó, bạn sẽ liệt kê các đặc điểm quan trọng của từng thiết bị như chủ sở hữu, vị trí và loại thiết bị. Cuối cùng, bạn sẽ chỉ định cho mỗi thiết bị một mức độ nhạy cảm dựa trên tầm quan trọng của việc bảo vệ thiết bị đó.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions and answer the end-of-activity question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

Làm theo hướng dẫn và trả lời câu hỏi kết thúc hoạt động để hoàn thành hoạt động. Sau đó, chuyển sang mục khóa học tiếp theo để so sánh bài tập của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the link below and select *Use Template*.  Link to template: [Home asset inventory](https://docs.google.com/spreadsheets/d/1x2MoqRGpK1WFj3kg5gPjCVTczWzQ0odc1LrO-ZZbIys/template/preview?resourcekey=0-IWZFZN2pMTG6JbJcaCc7ig) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn *Sử dụng Mẫu* .

Liên kết đến mẫu:[Kiểm kê tài sản nhà](https://docs.google.com/spreadsheets/d/1x2MoqRGpK1WFj3kg5gPjCVTczWzQ0odc1LrO-ZZbIys/template/preview?resourcekey=0-IWZFZN2pMTG6JbJcaCc7ig)

|  |
| --- |
| **Step 2: Identify assets**  In the asset inventory spreadsheet, find the **Asset** column header. Consider the devices that may be connected to the home network. Examine devices in the scenario graphic to help you brainstorm.  Choose three devices that are not already listed in the spreadsheet and add them to the empty rows in the **Asset** column.  ***Note****: A few devices, like a network router, desktop, and a guest smartphone have already been added for your reference.* |

**Bước 2: Xác định tài sản**

Trong bảng tính kiểm kê tài sản, hãy tìm tiêu đề cột **Tài sản** . Hãy xem xét các thiết bị có thể được kết nối với mạng gia đình. Kiểm tra các thiết bị trong đồ họa kịch bản để giúp bạn động não.

Chọn ba thiết bị chưa được liệt kê trong bảng tính và thêm chúng vào các hàng trống trong cột **Nội dung** .

***Lưu ý*** *: Một số thiết bị như bộ định tuyến mạng, máy tính để bàn và điện thoại thông minh dành cho khách đã được thêm vào để bạn tham khảo.*

|  |
| --- |
| **Step 3: Fill in the characteristics of each asset**  List important characteristics, including **Network access, Owner**, and **Location** for each asset that you’ve identified.  Here’s an explanation of each characteristic:   * **Network access** describes how often the device is connected to the network. * **Owner** describes the person responsible for the device. * **Location** describes where the device is located in relation to the router. |

**Bước 3: Điền đặc điểm của từng tài sản**

Liệt kê các đặc điểm quan trọng, bao gồm **Quyền truy cập mạng, Chủ sở hữu** và **Vị trí** cho từng nội dung mà bạn đã xác định.

Dưới đây là giải thích về từng đặc điểm:

* **Truy cập mạng** mô tả tần suất thiết bị được kết nối với mạng.
* **Chủ sở hữu** mô tả người chịu trách nhiệm về thiết bị.
* **Vị trí** mô tả vị trí của thiết bị so với bộ định tuyến.

|  |
| --- |
| **Step 4: Evaluate the access of network devices**  Review the information that you’ve listed in the **Network access, Owner**, and **Location** columns.  In the **Notes** column, record 1 or 2 details or characteristics of each device. Do this by asking yourself questions about each:   * *What kind of information is stored on the device?* * *How does it connect to the network?* * *Is the owner careful about securing it?*   For example, the desktop computer contains sensitive information, like photos, that only the owner should have access to. In contrast, the network router uses one frequency for smart home devices and another for all other devices.  ***Note:*** *Keep in mind that there might be some variation within each category. Try to identify details that could impact the confidentiality, integrity, or availability of information that’s connected to the network.* |

**Bước 4: Đánh giá khả năng truy cập của các thiết bị mạng**

Xem lại thông tin bạn đã liệt kê trong các cột **Truy cập mạng, Chủ sở hữu** và **Vị trí** .

Tại cột **Ghi chú** ghi 1 hoặc 2 thông tin chi tiết hoặc đặc điểm của từng thiết bị. Hãy thực hiện việc này bằng cách tự đặt câu hỏi cho từng vấn đề:

* *Loại thông tin nào được lưu trữ trên thiết bị?*
* *Làm thế nào nó kết nối với mạng?*
* *Chủ sở hữu có cẩn thận trong việc bảo vệ nó không?*

Ví dụ: máy tính để bàn chứa thông tin nhạy cảm, như ảnh, mà chỉ chủ sở hữu mới có quyền truy cập. Ngược lại, bộ định tuyến mạng sử dụng một tần số cho các thiết bị nhà thông minh và một tần số khác cho tất cả các thiết bị khác.

***Lưu ý:*** *Hãy nhớ rằng có thể có một số biến thể trong mỗi danh mục. Cố gắng xác định các chi tiết có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của thông tin được kết nối với mạng.*

|  |
| --- |
| **Step 5: Classify the sensitivity of network devices**  It’s time to classify assets based on the information you’ve collected. Do this by thinking about how an asset could impact your business if its security was compromised:   * *What types of information would be disclosed or stolen?* * *Could an attacker alter information on the device?* * *What would happen to the business if this information were destroyed?*   For example, the network router is classified as confidential because the owner has granted limited access to the device to specific users.  Find the **Sensitivity** column in the asset inventory. Type one of the four levels of sensitivity you previously learned about.  ***Note:*** *You can use the Categories table as a guide for choosing an appropriate classification.* |

**Bước 5: Phân loại độ nhạy của thiết bị mạng**

Đã đến lúc phân loại nội dung dựa trên thông tin bạn đã thu thập. Hãy thực hiện việc này bằng cách suy nghĩ xem một tài sản có thể tác động như thế nào đến doanh nghiệp của bạn nếu tính bảo mật của tài sản đó bị xâm phạm:

* *Những loại thông tin nào sẽ bị tiết lộ hoặc bị đánh cắp?*
* *Kẻ tấn công có thể thay đổi thông tin trên thiết bị không?*
* *Điều gì sẽ xảy ra với doanh nghiệp nếu thông tin này bị tiêu hủy?*

Ví dụ: bộ định tuyến mạng được phân loại là bí mật vì chủ sở hữu đã cấp quyền truy cập hạn chế vào thiết bị cho những người dùng cụ thể.

Tìm cột **Độ nhạy** trong kho tài sản. Nhập một trong bốn mức độ nhạy cảm mà bạn đã tìm hiểu trước đây.

***Lưu ý:*** *Bạn có thể sử dụng bảng Danh mục làm hướng dẫn để chọn cách phân loại thích hợp.*

|  |
| --- |
| **Pro Tip: Save the template**  Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers. |

**Mẹo chuyên nghiệp: Lưu mẫu**

Cuối cùng, hãy nhớ lưu một bản sao trống của mẫu bạn đã sử dụng để hoàn thành hoạt động này. Bạn có thể sử dụng nó để thực hành thêm hoặc trong các dự án chuyên nghiệp của mình. Những mẫu này sẽ giúp bạn vượt qua quá trình suy nghĩ và thể hiện kinh nghiệm của mình với các nhà tuyển dụng tiềm năng.

|  |
| --- |
| **What to Include in Your Response**  Be sure to include the following elements in your completed activity:   * List of 3 devices on the home network * List network access, owner, and location for each device * 1–2 notes on network access * A sensitivity classification |

**Những gì cần bao gồm trong phản hồi của bạn**

Hãy đảm bảo bao gồm các yếu tố sau trong hoạt động đã hoàn thành của bạn:

* Danh sách 3 thiết bị trong mạng gia đình
* Liệt kê quyền truy cập mạng, chủ sở hữu và vị trí cho từng thiết bị
* 1–2 lưu ý khi truy cập mạng
* Phân loại độ nhạy

***2.9. Activity Exemplar: Classify the assets connected to a home network - Ví dụ về hoạt động: Phân loại các tài sản được kết nối với mạng gia đình***

|  |
| --- |
| **Activity Exemplar: Classify the assets connected to a home network** |

**Ví dụ về hoạt động: Phân loại các tài sản được kết nối với mạng gia đình**

|  |
| --- |
| Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link and select *Use Template*.  Link to exemplar: [Home asset inventory exemplar](https://docs.google.com/spreadsheets/d/1kdMs5ejteq9ZyH9j4pdvSO2kSOVGeS5hKa4OWGrvlCU/template/preview#gid=0) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Ví dụ về kiểm kê tài sản nhà](https://docs.google.com/spreadsheets/d/1kdMs5ejteq9ZyH9j4pdvSO2kSOVGeS5hKa4OWGrvlCU/template/preview#gid=0)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed asset inventory. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.  ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your asset inventory lists the common characteristics of network connected devices and evaluates them based on their level of sensitivity.*  The exemplar uses detail from the given scenario and adheres to the following guidelines:   * Identify 3 devices on the home network * List network access, owner, and location details for each device * Include 1–2 notes on network access * Classify each asset based on level of sensitivity   The exemplar only lists devices with network access because that fits within the scope of this scenario. However, asset inventories might include non-network devices. For example, a homeowner might also keep track of physical assets like a safe or digital assets like family videos.  Classifying assets based on their level of importance can be subjective. Much of asset classification depends on identifying an asset's owner, their location, and other important characteristics. This information should be evaluated before determining who should have access to an asset and what they are authorized to do. Remember, classification helps determine the level of impact an asset can have on a business if it were disclosed, altered, or destroyed. |

**Đánh giá mẫu mực**

So sánh mẫu với bản kiểm kê tài sản đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong suốt khóa học.

***Lưu ý:*** *Ví dụ thể hiện một cách khả thi để hoàn thành hoạt động. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là kho tài sản của bạn liệt kê các đặc điểm chung của các thiết bị được kết nối mạng và đánh giá chúng dựa trên mức độ nhạy cảm của chúng.*

Ví dụ mẫu sử dụng chi tiết từ tình huống nhất định và tuân thủ các nguyên tắc sau:

* Nhận dạng 3 thiết bị trong mạng gia đình
* Liệt kê chi tiết quyền truy cập mạng, chủ sở hữu và vị trí cho từng thiết bị
* Bao gồm 1–2 lưu ý khi truy cập mạng
* Phân loại từng tài sản dựa trên mức độ nhạy cảm

Ví dụ mẫu chỉ liệt kê các thiết bị có quyền truy cập mạng vì điều đó phù hợp với phạm vi của trường hợp này. Tuy nhiên, việc kiểm kê tài sản có thể bao gồm các thiết bị không có mạng. Ví dụ: chủ nhà cũng có thể theo dõi các tài sản vật chất như két sắt hoặc tài sản kỹ thuật số như video gia đình.

Việc phân loại tài sản dựa trên mức độ quan trọng của chúng có thể mang tính chủ quan. Phần lớn việc phân loại tài sản phụ thuộc vào việc xác định chủ sở hữu tài sản, vị trí của họ và các đặc điểm quan trọng khác. Thông tin này cần được đánh giá trước khi xác định ai sẽ có quyền truy cập vào tài sản và họ được phép làm gì. Hãy nhớ rằng, việc phân loại giúp xác định mức độ tác động mà một tài sản có thể gây ra đối với doanh nghiệp nếu tài sản đó bị tiết lộ, thay đổi hoặc phá hủy.

|  |
| --- |
| **Key Takeaways** |

**Bài học chính**

|  |
| --- |
| Having an inventory of devices on your home network is a useful way to protect your personal assets. It’s also a useful artifact that you can show to prospective employers when interviewing for security analyst positions. Resources like this demonstrate your security mindset and ability to think critically about asset vulnerabilities. |

Có một danh sách kiểm kê thiết bị trên mạng gia đình là một cách hữu ích để bảo vệ tài sản cá nhân của bạn. Nó cũng là một tài liệu hữu ích mà bạn có thể trình bày cho các nhà tuyển dụng tiềm năng khi phỏng vấn vị trí nhà phân tích bảo mật. Những tài nguyên như thế này thể hiện tư duy bảo mật và khả năng suy nghĩ nghiêm túc của bạn về các lỗ hổng tài sản.

**3. Digital and physical assets – Tài sản kỹ thuật số và vật chất**

***3.1. Assets in a digital world - Tài sản trong thế giới kỹ thuật số***

|  |
| --- |
| Welcome back! We've covered a lot of information so far. I hope you're having as much fun exploring the role of security as I am! We've explored what organizational assets are and why they need protection. You've also gotten a sense of the tremendous amount of assets security teams protect. Previously, we began examining security asset management and the importance of keeping track of everything that's important to an organization. Security teams classify assets based on value. Next, let's expand our security mindset and think about this question. What exactly is valuable about an asset? |

Chào mừng trở lại! Chúng tôi đã bao gồm rất nhiều thông tin cho đến nay.Tôi hi vọng bạn cũng có nhiều niềm vui như vậykhám phá vai trò của an ninh như tôi!Chúng tôi đã khám phá những tài sản của tổ chứclà gì và tại sao họ cần được bảo vệ.Bạn cũng đã có cảm giácsố lượng lớn tài sản mà đội an ninh bảo vệ.Trước đó, chúng tôi đã bắt đầukiểm tra việc quản lý tài sản bảo đảm vàtầm quan trọng của việc theo dõimọi thứ quan trọng đối với một tổ chức.Đội bảo mật phân loại tài sản dựa trên giá trị.Tiếp theo, hãy mở rộngtư duy bảo mật của chúng ta và suy nghĩ về câu hỏi này.Chính xác thì điều gì có giá trị về một tài sản?

|  |
| --- |
| These days, the answer is often information. Most information is in a digital form. We call this data. Data is information that is translated, processed, or stored by a computer. We live in a connected world. Billions of devices around the world are linked to the internet and are exchanging data with each other all the time. In fact, millions of pieces of data are being passed to your device right now! When compared to physical assets, digital assets have additional challenges. What you need to understand is that protecting data depends on where that data is and what it's doing. Security teams protect data in three different states: in use, in transit, and at rest. Let's investigate this idea in greater detail. |

Ngày nay, câu trả lời thường là thông tin.Hầu hết thông tin đều ở dạng kỹ thuật số.Chúng tôi gọi đây là dữ liệu.Dữ liệu là thông tin được dịchđược xử lý hoặc lưu trữ bởi máy tính.Chúng ta đang sống trong một thế giới được kết nối.Hàng tỷ thiết bị trên khắp thế giới được kết nối vớiInternet và đang trao đổidữ liệu với nhau mọi lúc.Trên thực tế, hàng triệu mảnhdữ liệu đang được chuyển đến thiết bị của bạn ngay bây giờ!Khi so sánh với tài sản vật chất,tài sản kỹ thuật số có thêm thách thức.Điều bạn cần hiểu là việc bảo vệ dữ liệuphụ thuộc vào dữ liệu đó ở đâu và nó đang làm gì.Đội bảo mật bảo vệ dữ liệu trongba trạng thái khác nhau: đang sử dụng,trong quá trình di chuyển và khi nghỉ ngơi.Chúng ta hãy điều tra ý tưởng này chi tiết hơn.

|  |
| --- |
| Data in use is data being accessed by one or more users. Imagine being at a park with your laptop. It's a nice sunny day, and you stop at a bench to check your email. This is an example of data in use. As soon as you log in, your inbox is considered to be in use. |

Dữ liệu đang sử dụng là dữ liệu đang được một hoặc nhiều người dùng truy cập.Hãy tưởng tượng bạn đang ở công viên với chiếc máy tính xách tay của mình.Hôm nay là một ngày nắng đẹp và bạndừng lại ở một băng ghế để kiểm tra email của bạn.Đây là một ví dụ về dữ liệu đang được sử dụng.Ngay khi bạn đăng nhập,hộp thư đến của bạn được coi là đang được sử dụng.

|  |
| --- |
| Next, is data in transit. Data in transit is data traveling from one point to another. While you're signed into your account, a message from one of your friends appears. They sent you an interesting article about the growing security industry. You decide to reply, thanking them for sending this to you. When you click send, this is now an example of data in transit. |

Tiếp theo, là dữ liệu đang được chuyển tiếp.Dữ liệu đang truyền là dữ liệu di chuyển từ điểm này đến điểm kháckhác. Khi bạn đăng nhập vào tài khoản của mình,một tin nhắn từ một trong những người bạn của bạn xuất hiện.Họ đã gửi cho bạn một bài viết thú vịvề ngành công nghiệp an ninh đang phát triển.Bạn quyết định trả lời,cảm ơn họ đã gửi cái này cho bạn.Khi bạn bấm gửi,đây hiện là một ví dụ về dữ liệu đang được truyền.

|  |
| --- |
| Finally, there's data at rest. Data at rest is data not currently being accessed. In this state, data is typically stored on a physical device. An example of data at rest would be when you finish checking your email and close your laptop. You then decide to pack up and go to a nearby cafe for breakfast. As you make your way from the park towards the cafe, the data in your laptop is at rest. So now that we understand these states of data, let's connect this back to asset management. |

Cuối cùng, có dữ liệu ở phần còn lại.Dữ liệu ở trạng thái nghỉ là dữ liệu hiện không được truy cập.Ở trạng thái này, dữ liệu thường đượcđược lưu trữ trên một thiết bị vật lý.Một ví dụ về dữ liệu ở trạng thái nghỉ là khi bạnkiểm tra xong email và đóng máy tính xách tay của bạn lại.Sau đó bạn quyết định đóng góivà đi đến một quán cà phê gần đó để ăn sáng.Khi bạn đi từ công viên tới quán cà phê,dữ liệu trong máy tính xách tay của bạn ở trạng thái nghỉ ngơi.Vì vậy, bây giờ chúng ta đã hiểu được những trạng thái dữ liệu này,hãy kết nối điều này trở lại với việc quản lý tài sản.

|  |
| --- |
| Earlier, I mentioned that information is one of the most valuable assets that companies can have. Information security, or InfoSec, is the practice of keeping data in all states away from unauthorized users. Weak information security is a serious problem. It can lead to things like identity theft, financial loss, and reputational damage. These events have potential to harm organizations, their partners, and their customers. |

Trước đó, tôi đã đề cập rằng thông tin là một trong nhữngnhững tài sản có giá trị nhất mà công ty có thể có.Bảo mật thông tin, hay InfoSec, làthực hành lưu giữ dữ liệu trongtất cả các trạng thái tránh xa người dùng trái phép.Bảo mật thông tin yếu là một vấn đề nghiêm trọng.Nó có thể dẫn đến những việc như trộm danh tính,tổn thất về tài chính và thiệt hại về danh tiếng.Những sự kiện này có khả năng gây tổn hại cho các tổ chức,đối tác và khách hàng của họ.

|  |
| --- |
| And there's more to consider in your work as a security analyst. As our digital world continually changes, we are adapting our understanding of data at rest. Physical devices like our smartphones more commonly store data in the cloud, meaning that our information isn't necessarily at rest just because our phone is resting on a table. We should always be mindful of new vulnerabilities as our world becomes increasingly connected. |

Và còn nhiều điều cần xem xét trongcông việc của bạn là một nhà phân tích bảo mật.Khi thế giới kỹ thuật số của chúng ta liên tục thay đổi,chúng tôi đang điều chỉnh sự hiểu biết của mình về dữ liệu ở trạng thái nghỉ.Các thiết bị vật lý như điện thoại thông minh của chúng tôilưu trữ dữ liệu phổ biến hơn trên đám mây,có nghĩa là thông tin của chúng tôi không nhất thiết phải ởnghỉ ngơi chỉ vì điện thoại của chúng ta đang nằm trên bàn.Chúng ta phải luôn lưu tâm đếnnhững lỗ hổng mới như thế giới của chúng tangày càng trở nên kết nối.

|  |
| --- |
| Remember, protecting data depends on where the data is and what it's doing. Keeping track of information is part of the puzzle that companies solve when considering their security plan. Understanding the three states of data enable security teams to analyze risk and determine an asset management plan for different situations. |

Hãy nhớ, bảo vệ dữ liệuphụ thuộc vào dữ liệu ở đâu và nó đang làm gì.Theo dõi thông tin là một phần của câu đốmà các công ty giải quyết khixem xét kế hoạch an ninh của họ.Hiểu ba trạng thái của dữ liệucho phép các nhóm bảo mật phân tíchrủi ro và xác địnhmột kế hoạch quản lý tài sản cho các tình huống khác nhau.

***3.2. The challenges of securing digital devices - Những thách thức của việc bảo mật các thiết bị kỹ thuật số***

***3.3. Identify: States of data in the workplace - Xác định: Trạng thái dữ liệu tại nơi làm việc***

|  |  |
| --- | --- |
| Scenario | Data state |
| Following a security meeting, you open up a document and start writing a report detailing all the security vulnerabilities your team should address. | Data in use |
| You are looking at system logs from your antivirus software for any unusual activity on your computer. | Data in use |
| Your company has 2 servers that contain backups of databases, older versions of applications, and records of security compliance checks. No one is checking these servers at the moment. | Data at rest |
| You have just sent a text message to a coworker saying there is an urgent situation at work that requires their expertise and knowledge. It is being transmitted to their phone. | Data in transit |
| You’ve written an email to a coworker requesting the status on a recent system update. You have just clicked send, and the email is being routed to their inbox. | Data in transit |
| You have a presentation to give at a work conference across the country. In your bag, you carry a USB stick containing your slideshow and documents. You don’t access this USB stick during your 4-hour flight. | Data at rest |

|  |  |
| --- | --- |
| Kịch bản | Trạng thái dữ liệu |
| Sau cuộc họp bảo mật, bạn mở một tài liệu và bắt đầu viết báo cáo nêu chi tiết tất cả các lỗ hổng bảo mật mà nhóm của bạn cần giải quyết. | Dữ liệu đang được sử dụng |
| Bạn đang xem nhật ký hệ thống từ phần mềm chống vi-rút để tìm bất kỳ hoạt động bất thường nào trên máy tính của mình. | Dữ liệu đang được sử dụng |
| Công ty của bạn có 2 máy chủ chứa các bản sao lưu cơ sở dữ liệu, các phiên bản ứng dụng cũ hơn và hồ sơ kiểm tra tuân thủ bảo mật. Hiện tại không có ai kiểm tra các máy chủ này. | Dữ liệu ở trạng thái nghỉ |
| Bạn vừa gửi tin nhắn cho đồng nghiệp nói rằng có một tình huống khẩn cấp ở nơi làm việc cần đến chuyên môn và kiến ​​thức của họ. Nó đang được truyền tới điện thoại của họ. | Dữ liệu đang truyền |
| Bạn đã viết email cho đồng nghiệp yêu cầu trạng thái về bản cập nhật hệ thống gần đây. Bạn vừa nhấp vào gửi và email đang được chuyển đến hộp thư đến của họ. | Dữ liệu đang truyền |
| Bạn có một bài thuyết trình để trình bày tại một hội nghị việc làm trên toàn quốc. Trong túi xách của bạn, bạn mang theo một chiếc USB chứa trình chiếu và tài liệu của bạn. Bạn không thể truy cập vào thẻ USB này trong suốt chuyến bay kéo dài 4 giờ của mình. | Dữ liệu ở trạng thái nghỉ |

***3.4. The emergence of cloud security - Sự xuất hiện của bảo mật đám mây***

|  |
| --- |
| **The emergence of cloud security** |

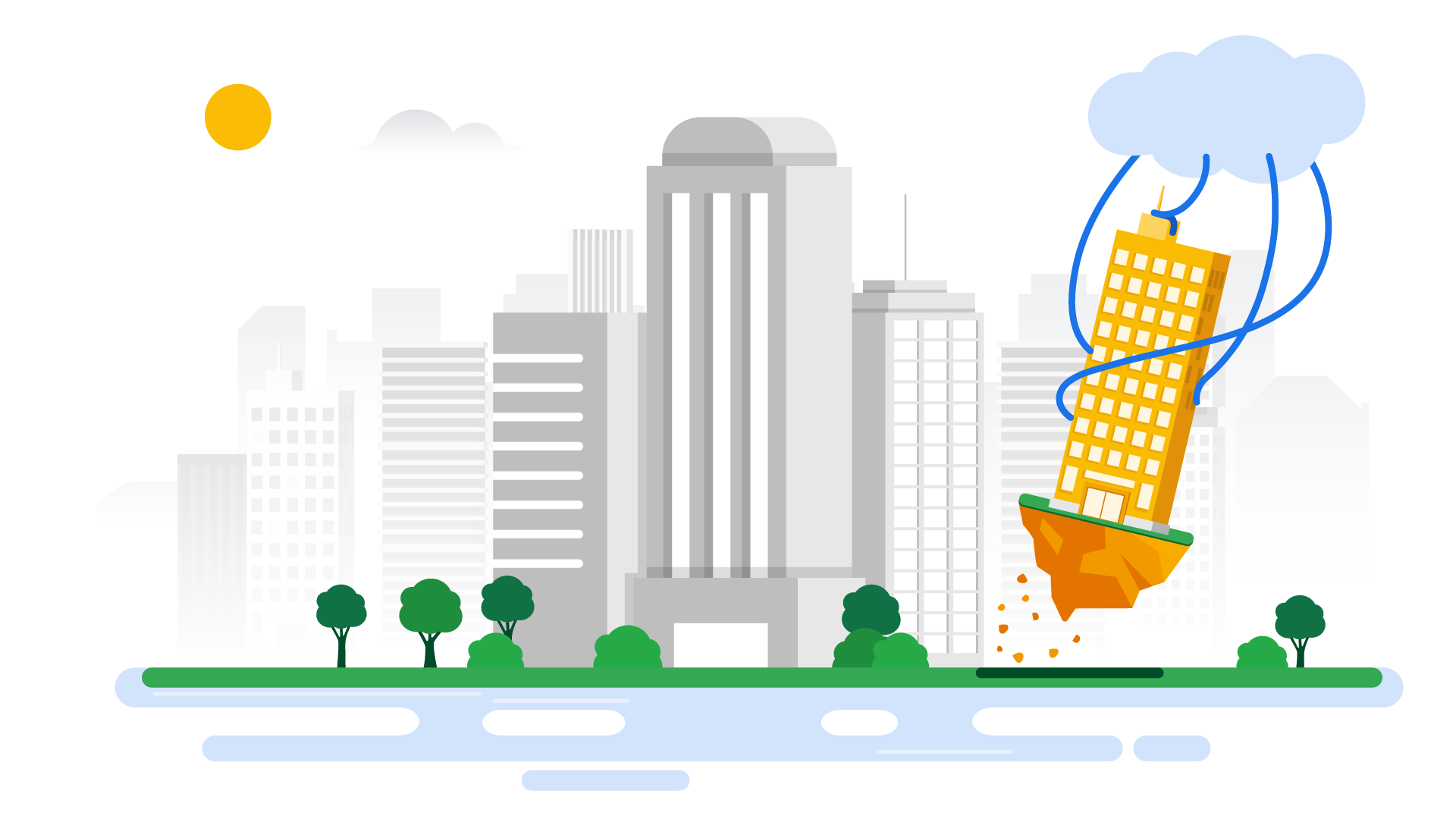
**Sự xuất hiện của bảo mật đám mây**

|  |
| --- |
| One of the most significant technology developments this century has been the emergence of cloud computing. The United Kingdom's National Cyber Security Centre defines cloud computing as, “An on-demand, massively scalable service, hosted on shared infrastructure, accessible via the internet.” |

Một trong những phát triển công nghệ quan trọng nhất trong thế kỷ này là sự xuất hiện của điện toán đám mây. Trung tâm An ninh Mạng Quốc gia của Vương quốc Anh định nghĩa điện toán đám mây là “Dịch vụ theo yêu cầu, có khả năng mở rộng quy mô lớn, được lưu trữ trên cơ sở hạ tầng dùng chung, có thể truy cập qua internet”.

|  |
| --- |
| Earlier, you learned that most information is in the form of data, which is in a constant state of change. In recent years, businesses started moving their data to the cloud. The adoption of cloud-based services has complicated how information is kept safe online. In this reading, you’ll learn about these challenges and the opportunities they’ve created for security professionals. |

Trước đó, bạn đã biết rằng hầu hết thông tin đều ở dạng dữ liệu và luôn ở trạng thái thay đổi. Trong những năm gần đây, các doanh nghiệp bắt đầu chuyển dữ liệu của họ lên đám mây. Việc áp dụng các dịch vụ dựa trên đám mây đã làm phức tạp thêm cách thức bảo mật thông tin trực tuyến. Trong bài đọc này, bạn sẽ tìm hiểu về những thách thức này và những cơ hội mà chúng đã tạo ra cho các chuyên gia bảo mật.



|  |
| --- |
| **Soaring into the cloud** |

**Bay lên mây**

|  |
| --- |
| Starting an online business used to be a complicated and costly process. In years past, companies had to build and maintain their own internal solutions to operate in the digital marketplace. Now, it’s much easier for anyone to participate because of the cloud. |

Bắt đầu kinh doanh trực tuyến từng là một quá trình phức tạp và tốn kém. Trong những năm trước, các công ty phải xây dựng và duy trì các giải pháp nội bộ của riêng mình để hoạt động trên thị trường kỹ thuật số. Giờ đây, mọi người đều có thể tham gia dễ dàng hơn nhiều nhờ có đám mây.

|  |
| --- |
| The availability of cloud technologies has drastically changed how businesses operate online. These new tools allow companies to scale and adapt quickly while also lowering their costs. Despite these benefits, the shift to cloud-based services has also introduced a range of new cybersecurity challenges that put assets at risk. |

Sự sẵn có của công nghệ đám mây đã thay đổi mạnh mẽ cách các doanh nghiệp hoạt động trực tuyến. Những công cụ mới này cho phép các công ty mở rộng quy mô và thích ứng nhanh chóng đồng thời giảm chi phí. Bất chấp những lợi ích này, việc chuyển sang các dịch vụ dựa trên đám mây cũng gây ra một loạt thách thức an ninh mạng mới khiến tài sản gặp rủi ro.

|  |
| --- |
| **Cloud-based services** |

**Dịch vụ dựa trên đám mây**

|  |
| --- |
| The term cloud-based services refers to a variety of on demand or web-based business solutions. Depending on a company’s needs and budget, services can range from website hosting, to application development environments, to entire back-end infrastructure. |

Thuật ngữ dịch vụ dựa trên đám mây đề cập đến nhiều giải pháp kinh doanh dựa trên web hoặc theo yêu cầu. Tùy thuộc vào nhu cầu và ngân sách của công ty, các dịch vụ có thể bao gồm từ lưu trữ trang web, môi trường phát triển ứng dụng đến toàn bộ cơ sở hạ tầng phụ trợ.

|  |
| --- |
| There are three main categories of cloud-based services:   * Software as a service (SaaS) * Platform as a service (PaaS) * Infrastructure as a service (IaaS) |

Có ba loại dịch vụ dựa trên đám mây chính:

* Phần mềm dưới dạng dịch vụ (SaaS)
* Nền tảng như một dịch vụ (PaaS)
* Cơ sở hạ tầng như một dịch vụ (IaaS)

|  |
| --- |
| **Software as a service (SaaS)** |

**Phần mềm dưới dạng dịch vụ (SaaS)**

|  |
| --- |
| SaaS refers to front-end applications that users access via a web browser. The service providers host, manage, and maintain all of the back-end systems for those applications. Common examples of SaaS services include applications like Gmail™ email service, Slack, and Zoom software. |

SaaS đề cập đến các ứng dụng front-end mà người dùng truy cập thông qua trình duyệt web. Các nhà cung cấp dịch vụ lưu trữ, quản lý và duy trì tất cả các hệ thống phụ trợ cho các ứng dụng đó. Các ví dụ phổ biến về dịch vụ SaaS bao gồm các ứng dụng như dịch vụ email Gmail™, phần mềm Slack và Zoom.

|  |
| --- |
| **Platform as a service (PaaS)** |

**Nền tảng như một dịch vụ (PaaS)**

|  |
| --- |
| PaaS refers to back-end application development tools that clients can access online. Developers use these resources to write code and build, manage, and deploy their own apps. Meanwhile, the cloud service providers host and maintain the back-end hardware and software that the apps use to operate. Some examples of PaaS services include Google App Engine™ platform, Heroku®, and VMware Cloud Foundry. |

PaaS đề cập đến các công cụ phát triển ứng dụng back-end mà khách hàng có thể truy cập trực tuyến. Nhà phát triển sử dụng các tài nguyên này để viết mã cũng như xây dựng, quản lý và triển khai ứng dụng của riêng họ. Trong khi đó, các nhà cung cấp dịch vụ đám mây lưu trữ và duy trì phần cứng và phần mềm phụ trợ mà ứng dụng sử dụng để vận hành. Một số ví dụ về dịch vụ PaaS bao gồm nền tảng Google App Engine™, Heroku® và VMware Cloud Foundry.

|  |
| --- |
| **Infrastructure as a service (IaaS)** |

**Cơ sở hạ tầng như một dịch vụ (IaaS)**

|  |
| --- |
| IaaS customers are given remote access to a range of back-end systems that are hosted by the cloud service provider. This includes data processing servers, storage, networking resources, and more. Resources are commonly licensed as needed, making it a cost-effective alternative to buying and maintaining on premises. |

Khách hàng IaaS được cấp quyền truy cập từ xa vào một loạt hệ thống phụ trợ do nhà cung cấp dịch vụ đám mây lưu trữ. Điều này bao gồm máy chủ xử lý dữ liệu, bộ lưu trữ, tài nguyên mạng, v.v. Các tài nguyên thường được cấp phép khi cần thiết, khiến nó trở thành một giải pháp thay thế hiệu quả về mặt chi phí cho việc mua và bảo trì tại cơ sở.

|  |
| --- |
| Cloud-based services allow companies to connect with their customers, employees, and business partners over the internet. Some of the largest organizations in the world offer cloud-based services:   * Google Cloud Platform * Microsoft Azure |

Các dịch vụ dựa trên đám mây cho phép các công ty kết nối với khách hàng, nhân viên và đối tác kinh doanh của họ qua internet. Một số tổ chức lớn nhất trên thế giới cung cấp dịch vụ dựa trên đám mây:

* Nền tảng đám mây của Google
* Microsoft Azure

|  |
| --- |
| **Cloud security** |

**Bảo mật đám mây**

|  |
| --- |
| Shifting applications and infrastructure over to the cloud can make it easier to operate an online business. It can also complicate keeping data private and safe. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud. |

Việc chuyển các ứng dụng và cơ sở hạ tầng sang đám mây có thể giúp việc vận hành doanh nghiệp trực tuyến trở nên dễ dàng hơn. Nó cũng có thể làm phức tạp việc giữ dữ liệu riêng tư và an toàn. Bảo mật đám mây là một lĩnh vực an ninh mạng đang phát triển, đặc biệt tập trung vào việc bảo vệ dữ liệu, ứng dụng và cơ sở hạ tầng trên đám mây.

|  |
| --- |
| In a traditional model, organizations had their entire IT infrastructure on premises. Protecting those systems was entirely up to the internal security team in that environment. These responsibilities are not so clearly defined when part or all of an operational environment is in the cloud. |

Trong mô hình truyền thống, các tổ chức có toàn bộ cơ sở hạ tầng CNTT tại cơ sở. Việc bảo vệ những hệ thống đó hoàn toàn phụ thuộc vào đội ngũ an ninh nội bộ trong môi trường đó. Những trách nhiệm này không được xác định rõ ràng khi một phần hoặc toàn bộ môi trường hoạt động nằm trên đám mây.

|  |
| --- |
| For example, a PaaS client pays to access the resources they need to build their applications. So, it is reasonable to expect them to be responsible for securing the apps they build. On the other hand, the responsibility for maintaining the security of the servers they are accessing should belong to the cloud service provider because there are other clients using the same systems. |

Ví dụ: khách hàng PaaS trả tiền để truy cập vào tài nguyên họ cần để xây dựng ứng dụng của mình. Vì vậy, thật hợp lý khi mong đợi họ chịu trách nhiệm bảo mật các ứng dụng mà họ xây dựng. Mặt khác, trách nhiệm duy trì tính bảo mật của máy chủ mà họ đang truy cập phải thuộc về nhà cung cấp dịch vụ đám mây vì có những khách hàng khác đang sử dụng cùng hệ thống.

|  |
| --- |
| In cloud security, this concept is known as the shared responsibility model. Clients are commonly responsible for securing anything that is directly within their control:   * Identity and access management * Resource configuration * Data handling |

Trong bảo mật đám mây, khái niệm này được gọi là mô hình trách nhiệm chung. Khách hàng thường chịu trách nhiệm bảo mật mọi thứ nằm trong tầm kiểm soát trực tiếp của họ:

* Quản lý danh tính và quyền truy cập
* Cấu hình tài nguyên
* Xử lý dữ liệu

|  |
| --- |
| **Note:** The amount of responsibility that is delegated to a service provider varies depending on the service being used: SaaS, PaaS, and IaaS. |

**Lưu ý:** Mức độ trách nhiệm được giao cho nhà cung cấp dịch vụ sẽ khác nhau tùy thuộc vào dịch vụ đang được sử dụng: SaaS, PaaS và IaaS.

|  |
| --- |
| **Cloud security challenges** |

**Những thách thức bảo mật đám mây**

|  |
| --- |
| All service providers do their best to deliver secure products to their customers. Much of their success depends on preventing breaches and how well they can protect sensitive information. However, since data is stored in the cloud and accessed over the internet, several challenges arise:   * **Misconfiguration** is one of the biggest concerns. Customers of cloud-based services are responsible for configuring their own security environment. Oftentimes, they use out-of-the-box configurations that fail to address their specific security objectives. * **Cloud-native breaches** are more likely to occur due to misconfigured services. * **Monitoring access might be difficult** depending onthe client and level of service. * **Meeting regulatory standards** is also a concern, particularly in industries that are required by law to follow specific requirements such as HIPAA, PCI DSS, and GDPR. |

Tất cả các nhà cung cấp dịch vụ đều cố gắng hết sức để cung cấp sản phẩm an toàn cho khách hàng của họ. Phần lớn thành công của họ phụ thuộc vào việc ngăn chặn hành vi vi phạm và mức độ họ có thể bảo vệ thông tin nhạy cảm. Tuy nhiên, do dữ liệu được lưu trữ trên đám mây và được truy cập qua internet nên một số thách thức sẽ nảy sinh:

* **Cấu hình sai** là một trong những mối quan tâm lớn nhất. Khách hàng sử dụng dịch vụ dựa trên đám mây chịu trách nhiệm định cấu hình môi trường bảo mật của riêng họ. Thông thường, họ sử dụng các cấu hình sẵn có nhưng không giải quyết được các mục tiêu bảo mật cụ thể của mình.
* **Các vi phạm trên nền tảng đám mây** có nhiều khả năng xảy ra hơn do các dịch vụ được định cấu hình sai.
* **Việc giám sát quyền truy cập có thể khó khăn** tùy thuộc vào khách hàng và mức độ dịch vụ.
* **Việc đáp ứng các tiêu chuẩn quy định** cũng là một mối quan tâm, đặc biệt là trong các ngành được pháp luật yêu cầu phải tuân theo các yêu cầu cụ thể như HIPAA, PCI DSS và GDPR.

|  |
| --- |
| Many other challenges exist besides these. As more businesses adopt cloud-based services, there’s a growing need for cloud security professionals to meet a growing number of risks. Burning Glass, a leading labor market analytics firm, ranks cloud security among the most in-demand skills in cybersecurity. |

Nhiều thách thức khác tồn tại bên cạnh những thách thức này. Khi ngày càng nhiều doanh nghiệp áp dụng các dịch vụ dựa trên đám mây, nhu cầu về các chuyên gia bảo mật đám mây sẽ ngày càng tăng để đáp ứng số lượng rủi ro ngày càng tăng. Burning Glass, một công ty phân tích thị trường lao động hàng đầu, xếp bảo mật đám mây là một trong những kỹ năng được yêu cầu cao nhất trong lĩnh vực an ninh mạng.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| So much of the global marketplace has shifted to cloud-based services. Cloud technology is still new, resulting in the emergence of new security models and a range of security challenges. And it’s likely that other concerns might arise as more businesses become reliant on the cloud. Being familiar with the cloud and the different services that are available is an important step towards supporting any organizations efforts to protect information online. |

Phần lớn thị trường toàn cầu đã chuyển sang các dịch vụ dựa trên đám mây. Công nghệ đám mây vẫn còn mới, kéo theo sự xuất hiện của các mô hình bảo mật mới và hàng loạt thách thức về bảo mật. Và có khả năng những mối lo ngại khác sẽ nảy sinh khi ngày càng có nhiều doanh nghiệp phụ thuộc vào đám mây. Làm quen với đám mây và các dịch vụ khác nhau hiện có là một bước quan trọng để hỗ trợ mọi nỗ lực của tổ chức trong việc bảo vệ thông tin trực tuyến.

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| Cloud security is one of the fastest growing subfields of cybersecurity. There are a variety of resources available online to learn more about this specialized topic. |

Bảo mật đám mây là một trong những lĩnh vực an ninh mạng phát triển nhanh nhất. Có rất nhiều tài nguyên có sẵn trực tuyến để tìm hiểu thêm về chủ đề chuyên ngành này.

|  |
| --- |
| * [The U.K.’s National Cyber Security Centre](https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model) has a detailed guide for choosing, using, and deploying cloud services securely based on the shared responsibility model. * [The Cloud Security Alliance®](https://cloudsecurityalliance.org/) is an organization dedicated to creating secure cloud environments. They offer access to cloud security-specific research, certification, and products to users with a paid membership. * [CompTIA Cloud+](https://www.comptia.org/blog/your-next-move-cloud-security-specialist) is a certificate program designed to teach you the foundational skills needed to become a cloud security specialist. |

* [Trung tâm An ninh mạng Quốc gia Vương quốc Anh](https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model)có hướng dẫn chi tiết về cách chọn, sử dụng và triển khai dịch vụ đám mây một cách an toàn dựa trên mô hình trách nhiệm chung.
* [Liên minh bảo mật đám mây®](https://cloudsecurityalliance.org/)là một tổ chức chuyên tạo ra môi trường đám mây an toàn. Họ cung cấp quyền truy cập vào nghiên cứu, chứng nhận và sản phẩm dành riêng cho bảo mật đám mây cho người dùng có tư cách thành viên trả phí.
* [Đám mây CompTIA+](https://www.comptia.org/blog/your-next-move-cloud-security-specialist)là chương trình chứng chỉ được thiết kế để dạy cho bạn những kỹ năng nền tảng cần thiết để trở thành chuyên gia bảo mật đám mây.

***3.5. Test your knowledge: Digital and physical assets - Kiểm tra kiến ​​thức của bạn: Tài sản vật chất và kỹ thuật số***

**4. Risk and asset security – Bảo mật rủi ro và tài sản**

***4.1. Elements of a security plan - Các yếu tố của một kế hoạch an ninh***

|  |
| --- |
| Security is all about people, processes, and technology. It's a team effort, and I mean that literally. Protecting assets extends well beyond one person or a group of people in an IT department. The truth of the matter is that security is a culture. It's a shared set of values that spans all levels of an organization. These values touch everyone, from employees, to vendors, to customers. Protecting digital and physical assets requires everyone to participate, which can be a challenge. |

Bảo mật là tất cả về con người, quy trình và công nghệ.Đó là nỗ lực của cả nhóm và ý tôi là theo nghĩa đen.Việc bảo vệ tài sản mở rộng ra ngoài phạm vi một người hoặcmột nhóm người trong bộ phận CNTT.Sự thật của vấn đề là an ninh là một nền văn hóa.Đó là một tập hợp các giá trị được chia sẻ trải rộng trên mọi cấp độ của một tổ chức.Những giá trị này tác động đến tất cả mọi người, từ nhân viên, nhà cung cấp đến khách hàng.Bảo vệ tài sản vật lý và kỹ thuật số đòi hỏi mọi người phải tham gia,đó có thể là một thách thức.

|  |
| --- |
| That's what security plans are for! Plans come in many shapes and sizes, but they all share a common goal: to be prepared for risks when they happen. Placing the focus on people is what leads to the most effective security plans. Considering the diverse backgrounds and perspectives of everyone involved ensures that no one is left out when something goes wrong. We talked earlier about the risk as being anything that can impact the confidentiality, integrity, or availability of an asset. Most security plans address risks by breaking them down according to categories and factors. |

Đó chính là mục đích của các kế hoạch bảo mật!Các kế hoạch có nhiều hình dạng và kích cỡ khác nhau nhưng tất cả đều có chung một mục tiêu:chuẩn bị sẵn sàng cho những rủi ro khi chúng xảy ra.Đặt trọng tâm vào con người là điều dẫn đến các kế hoạch bảo mật hiệu quả nhất.Xem xét nền tảng và quan điểm đa dạng của tất cả mọi người có liên quanđảm bảo không ai bị bỏ rơi khi có sự cố xảy ra.Chúng ta đã nói trước đó về rủi ro như bất cứ điều gì có thể tác độngtính bảo mật, tính toàn vẹn hoặc tính sẵn có của một tài sản.Hầu hết các kế hoạch bảo mật đều giải quyết rủi ro bằng cách chia nhỏ chúngtheo chủng loại và yếu tố.

|  |
| --- |
| Some common risk categories might include, the damage, disclosure, or loss of information. Any of these can be due to factors like the physical damage or malfunctions of a device. There are also factors like attacks and human error. For example, a new school teacher may be asked to sign a contract before their first day of class. The agreement may warn against some common risks associated with human error, like using a personal email to send sensitive information. A security plan may require that all new hires sign off on this agreement, effectively spreading the values that ensure everyone's in alignment. This is just one example of the types and causes of risk that a plan might address. These things vary widely depending on the company. But how these plans are communicated is similar across industries. |

Một số loại rủi ro phổ biến có thể bao gồm, thiệt hại,lộ hoặc mất thông tin.Bất kỳ điều nào trong số này có thể là do các yếu tố như thiệt hại vật chất hoặctrục trặc của một thiết bị.Ngoài ra còn có các yếu tố như tấn công và lỗi của con người.Ví dụ, một giáo viên mới vào trường có thể được yêu cầu ký hợp đồng trước khingày đầu tiên đi học.Thỏa thuận có thể cảnh báo một số rủi ro phổ biến liên quan đến lỗi của con người,như sử dụng email cá nhân để gửi thông tin nhạy cảm.Một kế hoạch bảo mật có thể yêu cầu tất cả những người mới được tuyển dụng phải ký vào thỏa thuận này,truyền bá một cách hiệu quả các giá trị nhằm đảm bảo sự đồng thuận của mọi người.Đây chỉ là một ví dụ về các loại và nguyên nhân rủi ro mà kế hoạch có thể giải quyết.Những điều này rất khác nhau tùy thuộc vào công ty.Nhưng cách truyền đạt những kế hoạch này là giống nhau giữa các ngành.

|  |
| --- |
| Security plans consist of three basic elements: policies, standards, and procedures. These three elements are how companies share their security plans. These words tend to be used interchangeably outside of security, but you'll soon discover that they each have a very specific meaning and function in this context. |

Kế hoạch bảo mật bao gồm ba yếu tố cơ bản: chính sách, tiêu chuẩn,và thủ tục.Ba yếu tố này là cách các công ty chia sẻ kế hoạch bảo mật của họ.Những từ này có xu hướng được sử dụng thay thế cho nhau bên ngoài vấn đề bảo mật, nhưngbạn sẽ sớm khám phá ra rằng mỗi cái đều có một ý nghĩa rất cụ thể vàhoạt động trong bối cảnh này.

|  |
| --- |
| A policy in security is a set of rules that reduce risk and protects information. Policies are the foundation of every security plan. They give everyone in and out of an organization guidance by addressing questions like, what are we protecting and why? Policies focus on the strategic side of things by identifying the scope, objectives, and limitations of a security plan. For instance, newly hired employees at many companies are required to sign off on acceptable use policy, or AUP. These provisions outline secure ways that an employee may access corporate systems. |

Chính sách bảo mật là một bộ quy tắc giúp giảm thiểu rủi ro và bảo vệ thông tin.Chính sách là nền tảng của mọi kế hoạch bảo mật.Họ đưa ra hướng dẫn cho mọi người trong và ngoài tổ chức bằng cách giải quyếtnhững câu hỏi như, chúng ta đang bảo vệ cái gì và tại sao?Các chính sách tập trung vào khía cạnh chiến lược của mọi việc bằng cách xác định phạm vi,mục tiêu và hạn chế của kế hoạch an ninh.Ví dụ, nhân viên mới được tuyển dụng ở nhiều công tyđược yêu cầu ký vào chính sách sử dụng được chấp nhận hoặc AUP.Những điều khoản này phác thảo những cách an toàn mà nhân viên có thể truy cập vào hệ thống của công ty.

|  |
| --- |
| Standards are the next part. These have a tactical function, as they concern how well we're protecting assets. In security, standards are references that inform how to set policies. A good way to think of standards is that they create a point of reference. For example, many companies use the password management standard identified in NIST Special Publication 800-63B to improve their security policies by specifying that employees' passwords must be at least eight characters long. |

Tiêu chuẩn là phần tiếp theo.Những điều này có chức năng chiến thuật vì chúng liên quan đến việc chúng ta bảo vệ tài sản tốt đến mức nào.Trong bảo mật, các tiêu chuẩn là tài liệu tham khảo cho biết cách thiết lập các chính sách.Một cách hay để nghĩ về các tiêu chuẩn là chúng tạo ra một điểm tham chiếu.Ví dụ: nhiều công ty sử dụng tiêu chuẩn quản lý mật khẩu được xác địnhtrong Ấn bản đặc biệt 800-63B của NIST để cải thiện chính sách bảo mật của họbằng cách chỉ định rằng mật khẩu của nhân viên phải dài ít nhất tám ký tự.

|  |
| --- |
| The last part of a plan is its procedures. Procedures are step-by-step instructions to perform a specific security task. Organizations usually keep multiple procedure documents that are used throughout the company, like how employees can choose secure passwords, or how they can securely reset a password if it's been locked. Sharing clear and actionable procedures with everyone creates accountability, consistency, and efficiency across an organization. |

Phần cuối cùng của một kế hoạch là các thủ tục của nó.Quy trình là hướng dẫn từng bước để thực hiện một nhiệm vụ bảo mật cụ thể.Các tổ chức thường lưu giữ nhiều tài liệu thủ tục được sử dụngtrong toàn công ty, như cách nhân viên có thể chọn mật khẩu an toàn,hoặc cách họ có thể đặt lại mật khẩu một cách an toàn nếu nó bị khóa.Việc chia sẻ các quy trình rõ ràng và có thể thực hiện được với mọi người sẽ tạo ra trách nhiệm giải trình,tính nhất quán và hiệu quả trong toàn bộ tổ chức.

|  |
| --- |
| Policies, standards, and procedures vary widely from one company to another because they are tailored to each organization's goals. Simply understanding the structure of security plans is a great start. For now, I hope you have a clearer picture of what policies, standards, and procedures are, and how they are essential to making security a team effort. |

Các chính sách, tiêu chuẩn và thủ tục rất khác nhau giữa các công tykhác vì chúng được điều chỉnh cho phù hợp với mục tiêu của mỗi tổ chức.Chỉ cần hiểu cấu trúc của các kế hoạch bảo mật là một khởi đầu tuyệt vời.Hiện tại, tôi hy vọng bạn có bức tranh rõ ràng hơn về những chính sách, tiêu chuẩn vàcác thủ tục là gì và chúng cần thiết như thế nào trong nỗ lực đảm bảo an ninh của nhóm.

***4.2. The NIST Cybersecurity Framework - Khung an ninh mạng NIST***

|  |
| --- |
| Having a plan is just one part of securing assets. Once the plan is in action, the other part is making sure everyone's following along. In security, we call this compliance. |

Có kế hoạch chỉ là một phần của việc đảm bảo tài sản.Sau khi kế hoạch được thực hiện, phần còn lại là đảm bảo mọi người đều tuân theo.Trong lĩnh vực bảo mật, chúng tôi gọi đây là sự tuân thủ.

|  |
| --- |
| Compliance is the process of adhering to internal standards and external regulations. Small companies and large organizations around the world place security compliance at the top of their list of priorities. At a high-level, maintaining trust, reputation, safety, and the integrity of your data are just a few reasons to be concerned about compliance. Fines, penalties, and lawsuits are other reasons. This is particularly true for companies in highly regulated industries, like health care, energy, and finance. Being out of compliance with a regulation can cause long lasting financial and reputational effects that can seriously impact a business. |

Tuân thủ là quá trình tuân thủ các tiêu chuẩn nội bộ vàquy định bên ngoài.Các công ty nhỏ và tổ chức lớn trên khắp thế giới đặt ra yêu cầu tuân thủ an ninhở đầu danh sách ưu tiên của họ.Ở mức độ cao, duy trì sự tin cậy, danh tiếng, an toàn vàtính toàn vẹn của dữ liệu của bạn chỉ là một vài lý do cần lo ngại về việc tuân thủ.Tiền phạt, hình phạt và kiện tụng là những lý do khác.Điều này đặc biệt đúng đối vớicác công ty trong các ngành được quản lý chặt chẽ, như chăm sóc sức khỏe, năng lượng và tài chính.Không tuân thủ quy định có thể gây ra hậu quả lâu dàinhững ảnh hưởng tài chính và danh tiếng có thể ảnh hưởng nghiêm trọng đến doanh nghiệp.

|  |
| --- |
| Regulations are rules set by a government or other authority to control the way something is done. Like policies, regulations exist to protect people and their information, but on a larger scale. Compliance can be a complex process because of the many regulations that exist all around the world. For our purpose, we're going to focus on a framework of security compliance, the U.S. based NIST Cybersecurity Framework. |

Quy định là những quy định do chính phủ hoặcquyền khác để kiểm soát cách thức thực hiện một việc gì đó.Giống như các chính sách, các quy định tồn tại để bảo vệ con người vàthông tin của họ, nhưng ở quy mô lớn hơn.Tuân thủ có thể là một quá trình phức tạp vì có nhiều quy địnhtồn tại khắp nơi trên thế giới.Vì mục đích của chúng ta, chúng ta sẽ tập trung vào khuôn khổ tuân thủ bảo mật,Khung an ninh mạng NIST có trụ sở tại Hoa Kỳ.

|  |
| --- |
| Earlier in the program, you learned the National Institute of Standards and Technology, or NIST. One of the primary roles of NIST is to openly provide companies with a set of frameworks and security standards that reflect key security related regulations. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Commonly known as the CSF, this framework was developed to help businesses secure one of their most important assets, information. The CSF consists of three main components: the core, it's tiers, and it's profiles. Let's explore each of these together to build a better understanding of how NIST's CSF is used. |

Ở phần trước của chương trình, bạn đã học về Viện Tiêu chuẩn Quốc gia vàCông nghệ, hoặc NIST.Một trong những vai trò chính của NIST là cung cấp công khai cho các công ty một bộkhuôn khổ và tiêu chuẩn bảo mật phản ánh các quy định quan trọng liên quan đến bảo mật.Khung an ninh mạng NIST là một khung tự nguyện bao gồmtiêu chuẩn, hướng dẫn và thực hành tốt nhấtđể quản lý rủi ro an ninh mạng. Thường được gọi là CSF,khuôn khổ này được phát triển để giúp các doanh nghiệp đảm bảo một trong những điều quan trọng nhất của họtài sản, thông tin.CSF bao gồm ba thành phần chính: lõi, các tầng và cấu hình của nó.Chúng ta hãy cùng nhau khám phá từng điều nàyđể xây dựng sự hiểu biết tốt hơn về cách sử dụng CSF của NIST.

|  |
| --- |
| The core is basically a simplified version of the functions, or duties, of a security plan. The CSF core identifies five broad functions: identify, protect, detect, respond, and recover. Think of these categories of the core as a security checklist. |

Phần lõi về cơ bản là một phiên bản đơn giản hóa của các chức năng, hoặcnhiệm vụ của một kế hoạch an ninh.Lõi CSF xác định năm chức năng rộng:xác định, bảo vệ, phát hiện, phản hồi và phục hồi.Hãy coi những danh mục cốt lõi này như một danh sách kiểm tra bảo mật.

|  |
| --- |
| After the core, the next NIST component we'll discuss is its tiers. These provide security teams with a way to measure performance across each of the five functions of the core. Tiers range from Level-1 to Level-4. Level-1, or passive, indicates a function is reaching bare minimum standards. Level-4, or adaptive, is an indication that a function is being performed at an exemplary standard. You may have noticed that CSF tiers aren't a yes or no proposition; instead, there's a range of values. That's because tiers are designed as a way of showing organizations what is and isn't working with their security plans. |

Sau lõi, thành phần NIST tiếp theo mà chúng ta sẽ thảo luận là các tầng của nó.Những điều này cung cấp cho các đội bảo mật một cách để đo lườnghiệu suất của từng chức năng trong năm chức năng cốt lõi.Các cấp độ dao động từ Cấp 1 đến Cấp 4.Cấp độ 1, hoặc thụ động, cho biết một chức năng đang đạt đến các tiêu chuẩn tối thiểu.Cấp độ 4, hoặcthích ứng, là dấu hiệu cho thấy một chức năng đang được thực hiện theo tiêu chuẩn mẫu.Bạn có thể nhận thấy rằng các cấp CSF không phải là đề xuất có hoặc không;thay vào đó, có một loạt các giá trị.Đó là bởi vì các cấp độ được thiết kế như một cách thể hiện cho các tổ chức thấy những gì vàkhông hoạt động với các kế hoạch bảo mật của họ.

|  |
| --- |
| Lastly, profiles are the final component of CSF. These provide insight into the current state of a security plan. One way to think of profiles is like photos capturing a moment in time. Comparing photos of the same subject taken at different times can provide useful insights. For example, without these photos, you might not notice how this tree has changed. It's the same with NIST profiles. |

Cuối cùng, hồ sơ là thành phần cuối cùng của CSF.Những điều này cung cấp cái nhìn sâu sắc về trạng thái hiện tại của một kế hoạch bảo mật.Một cách để hình dung về hồ sơ giống như những bức ảnh ghi lại một khoảnh khắc.So sánh các bức ảnh cùng chủ đề được chụp ở các thời điểm khác nhaucó thể cung cấp những hiểu biết hữu ích.Ví dụ: nếu không có những bức ảnh này, bạn có thể không nhận thấy cái cây này đã thay đổi như thế nào.Tương tự với hồ sơ NIST.

|  |
| --- |
| Good security practice is about more than avoiding fines and attacks. It demonstrates that you care about people and their information. Before we go, let's visit the core's functions one more time to look at where we've been and where we're going. The first function is identify. Our previous discussions on asset management and risk assessment relates to that function. Coming up, we're going to focus on many of the categories of the second function, the protect function. Meet you there! |

Thực hành bảo mật tốt không chỉ nhằm tránh bị phạt tiền và tấn công.Nó chứng tỏ rằng bạn quan tâm đến mọi người và thông tin của họ.Trước khi tiếp tục, chúng ta hãy ghé thăm các chức năng của lõi một lần nữa để xem vị tríchúng ta đã đến và chúng ta sẽ đi đâu.Chức năng đầu tiên là xác định. Các cuộc thảo luận trước đây của chúng tôi về tài sảnquản lý và đánh giá rủi ro liên quan đến chức năng đó.Sắp tới, chúng ta sẽ tập trung vào nhiều danh mục của hàm thứ hai,chức năng bảo vệ. Gặp bạn ở đó!

***4.3. Security guidelines in action - Hướng dẫn bảo mật đang hoạt động***

|  |
| --- |
| **Security guidelines in action** |

**Hướng dẫn bảo mật đang hoạt động**

|  |
| --- |
| Organizations often face an overwhelming amount of risk. Developing a security plan from the beginning that addresses all risk can be challenging. This makes security frameworks a useful option. |

Các tổ chức thường phải đối mặt với rất nhiều rủi ro. Việc phát triển một kế hoạch bảo mật ngay từ đầu nhằm giải quyết mọi rủi ro có thể là một thách thức. Điều này làm cho khung bảo mật trở thành một lựa chọn hữu ích.

|  |
| --- |
| Previously, you learned about the NIST Cybersecurity Framework (CSF). A major benefit of the CSF is that it's flexible and can be applied to any industry. In this reading, you’ll explore how the NIST CSF can be implemented. |

Trước đây, bạn đã tìm hiểu về Khung bảo mật không gian mạng (CSF) của NIST. Lợi ích chính của CSF là nó linh hoạt và có thể áp dụng cho bất kỳ ngành nào. Trong bài đọc này, bạn sẽ khám phá cách triển khai NIST CSF.



|  |
| --- |
| **Origins of the framework** |

**Nguồn gốc của khung**

|  |
| --- |
| Originally released in 2014, NIST developed the Cybersecurity Framework to protect critical infrastructure in the United States. NIST was selected to develop the CSF because they are an unbiased source of scientific data and practices. NIST eventually adapted the CSF to fit the needs of businesses in the public and private sector. Their goal was to make the framework more flexible, making it easier to adopt for small businesses or anyone else that might lack the resources to develop their own security plans. |

Được phát hành lần đầu vào năm 2014, NIST đã phát triển Khung an ninh mạng để bảo vệ cơ sở hạ tầng quan trọng ở Hoa Kỳ. NIST được chọn để phát triển CSF vì đây là nguồn dữ liệu và thực tiễn khoa học khách quan. NIST cuối cùng đã điều chỉnh CSF để phù hợp với nhu cầu của các doanh nghiệp trong khu vực công và tư nhân. Mục tiêu của họ là làm cho khuôn khổ này trở nên linh hoạt hơn, giúp các doanh nghiệp nhỏ hoặc bất kỳ ai khác có thể thiếu nguồn lực để phát triển các kế hoạch bảo mật của riêng họ dễ dàng áp dụng hơn.

|  |
| --- |
| **Components of the CSF** |

**Các thành phần của CSF**

|  |
| --- |
| As you might recall, the framework consists of three main components: the *core*, *tiers*, and *profiles*. In the following sections, you'll learn more about each of these CSF components. |

Như bạn có thể nhớ lại, khung này bao gồm ba thành phần chính: *lõi* , *tầng* và *cấu hình* . Trong các phần sau, bạn sẽ tìm hiểu thêm về từng thành phần CSF này.

|  |
| --- |
| **Core** |

**Cốt lõi**

|  |
| --- |
| The CSF core is a set of desired cybersecurity outcomes that help organizations customize their security plan. It consists of five functions, or parts: Identify, Protect, Detect, Respond, and Recover. These functions are commonly used as an informative reference to help organizations *identify* their most important assets and *protect* those assets with appropriate safeguards. The CSF core is also used to understand ways to *detect* attacks and develop *response* and *recovery* plans should an attack happen. |

Lõi CSF là tập hợp các kết quả an ninh mạng mong muốn giúp các tổ chức tùy chỉnh kế hoạch bảo mật của họ. Nó bao gồm năm chức năng hoặc bộ phận: Xác định, Bảo vệ, Phát hiện, Phản hồi và Phục hồi. Các chức năng này thường được sử dụng làm tài liệu tham khảo mang tính thông tin nhằm giúp các tổ chức *xác định* những tài sản quan trọng nhất của họ và *bảo vệ* những tài sản đó bằng các biện pháp bảo vệ thích hợp. Lõi CSF cũng được sử dụng để hiểu các cách *phát hiện* các cuộc tấn công và phát triển các kế hoạch *ứng phó* và *phục hồi* nếu một cuộc tấn công xảy ra.

|  |
| --- |
| **Tiers** |

**Bậc**

|  |
| --- |
| The CSF tiers are a way of measuring the sophistication of an organization's cybersecurity program. CSF tiers are measured on a scale of 1 to 4. Tier 1 is the lowest score, indicating that a limited set of security controls have been implemented. Overall, CSF tiers are used to assess an organization's security posture and identify areas for improvement. |

Các cấp CSF là một cách đo lường mức độ tinh vi của chương trình an ninh mạng của tổ chức. Các bậc CSF được đo theo thang điểm từ 1 đến 4. Bậc 1 là điểm thấp nhất, cho biết rằng một bộ biện pháp kiểm soát bảo mật có giới hạn đã được triển khai. Nhìn chung, các cấp độ CSF được sử dụng để đánh giá tình hình bảo mật của tổ chức và xác định các khu vực cần cải thiện.

|  |
| --- |
| **Profiles** |

**Hồ sơ**

|  |
| --- |
| The CSF profiles are pre-made templates of the NIST CSF that are developed by a team of industry experts. CSF profiles are tailored to address the specific risks of an organization or industry. They are used to help organizations develop a baseline for their cybersecurity plans, or as a way of comparing their current cybersecurity posture to a specific industry standard. |

Hồ sơ CSF là các mẫu được tạo sẵn của NIST CSF được phát triển bởi một nhóm chuyên gia trong ngành. Hồ sơ CSF được điều chỉnh để giải quyết các rủi ro cụ thể của một tổ chức hoặc ngành. Chúng được sử dụng để giúp các tổ chức phát triển cơ sở cho kế hoạch an ninh mạng của họ hoặc như một cách để so sánh tình trạng an ninh mạng hiện tại của họ với một tiêu chuẩn ngành cụ thể.

|  |
| --- |
| **Note:** The core, tiers, and profiles were each designed to help any business improve their security operations. Although there are only three components, the entire framework consists of a complex system of subcategories and processes. |

**Lưu ý:** Mỗi phần cốt lõi, cấp độ và hồ sơ đều được thiết kế để giúp mọi doanh nghiệp cải thiện hoạt động bảo mật của họ. Mặc dù chỉ có ba thành phần nhưng toàn bộ khuôn khổ bao gồm một hệ thống phức tạp gồm các tiểu mục và quy trình.

|  |
| --- |
| **Implementing the CSF** |

**Thực hiện CSF**

|  |
| --- |
| As you might recall, compliance is an important concept in security. **Compliance** is the process of adhering to internal standards and external regulations. In other words, compliance is a way of measuring how well an organization is protecting their assets. The **NIST Cybersecurity Framework (CSF)** is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Organizations may choose to use the CSF to achieve compliance with a variety of regulations. |

Như bạn có thể nhớ lại, tuân thủ là một khái niệm quan trọng trong bảo mật. **Tuân thủ** là quá trình tuân thủ các tiêu chuẩn nội bộ và các quy định bên ngoài. Nói cách khác, tuân thủ là một cách đo lường mức độ tổ chức bảo vệ tài sản của họ. Khung **an ninh mạng NIST (CSF)** là một khung tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và phương pháp hay nhất để quản lý rủi ro an ninh mạng. Các tổ chức có thể chọn sử dụng CSF để đạt được sự tuân thủ với nhiều quy định khác nhau.

|  |
| --- |
| **Note:** Regulations are rules that *must* be followed, while frameworks are resources you can *choose* to use. |

**Lưu ý:** Quy định là các quy tắc *phải* tuân theo, trong khi khuôn khổ là tài nguyên bạn có thể *chọn* sử dụng.

|  |
| --- |
| Since its creation, many businesses have used the NIST CSF. However, CSF can be a challenge to implement due to its high level of detail. It can also be tough to find where the framework fits in. For example, some businesses have established security plans, making it unclear how CSF can benefit them. Alternatively, some businesses might be in the early stages of building their plans and need a place to start. |

Kể từ khi thành lập, nhiều doanh nghiệp đã sử dụng NIST CSF. Tuy nhiên, CSF có thể là một thách thức để thực hiện do mức độ chi tiết cao. Cũng có thể khó tìm được khuôn khổ phù hợp ở đâu. Ví dụ: một số doanh nghiệp đã thiết lập các kế hoạch bảo mật, khiến không rõ CSF có thể mang lại lợi ích cho họ như thế nào. Ngoài ra, một số doanh nghiệp có thể đang ở giai đoạn đầu xây dựng kế hoạch của mình và cần một nơi để bắt đầu.

|  |
| --- |
| In any scenario, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides detailed guidance that any organization can use to implement the CSF. This is a quick overview and summary of their recommendations:   * **Create a current profile** of the security operations and outline the specific needs of your business. * **Perform a risk assessment** to identify which of your current operations are meeting business and regulatory standards. * **Analyze and prioritize existing gaps** in security operations that place the businesses assets at risk. * **Implement a plan of action** to achieve your organization’s goals and objectives. |

Trong mọi trường hợp, Cơ quan An ninh Cơ sở hạ tầng và An ninh mạng Hoa Kỳ (CISA) đều cung cấp hướng dẫn chi tiết mà bất kỳ tổ chức nào cũng có thể sử dụng để triển khai CSF. Đây là tổng quan nhanh và tóm tắt các khuyến nghị của họ:

* **Tạo hồ sơ hiện tại** về các hoạt động bảo mật và phác thảo các nhu cầu cụ thể của doanh nghiệp bạn.
* **Thực hiện đánh giá rủi ro** để xác định hoạt động nào hiện tại của bạn đang đáp ứng các tiêu chuẩn kinh doanh và quy định.
* **Phân tích và ưu tiên các lỗ hổng hiện có** trong hoạt động bảo mật khiến tài sản của doanh nghiệp gặp rủi ro.
* **Thực hiện kế hoạch hành động** để đạt được mục tiêu và mục đích của tổ chức.

|  |
| --- |
| **Pro tip:** Always consider current risk, threat, and vulnerability trends when using the NIST CSF. |

**Mẹo chuyên nghiệp:** Luôn xem xét các xu hướng rủi ro, mối đe dọa và lỗ hổng hiện tại khi sử dụng NIST CSF.

|  |
| --- |
| You can learn more about implementing the CSF in [this report by CISA that outlines how the framework was applied in the commercial facilities sector](https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf). |

Bạn có thể tìm hiểu thêm về việc triển khai CSF trong[báo cáo này của CISA trình bày cách áp dụng khuôn khổ này trong lĩnh vực cơ sở thương mại](https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf).

|  |
| --- |
| **Industries embracing the CSF** |

**Các ngành công nghiệp ủng hộ CSF**

|  |
| --- |
| The NIST CSF has continued to evolve since its introduction in 2014. Its design is influenced by the standards and best practices of some of the largest companies in the world. |

NIST CSF đã tiếp tục phát triển kể từ khi được giới thiệu vào năm 2014. Thiết kế của nó chịu ảnh hưởng bởi các tiêu chuẩn và phương pháp thực hành tốt nhất của một số công ty lớn nhất trên thế giới.

|  |
| --- |
| A benefit of the framework is that it aligns with the security practices of many organizations across the global economy. It also helps with regulatory compliance that might be shared by business partners. |

Lợi ích của khuôn khổ này là nó phù hợp với các biện pháp bảo mật của nhiều tổ chức trong nền kinh tế toàn cầu. Nó cũng giúp tuân thủ quy định mà các đối tác kinh doanh có thể chia sẻ.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| The NIST CSF is a flexible resource that organizations may choose to use to assess and improve their security posture. It's a useful framework that combines the security best practices of industries around the world. Implementing the CSF can be a challenge for any organization. The CSF can help business meet regulatory compliance requirements to avoid financial and reputational risks. |

NIST CSF là một nguồn tài nguyên linh hoạt mà các tổ chức có thể chọn sử dụng để đánh giá và cải thiện tình trạng bảo mật của mình. Đó là một khuôn khổ hữu ích kết hợp các phương pháp bảo mật tốt nhất của các ngành trên toàn thế giới. Việc thực hiện CSF có thể là một thách thức đối với bất kỳ tổ chức nào. CSF có thể giúp doanh nghiệp đáp ứng các yêu cầu tuân thủ quy định để tránh rủi ro tài chính và danh tiếng.

***4.4. Test your knowledge: Risk and asset security - Kiểm tra kiến ​​thức của bạn: Bảo mật rủi ro và tài sản***

***4.5. Activity: Score risks based on their likelihood and severity - Hoạt động: Đánh giá rủi ro dựa trên khả năng xảy ra và mức độ nghiêm trọng của chúng***

|  |
| --- |
| **Activity Overview**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/p6bA4_W6Rti2hSc-chizkg_35818ee471f5453cac13218b3236edf1_image.png?expiry=1718928000000&hmac=T6pj3v3TlthwAa9k_G_1ggxeMGqFN-ifZa4m0XTaoqM  In this activity, you will practice performing a risk assessment by evaluating vulnerabilities that commonly threaten business operations. Then, you will decide how to prioritize your resources based on the risk scores you assign each vulnerability.  You might recall that the purpose of having a security plan is to be prepared for risks. Assessing potential risks is one of the first steps of the **NIST Cybersecurity Framework (CSF)**, a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Risk assessments are how security teams determine whether their security operations are adequately positioned to prevent cyber attacks and protect sensitive information.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/p6bA4_W6Rti2hSc-chizkg_35818ee471f5453cac13218b3236edf1_image.png?expiry=1718928000000&hmac=T6pj3v3TlthwAa9k_G_1ggxeMGqFN-ifZa4m0XTaoqM

Trong hoạt động này, bạn sẽ thực hành thực hiện đánh giá rủi ro bằng cách đánh giá các lỗ hổng thường đe dọa hoạt động kinh doanh. Sau đó, bạn sẽ quyết định cách ưu tiên các tài nguyên của mình dựa trên điểm rủi ro mà bạn chỉ định cho từng lỗ hổng.

Bạn có thể nhớ lại rằng mục đích của việc lập kế hoạch bảo mật là chuẩn bị cho những rủi ro. Đánh giá rủi ro tiềm ẩn là một trong những bước đầu tiên của **Khung an ninh mạng NIST (CSF)** , một khung tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và biện pháp thực hành tốt nhất để quản lý rủi ro an ninh mạng. Đánh giá rủi ro là cách các nhóm bảo mật xác định xem liệu hoạt động bảo mật của họ có được bố trí phù hợp để ngăn chặn các cuộc tấn công mạng và bảo vệ thông tin nhạy cảm hay không.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/9S-IzWNqSDO3d1c8xJo9eA_b36c719b7486409f86bbf482cf26c0f1_image.png?expiry=1718928000000&hmac=3BvUKgYF1u1N0DnpaLdfA3hmVOgBICJFqo7vSEAOayk  Review the following scenario. Then complete the step-by-step instructions.  You've joined a new cybersecurity team at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, they are creating a risk register to help them focus on securing the most vulnerable risks.  A **risk register** is a central record of potential risks to an organization's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.  Your supervisor asks you to evaluate a set of risks that the cybersecurity team has recorded in the risk register. For each risk, you will first determine how likely that risk is to occur. Then, you will determine how severely that risk may impact the bank. Finally, you will calculate a score for the severity of that risk. You will then compare scores across all risks so your team can determine how to prioritize their attention for each risk. |

**Kịch bản**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/9S-IzWNqSDO3d1c8xJo9eA_b36c719b7486409f86bbf482cf26c0f1_image.png?expiry=1718928000000&hmac=3BvUKgYF1u1N0DnpaLdfA3hmVOgBICJFqo7vSEAOayk

Xem lại tình huống sau. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn đã tham gia nhóm an ninh mạng mới tại một ngân hàng thương mại. Nhóm đang tiến hành đánh giá rủi ro về môi trường hoạt động hiện tại của ngân hàng. Là một phần của đánh giá, họ đang tạo một sổ đăng ký rủi ro để giúp họ tập trung vào việc đảm bảo những rủi ro dễ bị tổn thương nhất.

Sổ **đăng ký rủi ro** là bản ghi trung tâm về các rủi ro tiềm ẩn đối với tài sản, hệ thống thông tin và dữ liệu của tổ chức. Các nhóm bảo mật thường sử dụng sổ đăng ký rủi ro khi tiến hành đánh giá rủi ro.

Người giám sát của bạn yêu cầu bạn đánh giá một loạt rủi ro mà nhóm an ninh mạng đã ghi lại trong sổ đăng ký rủi ro. Đối với mỗi rủi ro, trước tiên bạn sẽ xác định khả năng rủi ro đó xảy ra. Sau đó, bạn sẽ xác định mức độ nghiêm trọng mà rủi ro đó có thể ảnh hưởng đến ngân hàng. Cuối cùng, bạn sẽ tính điểm cho mức độ nghiêm trọng của rủi ro đó. Sau đó, bạn sẽ so sánh điểm số của tất cả các rủi ro để nhóm của bạn có thể xác định cách ưu tiên chú ý cho từng rủi ro.

|  |
| --- |
| **Step-By-Step Instructions**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/1XZHpgt-QaK5p8J6R1hsaA_c1c6acf94b6b4a38a68b310708a48df1_image.png?expiry=1718928000000&hmac=24Quz2x2AdUD9Q42FZw3TVhnsBnSK1PWZ7prsbGGjeI  Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/1XZHpgt-QaK5p8J6R1hsaA_c1c6acf94b6b4a38a68b310708a48df1_image.png?expiry=1718928000000&hmac=24Quz2x2AdUD9Q42FZw3TVhnsBnSK1PWZ7prsbGGjeI

Thực hiện theo hướng dẫn và trả lời câu hỏi bên dưới để hoàn thành hoạt động. Sau đó, chuyển sang mục khóa học tiếp theo để so sánh bài tập của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the following link and select *Use Template*.  Link to template:[Risk register](https://docs.google.com/document/d/1fqPEK1Cy9cLsR4SvewhqfanU75JkAegy1TAJNcWex5U/template/preview?usp=sharing&resourcekey=0-rYoRJ_z6hCgITUqRwmOoCQ) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

Liên kết đến mẫu:[Đăng ký rủi ro](https://docs.google.com/document/d/1fqPEK1Cy9cLsR4SvewhqfanU75JkAegy1TAJNcWex5U/template/preview?usp=sharing&resourcekey=0-rYoRJ_z6hCgITUqRwmOoCQ)

|  |
| --- |
| **Step 2: Understand the operating environment**  When conducting a risk assessment, it's important to consider the factors that could cause a security event. This often starts with understanding the operating environment.  In this scenario, your team has identified characteristics of the operating environment that could factor into the bank's risk profile:  *The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure their data and funds, like having enough cash available each day to meet Federal Reserve requirements.* |

**Bước 2: Tìm hiểu môi trường hoạt động**

Khi tiến hành đánh giá rủi ro, điều quan trọng là phải xem xét các yếu tố có thể gây ra sự kiện bảo mật. Điều này thường bắt đầu bằng sự hiểu biết về môi trường hoạt động.

Trong trường hợp này, nhóm của bạn đã xác định được các đặc điểm của môi trường hoạt động có thể ảnh hưởng đến hồ sơ rủi ro của ngân hàng:

*Ngân hàng nằm ở khu vực ven biển với tỷ lệ tội phạm thấp. Nhiều người và hệ thống xử lý dữ liệu của ngân hàng—100 nhân viên tại chỗ và 20 nhân viên từ xa. Cơ sở khách hàng của ngân hàng bao gồm 2.000 tài khoản cá nhân và 200 tài khoản thương mại. Các dịch vụ của ngân hàng được tiếp thị bởi một đội thể thao chuyên nghiệp và mười doanh nghiệp địa phương trong cộng đồng. Có những quy định tài chính nghiêm ngặt yêu cầu ngân hàng phải bảo mật dữ liệu và tiền của họ, chẳng hạn như có đủ tiền mặt mỗi ngày để đáp ứng yêu cầu của Cục Dự trữ Liên bang.*

|  |
| --- |
| **Step 3: Consider potential risks to assets**  Security events are possible when assets are at risk. The source of a risk can range from malicious attackers to accidental human errors. A risk source can even come from natural or environmental hazards, such as a structural failure or power outage.  The bank's funds are one of its key assets. Your team has listed five primary risks to the bank's funds:   * Business email compromise * Compromised user database * Financial records leak * Theft * Supply chain attack   Consider these potential risks in relation to the bank's operating environment. Then, write **2-3 sentences (40-60 words)** in the **Notes** area of the template describing how security events are possible considering the risks facing the funds in this operating environment. |

**Bước 3: Xem xét rủi ro tiềm ẩn đối với tài sản**

Các sự kiện bảo mật có thể xảy ra khi tài sản gặp rủi ro. Nguồn gốc của rủi ro có thể bao gồm từ những kẻ tấn công có ác tâm đến lỗi vô tình của con người. Nguồn rủi ro thậm chí có thể đến từ các mối nguy hiểm tự nhiên hoặc môi trường, chẳng hạn như lỗi cấu trúc hoặc mất điện.

Các quỹ của ngân hàng là một trong những tài sản quan trọng của nó. Nhóm của bạn đã liệt kê năm rủi ro chính đối với quỹ của ngân hàng:

* Thỏa hiệp email doanh nghiệp
* Cơ sở dữ liệu người dùng bị xâm phạm
* Hồ sơ tài chính bị rò rỉ
* Trộm cắp
* Tấn công chuỗi cung ứng

Hãy xem xét những rủi ro tiềm ẩn này liên quan đến môi trường hoạt động của ngân hàng. Sau đó, viết **2-3 câu (40-60 từ)** vào phần **Ghi chú** của mẫu mô tả các sự kiện bảo mật có thể xảy ra khi xem xét các rủi ro mà quỹ phải đối mặt trong môi trường hoạt động này.

|  |
| --- |
| **Step 4: Score risks based on their likelihood**  As you might recall, risk can be calculated with this simple formula:  **Likelihood x Impact = Risk**  In order to calculate the score for a security risk, you must first estimate and score the likelihood of the risk causing a security event. The likelihood of a risk can be based on available evidence, prior experience, or expert judgment. A common way to estimate the likelihood of the risk is to determine the potential frequency of the risk occurring:   * *Could the risk happen once a day?* * *Could the risk happen once a month?* * *Could the risk happen once in a year?*   For example, the bank must have enough funds available each day to meet its legal requirements. A potential risk that could prevent the bank from replenishing its funds is a supply chain disruption. Being located in a coastal area, there's a likelihood that the bank may experience supply chain disruptions caused by hurricanes. However, a hurricane might only impact the bank every few years, so you can score the likelihood as low.  In this instance, the team is scoring the likelihood of an event on a scale of 1-3:   * **1**represents an event with a *low* chance of occuring. * **2** represents an event with a *moderate* chance of occuring. * ***3***represents a *high* chance of occuring.   Review the **Risk(s)**, **Description**, and **Notes** of the risk register template. Refer to the risk matrix and use it to estimate a likelihood score for each risk. Then, enter a **score (1-3)** for each risk in the **Likelihood** column of the register. |

**Bước 4: Đánh giá rủi ro dựa trên khả năng xảy ra của chúng**

**Khả năng xảy ra x Tác động = Rủi ro**

Để tính điểm cho một rủi ro bảo mật, trước tiên bạn phải ước tính và cho điểm khả năng rủi ro gây ra sự kiện bảo mật. Khả năng xảy ra rủi ro có thể dựa trên bằng chứng sẵn có, kinh nghiệm trước đó hoặc đánh giá của chuyên gia. Một cách phổ biến để ước tính khả năng xảy ra rủi ro là xác định tần suất xảy ra rủi ro tiềm ẩn:

* *Rủi ro có thể xảy ra một lần một ngày?*
* *Rủi ro có thể xảy ra mỗi tháng một lần?*
* *Rủi ro có thể xảy ra mỗi năm một lần?*

Ví dụ, ngân hàng phải có đủ tiền mỗi ngày để đáp ứng các yêu cầu pháp lý của mình. Một rủi ro tiềm ẩn có thể ngăn cản ngân hàng bổ sung vốn là sự gián đoạn chuỗi cung ứng. Nằm ở khu vực ven biển, ngân hàng có khả năng gặp phải sự gián đoạn chuỗi cung ứng do bão gây ra. Tuy nhiên, một cơn bão chỉ có thể ảnh hưởng đến ngân hàng vài năm một lần, vì vậy bạn có thể cho điểm khả năng xảy ra là thấp.

Trong trường hợp này, nhóm đang cho điểm khả năng xảy ra sự kiện theo thang điểm từ 1-3:

* **1** đại diện cho một sự kiện có khả năng xảy ra *thấp* .
* **2** đại diện cho một sự kiện có khả năng xảy ra *vừa phải* .
* ***3*** thể hiệnkhả năng xảy ra *cao .*

Xem lại **(các) Rủi ro** , **Mô tả** và **Ghi chú** của mẫu đăng ký rủi ro. Tham khảo ma trận rủi ro và sử dụng nó để ước tính điểm khả năng cho từng rủi ro. Sau đó, nhập điểm **(1-3)** cho từng rủi ro vào cột **Khả năng** của sổ đăng ký.

|  |
| --- |
| **Step 5: Score risks based on their severity**  A severity score is an estimate of the overall impact that might occur as a result of an event. For example, damage can occur to a company's reputation or finances and there may be a loss of data, customers, or assets. Evaluating the severity of a risk helps businesses determine the level of risk they can tolerate and how assets might be affected.  When evaluating the severity of a risk, consider the potential consequences of that risk occurring:   * *How would the business be affected?* * *What's the financial harm to the business and its customers?* * *Can important operations or services be impacted?* * *Are there regulations that can be violated?* * *What is the reputational damage to the company's standing?*   Use the top row of the risk matrix and consider the potential *impact* of each risk. Estimate a severity score for each risk. Then, enter a **score (1-3)** for each risk in the **Severity** column of the register:   * **1** *(low severity)* * **2** *(moderate severity)* * **3** *(high severity)*   For example, a leak of financial records might lead to a loss of profits, a loss of customers, and heavy regulatory fines. A risk such as this might receive a severity score of 3 because it greatly impacts the bank's ability to operate. |

**Bước 5: Đánh giá rủi ro dựa trên mức độ nghiêm trọng của chúng**

Điểm mức độ nghiêm trọng là ước tính về tác động tổng thể có thể xảy ra do một sự kiện. Ví dụ: thiệt hại có thể xảy ra đối với danh tiếng hoặc tài chính của công ty và có thể mất dữ liệu, khách hàng hoặc tài sản. Đánh giá mức độ nghiêm trọng của rủi ro giúp doanh nghiệp xác định mức độ rủi ro mà họ có thể chịu đựng và tài sản có thể bị ảnh hưởng như thế nào.

Khi đánh giá mức độ nghiêm trọng của một rủi ro, hãy xem xét các hậu quả tiềm ẩn khi rủi ro đó xảy ra:

* *Việc kinh doanh sẽ bị ảnh hưởng như thế nào?*
* *Tác hại tài chính đối với doanh nghiệp và khách hàng là gì?*
* *Các hoạt động hoặc dịch vụ quan trọng có thể bị ảnh hưởng không?*
* *Có những quy định nào có thể bị vi phạm?*
* *Thiệt hại về danh tiếng đối với vị thế của công ty là gì?*

Sử dụng hàng trên cùng của ma trận rủi ro và xem xét *tác động* tiềm tàng của từng rủi ro. Ước tính mức độ nghiêm trọng cho từng rủi ro. Sau đó, nhập điểm **(1-3)** cho từng rủi ro vào cột **Mức độ nghiêm trọng** của sổ đăng ký:

* **1** *(mức độ nghiêm trọng thấp)*
* **2** *(mức độ nghiêm trọng vừa phải)*
* **3** *(mức độ nghiêm trọng cao)*

Ví dụ, việc rò rỉ hồ sơ tài chính có thể dẫn đến mất lợi nhuận, mất khách hàng và bị phạt nặng theo quy định. Rủi ro như thế này có thể nhận được điểm nghiêm trọng là 3 vì nó ảnh hưởng lớn đến khả năng hoạt động của ngân hàng.

|  |
| --- |
| **Step 6: Calculate an overall risk score**  Ultimately, the goal of performing a risk assessment is to help security teams prioritize their efforts and resources.  Using the risk formula, multiply the likelihood and severity score for each risk. Then, enter apriority **score (1-9)** for each of the risks in the **Priority** column of the register. |

**Bước 6: Tính điểm rủi ro tổng thể**

Cuối cùng, mục tiêu của việc thực hiện đánh giá rủi ro là giúp các nhóm bảo mật ưu tiên nỗ lực và nguồn lực của họ.

Sử dụng công thức rủi ro, nhân số khả năng xảy ra và mức độ nghiêm trọng của từng rủi ro. Sau đó, nhập điểm ưu tiên **(1-9)** cho từng rủi ro vào cột **Ưu tiên** của sổ đăng ký.

|  |
| --- |
| **What to Include in Your Response**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/d2Uj9VrGTUiBMpWaZRzVOA_e818b0f4bbef49b4ad7b2c406805d3f1_image.png?expiry=1718928000000&hmac=EIUAhxm5w1NSe7gwzmh_wYaJWKIoIPxSLWdbPDvKHUQ  Be sure to address the following criteria in your completed activity:   * 2-3 sentences describing the risk factors * 5 likelihood scores * 5 severity scores * 5 overall risk scores |

**Những gì cần bao gồm trong phản hồi của bạn**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/d2Uj9VrGTUiBMpWaZRzVOA_e818b0f4bbef49b4ad7b2c406805d3f1_image.png?expiry=1718928000000&hmac=EIUAhxm5w1NSe7gwzmh_wYaJWKIoIPxSLWdbPDvKHUQ

Hãy đảm bảo giải quyết các tiêu chí sau trong hoạt động đã hoàn thành của bạn:

* 2-3 câu mô tả yếu tố nguy cơ
* 5 điểm khả năng
* 5 điểm mức độ nghiêm trọng
* 5 điểm rủi ro tổng thể

***4.6. Activity Exemplar: Score risks based on their likelihood and severity - Ví dụ về hoạt động: Đánh giá rủi ro dựa trên khả năng xảy ra và mức độ nghiêm trọng của chúng***

|  |
| --- |
| **Activity Exemplar: Score risks based on their likelihood and severity**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Ví dụ về hoạt động: Đánh giá rủi ro dựa trên khả năng xảy ra và mức độ nghiêm trọng của chúng**

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/4uSbN9IKSGKp7mmMgynaFw_91083a84620e42d5a6f98c51cfacbff1_image.png?expiry=1718928000000&hmac=JB5VrSbvtgw7ky34VDkWIdhZ6Y0soTImQCj4Ge7F1gA  To review the exemplar for this course item, click the following link and select *Use Template*.  Link to exemplar:[Risk register](https://docs.google.com/document/d/1go-P591TEFasex_iNcz8D8FmYNelwaGDyahGZD2swh4/template/preview?usp=sharing) |

**Mẫu đã hoàn thành**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/4uSbN9IKSGKp7mmMgynaFw_91083a84620e42d5a6f98c51cfacbff1_image.png?expiry=1718928000000&hmac=JB5VrSbvtgw7ky34VDkWIdhZ6Y0soTImQCj4Ge7F1gA

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Đăng ký rủi ro](https://docs.google.com/document/d/1go-P591TEFasex_iNcz8D8FmYNelwaGDyahGZD2swh4/template/preview?usp=sharing)

|  |
| --- |
| **Assessment of Exemplar**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/PbMiD4olS_Wu94ezCyVg3g_8e949e2d845c4e37ad3f90766ca3eaf1_image.png?expiry=1718928000000&hmac=ntiNsbZWX8jEjyu3wkcvgVU74MOAlEsYmQC7pArk1lQ  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course. |

**Đánh giá mẫu mực**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/PbMiD4olS_Wu94ezCyVg3g_8e949e2d845c4e37ad3f90766ca3eaf1_image.png?expiry=1718928000000&hmac=ntiNsbZWX8jEjyu3wkcvgVU74MOAlEsYmQC7pArk1lQ

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong suốt khóa học.

|  |
| --- |
| ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that you've considered how likelihood and impact affect how organizations approach risk management.* |

***Lưu ý:*** *Ví dụ thể hiện một cách khả thi để hoàn thành hoạt động. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là bạn đã xem xét khả năng xảy ra và tác động ảnh hưởng như thế nào đến cách các tổ chức tiếp cận quản lý rủi ro.*

|  |
| --- |
| https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/fHJszLYKTsWS6CWbYRaS9Q_f40dcdc681c8425ba9249ff265e4bbf1_image.png?expiry=1718928000000&hmac=tHCS0n66M5whHWIpZ8IPQrfEe8BclYRFVOgNjC4hhAY  Next, you can review the results of a completed risk register: |

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/fHJszLYKTsWS6CWbYRaS9Q_f40dcdc681c8425ba9249ff265e4bbf1_image.png?expiry=1718928000000&hmac=tHCS0n66M5whHWIpZ8IPQrfEe8BclYRFVOgNjC4hhAY

Tiếp theo, bạn có thể xem lại kết quả của việc đăng ký rủi ro đã hoàn thành:

|  |
| --- |
| **Notes** |

**Ghi chú**

|  |
| --- |
| Some risk factors to have considered might have been the number of other companies that interact with the bank. These sources of risk might introduce incidents beyond the bank's control. Also, the risk of theft is important to consider because of the number of customers and the operational impact it could have to the business. |

Một số yếu tố rủi ro cần xem xét có thể là số lượng các công ty khác tương tác với ngân hàng. Những nguồn rủi ro này có thể gây ra các sự cố ngoài tầm kiểm soát của ngân hàng. Ngoài ra, nguy cơ trộm cắp là điều quan trọng cần xem xét vì số lượng khách hàng và tác động hoạt động mà nó có thể gây ra cho doanh nghiệp.

|  |
| --- |
| **Likelihood** |

**Khả năng**

|  |
| --- |
| A range of likelihood scores were estimated based on factors that could lead to a security incident. Each risk was scored as a 1, 2, or 3 on a risk matrix, meaning the chances of occurring were rare, likely, or certain. A supply chain attack caused by natural disaster was scored with a 1, meaning it was regarded as unlikely due to the unpredictability of those events. On the other hand, compromised data events were scored a 2 because they are likely to occur given the possible causes. |

Một loạt các điểm có khả năng được ước tính dựa trên các yếu tố có thể dẫn đến sự cố bảo mật. Mỗi rủi ro được tính điểm 1, 2 hoặc 3 trên ma trận rủi ro, nghĩa là khả năng xảy ra là hiếm, có thể xảy ra hoặc chắc chắn. Một cuộc tấn công vào chuỗi cung ứng do thiên tai gây ra được cho điểm 1, nghĩa là nó được coi là khó xảy ra do không thể đoán trước được những sự kiện đó. Mặt khác, các sự kiện dữ liệu bị xâm phạm được cho điểm 2 vì chúng có khả năng xảy ra do các nguyên nhân có thể xảy ra.

|  |
| --- |
| **Severity** |

**Mức độ nghiêm trọng**

|  |
| --- |
| No risk received a severity score less than 2 because risks that involve data breaches such as business email compromise, can have serious consequences. Customers at a bank trust the businesses to protect their money and personal information. Also, the bank's operations could be terminated if they fail to comply with regulations. |

Không có rủi ro nào nhận được điểm nghiêm trọng dưới 2 vì các rủi ro liên quan đến vi phạm dữ liệu như xâm phạm email doanh nghiệp có thể gây ra hậu quả nghiêm trọng. Khách hàng tại ngân hàng tin tưởng doanh nghiệp sẽ bảo vệ tiền và thông tin cá nhân của họ. Ngoài ra, hoạt động của ngân hàng có thể bị chấm dứt nếu không tuân thủ quy định.

|  |
| --- |
| **Priority** |

**Sự ưu tiên**

|  |
| --- |
| A financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and would greatly impact the bank's ability to operate. Such a high overall score signals the security team to prioritize remediating, or resolving any issues related to that risk before moving on to risks that scored lower. |

Vụ rò rỉ hồ sơ tài chính nhận được điểm rủi ro tổng thể cao nhất là 9. Điều này cho thấy rủi ro này gần như chắc chắn xảy ra và sẽ ảnh hưởng lớn đến khả năng hoạt động của ngân hàng. Điểm tổng thể cao như vậy báo hiệu cho nhóm bảo mật ưu tiên khắc phục hoặc giải quyết mọi vấn đề liên quan đến rủi ro đó trước khi chuyển sang các rủi ro có điểm thấp hơn.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Risk assessments are useful for identifying risks to an organization’s information, networks and systems. Security plans can benefit from regular risk assessments as a way of highlighting important concerns that should be addressed. Additionally, these assessments help keep track of any changes that can occur in an organization's operating environment. |

Đánh giá rủi ro rất hữu ích trong việc xác định rủi ro đối với thông tin, mạng và hệ thống của tổ chức. Các kế hoạch bảo mật có thể được hưởng lợi từ việc đánh giá rủi ro thường xuyên như một cách làm nổi bật những mối quan tâm quan trọng cần được giải quyết. Ngoài ra, những đánh giá này giúp theo dõi mọi thay đổi có thể xảy ra trong môi trường hoạt động của tổ chức.

**5. Review: Introduction to asset security – Review: Giới thiệu về bảo đảm tài sản**

***5.1. Wrap-up – Tóm tắt***

|  |
| --- |
| Well done! You made it to the end of this section! Being a security practitioner takes commitment and a desire to learn. A big part of the job involves keeping current with best practices and emerging trends. Thinking back on my own journey into the world of security, I'm so proud of you for your continued commitment. We've covered a lot of material this week, and this is a good time to reflect and look back on the key concepts we explored together. |

Làm tốt! Bạn đã đi đến cuối phần này!Là một người thực hành an ninhcó sự cam kết và mong muốn học hỏi.Một phần lớn công việc liên quan đến việc cập nhật thông tinthực tiễn tốt nhất và xu hướng mới nổi.Nghĩ lại hành trình của chính mìnhvào thế giới an ninh,Tôi rất tự hào về bạn vì sự cam kết liên tục của bạn.Chúng tôi đã đề cập đến rất nhiều tài liệu trong tuần này vàđây là thời điểm tốt để suy ngẫm và nhìn lạivề các khái niệm chính mà chúng ta đã cùng nhau khám phá.

|  |
| --- |
| We covered the building blocks of organizational risk management: assets, threats, and vulnerabilities. |

Chúng tôi đã đề cập đến các khối xây dựng củaQuản lý rủi ro tổ chức:tài sản, mối đe dọa và điểm yếu.

|  |
| --- |
| We also spent some time demonstrating the importance of asset inventories. It's much easier to protect company assets if you know where they are and who's responsible for them. |

Chúng tôi cũng dành thời gian chứng minhtầm quan trọng của việc kiểm kê tài sản.Việc bảo vệ tài sản của công ty sẽ dễ dàng hơn nhiều nếubạn biết họ ở đâu và ai chịu trách nhiệm về họ.

|  |
| --- |
| After that, we moved on to explore the challenges in a rapidly changing digital world. Part of protecting data in this world is understanding if it's in use, in transit, or at rest. |

Sau đó chúng tôi chuyển sang tìm hiểunhững thách thức trong một thế giới kỹ thuật số đang thay đổi nhanh chóng.Một phần của việc bảo vệ dữ liệu trên thế giới nàylà hiểu nếu nó được sử dụng,đang di chuyển hoặc ở trạng thái nghỉ ngơi.

|  |
| --- |
| Finally, in our high-level exploration of policies, standards, and procedures, we talked about how each of them factor into achieving security goals. There's no one-size-fits-all approach to achieving security. While exploring the NIST Cybersecurity Framework, you gained an appreciation of how it supports good security practices. |

Cuối cùng, trong cuộc khám phá cấp cao của chúng tôichính sách, tiêu chuẩn,và các thủ tục, chúng tôi đã nói vềmỗi yếu tố trong số đó ảnh hưởng như thế nào đến việc đạt được các mục tiêu bảo mật.Không có một kích cỡ phù hợp cho tất cảcách tiếp cận để đạt được an ninh.Trong khi khám phá Khung an ninh mạng NIST,bạn đã có được sự đánh giá cao về cách nóhỗ trợ thực hành bảo mật tốt.

|  |
| --- |
| Attackers are also constantly building their skills and finding new ways to break through the defenses we put up. Remember, the landscape is always changing. There's always more to learn if you want to be a good security practitioner. |

Những kẻ tấn công cũng không ngừng xây dựng kỹ năng của mìnhvà tìm ra những cách mới để phá vỡthông qua hàng phòng thủ mà chúng tôi đã dựng lên.Hãy nhớ rằng, cảnh quan luôn thay đổi.Luôn có nhiều điều để học nếu bạn muốnđể trở thành một người thực hành an ninh tốt.

|  |
| --- |
| Next up, we're going to expand our security mindset by learning more about the different systems security teams use to protect organizational assets. I'm looking forward to it! |

Tiếp theo, chúng tôi sẽ mở rộngtư duy bảo mật của chúng tôi bằng cách tìm hiểu thêm vềcác nhóm bảo mật hệ thống khác nhau sử dụngđể bảo vệ tài sản của tổ chức.Tôi đang mong chờ nó!

***5.2. Glossary terms from module 1 - Thuật ngữ thuật ngữ từ mô-đun 1***

|  |
| --- |
| **Glossary terms from module 1** |

**Thuật ngữ thuật ngữ từ mô-đun 1**

|  |
| --- |
| **Terms and definitions from Course 5, Module 1** |

**Các thuật ngữ và định nghĩa trong Khóa 5, Học phần 1**

|  |
| --- |
| **Asset:** An item perceived as having value to an organization |

**Tài sản:** Một vật phẩm được coi là có giá trị đối với một tổ chức

|  |
| --- |
| **Asset classification:** The practice of labeling assets based on sensitivity and importance to an organization |

**Phân loại tài sản:** Việc dán nhãn tài sản dựa trên mức độ nhạy cảm và tầm quan trọng đối với một tổ chức

|  |
| --- |
| **Asset inventory:** A catalog of assets that need to be protected |

**Kiểm kê tài sản:** Danh mục tài sản cần được bảo vệ

|  |
| --- |
| **Asset management:** The process of tracking assets and the risks that affect them |

**Quản lý tài sản:** Quá trình theo dõi tài sản và những rủi ro ảnh hưởng đến chúng

|  |
| --- |
| **Compliance:** The process of adhering to internal standards and external regulations |

**Tuân thủ:** Quá trình tuân thủ các tiêu chuẩn nội bộ và quy định bên ngoài

|  |
| --- |
| **Data:** Information that is translated, processed, or stored by a computer |

**Dữ liệu:** Thông tin được dịch, xử lý hoặc lưu trữ bởi máy tính

|  |
| --- |
| **Data at rest:** Data not currently being accessed |

**Dữ liệu ở trạng thái nghỉ:** Dữ liệu hiện không được truy cập

|  |
| --- |
| **Data in transit:** Data traveling from one point to another |

**Dữ liệu đang truyền:** Dữ liệu di chuyển từ điểm này sang điểm khác

|  |
| --- |
| **Data in use:** Data being accessed by one or more users |

**Dữ liệu đang sử dụng:** Dữ liệu đang được một hoặc nhiều người dùng truy cập

|  |
| --- |
| **Information security (InfoSec):** The practice of keeping data in all states away from unauthorized users |

**Bảo mật thông tin (InfoSec):** Thực hành giữ dữ liệu ở mọi trạng thái tránh xa người dùng trái phép

|  |
| --- |
| **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk |

**Khung an ninh mạng (CSF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST):** Một khung tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và biện pháp thực hành tốt nhất để quản lý rủi ro an ninh mạng

|  |
| --- |
| **Policy:** A set of rules that reduce risk and protect information |

**Chính sách:** Một bộ quy tắc nhằm giảm thiểu rủi ro và bảo vệ thông tin

|  |
| --- |
| **Procedures:** Step-by-step instructions to perform a specific security task |

**Quy trình:** Hướng dẫn từng bước để thực hiện một tác vụ bảo mật cụ thể

|  |
| --- |
| **Regulations:** Rules set by a government or other authority to control the way something is done |

**Quy định:** Các quy tắc do chính phủ hoặc cơ quan có thẩm quyền khác đặt ra để kiểm soát cách thức thực hiện một việc gì đó

|  |
| --- |
| **Risk**: Anything that can impact confidentiality, integrity, or availability of an asset |

**Rủi ro** : Bất cứ điều gì có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của tài sản

|  |
| --- |
| **Standards:** References that inform how to set policies |

**Tiêu chuẩn:** Tài liệu tham khảo cho biết cách thiết lập chính sách

|  |
| --- |
| **Threat:** Any circumstance or event that can negatively impact assets |

**Mối đe dọa:** Bất kỳ tình huống hoặc sự kiện nào có thể tác động tiêu cực đến tài sản

|  |
| --- |
| **Vulnerability:** A weakness that can be exploited by a threat |

**Tính dễ bị tổn thương:** Điểm yếu có thể bị khai thác bởi mối đe dọa

***5.3. Module 1 challenge - Thử thách mô-đun 1***

# **Module 2: Protect organizational assets - Bảo vệ tài sản tổ chức**

|  |
| --- |
| You will focus on security controls that protect organizational assets. You'll explore how privacy impacts asset security and understand the role that encryption plays in maintaining the privacy of digital assets. You'll also explore how authentication and authorization systems help verify a user’s identity. |

Bạn sẽ tập trung vào các biện pháp kiểm soát bảo mật để bảo vệ tài sản của tổ chức. Bạn sẽ khám phá quyền riêng tư tác động như thế nào đến bảo mật tài sản và hiểu vai trò của mã hóa trong việc duy trì quyền riêng tư của tài sản kỹ thuật số. Bạn cũng sẽ khám phá cách hệ thống xác thực và ủy quyền giúp xác minh danh tính người dùng.

|  |
| --- |
| **Learning Objectives**   * Identify effective data handling processes. * Identify how security controls mitigate risk. * Discuss the role encryption and hashing play in securing assets. * Describe how to effectively use authentication as a security control. * Describe effective authorization practices that verify user access. |

**Mục tiêu học tập**

* Xác định các quy trình xử lý dữ liệu hiệu quả.
* Xác định cách kiểm soát bảo mật giảm thiểu rủi ro.
* Thảo luận về vai trò của mã hóa và băm trong việc bảo mật tài sản.
* Mô tả cách sử dụng hiệu quả xác thực như một biện pháp kiểm soát bảo mật.
* Mô tả các phương pháp ủy quyền hiệu quả để xác minh quyền truy cập của người dùng.

**1. Safeguard information - Thông tin bảo vệ**

***1.1. Welcome to module 2 - Chào mừng đến với mô-đun 2***

|  |
| --- |
| I was fascinated by a world-wide malware event that happened in 2017. I started watching videos and preparing to take certification tests, just like you. I felt overwhelmed at first, but my curiosity and passion has driven me to continue learning in this field. I always remind myself that no one is born knowing everything and everyone is on a learning journey. Even now, I still remember what it was like to start out in this profession. So, believe me when I tell you that you're making great progress, and I am proud of your effort! Now, before looking ahead to where we're headed on our journey into the world of security, let's take a moment to look back on where we've been. |

Tôi bị mê hoặc bởimột sự kiện phần mềm độc hại trên toàn thế giới đã xảy ra vào năm 2017.Tôi bắt đầu xem video và chuẩn bị quaykiểm tra chứng chỉ, giống như bạn.Lúc đầu tôi cảm thấy choáng ngợp,nhưng sự tò mò và đam mê của tôi đãthúc đẩy tôi tiếp tục học tập trong lĩnh vực này.Tôi luôn nhắc nhở mình rằng không có aisinh ra đã biết mọi thứ vàmọi người đều đang trên hành trình học tập.Đến tận bây giờ tôi vẫn nhớ nó là gìmuốn bắt đầu với nghề này.Vì vậy, hãy tin tôi khi tôi nói với bạn rằng bạn đang làmsự tiến bộ vượt bậc và tôi tự hào về nỗ lực của bạn!Bây giờ, trước khi nhìn về phía trước nơi chúng ta đang ởhướng tới cuộc hành trình của chúng ta vào thế giới an ninh,hãy dành một chút thời gian để nhìn lại nơi chúng ta đã đến.

|  |
| --- |
| Previously, we focused mostly on the concept of assets and risks in security. We covered topics like the importance of managing assets and keeping them safe. We discussed how the digital world presents new challenges and opportunities in the field of security. We also spent some time exploring security plans. |

Trước đây chúng tôi tập trung chủ yếu vàokhái niệm về tài sản và rủi ro trong chứng khoán.Chúng tôi đề cập đến các chủ đề như tầm quan trọng củaquản lý tài sản và giữ chúng an toàn.Chúng tôi đã thảo luận về cách thế giới kỹ thuật số thể hiệnnhững thách thức và cơ hội mớitrong lĩnh vực an ninh.Chúng tôi cũng dành thời gian khám phá các kế hoạch bảo mật.

|  |
| --- |
| With this solid foundation, we're ready to keep expanding our security mindset. In this section, we'll cover the security controls that are used to proactively keep assets safe. I used the word proactively there on purpose. As you'll soon discover, these controls are the protections that we put in place to stop problems before they happen. |

Với nền tảng vững chắc này,chúng tôi sẵn sàng tiếp tục mở rộng tư duy bảo mật của mình.Trong phần này, chúng tôi sẽ đề cập đến các biện pháp kiểm soát bảo mậtđược sử dụng để chủ động giữ tài sản an toàn.Tôi đã cố ý sử dụng từ này một cách chủ động.Như bạn sẽ sớm khám phá ra,những biện pháp kiểm soát này là biện pháp bảo vệ mà chúng tôi đặttại chỗ để ngăn chặn vấn đề trước khi chúng xảy ra.

|  |
| --- |
| We're going to begin by taking an in-depth look at privacy. Here, you'll learn about the effective data handling processes that keep information safe. Next, you'll explore the role of encryption and hashing in safeguarding information. Finally, you'll learn about the standard access controls that companies use to authorize and authenticate users. Alright, are you ready to keep moving ahead? I know I am! |

Chúng ta sẽ bắt đầu bằng việc lấycái nhìn sâu sắc về quyền riêng tư.Tại đây, bạn sẽ tìm hiểu về cách xử lý dữ liệu hiệu quảcác quy trình giữ thông tin an toàn.Tiếp theo, bạn sẽ khám phá vai trò củamã hóa và băm trong việc bảo vệ thông tin.Cuối cùng, bạn sẽ tìm hiểu vềcác biện pháp kiểm soát truy cập tiêu chuẩncác công ty sử dụng để ủy quyền và xác thực người dùng.Được rồi, bạn đã sẵn sàng tiếp tục tiến về phía trước chưa? Tôi biết tôi là vậy!

***1.2. Security controls - Kiểm soát an ninh***

|  |
| --- |
| These days, information is in so many places at once. As a result, organizations are under a lot of pressure to implement effective security controls that protects everyone's information from being stolen or exposed. Security controls are safeguards designed to reduce specific security risks. They include a wide range of tools that protect assets before, during, and after an event. |

Ngày nay, thông tin có ở rất nhiều nơi cùng một lúc.Kết quả là, các tổ chức phải chịu rất nhiều áp lực để thực hiện hiệu quảkiểm soát bảo mật nhằm bảo vệ thông tin của mọi người khỏi bị đánh cắp hoặc bị lộ.Kiểm soát bảo mật là các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể.Chúng bao gồm một loạt các công cụ bảo vệ tài sản trước, trong vàsau một sự kiện.

|  |
| --- |
| Security controls can be organized into three types: technical, operational, and managerial. |

Kiểm soát an ninh có thể được tổ chức thành ba loại:kỹ thuật, vận hành và quản lý.

|  |
| --- |
| Technical control types include the many technologies used to protect assets. This includes encryption, authentication systems, and others. |

Các loại kiểm soát kỹ thuật bao gồm nhiều công nghệ được sử dụng để bảo vệ tài sản.Điều này bao gồm mã hóa, hệ thống xác thực và các hệ thống khác.

|  |
| --- |
| Operational controls relate to maintaining the day-to-day security environment. Generally, people perform these controls like awareness training and incident response. |

Kiểm soát hoạt động liên quan đến việc duy trì môi trường an ninh hàng ngày.Nói chung, mọi người thực hiện các biện pháp kiểm soát này như đào tạo nhận thức vàứng phó sự cố.

|  |
| --- |
| Managerial controls are centered around how the other two reduce risk. Examples of management controls include policies, standards, and procedures. |

Kiểm soát quản lý tập trung vào cách hai biện pháp còn lại giảm thiểu rủi ro.Ví dụ về kiểm soát quản lý bao gồm các chính sách, tiêu chuẩn và thủ tục.

|  |
| --- |
| Typically, organization's security policy outlines the controls needed to achieve their goals. Information privacy plays a key role in these decisions. Information privacy is the protection of unauthorized access and distribution of data. Information privacy is about the right to choose. People and organizations alike deserve the right to decide when, how, and to what extent private information about them is shared. Security controls are the technologies used to regulate information privacy. |

Thông thường, chính sách bảo mật của tổ chức phác thảo các biện pháp kiểm soát cần thiết để đạt được mục tiêu của họ.Quyền riêng tư thông tin đóng một vai trò quan trọng trong các quyết định này.Bảo mật thông tin là việc bảo vệ những truy cập trái phép vàphân phối dữ liệu.Bảo mật thông tin là về quyền lựa chọn.Mọi người và các tổ chức đều xứng đáng có quyền quyết định khi nào, như thế nào vàthông tin cá nhân về họ được chia sẻ ở mức độ nào.Kiểm soát bảo mật là các công nghệ được sử dụng để quản lý quyền riêng tư thông tin.

|  |
| --- |
| For example, imagine using a travel app to book a flight. You might browse through a list of flights and find one at a good price. To reserve a seat, you enter some personal information, like your name, email, and credit card number for payment. The transaction goes through successfully, and you booked your flight. Now, you reasonably expect the airline company to access this information you enter when signing up to complete the reservation. |

Ví dụ: hãy tưởng tượng bạn sử dụng ứng dụng du lịch để đặt chuyến bay.Bạn có thể duyệt qua danh sách các chuyến bay và tìm một chuyến bay có giá tốt.Để đặt chỗ, bạn nhập một số thông tin cá nhân, như tên, email vàsố thẻ tín dụng để thanh toán.Giao dịch diễn ra thành công và bạn đã đặt chuyến bay.Bây giờ, bạn có lý do hợp lý để mong đợi công ty hàng không truy cập được thông tin nàythông tin bạn nhập khi đăng ký để hoàn tất việc đặt chỗ.

|  |
| --- |
| However, should everyone at the company have access to your information? A person working in the marketing department shouldn't need access to your credit card information. It makes sense to share that information with a customer support agent. Except, they should only need to access it while helping with your reservation. To maintain privacy, security controls are intended to limit access based on the user and situation. This is known as the principle of least privilege. |

Tuy nhiên, mọi người trong công ty có nên truy cập vào thông tin của bạn không?Một người làm việc trong bộ phận tiếp thị không cần truy cậpđến thông tin thẻ tín dụng của bạn.Việc chia sẻ thông tin đó với nhân viên hỗ trợ khách hàng là điều hợp lý.Ngoại trừ việc họ chỉ cần truy cập nó trong khi giúp bạn đặt chỗ.Để duy trì sự riêng tư,kiểm soát bảo mật nhằm hạn chế quyền truy cập dựa trên người dùng và tình huống.Điều này được gọi là nguyên tắc đặc quyền tối thiểu.

|  |
| --- |
| Security controls should be designed with the principle of least privilege in mind. When they are, they rely on differentiating between data owners and data custodians. |

Các biện pháp kiểm soát an ninh phải được thiết kế dựa trên nguyên tắc đặc quyền tối thiểu.Khi đó, họ dựa vào sự khác biệt giữa chủ sở hữu dữ liệu vàngười giám sát dữ liệu.

|  |
| --- |
| A data owner is a person who decides who can access, edit, use, or destroy their information. The idea is very straightforward except in cases where there are multiple owners. For example, the intellectual property of an organization can have multiple data owners. |

Chủ sở hữu dữ liệu là người quyết định ai có thể truy cập, chỉnh sửa, sử dụng hoặchủy thông tin của họ.Ý tưởng rất đơn giản trừ trường hợp có nhiều chủ sở hữu.Ví dụ, tài sản trí tuệ của một tổ chức có thể cónhiều chủ sở hữu dữ liệu.

|  |
| --- |
| A data custodian is anyone or anything that's responsible for the safe handling, transport, and storage of information. Did you notice that I mentioned, "anything?" That's because, aside from people, organizations and their systems are also custodians of people's information. |

Người giám sát dữ liệu là bất cứ ai hoặc bất cứ điều gì chịu trách nhiệm vềxử lý, vận chuyển và lưu trữ thông tin một cách an toàn.Bạn có để ý rằng tôi đã đề cập đến "bất cứ điều gì không?"Đó là bởi vì, ngoài con người, các tổ chức vàhệ thống của họ cũng là người giám sát thông tin của mọi người.

|  |
| --- |
| There are other considerations besides these when implementing security controls. Remember that data is an asset. Like any other asset, information privacy requires proper classification and handling. As we progress in this section, we'll continue exploring other security controls that make this possible. |

Có những cân nhắc khác ngoài những điều này khi thực hiện kiểm soát bảo mật.Hãy nhớ rằng dữ liệu là một tài sản.Giống như bất kỳ tài sản nào khác, quyền riêng tư thông tin đòi hỏi phải có sự phân loại vàsự điều khiển.Khi chúng ta tiến triển trong phần này,chúng tôi sẽ tiếp tục khám phá các biện pháp kiểm soát bảo mật khác để biến điều này thành hiện thực.

***1.3. Principle of least privilege - Nguyên tắc đặc quyền tối thiểu***

|  |
| --- |
| **Principle of least privilege** |

**Nguyên tắc đặc quyền tối thiểu**

|  |
| --- |
| Security controls are essential to keeping sensitive data private and safe. One of the most common controls is the principle of least privilege, also referred to as PoLP or least privilege. The **principle of least privilege** is a security concept in which a user is only granted the minimum level of access and authorization required to complete a task or function. |

Kiểm soát bảo mật là điều cần thiết để giữ cho dữ liệu nhạy cảm được riêng tư và an toàn. Một trong những biện pháp kiểm soát phổ biến nhất là nguyên tắc đặc quyền tối thiểu, còn được gọi là PoLP hoặc đặc quyền tối thiểu. Nguyên **tắc đặc quyền tối thiểu** là một khái niệm bảo mật trong đó người dùng chỉ được cấp mức truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ hoặc chức năng.

|  |
| --- |
| Least privilege is a fundamental security control that supports the confidentiality, integrity, and availability (CIA) triad of information. In this reading, you'll learn how the principle of least privilege reduces risk, how it's commonly implemented, and why it should be routinely audited. |

Đặc quyền tối thiểu là biện pháp kiểm soát bảo mật cơ bản hỗ trợ bộ ba thông tin bảo mật, toàn vẹn và sẵn sàng (CIA). Trong bài đọc này, bạn sẽ tìm hiểu nguyên tắc đặc quyền tối thiểu làm giảm rủi ro như thế nào, nguyên tắc này được triển khai phổ biến như thế nào và tại sao nguyên tắc này cần được kiểm tra thường xuyên.

|  |
| --- |
| **Limiting access reduces risk** |

**Hạn chế quyền truy cập làm giảm rủi ro**

|  |
| --- |
| Every business needs to plan for the risk of data theft, misuse, or abuse. Implementing the principle of least privilege can greatly reduce the risk of costly incidents like data breaches by:   * Limiting access to sensitive information * Reducing the chances of accidental data modification, tampering, or loss * Supporting system monitoring and administration |

Mỗi doanh nghiệp cần lập kế hoạch cho nguy cơ bị đánh cắp, sử dụng sai hoặc lạm dụng dữ liệu. Việc thực hiện nguyên tắc đặc quyền tối thiểu có thể giảm đáng kể nguy cơ xảy ra các sự cố tốn kém như vi phạm dữ liệu bằng cách:

* Hạn chế quyền truy cập vào thông tin nhạy cảm
* Giảm nguy cơ vô tình sửa đổi, giả mạo hoặc mất dữ liệu
* Hỗ trợ giám sát và quản lý hệ thống

|  |
| --- |
| Least privilege greatly reduces the likelihood of a successful attack by connecting specific resources to specific users and placing limits on what they can do. It's an important security control that should be applied to any asset. Clearly defining who or what your users are is usually the first step of implementing least privilege effectively. |

Đặc quyền tối thiểu làm giảm đáng kể khả năng tấn công thành công bằng cách kết nối các tài nguyên cụ thể với người dùng cụ thể và đặt giới hạn cho những gì họ có thể làm. Đó là một biện pháp kiểm soát bảo mật quan trọng nên được áp dụng cho bất kỳ tài sản nào. Xác định rõ ràng ai hoặc người dùng của bạn là ai thường là bước đầu tiên để triển khai đặc quyền tối thiểu một cách hiệu quả.

|  |
| --- |
| **Note:** Least privilege is closely related to another fundamental security principle, the *separation of duties—*a security concept that divides tasks and responsibilities among different users to prevent giving a single user complete control over critical business functions. You'll learn more about separation of duties in a different reading about identity and access management. |

**Lưu ý:** Đặc quyền tối thiểu có liên quan chặt chẽ đến một nguyên tắc bảo mật cơ bản khác, đó là *sự phân chia nhiệm vụ—* một khái niệm bảo mật phân chia nhiệm vụ và trách nhiệm giữa những người dùng khác nhau nhằm ngăn chặn việc trao cho một người dùng duy nhất quyền kiểm soát hoàn toàn đối với các chức năng kinh doanh quan trọng. Bạn sẽ tìm hiểu thêm về việc phân chia nhiệm vụ trong phần đọc khác về quản lý danh tính và quyền truy cập.

|  |
| --- |
| **Determining access and authorization** |

**Xác định quyền truy cập và ủy quyền**

|  |
| --- |
| To implement least privilege, access and authorization must be determined first. There are two questions to ask to do so:   * Who is the user? * How much access do they need to a specific resource? |

Để thực hiện đặc quyền tối thiểu, quyền truy cập và ủy quyền phải được xác định trước tiên. Có hai câu hỏi để yêu cầu làm như vậy:

* Người sử dụng là ai?
* Họ cần bao nhiêu quyền truy cập vào một tài nguyên cụ thể?

|  |
| --- |
| Determining who the user is usually straightforward. A user can refer to a person, like a customer, an employee, or a vendor. It can also refer to a device or software that's connected to your business network. In general, every user should have their own account. Accounts are typically stored and managed within an organization's directory service. |

Việc xác định ai là người dùng thường đơn giản. Người dùng có thể đề cập đến một người, như khách hàng, nhân viên hoặc nhà cung cấp. Nó cũng có thể đề cập đến một thiết bị hoặc phần mềm được kết nối với mạng doanh nghiệp của bạn. Nói chung, mỗi người dùng nên có tài khoản riêng. Các tài khoản thường được lưu trữ và quản lý trong dịch vụ thư mục của tổ chức.

|  |
| --- |
| These are the most common types of user accounts:   * **Guest accounts** are provided to external users who need to access an internal network, like customers, clients, contractors, or business partners. * **User accounts** are assigned to staff based on their job duties. * **Service accounts** are granted to applications or software that needs to interact with other software on the network. * **Privileged accounts** have elevated permissions or administrative access. |

Đây là những loại tài khoản người dùng phổ biến nhất:

* **Tài khoản khách** được cung cấp cho người dùng bên ngoài cần truy cập mạng nội bộ, như khách hàng, khách hàng, nhà thầu hoặc đối tác kinh doanh.
* **Tài khoản người dùng** được phân công cho nhân viên dựa trên nhiệm vụ công việc của họ.
* **Tài khoản dịch vụ** được cấp cho các ứng dụng hoặc phần mềm có nhu cầu tương tác với các phần mềm khác trên mạng.
* **Tài khoản đặc quyền** có quyền nâng cao hoặc quyền truy cập quản trị.

|  |
| --- |
| It's best practice to determine a baseline access level for each account type before implementing least privilege. However, the appropriate access level can change from one moment to the next. For example, a customer support representative should only have access to your information while they are helping you. Your data should then become inaccessible when the support agent starts working with another customer and they are no longer actively assisting you. Least privilege can only reduce risk if user accounts are routinely and consistently monitored. |

Cách tốt nhất là xác định cấp truy cập cơ bản cho từng loại tài khoản trước khi triển khai đặc quyền tối thiểu. Tuy nhiên, mức độ truy cập phù hợp có thể thay đổi theo từng thời điểm. Ví dụ: đại diện hỗ trợ khách hàng chỉ được phép truy cập thông tin của bạn khi họ đang trợ giúp bạn. Sau đó, dữ liệu của bạn sẽ không thể truy cập được khi nhân viên hỗ trợ bắt đầu làm việc với một khách hàng khác và họ không còn tích cực hỗ trợ bạn nữa. Đặc quyền tối thiểu chỉ có thể giảm thiểu rủi ro nếu tài khoản người dùng được giám sát thường xuyên và nhất quán.

|  |
| --- |
| **Pro tip:** Passwords play an important role when implementing the principle of least privilege. Even if user accounts are assigned appropriately, an insecure password can compromise your systems. |

**Mẹo chuyên nghiệp:** Mật khẩu đóng vai trò quan trọng khi thực hiện nguyên tắc đặc quyền tối thiểu. Ngay cả khi tài khoản người dùng được chỉ định phù hợp, mật khẩu không an toàn có thể làm tổn hại đến hệ thống của bạn.

|  |
| --- |
| **Auditing account privileges** |

**Kiểm tra đặc quyền tài khoản**

|  |
| --- |
| Setting up the right user accounts and assigning them the appropriate privileges is a helpful first step. Periodically auditing those accounts is a key part of keeping your company’s systems secure. |

Thiết lập đúng tài khoản người dùng và gán cho họ những đặc quyền phù hợp là bước đầu tiên hữu ích. Kiểm tra định kỳ các tài khoản đó là một phần quan trọng để giữ an toàn cho hệ thống của công ty bạn.

|  |
| --- |
| There are three common approaches to auditing user accounts:   * Usage audits * Privilege audits * Account change audits |

Có ba cách tiếp cận phổ biến để kiểm tra tài khoản người dùng:

* Kiểm tra việc sử dụng
* Kiểm tra đặc quyền
* Kiểm tra thay đổi tài khoản

|  |
| --- |
| As a security professional, you might be involved with any of these processes. |

Là một chuyên gia bảo mật, bạn có thể tham gia vào bất kỳ quy trình nào trong số này.

|  |
| --- |
| **Usage audits** |

**Kiểm tra việc sử dụng**

|  |
| --- |
| When conducting a usage audit, the security team will review which resources each account is accessing and what the user is doing with the resource. Usage audits can help determine whether users are acting in accordance with an organization’s security policies. They can also help identify whether a user has permissions that can be revoked because they are no longer being used. |

Khi tiến hành kiểm tra việc sử dụng, nhóm bảo mật sẽ xem xét tài nguyên nào mỗi tài khoản đang truy cập và người dùng đang làm gì với tài nguyên đó. Kiểm tra việc sử dụng có thể giúp xác định xem người dùng có hành động phù hợp với chính sách bảo mật của tổ chức hay không. Họ cũng có thể giúp xác định xem người dùng có các quyền có thể bị thu hồi vì họ không còn sử dụng nữa hay không.

|  |
| --- |
| **Privilege audits** |

**Kiểm tra đặc quyền**

|  |
| --- |
| Users tend to accumulate more access privileges than they need over time, an issue known as *privilege creep*. This might occur if an employee receives a promotion or switches teams and their job duties change. Privilege audits assess whether a user's role is in alignment with the resources they have access to. |

Người dùng có xu hướng tích lũy nhiều đặc quyền truy cập hơn mức họ cần theo thời gian, vấn đề này được gọi là *leo thang đặc quyền* . Điều này có thể xảy ra nếu một nhân viên được thăng chức hoặc chuyển nhóm và nhiệm vụ công việc của họ thay đổi. Kiểm tra đặc quyền đánh giá xem vai trò của người dùng có phù hợp với tài nguyên mà họ có quyền truy cập hay không.

|  |
| --- |
| **Account change audits** |

**Kiểm tra thay đổi tài khoản**

|  |
| --- |
| Account directory services keep records and logs associated with each user. Changes to an account are usually saved and can be used to audit the directory for suspicious activity, like multiple attempts to change an account password. Performing account change audits helps to ensure that all account changes are made by authorized users. |

Dịch vụ thư mục tài khoản lưu giữ hồ sơ và nhật ký liên quan đến mỗi người dùng. Các thay đổi đối với tài khoản thường được lưu và có thể được sử dụng để kiểm tra thư mục nhằm phát hiện hoạt động đáng ngờ, chẳng hạn như nhiều lần cố gắng thay đổi mật khẩu tài khoản. Thực hiện kiểm tra thay đổi tài khoản giúp đảm bảo rằng tất cả các thay đổi tài khoản đều được thực hiện bởi người dùng được ủy quyền.

|  |
| --- |
| **Note:** Most directory services can be configured to alert system administrators of suspicious activity. |

**Lưu ý:** Hầu hết các dịch vụ thư mục đều có thể được cấu hình để cảnh báo cho quản trị viên hệ thống về hoạt động đáng ngờ.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| The principle of least privilege is a security control that can reduce the risk of unauthorized access to sensitive information and resources. Setting up and configuring user accounts with the right levels of access and authorization is an important step toward implementing least privilege. Auditing user accounts and revoking unnecessary access rights is an important practice that helps to maintain the confidentiality, integrity, and availability of information. |

Nguyên tắc đặc quyền tối thiểu là biện pháp kiểm soát bảo mật có thể giảm nguy cơ truy cập trái phép vào thông tin và tài nguyên nhạy cảm. Thiết lập và định cấu hình tài khoản người dùng với cấp độ truy cập và ủy quyền phù hợp là một bước quan trọng để triển khai đặc quyền tối thiểu. Kiểm tra tài khoản người dùng và thu hồi các quyền truy cập không cần thiết là một biện pháp quan trọng giúp duy trì tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin.

***1.4. The data lifecycle - Vòng đời dữ liệu***

|  |
| --- |
| **The data lifecycle** |

**Vòng đời dữ liệu**

|  |
| --- |
| Organizations of all sizes handle a large amount of data that must be kept private. You learned that data can be vulnerable whether it is at rest, in use, or in transit. Regardless of the state it is in, information should be kept private by limiting access and authorization. |

Các tổ chức thuộc mọi quy mô xử lý một lượng lớn dữ liệu phải được giữ kín. Bạn đã biết rằng dữ liệu có thể dễ bị tổn thương dù đang ở trạng thái nghỉ, đang sử dụng hay đang di chuyển. Bất kể trạng thái đó là gì, thông tin phải được giữ kín bằng cách hạn chế quyền truy cập và ủy quyền.

|  |
| --- |
| In security, data vulnerabilities are often mapped in a model known as the data lifecycle. Each stage of the data lifecycle plays an important role in the security controls that are put in place to maintain the CIA triad of information. In this reading, you will learn about the data lifecycle, the plans that determine how data is protected, and the specific types of data that require extra attention. |

Trong bảo mật, các lỗ hổng dữ liệu thường được ánh xạ trong một mô hình được gọi là vòng đời dữ liệu. Mỗi giai đoạn của vòng đời dữ liệu đóng một vai trò quan trọng trong các biện pháp kiểm soát bảo mật được áp dụng để duy trì bộ ba thông tin của CIA. Trong bài đọc này, bạn sẽ tìm hiểu về vòng đời dữ liệu, các kế hoạch xác định cách bảo vệ dữ liệu và các loại dữ liệu cụ thể cần được chú ý thêm.

|  |
| --- |
| **The data lifecycle** |

**Vòng đời dữ liệu**

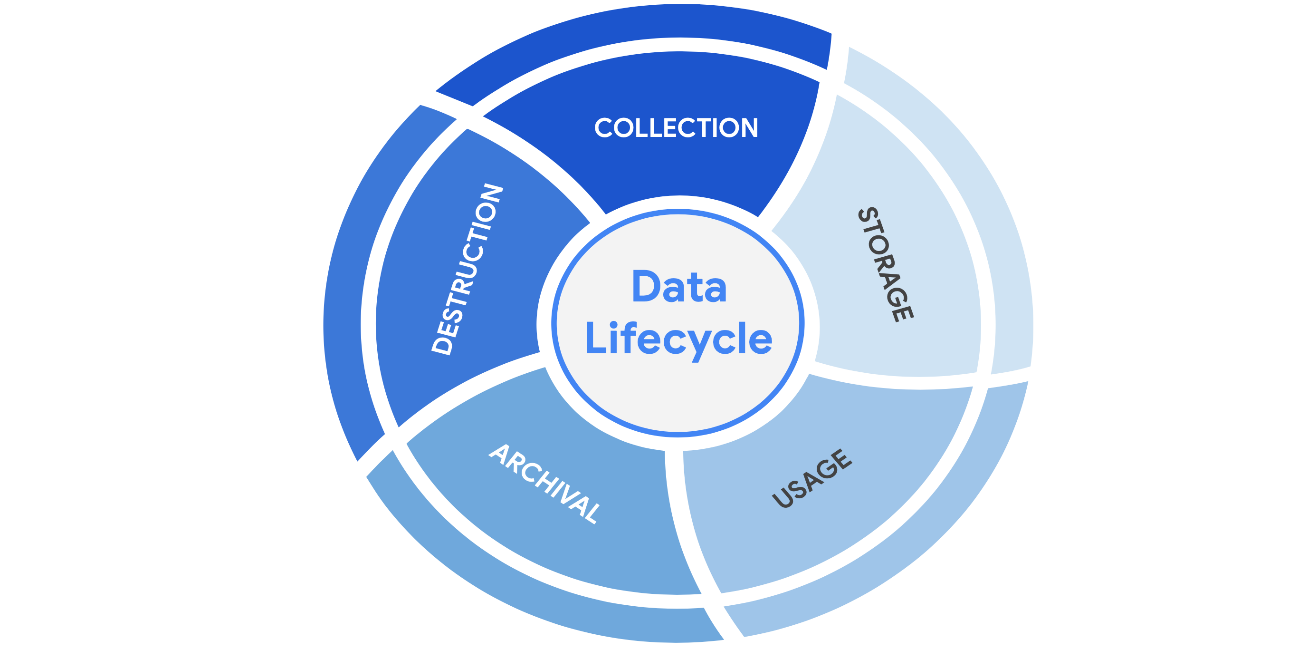
|  |
| --- |
| The data lifecycle is an important model that security teams consider when protecting information. It influences how they set policies that align with business objectives. It also plays an important role in the technologies security teams use to make information accessible. |

Vòng đời dữ liệu là một mô hình quan trọng mà các nhóm bảo mật cân nhắc khi bảo vệ thông tin. Nó ảnh hưởng đến cách họ thiết lập các chính sách phù hợp với mục tiêu kinh doanh. Nó cũng đóng một vai trò quan trọng trong các công nghệ mà nhóm bảo mật sử dụng để giúp thông tin có thể truy cập được.

|  |
| --- |
| In general, the data lifecycle has five stages. Each describe how data flows through an organization from the moment it is created until it is no longer useful:   * Collect * Store * Use * Archive * Destroy |

Nói chung, vòng đời dữ liệu có năm giai đoạn. Mỗi mô tả cách dữ liệu chảy qua một tổ chức từ thời điểm nó được tạo cho đến khi nó không còn hữu ích nữa:

* Sưu tầm
* Cửa hàng
* Sử dụng
* Lưu trữ
* Hủy hoại



|  |
| --- |
| Protecting information at each stage of this process describes the need to keep it accessible and recoverable should something go wrong. |

Việc bảo vệ thông tin ở từng giai đoạn của quy trình này mô tả nhu cầu giữ cho thông tin có thể truy cập và phục hồi được nếu có sự cố xảy ra.

|  |
| --- |
| **Data governance** |

**Quản trị dữ liệu**

|  |
| --- |
| Businesses handle massive amounts of data every day. New information is constantly being collected from internal and external sources. A structured approach to managing all of this data is the best way to keep it private and secure. |

Các doanh nghiệp xử lý lượng dữ liệu khổng lồ mỗi ngày. Thông tin mới liên tục được thu thập từ các nguồn bên trong và bên ngoài. Cách tiếp cận có cấu trúc để quản lý tất cả dữ liệu này là cách tốt nhất để giữ dữ liệu riêng tư và an toàn.

|  |
| --- |
| *Data governance* is a set of processes that define how an organization manages information. Governance often includes policies that specify how to keep data private, accurate, available, and secure throughout its lifecycle. |

*Quản trị dữ liệu* là một tập hợp các quy trình xác định cách tổ chức quản lý thông tin. Quản trị thường bao gồm các chính sách chỉ định cách giữ dữ liệu ở chế độ riêng tư, chính xác, khả dụng và bảo mật trong suốt vòng đời của dữ liệu.

|  |
| --- |
| Effective data governance is a collaborative activity that relies on people. Data governance policies commonly categorize individuals into a specific role:   * **Data owner:** the person that decides who can access, edit, use, or destroy their information. * **Data custodian**: anyone or anything that's responsible for the safe handling, transport, and storage of information. * **Data steward**: the person or group that maintains and implements data governance policies set by an organization. |

Quản trị dữ liệu hiệu quả là một hoạt động hợp tác dựa vào con người. Chính sách quản trị dữ liệu thường phân loại các cá nhân vào một vai trò cụ thể:

* **Chủ sở hữu dữ liệu:** người quyết định ai có thể truy cập, chỉnh sửa, sử dụng hoặc hủy thông tin của họ.
* **Người giám sát dữ liệu** : bất kỳ ai hoặc bất kỳ thứ gì chịu trách nhiệm xử lý, vận chuyển và lưu trữ thông tin một cách an toàn.
* **Người quản lý dữ liệu** : người hoặc nhóm duy trì và thực hiện các chính sách quản trị dữ liệu do tổ chức đặt ra.

|  |
| --- |
| Businesses store, move, and transform data using a wide range of IT systems. Data governance policies often assign accountability to data owners, custodians, and stewards. |

Các doanh nghiệp lưu trữ, di chuyển và chuyển đổi dữ liệu bằng nhiều hệ thống CNTT. Chính sách quản trị dữ liệu thường giao trách nhiệm giải trình cho chủ sở hữu dữ liệu, người giám sát và người quản lý.

|  |
| --- |
| **Note:** As a data custodian, you will primarily be  responsible for maintaining security and privacy rules for your organization. |

**Lưu ý:** Với tư cách là người giám sát dữ liệu, bạn sẽ chịu trách nhiệm chính trong việc duy trì các quy tắc bảo mật và quyền riêng tư cho tổ chức của mình.

|  |
| --- |
| **Protecting data at every stage** |

**Bảo vệ dữ liệu ở mọi giai đoạn**

|  |
| --- |
| Most security plans include a specific policy that outlines how information will be managed across an organization. This is known as a data governance policy. These documents clearly define procedures that should be followed to participate in keeping data safe. They place limits on who or what can access data. Security professionals are important participants in data governance. As a data custodian, you will be responsible for ensuring that data isn’t damaged, stolen, or misused. |

Hầu hết các kế hoạch bảo mật đều bao gồm một chính sách cụ thể nêu rõ cách quản lý thông tin trong toàn tổ chức. Đây được gọi là chính sách quản trị dữ liệu. Những tài liệu này xác định rõ ràng các thủ tục cần tuân thủ để tham gia giữ an toàn cho dữ liệu. Họ đặt giới hạn về ai hoặc những gì có thể truy cập dữ liệu. Các chuyên gia bảo mật là những người tham gia quan trọng trong quản trị dữ liệu. Với tư cách là người giám sát dữ liệu, bạn sẽ chịu trách nhiệm đảm bảo rằng dữ liệu không bị hư hỏng, bị đánh cắp hoặc sử dụng sai mục đích.

|  |
| --- |
| **Legally protected information** |

**Thông tin được bảo vệ hợp pháp**

|  |
| --- |
| Data is more than just a bunch of 1s and 0s being processed by a computer. Data can represent someone's personal thoughts, actions, and choices. It can represent a purchase, a sensitive medical decision, and everything in between. For this reason, data owners should be the ones deciding whether or not to share their data. As a security professional, protecting a person's data privacy decisions must always be respected. |

Dữ liệu không chỉ là một loạt các số 1 và 0 đang được máy tính xử lý. Dữ liệu có thể thể hiện suy nghĩ, hành động và lựa chọn cá nhân của ai đó. Nó có thể đại diện cho việc mua hàng, một quyết định y tế nhạy cảm và mọi thứ liên quan. Vì lý do này, chủ sở hữu dữ liệu phải là người quyết định có chia sẻ dữ liệu của mình hay không. Là một chuyên gia bảo mật, việc bảo vệ các quyết định về quyền riêng tư dữ liệu của một người phải luôn được tôn trọng.

|  |
| --- |
| Securing data can be challenging. In large part, that's because data owners generate more data than they can manage. As a result, data custodians and stewards sometimes lack direct, explicit instructions on how they should handle specific types of data. Governments and other regulatory agencies have bridged this gap by creating rules that specify the types of information that organizations must protect by default:   * **PII** is any information used to infer an individual's identity. Personally identifiable information, or PII, refers to information that can be used to contact or locate someone. * **PHI** stands for protected health information.  In the U.S., it is regulated by the Health Insurance Portability and Accountability Act (HIPAA), which defines PHI as “information that relates to the past, present, or future physical or mental health or condition of an individual.” In the EU, PHI has a similar definition but it is regulated by the General Data Protection Regulation (GDPR). * **SPII** is a specific type of PII that falls under stricter handling guidelines. The *S* stands for sensitive, meaning this is a type of personally identifiable information that should only be accessed on a need-to-know basis, such as a bank account number or login credentials. |

Bảo mật dữ liệu có thể là một thách thức. Phần lớn, đó là do chủ sở hữu dữ liệu tạo ra nhiều dữ liệu hơn mức họ có thể quản lý. Kết quả là, người giám sát và quản lý dữ liệu đôi khi thiếu hướng dẫn trực tiếp, rõ ràng về cách họ nên xử lý các loại dữ liệu cụ thể. Chính phủ và các cơ quan quản lý khác đã thu hẹp khoảng cách này bằng cách tạo ra các quy tắc chỉ định các loại thông tin mà các tổ chức phải bảo vệ theo mặc định:

* **PII** là bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân. Thông tin nhận dạng cá nhân, hay PII, đề cập đến thông tin có thể được sử dụng để liên hệ hoặc xác định vị trí của ai đó.
* **PHI** là viết tắt của thông tin sức khỏe được bảo vệ. Tại Hoa Kỳ, nó được quản lý bởi Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA), trong đó định nghĩa PHI là “thông tin liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân”. Tại EU, PHI có định nghĩa tương tự nhưng được quy định bởi Quy định chung về bảo vệ dữ liệu (GDPR).
* **SPII** là một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn. Chữ *S* là viết tắt của nhạy cảm, nghĩa là đây là loại thông tin nhận dạng cá nhân chỉ nên được truy cập khi cần biết, chẳng hạn như số tài khoản ngân hàng hoặc thông tin đăng nhập.

|  |
| --- |
| Overall, it's important to protect all types of personal information from unauthorized use and disclosure. |

Nhìn chung, điều quan trọng là phải bảo vệ tất cả các loại thông tin cá nhân khỏi việc sử dụng và tiết lộ trái phép.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Keeping information private has never been so important. Many organizations have data governance policies that outline how they plan to protect sensitive information. As a data custodian, you will play a key role in keeping information accessible and safe throughout its lifecycle. There are various types of information and controls that you’ll encounter in the field. As you continue through this course, you’ll learn more about major security controls that keep data private. |

Giữ thông tin riêng tư chưa bao giờ quan trọng đến thế. Nhiều tổ chức có chính sách quản trị dữ liệu nêu rõ cách họ dự định bảo vệ thông tin nhạy cảm. Với tư cách là người giám sát dữ liệu, bạn sẽ đóng vai trò quan trọng trong việc giữ cho thông tin có thể truy cập và an toàn trong suốt vòng đời của nó. Có nhiều loại thông tin và biện pháp kiểm soát khác nhau mà bạn sẽ gặp ở hiện trường. Khi tiếp tục khóa học này, bạn sẽ tìm hiểu thêm về các biện pháp kiểm soát bảo mật chính giúp giữ dữ liệu ở chế độ riêng tư.

***1.5. Information privacy: Regulations and compliance - Quyền riêng tư thông tin: Quy định và tuân thủ***

|  |
| --- |
| **Information privacy: Regulations and compliance** |

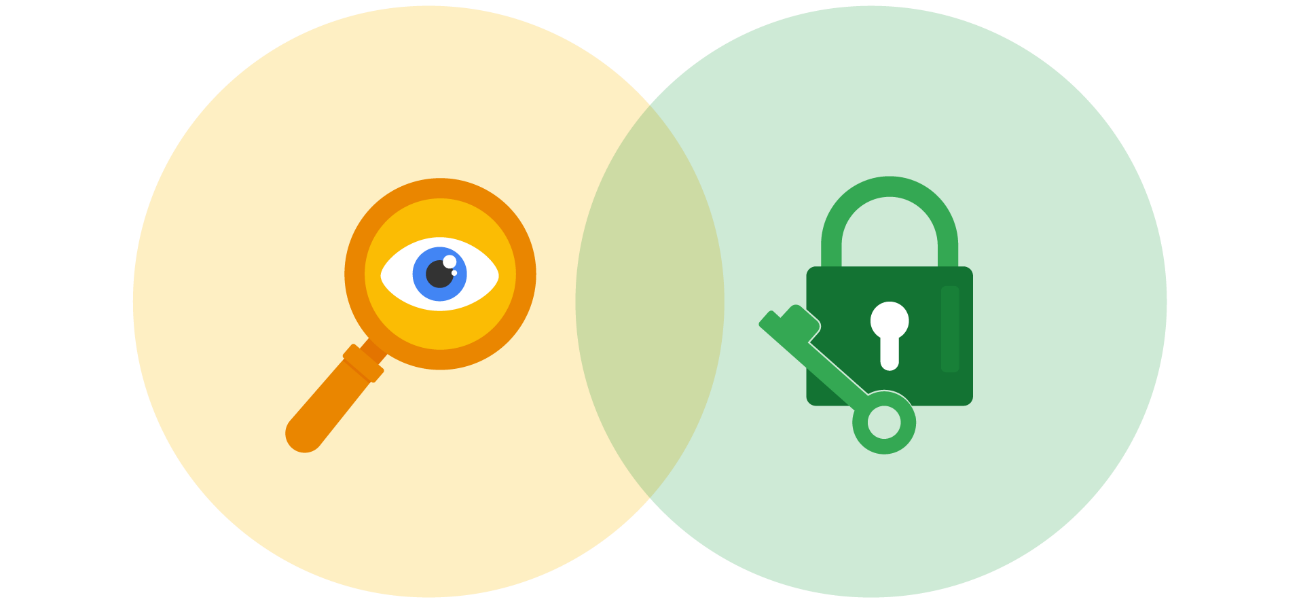
**Quyền riêng tư thông tin: Quy định và tuân thủ**

|  |
| --- |
| Security and privacy have a close relationship. As you may recall, people have the right to control how their personal data is collected and used. Organizations also have a responsibility to protect the information they are collecting from being compromised or misused. As a security professional, you will be highly involved in these efforts. |

Bảo mật và quyền riêng tư có mối quan hệ chặt chẽ. Như bạn có thể nhớ lại, mọi người có quyền kiểm soát cách thu thập và sử dụng dữ liệu cá nhân của họ. Các tổ chức cũng có trách nhiệm bảo vệ thông tin họ đang thu thập khỏi bị xâm phạm hoặc sử dụng sai mục đích. Là một chuyên gia bảo mật, bạn sẽ tham gia nhiều vào những nỗ lực này.

|  |
| --- |
| Previously, you learned how regulations and compliance reduce security risk. To review, refer to [the reading about how security controls, frameworks, and compliance regulations](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) are used together to manage security and minimize risk. In this reading, you will learn how information privacy regulations affect data handling practices. You'll also learn about some of the most influential security regulations in the world. |

Trước đây, bạn đã biết các quy định và sự tuân thủ làm giảm rủi ro bảo mật như thế nào. Để xem xét, hãy tham khảo[đọc về cách kiểm soát bảo mật, khuôn khổ và quy định tuân thủ](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance)được sử dụng cùng nhau để quản lý bảo mật và giảm thiểu rủi ro. Trong bài đọc này, bạn sẽ tìm hiểu các quy định về quyền riêng tư thông tin ảnh hưởng như thế nào đến hoạt động xử lý dữ liệu. Bạn cũng sẽ tìm hiểu về một số quy định bảo mật có ảnh hưởng nhất trên thế giới.



|  |
| --- |
| **Information security vs. information privacy** |

**Bảo mật thông tin so với quyền riêng tư thông tin**

|  |
| --- |
| Security and privacy are two terms that often get used interchangeably outside of this field. Although the two concepts are connected, they represent specific functions:   * **Information privacy** refers to the protection of unauthorized access and distribution of data. * **Information security** (InfoSec) refers to the practice of keeping data in all states away from unauthorized users. |

Bảo mật và quyền riêng tư là hai thuật ngữ thường được sử dụng thay thế cho nhau bên ngoài lĩnh vực này. Mặc dù hai khái niệm này được kết nối với nhau nhưng chúng đại diện cho các chức năng cụ thể:

* **Quyền riêng tư thông tin** đề cập đến việc bảo vệ việc truy cập và phân phối dữ liệu trái phép.
* **Bảo mật thông tin** (InfoSec) đề cập đến biện pháp giữ dữ liệu ở mọi trạng thái tránh xa những người dùng trái phép.

|  |
| --- |
| The key difference: Privacy is about providing people with control over their personal information and how it's shared. Security is about protecting people’s choices and keeping their information safe from potential threats. |

Điểm khác biệt chính: Quyền riêng tư là việc cung cấp cho mọi người quyền kiểm soát thông tin cá nhân của họ và cách chia sẻ thông tin đó. Bảo mật là bảo vệ sự lựa chọn của mọi người và giữ thông tin của họ an toàn trước các mối đe dọa tiềm ẩn.

|  |
| --- |
| For example, a retail company might want to collect specific kinds of personal information about its customers for marketing purposes, like their age, gender, and location. How this private information will be used should be disclosed to customers before it's collected. In addition, customers should be given an option to opt-out if they decide not to share their data. |

Ví dụ: một công ty bán lẻ có thể muốn thu thập các loại thông tin cá nhân cụ thể về khách hàng của mình cho mục đích tiếp thị, như tuổi, giới tính và địa điểm của họ. Thông tin cá nhân này sẽ được sử dụng như thế nào phải được tiết lộ cho khách hàng trước khi thu thập. Ngoài ra, khách hàng nên được cung cấp tùy chọn từ chối nếu họ quyết định không chia sẻ dữ liệu của mình.

|  |
| --- |
| Once the company obtains consent to collect personal information, it might implement specific security controls in place to protect that private data from unauthorized access, use, or disclosure. The company should also have security controls in place to respect the privacy of all stakeholders and anyone who chose to opt-out. |

Sau khi công ty nhận được sự đồng ý thu thập thông tin cá nhân, công ty có thể triển khai các biện pháp kiểm soát bảo mật cụ thể để bảo vệ dữ liệu riêng tư đó khỏi bị truy cập, sử dụng hoặc tiết lộ trái phép. Công ty cũng nên có sẵn các biện pháp kiểm soát bảo mật để tôn trọng quyền riêng tư của tất cả các bên liên quan và bất kỳ ai chọn không tham gia.

|  |
| --- |
| **Note:** Privacy and security are both essential for maintaining customer trust and brand reputation. |

**Lưu ý:** Quyền riêng tư và bảo mật đều cần thiết để duy trì niềm tin của khách hàng và danh tiếng thương hiệu.

|  |
| --- |
| **Why privacy matters in security** |

**Tại sao quyền riêng tư lại quan trọng trong bảo mật**

|  |
| --- |
| Data privacy and protection are topics that started gaining a lot of attention in the late 1990s. At that time, tech companies suddenly went from processing people’s data to storing and using it for business purposes. For example, if a user searched for a product online, companies began storing and sharing access to information about that user’s search history with other companies. Businesses were then able to deliver personalized shopping experiences to the user for free. |

Quyền riêng tư và bảo vệ dữ liệu là những chủ đề bắt đầu thu hút nhiều sự chú ý vào cuối những năm 1990. Vào thời điểm đó, các công ty công nghệ đột nhiên chuyển từ xử lý dữ liệu của con người sang lưu trữ và sử dụng nó cho mục đích kinh doanh. Ví dụ: nếu người dùng tìm kiếm sản phẩm trực tuyến, các công ty sẽ bắt đầu lưu trữ và chia sẻ quyền truy cập thông tin về lịch sử tìm kiếm của người dùng đó với các công ty khác. Sau đó, các doanh nghiệp có thể cung cấp miễn phí trải nghiệm mua sắm được cá nhân hóa cho người dùng.

|  |
| --- |
| Eventually this practice led to a global conversation about whether these organizations had the right to collect and share someone’s private data. Additionally, the issue of data security became a greater concern; the more organizations collected data, the more vulnerable it was to being abused, misused, or stolen. |

Cuối cùng, hoạt động này đã dẫn đến một cuộc tranh luận toàn cầu về việc liệu các tổ chức này có quyền thu thập và chia sẻ dữ liệu riêng tư của ai đó hay không. Ngoài ra, vấn đề bảo mật dữ liệu trở thành mối quan tâm lớn hơn; càng nhiều tổ chức thu thập dữ liệu thì càng dễ bị lạm dụng, lạm dụng hoặc đánh cắp.

|  |
| --- |
| Many organizations became more concerned about the issues of data privacy. Businesses became more transparent about how they were collecting, storing, and using information. They also began implementing more security measures to protect people's data privacy. However, without clear rules in place, protections were inconsistently applied. |

Nhiều tổ chức trở nên quan tâm hơn đến các vấn đề về quyền riêng tư dữ liệu. Các doanh nghiệp trở nên minh bạch hơn về cách họ thu thập, lưu trữ và sử dụng thông tin. Họ cũng bắt đầu thực hiện nhiều biện pháp bảo mật hơn để bảo vệ quyền riêng tư dữ liệu của mọi người. Tuy nhiên, do không có quy định rõ ràng nên các biện pháp bảo vệ được áp dụng không nhất quán.

|  |
| --- |
| **Note:** The more data is collected, stored, and used, the more vulnerable it is to breaches and threats. |

**Lưu ý:** Càng thu thập, lưu trữ và sử dụng nhiều dữ liệu thì càng dễ bị vi phạm và đe dọa.

|  |
| --- |
| **Notable privacy regulations** |

**Các quy định về quyền riêng tư đáng chú ý**

|  |
| --- |
| Businesses are required to abide by certain laws to operate. As you might recall, **regulations** are rules set by a government or another authority to control the way something is done. Privacy regulations in particular exist to protect a user from having their information collected, used, or shared without their consent. Regulations may also describe the security measures that need to be in place to keep private information away from threats. |

Các doanh nghiệp phải tuân thủ một số luật nhất định để hoạt động. Như bạn có thể nhớ lại, **quy định** là những quy tắc do chính phủ hoặc cơ quan có thẩm quyền khác đặt ra để kiểm soát cách thức thực hiện một việc gì đó. Các quy định về quyền riêng tư đặc biệt tồn tại để bảo vệ người dùng khỏi bị thu thập, sử dụng hoặc chia sẻ thông tin mà không có sự đồng ý của họ. Các quy định cũng có thể mô tả các biện pháp bảo mật cần được áp dụng để giữ thông tin cá nhân tránh khỏi các mối đe dọa.

|  |
| --- |
| Three of the most influential industry regulations that every security professional should know about are:   * General Data Protection Regulation (GDPR) * Payment Card Industry Data Security Standard (PCI DSS) * Health Insurance Portability and Accountability Act (HIPAA) |

Ba trong số các quy định có ảnh hưởng nhất của ngành mà mọi chuyên gia bảo mật nên biết là:

* Quy định chung về bảo vệ dữ liệu (GDPR)
* Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)
* Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế (HIPAA)

|  |
| --- |
| **GDPR** |

**GDPR**

|  |
| --- |
| GDPR is a set of rules and regulations developed by the European Union (EU) that puts data owners in total control of their personal information. Under GDPR, types of personal information include a person's name, address, phone number, financial information, and medical information. |

GDPR là một bộ quy tắc và quy định do Liên minh Châu Âu (EU) phát triển nhằm đặt chủ sở hữu dữ liệu có toàn quyền kiểm soát thông tin cá nhân của họ. Theo GDPR, các loại thông tin cá nhân bao gồm tên, địa chỉ, số điện thoại, thông tin tài chính và thông tin y tế của một người.

|  |
| --- |
| The GDPR applies to any business that handles the data of EU citizens or residents, regardless of where that business operates. For example, a US based company that handles the data of EU visitors to their website is subject to the GDPRs provisions. |

GDPR áp dụng cho mọi doanh nghiệp xử lý dữ liệu của công dân hoặc cư dân EU, bất kể doanh nghiệp đó hoạt động ở đâu. Ví dụ: một công ty có trụ sở tại Hoa Kỳ xử lý dữ liệu của khách truy cập EU vào trang web của họ phải tuân theo các quy định của GDPR.

|  |
| --- |
| **PCI DSS** |

**PCI DSS**

|  |
| --- |
| PCI DSS is a set of security standards formed by major organizations in the financial industry. This regulation aims to secure credit and debit card transactions against data theft and fraud. |

PCI DSS là bộ tiêu chuẩn bảo mật được hình thành bởi các tổ chức lớn trong ngành tài chính. Quy định này nhằm mục đích đảm bảo các giao dịch thẻ tín dụng và thẻ ghi nợ chống lại hành vi trộm cắp và gian lận dữ liệu.

|  |
| --- |
| **HIPAA** |

**HIPAA**

|  |
| --- |
| HIPAA is a U.S. law that requires the protection of sensitive patient health information. HIPAA prohibits the disclosure of a person's medical information without their knowledge and consent. |

HIPAA là luật của Hoa Kỳ yêu cầu bảo vệ thông tin sức khỏe nhạy cảm của bệnh nhân. HIPAA nghiêm cấm tiết lộ thông tin y tế của một người mà họ không biết và không đồng ý.

|  |
| --- |
| **Note:** These regulations influence data handling at many organizations around the world even though they were developed by specific nations. |

**Lưu ý:** Các quy định này ảnh hưởng đến việc xử lý dữ liệu tại nhiều tổ chức trên thế giới mặc dù chúng được phát triển bởi các quốc gia cụ thể.

|  |
| --- |
| Several other security and privacy compliance laws exist. Which ones your organization needs to follow will depend on the industry and the area of authority. Regardless of the circumstances, regulatory compliance is important to every business. |

Hiện có một số luật tuân thủ về bảo mật và quyền riêng tư khác. Những tổ chức của bạn cần tuân theo những gì sẽ phụ thuộc vào ngành và lĩnh vực thẩm quyền. Bất kể hoàn cảnh nào, việc tuân thủ quy định đều quan trọng đối với mọi doanh nghiệp.

|  |
| --- |
| **Security assessments and audits** |

**Đánh giá và kiểm tra an ninh**

|  |
| --- |
| Businesses should comply with important regulations in their industry. Doing so validates that they have met a minimum level of security while also demonstrating their dedication to maintaining data privacy. |

Các doanh nghiệp nên tuân thủ các quy định quan trọng trong ngành của mình. Làm như vậy xác nhận rằng họ đã đáp ứng mức độ bảo mật tối thiểu đồng thời thể hiện sự cống hiến của họ trong việc duy trì quyền riêng tư dữ liệu.

|  |
| --- |
| Meeting compliance standards is usually a continual, two-part process of security audits and assessments:   * A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations. * A **security assessment** is a check to determine how resilient current security implementations are against threats. |

Việc đáp ứng các tiêu chuẩn tuân thủ thường là một quá trình kiểm tra và đánh giá bảo mật gồm hai phần liên tục:

* Kiểm **toán bảo mật** là việc xem xét các biện pháp kiểm soát, chính sách và quy trình bảo mật của tổ chức so với một loạt các kỳ vọng.
* Đánh **giá bảo mật** là bước kiểm tra để xác định mức độ linh hoạt của việc triển khai bảo mật hiện tại trước các mối đe dọa.

|  |
| --- |
| For example, if a regulation states that multi-factor authentication (MFA) must be enabled for all administrator accounts, an audit might be conducted to check those user accounts for compliance. After the audit, the internal team might perform a security assessment that determines many users are using weak passwords. Based on their assessment, the team could decide to enable MFA on all user accounts to improve their overall security posture. |

Ví dụ: nếu quy định nêu rõ rằng xác thực đa yếu tố (MFA) phải được bật cho tất cả tài khoản quản trị viên thì có thể tiến hành kiểm tra để kiểm tra xem các tài khoản người dùng đó có tuân thủ hay không. Sau khi kiểm tra, nhóm nội bộ có thể thực hiện đánh giá bảo mật để xác định nhiều người dùng đang sử dụng mật khẩu yếu. Dựa trên đánh giá của họ, nhóm có thể quyết định bật MFA trên tất cả tài khoản người dùng để cải thiện tình trạng bảo mật tổng thể của họ.

|  |
| --- |
| **Note:** Compliance with legal regulations, such as GDPR, can be determined during audits. |

**Lưu ý:** Việc tuân thủ các quy định pháp lý, chẳng hạn như GDPR, có thể được xác định trong quá trình kiểm tra.

|  |
| --- |
| As a security analyst, you are likely to be involved with security audits and assessments in the field. Businesses usually perform security audits less frequently, approximately once per year. Security audits may be performed both internally and externally by different third-party groups. |

Là một nhà phân tích bảo mật, bạn có thể sẽ tham gia vào các cuộc kiểm tra và đánh giá bảo mật trong lĩnh vực này. Các doanh nghiệp thường thực hiện kiểm tra bảo mật ít thường xuyên hơn, khoảng một lần mỗi năm. Kiểm tra bảo mật có thể được thực hiện cả bên trong và bên ngoài bởi các nhóm bên thứ ba khác nhau.

|  |
| --- |
| In contrast, security assessments are usually performed more frequently, about every three-to-six months. Security assessments are typically performed by internal employees, often as preparation for a security audit. Both evaluations are incredibly important ways to ensure that your systems are effectively protecting everyone's privacy. |

Ngược lại, đánh giá bảo mật thường được thực hiện thường xuyên hơn, khoảng ba đến sáu tháng một lần. Đánh giá bảo mật thường được thực hiện bởi nhân viên nội bộ, thường là để chuẩn bị cho kiểm tra bảo mật. Cả hai đánh giá đều là những cách cực kỳ quan trọng để đảm bảo rằng hệ thống của bạn đang bảo vệ quyền riêng tư của mọi người một cách hiệu quả.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| A growing number of businesses are making it a priority to protect and govern the use of sensitive data to maintain customer trust. Security professionals should think about data and the need for privacy in these terms. Organizations commonly use security assessments and audits to evaluate gaps in their security plans. While it is possible to overlook or delay addressing the results of an assessment, doing so can have serious business consequences, such as fines or data breaches. |

Ngày càng có nhiều doanh nghiệp ưu tiên bảo vệ và quản lý việc sử dụng dữ liệu nhạy cảm để duy trì niềm tin của khách hàng. Các chuyên gia bảo mật nên suy nghĩ về dữ liệu và nhu cầu về quyền riêng tư trong các điều khoản này. Các tổ chức thường sử dụng các đánh giá và kiểm toán bảo mật để đánh giá các lỗ hổng trong kế hoạch bảo mật của họ. Mặc dù có thể bỏ qua hoặc trì hoãn việc giải quyết kết quả đánh giá nhưng làm như vậy có thể gây ra những hậu quả nghiêm trọng về mặt kinh doanh, chẳng hạn như bị phạt tiền hoặc vi phạm dữ liệu.

***1.6. Heather: The importance of protecting PII - Heather: Tầm quan trọng của việc bảo vệ PII***

|  |
| --- |
| Hello, my name is Heather and I'm the Vice President of Security Engineering at Google. PII is everywhere. It's a fundamental part of how we are all working online all the time. If you are using online resources, you are probably putting your PII out there somewhere. There's some of your PII that lots of people know, such as your name. And then there's sensitive data that you don't want very many people to know, such as your bank account number or your private medical health information. And so we make these distinctions often because this kind of information needs to be handled differently. Everything that we do now, from school to voting, to registering our car happens online. And because of that, it's so important that we have safety built-in by default into all of our systems. Here's some tips. You should always encrypt the data as much as you can when it's being stored at rest. And secondly, when it's transitting over the Internet, we always want to encrypt it using TLS or SSL. Third, within your company, you should think very clearly about who has access to that data. It should be almost no one if it's very sensitive. And in the rare cases where somebody does need to access that data, there should be a record of that access, who accessed it, and a justification as to why. And you should have a program to look at the audit records for that data. The most important thing to remember is if you have a situation where PII has been compromised, remember that's someone's personal information and your response wants to be grounded in that reality. They need to be able to trust the infrastructure, the systems, the websites, the devices. They need to be able to trust the experience they're having. For me, that's the mission: To help keep billions of people safe online every day. |

Xin chào, tên tôi là Heather và tôi làPhó Chủ tịch Kỹ thuật Bảo mật tại Google.PII ở khắp mọi nơi.Đó là một phần cơ bản về cáchtất cả chúng ta đều làm việc trực tuyến mọi lúc.Nếu bạn đang sử dụng tài nguyên trực tuyến,có thể bạn đang đặt PII của mình ở đâu đó.Có một số PII của bạn mà nhiều người biết,chẳng hạn như tên của bạn.Và sau đó có dữ liệu nhạy cảmbạn không muốn nhiều người biết,chẳng hạn như số tài khoản ngân hàng của bạnhoặc thông tin sức khỏe y tế riêng tư của bạn.Và vì vậy chúng tôi thường xuyên thực hiện những sự phân biệt nàybởi vì loại nàythông tin cần được xử lý khác nhau.Mọi việc chúng ta làm bây giờ,từ trường học đến bầu cử,việc đăng ký xe của chúng tôi diễn ra trực tuyến.Và vì lý do đó, điều quan trọng là chúng ta có được sự an toànđược tích hợp sẵn theo mặc định vào tất cảhệ thống của chúng tôi. Dưới đây là một số lời khuyên.Bạn phải luôn mã hóa dữ liệu nhiều nhất có thểcó thể khi nó được lưu trữ ở trạng thái nghỉ.Và thứ hai, khi nó truyền qua Internet,chúng tôi luôn muốn mã hóa nó bằng TLS hoặc SSL.Thứ ba, trong công ty của bạn,bạn nên suy nghĩ thật rõ ràngvề người có quyền truy cập vào dữ liệu đó.Hầu như không có ai nếu nó rất nhạy cảm.Và trong những trường hợp hiếm hoi khiai đó cần truy cập vào dữ liệu đó,cần có hồ sơ về việc truy cập đó,ai đã truy cập nó và giải thích lý do tại sao.Và bạn nên có một chương trình để xem xéttại hồ sơ kiểm toán đối với dữ liệu đó.Điều quan trọng nhất cần nhớ là nếu bạn cótình huống mà PII đã bị xâm phạm,hãy nhớ đó là thông tin cá nhân của ai đó vàcâu trả lời của bạn muốn được căn cứ vào thực tế đó.Họ cần có thể tin tưởng vào cơ sở hạ tầng,hệ thống, trang web, thiết bị.Họ cần có thể tin tưởngtrải nghiệm họ đang có.Đối với tôi đó là sứ mệnh: Giúp đỡgiữ cho hàng tỷ người trực tuyến an toàn mỗi ngày.

***1.7. Activity: Determine appropriate data handling practices - Hoạt động: Xác định các phương pháp xử lý dữ liệu thích hợp***

|  |
| --- |
| **Activity Overview**  In this activity, you will review the results of a data risk assessment. You will determine whether effective data handling processes are being implemented to protect **information privacy**.  Data is among the most valuable assets in the world today. Everything from intellectual property to guest WiFi networks should be protected with a combination of technical, operational, and managerial controls. Implementing the **principle of least privilege** is essential to protect information privacy.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ xem xét kết quả đánh giá rủi ro dữ liệu. Bạn sẽ xác định liệu các quy trình xử lý dữ liệu hiệu quả có được triển khai để bảo vệ **quyền riêng tư của thông tin** hay không .

Dữ liệu là một trong những tài sản có giá trị nhất trên thế giới hiện nay. Mọi thứ từ sở hữu trí tuệ đến mạng WiFi dành cho khách phải được bảo vệ bằng sự kết hợp của các biện pháp kiểm soát kỹ thuật, vận hành và quản lý. Việc thực hiện **nguyên tắc đặc quyền tối thiểu** là điều cần thiết để bảo vệ quyền riêng tư thông tin.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the following scenario. Then complete the step-by-step instructions.  You work for an educational technology company that developed an application to help teachers automatically grade assignments. The application handles a wide range of data that it collects from academic institutions, instructors, parents, and students.  Your team was alerted to a data leak of internal business plans on social media. An investigation by the team discovered that an employee accidentally shared those confidential documents with an external business partner. An audit into the leak is underway to determine how similar incidents can be avoided.  A supervisor provided you with information regarding the leak. It appears that the principle of least privilege was not observed by employees at the company during a sales meeting. You have been asked to analyze the situation and find ways to prevent it from happening again.  First, you'll need to evaluate details about the incident. Then, you'll review the controls in place to prevent data leaks. Next, you'll identify ways to improve information privacy at the company. Finally, you'll justify why you think your recommendations will make data handling at the company more secure. |

**Kịch bản**

Xem lại tình huống sau. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn làm việc cho một công ty công nghệ giáo dục đã phát triển một ứng dụng giúp giáo viên tự động chấm điểm bài tập. Ứng dụng này xử lý nhiều loại dữ liệu được thu thập từ các tổ chức học thuật, người hướng dẫn, phụ huynh và sinh viên.

Nhóm của bạn đã được cảnh báo về vụ rò rỉ dữ liệu về kế hoạch kinh doanh nội bộ trên mạng xã hội. Một cuộc điều tra của nhóm đã phát hiện ra rằng một nhân viên đã vô tình chia sẻ những tài liệu bí mật đó với một đối tác kinh doanh bên ngoài. Một cuộc kiểm tra rò rỉ đang được tiến hành để xác định cách có thể tránh được những sự cố tương tự.

Người giám sát đã cung cấp cho bạn thông tin về vụ rò rỉ. Có vẻ như nguyên tắc về đặc quyền tối thiểu đã không được nhân viên công ty tuân thủ trong một cuộc họp bán hàng. Bạn được yêu cầu phân tích tình huống và tìm cách ngăn chặn nó xảy ra lần nữa.

Đầu tiên, bạn cần đánh giá chi tiết về vụ việc. Sau đó, bạn sẽ xem xét các biện pháp kiểm soát hiện có để ngăn chặn rò rỉ dữ liệu. Tiếp theo, bạn sẽ xác định các cách để cải thiện quyền riêng tư thông tin tại công ty. Cuối cùng, bạn sẽ giải thích lý do tại sao bạn cho rằng đề xuất của mình sẽ giúp việc xử lý dữ liệu tại công ty trở nên an toàn hơn.

|  |
| --- |
| **Step-By-Step Instructions** |

**Hướng dẫn từng bước một**

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the link and select *Use Template*.j  Link to template: [Data leak worksheet](https://docs.google.com/document/d/1677CNrxn-Ap6oFX-OY0r23yoPQq46wPWZQmZus28oDo/template/preview?resourcekey=0-gr_UkcEPsUVSOMNRLyS8aw) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng Mẫu* .j

Liên kết đến mẫu:[Bảng tính rò rỉ dữ liệu](https://docs.google.com/document/d/1677CNrxn-Ap6oFX-OY0r23yoPQq46wPWZQmZus28oDo/template/preview?resourcekey=0-gr_UkcEPsUVSOMNRLyS8aw)

|  |
| --- |
| **Step 2: Analyze the situation**  The principle of least privilege is a fundamental security control that helps maintain information privacy. However, least privilege starts to lose its effectiveness when too many users are given access to information. Data leaks commonly happen as information gets passed between people without oversight.  To start your analysis, review the following incident summary provided by your supervisor:  *A customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to unshare the folder. Later, the representative copied a link to the marketing materials to share with a business partner during a sales call. Instead, the representative shared a link to the entire folder. During the sales call, the business partner received the link to internal documents and posted it to their social media page.*  After reviewing the summary, write **20-60 words (2-3 sentences)** in the **Issue(s)** row of the *Data leak worksheet* describing the factors that led to the data leak. |

**Bước 2: Phân tích tình huống**

Nguyên tắc đặc quyền tối thiểu là biện pháp kiểm soát bảo mật cơ bản giúp duy trì quyền riêng tư của thông tin. Tuy nhiên, đặc quyền tối thiểu bắt đầu mất tác dụng khi có quá nhiều người dùng được cấp quyền truy cập thông tin. Rò rỉ dữ liệu thường xảy ra khi thông tin được truyền giữa mọi người mà không có sự giám sát.

Để bắt đầu phân tích, hãy xem lại bản tóm tắt sự việc sau do người giám sát của bạn cung cấp:

*Đại diện thành công của khách hàng đã nhận được quyền truy cập vào thư mục tài liệu nội bộ từ người quản lý. Nó chứa các tệp liên quan đến việc cung cấp sản phẩm mới, bao gồm các tài liệu tiếp thị và phân tích khách hàng. Người quản lý quên hủy chia sẻ thư mục. Sau đó, người đại diện đã sao chép đường liên kết đến tài liệu tiếp thị để chia sẻ với đối tác kinh doanh trong cuộc gọi bán hàng. Thay vào đó, người đại diện đã chia sẻ một liên kết tới toàn bộ thư mục. Trong cuộc gọi bán hàng, đối tác kinh doanh đã nhận được liên kết đến các tài liệu nội bộ và đăng nó lên trang mạng xã hội của họ.*

Sau khi xem lại bản tóm tắt, hãy viết **20-60 từ (2-3 câu)** vào **hàng (các)** Vấn đề của *bảng tính Rò rỉ dữ liệu* mô tả các yếu tố dẫn đến rò rỉ dữ liệu.

|  |
| --- |
| **Step 3: Review current data privacy controls**  Data leaks are a major risk due to the amount of data handled by the application. The company used the NIST Cybersecurity Framework (CSF) to develop their plan for addressing their information privacy concerns.  Review the **Security plan snapshot** resource of the worksheet. Then, review the **NIST SP 800-53: AC-6** resource of the worksheet.  After, write **20-60 words (2-3 sentences)** in the **Review** row of the *Data leak worksheet* to summarize what you've learned about NIST SP 800-53: AC-6. |

**Bước 3: Xem lại các biện pháp kiểm soát quyền riêng tư dữ liệu hiện tại**

Rò rỉ dữ liệu là một rủi ro lớn do lượng dữ liệu được ứng dụng xử lý. Công ty đã sử dụng Khung bảo mật không gian mạng (CSF) của NIST để phát triển kế hoạch giải quyết các mối lo ngại về quyền riêng tư thông tin của họ.

Xem lại tài nguyên **ảnh chụp nhanh Kế hoạch bảo mật** của trang tính. Sau đó, xem lại tài nguyên **NIST SP 800-53: AC-6** của bảng tính.

Sau đó, viết **20-60 từ (2-3 câu)** vào hàng **Review** của *bảng Data Leak* để tóm tắt những gì bạn đã học về NIST SP 800-53: AC-6.

|  |
| --- |
| **Step 4: Identify control enhancements**  The company's implementation of least privilege is based on NIST Special Publication 800-53 (SP 800-53). NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories, including least privilege.  Use the **NIST SP 800-53: AC-6** resource to determine *two control enhancements* that might have prevented the data leak. List the **two improvements** in the **Recommendation(s)** row of the worksheet. |

**Bước 4: Xác định các cải tiến kiểm soát**

Việc thực hiện đặc quyền tối thiểu của công ty dựa trên Ấn bản Đặc biệt 800-53 (SP 800-53) của NIST. NIST đã phát triển SP 800-53 để cung cấp cho doanh nghiệp gói bảo mật thông tin có thể tùy chỉnh. Đó là một nguồn tài nguyên toàn diện mô tả nhiều loại điều khiển, bao gồm cả đặc quyền tối thiểu.

Sử dụng tài nguyên **NIST SP 800-53: AC-6** để xác định *hai cải tiến kiểm soát* có thể đã ngăn chặn rò rỉ dữ liệu. Liệt kê **hai cải tiến** trong **hàng (các)** Đề xuất của bảng tính.

|  |
| --- |
| **Step 5: Justify your recommendations**  At the end of your analysis, it's time to communicate your findings to your supervisor. It's important to justify your recommendations so that the supervisor can relay this information to other decision makers at the company.  Consider the issues you identified earlier. Then, write **20-60 words (2-3 sentences)** in the **Justification** row describing why you think the control enhancements you recommend will reduce the likelihood of another data leak. |

**Bước 5: Chứng minh đề xuất của bạn**

Khi kết thúc quá trình phân tích, đã đến lúc truyền đạt những phát hiện của bạn cho người giám sát. Điều quan trọng là phải biện minh cho các đề xuất của bạn để người giám sát có thể chuyển thông tin này đến những người ra quyết định khác trong công ty.

Hãy xem xét các vấn đề bạn đã xác định trước đó. Sau đó, viết **20-60 từ (2-3 câu)** vào hàng **Biện minh mô** tả lý do tại sao bạn cho rằng những cải tiến kiểm soát mà bạn đề xuất sẽ làm giảm khả năng xảy ra rò rỉ dữ liệu khác.

|  |
| --- |
| **Pro Tip: Save the template** |

**Mẹo chuyên nghiệp: Lưu mẫu**

|  |
| --- |
| Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers. |

Cuối cùng, hãy nhớ lưu một bản sao trống của mẫu bạn đã sử dụng để hoàn thành hoạt động này. Bạn có thể sử dụng nó để thực hành thêm hoặc trong các dự án chuyên nghiệp của mình. Những mẫu này sẽ giúp bạn giải quyết quá trình suy nghĩ của mình và thể hiện kinh nghiệm của bạn với các nhà tuyển dụng tiềm năng.

|  |
| --- |
| **What to Include in Your Response**  Be sure to address the following elements in your completed activity:   * **2-3** sentences analyzing the factors that led to the incident * **2-3 sentences** summarizing NIST SP 800-53: AC-6 * **2** control enhancement recommendations to improve least privilege * **2-3** sentences justifying your recommendations |

**Những gì cần bao gồm trong phản hồi của bạn**

Hãy đảm bảo giải quyết các yếu tố sau trong hoạt động đã hoàn thành của bạn:

* **2-3** câu phân tích các yếu tố dẫn đến sự việc
* **2-3 câu** tóm tắt NIST SP 800-53: AC-6
* **2** đề xuất nâng cao kiểm soát để cải thiện đặc quyền tối thiểu
* **2-3** câu biện minh cho đề xuất của bạn

***1.8. Activity Exemplar: Determine appropriate data handling practices - Mẫu hoạt động: Xác định các phương pháp xử lý dữ liệu thích hợp***

|  |
| --- |
| **Activity Exemplar: Determine appropriate data handling practices** |

**Mẫu hoạt động: Xác định các phương pháp xử lý dữ liệu thích hợp**

|  |
| --- |
| Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link and select *Use Template*.  Link to exemplar: [Data leak worksheet](https://docs.google.com/document/d/1efJnLe_9HnP0OlMFeUrKOuiHcliaj-Gzi1LNF_qTszQ/template/preview?resourcekey=0-IxXwuyXndQIxP97Gvfi2Yw) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Bảng tính rò rỉ dữ liệu](https://docs.google.com/document/d/1efJnLe_9HnP0OlMFeUrKOuiHcliaj-Gzi1LNF_qTszQ/template/preview?resourcekey=0-IxXwuyXndQIxP97Gvfi2Yw)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course. |

**Đánh giá mẫu mực**

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong suốt khóa học.

|  |
| --- |
| ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your activity reflects your analysis of appropriate data handling practices.* |

***Lưu ý:*** *Ví dụ thể hiện một cách khả thi để hoàn thành hoạt động. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là hoạt động của bạn phản ánh phân tích của bạn về các phương pháp xử lý dữ liệu phù hợp.*

|  |
| --- |
| Next, review the details of the completed data leak worksheet: |

Tiếp theo, xem lại chi tiết của bảng tính rò rỉ dữ liệu đã hoàn thành:

|  |
| --- |
| **Issues**  Many people neglected to keep the confidential information private. The manager should have done a better job keeping track of the internal folder by limiting access to the representative and themselves. The customer also could have done a better job of communicating their plans to share the marketing information before posting it to social media. |

**Vấn đề**

Nhiều người bỏ bê việc giữ bí mật thông tin riêng tư. Người quản lý đáng lẽ phải thực hiện công việc theo dõi thư mục nội bộ tốt hơn bằng cách hạn chế quyền truy cập của người đại diện và chính họ. Khách hàng cũng có thể thực hiện công việc tốt hơn trong việc truyền đạt kế hoạch chia sẻ thông tin tiếp thị của họ trước khi đăng nó lên mạng xã hội.

|  |
| --- |
| **Review**  NIST SP 800-53 is a resource that's designed to help organizations address data privacy risks. The document defines security controls, describes implementation strategies, and suggests individual control enhancements. AC-6 is a section about access controls that relate to the principle of least privilege. |

**Ôn tập**

NIST SP 800-53 là tài nguyên được thiết kế để giúp các tổ chức giải quyết các rủi ro về quyền riêng tư dữ liệu. Tài liệu xác định các biện pháp kiểm soát bảo mật, mô tả các chiến lược triển khai và đề xuất các cải tiến kiểm soát riêng lẻ. AC-6 là phần về kiểm soát truy cập liên quan đến nguyên tắc đặc quyền tối thiểu.

|  |
| --- |
| **Recommendation(s)**  Based on the suggestion of NIST SP 800-53: AC-6, the data leak might have been avoided with the following controls:   * *Automatically revoke access to information after a period of time.* * *Regularly audit user privileges.* |

**Khuyến nghị)**

Dựa trên đề xuất của NIST SP 800-53: AC-6, có thể tránh được rò rỉ dữ liệu bằng các biện pháp kiểm soát sau:

* *Tự động thu hồi quyền truy cập thông tin sau một khoảng thời gian.*
* *Thường xuyên kiểm tra đặc quyền của người dùng.*

|  |
| --- |
| **Justification**  Automating security tasks whenever possible is a good way to reduce the chances of human error. In this case, creating a policy that sets expiration dates for access links might have avoided the leak. Requiring managers to regularly audit who can access their files is another way that information could be kept private. |

**sự biện minh**

Tự động hóa các tác vụ bảo mật bất cứ khi nào có thể là một cách tốt để giảm nguy cơ xảy ra lỗi của con người. Trong trường hợp này, việc tạo chính sách đặt ngày hết hạn cho các liên kết truy cập có thể tránh được rò rỉ. Yêu cầu người quản lý thường xuyên kiểm tra xem ai có thể truy cập vào tệp của họ là một cách khác để thông tin có thể được giữ kín.

***1.9. Test your knowledge: Safeguard information - Kiểm tra kiến ​​thức của bạn: Bảo vệ thông tin***

**2. Encryption methods - Phương pháp mã hóa**

***2.1. Fundamentals of cryptography - Nguyên tắc cơ bản của mật mã***

|  |
| --- |
| The internet is an open, public system with a lot of data flowing through it. Even though we all send and store information online, there's some information that we choose to keep private. In security, this type of data is known as personally identifiable information. Personally identifiable information, or PII, is any information that can be used to infer an individual's identity. This can include things like someone's name, medical and financial information, photos, emails, or fingerprints. |

Internet là một hệ thống công cộng mở với rất nhiều dữ liệu được truyền qua nó.Mặc dù tất cả chúng ta đều gửi và lưu trữ thông tin trực tuyến,có một số thông tin mà chúng tôi chọn giữ kín.Trong bảo mật, loại dữ liệu này được gọi là thông tin nhận dạng cá nhân.Thông tin nhận dạng cá nhân, hoặc PII,là bất kỳ thông tin nào có thể được sử dụng để suy ra danh tính của một cá nhân.Điều này có thể bao gồm những thứ như tên của ai đó, y tế và tài chínhthông tin, hình ảnh, email hoặc dấu vân tay.

|  |
| --- |
| Maintaining the privacy of PII online is difficult. It takes the right security controls to do so. One of the main security controls used to protect information online is cryptography. Cryptography is the process of transforming information into a form that unintended readers can't understand. Data of any kind is kept secret using a two-step process: encryption to hide the information, and decryption to unhide it. |

Việc duy trì sự riêng tư của PII trực tuyến là rất khó.Cần có các biện pháp kiểm soát bảo mật phù hợp để làm như vậy.Một trong những biện pháp kiểm soát bảo mật chính được sử dụng để bảo vệthông tin trực tuyến là mật mã.Mật mã học là quá trình chuyển đổi thông tin thành một dạngđộc giả ngoài ý muốn không thể hiểu được.Bất kỳ loại dữ liệu nào đều được giữ bí mật bằng quy trình gồm hai bước:mã hóa để ẩn thông tin và giải mã để hiện thông tin đó.

|  |
| --- |
| Imagine sending an email to a friend. The process starts by taking data in its original and readable form, known as plaintext. Encryption takes that information and scrambles it into an unreadable form, known as ciphertext. We then use decryption to unscramble the ciphertext back into plaintext form, making it readable again. |

Hãy tưởng tượng gửi một email cho một người bạn.Quá trình bắt đầu bằng cách lấy dữ liệu ở dạng ban đầu vàdạng có thể đọc được, được gọi là bản rõ.Mã hóa lấy thông tin đó vàxáo trộn nó thành một dạng không thể đọc được, được gọi là bản mã.Sau đó, chúng tôi sử dụng phương pháp giải mã để giải mã văn bản mã hóa trở lại dạng văn bản gốc,làm cho nó có thể đọc được trở lại.

|  |
| --- |
| Hiding and unhiding private information is a practice that's been around for a long time. Way before computers! One of the earliest cryptographic methods is known as Caesar's cipher. This method is named after a Roman general, Julius Caesar, who ruled the Roman empire near the end of the first century BC. He used it to keep messages between him and his military generals private. |

Ẩn và hiện thông tin cá nhân là một thói quen đã có từ lâu.Đi trước máy tính!Một trong những phương pháp mã hóa sớm nhất được gọi là mật mã Caesar.Phương pháp này được đặt theo tên của một vị tướng La Mã, Julius Caesar,người cai trị đế chế La Mã vào gần cuối thế kỷ thứ nhất trước Công nguyên.Anh ta sử dụng nó để giữ bí mật các tin nhắn giữa anh ta và các tướng quân đội của mình.

|  |
| --- |
| Caesar's cipher is a pretty simple algorithm that works by shifting letters in the Roman alphabet forward by a fixed number of spaces. An algorithm is a set of rules that solve a problem. Specifically in cryptography, a cipher is an algorithm that encrypts information. |

Mật mã Caesar là một thuật toán khá đơn giản hoạt động bằng cách dịch chuyển các chữ cái theobảng chữ cái La Mã chuyển tiếp theo một số khoảng trắng cố định.Thuật toán là một tập hợp các quy tắc để giải quyết một vấn đề.Cụ thể trong mật mã, mật mã là một thuật toán mã hóa thông tin.

|  |
| --- |
| For example, a message encoded with Caesar's cipher using a shift of 3 would encode an A as a D, a B as an E, a C as an F, and so on. In this example, you could send a friend a message that said, "hello" using a shift of 3, and it would read "khoor." Now, you might be wondering how would you know the shift a message encrypted with Caesar's cipher is using. The answer to that is, you need the key! |

Ví dụ: một tin nhắn được mã hóa bằng mật mã Caesar sử dụng độ dịch chuyển 3 sẽ mã hóaA là D, B là E, C là F, v.v.Trong ví dụ này, bạn có thể gửi cho bạn bè một tin nhắn có nội dung "xin chào"sử dụng dịch chuyển 3 và nó sẽ đọc là "khoor."Bây giờ, bạn có thể đang tự hỏi làm thế nào bạn có thể biết được sự dịch chuyển của một tin nhắn được mã hóa bằngMật mã của Caesar đang sử dụng. Câu trả lời là bạn cần chìa khóa!

|  |
| --- |
| A cryptographic key is a mechanism that decrypts ciphertext. In our example, the key would tell you that my message is encrypted by 3 shifts. With that information, you can unlock the hidden message! |

Khóa mật mã là một cơ chế giải mã văn bản mã hóa.Trong ví dụ của chúng tôi, khóa sẽ cho bạn biết rằng tin nhắn của tôi được mã hóa theo 3 ca.Với thông tin đó, bạn có thể mở khóa tin nhắn ẩn!

|  |
| --- |
| Every form of encryption relies on both a cipher and key to secure the exchange of information. Caesar's cipher is not widely used today because of a couple of major flaws. One concerns the cipher itself. The other relates to the key. This particular cipher relies entirely on the characters of the Roman alphabet to hide information. For example, consider a message written using the English alphabet, which is only 26 characters. Even without the key, it's pretty simple to crack a message secured with Caesar's cipher by shifting letters 26 different ways. |

Mọi hình thức mã hóa đều dựa vào cả mật mã vàchìa khóa để đảm bảo việc trao đổi thông tin.Mật mã của Caesar ngày nay không được sử dụng rộng rãi vì có một số sai sót lớn.Người ta liên quan đến chính mật mã. Cái còn lại liên quan đến chìa khóa.Mật mã đặc biệt này dựa hoàn toàn vào các ký tự của bảng chữ cái La Mã để che giấuthông tin.Ví dụ, hãy xem xét một tin nhắn được viết bằng bảng chữ cái tiếng Anh, bảng chữ cái này chỉ có 26nhân vật.Ngay cả khi không có chìa khóa, việc bẻ khóa một tin nhắn được bảo mật bằngMật mã của Caesar bằng cách dịch chuyển các chữ cái 26 cách khác nhau.

|  |
| --- |
| In information security, this tactic is known as brute force attack, a trial-and-error process of discovering private information. |

Trong bảo mật thông tin, chiến thuật này được gọi là tấn công vũ phu,một quá trình thử và sai để khám phá thông tin cá nhân.

|  |
| --- |
| The other major flaw of Caesar's cipher is that it relies on a single key. If that key was lost or stolen, there's nothing stopping someone from accessing private information. Properly keeping track of cryptographic keys is an important part of security. To start, it's important to ensure that these keys are not stored in public places, and to share them separately from the information they will decrypt. |

Khuyết điểm lớn khác của mật mã Caesar là nó chỉ dựa vào một chìa khóa duy nhất.Nếu chìa khóa đó bị mất hoặc bị đánh cắp,không có gì ngăn cản ai đó truy cập thông tin cá nhân.Theo dõi đúng cách các khóa mật mã là một phần quan trọng của bảo mật.Để bắt đầu, điều quan trọng là đảm bảo rằng các khóa này không được lưu trữ ở những nơi công cộng,và chia sẻ chúng một cách riêng biệt với thông tin mà họ sẽ giải mã.

|  |
| --- |
| Caesar's cipher is just one of many algorithms used to protect people's privacy. Due to its limitations, we rely on more complex algorithms to secure information online. Our next focus is exploring how modern algorithms work to keep information private. |

Mật mã của Caesar chỉ là một trong nhiều thuật toán được sử dụng để bảo vệsự riêng tư.Do những hạn chế của nó,chúng tôi dựa vào các thuật toán phức tạp hơn để bảo mật thông tin trực tuyến.Trọng tâm tiếp theo của chúng tôi là khám phá cách các thuật toán hiện đạilàm việc để giữ thông tin bí mật.

***2.2. Public key infrastructure - Cơ sở hạ tầng nơi công cộng***

|  |
| --- |
| Computers use a lot of encryption algorithms to send and store information online. They're all helpful when it comes to hiding private information, but only as long as their keys are protected. Can you imagine having to keep track of the encryption keys protecting all of your personal information online? Neither can I, and we don't have to, thanks to something known as public key infrastructure. |

Máy tính sử dụng rất nhiềuthuật toán mã hóa để gửivà lưu trữ thông tin trực tuyến.Tất cả đều hữu ích khi trốnthông tin riêng tư nhưng chỉmiễn là chìa khóa của họ được bảo vệ.Bạn có thể tưởng tượng việc phải giữtheo dõi các khóa mã hóa bảo vệtất cả thông tin cá nhân của bạn trực tuyến? Tôi cũng không thể,và chúng ta không cần phải làm vậy, nhờ có điều gì đó đã biếtnhư cơ sở hạ tầng khóa công khai.

|  |
| --- |
| Public key infrastructure, or PKI, is an encryption framework that secures the exchange of information online. It's a broad system that makes accessing information fast, easy, and secure. So, how does it all work? |

Cơ sở hạ tầng khóa công khai, hay PKI,là một khung mã hóađảm bảo việc trao đổi thông tin trực tuyến.Đó là một hệ thống rộng lớn giúp truy cậpthông tin nhanh chóng, dễ dàng và an toàn.Vậy mọi chuyện diễn ra như thế nào?

|  |
| --- |
| PKI is a two-step process. It all starts with the exchange of encrypted information. This involves either asymmetric encryption, symmetric encryption, or both. |

PKI là một quá trình gồm hai bước.Tất cả bắt đầu bằng việc trao đổi thông tin được mã hóa.Điều này liên quan đến mã hóa bất đối xứng,mã hóa đối xứng, hoặc cả hai.

|  |
| --- |
| Asymmetric encryption involves the use of a public and private key pair for encryption and decryption of data. Let's imagine this as a box that can be opened with two keys. One key, the public key, can only be used to access the slot and add items to the box. Since the public key can't be used to remove items, it can be copied and shared with people all around the world to add items. On the other hand, the second key, the private key, opens the box fully, so that the items inside can be removed. Only the owner of the box has access to the private key that unlocks it. |

Mã hóa bất đối xứng liên quan đến việc sử dụngmột cặp khóa công khai và riêng tưđể mã hóa và giải mã dữ liệu.Hãy tưởng tượng đây là một cái hộpcó thể mở được bằng hai chìa khóa.Một khóa, khóa chung,chỉ có thể được sử dụng để truy cậpkhe và thêm vật phẩm vào hộp.Vì khóa chung không thể được sử dụng để xóa các mục,nó có thể được sao chép và chia sẻ với mọi ngườitrên toàn thế giới để thêm các mặt hàng.Mặt khác, khóa thứ hai, khóa riêng,mở hộp hoàn toàn, đểcác mục bên trong có thể được gỡ bỏ.Chỉ có chủ nhân của chiếc hộp mới cótruy cập vào khóa riêng để mở nó.

|  |
| --- |
| Using a public key allows the people and servers you're communicating with to see and send you encrypted information that only you can decrypt with your private key. This two-key system makes asymmetric encryption a secure way to exchange information online; however, it also slows down the process. |

Việc sử dụng khóa công khai cho phépnhững người và máy chủ mà bạn đang giao tiếpđể xem và gửi cho bạnthông tin được mã hóa mà chỉ có bạncó thể giải mã bằng khóa riêng của bạn.Hệ thống hai phím này làm chomã hóa bất đối xứng một cách an toàntrao đổi thông tin trực tuyến;tuy nhiên, nó cũng làm chậm quá trình.

|  |
| --- |
| Symmetric encryption, on the other hand, is a faster and simpler approach to key management. Symmetric encryption involves the use of a single secret key to exchange information. |

Mặt khác, mã hóa đối xứnglà một cách tiếp cận nhanh hơn và đơn giản hơn để quản lý khóa.Mã hóa đối xứng liên quan đến việc sử dụngmột khóa bí mật duy nhất để trao đổi thông tin.

|  |
| --- |
| Let's imagine the locked box again. Instead of two keys, symmetric encryption uses the same key. The owner can use it to open the box, add items, and close it again. When they want to share access, they can give the secret key to anyone else to do the same. Exchanging a single secret key may make web communications faster, but it also makes it less secure. |

Hãy tưởng tượng lại chiếc hộp bị khóa.Thay vì hai phím,mã hóa đối xứng sử dụng cùng một khóa.Chủ sở hữu có thể sử dụng nó để mở hộp, thêm vật phẩm,và đóng nó lại. Khi họ muốn chia sẻ quyền truy cập,họ có thể đưa chìa khóa bí mật chobất kỳ ai khác cũng có thể làm điều tương tự.Trao đổi một khóa bí mật duy nhấtcó thể làm cho giao tiếp trên web nhanh hơn,nhưng nó cũng làm cho nó kém an toàn hơn.

|  |
| --- |
| PKI uses both asymmetric and symmetric encryption, sometimes in conjunction with one another. It all depends on whether speed or security is the priority. For example, mobile chat applications use asymmetric encryption to establish a connection between people at the start of a conversation when security is the priority. Afterwards, when the speed of communications back-and-forth is the priority, symmetric encryption takes over. |

PKI sử dụng cả mã hóa bất đối xứng và đối xứng,đôi khi kết hợp với nhau.Tất cả phụ thuộc vào việc tốc độhoặc bảo mật là ưu tiên hàng đầu.Ví dụ: ứng dụng trò chuyện trên thiết bị di độngsử dụng mã hóa bất đối xứng đểthiết lập sự kết nối giữa mọi người tạisự bắt đầu của một cuộc trò chuyệnkhi an ninh là ưu tiên hàng đầu.Sau đó, khi tốc độ củaưu tiên liên lạc qua lại,mã hóa đối xứng tiếp quản.

|  |
| --- |
| While both have their own strengths and weaknesses, they share a common vulnerability, establishing trust between the sender and receiver. Both processes rely on sharing keys that can be misused, lost, or stolen. This isn't a problem when we exchange information in person because we can use our senses to tell the difference between those we trust and those we don't trust. Computers, on the other hand, aren't naturally equipped to make this distinction. That's where the second step of PKI applies. PKI addresses the vulnerability of key sharing by establishing trust using a system of digital certificates between computers and networks. |

Mặc dù cả hai đều có điểm mạnh và điểm yếu riêng,họ có chung một điểm yếu,tạo sự tin cậy giữa người gửi và người nhận.Cả hai quá trình đều dựa vào việc chia sẻ khóacó thể bị sử dụng sai mục đích, bị mất hoặc bị đánh cắp.Đây không phải là vấn đề khi chúng tôitrao đổi thông tin trực tiếp vìchúng ta có thể sử dụng các giác quan của mình để nhận biết sự khác biệt giữanhững người chúng ta tin tưởng và những người chúng ta không tin tưởng.Mặt khác, máy tính,không được trang bị một cách tự nhiên để tạo ra sự khác biệt này.Đó là nơi áp dụng bước thứ hai của PKI.PKI giải quyết lỗ hổngchia sẻ khóa bằng cách thiết lậptin cậy bằng cách sử dụng một hệ thốngchứng chỉ số giữa máy tính và mạng.

|  |
| --- |
| A digital certificate is a file that verifies the identity of a public key holder. Most online information is exchanged using digital certificates. Users, companies, and networks hold one and exchange them when communicating information online as a way of signaling trust. Let's look at an example of how digital certificates are created. |

Chứng chỉ số là một tập tinxác minh danh tính của người giữ khóa công khai.Hầu hết các thông tin trực tuyến đềuđược trao đổi bằng chứng chỉ số.Người dùng, công ty vàmạng giữ một và trao đổi chúngkhi truyền đạt thông tin trực tuyếnnhư một cách thể hiện sự tin tưởng.Hãy xem một ví dụ về cáchchứng chỉ số được tạo ra.

|  |
| --- |
| Let's say an online business is about to launch their website, and they want to obtain a digital certificate. When they register their domain, the hosting company sends certain information over to a trusted certificate authority, or CA. The information provided is usually basic things like the company name and the country where its headquarters are located. A public key for the site is also provided. The certificate authority then uses this data to verify the company's identity. When it's confirmed, the CA encrypts the data with its own private key. Finally, they create a digital certificate that contains the encrypted company data. It also contains CA's digital signature to prove that it's authentic. |

Giả sử một doanh nghiệp trực tuyến sắp ra mắttrang web của họ và họ muốnnhận được chứng chỉ số.Khi họ đăng ký tên miền của mình,công ty lưu trữ gửi thông tin nhất định quatới cơ quan cấp chứng chỉ đáng tin cậy hoặc CA.Thông tin được cung cấp thường là những điều cơ bản nhưtên công ty và quốc gianơi đặt trụ sở chính của nó.Một khóa công khai cho trang web cũng được cung cấp.Cơ quan cấp chứng chỉ sau đó sử dụngdữ liệu này để xác minh danh tính của công ty.Khi nó được xác nhận, CAmã hóa dữ liệu bằng khóa riêng của nó.Cuối cùng, họ tạo chứng chỉ sốcó chứa dữ liệu công ty được mã hóa.Nó cũng chứa chữ ký số của CAđể chứng minh rằng nó là xác thực.

|  |
| --- |
| Digital certificates are a lot like a digital ID badge that's used online to restrict or grant access to information. This is how PKI solves the trust issue. Combined with asymmetric and symmetric encryption, this two-step approach to exchanging secure information between trusted sources is what makes PKI such a useful security control. |

Chứng chỉ kỹ thuật số rất giống huy hiệu ID kỹ thuật sốđược sử dụng trực tuyến để hạn chế hoặccấp quyền truy cập thông tin.Đây là cách PKI giải quyết vấn đề tin cậy.Kết hợp với sự bất đối xứng vàmã hóa đối xứng,cách tiếp cận hai bước này để trao đổithông tin an toàn giữa các nguồn đáng tin cậy làđiều gì làm cho PKI trở thành một biện pháp kiểm soát bảo mật hữu ích như vậy.

***2.3. Symmetric and asymmetric encryption - Mã hóa đối xứng và bất đối xứng***

|  |
| --- |
| **Symmetric and asymmetric encryption** |

**Mã hóa đối xứng và bất đối xứng**

|  |
| --- |
| Previously, you learned these terms:   * **Encryption**: the process of converting data from a readable format to an encoded format * **Public key infrastructure** (PKI):  an encryption framework that secures the exchange of online information * **Cipher**: an algorithm that encrypts information |

Trước đây, bạn đã học những thuật ngữ này:

* **Mã hóa** : quá trình chuyển đổi dữ liệu từ định dạng có thể đọc được sang định dạng được mã hóa
* **Cơ sở hạ tầng khóa công khai** (PKI): khung mã hóa đảm bảo việc trao đổi thông tin trực tuyến
* **Cipher** : thuật toán mã hóa thông tin

|  |
| --- |
| All digital information deserves to be kept private, safe, and secure. Encryption is one key to doing that! It is useful for transforming information into a form that unintended recipients cannot understand. In this reading, you’ll compare symmetric and asymmetric encryption and learn about some well-known algorithms for each. |

Tất cả thông tin kỹ thuật số xứng đáng được giữ riêng tư, an toàn và bảo mật. Mã hóa là một chìa khóa để làm điều đó! Nó rất hữu ích cho việc chuyển đổi thông tin thành một dạng mà người nhận ngoài ý muốn không thể hiểu được. Trong bài đọc này, bạn sẽ so sánh mã hóa đối xứng và bất đối xứng, đồng thời tìm hiểu về một số thuật toán phổ biến cho từng thuật toán.

|  |
| --- |
| **Types of encryption** |

**Các loại mã hóa**

|  |
| --- |
| There are two main types of encryption:   * **Symmetric encryption** is the use of a single secret key to exchange information. Because it uses one key for encryption and decryption, the sender and receiver must know the secret key to lock or unlock the cipher. * **Asymmetric encryption** is the use of a public and private key pair for encryption and decryption of data. It uses two separate keys: a public key and a private key. The public key is used to encrypt data, and the private key decrypts it. The private key is only given to users with authorized access. |

Có hai loại mã hóa chính:

* **Mã hóa đối xứng** là việc sử dụng một khóa bí mật duy nhất để trao đổi thông tin. Bởi vì nó sử dụng một khóa để mã hóa và giải mã nên người gửi và người nhận phải biết khóa bí mật để khóa hoặc mở khóa mật mã.
* **Mã hóa bất đối xứng** là việc sử dụng cặp khóa chung và khóa riêng để mã hóa và giải mã dữ liệu. Nó sử dụng hai khóa riêng biệt: khóa chung và khóa riêng. Khóa chung được sử dụng để mã hóa dữ liệu và khóa riêng sẽ giải mã nó. Khóa riêng chỉ được cấp cho người dùng có quyền truy cập được ủy quyền.

|  |
| --- |
| **The importance of key length** |

**Tầm quan trọng của độ dài khóa**

|  |
| --- |
| Ciphers are vulnerable to **brute force attacks**, which use a trial and error process to discover private information. This tactic is the digital equivalent of trying every number in a combination lock trying to find the right one. In modern encryption, longer key lengths are considered to be more secure. Longer key lengths mean more possibilities that an attacker needs to try to unlock a cipher. |

Mật mã dễ bị **tấn công vũ phu** , sử dụng quy trình thử và sai để khám phá thông tin cá nhân. Chiến thuật này tương đương với việc thử mọi số trong một tổ hợp khóa để tìm ra số đúng. Trong mã hóa hiện đại, độ dài khóa dài hơn được coi là an toàn hơn. Độ dài khóa dài hơn có nghĩa là kẻ tấn công cần có nhiều khả năng hơn để cố gắng mở khóa mật mã.

|  |
| --- |
| One drawback to having long encryption keys is slower processing times. Although short key lengths are generally less secure, they’re much faster to compute. Providing fast data communication online while keeping information safe is a delicate balancing act. |

Một nhược điểm của việc có khóa mã hóa dài là thời gian xử lý chậm hơn. Mặc dù độ dài khóa ngắn thường kém an toàn hơn nhưng chúng được tính toán nhanh hơn nhiều. Cung cấp liên lạc dữ liệu trực tuyến nhanh chóng trong khi vẫn giữ thông tin an toàn là một hành động cân bằng tinh tế.

|  |
| --- |
| **Approved algorithms** |

**Thuật toán được phê duyệt**

|  |
| --- |
| Many web applications use a combination of symmetric and asymmetric encryption. This is how they balance user experience with safeguarding information. As an analyst, you should be aware of the most widely-used algorithms. |

Nhiều ứng dụng web sử dụng kết hợp mã hóa đối xứng và bất đối xứng. Đây là cách họ cân bằng trải nghiệm người dùng với việc bảo vệ thông tin. Là một nhà phân tích, bạn nên biết về các thuật toán được sử dụng rộng rãi nhất.

|  |
| --- |
| **Symmetric algorithms** |

**Thuật toán đối xứng**

|  |
| --- |
| * *Triple DES (3DES)* is known as a block cipher because of the way it converts plaintext into ciphertext in “blocks.” Its origins trace back to the Data Encryption Standard (DES), which was developed in the early 1970s. DES was one of the earliest symmetric encryption algorithms that generated 64-bit keys. A **bit** is the smallest unit of data measurement on a computer. As you might imagine, Triple DES generates keys that are 192 bits, or three times as long. Despite the longer keys, many organizations are moving away from using Triple DES due to limitations on the amount of data that can be encrypted. However, Triple DES is likely to remain in use for backwards compatibility purposes. * *Advanced Encryption Standard (AES)*is one of the most secure symmetric algorithms today. AES generates keys that are 128, 192, or 256 bits. Cryptographic keys of this size are considered to be safe from brute force attacks. It’s estimated that brute forcing an AES 128-bit key could take a modern computer billions of years! |

* *Triple DES (3DES)* được biết đến như một mật mã khối vì cách nó chuyển đổi văn bản gốc thành văn bản mã hóa trong “khối”. Nguồn gốc của nó bắt nguồn từ Tiêu chuẩn mã hóa dữ liệu (DES), được phát triển vào đầu những năm 1970. DES là một trong những thuật toán mã hóa đối xứng sớm nhất tạo ra khóa 64 bit. Bit **là** đơn vị đo lường dữ liệu nhỏ nhất trên máy tính. Như bạn có thể tưởng tượng, Triple DES tạo ra các khóa có độ dài 192 bit hoặc dài gấp ba lần. Mặc dù có khóa dài hơn nhưng nhiều tổ chức đang ngừng sử dụng Triple DES do hạn chế về lượng dữ liệu có thể được mã hóa. Tuy nhiên, Triple DES có thể vẫn được sử dụng cho mục đích tương thích ngược.
* *Tiêu chuẩn mã hóa nâng cao (AES)* là một trong những thuật toán đối xứng an toàn nhất hiện nay. AES tạo các khóa có độ dài 128, 192 hoặc 256 bit. Khóa mật mã có kích thước này được coi là an toàn trước các cuộc tấn công vũ phu. Người ta ước tính rằng việc ép buộc một khóa AES 128-bit một cách thô bạo có thể khiến một máy tính hiện đại mất hàng tỷ năm!

|  |
| --- |
| **Asymmetric algorithms** |

**Thuật toán bất đối xứng**

|  |
| --- |
| * *Rivest Shamir Adleman (RSA)*is named after its three creators who developed it while at the Massachusetts Institute of Technology (MIT). RSA is one of the first asymmetric encryption algorithms that produces a public and private key pair. Asymmetric algorithms like RSA produce even longer key lengths. In part, this is due to the fact that these functions are creating two keys. RSA key sizes are 1,024, 2,048, or 4,096 bits. RSA is mainly used to protect highly sensitive data. * *Digital Signature Algorithm (DSA)*is a standard asymmetric algorithm that was introduced by NIST in the early 1990s. DSA also generates key lengths of 2,048 bits. This algorithm is widely used today as a complement to RSA in public key infrastructure. |

* *Rivest Shamir Adleman (RSA)* được đặt theo tên của ba người sáng tạo ra nó, những người đã phát triển nó khi còn ở Viện Công nghệ Massachusetts (MIT). RSA là một trong những thuật toán mã hóa bất đối xứng đầu tiên tạo ra cặp khóa chung và khóa riêng. Các thuật toán bất đối xứng như RSA thậm chí còn tạo ra độ dài khóa dài hơn. Điều này một phần là do các hàm này đang tạo hai khóa. Kích thước khóa RSA là 1.024, 2.048 hoặc 4.096 bit. RSA chủ yếu được sử dụng để bảo vệ dữ liệu có độ nhạy cao.
* *Thuật toán chữ ký số (DSA)* là thuật toán bất đối xứng tiêu chuẩn được NIST giới thiệu vào đầu những năm 1990. DSA cũng tạo ra độ dài khóa là 2.048 bit. Thuật toán này ngày nay được sử dụng rộng rãi như một phần bổ sung cho RSA trong cơ sở hạ tầng khóa công khai.

|  |
| --- |
| **Generating keys** |

**Tạo khóa**

|  |
| --- |
| These algorithms must be implemented when an organization chooses one to protect their data. One way this is done is using OpenSSL, which is an open-source command line tool that can be used to generate public and private keys. OpenSSL is commonly used by computers to verify digital certificates that are exchanged as part of public key infrastructure. |

Các thuật toán này phải được triển khai khi một tổ chức chọn một thuật toán để bảo vệ dữ liệu của họ. Một cách để thực hiện điều này là sử dụng OpenSSL, một công cụ dòng lệnh nguồn mở có thể được sử dụng để tạo khóa chung và khóa riêng. OpenSSL thường được máy tính sử dụng để xác minh chứng chỉ kỹ thuật số được trao đổi như một phần của cơ sở hạ tầng khóa công khai.

|  |
| --- |
| **Note:** OpenSSL is just one option. There are various others available that can generate keys with any of these common algorithms. |

**Lưu ý:** OpenSSL chỉ là một lựa chọn. Có nhiều thuật toán khác có sẵn có thể tạo khóa bằng bất kỳ thuật toán phổ biến nào.

|  |
| --- |
| In early 2014, OpenSSL disclosed a vulnerability, known as the [Heartbleed bug](https://en.wikipedia.org/wiki/Heartbleed), that exposed sensitive data in the memory of websites and applications. Although unpatched versions of OpenSSL are still available, the Heartbleed bug was patched later that year (2014). Many businesses today use the secure versions of OpenSSL to generate public and private keys, demonstrating the importance of using up-to-date software. |

Đầu năm 2014, OpenSSL đã tiết lộ một lỗ hổng bảo mật được gọi là[Lỗi chảy máu tim](https://en.wikipedia.org/wiki/Heartbleed), làm lộ dữ liệu nhạy cảm trong bộ nhớ của các trang web và ứng dụng. Mặc dù vẫn còn các phiên bản OpenSSL chưa được vá nhưng lỗi Heartbleed đã được vá vào cuối năm đó (2014). Nhiều doanh nghiệp ngày nay sử dụng các phiên bản bảo mật của OpenSSL để tạo khóa chung và khóa riêng, thể hiện tầm quan trọng của việc sử dụng phần mềm cập nhật.

|  |
| --- |
| **Obscurity is not security** |

**Sự tối nghĩa không phải là bảo mật**

|  |
| --- |
| In the world of cryptography, a cipher must be proven to be unbreakable before claiming that it is secure. According to [Kerchoff’s principle](https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle), cryptography should be designed in such a way that all the details of an algorithm—except for the private key—should be knowable without sacrificing its security. For example, you can access all the details about how AES encryption works online and yet it is still unbreakable. |

Trong thế giới mật mã, mật mã phải được chứng minh là không thể phá vỡ trước khi tuyên bố rằng nó an toàn. Dựa theo[nguyên lý Kerchoff](https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle), mật mã phải được thiết kế theo cách mà tất cả các chi tiết của thuật toán—ngoại trừ khóa riêng—có thể được biết mà không làm mất đi tính bảo mật của nó. Ví dụ: bạn có thể truy cập tất cả thông tin chi tiết về cách mã hóa AES hoạt động trực tuyến nhưng nó vẫn không thể bị phá vỡ.

|  |
| --- |
| Occasionally, organizations implement their own, custom encryption algorithms. There have been instances where those secret cryptographic systems have been quickly cracked after being made public. |

Đôi khi, các tổ chức triển khai thuật toán mã hóa tùy chỉnh của riêng họ. Đã có những trường hợp hệ thống mật mã bí mật đó nhanh chóng bị bẻ khóa sau khi được công khai.

|  |
| --- |
| **Pro tip:** A cryptographic system *should not* be considered secure if it requires secrecy around how it works. |

**Mẹo chuyên nghiệp:** Một hệ thống mật mã *không được* coi là an toàn nếu nó yêu cầu tính bí mật về cách thức hoạt động của nó.

|  |
| --- |
| **Encryption is everywhere** |

**Mã hóa ở khắp mọi nơi**

|  |
| --- |
| Companies use both symmetric and asymmetric encryption. They often work as a team, balancing security with user experience. |

Các công ty sử dụng cả mã hóa đối xứng và bất đối xứng. Họ thường làm việc theo nhóm, cân bằng giữa bảo mật với trải nghiệm người dùng.

|  |
| --- |
| For example, websites tend to use asymmetric encryption to secure small blocks of data that are important. Usernames and passwords are often secured with asymmetric encryption while processing login requests. Once a user gains access, the rest of their web session often switches to using symmetric encryption for its speed. |

Ví dụ: các trang web có xu hướng sử dụng mã hóa bất đối xứng để bảo mật các khối dữ liệu nhỏ quan trọng. Tên người dùng và mật khẩu thường được bảo mật bằng mã hóa bất đối xứng trong khi xử lý yêu cầu đăng nhập. Sau khi người dùng có được quyền truy cập, phần còn lại của phiên web của họ thường chuyển sang sử dụng mã hóa đối xứng để đạt được tốc độ của nó.

|  |
| --- |
| Using data encryption like this is increasingly required by law. Regulations like the Federal Information Processing Standards (FIPS 140-3) and the General Data Protection Regulation (GDPR) outline how data should be collected, used, and handled. Achieving compliance with either regulation is critical to demonstrating to business partners and governments that customer data is handled responsibly. |

Việc sử dụng mã hóa dữ liệu như thế này ngày càng được pháp luật yêu cầu. Các quy định như Tiêu chuẩn xử lý thông tin liên bang (FIPS 140-3) và Quy định bảo vệ dữ liệu chung (GDPR) nêu rõ cách thu thập, sử dụng và xử lý dữ liệu. Việc đạt được sự tuân thủ một trong hai quy định là rất quan trọng để chứng minh cho các đối tác kinh doanh và chính phủ rằng dữ liệu khách hàng được xử lý một cách có trách nhiệm.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Knowing the basics of encryption is important for all security professionals. Symmetric encryption relies on a single secret key to protect data. On the other hand, asymmetric uses a public and private key pair. Their encryption algorithms create different key sizes. Both types of encryption are used to meet compliance regulations and protect data online. |

Biết những điều cơ bản về mã hóa là điều quan trọng đối với tất cả các chuyên gia bảo mật. Mã hóa đối xứng dựa trên một khóa bí mật duy nhất để bảo vệ dữ liệu. Mặt khác, bất đối xứng sử dụng cặp khóa chung và khóa riêng. Thuật toán mã hóa của họ tạo ra các kích thước khóa khác nhau. Cả hai loại mã hóa đều được sử dụng để đáp ứng các quy định tuân thủ và bảo vệ dữ liệu trực tuyến.

***2.4. Resources for completing labs - Tài nguyên để hoàn thành phòng thí nghiệm***

|  |
| --- |
| **Resources for completing labs** |

**Tài nguyên để hoàn thành phòng thí nghiệm**

|  |
| --- |
| This course features hands-on lab activities where you’ll have the opportunity to practice what you’ve learned so far. You’ll use a platform called Qwiklabs to complete these labs. In this reading, you’ll learn how to use Qwiklabs. |

Khóa học này có các hoạt động thực hành trong phòng thí nghiệm, nơi bạn sẽ có cơ hội thực hành những gì bạn đã học cho đến nay. Bạn sẽ sử dụng nền tảng có tên Qwiklabs để hoàn thành các phòng thí nghiệm này. Trong bài đọc này, bạn sẽ học cách sử dụng Qwiklabs.

|  |
| --- |
| **How to use Qwiklabs** |

**Cách sử dụng Qwiklabs**

|  |
| --- |
| **Launching Qwiklabs** |

**Ra mắt Qwiklabs**

|  |
| --- |
| When you select a lab, you start from a Coursera page. You will need to click **Launch App** on that page. After you click **Launch App**, a new tab will open with a Qwiklabs page that contains instructions for that particular lab. |

Khi bạn chọn một phòng thí nghiệm, bạn bắt đầu từ trang Coursera. Bạn sẽ cần nhấp vào **Khởi chạy ứng dụng** trên trang đó. Sau khi bạn nhấp vào **Khởi chạy ứng dụng** , một tab mới sẽ mở ra với trang Qwiklabs chứa hướng dẫn cho phòng thí nghiệm cụ thể đó.

|  |
| --- |
| **Start Lab button** |

**Nút bắt đầu phòng thí nghiệm**

|  |
| --- |
| On the Qwiklabs page, you must click **Start Lab** to open a temporary terminal. The instructions for the lab will move to the right side of the screen. |

Trên trang Qwiklabs, bạn phải nhấp vào **Start Lab** để mở thiết bị đầu cuối tạm thời. Các hướng dẫn cho phòng thí nghiệm sẽ di chuyển sang phía bên phải của màn hình.



|  |
| --- |
| Read the instructions and complete all the tasks in the lab by entering commands in the terminal. |

Đọc hướng dẫn và hoàn thành tất cả các nhiệm vụ trong phòng thí nghiệm bằng cách nhập lệnh trong thiết bị đầu cuối.

|  |
| --- |
| **Note**: It may take a moment for the terminal to start. |

**Lưu ý** : Có thể mất một chút thời gian để thiết bị đầu cuối khởi động.

|  |
| --- |
| **Lab control dialog box** |

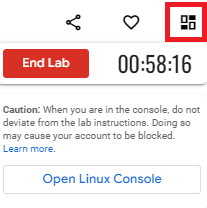
**Hộp thoại điều khiển phòng thí nghiệm**

|  |
| --- |
| After you click **Start Lab**, the lab control dialog box opens. It contains the **End Lab** button, the **timer**, and the **Open Linux Console** button. |

Sau khi bạn nhấn **Start Lab** , hộp thoại điều khiển lab sẽ mở ra. Nó chứa nút **End Lab**  , **bộ hẹn giờ** và nút **Open Linux Console** .

|  |
| --- |
| You can hide or unhide the dialog box by clicking the following icon in the red box: |

Bạn có thể ẩn hoặc hiện hộp thoại bằng cách nhấp vào biểu tượng sau trong hộp màu đỏ:



|  |
| --- |
| **The timer** |

**Đồng hồ bấm giờ**

|  |
| --- |
| The **timer** starts when the terminal has loaded. The timer keeps track of the amount of time you have left to complete a lab. The timer counts down until it reaches 00:00:00. When it does, your temporary terminal and resources are deleted. |

Bộ **đếm thời gian** bắt đầu khi thiết bị đầu cuối đã được tải. Bộ hẹn giờ theo dõi lượng thời gian bạn còn lại để hoàn thành phòng thí nghiệm. Đồng hồ đếm ngược cho đến khi về 00:00:00. Khi đó, thiết bị đầu cuối và tài nguyên tạm thời của bạn sẽ bị xóa.

|  |
| --- |
| You will have ample time to complete the labs. But, stay focused on completing the tasks to ensure you use your time well. |

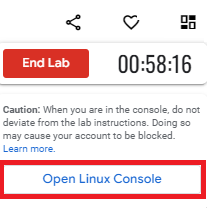
Bạn sẽ có nhiều thời gian để hoàn thành các bài thí nghiệm. Tuy nhiên, hãy tập trung hoàn thành nhiệm vụ để đảm bảo bạn sử dụng tốt thời gian của mình.

|  |
| --- |
| **Open Linux Console button** |

**Nút mở bảng điều khiển Linux**

|  |
| --- |
| When you click the button to **Open Linux Console**, the terminal opens in a new browser window: |

Khi bạn nhấp vào nút **Open Linux Console** , terminal sẽ mở trong cửa sổ trình duyệt mới:



|  |
| --- |
| Use this feature if you want a full-screen view of the terminal. You can close this window at any time. Closing the window does not end your lab, and you can continue working in the terminal in the original tab. |

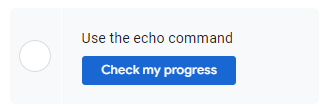
Sử dụng tính năng này nếu bạn muốn xem toàn màn hình của thiết bị đầu cuối. Bạn có thể đóng cửa sổ này bất cứ lúc nào. Việc đóng cửa sổ không kết thúc phòng thí nghiệm của bạn và bạn có thể tiếp tục làm việc trong thiết bị đầu cuối trong tab ban đầu.

|  |
| --- |
| **Check progress** |

**Kiểm tra tiến độ**

|  |
| --- |
| You can check your progress by clicking **Check my progress** at the end of each task. |

Bạn có thể kiểm tra tiến độ của mình bằng cách nhấp vào **Kiểm tra tiến độ của tôi** ở cuối mỗi nhiệm vụ.



|  |
| --- |
| If you haven’t yet completed a task, you’ll receive hints on what you must do to complete it. |

Nếu bạn chưa hoàn thành nhiệm vụ, bạn sẽ nhận được gợi ý về những gì bạn phải làm để hoàn thành nhiệm vụ đó.

|  |
| --- |
| You can click **Check my progress** whenever you want to check the completion status of a task or receive a hint. |

Bạn có thể nhấp vào **Kiểm tra tiến trình của tôi** bất cứ khi nào bạn muốn kiểm tra trạng thái hoàn thành của một nhiệm vụ hoặc nhận gợi ý.

|  |
| --- |
| **Using copy/paste commands** |

**Sử dụng lệnh sao chép/dán**

|  |
| --- |
| The first time you try to use copy or paste keyboard shortcuts (such as **CTRL + C**), you’ll receive a pop-up requesting permission to use your device’s clipboard:  “**googlecoursera.qwiklabs.com wants to see text and images copied to the clipboard.**” |

Lần đầu tiên bạn cố gắng sử dụng sao chép hoặc dán các phím tắt (chẳng hạn như **CTRL + C** ), bạn sẽ nhận được một cửa sổ bật lên yêu cầu quyền sử dụng bảng nhớ tạm của thiết bị: “ **googlecoursera.qwiklabs.com muốn xem văn bản và hình ảnh được sao chép sang bảng nhớ tạm.** ”

|  |
| --- |
| Please click **Allow** if you would like to be able to use these shortcuts in the Qwiklabs platform. If you choose not to allow Qwiklabs access to your clipboard, you cannot use keyboard shortcuts but you can still complete the lab. |

Vui lòng nhấp vào **Cho phép** nếu bạn muốn có thể sử dụng các phím tắt này trong nền tảng Qwiklabs. Nếu bạn chọn không cho phép Qwiklabs truy cập vào khay nhớ tạm của mình, bạn không thể sử dụng phím tắt nhưng vẫn có thể hoàn thành bài thí nghiệm.

|  |
| --- |
| **Code block** |

**Khối mã**

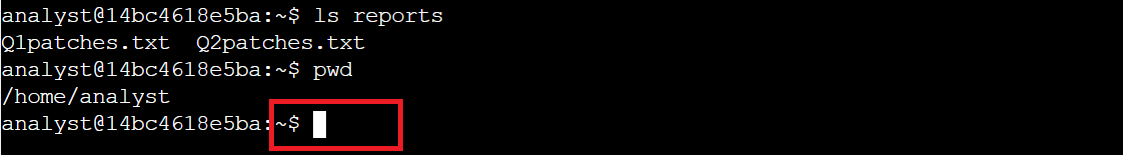
|  |
| --- |
| Certain steps may include a code block. Click the copy button to copy the code provided and then paste it into the terminal. |

Một số bước nhất định có thể bao gồm một khối mã. Nhấp vào nút sao chép để sao chép mã được cung cấp rồi dán vào thiết bị đầu cuối.



|  |
| --- |
| To paste code or other text content that you have copied from the instructions into the terminal, activate the terminal by clicking anywhere inside it. The terminal is active when the cursor in the terminal changes from a static empty outline to a flashing solid block. |

Để dán mã hoặc nội dung văn bản khác mà bạn đã sao chép từ hướng dẫn vào thiết bị đầu cuối, hãy kích hoạt thiết bị đầu cuối bằng cách nhấp vào bất kỳ vị trí nào bên trong thiết bị đầu cuối. Thiết bị đầu cuối hoạt động khi con trỏ trong thiết bị đầu cuối thay đổi từ đường viền trống tĩnh sang khối rắn nhấp nháy.



|  |
| --- |
| Once the terminal is active, use the keyboard shortcut **CTRL + V** (hold down the **CTRL** key and press the **V** key) to insert the copied text into the terminal at the location of the flashing cursor. |

Khi thiết bị đầu cuối hoạt động, hãy sử dụng phím tắt **CTRL + V** (giữ phím **CTRL** và nhấn phím **V** ) để chèn văn bản đã sao chép vào thiết bị đầu cuối tại vị trí con trỏ nhấp nháy.

|  |
| --- |
| **Scrolling** |

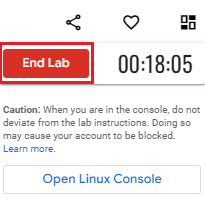
**Cuộn**

|  |
| --- |
| In certain situations, you may want to scroll within the terminal window. To do so, use the scroll wheel on your mouse or the touchpad of your computer. |

Trong một số trường hợp nhất định, bạn có thể muốn cuộn trong cửa sổ terminal. Để làm như vậy, hãy sử dụng con lăn trên chuột hoặc bàn di chuột của máy tính.

|  |
| --- |
| **End Lab button** |

**Nút kết thúc phòng thí nghiệm**



|  |
| --- |
| Finally, click **End Lab** when you’ve completed the tasks in the lab. |

Cuối cùng, nhấp vào **End Lab** khi bạn đã hoàn thành các nhiệm vụ trong lab.

|  |
| --- |
| **Note**: Don't click **End Lab** until you're finished; you'll lose access to the work you've done throughout the lab. |

**Lưu ý** : Đừng nhấp vào **End Lab** cho đến khi bạn hoàn thành; bạn sẽ mất quyền truy cập vào công việc bạn đã thực hiện trong phòng thí nghiệm.

|  |
| --- |
| **Tracking progress on Coursera** |

**Theo dõi tiến trình trên Coursera**

|  |
| --- |
| If you complete a lab but your progress hasn’t been tracked on Coursera, you may need to refresh the page for your progress to be registered. Once you complete the lab and refresh the page, the green check mark should appear. |

Nếu bạn hoàn thành bài thí nghiệm nhưng tiến trình của bạn chưa được theo dõi trên Coursera, bạn có thể cần phải làm mới trang để đăng ký tiến trình của mình. Sau khi bạn hoàn thành bài thực hành và làm mới trang, dấu kiểm màu xanh lục sẽ xuất hiện.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Knowing how to navigate Qwiklabs will be useful as you complete the labs throughout this course. These labs can help you practice what you’ve learned in an interactive environment. |

Biết cách điều hướng Qwiklabs sẽ hữu ích khi bạn hoàn thành các phòng thí nghiệm trong suốt khóa học này. Những phòng thí nghiệm này có thể giúp bạn thực hành những gì bạn đã học trong môi trường tương tác.

***2.5. Lab tips and troubleshooting steps - Mẹo trong phòng thí nghiệm và các bước khắc phục sự cố***

|  |
| --- |
| **Lab tips and troubleshooting steps** |

**Mẹo trong phòng thí nghiệm và các bước khắc phục sự cố**

|  |
| --- |
| Throughout this certificate you will use Qwiklabs and Jupyter Notebooks to complete hands-on activities that  include Linux command line, packet capture, and Python programming tasks. In this reading, we will cover some tips and troubleshooting steps for using Qwiklabs and Jupyter Notebooks on your computer. |

Trong suốt chứng chỉ này, bạn sẽ sử dụng Qwiklabs và Jupyter Notebook để hoàn thành các hoạt động thực hành bao gồm dòng lệnh Linux, chụp gói và các tác vụ lập trình Python. Trong bài đọc này, chúng tôi sẽ đề cập đến một số mẹo và các bước khắc phục sự cố khi sử dụng Qwiklabs và Jupyter Notebook trên máy tính của bạn.

|  |
| --- |
| **Browser compatibility** |

**Tính tương thích của trình duyệt web**

|  |
| --- |
| Make sure your internet browser is updated regularly. Qwiklabs and Jupyter Notebooks require the latest version of Google Chrome, Firefox, Safari, or Microsoft Edge. If your browser is outdated or you are using a browser that is not supported by Qwiklabs or Jupyter Notebooks, you may encounter a problem. If your browser is up to date and you are using one of the browsers listed above and still encountering problems try restarting your browser or clearing your browser’s cache and cookies. You can also use incognito mode which prevents your browser from storing cookies and other temporary data. |

Đảm bảo trình duyệt internet của bạn được cập nhật thường xuyên. Sổ ghi chép Qwiklabs và Jupyter yêu cầu phiên bản mới nhất của Google Chrome, Firefox, Safari hoặc Microsoft Edge. Nếu trình duyệt của bạn đã lỗi thời hoặc bạn đang sử dụng trình duyệt không được Qwiklabs hoặc Jupyter Notebooks hỗ trợ, bạn có thể gặp phải sự cố. Nếu trình duyệt của bạn được cập nhật và bạn đang sử dụng một trong các trình duyệt được liệt kê ở trên mà vẫn gặp sự cố, hãy thử khởi động lại trình duyệt hoặc xóa bộ nhớ đệm và cookie của trình duyệt. Bạn cũng có thể sử dụng chế độ ẩn danh để ngăn trình duyệt lưu trữ cookie và dữ liệu tạm thời khác.

|  |
| --- |
| **Note:** The Qwiklabs user interface works best with Google Chrome. |

**Lưu ý:** Giao diện người dùng Qwiklabs hoạt động tốt nhất với Google Chrome.

|  |
| --- |
| **Internet connection** |

**kết nối Internet**

|  |
| --- |
| Qwiklabs and Jupyter Notebooks require a stable internet connection. If you are experiencing problems starting or completing Qwiklabs or Jupyter Notebooks, your internet connection may be slow or unreliable. Some signs of an unstable internet connection may be freezing labs, difficulty connecting to virtual machines, or the inability to type or enter commands within the lab environment. |

Máy tính xách tay Qwiklabs và Jupyter yêu cầu kết nối Internet ổn định. Nếu bạn gặp sự cố khi bắt đầu hoặc hoàn thành Sổ ghi chép Qwiklabs hoặc Jupyter thì kết nối Internet của bạn có thể chậm hoặc không đáng tin cậy. Một số dấu hiệu của kết nối Internet không ổn định có thể là phòng thí nghiệm bị treo, khó kết nối với máy ảo hoặc không thể nhập hoặc nhập lệnh trong môi trường phòng thí nghiệm.

|  |
| --- |
| **Pro Tip:** If you are unable to complete a Qwiklab or Jupyter Notebooks lab on one device, try using another device. |

**Mẹo của chuyên gia:** Nếu bạn không thể hoàn thành lab Qwiklab hoặc Jupyter Notebooks trên một thiết bị, hãy thử sử dụng một thiết bị khác.

|  |
| --- |
| **Troubleshooting steps** |

**Các bước khắc phục sự cố**

|  |
| --- |
| To summarize, here are the troubleshooting steps to try if you encounter a problem with Qwiklabs or Jupyter Notebooks. |

Tóm lại, đây là các bước khắc phục sự cố để thử nếu bạn gặp sự cố với Qwiklabs hoặc Jupyter Notebook.

|  |
| --- |
| 1. Make sure you are using the latest version of a supported browser: Google Chrome, Firefox, Safari, or Microsoft Edge. 2. Restart your browser and clear your browser’s cache and cookies. You can also use incognito mode. 3. Check your internet connection and make sure it is stable. You can try restarting your router and modem to regain a stable connection. 4. Try restarting Qwiklabs or Jupyter Notebooks again. 5. **For Qwiklabs only:** If problems persist or you receive a message stating that you have exceeded the quota for a Qwiklab, submit this [form](https://qwiklab.zendesk.com/hc/en-us/requests/new) to Qwiklabs support for assistance. |

1. Đảm bảo bạn đang sử dụng phiên bản mới nhất của trình duyệt được hỗ trợ: Google Chrome, Firefox, Safari hoặc Microsoft Edge.
2. Khởi động lại trình duyệt của bạn và xóa bộ nhớ cache và cookie của trình duyệt. Bạn cũng có thể sử dụng chế độ ẩn danh.
3. Kiểm tra kết nối internet của bạn và đảm bảo nó ổn định. Bạn có thể thử khởi động lại bộ định tuyến và modem để lấy lại kết nối ổn định.
4. Hãy thử khởi động lại Qwiklabs hoặc Jupyter Notebook một lần nữa.
5. **Chỉ dành cho Qwiklabs:** Nếu sự cố vẫn tiếp diễn hoặc bạn nhận được thông báo cho biết rằng bạn đã vượt quá hạn ngạch cho Qwiklab, hãy gửi thông báo này[hình thức](https://qwiklab.zendesk.com/hc/en-us/requests/new)tới bộ phận hỗ trợ của Qwiklabs để được hỗ trợ.

***2.6. Activity: Decrypt an encrypted message - Hoạt động: Giải mã tin nhắn được mã hóa***

***2.7. Optional Exemplar: Decrypt an encrypted message - Mẫu tùy chọn: Giải mã tin nhắn được mã hóa***

***2.8. Non-repudiation and hashing - Chống chối bỏ và băm***

|  |
| --- |
| Security professionals are always thinking about vulnerabilities. It's how we stay ahead of threats. |

Các chuyên gia bảo mật luôn suy nghĩvề các lỗ hổng. Đó là cách chúng tôi đón đầu các mối đe dọa.

|  |
| --- |
| We've spent some time together exploring a couple forms of encryption. The two types we've discussed produce keys that are shared when communicating information. Encryption keys are vulnerable to being lost or stolen, which can lead to sensitive information at risk. Let's explore another security control that helps companies address this weakness. |

Chúng tôi đã dành thời gian cùng nhau khám phá một số hình thức mã hóa.Hai loại chúng ta đã thảo luận tạo ra các khóa được chia sẻkhi truyền đạt thông tin.Khóa mã hóa dễ bị mất hoặc bị đánh cắp,có thể dẫn đến thông tin nhạy cảm có nguy cơ.Hãy cùng khám phá một biện pháp kiểm soát bảo mật khác giúp các công ty giải quyết vấn đề nàyyếu đuối.

|  |
| --- |
| A hash function is an algorithm that produces a code that can't be decrypted. Unlike asymmetric and symmetric algorithms, hash functions are one-way processes that do not generate decryption keys. Instead, these algorithms produce a unique identifier known as a hash value, or digest. Here's an example to demonstrate this. |

Hàm băm là một thuật toán tạo ra mã không thể giải mã được.Không giống như các thuật toán bất đối xứng và đối xứng,hàm băm là các quy trình một chiều không tạo ra khóa giải mã.Thay vào đó, các thuật toán này tạo ra một mã định danh duy nhất được gọi là giá trị băm hoặctiêu.Đây là một ví dụ để chứng minh điều này.

|  |
| --- |
| Imagine a company has an internal application that is used by employees and is stored in a shared drive. After passing through a hashing function, the program receives its hash value. For example purposes, we created this relatively short hash value with the MD5 hashing function. Generally, standard hash functions that produce longer hashes are preferred for being more secure. |

Hãy tưởng tượng một công ty có một ứng dụng nội bộ được nhân viên sử dụng vàđược lưu trữ trong một ổ đĩa chung.Sau khi chuyển qua hàm băm, chương trình sẽ nhận được giá trị băm của nó.Ví dụ như mục đích,chúng tôi đã tạo giá trị băm tương đối ngắn này bằng hàm băm MD5.Nói chung, các hàm băm tiêu chuẩn tạo ra các giá trị băm dài hơn được ưu tiên chođược an toàn hơn.

|  |
| --- |
| Next, let's imagine an attacker replaces the program with a modified version that performs malicious actions. The malicious program may work like the original. However, if so much as one line of code is different from the original, it will produce a different hash value. By comparing the hash values, we can validate that the programs are different. Attackers use tricks like this often because they're easily overlooked. Fortunately, hash values help us identify when something like this is happening. |

Tiếp theo, hãy tưởng tượng kẻ tấn công thay thế chương trìnhvới một phiên bản sửa đổi thực hiện các hành động độc hại.Chương trình độc hại có thể hoạt động giống như bản gốc.Tuy nhiên, nếu có quá nhiều dòng mã khác với mã gốc,nó sẽ tạo ra một giá trị băm khác.Bằng cách so sánh các giá trị băm, chúng ta có thể xác nhận rằng các chương trình là khác nhau.Những kẻ tấn công thường sử dụng những thủ thuật như thế này vì chúng dễ bị bỏ qua.May mắn thay, giá trị băm giúp chúng tôi xác định thời điểm xảy ra sự cố như thế này.

|  |
| --- |
| In security, hashes are primarily used as a way to determine the integrity of files and applications. |

Trong bảo mật, hàm băm chủ yếu được sử dụng như một cách đểxác định tính toàn vẹn của các tập tin và ứng dụng.

|  |
| --- |
| Data integrity relates to the accuracy and consistency of information. This is known as non-repudiation, the concept that authenticity of information can't be denied. |

Tính toàn vẹn dữ liệu liên quan đến tính chính xác và nhất quán của thông tin.Điều này được biết đến như là sự không chối bỏ,khái niệm rằng tính xác thực của thông tin không thể bị từ chối.

|  |
| --- |
| Hash functions are important security controls that make proven data integrity possible. Analysts use them frequently. One way to do this is by finding the hash value of files or applications and comparing them against known malicious files. |

Hàm băm là các biện pháp kiểm soát bảo mật quan trọng giúp đảm bảo tính toàn vẹn của dữ liệu đã được chứng minhkhả thi. Các nhà phân tích sử dụng chúng thường xuyên.Một cách để làm điều này là tìm giá trị băm của tệp hoặccác ứng dụng và so sánh chúng với các tệp độc hại đã biết.

|  |
| --- |
| For example, we can use the Linux command line to generate the hash value for any file on your computer. We just launch a shell and type the name of the hashing algorithm we want to use. In this case, we're using a common one known as sha256. Next, we need to enter the file name of any file we want to hash. Let's hash the contents of newfile.txt. Now, we'll press Enter. The terminal generates this unique hash value for the file. |

Ví dụ: chúng ta có thể sử dụng dòng lệnh Linux để tạo giá trị băm chobất kỳ tập tin nào trên máy tính của bạn.Chúng tôi chỉ cần khởi chạy một shell và nhập tên của thuật toán băm mà chúng tôi muốn sử dụng.Trong trường hợp này, chúng tôi đang sử dụng một cái phổ biến được gọi là sha256.Tiếp theo, chúng ta cần nhập tên file của bất kỳ file nào muốn băm.Hãy băm nội dung của newfile.txt.Bây giờ chúng ta sẽ nhấn Enter.Thiết bị đầu cuối tạo ra giá trị băm duy nhất này cho tệp.

|  |
| --- |
| These tools can be compared with the hash values of known online viruses. One such database is VirusTotal. This is a popular tool among security practitioners that's useful for analyzing suspicious files, domains, IPs, and URLs. |

Những công cụ này có thể được so sánh với giá trị băm của các loại virus trực tuyến đã biết.Một cơ sở dữ liệu như vậy là VirusTotal.Đây là một công cụ phổ biến trong số những người thực hành bảo mật, hữu ích cho việc phân tíchcác tệp, tên miền, IP và URL đáng ngờ.

|  |
| --- |
| As we've explored, even the slightest change in input results in a totally different hash value. Hash functions are intentionally designed this way to assist with matters of non-repudiation. They equip computers with a quick and easy way to compare input and output values and validate data integrity. Pretty cool, right? |

Như chúng ta đã khám phá, ngay cả sự thay đổi nhỏ nhất trong đầu vào cũng dẫn đến một kết quả hoàn toàngiá trị băm khác nhau.Các hàm băm được thiết kế có chủ đích theo cách này để hỗ trợ các vấn đề về chống chối bỏ.Họ trang bị cho máy tính một cách nhanh chóng và dễ dàng để so sánh đầu vào và đầu ragiá trị và xác nhận tính toàn vẹn của dữ liệu.Khá tuyệt phải không?

***2.9. The evolution of hash functions - Sự phát triển của hàm băm***

|  |
| --- |
| **The evolution of hash functions** |

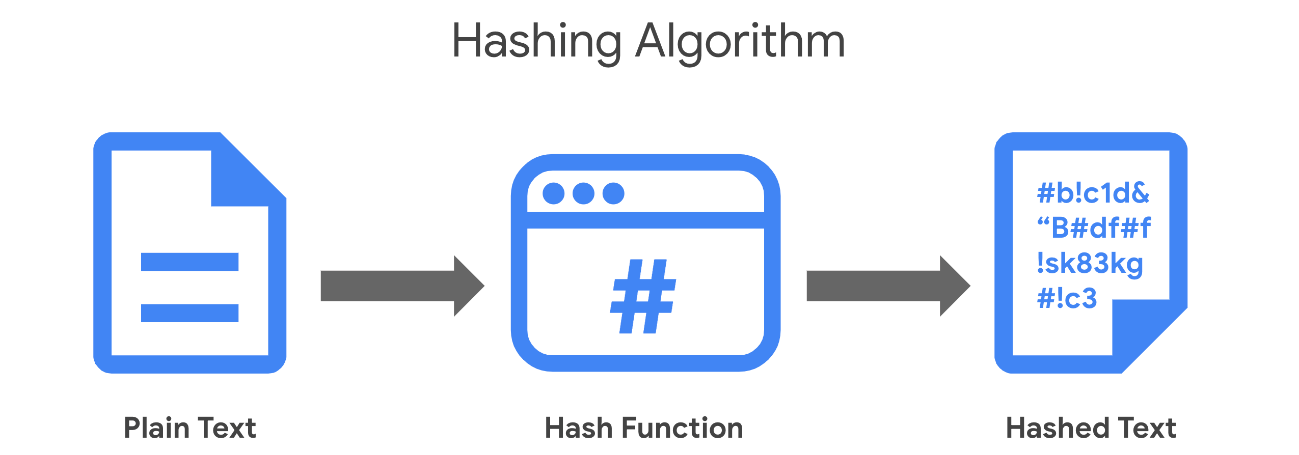
**Sự phát triển của hàm băm**

|  |
| --- |
| Hash functions are important controls that are part of every company's security strategy. Hashing is widely used for authentication and **non-repudiation**, the concept that the authenticity of information can’t be denied. |

Hàm băm là các biện pháp kiểm soát quan trọng nằm trong chiến lược bảo mật của mọi công ty. Băm được sử dụng rộng rãi để xác thực và **chống chối bỏ** , khái niệm cho rằng tính xác thực của thông tin không thể bị từ chối.

|  |
| --- |
| Previously, you learned that **hash functions** are algorithms that produce a code that can't be decrypted.Hash functions convert information into a unique value that can then be used to determine its integrity. In this reading, you’ll learn about the origins of hash functions and how they’ve changed over time. |

Trước đây, bạn đã biết rằng **hàm băm** là thuật toán tạo ra mã không thể giải mã được. Hàm băm chuyển đổi thông tin thành một giá trị duy nhất, sau đó có thể được sử dụng để xác định tính toàn vẹn của nó. Trong bài đọc này, bạn sẽ tìm hiểu về nguồn gốc của hàm băm và cách chúng thay đổi theo thời gian.



|  |
| --- |
| **Origins of hashing** |

**Nguồn gốc của băm**

|  |
| --- |
| Hash functions have been around since the early days of computing. They were originally created as a way to quickly search for data. Since the beginning, these algorithms have been designed to represent data of any size as small, fixed-size values, or digests. Using a hash table, which is a data structure that's used to store and reference hash values, these small values became a more secure and efficient way for computers to reference data. |

Hàm băm đã xuất hiện từ những ngày đầu của máy tính. Ban đầu chúng được tạo ra như một cách để nhanh chóng tìm kiếm dữ liệu. Ngay từ đầu, các thuật toán này đã được thiết kế để biểu diễn dữ liệu ở bất kỳ kích thước nào dưới dạng các giá trị nhỏ, có kích thước cố định hoặc bản tóm tắt. Bằng cách sử dụng bảng băm, là cấu trúc dữ liệu dùng để lưu trữ và tham chiếu các giá trị băm, những giá trị nhỏ này đã trở thành cách an toàn và hiệu quả hơn để máy tính tham chiếu dữ liệu.

|  |
| --- |
| One of the earliest hash functions is Message Digest 5, more commonly known as MD5. Professor Ronald Rivest of the Massachusetts Institute of Technology (MIT) developed MD5 in the early 1990s as a way to verify that a file sent over a network matched its source file. |

Một trong những hàm băm sớm nhất là Message Digest 5, thường được gọi là MD5. Giáo sư Ronald Rivest của Viện Công nghệ Massachusetts (MIT) đã phát triển MD5 vào đầu những năm 1990 như một cách để xác minh rằng tệp được gửi qua mạng có khớp với tệp nguồn của nó hay không.

|  |
| --- |
| Whether it’s used to convert a single email or the source code of an application, MD5 works by converting data into a 128-bit value. You might recall that a **bit** is the smallest unit of data measurement on a computer. Bits can either be a 0 or 1. In a computer, bits represent user input in a way that computers can interpret. In a hash table, this appears as a string of 32 characters. Altering anything in the source file generates an entirely new hash value. |

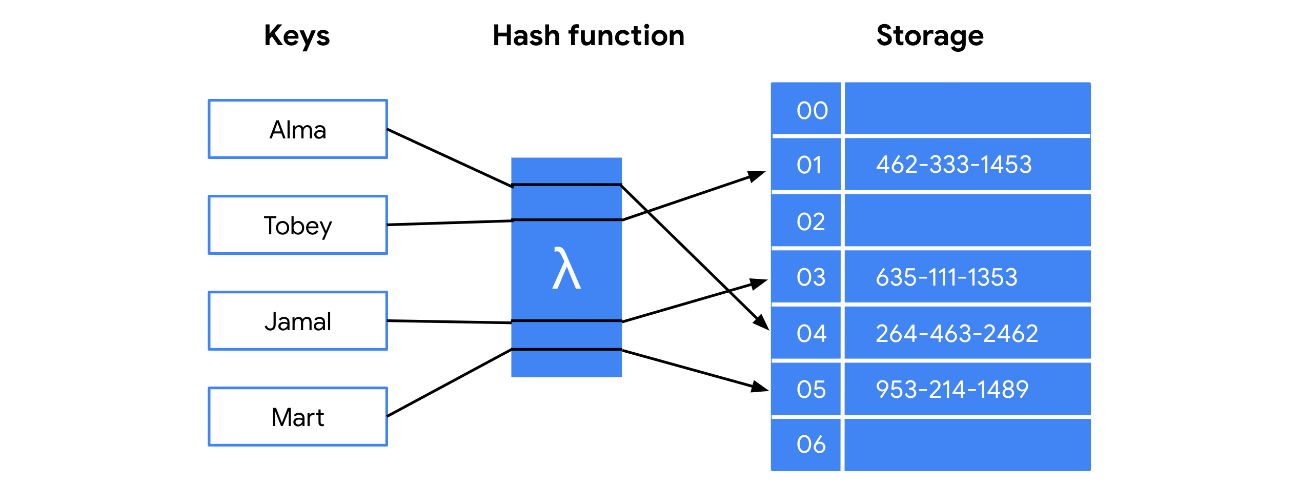
Cho dù được sử dụng để chuyển đổi một email hay mã nguồn của ứng dụng, MD5 hoạt động bằng cách chuyển đổi dữ liệu thành giá trị 128 bit. Bạn có thể nhớ lại rằng **bit** là đơn vị đo lường dữ liệu nhỏ nhất trên máy tính. Bit có thể là 0 hoặc 1. Trong máy tính, bit thể hiện dữ liệu đầu vào của người dùng theo cách mà máy tính có thể hiểu được. Trong bảng băm, nó xuất hiện dưới dạng một chuỗi gồm 32 ký tự. Việc thay đổi mọi thứ trong tệp nguồn sẽ tạo ra một giá trị băm hoàn toàn mới.

|  |
| --- |
| Generally, the longer the hash value, the more secure it is. It wasn’t long after MD5's creation that security practitioners discovered 128-bit digests resulted in a major vulnerability. |

Nói chung, giá trị băm càng dài thì càng an toàn. Không lâu sau khi MD5 được tạo ra, các nhà thực hành bảo mật đã phát hiện ra các bản tóm tắt 128-bit dẫn đến một lỗ hổng lớn.

|  |
| --- |
| Here is an example of how plaintext gets turned into hash values: |

Đây là một ví dụ về cách bản rõ được chuyển thành giá trị băm:



|  |
| --- |
| **Hash collisions** |

**Xung đột băm**

|  |
| --- |
| One of the flaws in MD5 happens to be a characteristic of all hash functions. Hash algorithms map any input, regardless of its length, into a fixed-size value of letters and numbers. What’s the problem with that? Although there are an infinite amount of possible inputs, there’s only a finite set of available outputs! |

Một trong những sai sót trong MD5 tình cờ lại là một đặc điểm của tất cả các hàm băm. Thuật toán băm ánh xạ bất kỳ đầu vào nào, bất kể độ dài của nó, thành một giá trị có kích thước cố định của các chữ cái và số. Có vấn đề gì với điều đó vậy? Mặc dù có vô số đầu vào có thể có nhưng chỉ có một tập hợp hữu hạn các đầu ra khả dụng!

|  |
| --- |
| MD5 values are limited to 32 characters in length. Due to the limited output size, the algorithm is considered to be vulnerable to **hash collision**, an instance when different inputs produce the same hash value. Because hashes are used for authentication, a hash collision is similar to copying someone’s identity. Attackers can carry out collision attacks to fraudulently impersonate authentic data. |

Giá trị MD5 được giới hạn ở độ dài 32 ký tự. Do kích thước đầu ra hạn chế, thuật toán được coi là dễ bị **xung đột băm** , một trường hợp khi các đầu vào khác nhau tạo ra cùng một giá trị băm. Vì hàm băm được sử dụng để xác thực nên xung đột hàm băm cũng tương tự như việc sao chép danh tính của ai đó. Những kẻ tấn công có thể thực hiện các cuộc tấn công va chạm để mạo danh dữ liệu xác thực một cách gian lận.

|  |
| --- |
| **Next-generation hashing** |

**Băm thế hệ tiếp theo**

|  |
| --- |
| To avoid the risk of hash collisions, functions that generated longer values were needed. MD5's shortcomings gave way to a new group of functions known as the Secure Hashing Algorithms, or SHAs. |

Để tránh nguy cơ xung đột hàm băm, cần có các hàm tạo ra giá trị dài hơn. Những thiếu sót của MD5 đã nhường chỗ cho một nhóm chức năng mới được gọi là Thuật toán băm an toàn hoặc SHA.

|  |
| --- |
| The National Institute of Standards and Technology (NIST) approves each of these algorithms. Numbers besides each SHA function indicate the size of its hash value in bits. Except for SHA-1, which produces a 160-bit digest, these algorithms are considered to be collision-resistant. However, that doesn’t make them invulnerable to other exploits. |

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) phê duyệt từng thuật toán này. Các số bên cạnh mỗi hàm SHA cho biết kích thước giá trị băm của nó tính bằng bit. Ngoại trừ SHA-1 tạo ra bản tóm tắt 160 bit, các thuật toán này được coi là có khả năng chống va chạm. Tuy nhiên, điều đó không làm cho chúng trở nên bất khả xâm phạm trước các hoạt động khai thác khác.

|  |
| --- |
| **Five functions make up the SHA family of algorithms:**   * SHA-1 * SHA-224 * SHA-256 * SHA-384 * SHA-512 |

**Năm hàm tạo nên nhóm thuật toán SHA:**

* SHA-1
* SHA-224
* SHA-256
* SHA-384
* SHA-512

|  |
| --- |
| **Secure password storage** |

**Lưu trữ mật khẩu an toàn**

|  |
| --- |
| Passwords are typically stored in a database where they are mapped to a username. The server receives a request for authentication that contains the credentials supplied by the user. It then looks up the username in the database and compares it with the password that was provided and verifies that it matches before granting them access. |

Mật khẩu thường được lưu trữ trong cơ sở dữ liệu nơi chúng được ánh xạ tới tên người dùng. Máy chủ nhận được yêu cầu xác thực có chứa thông tin xác thực do người dùng cung cấp. Sau đó, nó tra cứu tên người dùng trong cơ sở dữ liệu và so sánh nó với mật khẩu đã được cung cấp và xác minh rằng nó khớp trước khi cấp cho họ quyền truy cập.

|  |
| --- |
| This is a safe system unless an attacker gains access to the user database. If passwords are stored in plaintext, then an attacker can steal that information and use it to access company resources. Hashing adds an additional layer of security. Because hash values can't be reversed, an attacker would not be able to steal someone's login credentials if they managed to gain access to the database. |

Đây là một hệ thống an toàn trừ khi kẻ tấn công giành được quyền truy cập vào cơ sở dữ liệu người dùng. Nếu mật khẩu được lưu trữ ở dạng văn bản gốc thì kẻ tấn công có thể đánh cắp thông tin đó và sử dụng nó để truy cập tài nguyên của công ty. Băm thêm một lớp bảo mật bổ sung. Vì không thể đảo ngược các giá trị băm nên kẻ tấn công sẽ không thể lấy cắp thông tin đăng nhập của ai đó nếu họ giành được quyền truy cập vào cơ sở dữ liệu.

|  |
| --- |
| **Rainbow tables** |

**Bàn cầu vồng**

|  |
| --- |
| A **rainbow table** is a file of pre-generated hash values and their associated plaintext. They’re like dictionaries of weak passwords. Attackers capable of obtaining an organization’s password database can use a rainbow table to compare them against all possible values. |

Bảng **Rainbow** là một tệp chứa các giá trị băm được tạo trước và văn bản gốc liên quan của chúng. Chúng giống như những cuốn từ điển về mật khẩu yếu. Những kẻ tấn công có khả năng lấy được cơ sở dữ liệu mật khẩu của tổ chức có thể sử dụng bảng Rainbow để so sánh chúng với tất cả các giá trị có thể.

|  |
| --- |
| **Adding some “salt”** |

**Thêm chút “muối”**

|  |
| --- |
| Functions with larger digests are less vulnerable to collision and rainbow table attacks. But as you’re learning, no security control is perfect. |

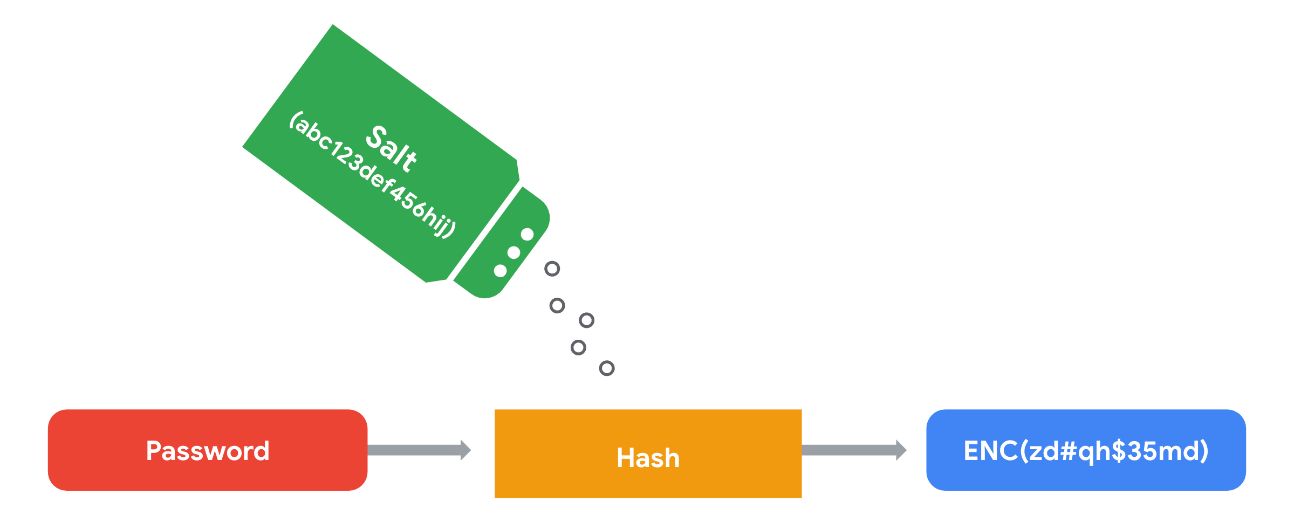
Các hàm có bảng tóm tắt lớn hơn sẽ ít bị tổn thương hơn trước các cuộc tấn công va chạm và bảng cầu vồng. Nhưng khi bạn đang tìm hiểu, không có biện pháp kiểm soát bảo mật nào là hoàn hảo.

|  |
| --- |
| **Salting** is an additional safeguard that's used to strengthen hash functions. A *salt* is a random string of characters that's added to data before it's hashed. The additional characters produce a more unique hash value, making salted data resilient to rainbow table attacks. |

**Muối** là một biện pháp bảo vệ bổ sung được sử dụng để tăng cường hàm băm. Muối là một chuỗi ký tự ngẫu nhiên được thêm vào dữ liệu trước khi được băm *.* Các ký tự bổ sung tạo ra giá trị băm độc đáo hơn, giúp dữ liệu muối có khả năng phục hồi trước các cuộc tấn công bảng cầu vồng.

|  |
| --- |
| For example, a database containing passwords might have several hashed entries for the password "password." If those passwords were all salted, each entry would be completely different. That means an attacker using a rainbow table would be unable to find matching values for "password" in the database. |

Ví dụ: cơ sở dữ liệu chứa mật khẩu có thể có một số mục nhập được băm cho "mật khẩu" mật khẩu. Nếu những mật khẩu đó đều được đánh dấu muối thì mỗi mục sẽ hoàn toàn khác nhau. Điều đó có nghĩa là kẻ tấn công sử dụng bảng Rainbow sẽ không thể tìm thấy các giá trị phù hợp cho "mật khẩu" trong cơ sở dữ liệu.



|  |
| --- |
| For this reason, salting has become increasingly common when storing passwords and other types of sensitive data. The length and uniqueness of a salt is important. Similar to hash values, the longer and more complex a salt is, the harder it is to crack. |

Vì lý do này, việc đánh muối ngày càng trở nên phổ biến khi lưu trữ mật khẩu và các loại dữ liệu nhạy cảm khác. Độ dài và tính độc đáo của muối rất quan trọng. Tương tự như giá trị băm, muối càng dài và phức tạp thì càng khó bẻ khóa.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Security professionals often use hashing as a tool to validate the integrity of program files, documents, and other types of data. Another way it’s used is to reduce the chances of a data breach. As you’ve learned, not all hashing functions provide the same level of protection. Rainbow table attacks are more likely to work against algorithms that generate shorter keys, like MD5. Many small- and medium-sized businesses still rely on MD5 to secure sensitive data. Knowing about alternative algorithms and salting better prepares you to make impactful security recommendations. |

Các chuyên gia bảo mật thường sử dụng hàm băm như một công cụ để xác thực tính toàn vẹn của tệp chương trình, tài liệu và các loại dữ liệu khác. Một cách khác nó được sử dụng là giảm nguy cơ vi phạm dữ liệu. Như bạn đã biết, không phải tất cả các hàm băm đều cung cấp mức độ bảo vệ như nhau. Các cuộc tấn công bảng cầu vồng có nhiều khả năng chống lại các thuật toán tạo ra các khóa ngắn hơn, như MD5. Nhiều doanh nghiệp vừa và nhỏ vẫn dựa vào MD5 để bảo mật dữ liệu nhạy cảm. Biết về các thuật toán thay thế và chuẩn bị kỹ càng hơn sẽ giúp bạn đưa ra các đề xuất bảo mật có tác động mạnh mẽ.

***2.10. Activity: Create hash values - Hoạt động: Tạo giá trị băm***

***2.11. Optional Exemplar: Create hash values - Mẫu tùy chọn: Tạo giá trị băm***

***2.12. Test your knowledge: Encryption methods - Kiểm tra kiến ​​thức của bạn: Phương pháp mã hóa***

**3. Authentication, authorization, and accounting - Xác thực, ủy quyền và kế toán**

***3.1. Access controls and authentication systems - Kiểm soát truy cập và hệ thống xác thực***

|  |
| --- |
| Protecting data is a fundamental feature of security controls. When it comes to keeping information safe and secure, hashing and encryption are powerful, yet limited tools. Managing who or what has access to information is also key to safeguarding information. |

Bảo vệ dữ liệu là một tính năng cơ bản của kiểm soát bảo mật.Khi nói đến việc giữ thông tin an toàn và bảo mật, băm và mã hóalà những công cụ mạnh mẽ nhưng còn hạn chế.Quản lý ai hoặcnhững gì có quyền truy cập vào thông tin cũng là chìa khóa để bảo vệ thông tin.

|  |
| --- |
| The next series of controls that we'll be exploring are access controls, the security controls that manage access, authorization, and accountability of information. When done well, access controls maintain data confidentiality, integrity, and availability. They also get users the information they need quickly. |

Chuỗi kiểm soát tiếp theo mà chúng ta sẽ khám phá là kiểm soát quyền truy cập,các biện pháp kiểm soát bảo mật quản lý quyền truy cập, ủy quyền vàtrách nhiệm giải trình về thông tin.Khi được thực hiện tốt, kiểm soát truy cập sẽ duy trì tính bảo mật của dữ liệu,tính toàn vẹn và tính sẵn có.Họ cũng cung cấp cho người dùng thông tin họ cần một cách nhanh chóng.

|  |
| --- |
| These systems are commonly broken down into three separate, yet related functions known as the authentication, authorization, and accounting framework. Each control has its own protocol and systems that make them work. In this video, let's get comfortable with the basics of the first one on the list, authentication. |

Các hệ thống này thường được chia thành ba chức năng riêng biệt nhưng có liên quan đến nhau.được gọi là khung xác thực, ủy quyền và kế toán.Mỗi điều khiển có giao thức và hệ thống riêng giúp chúng hoạt động.Trong video này, chúng ta hãy cùng làm quen với những kiến ​​thức cơ bản về phần đầu tiên trong danh sách,xác thực.

|  |
| --- |
| Authentication systems are access controls that serve a very basic purpose. They ask anything attempting to access information this simple question: who are you? Organizations go about collecting answers to these questions differently, depending on the objectives of their security policy. Some are more thorough than others, but in general, responses to this question can be based on three factors of authentication. |

Hệ thống xác thực là các biện pháp kiểm soát truy cập phục vụ mục đích rất cơ bản.Họ hỏi bất cứ điều gì cố gắng truy cập thông tincâu hỏi đơn giản này: bạn là ai?Các tổ chức tiến hành thu thập câu trả lời cho những câu hỏi này một cách khác nhau,tùy thuộc vào mục tiêu của chính sách bảo mật của họ.Một số kỹ lưỡng hơn những cái khác, nhưng nói chung,câu trả lời cho câu hỏi này có thể dựa trên ba yếu tố xác thực.

|  |
| --- |
| The first is knowledge. Authentication by knowledge refers to something the user knows, like a password or the answer to a security question they provided previously. |

Đầu tiên là kiến ​​thức. Xác thực bằng kiến ​​thức đề cập đến điều gì đó mà người dùngbiết, như mật khẩu hoặccâu trả lời cho câu hỏi bảo mật mà họ đã cung cấp trước đó.

|  |
| --- |
| Another factor is ownership, referring to something the user possesses. A commonly used type of authentication by ownership is a one-time passcode, or OTP. You've probably experienced these at one time or another. They're a random number sequence that an application or website will send you via text or email and ask you to provide. |

Một yếu tố khác là quyền sở hữu, đề cập đến thứ mà người dùng sở hữu.Loại xác thực thường được sử dụng theo quyền sở hữu là mật mã một lần hoặc OTP.Có lẽ bạn đã từng trải qua những điều này lúc này hay lúc khác.Chúng là một chuỗi số ngẫu nhiên mà một ứng dụng hoặc trang websẽ gửi cho bạn qua tin nhắn hoặc email và yêu cầu bạn cung cấp.

|  |
| --- |
| Last is characteristic. Authentication by this factor is something the user is. Biometrics, like fingerprint scans on your smartphone, are example of this type of authentication. While not used everywhere, this form of authentication is becoming more common because it's much tougher for criminals to impersonate someone if they have to mimic a fingerprint or facial scan as opposed to a password. |

Cuối cùng là đặc trưng. Xác thực bởi yếu tố này là điều mà người dùng phải làm.Sinh trắc học, như quét dấu vân tay trên điện thoại thông minh của bạn, là ví dụ về loạixác thực.Mặc dù không được sử dụng ở mọi nơi nhưng hình thức xác thực này đang trở nên phổ biến hơnbởi vì tội phạm sẽ khó mạo danh ai đó hơn nhiềunếu họ phải bắt chước quét dấu vân tay hoặc khuôn mặt thay vì mật khẩu.

|  |
| --- |
| The information provided during authentication needs to match the information on file for these access controls to work. When the credentials don't match, authentication fails and access is denied. When they match, access is granted. |

Thông tin được cung cấp trong quá trình xác thực cần phải khớpthông tin trong hồ sơ để các biện pháp kiểm soát truy cập này hoạt động.Khi thông tin đăng nhập không khớp, xác thực không thành công và quyền truy cập bị từ chối.Khi chúng khớp nhau, quyền truy cập sẽ được cấp.

|  |
| --- |
| Incorrectly denying access can be frustrating to anyone. To make access systems more convenient, many organizations these days rely on single sign-on. Single sign-on, or SSO, is a technology that combines several different logins into one. Can you imagine having to reintroduce yourself every time you meet up with a friend? That's exactly the sort of problem SSO solves. |

Việc từ chối quyền truy cập không chính xác có thể gây khó chịu cho bất kỳ ai.Để làm cho hệ thống truy cập thuận tiện hơn,nhiều tổ chức ngày nay dựa vào đăng nhập một lần.Đăng nhập một lần, hoặcSSO, là công nghệ kết hợp nhiều thông tin đăng nhập khác nhau thành một.Bạn có thể tưởng tượng việc phải giới thiệu lại bản thân mỗi lần gặp gỡmột người bạn?Đó chính xác là loại vấn đề mà SSO giải quyết.

|  |
| --- |
| Instead of requiring users to authenticate over and over again, SSO establishes their identity once, allowing them to gain access to company resources faster. While SSO systems are helpful when it comes to speeding up the authentication process, they present a significant vulnerability when used alone. |

Thay vì yêu cầu người dùng xác thực nhiều lần, SSO thiết lậpdanh tính của họ một lần, cho phép họ truy cập vào tài nguyên của công ty nhanh hơn.Mặc dù hệ thống SSO rất hữu ích trong việc tăng tốc quá trình xác thực,chúng có một lỗ hổng đáng kể khi được sử dụng một mình.

|  |
| --- |
| Denying access to authorized users can be frustrating, but you know what's even worse? Incorrectly granting access to the wrong user. SSO technology is great, but not if it relies on just a single factor of authentication. Adding more authentication factors strengthen these systems. |

Việc từ chối quyền truy cập của người dùng được ủy quyền có thể gây khó chịu,nhưng bạn biết điều gì còn tệ hơn nữa không? Cấp quyền truy cập không chính xác cho người dùng sai.Công nghệ SSO rất tuyệt vời, nhưng sẽ không tốt nếu nó chỉ dựa vào một yếu tố duy nhất.xác thực. Việc bổ sung thêm nhiều yếu tố xác thực sẽ củng cố các hệ thống này.

|  |
| --- |
| Multi-factor authentication, or MFA, is a security measure, which requires a user to verify their identity in two or more ways to access a system or network. MFA combines two or more independent credentials, like knowledge and ownership, to prove that someone is who they claim to be. |

Xác thực đa yếu tố, hay MFA, là một biện pháp bảo mật yêu cầungười dùng xác minh danh tính của họ theo hai hoặc nhiều cách để truy cập hệ thống hoặc mạng.MFA kết hợp hai hoặc nhiều thông tin độc lập, như kiến ​​thức vàquyền sở hữu, để chứng minh rằng ai đó chính là người mà họ tuyên bố.

|  |
| --- |
| SSO and MFA are often used in conjunction with one another to layer the defense capabilities of authentication systems. When both are used, organizations can ensure convenient access that is also secure. Now that we covered authentication, we're ready to explore the second part of the framework. Next, we'll learn about authorization! |

SSO và MFA thường được sử dụng kết hợp với nhauđể phân tầng khả năng phòng thủ của các hệ thống xác thực.Khi cả hai đều được sử dụng, các tổ chức có thể đảm bảo truy cập thuận tiệnđiều đó cũng an toàn.Bây giờ chúng ta đã đề cập đến việc xác thực,chúng ta đã sẵn sàng khám phá phần thứ hai của khuôn khổ này.Tiếp theo chúng ta sẽ tìm hiểu về ủy quyền!

***3.2. The rise of SSO and MFA - Sự trỗi dậy của SSO và MFA***

|  |
| --- |
| **The rise of SSO and MFA** |

**Sự trỗi dậy của SSO và MFA**

|  |
| --- |
| Most companies help keep their data safely locked up behind authentication systems. Usernames and passwords are the keys that unlock information for most organizations. But are those credentials enough? Information security often focuses on managing a user's access of, and authorization to, information. |

Hầu hết các công ty đều giúp giữ dữ liệu của họ được khóa an toàn sau các hệ thống xác thực. Tên người dùng và mật khẩu là chìa khóa mở khóa thông tin cho hầu hết các tổ chức. Nhưng những thông tin đó có đủ không? Bảo mật thông tin thường tập trung vào việc quản lý quyền truy cập và ủy quyền của người dùng đối với thông tin.

|  |
| --- |
| Previously, you learned about the three factors of authentication: knowledge, ownership, and characteristic. Single sign-on (SSO) and multi-factor authentication (MFA) are two technologies that have become popular for implementing these authentication factors. In this reading, you’ll learn how these technologies work and why companies are adopting them. |

Trước đây, bạn đã tìm hiểu về ba yếu tố xác thực: kiến ​​thức, quyền sở hữu và đặc điểm. Đăng nhập một lần (SSO) và xác thực đa yếu tố (MFA) là hai công nghệ đã trở nên phổ biến để triển khai các yếu tố xác thực này. Trong bài đọc này, bạn sẽ tìm hiểu cách các công nghệ này hoạt động và lý do tại sao các công ty áp dụng chúng.

|  |
| --- |
| **A better approach to authentication** |

**Một cách tiếp cận tốt hơn để xác thực**

|  |
| --- |
| **Single sign-on** (SSO) is a technology that combines several different logins into one. More companies are turning to SSO as a solution to their authentication needs for three reasons:   1. **SSO improves the user experience** by eliminating the number of usernames and passwords people have to remember. 2. **Companies can lower costs** by streamlining how they manage connected services. 3. **SSO improves overall security** by reducing the number of access points attackers can target. |

**Đăng nhập một lần** (SSO) là công nghệ kết hợp nhiều thông tin đăng nhập khác nhau thành một. Nhiều công ty đang chuyển sang SSO như một giải pháp cho nhu cầu xác thực của họ vì ba lý do:

1. **SSO cải thiện trải nghiệm người dùng** bằng cách loại bỏ số lượng tên người dùng và mật khẩu mà mọi người phải nhớ.
2. **Các công ty có thể giảm chi phí** bằng cách hợp lý hóa cách họ quản lý các dịch vụ được kết nối.
3. **SSO cải thiện bảo mật tổng thể** bằng cách giảm số lượng điểm truy cập mà kẻ tấn công có thể nhắm mục tiêu.

|  |
| --- |
| This technology became available in the mid-1990s as a way to combat *password fatigue*, which refers to people’s tendency to reuse passwords across services. Remembering many different passwords can be a challenge, but using the same password repeatedly is a major security risk. SSO solves this dilemma by shifting the burden of authentication away from the user. |

Công nghệ này xuất hiện vào giữa những năm 1990 như một cách để chống lại *sự mệt mỏi của mật khẩu* , đề cập đến xu hướng sử dụng lại mật khẩu trên các dịch vụ của mọi người. Việc nhớ nhiều mật khẩu khác nhau có thể là một thách thức nhưng việc sử dụng cùng một mật khẩu nhiều lần lại là một rủi ro bảo mật lớn. SSO giải quyết vấn đề nan giải này bằng cách chuyển gánh nặng xác thực khỏi người dùng.

|  |
| --- |
| **How SSO works** |

**Cách hoạt động của SSO**

|  |
| --- |
| SSO works by automating how trust is established between a user and a service provider. Rather than placing the responsibility on an employee or customer, SSO solutions use trusted third-parties to prove that a user is who they claim to be. This is done through the exchange of encrypted access tokens between the identity provider and the service provider. |

SSO hoạt động bằng cách tự động hóa cách thiết lập niềm tin giữa người dùng và nhà cung cấp dịch vụ. Thay vì đặt trách nhiệm lên nhân viên hoặc khách hàng, giải pháp SSO sử dụng các bên thứ ba đáng tin cậy để chứng minh rằng người dùng chính là người mà họ tuyên bố. Điều này được thực hiện thông qua việc trao đổi mã thông báo truy cập được mã hóa giữa nhà cung cấp danh tính và nhà cung cấp dịch vụ.

|  |
| --- |
| Similar to other kinds of digital information, these access tokens are exchanged using specific protocols. SSO implementations commonly rely on two different authentication protocols: LDAP and SAML. LDAP, which stands for Lightweight Directory Access Protocol, is mostly used to transmit information on-premises; SAML, which stands for Security Assertion Markup Language, is mostly used to transmit information off-premises, like in the cloud. |

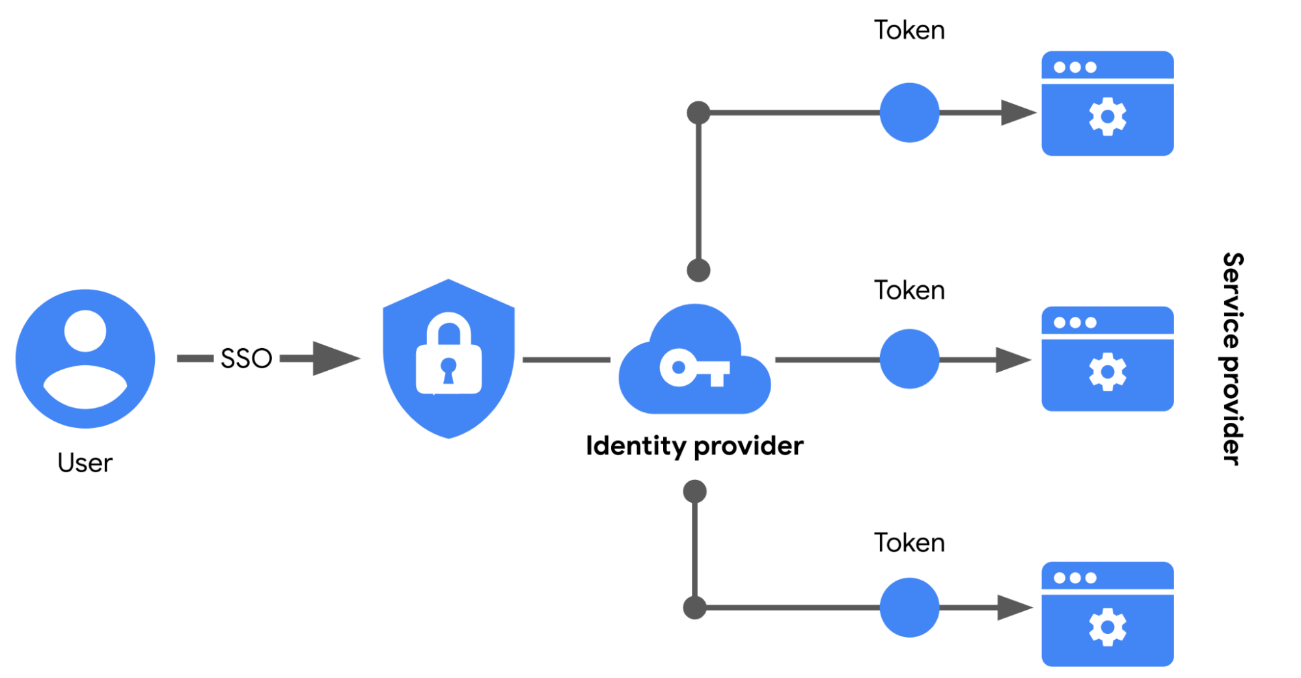
Tương tự như các loại thông tin kỹ thuật số khác, các mã thông báo truy cập này được trao đổi bằng các giao thức cụ thể. Việc triển khai SSO thường dựa vào hai giao thức xác thực khác nhau: LDAP và SAML. LDAP, viết tắt của Giao thức truy cập thư mục nhẹ, chủ yếu được sử dụng để truyền thông tin tại chỗ; SAML, viết tắt của Ngôn ngữ đánh dấu xác nhận bảo mật, chủ yếu được sử dụng để truyền thông tin ra bên ngoài cơ sở, như trên đám mây.

|  |
| --- |
| **Note:** LDAP and SAML protocols are often used together. |

**Lưu ý:** Giao thức LDAP và SAML thường được sử dụng cùng nhau.

|  |
| --- |
| Here's an example of how SSO can connect a user to multiple applications with one access token: |

Dưới đây là ví dụ về cách SSO có thể kết nối người dùng với nhiều ứng dụng bằng một mã thông báo truy cập:



|  |
| --- |
| **Limitations of SSO** |

**Hạn chế của SSO**

|  |
| --- |
| Usernames and passwords alone are not always the most secure way of protecting sensitive information. SSO provides useful benefits, but there’s still the risk associated with using one form of authentication. For example, a lost or stolen password could expose information across multiple services. Thankfully, there’s a solution to this problem. |

Riêng tên người dùng và mật khẩu không phải lúc nào cũng là cách an toàn nhất để bảo vệ thông tin nhạy cảm. SSO mang lại những lợi ích hữu ích nhưng vẫn có rủi ro liên quan đến việc sử dụng một hình thức xác thực. Ví dụ: mật khẩu bị mất hoặc bị đánh cắp có thể làm lộ thông tin trên nhiều dịch vụ. Rất may, có một giải pháp cho vấn đề này.

|  |
| --- |
| **MFA to the rescue** |

**MFA để giải cứu**

|  |
| --- |
| **Multi-factor authentication** (MFA) requires a user to verify their identity in two or more ways to access a system or network. In a sense, MFA is similar to using an ATM to withdraw money from your bank account. First, you insert a debit card into the machine as one form of identification. Then, you enter your PIN number as a second form of identification. Combined, both steps, or factors, are used to verify your identity before authorizing you to access the account. |

**Xác thực đa yếu tố** (MFA) yêu cầu người dùng xác minh danh tính của họ theo hai cách trở lên để truy cập hệ thống hoặc mạng. Ở một khía cạnh nào đó, MFA tương tự như việc sử dụng máy ATM để rút tiền từ tài khoản ngân hàng của bạn. Đầu tiên, bạn đưa thẻ ghi nợ vào máy như một hình thức nhận dạng. Sau đó, bạn nhập số PIN của mình làm hình thức nhận dạng thứ hai. Kết hợp cả hai bước hoặc yếu tố, được sử dụng để xác minh danh tính của bạn trước khi cho phép bạn truy cập vào tài khoản.



|  |
| --- |
| **Strengthening authentication** |

**Tăng cường xác thực**

|  |
| --- |
| **Strengthening authentication**  MFA builds on the benefits of SSO. It works by having users prove that they are who they claim to be. The user must provide two factors (2FA) or three factors (3FA) to authenticate their identification. The MFA process asks users to provide these proofs, such as:   * **Something a user knows:** most commonly a username and password * **Something a user has:** normally received from a service provider, like a one-time passcode (OTP) sent via SMS * **Something a user is:** refers to physical characteristics of a user, like their fingerprints or facial scans |

MFA được xây dựng dựa trên lợi ích của SSO. Nó hoạt động bằng cách yêu cầu người dùng chứng minh rằng họ chính là người mà họ tuyên bố. Người dùng phải cung cấp hai yếu tố (2FA) hoặc ba yếu tố (3FA) để xác thực danh tính của họ. Quy trình MFA yêu cầu người dùng cung cấp các bằng chứng này, chẳng hạn như:

* **Thông tin mà người dùng biết:** phổ biến nhất là tên người dùng và mật khẩu
* **Thứ mà người dùng có:** thường nhận được từ nhà cung cấp dịch vụ, như mật mã một lần (OTP) được gửi qua SMS
* **Đặc điểm của người dùng:** đề cập đến các đặc điểm vật lý của người dùng, như dấu vân tay hoặc quét khuôn mặt của họ

|  |
| --- |
| Requiring multiple forms of identification is an effective security measure, especially in cloud environments. It can be difficult for businesses in the cloud to ensure that the users remotely accessing their systems are not threat actors. MFA can reduce the risk of authenticating the wrong users by requiring forms of identification that are difficult to imitate or brute force. |

Yêu cầu nhiều hình thức nhận dạng là một biện pháp bảo mật hiệu quả, đặc biệt là trong môi trường đám mây. Các doanh nghiệp trên đám mây có thể gặp khó khăn trong việc đảm bảo rằng người dùng truy cập từ xa vào hệ thống của họ không phải là tác nhân đe dọa. MFA có thể giảm nguy cơ xác thực nhầm người dùng bằng cách yêu cầu các hình thức nhận dạng khó bắt chước hoặc khó bắt chước.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Implementing both SSO and MFA security controls improves security without sacrificing the user experience. Relying on passwords alone is a serious vulnerability. Implementing SSO means fewer points of entry, but that’s not enough. Combining SSO and MFA can be an effective way to protect information, so that users have a streamlined experience while unauthorized people are kept away from important information. |

Việc triển khai cả biện pháp kiểm soát bảo mật SSO và MFA sẽ cải thiện tính bảo mật mà không ảnh hưởng đến trải nghiệm người dùng. Chỉ dựa vào mật khẩu là một lỗ hổng nghiêm trọng. Triển khai SSO đồng nghĩa với việc có ít điểm truy cập hơn, nhưng điều đó vẫn chưa đủ. Kết hợp SSO và MFA có thể là một cách hiệu quả để bảo vệ thông tin, nhờ đó người dùng có được trải nghiệm hợp lý trong khi những người không được ủy quyền sẽ tránh xa được những thông tin quan trọng.

***3.3. The mechanisms of authorization - Cơ chế ủy quyền***

|  |
| --- |
| Access is as much about authorization as it is about authentication. One of the most important functions of access controls is how they assign responsibility for certain systems and processes. Next up in our exploration of access control systems are the mechanisms of authorization. |

Quyền truy cập cũng giống như ủy quyềnvì đó là về xác thực.Một trong những chức năng quan trọng nhấtkiểm soát truy cập là cách họgiao trách nhiệm cho các hệ thống và quy trình nhất định.Tiếp theo trong cuộc khám phá của chúng tôi vềhệ thống kiểm soát truy cập làcác cơ chế ủy quyền.

|  |
| --- |
| These protocols actually work closely together with authentication technologies. While one validates who the user is, the other determines what they're allowed to do. Let's take a look at the next part of the authentication, authorization, and accounting framework that protects private information. |

Các giao thức này thực sự làm việc chặt chẽ với nhaucác công nghệ xác thực. Trong khi mộtxác thực người dùng là ai,người kia xác định những gì họ được phép làm.Chúng ta hãy xem phần tiếp theo của quá trình xác thực,ủy quyền và khuôn khổ kế toánbảo vệ thông tin cá nhân.

|  |
| --- |
| Earlier, we learned about the principle of least privilege. Authorization is linked to the idea that access to information only lasts as long as needed. Authorization systems are also heavily influenced by this idea in addition to another important security principle, the separation of duties. |

Trước đó chúng ta đã tìm hiểu vềnguyên tắc đặc quyền tối thiểu.Sự ủy quyền được liên kết với ý tưởng rằngviệc tiếp cận thông tin chỉ kéo dài khi cần thiết.Hệ thống ủy quyền cũngbị ảnh hưởng nặng nề bởi ý tưởng nàybên cạnh một nguyên tắc bảo mật quan trọng khác,sự phân chia nhiệm vụ.

|  |
| --- |
| Separation of duties is the principle that users should not be given levels of authorization that will allow them to misuse a system. Separating duties reduces the risk of system failures and inappropriate behavior from users. |

Sự phân chia nhiệm vụ lànguyên tắc người dùng không nên được đưa ramức độ ủy quyền sẽcho phép họ lạm dụng một hệ thống.Việc tách biệt các nhiệm vụ làm giảm nguy cơlỗi hệ thống và hành vi không phù hợp từ người dùng.

|  |
| --- |
| For example, a person responsible for providing customer service shouldn't also be authorized to rate their own performance. In this position, they could easily neglect their duties while continuing to give themselves high marks with no oversight. Similarly, if one person was authorized to develop and test a security system, they are much more likely to be unaware of its weaknesses. |

Ví dụ, một ngườichịu trách nhiệm cung cấp dịch vụ khách hàngcũng không được phép xếp hạnghiệu suất của riêng họ. Ở vị trí này,họ có thể dễ dàng bỏ bê nhiệm vụ của mình trong khitiếp tục cống hiến hết mìnhđiểm cao mà không có sự giám sát.Tương tự, nếu một người đượcđược phép phát triển và thử nghiệm một hệ thống bảo mật,họ có nhiều khả năngkhông nhận thức được điểm yếu của nó.

|  |
| --- |
| Both the principle of least privilege and the concept of separating duties apply to more than just people. They apply to all systems including networks, databases, processes, and any other aspect of an organization. Ultimately, authorization depends on a system or user's role. When it comes to securing data over a network, there are a couple of frequently used access controls that you should be familiar with: HTTP basic auth and OAuth. |

Nguyên tắc đặc quyền tối thiểu và khái niệm vềnhiệm vụ tách biệt áp dụng cho không chỉ con người.Chúng áp dụng cho tất cả các hệ thống bao gồm mạng,cơ sở dữ liệu, quy trình vàbất kỳ khía cạnh nào khác của một tổ chức.Cuối cùng, việc ủy ​​quyền phụ thuộcvề hệ thống hoặc vai trò của người dùng.Khi nói đến việc bảo mật dữ liệu qua mạng,có một vài cái được sử dụng thường xuyênkiểm soát truy cập mà bạn nên làm quen:Xác thực cơ bản HTTP và OAuth.

|  |
| --- |
| Have you ever wondered what the HTTP in web addresses stood for. It stands for hypertext transfer protocol, which is how communications are established over network. HTTP uses what is known as basic auth, the technology used to establish a user's request to access a server. Basic auth works by sending an identifier every time a user communicates with a web page. |

Bạn đã bao giờ tự hỏi điều gìHTTP trong địa chỉ web là viết tắt của.Nó là viết tắt của giao thức truyền siêu văn bản,đó là cách thông tin liên lạc được thiết lập qua mạng.HTTP sử dụng cái được gọi là xác thực cơ bản,công nghệ được sử dụng để thiết lậpyêu cầu của người dùng để truy cập vào máy chủ.Xác thực cơ bản hoạt động bằng cách gửimột mã định danh mọi lúcngười dùng giao tiếp với một trang web.

|  |
| --- |
| Some websites still use basic auth to tell whether or not someone is authorized to access information on that site. However, their protocol is considered to be vulnerable to attacks because it transmits usernames and password openly over the network. Most websites today use HTTPS instead, which stands for hypertext transfer protocol secure. This protocol doesn't expose sensitive information, like access credentials, when communicating over the network. |

Một số trang web vẫn sử dụng xác thực cơ bản để biết liệukhông phải ai đó được ủy quyền đểtruy cập thông tin trên trang web đó.Tuy nhiên, giao thức của họđược coi là dễ bị tấn côngbởi vì nó truyền tên người dùng vàmật khẩu công khai trên mạng.Hầu hết các trang web ngày nay đều sử dụng HTTPS thay thế,viết tắt của giao thức truyền siêu văn bản an toàn.Giao thức này không tiết lộ thông tin nhạy cảm,như thông tin truy cập, khigiao tiếp qua mạng.

|  |
| --- |
| Another secure authentication technology used today is OAuth. OAuth is an open-standard authorization protocol that shares designated access between applications. For example, you can tell Google that it's okay for another website to access your profile to create an account. Instead of requesting and sending sensitive usernames and passwords over the network, OAuth uses API tokens to verify access between you and a service provider. |

Một công nghệ xác thực an toàn khácđược sử dụng ngày nay là OAuth.OAuth là một giao thức ủy quyền tiêu chuẩn mởchia sẻ quyền truy cập được chỉ định giữa các ứng dụng.Ví dụ: bạn có thể nói với Google rằng đó làđược cho một trang web khác truy cập hồ sơ của bạnđể tạo một tài khoản.Thay vì yêu cầu và gửitên người dùng và mật khẩu nhạy cảm qua mạng,OAuth sử dụng mã thông báo API để xác minhtruy cập giữa bạn và nhà cung cấp dịch vụ.

|  |
| --- |
| An API token is a small block of encrypted code that contains information about a user. These tokens contain things like your identity, site permissions, and more. OAuth sends and receives access requests using API tokens by passing them from a server to a user's device. |

Mã thông báo API là một khối nhỏmã được mã hóa có chứa thông tin về người dùng.Những mã thông báo này chứa những thứ như danh tính của bạn,quyền của trang web và hơn thế nữa.OAuth gửi và nhận yêu cầu truy cập bằng cách sử dụngMã thông báo API bằng cách chuyển chúng từmột máy chủ đến thiết bị của người dùng.

|  |
| --- |
| Let's explore what's going on behind the scenes. When you authorize a site to create an account using your Google profile, all of Google's usual login protocols are still active. If you have multi-factor authentication enabled on your account, and you should, you'll still have the security benefits that it provides. API tokens minimize risks in a major way. These API tokens serve as an additional layer of encryption that helps to keep your Google password safe in the event of a breach on another platform. |

Hãy cùng khám phá những gì đang diễn ra đằng sau hậu trường.Khi bạn ủy quyền cho một trang web được tạomột tài khoản sử dụng hồ sơ trên Google của bạn,tất cả các giao thức đăng nhập thông thường của Google vẫn hoạt động.Nếu bạn có xác thực đa yếu tốđược bật trên tài khoản của bạn và bạn nên,bạn vẫn sẽ có những lợi ích bảo mật mà nó cung cấp.Mã thông báo API giảm thiểu rủi ro một cách chủ yếu.Các mã thông báo API này đóng vai tròmột lớp mã hóa bổ sung giúpgiữ mật khẩu Google của bạn an toàn trongtrường hợp vi phạm trên nền tảng khác.

|  |
| --- |
| Basic auth and OAuth are just a couple of examples of authorization tools that are designed with the principles of least privilege and separation of duty in mind. There are many other controls that help limit the risk of unauthorized access to information. In addition to controlling access, it's also important to monitor it. |

Xác thực cơ bản và OAuth làchỉ là một vài ví dụ về công cụ ủy quyềnđược thiết kế với các nguyên tắc củaít đặc quyền và phân chia nhiệm vụ trong tâm trí.Có nhiều biện pháp kiểm soát khác giúp hạn chếnguy cơ truy cập thông tin trái phép.Ngoài việc kiểm soát truy cập,điều quan trọng là phải theo dõi nó.

|  |
| --- |
| In our next video, we'll focus on the third and final part of the authentication, authorization, and accounting framework. |

Trong video tiếp theo, chúng tôi sẽ tập trung vàophần thứ ba và cuối cùng của xác thực,ủy quyền và khuôn khổ kế toán.

***3.4. Why we audit user activity - Tại sao chúng tôi kiểm tra hoạt động của người dùng***

|  |
| --- |
| Have you ever wondered if your employer is keeping a record of when you log into company systems? Well, they are, if they're implementing the third and final function of the authentication, authorization, and accounting framework. |

Bạn đã bao giờ tự hỏi liệu người chủ của bạn có đang giữhồ sơ về thời điểm bạn đăng nhập vào hệ thống công ty?Đúng vậy, nếu họ đang triển khaichức năng thứ ba và cuối cùng của xác thực,ủy quyền và khuôn khổ kế toán.

|  |
| --- |
| Accounting is the practice of monitoring the access logs of a system. These logs contain information like who accessed the system, and when they accessed it, and what resources they used. |

Kế toán là việc thực hànhgiám sát nhật ký truy cập của hệ thống.Những nhật ký này chứa thông tin như aiđã truy cập vào hệ thống, và khi họ truy cập vào nó,và họ đã sử dụng những tài nguyên nào.

|  |
| --- |
| Security analysts use access logs a lot. The data they contain is a helpful way to identify trends, like failed login attempts. They're also used to uncover hackers who have gained access to a system, and for detecting an incident, like a data breach. |

Các nhà phân tích bảo mật sử dụng nhật ký truy cập rất nhiều.Dữ liệu chúng chứa là một cách hữu ích đểxác định xu hướng, chẳng hạn như các lần đăng nhập thất bại.Chúng cũng được sử dụng để khám phátin tặc đã có quyền truy cập vàomột hệ thống và chophát hiện một sự cố, chẳng hạn như vi phạm dữ liệu.

|  |
| --- |
| In this field, access logs are essential. Oftentimes, analyzing them is the first procedure you'll follow when investigating a security event. So, how do access logs compile all this useful information? Let's examine this more closely. |

Trong lĩnh vực này, nhật ký truy cập là rất cần thiết.Thông thường, việc phân tích chúng làquy trình đầu tiên bạn sẽ làm theokhi điều tra một sự kiện bảo mật.Vì vậy, làm cách nào để nhật ký truy cập tổng hợp tất cả thông tin hữu ích này?Hãy xem xét điều này chặt chẽ hơn.

|  |
| --- |
| Anytime a user accesses a system, they initiate what's called a session. A session is a sequence of network HTTP basic auth requests and responses associated with the same user, like when you visit a website. Access logs are essentially records of sessions that capture the moment a user enters a system until the moment they leave it. |

Bất cứ khi nào người dùng truy cập vào hệ thống,họ bắt đầu cái gọi là phiên.Phiên là một chuỗi HTTP mạngyêu cầu xác thực cơ bản vàphản hồi liên quan đến cùng một người dùng,giống như khi bạn truy cập một trang web.Nhật ký truy cập về cơ bản là bản ghi của các phiênghi lại khoảnh khắc người dùng bước vàomột hệ thống cho đến thời điểm họ rời bỏ nó.

|  |
| --- |
| Two actions are triggered when the session begins. The first is the creation of a session ID. A session ID is a unique token that identifies a user and their device while accessing the system. Session IDs are attached to the user until they either close their browser or the session times out. |

Hai hành động được kích hoạt khi phiên bắt đầu.Đầu tiên là việc tạo ID phiên.ID phiên là mã thông báo duy nhất xác địnhngười dùng và thiết bị của họ trong khi truy cập hệ thống.ID phiên được đính kèm với người dùng cho đến khihọ đóng trình duyệt hoặc hết phiên.

|  |
| --- |
| The second action that takes place at the start of a session is an exchange of session cookies between a server and a user's device. A session cookie is a token that websites use to validate a session and determine how long that session should last. When cookies are exchanged between your computer and a server, your session ID is read to determine what information the website should show you. |

Hành động thứ hai được thực hiệnvị trí khi bắt đầu một phiên làtrao đổi cookie phiêngiữa máy chủ và thiết bị của người dùng.Cookie phiên là mã thông báo mà các trang web sử dụng đểxác thực một phiên và xác định cáchphiên đó sẽ kéo dài.Khi cookie được trao đổigiữa máy tính của bạn và máy chủ,ID phiên của bạn được đọc để xác địnhnhững thông tin nào trang web sẽ hiển thị cho bạn.

|  |
| --- |
| Cookies make web sessions safer and more efficient. The exchange of tokens means that no sensitive information, like usernames and passwords, are shared. Session cookies prevent attackers from obtaining sensitive data. However, there's other damage that they can do. With a stolen cookie, an attacker can impersonate a user using their session token. This kind of attack is known as session hijacking. |

Cookie làm cho các phiên truy cập web an toàn hơn và hiệu quả hơn.Việc trao đổi token có nghĩa làkhông có thông tin nhạy cảm, nhưtên người dùng và mật khẩu, được chia sẻ.Cookie phiên ngăn chặn kẻ tấn côngtừ việc lấy được dữ liệu nhạy cảm.Tuy nhiên, có những thiệt hại khác mà họ có thể gây ra.Với một chiếc bánh quy bị đánh cắp,kẻ tấn công có thể mạo danhngười dùng sử dụng mã thông báo phiên của họ.Kiểu tấn công này được gọi là chiếm quyền điều khiển phiên.

|  |
| --- |
| Session hijacking is an event when attackers obtain a legitimate user's session ID. During these kinds of attacks, cyber criminals impersonate the user, causing all sorts of harm. Money or private data can be stolen. If, for example, hijackers obtain a single sign-on credential from stolen cookies, they can even gain access to additional systems that otherwise seem secure. |

Chiếm quyền điều khiển phiên là một sự kiện khikẻ tấn công lấy được ID phiên của người dùng hợp pháp.Trong các cuộc tấn công kiểu này,tội phạm mạng mạo danh người dùng,gây ra đủ thứ tai hại.Tiền hoặc dữ liệu riêng tư có thể bị đánh cắp.Nếu, ví dụ,những kẻ tấn công có được một lần đăng nhậpthông tin xác thực từ cookie bị đánh cắp,họ thậm chí có thể truy cập vàocác hệ thống bổ sung có vẻ an toàn.

|  |
| --- |
| This is one reason why accounting and monitoring session logs is so important. Unusual activity on access logs can be an indication that information has been improperly accessed or stolen. At the end of the day, accounting is how we gain valuable insight that makes information safer. |

Đây là một lý do tại sao kế toán vàgiám sát nhật ký phiên là rất quan trọng.Hoạt động bất thường trên nhật ký truy cập có thể là dấu hiệu cho thấythông tin đã bị truy cập không đúng cách hoặc bị đánh cắp.Suy cho cùng, kế toán là cách chúng ta đạt đượccái nhìn sâu sắc có giá trị giúp thông tin an toàn hơn.

***3.5. Tim: Finding purpose in protecting assets - Tim: Tìm mục đích bảo vệ tài sản***

|  |
| --- |
| [MUSIC] My name is Tim and I work on the Detection and Response team at Google. You can think of us as the smoke detectors and the fire departments at Google. So what our job is, is to detect harmful activity that may affect Google and its users. The stakes here are very, very high. So imagine what you have on Google, whether it's docs, it's pictures, your financial information, some of your secrets. Some things that you don't want anybody to know. Those are the things that we're protecting. Cybersecurity professionals are there to protect the most valuable assets of the company. You'll be there to protect that, and that direct line from what you're doing to what the company feels is most important, most valuable, and protecting that, I think provides a lot of purpose for folks. And provides a lot of motivation and provides the basis and the foundation for a very, very satisfying career. Cybersecurity is a profoundly rewarding career. It is a function that is critical at many, many companies and it is a career that is in high demand, and there is an absolute shortage of talented labor out there. So from that aspect, if you're looking for a path to a viable, long term, rewarding career, this is as straight a path to that as you can imagine. |

[ÂM NHẠC]Tên tôi là Tim và tôi làm việc trong nhóm Phát hiện và Phản hồi tại Google.Bạn có thể coi chúng tôi như những người phát hiện khói và sở cứu hỏa tại Google.Vì vậy công việc của chúng tôi là phát hiện hoạt động có hại có thểảnh hưởng đến Google và người dùng của Google.Tiền đặt cược ở đây rất, rất cao.Vì vậy, hãy tưởng tượng những gì bạn có trên Google, cho dù đó là tài liệu,đó là những bức ảnh, thông tin tài chính của bạn, một số bí mật của bạn.Một số điều bạn không muốn ai biết.Đó là những thứ chúng tôi đang bảo vệ.Chuyên gia an ninh mạngcó mặt để bảo vệ những tài sản có giá trị nhất của công ty.Bạn sẽ ở đó để bảo vệ điều đó, vàđường dẫn trực tiếp từ những gì bạn đang làm đến những gì công ty cảm thấy là quan trọng nhất,giá trị nhất và việc bảo vệ điều đó, tôi nghĩ mang lại rất nhiều mục đích cho mọi người.Và cung cấp rất nhiều động lực và cung cấp cơ sở vànền tảng cho một sự nghiệp rất, rất thỏa mãn.An ninh mạng là một nghề nghiệp có thu nhập cao.Đây là một chức năng quan trọng ở rất nhiều công ty vàđó là một nghề nghiệp có nhu cầu cao vàngoài kia đang thiếu hụt trầm trọng lao động tài năng.Vì vậy, từ khía cạnh đó, nếu bạn đang tìm kiếmmột con đường dẫn đến một sự nghiệp khả thi, lâu dài và xứng đáng,đây là con đường thẳng đến đó như bạn có thể tưởng tượng.

***3.6. Identity and access management - Quản lý danh tính và quyền truy cập***

|  |
| --- |
| **Identity and access management** |

**Quản lý danh tính và quyền truy cập**

|  |
| --- |
| Security is more than simply combining processes and technologies to protect assets. Instead, security is about ensuring that these processes and technologies are creating a secure environment that supports a defense strategy. A key to doing this is implementing two fundamental security principles that limit access to organizational resources:   * The **principle of least privilege** in which a user is only granted the minimum level of access and authorization required to complete a task or function. * **Separation of duties**, which is the principle that users should not be given levels of authorization that would allow them to misuse a system. |

Bảo mật không chỉ đơn giản là kết hợp các quy trình và công nghệ để bảo vệ tài sản. Thay vào đó, bảo mật là đảm bảo rằng các quy trình và công nghệ này đang tạo ra một môi trường an toàn hỗ trợ chiến lược phòng thủ. Chìa khóa để thực hiện điều này là triển khai hai nguyên tắc bảo mật cơ bản nhằm hạn chế quyền truy cập vào tài nguyên của tổ chức:

* Nguyên **tắc đặc quyền tối thiểu** trong đó người dùng chỉ được cấp mức truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ hoặc chức năng.
* **Phân chia nhiệm vụ** , đó là nguyên tắc mà người dùng không được cấp các cấp độ ủy quyền có thể cho phép họ lạm dụng hệ thống.

|  |
| --- |
| Both principles typically support each other. For example, according to least privilege, a person who needs permission to approve purchases from the IT department shouldn't have the permission to approve purchases from every department. Likewise, according to separation of duties, the person who can approve purchases from the IT department should be different from the person who can input new purchases. |

Cả hai nguyên tắc thường hỗ trợ lẫn nhau. Ví dụ: theo đặc quyền tối thiểu, một người cần có quyền phê duyệt các giao dịch mua hàng từ bộ phận CNTT sẽ không có quyền phê duyệt các giao dịch mua hàng từ mọi bộ phận. Tương tự như vậy, theo sự phân chia nhiệm vụ, người có thể phê duyệt các giao dịch mua hàng từ bộ phận CNTT phải khác với người có thể nhập các giao dịch mua mới.

|  |
| --- |
| In other words, least privilege *limits* *the access* that an individual receives, while separation of duties *divides responsibilities* among multiple people to prevent any one person from having too much control. |

Nói cách khác, đặc quyền tối thiểu *sẽ giới hạn quyền truy cập* mà một cá nhân nhận được, trong khi việc phân chia nhiệm vụ *sẽ phân chia trách nhiệm* giữa nhiều người để ngăn không cho một người nào có quá nhiều quyền kiểm soát.

|  |
| --- |
| **Note:** Separation of duties is sometimes referred to as segregation of duties. |

**Lưu ý:** Sự phân chia nhiệm vụ đôi khi được gọi là sự phân chia nhiệm vụ.

|  |
| --- |
| Previously, you learned about the authentication, authorization, and accounting (AAA) framework. Many businesses used this model to implement these two security principles and manage user access. In this reading, you’ll learn about the other major framework for managing user access,identity and access management(IAM). You will learn about the similarities between AAA and IAM and how they're commonly implemented. |

Trước đây, bạn đã tìm hiểu về khung xác thực, ủy quyền và kế toán (AAA). Nhiều doanh nghiệp đã sử dụng mô hình này để triển khai hai nguyên tắc bảo mật này và quản lý quyền truy cập của người dùng. Trong bài đọc này, bạn sẽ tìm hiểu về khuôn khổ chính khác để quản lý quyền truy cập, danh tính và quản lý quyền truy cập (IAM) của người dùng. Bạn sẽ tìm hiểu về những điểm tương đồng giữa AAA và IAM cũng như cách chúng được triển khai phổ biến.

|  |
| --- |
| **Identity and access management (IAM)** |

**Quản lý danh tính và quyền truy cập (IAM)**

|  |
| --- |
| As organizations become more reliant on technology, regulatory agencies have put more pressure on them to demonstrate that they’re doing everything they can to prevent threats. **Identity and access management** (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. Both AAA and IAM systems are designed to authenticate users, determine their access privileges, and track their activities within a system. |

Khi các tổ chức trở nên phụ thuộc hơn vào công nghệ, các cơ quan quản lý đã gây áp lực nhiều hơn cho họ để chứng minh rằng họ đang làm mọi thứ có thể để ngăn chặn các mối đe dọa. **Quản lý danh tính và quyền truy cập** (IAM) là tập hợp các quy trình và công nghệ giúp các tổ chức quản lý danh tính kỹ thuật số trong môi trường của họ. Cả hệ thống AAA và IAM đều được thiết kế để xác thực người dùng, xác định đặc quyền truy cập của họ và theo dõi hoạt động của họ trong hệ thống.

|  |
| --- |
| Either model used by your organization is more than a single, clearly defined system. They each consist of a collection of security controls that ensure the *right user* is granted access to the *right resources* at the *right time* and for the *right reasons*. Each of those four factors is determined by your organization's policies and processes. |

Mô hình mà tổ chức của bạn sử dụng không chỉ là một hệ thống duy nhất được xác định rõ ràng. Mỗi phần mềm đều bao gồm một tập hợp các biện pháp kiểm soát bảo mật nhằm đảm bảo *đúng người dùng* được cấp quyền truy cập vào *đúng tài nguyên* vào *đúng thời điểm* và vì *lý do chính đáng* . Mỗi yếu tố trong số bốn yếu tố đó được xác định bởi các chính sách và quy trình của tổ chức bạn.

|  |
| --- |
| **Note:** A user can either be a person, a device, or software. |

**Lưu ý:** Người dùng có thể là người, thiết bị hoặc phần mềm.

|  |
| --- |
| **Authenticating users** |

**Xác thực người dùng**

|  |
| --- |
| To ensure the right user is attempting to access a resource requires some form of proof that the user is who they claim to be. In a [video on authentication controls](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/item/r6XuB), you learned that there are a few factors that can be used to authenticate a user:   * **Knowledge**, or something the user knows * **Ownership**, or something the user possesses * **Characteristic**, or something the user is |

Để đảm bảo đúng người dùng đang cố truy cập vào tài nguyên, cần có một số dạng bằng chứng cho thấy người dùng đó chính là người mà họ tuyên bố. trong một[video về kiểm soát xác thực](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/item/r6XuB), bạn đã biết rằng có một số yếu tố có thể được sử dụng để xác thực người dùng:

* **Kiến thức** hoặc điều gì đó mà người dùng biết
* **Quyền sở hữu** hoặc thứ gì đó mà người dùng sở hữu
* **Đặc trưng** hoặc điều gì đó mà người dùng hướng tới

|  |
| --- |
| Authentication is mainly verified with login credentials. **Single sign-on** (SSO), a technology that combines several different logins into one, and **multi-factor authentication** (MFA), a security measure that requires a user to verify their identity in two or more ways to access a system or network, are other tools that organizations use to authenticate individuals and systems. |

Xác thực chủ yếu được xác minh bằng thông tin đăng nhập. **Đăng nhập một lần** (SSO), một công nghệ kết hợp nhiều thông tin đăng nhập khác nhau thành một và **xác thực đa yếu tố** (MFA), một biện pháp bảo mật yêu cầu người dùng xác minh danh tính của họ theo hai hoặc nhiều cách để truy cập hệ thống hoặc mạng, là những công cụ khác mà các tổ chức sử dụng để xác thực các cá nhân và hệ thống.

|  |
| --- |
| **Pro tip:** Another way to remember this authentication model is: something you know, something you have, and something you are. |

**Mẹo chuyên nghiệp:** Một cách khác để ghi nhớ mô hình xác thực này là: điều gì đó bạn biết, điều gì đó bạn có và điều gì đó về bạn.

|  |
| --- |
| **User provisioning** |

**Cung cấp người dùng**

|  |
| --- |
| Back-end systems need to be able to verify whether the information provided by a user is accurate. To accomplish this, users must be properly provisioned. **User provisioning** is the process of creating and maintaining a user's digital identity. For example, a college might create a new user account when a new instructor is hired. The new account will be configured to provide access to instructor-only resources while they are teaching. Security analysts are routinely involved with provisioning users and their access privileges. |

Hệ thống back-end cần có khả năng xác minh xem thông tin do người dùng cung cấp có chính xác hay không. Để thực hiện được điều này, người dùng phải được cung cấp đúng cách. **Cấp phép người dùng** là quá trình tạo và duy trì danh tính kỹ thuật số của người dùng. Ví dụ: một trường đại học có thể tạo một tài khoản người dùng mới khi thuê một người hướng dẫn mới. Tài khoản mới sẽ được định cấu hình để cung cấp quyền truy cập vào các tài nguyên chỉ dành cho người hướng dẫn trong khi họ đang giảng dạy. Các nhà phân tích bảo mật thường xuyên tham gia vào việc cung cấp cho người dùng và các đặc quyền truy cập của họ.

|  |
| --- |
| **Pro tip:** Another role analysts have in IAM is to deprovision users. This is an important practice that removes a user's access rights when they should no longer have them. |

**Mẹo chuyên nghiệp:** Một vai trò khác của nhà phân tích trong IAM là hủy cấp phép cho người dùng. Đây là một phương pháp quan trọng giúp loại bỏ quyền truy cập của người dùng khi lẽ ra họ không còn có các quyền đó nữa.

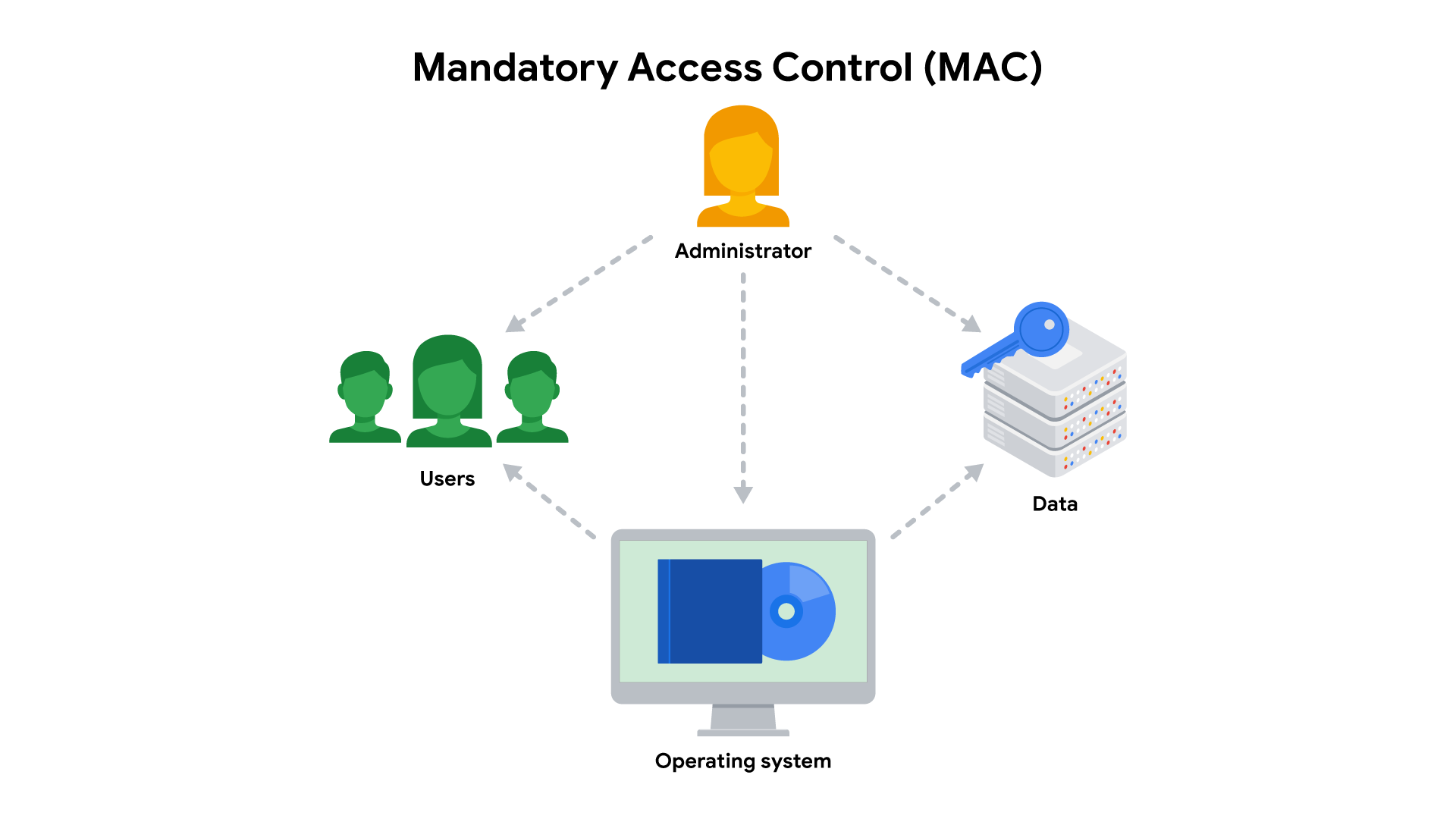
|  |
| --- |
| **Granting authorization** |

**Cấp ủy quyền**

|  |
| --- |
| If the right user has been authenticated, the network should ensure the right resources are made available. There are three common frameworks that organizations use to handle this step of IAM:   * Mandatory access control (MAC) * Discretionary access control (DAC) * Role-based access control (RBAC) |

Nếu đúng người dùng đã được xác thực, mạng phải đảm bảo cung cấp đúng tài nguyên. Có ba khung phổ biến mà các tổ chức sử dụng để xử lý bước này của IAM:

* Kiểm soát truy cập bắt buộc (MAC)
* Kiểm soát truy cập tùy ý (DAC)
* Kiểm soát truy cập dựa trên vai trò (RBAC)

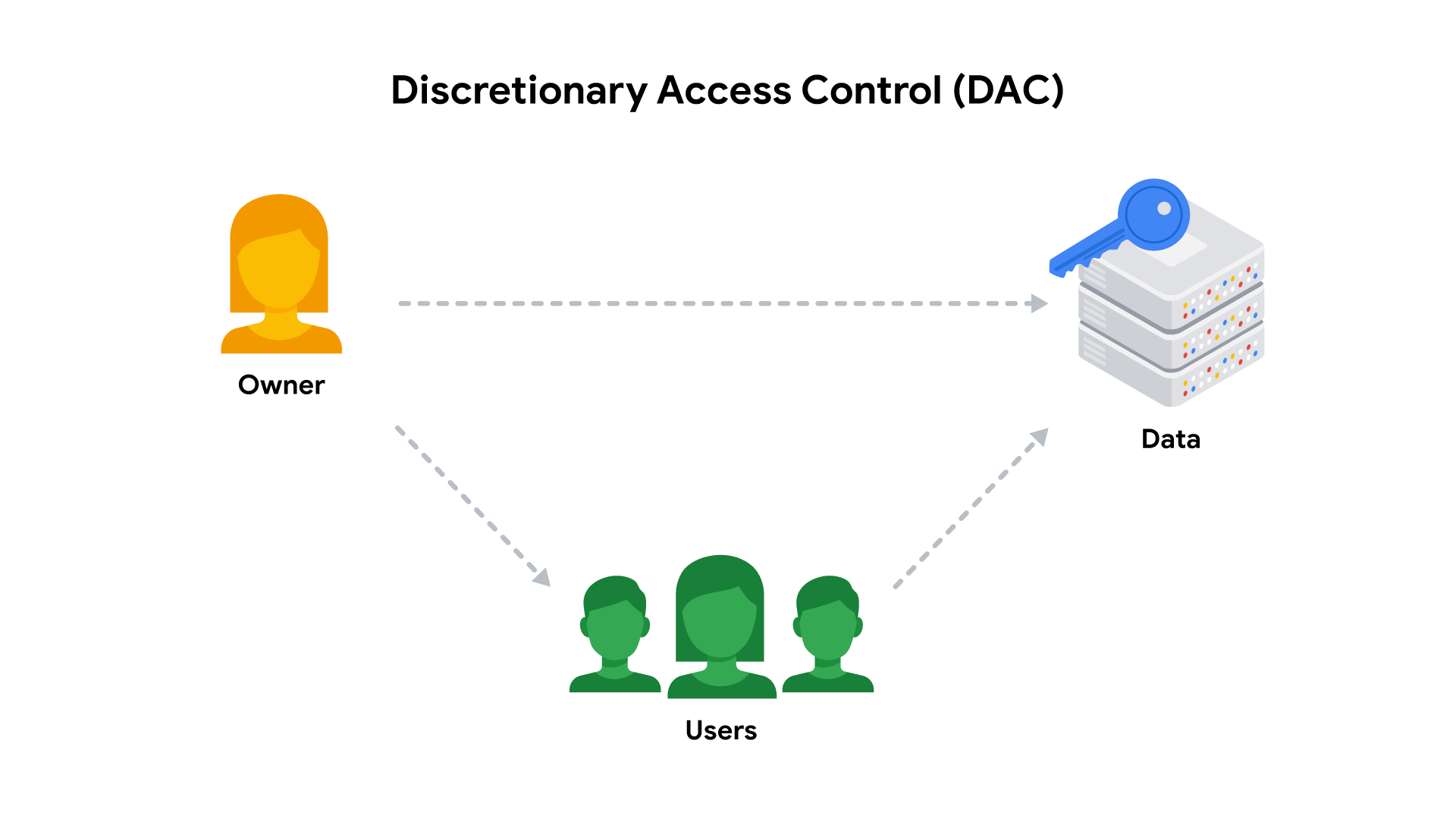


|  |
| --- |
| **Mandatory Access Control (MAC)** |

**Kiểm soát truy cập bắt buộc (MAC)**

|  |
| --- |
| MAC is the strictest of the three frameworks. Authorization in this model is based on a strict need-to-know basis. Access to information must be granted manually by a central authority or system administrator. For example, MAC is commonly applied in law enforcement, military, and other government agencies where users must request access through a chain of command. MAC is also known as non-discretionary control because access isn’t given at the discretion of the data owner. |

MAC là khung nghiêm ngặt nhất trong ba khung. Việc ủy ​​quyền trong mô hình này dựa trên cơ sở cần biết nghiêm ngặt. Quyền truy cập thông tin phải được cấp thủ công bởi cơ quan trung ương hoặc quản trị viên hệ thống. Ví dụ: MAC thường được áp dụng trong cơ quan thực thi pháp luật, quân đội và các cơ quan chính phủ khác, nơi người dùng phải yêu cầu quyền truy cập thông qua chuỗi lệnh. MAC còn được gọi là kiểm soát không tùy ý vì quyền truy cập không được cấp theo quyết định của chủ sở hữu dữ liệu.

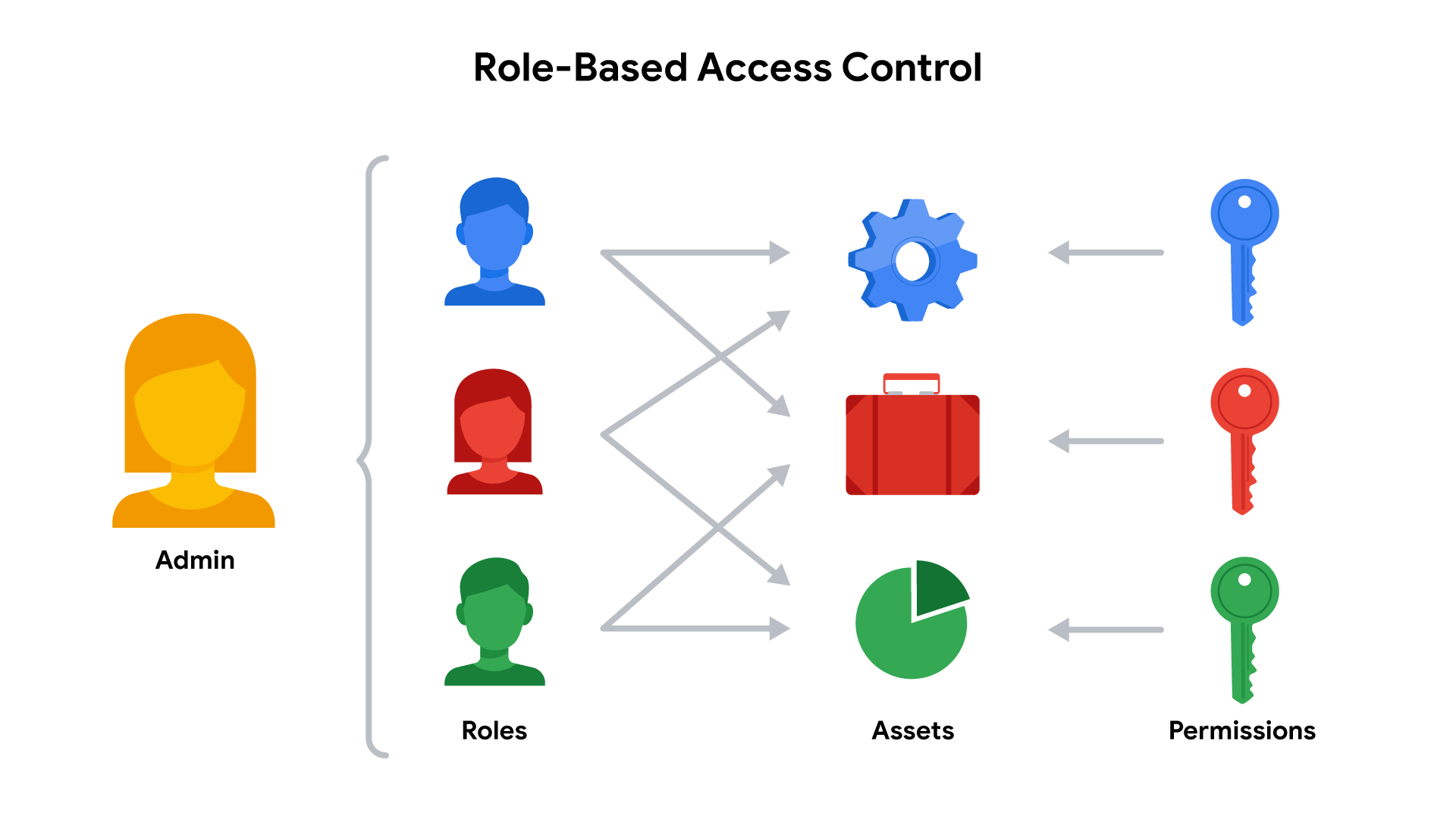


|  |
| --- |
| **Discretionary Access Control (DAC)** |

**Kiểm soát truy cập tùy ý (DAC)**

|  |
| --- |
| DAC is typically applied when a data owner decides appropriate levels of access. One example of DAC is when the owner of a Google Drive folder shares editor, viewer, or commentor access with someone else. |

DAC thường được áp dụng khi chủ sở hữu dữ liệu quyết định mức độ truy cập phù hợp. Một ví dụ về DAC là khi chủ sở hữu thư mục Google Drive chia sẻ quyền truy cập của người chỉnh sửa, người xem hoặc người nhận xét với người khác.



|  |
| --- |
| **Role-Based Access Control (RBAC)** |

**Kiểm soát truy cập dựa trên vai trò (RBAC)**

|  |
| --- |
| RBAC is used when authorization is determined by a user's role within an organization. For example, a user in the marketing department may have access to user analytics but not network administration. |

RBAC được sử dụng khi việc ủy ​​quyền được xác định bởi vai trò của người dùng trong tổ chức. Ví dụ: người dùng trong bộ phận tiếp thị có thể có quyền truy cập vào phân tích người dùng nhưng không có quyền truy cập vào quản trị mạng.

|  |
| --- |
| **Access control technologies** |

**Công nghệ kiểm soát truy cập**

|  |
| --- |
| Users often experience authentication and authorization as a single, seamless experience. In large part, that’s due to access control technologies that are configured to work together. These tools offer the speed and automation needed by administrators to monitor and modify access rights. They also decrease errors and potential risks. |

Người dùng thường trải nghiệm xác thực và ủy quyền như một trải nghiệm liền mạch, duy nhất. Phần lớn, đó là do các công nghệ kiểm soát truy cập được cấu hình để hoạt động cùng nhau. Những công cụ này cung cấp tốc độ và khả năng tự động hóa cần thiết cho quản trị viên để giám sát và sửa đổi quyền truy cập. Chúng cũng làm giảm sai sót và rủi ro tiềm ẩn.

|  |
| --- |
| An organization's IT department sometimes develops and maintains customized access control technologies on their own. A typical IAM or AAA system consists of a user directory, a set of tools for managing data in that directory, an authorization system, and an auditing system. Some organizations create custom systems to tailor them to their security needs. However, building an in-house solution comes at a steep cost of time and other resources. |

Bộ phận CNTT của một tổ chức đôi khi tự mình phát triển và duy trì các công nghệ kiểm soát truy cập tùy chỉnh. Hệ thống IAM hoặc AAA điển hình bao gồm thư mục người dùng, bộ công cụ để quản lý dữ liệu trong thư mục đó, hệ thống ủy quyền và hệ thống kiểm tra. Một số tổ chức tạo ra các hệ thống tùy chỉnh để điều chỉnh chúng theo nhu cầu bảo mật của họ. Tuy nhiên, việc xây dựng một giải pháp nội bộ tốn rất nhiều thời gian và các nguồn lực khác.

|  |
| --- |
| Instead, many organizations opt to license third-party solutions that offer a suite of tools that enable them to quickly secure their information systems. Keep in mind, security is about more than combining a bunch of tools. It’s always important to configure these technologies so they can help to provide a secure environment. |

Thay vào đó, nhiều tổ chức chọn cấp phép cho các giải pháp của bên thứ ba cung cấp bộ công cụ cho phép họ nhanh chóng bảo mật hệ thống thông tin của mình. Hãy nhớ rằng, bảo mật không chỉ đơn thuần là kết hợp nhiều công cụ. Điều quan trọng là phải định cấu hình các công nghệ này để chúng có thể giúp cung cấp một môi trường an toàn.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Controlling access requires a collection of systems and tools. IAM and AAA are common frameworks for implementing least privilege and separation of duties. As a security analyst, you might be responsible for user provisioning and collaborating with other IAM or AAA teams. Having familiarity with these models is valuable for helping organizations achieve their security objectives. They each ensure that the right user is granted access to the right resources at the right time and for the right reasons. |

Kiểm soát quyền truy cập yêu cầu một tập hợp các hệ thống và công cụ. IAM và AAA là các khuôn khổ chung để thực hiện đặc quyền tối thiểu và phân chia nhiệm vụ. Với tư cách là nhà phân tích bảo mật, bạn có thể chịu trách nhiệm cung cấp và cộng tác với người dùng với các nhóm IAM hoặc AAA khác. Việc làm quen với các mô hình này rất có giá trị trong việc giúp các tổ chức đạt được các mục tiêu bảo mật của mình. Mỗi người đều đảm bảo rằng đúng người dùng được cấp quyền truy cập vào đúng tài nguyên vào đúng thời điểm và vì những lý do chính đáng.

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| The identity and access management industry is growing at a rapid pace. As with other domains in security, it’s important to stay informed.   * [IDPro](https://idpro.org/)© is a professional organization dedicated to sharing essential IAM industry knowledge. |

Ngành quản lý danh tính và truy cập đang phát triển với tốc độ nhanh chóng. Cũng như các miền khác trong lĩnh vực bảo mật, điều quan trọng là phải luôn cập nhật thông tin.

* [IDPro](https://idpro.org/)© là một tổ chức chuyên nghiệp chuyên chia sẻ kiến ​​thức thiết yếu về ngành IAM.

***3.7. Activity: Improve authentication, authorization, and accounting for a small business - Hoạt động: Cải thiện xác thực, ủy quyền và kế toán cho một doanh nghiệp nhỏ***

|  |
| --- |
| **Activity Overview**  In this activity, you will assess the access controls used by a business. You’ll analyze their current process, identify issues, and make recommendations to improve their security practices.  Previously, you learned that **access controls** are security controls that manage access, authorization, and accountability of information. Authentication controls are used to verify who someone is, whereas authorization controls are used to grant a user permissions and set limits on the things they’re allowed to do. When done well, access controls are the key to decreasing the likelihood of a security risk.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ đánh giá các biện pháp kiểm soát truy cập được doanh nghiệp sử dụng. Bạn sẽ phân tích quy trình hiện tại của họ, xác định các vấn đề và đưa ra đề xuất để cải thiện các biện pháp bảo mật của họ.

Trước đây, bạn đã biết rằng **kiểm soát truy cập** là các biện pháp kiểm soát bảo mật giúp quản lý quyền truy cập, ủy quyền và trách nhiệm giải trình đối với thông tin. Kiểm soát xác thực được sử dụng để xác minh ai đó là ai, trong khi kiểm soát ủy quyền được sử dụng để cấp quyền cho người dùng và đặt giới hạn cho những việc họ được phép làm. Khi được thực hiện tốt, kiểm soát truy cập là chìa khóa để giảm khả năng xảy ra rủi ro bảo mật.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the scenario below. Then complete the step-by-step instructions.  You’re the first cybersecurity professional hired by a growing business.  Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn’t make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.  To do this, you’ll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs. |

**Kịch bản**

Xem lại kịch bản dưới đây. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn là chuyên gia an ninh mạng đầu tiên được một doanh nghiệp đang phát triển thuê.

Gần đây, doanh nghiệp đã gửi một khoản tiền gửi vào một tài khoản ngân hàng không xác định. Người quản lý tài chính nói rằng họ không phạm sai lầm. May mắn thay, họ đã có thể ngừng thanh toán. Chủ sở hữu đã yêu cầu bạn điều tra những gì đã xảy ra để ngăn chặn bất kỳ sự cố nào trong tương lai.

Để làm được điều này, bạn cần phải tính toán một số sự việc để hiểu rõ hơn chuyện gì đã xảy ra. Đầu tiên, bạn sẽ xem lại nhật ký truy cập của vụ việc. Tiếp theo, bạn sẽ ghi chú có thể giúp bạn xác định tác nhân đe dọa có thể xảy ra. Sau đó, bạn sẽ phát hiện các vấn đề với các biện pháp kiểm soát truy cập đã bị người dùng khai thác. Cuối cùng, bạn sẽ đề xuất các biện pháp giảm thiểu có thể cải thiện khả năng kiểm soát quyền truy cập của doanh nghiệp và giảm khả năng sự cố này tái diễn.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

Thực hiện theo hướng dẫn và trả lời câu hỏi bên dưới để hoàn thành hoạt động. Sau đó, chuyển sang mục khóa học tiếp theo để so sánh bài tập của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the link below and select *Use Template*.  Link to template: [Access control worksheet](https://docs.google.com/document/d/1Uhz4yTKO_tB5i1SS8OX9VTrc8pX6A9xE6__OwOAHUhs/template/preview?resourcekey=0-SzdtvOMbRvB1b-VD6d0Sog#heading=h.7nlk2ynsm6vx) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn *Sử dụng Mẫu* .

Liên kết đến mẫu:[Bảng tính kiểm soát truy cập](https://docs.google.com/document/d/1Uhz4yTKO_tB5i1SS8OX9VTrc8pX6A9xE6__OwOAHUhs/template/preview?resourcekey=0-SzdtvOMbRvB1b-VD6d0Sog#heading=h.7nlk2ynsm6vx)

|  |
| --- |
| **Step 2: Access supporting materials**  The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.  To use the supporting materials for this course item, click the link below and select “Use Template.”  **Note:** The spreadsheet for this supporting resource has two tabs.  Link to template: [Accounting exercise](https://docs.google.com/spreadsheets/d/1-WuEnbCzejBOR5833otgbkeolkxjvhG5qDTKMuKkyYo/template/preview?resourcekey=0-5JZRiXznziLl1teGdlyMEg#gid=253432744) |

**Bước 2: Truy cập tài liệu hỗ trợ**

Các tài liệu hỗ trợ sau đây sẽ giúp bạn hoàn thành hoạt động này. Giữ chúng mở khi bạn tiến hành các bước tiếp theo.

Để sử dụng các tài liệu hỗ trợ cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn “Sử dụng mẫu”.

**Lưu ý:** Bảng tính cho tài nguyên hỗ trợ này có hai tab.

Liên kết đến mẫu:[Bài tập kế toán](https://docs.google.com/spreadsheets/d/1-WuEnbCzejBOR5833otgbkeolkxjvhG5qDTKMuKkyYo/template/preview?resourcekey=0-5JZRiXznziLl1teGdlyMEg#gid=253432744)

|  |
| --- |
| **Step 3: Review the event log of this payroll incident**  Event logs contain information related to the operation and usage of a system. They can be utilized to identify suspicious activity, detect vulnerabilities, and track users.  Find the **Event log** tab of the *Accounting exercise* spreadsheet. Carefully review the event log of this incident to start your investigation. Notice the *Event Type*, *Date*, *Time*, and *IP Address* of the user in the log details.  Make **1-2 notes** of information that you learned about the user from reviewing the *Event log* details. Add your notes to the **Notes** column of the access control worksheet. |

**Bước 3: Xem lại nhật ký sự kiện của sự cố bảng lương này**

Nhật ký sự kiện chứa thông tin liên quan đến hoạt động và cách sử dụng hệ thống. Chúng có thể được sử dụng để xác định hoạt động đáng ngờ, phát hiện lỗ hổng và theo dõi người dùng.

Tìm tab **Nhật ký sự kiện** của bảng tính *bài tập Kế toán* . Hãy xem xét cẩn thận nhật ký sự kiện của sự cố này để bắt đầu điều tra. Lưu ý *Loại sự kiện* , *Ngày* , *Giờ* và *Địa chỉ IP* của người dùng trong chi tiết nhật ký.

Ghi lại **1-2** thông tin mà bạn đã biết về người dùng khi xem lại chi tiết *Nhật ký sự kiện* . Thêm ghi chú của bạn vào cột **Ghi chú** của bảng tính kiểm soát truy cập.

|  |
| --- |
| **Step 4: Identify access control issues that led to the incident**  Log details tell you a lot about a specific moment in time. You can find other useful details about an event by cross referencing that information with other sources.  This business has a range of different employees. They all currently manage company resources using a shared cloud drive.  Find the **Employee directory** tab of the *Accounting exercise* spreadsheet. Compare the information found in the *Employee directory* tab with the information in the *Event log* tab. Notice any similarities between the details in the *Event log* and the details in the *Employee directory*.  Then, list **1-2** issues that you discover with how the business handles employee access in the **Issues** column of the *Access control worksheet*. |

**Bước 4: Xác định các vấn đề kiểm soát truy cập dẫn đến sự cố**

Chi tiết nhật ký cho bạn biết rất nhiều về một thời điểm cụ thể. Bạn có thể tìm thấy những thông tin chi tiết hữu ích khác về một sự kiện bằng cách tham khảo chéo thông tin đó với các nguồn khác.

Doanh nghiệp này có nhiều nhân viên khác nhau. Tất cả họ hiện đang quản lý tài nguyên của công ty bằng ổ đĩa đám mây dùng chung.

Tìm tab **thư mục Nhân viên** của bảng tính *bài tập Kế toán* . So sánh thông tin tìm thấy trong tab *thư mục Nhân viên* với thông tin trong tab *Nhật ký sự kiện* . Lưu ý bất kỳ điểm tương đồng nào giữa các chi tiết trong *Nhật ký sự kiện* và các chi tiết trong *thư mục Nhân viên* .

Sau đó, liệt kê **1-2** vấn đề mà bạn phát hiện ra về cách doanh nghiệp xử lý quyền truy cập của nhân viên trong cột **Vấn đề** của *bảng tính Kiểm soát quyền truy cập* .

|  |
| --- |
| **Step 5: Recommend mitigations that can prevent a future breach**  You’ve completed your accounting of the strange payment and discovered flaws with how the business handles their information.  Find the **Recommendation(s)** column of the *Access control worksheet*. Make **at least 2** recommendations of mitigations the business can implement to prevent incidents like this in the future.  For example, one recommendation might be to have procedures in place to revoke access to files when an employee is no longer with the company. |

**Bước 5: Đề xuất các biện pháp giảm thiểu có thể ngăn chặn vi phạm trong tương lai**

Bạn đã hoàn thành việc hạch toán khoản thanh toán lạ và phát hiện ra sai sót trong cách doanh nghiệp xử lý thông tin của họ.

Tìm cột **Khuyến nghị** của *bảng tính Kiểm soát truy cập* . Đưa ra **ít nhất 2** khuyến nghị về các biện pháp giảm thiểu mà doanh nghiệp có thể thực hiện để ngăn chặn những sự cố như thế này trong tương lai.

Ví dụ: một khuyến nghị có thể là áp dụng các quy trình để thu hồi quyền truy cập vào các tệp khi nhân viên không còn ở công ty nữa.

|  |
| --- |
| **What to Include in Your Response**  Be sure to include the following elements in your completed activity:   * 1-2 notes about the user * 1-2 access control issues * 2 recommendations for access control mitigations |

**Những gì cần bao gồm trong phản hồi của bạn**

Hãy đảm bảo bao gồm các yếu tố sau trong hoạt động đã hoàn thành của bạn:

* 1-2 lưu ý về người dùng
* 1-2 vấn đề kiểm soát truy cập
* 2 khuyến nghị để giảm thiểu kiểm soát truy cập

***3.8. Activity Exemplar: Improve authentication and authorization for a small business - Ví dụ về hoạt động: Cải thiện xác thực và ủy quyền cho một doanh nghiệp nhỏ***

|  |
| --- |
| **Activity Exemplar: Improve authentication and authorization for a small business**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Ví dụ về hoạt động: Cải thiện xác thực và ủy quyền cho một doanh nghiệp nhỏ**

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link below and select *Use Template*.  Link to exemplar: [Access control worksheet exemplar](https://docs.google.com/document/d/1_jyynRjMBkeKW70f3P9EV9BAi7Wd1eoNYu01OyLtBkw/template/preview) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Mẫu bảng tính kiểm soát truy cập](https://docs.google.com/document/d/1_jyynRjMBkeKW70f3P9EV9BAi7Wd1eoNYu01OyLtBkw/template/preview)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed asset inventory. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course. |

**Đánh giá mẫu mực**

So sánh mẫu với bản kiểm kê tài sản đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong suốt khóa học.

|  |
| --- |
| ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your review of the security incident considers effective access controls that can be implemented and how a lack of controls can put information at risk.* |

***Lưu ý:*** *Ví dụ thể hiện một cách khả thi để hoàn thành hoạt động. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là việc đánh giá của bạn về sự cố bảo mật sẽ xem xét các biện pháp kiểm soát truy cập hiệu quả có thể được triển khai và việc thiếu các biện pháp kiểm soát có thể khiến thông tin gặp rủi ro như thế nào.*

|  |
| --- |
| Let's review the details of the completed access control worksheet: |

Hãy xem lại chi tiết của bảng tính kiểm soát truy cập đã hoàn thành:

|  |
| --- |
| **Note(s) about the user:**   * The event took place on 10/03/23. * The user is Legal/Administrator. * The IP address of the computer used to login is 152.207.255.255.   Event logs can often help you identify the who, what, and why of a security incident. |

**(Các) lưu ý về người dùng:**

* Sự việc diễn ra vào ngày 23/10.
* Người dùng là Pháp lý/Quản trị viên.
* Địa chỉ IP của máy tính dùng để đăng nhập là 152.207.255.255.

Nhật ký sự kiện thường có thể giúp bạn xác định ai, cái gì và tại sao xảy ra sự cố bảo mật.

|  |
| --- |
| **Access control issue(s):**   * Robert Taylor, Jr. is  a contractor with admin access. * His contract ended in 2019, but his account accessed payroll systems in 2023.   Oftentimes, incidents like this occur because systems are misconfigured or misused. That is the case with how this business is sharing information among its employees. |

**(Các) vấn đề kiểm soát truy cập:**

* Robert Taylor, Jr. là một nhà thầu có quyền truy cập quản trị viên.
* Hợp đồng của anh ấy kết thúc vào năm 2019, nhưng tài khoản của anh ấy đã truy cập vào hệ thống trả lương vào năm 2023.

Thông thường, những sự cố như thế này xảy ra do hệ thống bị định cấu hình sai hoặc bị sử dụng sai mục đích. Đó là trường hợp doanh nghiệp này chia sẻ thông tin giữa các nhân viên của mình.

|  |
| --- |
| **Recommendations:**   * User accounts should expire after 30 days. * Contractors should have limited access to business resources. * Enable multi-factor authentication (MFA).   It appears as though a former employee is potentially the threat actor. However, it's possible that they were not the person responsible for this security incident. |

**Khuyến nghị:**

* Tài khoản người dùng sẽ hết hạn sau 30 ngày.
* Các nhà thầu nên có quyền truy cập hạn chế vào các nguồn lực kinh doanh.
* Kích hoạt xác thực đa yếu tố (MFA).

Có vẻ như một nhân viên cũ có khả năng là tác nhân đe dọa. Tuy nhiên, có thể họ không phải là người chịu trách nhiệm về sự cố an ninh này.

|  |
| --- |
| It is common for people to reuse login credentials across many services. And if those credentials are compromised on one platform then an attacker can use them to gain access to others. In this case, implementing access controls, like password policies, limited file permissions, and MFA can protect the business from incidents like this. |

Mọi người thường sử dụng lại thông tin đăng nhập trên nhiều dịch vụ. Và nếu những thông tin xác thực đó bị xâm phạm trên một nền tảng thì kẻ tấn công có thể sử dụng chúng để giành quyền truy cập vào những nền tảng khác. Trong trường hợp này, việc triển khai các biện pháp kiểm soát quyền truy cập, như chính sách mật khẩu, quyền hạn chế đối với tệp và MFA có thể bảo vệ doanh nghiệp khỏi những sự cố như thế này.

|  |
| --- |
| **Key Takeaways** |

**Bài học chính**

|  |
| --- |
| This activity highlights how easy it can be to lose track of users, which  can leave a business open to unnecessary risk if effective access controls are not in place. The activity also demonstrates the risk of operating a business with open, shared access to resources. Setting boundaries around who can access information and what they are allowed to do should be the starting point of any security plan. |

Hoạt động này nêu bật việc mất dấu người dùng dễ dàng như thế nào, điều này có thể khiến doanh nghiệp gặp phải rủi ro không đáng có nếu không áp dụng các biện pháp kiểm soát quyền truy cập hiệu quả. Hoạt động này cũng thể hiện rủi ro khi điều hành một doanh nghiệp với quyền truy cập mở, chia sẻ vào các nguồn tài nguyên. Việc đặt ra ranh giới xung quanh việc ai có thể truy cập thông tin và những gì họ được phép làm phải là điểm khởi đầu của bất kỳ kế hoạch bảo mật nào.

***3.9. Test your knowledge: Authentication, authorization, and accounting - Kiểm tra kiến ​​thức của bạn: Xác thực, ủy quyền và kế toán***

**4. Review: Protect organizational assets - Đánh giá: Bảo vệ tài sản của tổ chức**

***4.1. Wrap-up – Tóm tắt***

|  |
| --- |
| Our focus in this section was on a major theme of security: protecting assets. A large part of this relates to privacy. We should all enjoy the right to decide who can access our information. As we learned, there are several controls in place that help secure assets. |

Trọng tâm của chúng tôi trong phần này là về chủ đề chính về bảo mật: bảo vệ tài sản.Một phần lớn trong số này liên quan đến quyền riêng tư.Tất cả chúng ta đều có quyền quyết định ai có thể truy cập thông tin của chúng ta.Như chúng ta đã tìm hiểu, có một số biện pháp kiểm soát giúp bảo đảm tài sản.

|  |
| --- |
| We began the section by exploring effective data handling processes that are founded on the principle of least privilege. We then explored the role of encryption and hashing and safeguarding information. We explored how symmetric and asymmetric encryption works and how hashes further safeguard data from harm. |

Chúng tôi bắt đầu phần này bằng cách khám phá các quy trình xử lý dữ liệu hiệu quảđược thành lập trên nguyên tắc đặc quyền tối thiểu.Sau đó, chúng tôi khám phá vai trò của mã hóa, băm và bảo vệ thông tin.Chúng tôi đã khám phá cách mã hóa đối xứng và bất đối xứng hoạt động vàcách băm bảo vệ dữ liệu khỏi bị tổn hại hơn nữa.

|  |
| --- |
| We then turned our attention to standard access controls. Properly authenticating and authorizing users is what maintaining the CIA triad of information is all about! |

Sau đó, chúng tôi chuyển sự chú ý sang các biện pháp kiểm soát truy cập tiêu chuẩn. Xác thực đúng cáchvà việc ủy ​​quyền cho người dùng chính là mục đích duy trì bộ ba thông tin của CIA!

|  |
| --- |
| We used the AAA framework of security to take a detailed tour of identity and access management systems and the access controls that validate whether or not someone is who they claim to be. |

Chúng tôi đã sử dụng khung bảo mật AAA để tìm hiểu chi tiết về danh tính vàhệ thống quản lý truy cập và các biện pháp kiểm soát truy cập để xác nhận xem cóai đó chính là người mà họ tuyên bố.

|  |
| --- |
| Well done making it through the first half of the course! You're making great progress so far, and I hope you keep it up. Remember, your background and experiences are valuable in this field. This combined with the concepts we're covering will make you a valuable contributor to any security team. |

Bạn đã hoàn thành xuất sắc việc vượt qua nửa đầu của khóa học!Cho đến nay, bạn đang tiến bộ rất nhiều và tôi hy vọng bạn sẽ tiếp tục duy trì điều đó.Hãy nhớ rằng nền tảng và kinh nghiệm của bạn rất có giá trị trong lĩnh vực này.Điều này kết hợp với các khái niệm chúng tôi đang đề cập sẽ giúp bạnmột người đóng góp có giá trị cho bất kỳ nhóm bảo mật nào.

|  |
| --- |
| Up until this point, we've been exploring the defensive side of security, but security isn't all about planning ahead and waiting for something to happen. In the next part of our journey, we're going to continue developing a security mindset by taking a more proactive look at security from the perspective of attackers. I'll meet you there! |

Cho đến thời điểm này, chúng ta đã khám phá khía cạnh phòng thủ của an ninh, nhưngbảo mật không chỉ là lập kế hoạch trước và chờ đợi điều gì đó xảy ra.Trong phần tiếp theo của cuộc hành trình của chúng tôi,chúng tôi sẽ tiếp tục phát triển tư duy bảo mật bằng cách thực hiện nhiều hơnchủ động xem xét vấn đề bảo mật từ góc độ của những kẻ tấn công.Tôi sẽ gặp bạn ở đó!

***4.2. Glossary terms from module 2 - Thuật ngữ trong học phần 2***

|  |
| --- |
| **Glossary terms from module 2** |

**Thuật ngữ trong học phần 2**

|  |
| --- |
| **Terms and definitions from Course 5, Module 2** |

**Các thuật ngữ và định nghĩa trong Khóa 5, Học phần 2**

|  |
| --- |
| **Access controls:** Security controls that manage access, authorization, and accountability of information |

**Kiểm soát truy cập:** Kiểm soát bảo mật quản lý quyền truy cập, ủy quyền và trách nhiệm giải trình thông tin

|  |
| --- |
| **Algorithm:** A set of rules used to solve a problem |

**Thuật toán:** Một tập hợp các quy tắc được sử dụng để giải quyết vấn đề

|  |
| --- |
| **Application programming interface (API) token:** A small block of encrypted code that contains information about a user |

**Mã thông báo giao diện lập trình ứng dụng (API):** Một khối mã nhỏ được mã hóa chứa thông tin về người dùng

|  |
| --- |
| **Asymmetric encryption:** The use of a public and private key pair for encryption and decryption of data |

**Mã hóa bất đối xứng:** Việc sử dụng cặp khóa chung và khóa riêng để mã hóa và giải mã dữ liệu

|  |
| --- |
| **Basic auth:** The technology used to establish a user’s request to access a server |

**Xác thực cơ bản:** Công nghệ được sử dụng để thiết lập yêu cầu truy cập máy chủ của người dùng

|  |
| --- |
| **Bit:** The smallest unit of data measurement on a computer |

**Bit:** Đơn vị đo lường dữ liệu nhỏ nhất trên máy tính

|  |
| --- |
| **Brute force attack:** The trial and error process of discovering private information |

**Tấn công Brute Force:** Quá trình thử và sai để khám phá thông tin cá nhân

|  |
| --- |
| **Cipher:** An algorithm that encrypts information |

**Cipher:** Thuật toán mã hóa thông tin

|  |
| --- |
| **Cryptographic key:** A mechanism that decrypts ciphertext |

**Khóa mật mã:** Cơ chế giải mã bản mã

|  |
| --- |
| **Cryptography:** The process of transforming information into a form that unintended readers can’t understand |

**Mật mã học:** Quá trình chuyển đổi thông tin thành dạng mà người đọc ngoài ý muốn không thể hiểu được

|  |
| --- |
| **Data custodian:** Anyone or anything that’s responsible for the safe handling, transport, and storage of information |

**Người giám sát dữ liệu:** Bất kỳ ai hoặc bất kỳ thứ gì chịu trách nhiệm xử lý, vận chuyển và lưu trữ thông tin một cách an toàn

|  |
| --- |
| **Data owner:** The person that decides who can access, edit, use, or destroy their information |

**Chủ sở hữu dữ liệu:** Người quyết định ai có thể truy cập, chỉnh sửa, sử dụng hoặc hủy thông tin của họ

|  |
| --- |
| **Digital certificate:** A file that verifies the identity of a public key holder |

**Chứng chỉ số:** Tệp xác minh danh tính của người giữ khóa công khai

|  |
| --- |
| **Encryption:** The process of converting data from a readable format to an encoded format |

**Mã hóa:** Quá trình chuyển đổi dữ liệu từ định dạng có thể đọc được sang định dạng được mã hóa

|  |
| --- |
| **Hash collision:** An instance when different inputs produce the same hash value |

**Xung đột băm:** Một trường hợp khi các đầu vào khác nhau tạo ra cùng một giá trị băm

|  |
| --- |
| **Hash function:** An algorithm that produces a code that can’t be decrypted |

**Hàm băm:** Thuật toán tạo ra mã không thể giải mã được

|  |
| --- |
| **Hash table:** A data structure that's used to store and reference hash values |

**Bảng băm:** Cấu trúc dữ liệu được sử dụng để lưu trữ và tham chiếu các giá trị băm

|  |
| --- |
| **Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment |

**Quản lý danh tính và quyền truy cập (IAM):** Tập hợp các quy trình và công nghệ giúp các tổ chức quản lý danh tính kỹ thuật số trong môi trường của họ

|  |
| --- |
| **Information privacy:** The protection of unauthorized access and distribution of data |

**Bảo mật thông tin:** Việc bảo vệ truy cập và phân phối dữ liệu trái phép

|  |
| --- |
| **Multi-factor authentication (MFA):** A security measure that requires a user to verify their identity in two or more ways to access a system or network |

**Xác thực đa yếu tố (MFA):** Một biện pháp bảo mật yêu cầu người dùng xác minh danh tính của họ theo hai cách trở lên để truy cập hệ thống hoặc mạng

|  |
| --- |
| **Non-repudiation:** The concept that the authenticity of information can’t be denied |

**Chống chối bỏ:** Khái niệm về tính xác thực của thông tin không thể bị từ chối

|  |
| --- |
| **OAuth:** An open-standard authorization protocol that shares designated access between applications |

**OAuth:** Giao thức ủy quyền tiêu chuẩn mở chia sẻ quyền truy cập được chỉ định giữa các ứng dụng

|  |
| --- |
| **Payment Card Industry Data Security Standards (PCI DSS):** A set of security standards formed by major organizations in the financial industry |

**Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS):** Một bộ tiêu chuẩn bảo mật được hình thành bởi các tổ chức lớn trong ngành tài chính

|  |
| --- |
| **Personally identifiable information (PII):** Any information used to infer an individual's identity |

**Thông tin nhận dạng cá nhân (PII):** Bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân

|  |
| --- |
| **Principle of least privilege:** The concept of granting only the minimal access and authorization required to complete a task or function |

**Nguyên tắc đặc quyền tối thiểu:** Khái niệm chỉ cấp quyền truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ hoặc chức năng

|  |
| --- |
| **Protected health information (PHI):** Information that relates to the past, present, or future physical or mental health or condition of an individual |

**Thông tin sức khỏe được bảo vệ (PHI):** Thông tin liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân

|  |
| --- |
| **Public key infrastructure (PKI):** An encryption framework that secures the exchange of online information |

**Cơ sở hạ tầng khóa công khai (PKI):** Khung mã hóa đảm bảo việc trao đổi thông tin trực tuyến

|  |
| --- |
| **Rainbow table:** A file of pre-generated hash values and their associated plaintext |

**Bảng cầu vồng:** Một tệp chứa các giá trị băm được tạo trước và văn bản gốc liên quan của chúng

|  |
| --- |
| **Salting:** An additional safeguard that’s used to strengthen hash functions |

**Salting:** Một biện pháp bảo vệ bổ sung được sử dụng để tăng cường chức năng băm

|  |
| --- |
| **Security assessment:** A check to determine how resilient current security implementations are against threats |

**Đánh giá bảo mật:** Kiểm tra để xác định mức độ linh hoạt của việc triển khai bảo mật hiện tại trước các mối đe dọa

|  |
| --- |
| **Security audit:** A review of an organization's security controls, policies, and procedures against a set of expectations |

**Kiểm toán bảo mật:** Đánh giá các biện pháp kiểm soát, chính sách và quy trình bảo mật của tổ chức so với một loạt các kỳ vọng

|  |
| --- |
| **Security controls:** Safeguards designed to reduce specific security risks |

**Kiểm soát bảo mật:** Các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể

|  |
| --- |
| **Separation of duties:** The principle that users should not be given levels of authorization that would allow them to misuse a system |

**Phân chia nhiệm vụ:** Nguyên tắc người dùng không được cấp các cấp độ ủy quyền cho phép họ lạm dụng hệ thống

|  |
| --- |
| **Session:** A sequence of network HTTP basic auth requests and responses associated with the same user |

**Phiên:** Một chuỗi các yêu cầu và phản hồi xác thực cơ bản HTTP mạng được liên kết với cùng một người dùng

|  |
| --- |
| **Session cookie:** A token that websites use to validate a session and determine how long that session should last |

**Cookie phiên:** Mã thông báo mà các trang web sử dụng để xác thực phiên và xác định phiên đó sẽ kéo dài bao lâu

|  |
| --- |
| **Session hijacking:** An event when attackers obtain a legitimate user’s session ID |

**Chiếm quyền điều khiển phiên:** Một sự kiện khi kẻ tấn công lấy được ID phiên của người dùng hợp pháp

|  |
| --- |
| **Session ID:** A unique token that identifies a user and their device while accessing a system |

**ID phiên:** Mã thông báo duy nhất xác định người dùng và thiết bị của họ khi truy cập hệ thống

|  |
| --- |
| **Single Sign-On (SSO):** A technology that combines several different logins into one |

**Đăng nhập một lần (SSO):** Công nghệ kết hợp nhiều thông tin đăng nhập khác nhau thành một

|  |
| --- |
| **Symmetric encryption:** The use of a single secret key to exchange information |

**Mã hóa đối xứng:** Việc sử dụng một khóa bí mật duy nhất để trao đổi thông tin

|  |
| --- |
| **User provisioning:** The process of creating and maintaining a user's digital identity |

**Cung cấp người dùng:** Quá trình tạo và duy trì danh tính kỹ thuật số của người dùng

***4.3. Module 2 challenge - Thử thách mô-đun***

# **Module 3: Vulnerabilities in systems - Lỗ hổng trong hệ thống**

|  |
| --- |
| You will build an understanding of the vulnerability management process. You'll learn about common vulnerabilities and develop an attacker mindset by examining the ways vulnerabilities can become threats to asset security if they are exploited. |

Bạn sẽ xây dựng sự hiểu biết về quy trình quản lý lỗ hổng. Bạn sẽ tìm hiểu về các lỗ hổng phổ biến và phát triển tư duy của kẻ tấn công bằng cách kiểm tra cách các lỗ hổng có thể trở thành mối đe dọa đối với an ninh tài sản nếu chúng bị khai thác.

|  |
| --- |
| **Learning Objectives**   * Differentiate between vulnerabilities and threats. * Describe the defense in depth strategy. * Explain how common vulnerability exposures are identified by MITRE. * Explain how vulnerability assessments are used to assess potential risk. * Analyze an attack surface. * Develop an attacker mindset to recognize threats. |

**Mục tiêu học tập**

* Phân biệt giữa lỗ hổng và mối đe dọa.
* Mô tả chiến lược phòng thủ theo chiều sâu.
* Giải thích cách MITER xác định mức độ phơi nhiễm lỗ hổng phổ biến.
* Giải thích cách sử dụng đánh giá lỗ hổng để đánh giá rủi ro tiềm ẩn.
* Phân tích bề mặt tấn công
* Phát triển tư duy của kẻ tấn công để nhận ra các mối đe dọa.

**1. Flaws in the system - Những sai sót trong hệ thống**

***1.1. Welcome to module 3 - Chào mừng đến với mô-đun 3***

|  |
| --- |
| Wow! We've covered a lot together! It's hard to believe we've reached the midpoint of this course. I hope you're getting a clearer picture of this exciting field and all the opportunities it has to offer. And most importantly, I hope you're having fun doing it. |

Ồ! Chúng ta đã cùng nhau che đậy rất nhiều điều!Thật khó để tin rằng chúng ta đã đạt đến điểm giữa của khóa học này.Tôi hy vọng bạn sẽ có được bức tranh rõ ràng hơn về lĩnh vực thú vị này vàtất cả những cơ hội mà nó mang lại.Và quan trọng nhất, tôi hy vọng bạn thấy vui khi làm việc đó.

|  |
| --- |
| We've come a long ways from where we started. When we began our journey together, we were introduced to the three building blocks of every security program: assets, threats, and vulnerabilities. We focused a lot on assets early on and the wide range of things security professionals work to protect. |

Chúng ta đã đi được một chặng đường dài từ nơi chúng ta bắt đầu.Khi chúng tôi bắt đầu cuộc hành trình cùng nhau, chúng tôi được giới thiệu về ba tòa nhà.các khối của mọi chương trình bảo mật: tài sản, mối đe dọa và lỗ hổng.Chúng tôi đã sớm tập trung rất nhiều vào tài sảnvà rất nhiều thứ mà các chuyên gia bảo mật nỗ lực bảo vệ.

|  |
| --- |
| We then turned our attention to a core component of asset security, protecting assets. You learned about the importance of guarding sensitive information. You also learned about some security controls that protect information from being lost or stolen. |

Sau đó chúng tôi chuyển sự chú ý sang thành phần cốt lõi của bảo mật tài sản,bảo vệ tài sản.Bạn đã biết về tầm quan trọng của việc bảo vệ thông tin nhạy cảm.Bạn cũng đã tìm hiểu về một số biện pháp kiểm soát bảo mật nhằm bảo vệ thông tin khỏibị mất hoặc bị đánh cắp.

|  |
| --- |
| On the next part of our journey, we're going to turn our focus to vulnerabilities. Every asset we protect has a series of vulnerabilities, or flaws, that we need to be aware of. Staying informed of these things is a critical part of protecting people and organizations from harm. |

Ở phần tiếp theo của cuộc hành trình,chúng ta sẽ chuyển trọng tâm sang các lỗ hổng.Mọi tài sản chúng tôi bảo vệ đều có một loạt lỗ hổng hoặc sai sót,mà chúng ta cần phải nhận thức được.Luôn cập nhật thông tin về những điều này là một phần quan trọng trong việc bảo vệ con người vàtổ chức khỏi bị tổn hại.

|  |
| --- |
| In this next part of the course, you'll gain an understanding of the vulnerability management process. First, you'll explore a common approach to vulnerability management: the defense and depth model. Then, you will learn about how vulnerabilities are documented in online libraries like the CVE list. We'll discuss the attack surfaces security teams protect. And lastly, you'll expand your attacker mindset by exploring the common attack vectors cybercriminals try to exploit. |

Trong phần tiếp theo của khóa học này,bạn sẽ hiểu được quy trình quản lý lỗ hổng.Trước tiên, bạn sẽ khám phá một cách tiếp cận chung để quản lý lỗ hổng:mô hình phòng thủ và chiều sâuSau đó, bạn sẽ tìm hiểu về cách các lỗ hổng được ghi lại trongthư viện trực tuyến như danh sách CVE.Chúng ta sẽ thảo luận về các bề mặt tấn công mà đội an ninh bảo vệ.Và cuối cùng, bạn sẽ mở rộng tư duy tấn công của mình bằng cách khám phá các cuộc tấn công thông thườngvectơ mà tội phạm mạng cố gắng khai thác.

|  |
| --- |
| Security analysts play an important role in identifying and correcting vulnerabilities in systems. I know I'm excited to keep exploring, are you? Then let's go! |

Các nhà phân tích chứng khoán đóng một vai trò quan trọng trong việc xác định vàkhắc phục các lỗ hổng trong hệ thống.Tôi biết tôi rất hào hứng khi tiếp tục khám phá,Bạn có phải?Đi thôi nào!

***1.2. Vulnerability management - Quản lý lỗ hổng***

|  |
| --- |
| For every asset that needs protecting, there are dozens of vulnerabilities. Finding those vulnerabilities and fixing them before they become a problem is the key to keep an asset safe. |

Đối với mọi tài sản cần bảo vệ đều có hàng tá lỗ hổng.Việc tìm ra những lỗ hổng đó vàkhắc phục chúng trước khi chúng trở thành vấn đề chính là chìa khóa để giữ an toàn cho tài sản.

|  |
| --- |
| We've already covered what a vulnerability is. Recall that a vulnerability is a weakness that can be exploited by a threat. That word, can, is an important part of this description. Why is that? Let's explore that together to find out more. |

Chúng tôi đã đề cập đến lỗ hổng là gì.Hãy nhớ lại rằng lỗ hổng là điểm yếu có thể bị khai thác bởi mối đe dọa.Từ đó, có thể, là một phần quan trọng của mô tả này.Tại sao vậy?Chúng ta hãy cùng nhau khám phá điều đó để tìm hiểu thêm.

|  |
| --- |
| Imagine I handed you an important document and asked you to keep it safe. How would you do that? Some of you might first think about locking it up in a safe place. Behind this is the understanding that, because documents can be easily moved, they are vulnerable to theft. When other vulnerabilities come to mind, like how paper burns easily or doesn't resist water, you might add other protections. |

Hãy tưởng tượng tôi đưa cho bạn một tài liệu quan trọng và yêu cầu bạn giữ nó an toàn.Bạn làm điều đó như thế nào?Một số bạn trước tiên có thể nghĩ đến việc khóa nó ở một nơi an toàn.Đằng sau điều này là sự hiểu biết rằng, vì tài liệu có thể được di chuyển dễ dàng,họ dễ bị trộm cắp.Khi nghĩ đến các lỗ hổng khác, chẳng hạn như giấy dễ cháy hoặckhông chống nước, bạn có thể thêm các biện pháp bảo vệ khác.

|  |
| --- |
| Similar to this example, security teams plan to protect assets according to their vulnerabilities and how they can be exploited. In security, an exploit is a way of taking advantage of a vulnerability. Besides finding vulnerabilities, security planning relies a lot on thinking of exploits. |

Tương tự như ví dụ này, các nhóm bảo mật có kế hoạch bảo vệtài sản theo tính dễ bị tổn thương của chúng và cách chúng có thể được khai thác.Trong bảo mật, khai thác là một cách tận dụng lỗ hổng.Bên cạnh việc tìm ra các lỗ hổng, việc lập kế hoạch bảo mật còn dựa rất nhiều vào việc nghĩ đến các cách khai thác.

|  |
| --- |
| For example, there are burglars out there who want to cause harm. Homes have vulnerable systems that can be exploited by a burglar. An example are the windows. Glass is vulnerable to being broken. A burglar can exploit this vulnerability by using a rock to break the window. Thinking of this vulnerability and exploit ahead of time allows us to plan ahead. We can have an alarm system in place to scare the burglar away and alert the police. |

Ví dụ, có những tên trộm ngoài kia muốn gây hại.Các ngôi nhà có hệ thống dễ bị tấn công có thể bị kẻ trộm khai thác. MỘTví dụ là các cửa sổ. Kính dễ bị vỡ.Kẻ trộm có thể khai thác lỗ hổng này bằng cách dùng đá để phá cửa sổ.Nghĩ đến lỗ hổng này và khai thác trước thời hạn cho phép chúng tôi lên kế hoạch trước.Chúng ta có thể lắp đặt một hệ thống báo động để xua đuổi tên trộm và báo cảnh sát.

|  |
| --- |
| Security teams spend a lot of time finding vulnerabilities and thinking of how they can be exploited. They do this with the process known as vulnerability management. Vulnerability management is the process of finding and patching vulnerabilities. Vulnerability management helps keep assets safe. It's a method of stopping threats before they can become a problem. Vulnerability management is a four step process. The first step is to identify vulnerabilities. The next step is to consider potential exploits of those vulnerabilities. Third is to prepare defenses against threats. And finally, the fourth step is to evaluate those defenses. |

Các nhóm bảo mật dành nhiều thời gian để tìm ra các lỗ hổng vàđang nghĩ cách khai thác chúng.Họ thực hiện việc này bằng quy trình được gọi là quản lý lỗ hổng.Quản lý lỗ hổng là quá trình tìm kiếm và vá các lỗ hổng.Quản lý lỗ hổng bảo mật giúp giữ an toàn cho tài sản.Đó là một phương pháp ngăn chặn các mối đe dọa trước khi chúng có thể trở thành vấn đề.Quản lý lỗ hổng bảo mật là một quá trình gồm bốn bước.Bước đầu tiên là xác định các lỗ hổng.Bước tiếp theo là xem xét khả năng khai thác những lỗ hổng đó.Thứ ba là chuẩn bị phòng thủ trước các mối đe dọa. Và cuối cùng,Bước thứ tư là đánh giá những biện pháp phòng vệ đó.

|  |
| --- |
| When the last step ends, the process starts again. Vulnerability management happens in a cycle. It's a regular part of what security teams do because there are always new vulnerabilities to be concerned about. |

Khi bước cuối cùng kết thúc, quá trình sẽ bắt đầu lại.Quản lý lỗ hổng xảy ra theo một chu kỳ.Đó là một phần thường xuyên của những gì đội an ninh làmbởi vì luôn có những lỗ hổng mới cần quan tâm.

|  |
| --- |
| This is exactly why a diverse set of perspectives is useful! Having a wide range of backgrounds and experiences only strengthens security teams and their ability to find exploits. However, even large and diverse security teams can't keep track of everything. |

Đây chính xác là lý do tại sao một tập hợp các quan điểm đa dạng lại hữu ích!Có nền tảng đa dạng vàkinh nghiệm chỉ củng cố các đội bảo mật và khả năng tìm ra cách khai thác của họ.Tuy nhiên, ngay cả những đội bảo mật lớn và đa dạng cũng không thể theo dõi được mọi thứ.

|  |
| --- |
| New vulnerabilities are constantly being discovered. These are known as zero-day exploits. A zero-day is an exploit that was previously unknown. The term zero-day refers to the fact that the exploit is happening in real time with zero days to fix it. These kind of exploits are dangerous. They represent threats that haven't been planned for yet. |

Các lỗ hổng mới liên tục được phát hiện.Chúng được gọi là khai thác zero-day.Zero-day là một cách khai thác mà trước đây chưa được biết đến.Thuật ngữ zero-day đề cập đến thực tế là việc khai thác đang diễn ra trong thời gian thựckhông có ngày nào để sửa nó.Những kiểu khai thác này rất nguy hiểm.Chúng đại diện cho những mối đe dọa chưa được lên kế hoạch.

|  |
| --- |
| For example, we can anticipate the possibility of a burglar breaking into our home. We can plan for this type of threat by having defenses in place, like locks on the doors and windows. A zero-day exploit would be something totally unexpected, like the lock on the door falling off from intense heat. Zero-day exploits are things that don't normally come to mind. For example, this might be a new form of spyware infecting a popular website. When zero-day exploits happen, they can leave assets even more vulnerable to threats than they already are. |

Ví dụ, chúng ta có thể đoán trước khả năng có một tên trộm đột nhập vào nhà mình.Chúng ta có thể lập kế hoạch đối phó với loại mối đe dọa này bằng cách chuẩn bị sẵn các biện pháp phòng vệ,như ổ khóa trên cửa ra vào và cửa sổ.Việc khai thác zero-day sẽ là một điều hoàn toàn bất ngờ,giống như ổ khóa trên cửa rơi ra do sức nóng dữ dội.Khai thác zero-day là những điều mà người ta thường không nghĩ tới.Ví dụ: đây có thể là một dạng phần mềm gián điệp mới lây nhiễm vào một trang web phổ biến.Khi việc khai thác zero-day xảy ra,họ có thể khiến tài sản dễ bị đe dọa hơn hiện tại.

|  |
| --- |
| Vulnerability management is the process of finding vulnerabilities and fixing their exploits. That's why the process is performed regularly at most organizations. Perhaps the most important step of the process is identifying vulnerabilities. We'll explore this step in more details next time we get together. I'll meet you again then! |

Quản lý lỗ hổng là quá trình tìm kiếm lỗ hổng và sửa lỗi khai thác chúng.Đó là lý do tại sao quy trình này được thực hiện thường xuyên ở hầu hết các tổ chức.Có lẽ bước quan trọng nhất của quy trình là xác định các lỗ hổng.Chúng ta sẽ khám phá bước này chi tiết hơn vào lần tới khi chúng ta gặp nhau.Lúc đó tôi sẽ gặp lại bạn!

***1.3. Defense in depth strategy - Chiến lược phòng thủ theo chiều sâu***

|  |
| --- |
| A layered defense is difficult to penetrate. When one barrier fails, another takes its place to stop an attack. Defense in depth is a security model that makes use of this concept. It's a layered approach to vulnerability management that reduces risk. Defense in depth is commonly referred to as the castle approach because it resembles the layered defenses of a castle. |

Một hàng phòng ngự nhiều lớp rất khó bị xuyên thủng.Khi một rào cản thất bại,một cái khác thay thế để ngăn chặn một cuộc tấn công.Phòng thủ theo chiều sâu làmột mô hình bảo mật sử dụng khái niệm này.Đó là một cách tiếp cận theo lớp đểquản lý lỗ hổng giúp giảm thiểu rủi ro.Phòng thủ theo chiều sâu thường được gọi làcách tiếp cận lâu đài bởi vì nógiống như hệ thống phòng thủ nhiều lớp của một lâu đài.

|  |
| --- |
| In the Middle Ages, these structures were very difficult to penetrate. They featured different defenses, each unique in its design, that posed different challenges for attackers. For example, a water-filled barrier called a moat usually formed a circle around the castle, preventing threats like large groups of attackers from reaching the castle walls. The few soldiers that made it past the first layer of defense were then faced with a new challenge, giant stone walls. A vulnerability of these structures were that they could be climbed. If attackers tried exploiting that weakness, guess what? They were met with another layer of defense, watch towers, filled with defenders ready to shoot arrows and keep them from climbing! Each level of defense of these medieval structures minimized the risk of attacks by identifying vulnerabilities and implementing a security control should one system fail. |

Vào thời Trung cổ,những cấu trúc này rất khó xuyên thủng.Họ có những cách phòng thủ khác nhau,mỗi thiết kế đều độc đáo, đó làđặt ra những thách thức khác nhau cho những kẻ tấn công.Ví dụ, một rào chắn đầy nướcđược gọi là hào thường được hình thànhmột vòng quanh lâu đài, ngăn chặn các mối đe dọa nhưnhóm lớn kẻ tấn công tiếp cận các bức tường lâu đài.Một số ít người lính đã vượt qua được lớp đầu tiênphòng thủ sau đó đã phải đối mặt vớimột thử thách mới, những bức tường đá khổng lồ.Tính dễ bị tổn thương của các cấu trúc nàylà chúng có thể leo lên được.Nếu kẻ tấn công cố gắng khai thác điểm yếu đó, hãy đoán xem?Họ gặp phải một lớp phòng thủ khác,tháp canh, đầy những người bảo vệsẵn sàng bắn mũi tên và ngăn chúng leo lên!Mỗi cấp độ phòng thủ củanhững cấu trúc thời trung cổ này đã giảm thiểu nguy cơtấn công bằng cách xác định các lỗ hổng vàthực hiện kiểm soát an ninh nếu một hệ thống bị lỗi.

|  |
| --- |
| Defense in depth works in a similar way. The defense in depth concept can be used to protect any asset. It's mainly used in cybersecurity to protect information using a five layer design. Each layer features a number of security controls that protect information as it travels in and out of the model. |

Phòng thủ theo chiều sâu hoạt động theo cách tương tự.Khái niệm phòng thủ theo chiều sâucó thể được sử dụng để bảo vệ bất kỳ tài sản nào.Nó chủ yếu được sử dụng trong an ninh mạng để bảo vệthông tin sử dụng thiết kế năm lớp.Mỗi lớp có một số điều khiển bảo mậtbảo vệ thông tin như nódi chuyển vào và ra khỏi mô hình.

|  |
| --- |
| The first layer of defense in depth is the perimeter layer. This layer includes some technologies that we've already explored, like usernames and passwords. Mainly, this is a user authentication layer that filters external access. Its function is to only allow access to trusted partners to reach the next layer of defense. |

Lớp phòng thủ đầu tiên trongđộ sâu là lớp chu vi.Lớp này bao gồm một số công nghệmà chúng tôi đã khám phá,như tên người dùng và mật khẩu.Chủ yếu, đây làlớp xác thực người dùng lọc truy cập bên ngoài.Chức năng của nó là chỉ cho phép truy cập vàođối tác đáng tin cậy để tiếp cận lớp phòng thủ tiếp theo.

|  |
| --- |
| Second, the network layer is more closely aligned with authorization. The network layer is made up of other technologies like network firewalls and others. |

Thứ hai, lớp mạng nhiều hơnliên kết chặt chẽ với ủy quyền.Lớp mạng được tạo thành từcác công nghệ khác như tường lửa mạng và các công nghệ khác.

|  |
| --- |
| Next, is the endpoint layer. Endpoints refer to the devices that have access on a network. They could be devices like a laptop, desktop, or a server. Some examples of technologies that protect these devices are anti-virus software. |

Tiếp theo là lớp điểm cuối.Điểm cuối đề cập đến các thiết bịcó quyền truy cập trên mạng.Chúng có thể là những thiết bị như máy tính xách tay,máy tính để bàn hoặc máy chủ.Một số ví dụ về công nghệ bảo vệnhững thiết bị này là phần mềm chống vi-rút.

|  |
| --- |
| After that, we get to the application layer. This includes all the interfaces that are used to interact with technology. At this layer, security measures are programmed as part of an application. One common example is multi-factor authentication. You may be familiar with having to enter both your password and a code sent by SMS. This is part of the application layer of defense. |

Sau đó, chúng ta đến lớp ứng dụng.Điều này bao gồm tất cả các giao diệnđược sử dụng để tương tác với công nghệ.Ở lớp này, các biện pháp bảo mật đượcđược lập trình như một phần của ứng dụng.Một ví dụ phổ biến là xác thực đa yếu tố.Bạn có thể quen với việc phải nhậpcả mật khẩu của bạn và mã được gửi qua SMS.Đây là một phần của lớp ứng dụng phòng thủ.

|  |
| --- |
| And finally, the fifth layer of defense is the data layer. At this layer, we've arrived at the critical data that must be protected, like personally identifiable information. One security control that is important here in this final layer of defense is asset classification. |

Và cuối cùng, lớp bảo vệ thứ năm là lớp dữ liệu.Ở lớp này, chúng ta đã đếndữ liệu quan trọng phải được bảo vệ,như thông tin nhận dạng cá nhân.Một biện pháp kiểm soát an ninh quan trọng ở đâylớp phòng thủ cuối cùng này là phân loại tài sản.

|  |
| --- |
| Like I mentioned earlier, information passes in and out of each of these five layers whenever it's exchanged over a network. There are many more security controls aside from the few that I mentioned that are part of the defense in depth model. A lot of businesses design their security systems using the defense in-depth model. Understanding this framework hopefully gives you a better sense of how an organization's security controls work together to protect important assets. |

Như tôi đã đề cập trước đó,thông tin đi vào và ra khỏi mỗinăm lớp này bất cứ khi nào nó được trao đổi qua mạng.Có nhiều biện pháp kiểm soát bảo mật hơn ngoài một số ítmà tôi đã đề cập đó là một phầncủa mô hình phòng thủ theo chiều sâu.Rất nhiều doanh nghiệp thiết kếhệ thống an ninh của họ bằng cách sử dụng mô hình phòng thủ chuyên sâu.Hy vọng hiểu được khuôn khổ nàymang lại cho bạn cảm giác tốt hơn về cáchcông việc kiểm soát an ninh của một tổ chứccùng nhau bảo vệ những tài sản quan trọng.

***1.4. Common vulnerabilities and exposures - Các lỗ hổng và rủi ro phổ biến***

|  |
| --- |
| We've discussed before that security is a team effort. Did you know the group extends well beyond a single security team? Protecting information is a global effort! |

Chúng ta đã thảo luận trước đó rằng bảo mật là nỗ lực của cả nhóm.Bạn có biết nhóm mở rộngvượt xa một đội an ninh duy nhất?Bảo vệ thông tin là nỗ lực toàn cầu!

|  |
| --- |
| When it comes to vulnerabilities, there are actually online public libraries. Individuals and organizations use them to share and document common vulnerabilities and exposures. We've been focusing a lot on vulnerabilities. Exposures are similar, but they have a key difference. While a vulnerability is a weakness of a system, an exposure is a mistake that can be exploited by a threat. |

Khi nói đến các lỗ hổng,thực sự có những thư viện công cộng trực tuyến.Các cá nhân và tổ chức sử dụng chúng đểchia sẻ và ghi lại các lỗ hổng và nguy cơ phổ biến.Chúng tôi đã tập trung rất nhiều vào các lỗ hổng.Sự tiếp xúc là tương tự nhau, nhưng chúng có một điểm khác biệt chính.Trong khi lỗ hổng là điểm yếu của hệ thống,tiếp xúc là một sai lầmcó thể bị khai thác bởi một mối đe dọa.

|  |
| --- |
| For example, imagine you're asked to protect an important document. Documents are vulnerable to being misplaced. If you laid the document down near an open window, it could be exposed to being blown away. |

Ví dụ, hãy tưởng tượng bạn đangđược yêu cầu bảo vệ một tài liệu quan trọng.Tài liệu dễ bị thất lạc.Nếu bạn đặt tài liệu xuống gần cửa sổ đang mở,nó có thể bị thổi bay.

|  |
| --- |
| One of the most popular libraries of vulnerabilities and exposures is the CVE list. The common vulnerabilities and exposures list, or CVE list, is an openly accessible dictionary of known vulnerabilities and exposures. It is a popular resource. |

Một trong những thư viện phổ biến nhất củalỗ hổng và mức độ phơi nhiễm là danh sách CVE.Những lỗ hổng phổ biến vàdanh sách phơi nhiễm hoặc danh sách CVE,là một từ điển có thể truy cập mởvề các lỗ hổng và mức độ phơi nhiễm đã biết.Nó là một nguồn tài nguyên phổ biến.

|  |
| --- |
| Many organizations use a CVE list to find ways to improve their defenses. The CVE list was originally created by MITRE corporation in 1999. MITRE is a collection of non-profit research and development centers. They're sponsored by the US government. Their focus is on improving security technologies around the world. |

Nhiều tổ chức sử dụng danh sách CVEđể tìm cách cải thiện khả năng phòng thủ của họ.Danh sách CVE ban đầu được tạobởi tập đoàn MITER vào năm 1999.MITER là một bộ sưu tập củatrung tâm nghiên cứu và phát triển phi lợi nhuận.Họ được chính phủ Mỹ tài trợ.Trọng tâm của họ là cải thiệncông nghệ bảo mật trên toàn thế giới.

|  |
| --- |
| The main purpose of the CVE list is to offer a standard way of identifying and categorizing known vulnerabilities and exposures. Most CVEs in the list are reported by independent researchers, technology vendors, and ethical hackers, but anyone can report one. Before a CVE can make it onto the CVE list, it first goes through a strict review process by a CVE Numbering Authority, or CNA. |

Mục đích chính của danh sách CVE là đểđưa ra một cách tiêu chuẩn để xác địnhvà phân loại các lỗ hổng và mức độ phơi nhiễm đã biết.Hầu hết các CVE trong danh sách đềubáo cáo của các nhà nghiên cứu độc lập,các nhà cung cấp công nghệ và các hacker có đạo đức,nhưng bất cứ ai cũng có thể báo cáo một.Trước khi CVE có thể lọt vào danh sách CVE,đầu tiên nó phải trải qua một quá trình xem xét nghiêm ngặt bởiCơ quan đánh số CVE hoặc CNA.

|  |
| --- |
| A CNA is an organization that volunteers to analyze and distribute information on eligible CVEs. All of these groups have an established record of researching vulnerabilities and demonstrating security advisory capabilities. When a vulnerability or exposure is reported to them, a rigorous testing process takes place. |

CNA là một tổ chức tình nguyện thực hiệnphân tích và phân phối thông tin về các CVE đủ điều kiện.Tất cả các nhóm này đều cómột hồ sơ đã được thiết lập về việc nghiên cứu các lỗ hổngvà thể hiện khả năng tư vấn bảo mật.Khi một lỗ hổng hoặc nguy cơ bị phơi nhiễm được báo cáo cho họ,một quá trình kiểm tra nghiêm ngặt diễn ra.

|  |
| --- |
| The CVE list tests four criteria that a vulnerability must have before it's assigned an ID. First, it must be independent of other issues. In other words, the vulnerability should be able to be fixed without having to fix something else. Second, it must be recognized as a potential security risk by whoever reports it. Third, the vulnerability must be submitted with supporting evidence. And finally, the reported vulnerability can only affect one codebase, or in other words, only one program's source code. For instance, the desktop version of Chrome may be vulnerable, but the Android application may not be. If the reported flaw passes all of these tests, it is assigned a CVE ID. |

Danh sách CVE kiểm tra bốn tiêu chímột lỗ hổng phải có trước khi được gán ID.Đầu tiên, nó phải độc lập với các vấn đề khác.Nói cách khác, lỗ hổng có thểđược sửa mà không cần phải sửa cái gì khác.Thứ hai, nó phải được thừa nhận làmột nguy cơ bảo mật tiềm ẩn bởi bất cứ ai báo cáo nó.Thứ ba, lỗ hổng phải đượcnộp với bằng chứng hỗ trợ.Và cuối cùng, lỗ hổng được báo cáochỉ có thể ảnh hưởng đến một cơ sở mã,hay nói cách khác, chỉ có mã nguồn của một chương trình.Ví dụ: phiên bản máy tính để bàncủa Chrome có thể dễ bị tấn công,nhưng ứng dụng Android có thể không.Nếu lỗ hổng được báo cáo vượt qua tất cả các thử nghiệm này,nó được gán một ID CVE.

|  |
| --- |
| Vulnerabilities added to the CVE list are often reviewed by other online vulnerability databases. These organizations put them through additional tests to reveal how significant the flaws are and to determine what kind of threat they pose. One of the most popular is the NIST National Vulnerabilities Database. |

Các lỗ hổng được thêm vào danh sách CVE làthường được xem xét bởi các cơ sở dữ liệu về lỗ hổng trực tuyến khác.Các tổ chức này đưa họ quakiểm tra bổ sung để tiết lộ làm thế nàonhững sai sót đáng kể làvà để xác định loại mối đe dọa mà chúng gây ra.Một trong những phổ biến nhất làCơ sở dữ liệu về lỗ hổng bảo mật quốc gia của NIST.

|  |
| --- |
| The NIST National Vulnerabilities Database uses what's known as the common vulnerability scoring system, or CVSS, which is a measurement system that scores the severity of a vulnerability. Security teams use CVSS as a way of calculating the impact a vulnerability could have on a system. They also use them to determine how quickly a vulnerability should be patched. |

Cơ sở dữ liệu về lỗ hổng bảo mật quốc gia của NIST sử dụngcái được gọi là hệ thống tính điểm dễ bị tổn thương phổ biến,hoặc CVSS, đó làmột hệ thống đo lường cho điểmmức độ nghiêm trọng của một lỗ hổng.Các nhóm bảo mật sử dụng CVSS như một cáchtính toán tác động của lỗ hổngcó thể có trên một hệ thống.Họ cũng sử dụng chúng để xác định cáchmột lỗ hổng cần được vá nhanh chóng.

|  |
| --- |
| The NIST National Vulnerabilities Database provides a base score of CVEs on a scale of 0-10. Base scores reflect the moment a vulnerability is evaluated, so they don't change over time. In general, a CVSS that scores below a 4.0 is considered to be low risk and doesn't require immediate attention. However, anything above a 9.0 is considered to be a critical risk to company assets that should be addressed right away. |

Cơ sở dữ liệu về lỗ hổng quốc gia của NIST cung cấpđiểm cơ bản của CVE theo thang điểm từ 0-10.Điểm cơ bản phản ánh thời điểmmột lỗ hổng được đánh giá,nên chúng không thay đổi theo thời gian.Nhìn chung, CVSS cho điểmdưới 4.0 được coi là rủi ro thấpvà không cần chú ý ngay lập tức.Tuy nhiên, bất kỳ điểm nào trên 9,0 đều được coi làmột nguy cơ nghiêm trọng đối vớitài sản của công ty cần được giải quyết ngay lập tức.

|  |
| --- |
| Security teams commonly use the CVE list and CVSS scores as part of their vulnerability management strategy. These references provide recommendations for prioritizing security fixes, like installing software updates before patches. |

Các nhóm bảo mật thường sử dụng danh sách CVE vàĐiểm CVSS là một phần củachiến lược quản lý lỗ hổng của họ.Những tài liệu tham khảo này cung cấp các khuyến nghịđể ưu tiên sửa lỗi bảo mật,giống như cài đặt bản cập nhật phần mềm trước khi có bản vá.

|  |
| --- |
| Libraries like the CVE list, help organizations answer questions. Is a vulnerability dangerous to our business? If so, how soon should we address it? |

Các thư viện như danh sách CVE,giúp các tổ chức trả lời các câu hỏi.Lỗ hổng có nguy hiểm cho hoạt động kinh doanh của chúng ta không?Nếu vậy, chúng ta nên giải quyết nó trong bao lâu?

|  |
| --- |
| These online libraries bring together diverse perspectives from across the world. Contributing to this effort is one of my favorite parts of working in this field. Keep gaining experience, and I hope you'll participate too! |

Những thư viện trực tuyến này tập hợpnhững quan điểm đa dạng từ khắp nơi trên thế giới.Đóng góp vào nỗ lực này là một trong nhữngphần yêu thích của tôi khi làm việc trong lĩnh vực này.Tiếp tục tích lũy kinh nghiệm,và tôi hy vọng bạn cũng sẽ tham gia!

***1.5. The OWASP Top 10 - Top 10 của OWASP***

|  |
| --- |
| **The OWASP Top 10** |

**Top 10 của OWASP**

|  |
| --- |
| To prepare for future risks, security professionals need to stay informed. Previously, you learned about the **CVE® list**, an openly accessible dictionary of known vulnerabilities and exposures. The CVE® list is an important source of information that the global security community uses to share information with each other. |

Để chuẩn bị cho những rủi ro trong tương lai, các chuyên gia bảo mật cần cập nhật thông tin. Trước đây, bạn đã tìm hiểu về **danh sách CVE®** , một từ điển có thể truy cập mở về các lỗ hổng và nguy cơ đã biết. Danh sách CVE® là nguồn thông tin quan trọng được cộng đồng bảo mật toàn cầu sử dụng để chia sẻ thông tin với nhau.

|  |
| --- |
| In this reading, you’ll learn about another important resource that security professionals reference, the Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP). You’ll learn about OWASP’s role in the global security community and how companies use this resource to focus their efforts. |

Trong bài đọc này, bạn sẽ tìm hiểu về một tài nguyên quan trọng khác mà các chuyên gia bảo mật tham khảo, Dự án Bảo mật Ứng dụng Web Mở, gần đây đã được đổi tên thành Dự án Bảo mật Ứng dụng Toàn cầu Mở® (OWASP). Bạn sẽ tìm hiểu về vai trò của OWASP trong cộng đồng bảo mật toàn cầu và cách các công ty sử dụng tài nguyên này để tập trung nỗ lực.

|  |
| --- |
| **What is OWASP?** |

**OWASP là gì?**

|  |
| --- |
| OWASP is a nonprofit foundation that works to improve the security of software. OWASP is an open platform that security professionals from around the world use to share information, tools, and events that are focused on securing the web. |

OWASP là một tổ chức phi lợi nhuận hoạt động nhằm cải thiện tính bảo mật của phần mềm. OWASP là một nền tảng mở được các chuyên gia bảo mật trên khắp thế giới sử dụng để chia sẻ thông tin, công cụ và sự kiện tập trung vào việc bảo mật web.

|  |
| --- |
| **The OWASP Top 10** |

**Top 10 của OWASP**

|  |
| --- |
| One of OWASP’s most valuable resources is the OWASP Top 10. The organization has published this list since 2003 as a way to spread awareness of the web’s most targeted vulnerabilities. The Top 10 mainly applies to new or custom made software. Many of the world's largest organizations reference the OWASP Top 10 during application development to help ensure their programs address common security mistakes. |

Một trong những tài nguyên quý giá nhất của OWASP là OWASP Top 10. Tổ chức này đã công bố danh sách này từ năm 2003 như một cách để truyền bá nhận thức về các lỗ hổng được nhắm mục tiêu nhiều nhất trên web. Top 10 chủ yếu áp dụng cho phần mềm mới hoặc phần mềm tùy chỉnh. Nhiều tổ chức lớn nhất thế giới tham khảo Top 10 OWASP trong quá trình phát triển ứng dụng để giúp đảm bảo chương trình của họ giải quyết các lỗi bảo mật phổ biến.

|  |
| --- |
| **Pro tip:** OWASP’s Top 10 is updated every few years as technologies evolve. Rankings are based on how often the vulnerabilities are discovered and the level of risk they present. |

**Mẹo chuyên nghiệp:** Top 10 của OWASP được cập nhật vài năm một lần khi công nghệ phát triển. Thứ hạng dựa trên tần suất phát hiện các lỗ hổng và mức độ rủi ro mà chúng mang lại.

|  |
| --- |
| **Note:** Auditors also use the OWASP Top 10 as one point of reference when checking for regulatory compliance. |

**Lưu ý:** Kiểm toán viên cũng sử dụng OWASP Top 10 làm điểm tham chiếu khi kiểm tra việc tuân thủ quy định.

|  |
| --- |
| **Common vulnerabilities** |

**Các lỗ hổng phổ biến**

|  |
| --- |
| Businesses often make critical security decisions based on the vulnerabilities listed in the OWASP Top 10. This resource influences how businesses design new software that will be on their network, unlike the CVE® list, which helps them identify improvements to existing programs. These are the most regularly listed vulnerabilities that appear in their rankings to know about: |

Các doanh nghiệp thường đưa ra các quyết định bảo mật quan trọng dựa trên các lỗ hổng được liệt kê trong Top 10 của OWASP. Tài nguyên này ảnh hưởng đến cách các doanh nghiệp thiết kế phần mềm mới sẽ có trên mạng của họ, không giống như danh sách CVE®, danh sách này giúp họ xác định các cải tiến đối với các chương trình hiện có. Đây là những lỗ hổng được liệt kê thường xuyên nhất xuất hiện trong bảng xếp hạng của họ để biết về:

|  |
| --- |
| **Broken access control** |

**Kiểm soát truy cập bị hỏng**

|  |
| --- |
| Access controls limit what users can do in a web application. For example, a blog might allow visitors to post comments on a recent article but restricts them from deleting the article entirely. Failures in these mechanisms can lead to unauthorized information disclosure, modification, or destruction. They can also give someone unauthorized access to other business applications. |

Kiểm soát truy cập giới hạn những gì người dùng có thể làm trong ứng dụng web. Ví dụ: một blog có thể cho phép khách truy cập đăng nhận xét về một bài viết gần đây nhưng hạn chế họ xóa toàn bộ bài viết đó. Thất bại trong các cơ chế này có thể dẫn đến việc tiết lộ, sửa đổi hoặc phá hủy thông tin trái phép. Họ cũng có thể cấp cho ai đó quyền truy cập trái phép vào các ứng dụng kinh doanh khác.

|  |
| --- |
| **Cryptographic failures** |

**Lỗi mật mã**

|  |
| --- |
| Information is one of the most important assets businesses need to protect. Privacy laws such as General Data Protection Regulation (GDPR) require sensitive data to be protected by effective encryption methods. Vulnerabilities can occur when businesses fail to encrypt things like personally identifiable information (PII). For example, if a web application uses a weak hashing algorithm, like MD5, it’s more at risk of suffering a data breach. |

Thông tin là một trong những tài sản quan trọng nhất mà doanh nghiệp cần bảo vệ. Các luật về quyền riêng tư như Quy định chung về bảo vệ dữ liệu (GDPR) yêu cầu dữ liệu nhạy cảm phải được bảo vệ bằng các phương pháp mã hóa hiệu quả. Lỗ hổng có thể xảy ra khi doanh nghiệp không mã hóa những thứ như thông tin nhận dạng cá nhân (PII). Ví dụ: nếu một ứng dụng web sử dụng thuật toán băm yếu, như MD5, thì ứng dụng đó sẽ có nhiều nguy cơ bị vi phạm dữ liệu hơn.

|  |
| --- |
| **Injection** |

**Mũi tiêm**

|  |
| --- |
| Injection occurs when malicious code is inserted into a vulnerable application. Although the app appears to work normally, it does things that it wasn’t intended to do. Injection attacks can give threat actors a backdoor into an organization’s information system. A common target is a website’s login form. When these forms are vulnerable to injection, attackers can insert malicious code that gives them access to modify or steal user credentials. |

Việc tiêm nhiễm xảy ra khi mã độc được chèn vào một ứng dụng dễ bị tấn công. Mặc dù ứng dụng có vẻ hoạt động bình thường nhưng nó vẫn thực hiện những việc không như mong muốn. Các cuộc tấn công tiêm nhiễm có thể tạo cho các tác nhân đe dọa một cửa sau để xâm nhập vào hệ thống thông tin của tổ chức. Mục tiêu chung là hình thức đăng nhập của trang web. Khi những biểu mẫu này dễ bị tấn công, kẻ tấn công có thể chèn mã độc để chúng có quyền truy cập để sửa đổi hoặc đánh cắp thông tin xác thực của người dùng.

|  |
| --- |
| **Insecure design** |

**Thiết kế không an toàn**

|  |
| --- |
| Applications should be designed in such a way that makes them resilient to attack. When they aren’t, they’re much more vulnerable to threats like injection attacks or malware infections. Insecure design refers to a wide range of missing or poorly implemented security controls that should have been programmed into an application when it was being developed. |

Các ứng dụng phải được thiết kế theo cách giúp chúng có khả năng chống chịu sự tấn công. Khi không làm như vậy, chúng sẽ dễ bị tổn thương hơn trước các mối đe dọa như tấn công tiêm nhiễm hoặc lây nhiễm phần mềm độc hại. Thiết kế không an toàn đề cập đến một loạt các biện pháp kiểm soát bảo mật bị thiếu hoặc được triển khai kém mà lẽ ra phải được lập trình vào ứng dụng khi ứng dụng đó đang được phát triển.

|  |
| --- |
| **Security misconfiguration** |

**Cấu hình bảo mật sai**

|  |
| --- |
| Misconfigurations occur when security settings aren’t properly set or maintained. Companies use a variety of different interconnected systems. Mistakes often happen when those systems aren’t properly set up or audited. A common example is when businesses deploy equipment, like a network server, using default settings. This can lead businesses to use settings that fail to address the organization's security objectives. |

Cấu hình sai xảy ra khi cài đặt bảo mật không được đặt hoặc duy trì đúng cách. Các công ty sử dụng nhiều hệ thống kết nối khác nhau. Sai lầm thường xảy ra khi những hệ thống đó không được thiết lập hoặc kiểm tra đúng cách. Một ví dụ phổ biến là khi doanh nghiệp triển khai thiết bị, như máy chủ mạng, sử dụng cài đặt mặc định. Điều này có thể khiến doanh nghiệp sử dụng các cài đặt không giải quyết được các mục tiêu bảo mật của tổ chức.

|  |
| --- |
| **Vulnerable and outdated components** |

**Các thành phần dễ bị tổn thương và lỗi thời**

|  |
| --- |
| Vulnerable and outdated components is a category that mainly relates to application development. Instead of coding everything from scratch, most developers use open-source libraries to complete their projects faster and easier. This publicly available software is maintained by communities of programmers on a volunteer basis. Applications that use vulnerable components that have not been maintained are at greater risk of being exploited by threat actors. |

Các thành phần dễ bị tổn thương và lỗi thời là một danh mục chủ yếu liên quan đến phát triển ứng dụng. Thay vì mã hóa mọi thứ từ đầu, hầu hết các nhà phát triển đều sử dụng thư viện nguồn mở để hoàn thành dự án của họ nhanh hơn và dễ dàng hơn. Phần mềm có sẵn công khai này được duy trì bởi cộng đồng lập trình viên trên cơ sở tình nguyện. Các ứng dụng sử dụng các thành phần dễ bị tổn thương chưa được bảo trì sẽ có nguy cơ bị các tác nhân đe dọa khai thác cao hơn.

|  |
| --- |
| **Identification and authentication failures** |

**Lỗi nhận dạng và xác thực**

|  |
| --- |
| Identification is the keyword in this vulnerability category. When applications fail to recognize who should have access and what they’re authorized to do, it can lead to serious problems. For example, a home Wi-Fi router normally uses a simple login form to keep unwanted guests off the network. If this defense fails, an attacker can invade the homeowner’s privacy. |

Nhận dạng là từ khóa trong danh mục lỗ hổng này. Khi các ứng dụng không nhận ra ai sẽ có quyền truy cập và những gì họ được phép làm, điều đó có thể dẫn đến các vấn đề nghiêm trọng. Ví dụ: bộ định tuyến Wi-Fi gia đình thường sử dụng biểu mẫu đăng nhập đơn giản để ngăn những vị khách không mong muốn truy cập mạng. Nếu cách phòng thủ này không thành công, kẻ tấn công có thể xâm phạm quyền riêng tư của chủ nhà.

|  |
| --- |
| **Software and data integrity failures** |

**Lỗi toàn vẹn dữ liệu và phần mềm**

|  |
| --- |
| Software and data integrity failures are instances when updates or patches are inadequately reviewed before implementation. Attackers might exploit these weaknesses to deliver malicious software. When that occurs, there can be serious downstream effects. Third parties are likely to become infected if a single system is compromised, an event known as a supply chain attack. |

Lỗi về tính toàn vẹn của phần mềm và dữ liệu là những trường hợp khi các bản cập nhật hoặc bản vá lỗi không được xem xét đầy đủ trước khi triển khai. Những kẻ tấn công có thể khai thác những điểm yếu này để phát tán phần mềm độc hại. Khi điều đó xảy ra, có thể có những ảnh hưởng nghiêm trọng về sau. Các bên thứ ba có khả năng bị lây nhiễm nếu một hệ thống bị xâm phạm, một sự kiện được gọi là tấn công chuỗi cung ứng.

|  |
| --- |
| A famous example of a supply chain attack is the [SolarWinds cyber attack (2020)](https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic) where hackers injected malicious code into software updates that the company unknowingly released to their customers. |

Một ví dụ nổi tiếng về cuộc tấn công chuỗi cung ứng là[Tấn công mạng SolarWinds (2020)](https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic)nơi tin tặc đã tiêm mã độc vào các bản cập nhật phần mềm mà công ty đã vô tình phát hành cho khách hàng của họ.

|  |
| --- |
| **Security logging and monitoring failures** |

**Lỗi ghi nhật ký và giám sát bảo mật**

|  |
| --- |
| In security, it’s important to be able to log and trace back events. Having a record of events like user login attempts is critical to finding and fixing problems. Sufficient monitoring and incident response is equally important. |

Trong vấn đề bảo mật, điều quan trọng là có thể ghi nhật ký và theo dõi các sự kiện. Việc có bản ghi các sự kiện như số lần đăng nhập của người dùng là rất quan trọng để tìm và khắc phục sự cố. Giám sát đầy đủ và ứng phó sự cố cũng quan trọng không kém.

|  |
| --- |
| **Server-side request forgery** |

**Giả mạo yêu cầu phía máy chủ**

|  |
| --- |
| Companies have public and private information stored on web servers. When you use a hyperlink or click a button on a website, a request is sent to a server that should validate who you are, fetch the appropriate data, and then return it to you. |

Các công ty có thông tin công khai và riêng tư được lưu trữ trên máy chủ web. Khi bạn sử dụng siêu liên kết hoặc nhấp vào nút trên trang web, một yêu cầu sẽ được gửi đến máy chủ để xác thực bạn là ai, tìm nạp dữ liệu thích hợp rồi gửi lại cho bạn.



|  |
| --- |
| Server-side request forgeries (SSRFs) are when attackers manipulate the normal operations of a server to read or update other resources on that server. These are possible when an application on the server is vulnerable. Malicious code can be carried by the vulnerable app to the host server that will fetch unauthorized data. |

Giả mạo yêu cầu phía máy chủ (SSRF) là khi kẻ tấn công thao túng các hoạt động bình thường của máy chủ để đọc hoặc cập nhật các tài nguyên khác trên máy chủ đó. Những điều này có thể xảy ra khi một ứng dụng trên máy chủ dễ bị tấn công. Mã độc hại có thể được ứng dụng dễ bị tấn công mang đến máy chủ lưu trữ để lấy dữ liệu trái phép.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Staying informed and maintaining awareness about the latest cybersecurity trends can be a useful way to help defend against attacks and prepare for future risks in your security career. [OWASP’s Top 10](https://owasp.org/www-project-top-ten/) is a useful resource where you can learn more about these vulnerabilities. |

Luôn cập nhật thông tin và duy trì nhận thức về các xu hướng an ninh mạng mới nhất có thể là một cách hữu ích để giúp chống lại các cuộc tấn công và chuẩn bị cho những rủi ro trong tương lai trong sự nghiệp bảo mật của bạn.[Top 10 của OWASP](https://owasp.org/www-project-top-ten/)là một nguồn tài nguyên hữu ích nơi bạn có thể tìm hiểu thêm về các lỗ hổng này.

***1.6. Open source intelligence - Thông tin nguồn mở***

|  |
| --- |
| **Open source intelligence** |

**Thông tin nguồn mở**

|  |
| --- |
| Cyber attacks can sometimes be prevented with the right information, which starts with knowing where your systems are vulnerable. Previously, you learned that the CVE® list and scanning tools are two useful ways of finding weaknesses. But, there are other ways to identify vulnerabilities and threats. |

Các cuộc tấn công mạng đôi khi có thể được ngăn chặn bằng thông tin phù hợp, bắt đầu bằng việc biết hệ thống của bạn dễ bị tổn thương ở đâu. Trước đây, bạn đã biết rằng danh sách CVE® và các công cụ quét là hai cách hữu ích để tìm ra điểm yếu. Tuy nhiên, có nhiều cách khác để xác định các lỗ hổng và mối đe dọa.

|  |
| --- |
| In this reading, you’ll learn about open-source intelligence, commonly known as OSINT. OSINT is the collection and analysis of information from publicly available sources to generate usable intelligence. It's commonly used to support cybersecurity activities, like identifying potential threats and vulnerabilities. You'll learn why open-source intelligence is gathered and how it can improve cybersecurity. You’ll also learn about commonly used resources and tools for gathering information and intelligence. |

Trong bài đọc này, bạn sẽ tìm hiểu về trí thông minh nguồn mở, thường được gọi là OSINT. OSINT là việc thu thập và phân tích thông tin từ các nguồn có sẵn công khai để tạo ra thông tin có thể sử dụng được. Nó thường được sử dụng để hỗ trợ các hoạt động an ninh mạng, như xác định các mối đe dọa và lỗ hổng tiềm ẩn. Bạn sẽ tìm hiểu lý do tại sao thông tin nguồn mở được thu thập và cách thông tin đó có thể cải thiện an ninh mạng. Bạn cũng sẽ tìm hiểu về các tài nguyên và công cụ thường được sử dụng để thu thập thông tin và thông tin tình báo.

|  |
| --- |
| **Information vs intelligence** |

**Thông tin vs trí thông minh**

|  |
| --- |
| The terms intelligence and information are often used interchangeably, making it easy to mix them up. Both are important aspects of cybersecurity that differ in their focus and objectives. |

Các thuật ngữ trí thông minh và thông tin thường được sử dụng thay thế cho nhau, khiến chúng ta dễ nhầm lẫn giữa chúng. Cả hai đều là những khía cạnh quan trọng của an ninh mạng, khác nhau về trọng tâm và mục tiêu.

|  |
| --- |
| *Information* refers to the collection of raw data or facts about a specific subject. *Intelligence*, on the other hand, refers to the analysis of information to produce knowledge or insights that can be used to support decision-making. |

*Thông tin* đề cập đến việc thu thập dữ liệu thô hoặc sự kiện về một chủ đề cụ thể. Mặt khác, *trí thông minh đề cập đến việc phân tích thông tin để tạo ra kiến ​​thức hoặc hiểu biết sâu sắc có thể được sử dụng để hỗ trợ việc ra quyết định.*

|  |
| --- |
| For example, new information might be released about an update to the operating system (OS) that's installed on your organization's workstations. Later, you might find that new cyber threats have been linked to this new update by researching multiple cybersecurity news resources. The analysis of this information can be used as intelligence to guide your organization's decision about installing the OS updates on employee workstations. |

Ví dụ: thông tin mới có thể được phát hành về bản cập nhật cho hệ điều hành (OS) được cài đặt trên máy trạm của tổ chức bạn. Sau này, bạn có thể phát hiện ra rằng các mối đe dọa mạng mới có liên quan đến bản cập nhật mới này bằng cách nghiên cứu nhiều nguồn tin tức về an ninh mạng. Việc phân tích thông tin này có thể được sử dụng làm thông tin tình báo để hướng dẫn tổ chức của bạn đưa ra quyết định về việc cài đặt các bản cập nhật hệ điều hành trên máy trạm của nhân viên.

|  |
| --- |
| In other words, intelligence is derived from information through the process of analysis, interpretation, and integration. Gathering information and intelligence are both important aspects of cybersecurity. |

Nói cách khác, trí thông minh có nguồn gốc từ thông tin thông qua quá trình phân tích, giải thích và tích hợp. Thu thập thông tin và trí thông minh đều là những khía cạnh quan trọng của an ninh mạng.

|  |
| --- |
| **Intelligence improves decision-making** |

**Trí thông minh cải thiện việc ra quyết định**

|  |
| --- |
| Businesses often use information to gain insights into the behavior of their customers. Insights, or intelligence, can then be used to improve their decision making. In security, open-source information is used in a similar way to gain insights into threats and vulnerabilities that can pose risks to an organization. |

Các doanh nghiệp thường sử dụng thông tin để hiểu rõ hơn về hành vi của khách hàng. Những hiểu biết sâu sắc hoặc trí thông minh sau đó có thể được sử dụng để cải thiện việc ra quyết định của họ. Trong bảo mật, thông tin nguồn mở được sử dụng theo cách tương tự để hiểu rõ hơn về các mối đe dọa và lỗ hổng có thể gây rủi ro cho tổ chức.

|  |
| --- |
| OSINT plays a significant role in **information security (InfoSec)**, which is the practice of keeping data in all states away from unauthorized users. |

OSINT đóng một vai trò quan trọng trong **bảo mật thông tin (InfoSec)** , đó là phương pháp giữ dữ liệu ở tất cả các trạng thái tránh xa những người dùng trái phép.

|  |
| --- |
| For example, a company's InfoSec team is responsible for protecting their network from potential threats. They might utilize OSINT to monitor online forums and hacker communities for discussions about emerging vulnerabilities. If they come across a forum post discussing a newly discovered weakness in a popular software that the company uses, the team can quickly assess the risk, prioritize patching efforts, and implement necessary safeguards to prevent an attack. |

Ví dụ: nhóm InfoSec của một công ty chịu trách nhiệm bảo vệ mạng của họ khỏi các mối đe dọa tiềm ẩn. Họ có thể sử dụng OSINT để giám sát các diễn đàn trực tuyến và cộng đồng hacker để thảo luận về các lỗ hổng mới nổi. Nếu họ tình cờ thấy một bài đăng trên diễn đàn thảo luận về điểm yếu mới được phát hiện trong một phần mềm phổ biến mà công ty sử dụng, thì nhóm có thể nhanh chóng đánh giá rủi ro, ưu tiên nỗ lực vá lỗi và thực hiện các biện pháp bảo vệ cần thiết để ngăn chặn một cuộc tấn công.

|  |
| --- |
| Here are some of the ways OSINT can be used to generate intelligence:   * To provide insights into cyber attacks * To detect potential data exposures * To evaluate existing defenses * To identify unknown vulnerabilities |

Dưới đây là một số cách OSINT có thể được sử dụng để tạo ra thông tin tình báo:

* Để cung cấp cái nhìn sâu sắc về các cuộc tấn công mạng
* Để phát hiện khả năng phơi nhiễm dữ liệu
* Để đánh giá các biện pháp phòng thủ hiện có
* Để xác định các lỗ hổng chưa biết

|  |
| --- |
| Collecting intelligence is sometimes part of the vulnerability management process. Security teams might use OSINT to develop profiles of potential targets and make data driven decisions on improving their defenses. |

Thu thập thông tin đôi khi là một phần của quy trình quản lý lỗ hổng. Các nhóm bảo mật có thể sử dụng OSINT để phát triển hồ sơ về các mục tiêu tiềm năng và đưa ra quyết định dựa trên dữ liệu nhằm cải thiện khả năng phòng thủ của họ.

|  |
| --- |
| **OSINT tools** |

**Công cụ OSINT**

|  |
| --- |
| There's an enormous amount of open-source information online. Finding relevant information that can be used to gather intelligence is a challenge. Information can be gathered from a variety of sources, such as search engines, social media, discussion boards, blogs, and more. Several tools also exist that can be used in your intelligence gathering process. Here are just a few examples of tools that you can explore:   * [VirusTotal](https://www.virustotal.com/gui/home/upload) is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. * [MITRE ATT&CK®](https://attack.mitre.org/) is a knowledge base of adversary tactics and techniques based on real-world observations. * [OSINT Framework](https://osintframework.com/) is a web-based interface where you can find OSINT tools for almost any kind of source or platform. * [Have I been Pwned](https://haveibeenpwned.com/) is a tool that can be used to search for breached email accounts. |

Có một lượng lớn thông tin nguồn mở trực tuyến. Việc tìm kiếm thông tin liên quan có thể được sử dụng để thu thập thông tin tình báo là một thách thức. Thông tin có thể được thu thập từ nhiều nguồn khác nhau, chẳng hạn như công cụ tìm kiếm, phương tiện truyền thông xã hội, diễn đàn thảo luận, blog, v.v. Một số công cụ cũng tồn tại có thể được sử dụng trong quá trình thu thập thông tin tình báo của bạn. Đây chỉ là một vài ví dụ về các công cụ mà bạn có thể khám phá:

* [Tổng số virus](https://www.virustotal.com/gui/home/upload)là dịch vụ cho phép mọi người phân tích các tệp, miền, URL và địa chỉ IP đáng ngờ để tìm nội dung độc hại.
* [MITER ATT&CK®](https://attack.mitre.org/)là cơ sở kiến ​​thức về chiến thuật và kỹ thuật của đối thủ dựa trên những quan sát trong thế giới thực.
* [Khung OSINT](https://osintframework.com/)là một giao diện dựa trên web nơi bạn có thể tìm thấy các công cụ OSINT cho hầu hết mọi loại nguồn hoặc nền tảng.
* [Tôi đã bị Pwned chưa](https://haveibeenpwned.com/)là một công cụ có thể được sử dụng để tìm kiếm các tài khoản email bị vi phạm.

|  |
| --- |
| There are numerous other OSINT tools that can be used to find specific types of information. Remember, information can be gathered from a variety of sources. Ultimately, it's your responsibility to thoroughly research any available information that's relevant to the problem you’re trying to solve. |

Có rất nhiều công cụ OSINT khác có thể được sử dụng để tìm các loại thông tin cụ thể. Hãy nhớ rằng, thông tin có thể được thu thập từ nhiều nguồn khác nhau. Cuối cùng, trách nhiệm của bạn là nghiên cứu kỹ lưỡng mọi thông tin sẵn có liên quan đến vấn đề bạn đang cố gắng giải quyết.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Gathering information and intelligence are important aspects of cybersecurity. OSINT is used to make evidence-based decisions that can be used to prevent attacks. There’s so much information available, which is why it's important for security professionals to be skilled with searching for information. Having familiarity with popular OSINT tools and resources will make your research easier when gathering information and collecting intelligence. |

Thu thập thông tin và trí thông minh là những khía cạnh quan trọng của an ninh mạng. OSINT được sử dụng để đưa ra các quyết định dựa trên bằng chứng có thể được sử dụng để ngăn chặn các cuộc tấn công. Có rất nhiều thông tin có sẵn, đó là lý do tại sao điều quan trọng đối với các chuyên gia bảo mật là phải có kỹ năng tìm kiếm thông tin. Việc làm quen với các công cụ và tài nguyên OSINT phổ biến sẽ giúp việc nghiên cứu của bạn dễ dàng hơn khi thu thập thông tin và thu thập thông tin tình báo.

***1.7. Test your knowledge: Flaws in the system - Kiểm tra kiến ​​thức của bạn: Lỗ hổng trong hệ thống***

**2. Identify system vulnerabilities - Xác định các lỗ hổng hệ thống**

***2.1. Vulnerability assessments - Đánh giá tính dễ bị tổn thương***

|  |
| --- |
| Our exploration of the vulnerability management process so far has been focused on a couple of topics. We've discussed how vulnerabilities influence the design of defenses. We've also talked about how common vulnerabilities are shared. A topic we're yet to cover is how vulnerabilities are found in the first place. |

Khám phá của chúng tôi về quy trình quản lý lỗ hổngcho đến nay đã được tập trung vào một vài chủ đề.Chúng ta đã thảo luận về cách các lỗ hổngảnh hưởng đến thiết kế phòng thủ.Chúng tôi cũng đã nói về cáchcác lỗ hổng phổ biến được chia sẻ.Một chủ đề chúng tôi chưa đề cập đến làlàm thế nào các lỗ hổng được tìm thấy ngay từ đầu.

|  |
| --- |
| Weaknesses and flaws are generally found during a vulnerability assessment. A vulnerability assessment is the internal review process of an organization's security systems. These assessments work similar to the process of identifying and categorizing vulnerabilities on the CVE list. The main difference is the organization's security team performs, evaluates, scores, and fixes them on their own. Security analysts play a key role throughout this process. |

Những điểm yếu và sai sót nói chung làđược tìm thấy trong quá trình đánh giá lỗ hổng.Đánh giá tính dễ bị tổn thương làquá trình đánh giá nội bộ củahệ thống an ninh của một tổ chức.Những đánh giá này hoạt động tương tự như quá trìnhxác định và phân loại các lỗ hổngtrong danh sách CVE.Sự khác biệt chính làđội an ninh của tổ chức thực hiện,tự đánh giá, cho điểm và sửa lỗi.Các nhà phân tích bảo mật chơivai trò quan trọng trong suốt quá trình này.

|  |
| --- |
| Overall, the goal of a vulnerability assessment is to identify weak points and prevent attacks. They're also how security teams determine whether their security controls meet regulatory standards. Organizations perform vulnerability assessments a lot. Because companies have so many assets to protect, security teams sometimes need to select which area to focus on through vulnerability assessments. |

Nhìn chung, mục tiêu củađánh giá tính dễ bị tổn thương làxác định điểm yếu và ngăn chặn các cuộc tấn công.Chúng cũng là cách các nhóm bảo mật xác định liệukiểm soát an ninh của họ đáp ứng các tiêu chuẩn quy định.Các tổ chức thực hiện đánh giá lỗ hổng rất nhiều.Bởi vì công ty có rất nhiều tài sảnđể bảo vệ, đội an ninhđôi khi cần chọn khu vực nàotập trung vào việc đánh giá tính dễ bị tổn thương.

|  |
| --- |
| Once they decide what to focus on, vulnerability assessments typically follow a four-step process. The first step is identification. Here, scanning tools and manual testing are used to find vulnerabilities. During the identification step, the goal is to understand the current state of a security system, like taking a picture of it. |

Một khi họ quyết định nên tập trung vào điều gì,đánh giá tính dễ bị tổn thương thường tuân theomột quá trình bốn bước.Bước đầu tiên là nhận dạng.Ở đây, các công cụ quét vàkiểm tra thủ công được sử dụng để tìm lỗ hổng.Trong bước nhận dạng,mục tiêu là để hiểutình trạng hiện tại của hệ thống an ninh,giống như chụp ảnh nó.

|  |
| --- |
| A large number of findings usually appear after identification. The next step of the process is vulnerability analysis. During this step, each of the vulnerabilities that were identified are tested. By being a digital detective, the goal of vulnerability analysis is to find the source of the problem. |

Một số lượng lớn các phát hiệnthường xuất hiện sau khi nhận dạng.Bước tiếp theo của quy trình là phân tích lỗ hổng.Trong bước này, mỗicác lỗ hổng đã được xác định sẽ được kiểm tra.Bằng cách trở thành một thám tử kỹ thuật số, mục tiêu củaphân tích lỗ hổng làtìm ra nguồn gốc của vấn đề.

|  |
| --- |
| The third step of the process is risk assessment. During this step of the process, a score is assigned to each vulnerability. This score is assigned based on two factors: how severe the impact would be if the vulnerability were to be exploited and the likelihood of this happening. |

Bước thứ ba của quy trình là đánh giá rủi ro.Trong bước này của quy trình,một số điểm được gán cho mỗi lỗ hổng.Điểm này được chỉ định dựa trên hai yếu tố:mức độ tác động sẽ nghiêm trọng như thế nào nếu lỗ hổng bảo mật đượcbị khai thác và khả năng xảy ra điều này.

|  |
| --- |
| Vulnerabilities uncovered during the first two steps of this process often outnumber the people available to fix them. Risk assessments are a way of prioritizing resources to handle the vulnerabilities that need to be addressed based on their score. |

Các lỗ hổng được phát hiện trong quá trìnhhai bước đầu tiên của quá trình nàythường đông hơn số người có thể sửa chúng.Đánh giá rủi ro là một cách ưu tiên các nguồn lực đểxử lý các lỗ hổng cần khắc phụcđược giải quyết dựa trên điểm số của họ.

|  |
| --- |
| The fourth and final step of vulnerability assessment is remediation. It's during this step that the vulnerabilities that can impact the organization are addressed. Remediation occurs depending on the severity score assigned during the risk assessment step. |

Bước thứ tư và cuối cùng củađánh giá lỗ hổng là biện pháp khắc phục.Chính trong bước này, các lỗ hổngcó thể tác động đến tổ chức đều được giải quyết.Việc khắc phục xảy ra tùy thuộc vàođiểm mức độ nghiêm trọng được chỉ địnhtrong bước đánh giá rủi ro.

|  |
| --- |
| This part of the process is normally a joint effort between the security staff and IT teams to come up with the best approach to fixing the vulnerabilities that were uncovered earlier. Examples of remediation steps might include things like enforcing new security procedures, updating operating systems, or implementing system patches. |

Phần này của quá trình thường đượcnỗ lực chung giữa nhân viên an ninh và CNTTcác nhóm đưa ra cách tiếp cận tốt nhất đểkhắc phục các lỗ hổng đã được phát hiện trước đó.Ví dụ về các bước khắc phục có thể bao gồmnhững việc như thực thi các thủ tục bảo mật mới,cập nhật hệ điều hành,hoặc thực hiện các bản vá hệ thống.

|  |
| --- |
| Vulnerability assessments are great for identifying the flaws of a system. Most organizations use them to search for problems before they happen. But how do we know where to search? When we get together again, we'll explore how companies figure this out. |

Đánh giá lỗ hổng là tuyệt vờiđể xác định các sai sót của một hệ thống.Hầu hết các tổ chức sử dụng chúng đểtìm kiếm các vấn đề trước khi chúng xảy ra.Nhưng làm thế nào để chúng ta biết nơi để tìm kiếm?Khi chúng ta gặp lại nhau lần nữa, chúng ta sẽkhám phá cách các công ty tìm ra điều này.

***2.2. Approaches to vulnerability scanning - Các phương pháp quét lỗ hổng***

|  |
| --- |
| **Approaches to vulnerability scanning** |

**Các phương pháp quét lỗ hổng**

|  |
| --- |
| Previously, you learned about a **vulnerability assessment**, which is the internal review process of an organization's security systems. An organization performs vulnerability assessments to identify weaknesses and prevent attacks. Vulnerability scanning tools are commonly used to simulate threats by finding vulnerabilities in an attack surface. They also help security teams take proactive steps towards implementing their remediation strategy. |

Trước đây, bạn đã tìm hiểu về **đánh giá lỗ hổng bảo mật** , là quy trình đánh giá nội bộ hệ thống bảo mật của một tổ chức. Một tổ chức thực hiện đánh giá lỗ hổng để xác định điểm yếu và ngăn chặn các cuộc tấn công. Các công cụ quét lỗ hổng bảo mật thường được sử dụng để mô phỏng các mối đe dọa bằng cách tìm kiếm các lỗ hổng trên bề mặt tấn công. Họ cũng giúp các nhóm bảo mật thực hiện các bước chủ động để thực hiện chiến lược khắc phục của mình.

|  |
| --- |
| Vulnerability scanners are important tools that you'll likely use in the field. In this reading, you’ll explore how vulnerability scanners work and the types of scans they can perform. |

Máy quét lỗ hổng bảo mật là công cụ quan trọng mà bạn có thể sẽ sử dụng tại hiện trường. Trong bài đọc này, bạn sẽ khám phá cách hoạt động của các trình quét lỗ hổng và các kiểu quét mà chúng có thể thực hiện.

|  |
| --- |
| **What is a vulnerability scanner?** |

**Máy quét lỗ hổng là gì?**

|  |
| --- |
| A **vulnerability scanner** is software that automatically compares known vulnerabilities and exposures against the technologies on the network. In general, these tools scan systems to find misconfigurations or programming flaws. |

Trình **quét lỗ hổng** là phần mềm tự động so sánh các lỗ hổng và mức độ nguy hiểm đã biết với các công nghệ trên mạng. Nói chung, những công cụ này quét hệ thống để tìm cấu hình sai hoặc lỗi lập trình.

|  |
| --- |
| Scanning tools are used to analyze each of the five attack surfaces that you learned about in [the video about the defense in depth strategy](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/IdvXj/defense-in-depth-strategy):   1. **Perimeter layer**,like authentication systems that validate user access 2. **Network layer**,which is made up of technologies like network firewalls and others 3. **Endpoint layer**,which describes devices on a network, like laptops, desktops, or servers 4. **Application layer**,which involves the software that users interact with 5. **Data layer**, which includes any information that’s stored, in transit, or in use |

Các công cụ quét được sử dụng để phân tích từng bề mặt trong số năm bề mặt tấn công mà bạn đã tìm hiểu trong[Video về chiến lược phòng thủ có chiều sâu](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/IdvXj/defense-in-depth-strategy):

1. **Lớp chu vi** , giống như các hệ thống xác thực xác thực quyền truy cập của người dùng
2. **Lớp mạng** , được tạo thành từ các công nghệ như tường lửa mạng và các công nghệ khác
3. **Lớp điểm cuối** , mô tả các thiết bị trên mạng, như máy tính xách tay, máy tính để bàn hoặc máy chủ
4. **Lớp ứng dụng** , bao gồm phần mềm mà người dùng tương tác với
5. **Lớp dữ liệu** , bao gồm mọi thông tin được lưu trữ, truyền hoặc sử dụng

|  |
| --- |
| When a scan of any layer begins, the scanning tool compares the findings against databases of security threats. At the end of the scan, the tool flags any vulnerabilities that it finds and adds them to its reference database. Each scan adds more information to the database, helping the tool be more accurate in its analysis. |

Khi quá trình quét bất kỳ lớp nào bắt đầu, công cụ quét sẽ so sánh kết quả tìm thấy với cơ sở dữ liệu về các mối đe dọa bảo mật. Khi kết thúc quá trình quét, công cụ này sẽ gắn cờ mọi lỗ hổng mà nó tìm thấy và thêm chúng vào cơ sở dữ liệu tham chiếu của nó. Mỗi lần quét sẽ bổ sung thêm thông tin vào cơ sở dữ liệu, giúp công cụ phân tích chính xác hơn.

|  |
| --- |
| **Note:** Vulnerability databases are also routinely updated by the company that designed the scanning software. |

**Lưu ý:** Cơ sở dữ liệu về lỗ hổng bảo mật cũng được cập nhật thường xuyên bởi công ty thiết kế phần mềm quét.

|  |
| --- |
| **Performing scans** |

**Thực hiện quét**

|  |
| --- |
| Vulnerability scanners are meant to be non-intrusive. Meaning, they don’t break or take advantage of a system like an attacker would. Instead, they simply scan a surface and alert you to any potentially unlocked doors in your systems. |

Máy quét lỗ hổng có nghĩa là không xâm nhập. Có nghĩa là chúng không phá vỡ hoặc lợi dụng hệ thống như kẻ tấn công. Thay vào đó, chúng chỉ cần quét một bề mặt và cảnh báo bạn về bất kỳ cánh cửa nào có khả năng bị mở khóa trong hệ thống của bạn.

|  |
| --- |
| **Note:** While vulnerability scanners are non-intrusive, there are instances when a scan can inadvertently cause issues, like crash a system. |

**Lưu ý:** Mặc dù trình quét lỗ hổng không có tác dụng xâm nhập nhưng có những trường hợp quá trình quét có thể vô tình gây ra sự cố, chẳng hạn như làm hỏng hệ thống.

|  |
| --- |
| There are a few different ways that these tools are used to scan a surface. Each approach corresponds to the pathway a threat actor might take. Next, you can explore each type of scan to get a clearer picture of this. |

Có một số cách khác nhau mà các công cụ này được sử dụng để quét một bề mặt. Mỗi cách tiếp cận tương ứng với con đường mà tác nhân đe dọa có thể thực hiện. Tiếp theo, bạn có thể khám phá từng kiểu quét để có được bức tranh rõ ràng hơn về điều này.

|  |
| --- |
| **External vs. internal** |

**Bên ngoài so với nội bộ**

|  |
| --- |
| External and internal scans simulate an attacker's approach. |

Quét bên ngoài và bên trong mô phỏng cách tiếp cận của kẻ tấn công.

|  |
| --- |
| *External scans* test the perimeter layer outside of the internal network. They analyze outward facing systems, like websites and firewalls. These kinds of scans can uncover vulnerable things like vulnerable network ports or servers. |

*Quét bên ngoài* kiểm tra lớp chu vi bên ngoài mạng nội bộ. Họ phân tích các hệ thống hướng ra bên ngoài, như trang web và tường lửa. Những kiểu quét này có thể phát hiện ra những thứ dễ bị tấn công như cổng mạng hoặc máy chủ dễ bị tấn công.

|  |
| --- |
| *Internal scans* start from the opposite end by examining an organization's internal systems. For example, this type of scan might analyze application software for weaknesses in how it handles user input. |

*Quét nội bộ* bắt đầu từ đầu đối diện bằng cách kiểm tra hệ thống nội bộ của tổ chức. Ví dụ: kiểu quét này có thể phân tích phần mềm ứng dụng để tìm điểm yếu trong cách xử lý thông tin đầu vào của người dùng.

|  |
| --- |
| **Authenticated vs. unauthenticated** |

**Được xác thực và không được xác thực**

|  |
| --- |
| Authenticated and unauthenticatedscans simulate whether or not a user has access to a system. |

Quét được xác thực và không được xác thực mô phỏng xem người dùng có quyền truy cập vào hệ thống hay không.

|  |
| --- |
| *Authenticated scans* might test a system by logging in with a real user account or even with an admin account. These service accounts are used to check for vulnerabilities, like broken access controls. |

*Quét được xác thực* có thể kiểm tra hệ thống bằng cách đăng nhập bằng tài khoản người dùng thực hoặc thậm chí bằng tài khoản quản trị viên. Các tài khoản dịch vụ này được sử dụng để kiểm tra các lỗ hổng bảo mật, chẳng hạn như các biện pháp kiểm soát truy cập bị hỏng.

|  |
| --- |
| *Unauthenticated scans* simulate external threat actors that do not have access to your business resources. For example, a scan might analyze file shares within the organization that are used to house internal-only documents. Unauthenticated users should receive "access denied" results if they tried opening these files. However, a vulnerability would be identified if you were able to access a file. |

*Quá trình quét không được xác thực* sẽ mô phỏng các tác nhân đe dọa bên ngoài không có quyền truy cập vào tài nguyên doanh nghiệp của bạn. Ví dụ: quá trình quét có thể phân tích các chia sẻ tệp trong tổ chức được sử dụng để lưu trữ các tài liệu chỉ dành cho nội bộ. Người dùng chưa được xác thực sẽ nhận được kết quả "quyền truy cập bị từ chối" nếu họ cố mở các tệp này. Tuy nhiên, một lỗ hổng sẽ được xác định nếu bạn có thể truy cập một tệp.

|  |
| --- |
| **Limited vs. comprehensive** |

**Hạn chế và toàn diện**

|  |
| --- |
| Limited and comprehensive scans focus on particular devices that are accessed by internal and external users. |

Quét hạn chế và toàn diện tập trung vào các thiết bị cụ thể được người dùng nội bộ và bên ngoài truy cập.

|  |
| --- |
| *Limited scans* analyze particular devices on a network, like searching for misconfigurations on a firewall. |

*Quét giới hạn sẽ* phân tích các thiết bị cụ thể trên mạng, chẳng hạn như tìm kiếm cấu hình sai trên tường lửa.

|  |
| --- |
| *Comprehensive scans* analyze all devices connected to a network. This includes operating systems, user databases, and more. |

*Quét toàn diện* phân tích tất cả các thiết bị được kết nối với mạng. Điều này bao gồm hệ điều hành, cơ sở dữ liệu người dùng, v.v.

|  |
| --- |
| **Pro tip:** Discovery scanning should be done prior to limited or comprehensive scans. Discovery scanning is used to get an idea of the computers, devices, and open ports that are on a network. |

**Mẹo chuyên nghiệp:** Quét khám phá phải được thực hiện trước khi quét giới hạn hoặc toàn diện. Quét khám phá được sử dụng để lấy ý tưởng về máy tính, thiết bị và các cổng mở trên mạng.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Finding vulnerabilities requires thinking of all possibilities. Vulnerability scans vary depending on the surfaces that an organization is evaluating. Usually, seasoned security professionals lead the effort of configuring and performing these types of scans to create a profile of a company’s security posture. However, analysts also play an important role in the process. The results of a vulnerability scan often lead to renewed compliance efforts, procedural changes, and system patching. Understanding the objectives of common types of vulnerability scans will help you participate in these proactive security exercises whenever possible. |

Việc tìm kiếm các lỗ hổng đòi hỏi phải suy nghĩ về tất cả các khả năng. Việc quét lỗ hổng bảo mật khác nhau tùy thuộc vào bề mặt mà tổ chức đang đánh giá. Thông thường, các chuyên gia bảo mật dày dạn kinh nghiệm sẽ nỗ lực định cấu hình và thực hiện các kiểu quét này để tạo hồ sơ về tình hình bảo mật của công ty. Tuy nhiên, các nhà phân tích cũng đóng một vai trò quan trọng trong quá trình này. Kết quả quét lỗ hổng thường dẫn đến những nỗ lực tuân thủ mới, thay đổi quy trình và vá lỗi hệ thống. Hiểu mục tiêu của các loại quét lỗ hổng phổ biến sẽ giúp bạn tham gia vào các hoạt động bảo mật chủ động này bất cứ khi nào có thể.

|  |
| --- |
| **Tip:** To explore vulnerability scanner software commonly used in the cybersecurity industry, in your preferred browser enter search terms similar to “popular vulnerability scanner software” and/or “open source vulnerability scanner software used in cybersecurity”. |

**Mẹo:** Để khám phá phần mềm quét lỗ hổng thường được sử dụng trong ngành an ninh mạng, trong trình duyệt ưa thích của bạn, hãy nhập cụm từ tìm kiếm tương tự như “phần mềm quét lỗ hổng phổ biến” và/hoặc “phần mềm quét lỗ hổng nguồn mở được sử dụng trong an ninh mạng”.

***2.3. The importance of updates - Tầm quan trọng của các bản cập nhật***

|  |
| --- |
| **The importance of updates** |

**Tầm quan trọng của các bản cập nhật**

|  |
| --- |
| At some point in time, you may have wondered, “Why do my devices constantly need updating?” For consumers, updates provide improvements to performance, stability, and even new features! But from a security standpoint, they serve a specific purpose. Updates allow organizations to address security vulnerabilities that can place their users, devices, and networks at risk. |

Tại một thời điểm nào đó, bạn có thể thắc mắc: “Tại sao thiết bị của tôi liên tục cần cập nhật?” Đối với người tiêu dùng, các bản cập nhật mang lại những cải tiến về hiệu suất, độ ổn định và thậm chí cả các tính năng mới! Nhưng từ quan điểm bảo mật, chúng phục vụ một mục đích cụ thể. Các bản cập nhật cho phép các tổ chức giải quyết các lỗ hổng bảo mật có thể khiến người dùng, thiết bị và mạng của họ gặp rủi ro.

|  |
| --- |
| In a video, you learned that updates fit into every security team’s remediation strategy. They usually take place after a **vulnerability assessment**, which is the internal review process of an organization's security systems. In this reading, you’ll learn what updates do, how they’re delivered, and why they’re important to cybersecurity. |

Trong một video, bạn đã biết rằng các bản cập nhật phù hợp với chiến lược khắc phục của mọi nhóm bảo mật. Chúng thường diễn ra sau khi **đánh giá lỗ hổng** , đây là quy trình đánh giá nội bộ về hệ thống bảo mật của tổ chức. Trong bài đọc này, bạn sẽ tìm hiểu tác dụng của các bản cập nhật, cách chúng được phân phối và lý do chúng quan trọng đối với an ninh mạng.

|  |
| --- |
| **Patching gaps in security** |

**Vá các lỗ hổng trong bảo mật**

|  |
| --- |
| An outdated computer is a lot like a house with unlocked doors. Malicious actors use these gaps in security the same way, to gain unauthorized access. Software updates are similar to locking the doors to keep them out. |

Một chiếc máy tính lỗi thời cũng giống như một ngôi nhà không khóa cửa. Những kẻ độc hại sử dụng những lỗ hổng bảo mật này theo cách tương tự để có được quyền truy cập trái phép. Cập nhật phần mềm tương tự như việc khóa cửa để ngăn chúng ra ngoài.

|  |
| --- |
| A **patch update** is a software and operating system update that addresses security vulnerabilities within a program or product. Patches usually contain bug fixes that address common security vulnerabilities and exposures. |

Bản **cập nhật bản vá** là bản cập nhật phần mềm và hệ điều hành nhằm giải quyết các lỗ hổng bảo mật trong một chương trình hoặc sản phẩm. Các bản vá thường chứa các bản sửa lỗi nhằm giải quyết các lỗ hổng và lỗ hổng bảo mật phổ biến.

|  |
| --- |
| **Note:** Ideally, patches address common vulnerabilities and exposures before malicious hackers find them. However, patches are sometimes developed as a result of a **zero-day**, which is an exploit that was previously unknown. |

**Lưu ý:** Lý tưởng nhất là các bản vá giải quyết các lỗ hổng và nguy cơ phổ biến trước khi các tin tặc độc hại tìm thấy chúng. Tuy nhiên, các bản vá đôi khi được phát triển do lỗi **zero-day** , đây là một cách khai thác mà trước đây chưa được biết đến.

|  |
| --- |
| **Common update strategies** |

**Các chiến lược cập nhật phổ biến**

|  |
| --- |
| When software updates become available, clients and users have two installation options:   * Manual updates * Automatic updates |

Khi có bản cập nhật phần mềm, máy khách và người dùng có hai tùy chọn cài đặt:

* Cập nhật thủ công
* Cập nhật tự động

|  |
| --- |
| As you’ll learn, each strategy has both benefits and disadvantages. |

Khi bạn tìm hiểu, mỗi chiến lược đều có cả lợi ích và bất lợi.

|  |
| --- |
| **Manual updates** |

**Cập nhật thủ công**

|  |
| --- |
| A manual deployment strategy relies on IT departments or users obtaining updates from the developers. Home office or small business environments might require you to find, download, and install updates yourself. In enterprise settings, the process is usually handled with a configuration management tool. These tools offer a range of options to deploy updates, like to all clients on your network or a select group of users. |

Chiến lược triển khai thủ công phụ thuộc vào việc bộ phận CNTT hoặc người dùng nhận được thông tin cập nhật từ nhà phát triển. Môi trường văn phòng tại nhà hoặc doanh nghiệp nhỏ có thể yêu cầu bạn tự tìm, tải xuống và cài đặt các bản cập nhật. Trong cài đặt doanh nghiệp, quy trình này thường được xử lý bằng công cụ quản lý cấu hình. Những công cụ này cung cấp nhiều tùy chọn để triển khai các bản cập nhật, chẳng hạn như cho tất cả khách hàng trên mạng của bạn hoặc một nhóm người dùng được chọn.

|  |
| --- |
| **Advantage:** An advantage of manual update deployment strategies is control. That can be useful if software updates are not thoroughly tested by developers, leading to instability issues. |

**Ưu điểm:** Ưu điểm của chiến lược triển khai cập nhật thủ công là khả năng kiểm soát. Điều đó có thể hữu ích nếu các bản cập nhật phần mềm không được nhà phát triển kiểm tra kỹ lưỡng, dẫn đến các vấn đề không ổn định.

|  |
| --- |
| **Disadvantage:** A drawback to manual update deployments is that critical updates can be forgotten or disregarded entirely. |

**Nhược điểm:** Hạn chế của việc triển khai cập nhật thủ công là các cập nhật quan trọng có thể bị quên hoặc bị bỏ qua hoàn toàn.

|  |
| --- |
| **Automatic updates** |

**Cập nhật tự động**

|  |
| --- |
| An automatic deployment strategy takes the opposite approach. With this option, finding, downloading, and installing updates can be done by the system or application. |

Chiến lược triển khai tự động có cách tiếp cận ngược lại. Với tùy chọn này, hệ thống hoặc ứng dụng có thể thực hiện việc tìm kiếm, tải xuống và cài đặt các bản cập nhật.

|  |
| --- |
| **Pro tip:** The Cybersecurity and Infrastructure Security Agency (CISA) recommends using automatic options whenever they’re available. |

**Mẹo chuyên nghiệp:** Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) khuyến nghị sử dụng các tùy chọn tự động bất cứ khi nào chúng có sẵn.

|  |
| --- |
| Certain permissions need to be enabled by users or IT groups before updates can be installed, or pushed, when they're available. It is up to the developers to adequately test their patches before release. |

Người dùng hoặc nhóm CNTT cần phải bật một số quyền nhất định trước khi có thể cài đặt hoặc đẩy các bản cập nhật khi chúng có sẵn. Các nhà phát triển có trách nhiệm kiểm tra đầy đủ các bản vá của họ trước khi phát hành.

|  |
| --- |
| **Advantage:** An advantage to automatic updates is that the deployment process is simplified. It also keeps systems and software current with the latest, critical patches. |

**Ưu điểm:** Ưu điểm của cập nhật tự động là quá trình triển khai được đơn giản hóa. Nó cũng cập nhật các hệ thống và phần mềm với các bản vá quan trọng, mới nhất.

|  |
| --- |
| **Disadvantage:** A drawback to automatic updates is that instability issues can occur if the patches were not thoroughly tested by the vendor. This can result in performance problems and a poor user experience. |

**Nhược điểm:** Hạn chế của cập nhật tự động là vấn đề không ổn định có thể xảy ra nếu các bản vá không được nhà cung cấp kiểm tra kỹ lưỡng. Điều này có thể dẫn đến các vấn đề về hiệu suất và trải nghiệm người dùng kém.

|  |
| --- |
| **End-of-life software** |

**Phần mềm hết hạn sử dụng**

|  |
| --- |
| Sometimes updates are not available for a certain type of software known as end-of-life (EOL) software. All software has a lifecycle. It begins when it’s produced and ends when a newer version is released. At that point, developers must allocate resources to the newer versions, which leads to EOL software. While the older software is still useful, the manufacturer no longer supports it. |

Đôi khi không có bản cập nhật cho một loại phần mềm nhất định được gọi là phần mềm hết hạn sử dụng (EOL). Tất cả phần mềm đều có vòng đời. Nó bắt đầu khi nó được sản xuất và kết thúc khi phiên bản mới hơn được phát hành. Khi đó, các nhà phát triển phải phân bổ tài nguyên cho các phiên bản mới hơn, dẫn đến phần mềm EOL. Mặc dù phần mềm cũ vẫn còn hữu ích nhưng nhà sản xuất không còn hỗ trợ nữa.

|  |
| --- |
| **Note:** Patches and updates are very different from upgrades. *Upgrades* refer to completely new versions of hardware or software that can be purchased. |

**Lưu ý:** Các bản vá và cập nhật rất khác với các bản nâng cấp. *Nâng cấp* đề cập đến các phiên bản phần cứng hoặc phần mềm hoàn toàn mới có thể mua được.

|  |
| --- |
| [CISA recommends discontinuing the use of EOL software](https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates) because it poses an unfixable risk to systems. But, this recommendation is not always followed. Replacing EOL technology can be costly for businesses and individual users. |

[CISA khuyến nghị ngừng sử dụng phần mềm EOL](https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates)bởi vì nó gây ra rủi ro không thể khắc phục được cho hệ thống. Tuy nhiên, khuyến nghị này không phải lúc nào cũng được tuân theo. Việc thay thế công nghệ EOL có thể gây tốn kém cho doanh nghiệp và người dùng cá nhân.

|  |
| --- |
| The risks that EOL software presents continues to grow as more connected devices enter the marketplace. For example, there are billions of Internet of Things (IoT) devices, like smart light bulbs, connected to home and work networks. In some business settings, all an attacker needs is a single unpatched device to gain access to the network and cause problems. |

Những rủi ro mà phần mềm EOL mang lại tiếp tục gia tăng khi ngày càng có nhiều thiết bị được kết nối tham gia vào thị trường. Ví dụ: có hàng tỷ thiết bị Internet of Things (IoT), như bóng đèn thông minh, được kết nối với mạng gia đình và cơ quan. Trong một số cài đặt doanh nghiệp, tất cả những gì kẻ tấn công cần là một thiết bị chưa được vá lỗi để có quyền truy cập vào mạng và gây ra sự cố.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Updating software and patching vulnerabilities is an important practice that everyone should participate in. Unfortunately, that’s not always the case. Many of the biggest cyber attacks in the world might have been prevented if systems were kept updated. One example is the WannaCry attack of 2017. The attack affected computers in more than 150 countries and caused an estimated $4 billion dollars in damages. Researchers have since found that WannaCry could have been prevented if the infected systems were up-to-date with a security patch that was made available months before the attack. Keeping software updated requires effort. However, the benefits they provide make them worthwhile. |

Cập nhật phần mềm và vá các lỗ hổng bảo mật là một hoạt động quan trọng mà mọi người nên tham gia. Thật không may, không phải lúc nào cũng như vậy. Nhiều cuộc tấn công mạng lớn nhất trên thế giới có thể đã được ngăn chặn nếu hệ thống được cập nhật liên tục. Một ví dụ là cuộc tấn công WannaCry năm 2017. Cuộc tấn công đã ảnh hưởng đến máy tính ở hơn 150 quốc gia và gây thiệt hại ước tính khoảng 4 tỷ đô la. Kể từ đó, các nhà nghiên cứu đã phát hiện ra rằng WannaCry có thể được ngăn chặn nếu các hệ thống bị nhiễm được cập nhật bản vá bảo mật được cung cấp vài tháng trước cuộc tấn công. Việc cập nhật phần mềm đòi hỏi nỗ lực. Tuy nhiên, những lợi ích mà chúng mang lại khiến chúng trở nên đáng giá.

***2.4. Omad: My learning journey into cybersecurity - Omad: Hành trình học tập của tôi về an ninh mạng***

|  |
| --- |
| [MUSIC] My name is Omad, I'm a corporate operations engineer at Google. All I do is solve problems. Googlers have problems, they need somebody to talk to, they usually talk to us. If you asked me at 18 years old where I'd be now, I would have never told you I'd be working as a security engineer. I would have told you I'd be working in a prison or I'd be working as a police officer in some township and just working a regular 9 to 5 shift. After high school, I went on to work at Trenton State Prison, which is the only maximum security prison in New Jersey. It was very stressful, but at the same time it's what I wanted to do at the time, or at least, that's what I thought I wanted to do at that time. Five years after becoming a correction officer, I took the test again to be a sheriff's officer. And on the last day of that academy, I decided this wasn't for me. I was tired of being on my face doing pushups, I was tired of being yelled at. I went home and I did what everybody else would do, do a Google search. And I saw one for Google and it was a residency program, it was at the top of the list and I applied to it as a joke. I even told my friends at the time, I'm just going to apply this, I'm not going to get in. I had no reference, no connections, I knew nobody that worked at Google. And within a couple of days a recruiter reached out to me, she said, "I think you're a great fit, you're a career changer. I like your application, I like your resume, I think you'd be a great fit." All the interviewers liked my background, they liked that I was self taught. A lot of interviewers were able to relate to me. They said, "Hey, I did the same thing." From there, I was offered the job and I started my career. When I was in orientation, somebody right next to me was actually the valedictorian of Princeton. Here I am with no college degree, no exposure, no work experience, and I'm in the same company. For career changers, what you have that other people don't have is a different mindset. You're coming from experience outside of the technical space that you can transfer into the technical space. Don't forget that we all have skillsets that can help you in the field. That's what employers are looking for, that's what hiring managers are looking for. One thing I learned as a correction officer is how to assess risk. Every situation is different, just like the security space. Every risk is different. Every vulnerability is different. Every threat is different. You can teach somebody tech, but you can't teach them a life of skills outside of tech. If I were to go back and tell my 18 year old self one piece of advice, it would be, don't be scared, do it. A career in cybersecurity is very fun. It's very interesting. It will work your brain. It changed my life, it'll change yours as well. |

[ÂM NHẠC]Tên tôi là Omad, tôi là kỹ sư vận hành công ty tại Google.Tất cả những gì tôi làm là giải quyết vấn đề.Nhân viên của Google gặp vấn đề, họ cần ai đó để nói chuyện, họ thường nói chuyện với chúng tôi.Nếu bạn hỏi tôi lúc 18 tuổi, bây giờ tôi đang ở đâu,Tôi chưa bao giờ nói với bạn rằng tôi sẽ làm kỹ sư an ninh.Lẽ ra tôi sẽ nói với bạn rằng tôi sẽ làm việc trong nhà tù hoặc tôi sẽ làm việclà một sĩ quan cảnh sát ở một thị trấn nào đó và chỉ làm việc theo ca từ 9 đến 5 giờ bình thường.Sau khi tốt nghiệp trung học, tôi tiếp tục làm việc ở nhà tù bang Trenton,đó là nhà tù an ninh tối đa duy nhất ở New Jersey.Điều đó rất căng thẳng, nhưng đồng thời đó cũng là điều tôi muốn làm vào thời điểm đó,hoặc ít nhất đó là điều tôi nghĩ mình muốn làm vào thời điểm đó.Năm năm sau khi trở thành sĩ quan cải huấn,Tôi lại làm bài kiểm tra để trở thành cảnh sát trưởng.Và vào ngày cuối cùng ở học viện đó, tôi đã quyết định rằng đây không phải là nơi dành cho tôi.Tôi mệt mỏi với việc chống đẩy trên mặt, tôi mệt mỏi vì bị la mắng.Tôi về nhà và làm điều mà mọi người vẫn làm, đó là tìm kiếm trên Google.Và tôi đã thấy một chương trình dành cho Google và đó là một chương trình cư trú,nó đứng đầu danh sách và tôi coi nó như một trò đùa.Lúc đó tôi thậm chí còn nói với bạn bè rằng, tôi sẽ áp dụng điều này,Tôi sẽ không vào.Tôi không có tài liệu tham khảo, không có mối quan hệ, tôi không biết ai làm việc tại Google.Và trong vòng vài ngày, một nhà tuyển dụng đã liên hệ với tôi, cô ấy nói,"Tôi nghĩ bạn rất phù hợp, bạn là người có thể thay đổi nghề nghiệp.Tôi thích đơn ứng tuyển của bạn, tôi thích sơ yếu lý lịch của bạn, tôi nghĩ bạn sẽ rất phù hợp."Tất cả những người phỏng vấn đều thích nền tảng của tôi, họ thích việc tôi tự học.Rất nhiều người phỏng vấn có thể liên hệ với tôi.Họ nói: "Này, tôi cũng làm điều tương tự."Từ đó, tôi được mời làm việc và bắt đầu sự nghiệp của mình.Khi tôi đang định hướng,ai đó ngay bên cạnh tôi thực ra là thủ khoa của Princeton.Ở đây tôi không có bằng đại học, không có kinh nghiệm làm việc, vàTôi ở cùng công ty.Đối với những người thay đổi nghề nghiệp,những gì bạn có mà người khác không có là một tư duy khác.Bạn đến từ kinh nghiệm bên ngoài không gian kỹ thuật mà bạn có thể chuyển giaovào không gian kỹ thuật.Đừng quên rằng tất cả chúng ta đều có những kỹ năng có thể giúp bạn trong lĩnh vực này.Đó là những gì nhà tuyển dụng đang tìm kiếm,đó là những gì các nhà quản lý tuyển dụng đang tìm kiếm.Một điều tôi học được khi làm nhân viên cải huấn là cách đánh giá rủi ro.Mọi tình huống đều khác nhau, giống như không gian an ninh. Mỗi rủi ro đềukhác biệt. Mỗi lỗ hổng đều khác nhau. Mỗi mối đe dọa đều khác nhau.Bạn có thể dạy ai đó về công nghệ, nhưngbạn không thể dạy họ một cuộc sống với những kỹ năng bên ngoài công nghệ.Nếu tôi được quay lại và nói với bản thân mình năm 18 tuổi một lời khuyên, thì đó sẽ là,đừng sợ, hãy làm đi.Nghề nghiệp trong lĩnh vực an ninh mạng rất thú vị.Nó rất thú vị.Nó sẽ hoạt động trí não của bạn.Nó đã thay đổi cuộc đời tôi, nó cũng sẽ thay đổi cuộc đời bạn.

***2.5. Penetration testing - Kiểm tra thâm nhập***

|  |
| --- |
| **Penetration testing** |

**Kiểm tra thâm nhập**

|  |
| --- |
| An effective security plan relies on regular testing to find an organization's weaknesses. Previously, you learned that **vulnerability assessments**, the internal review process of an organization's security systems, are used to design defense strategies based on system weaknesses. In this reading, you'll learn how security teams evaluate the effectiveness of their defenses using penetration testing. |

Một kế hoạch bảo mật hiệu quả dựa vào việc kiểm tra thường xuyên để tìm ra điểm yếu của tổ chức. Trước đây, bạn đã biết rằng **đánh giá lỗ hổng** , quy trình đánh giá nội bộ hệ thống bảo mật của tổ chức, được sử dụng để thiết kế các chiến lược phòng thủ dựa trên điểm yếu của hệ thống. Trong bài đọc này, bạn sẽ tìm hiểu cách các nhóm bảo mật đánh giá hiệu quả của biện pháp phòng thủ của họ bằng cách sử dụng thử nghiệm thâm nhập.

|  |
| --- |
| **Penetration testing** |

**Kiểm tra thâm nhập**

|  |
| --- |
| A **penetration test**, or pen test, is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. The simulated attack in a pen test involves using the same tools and techniques as malicious actors in order to mimic a real life attack. Since a pen test is an authorized attack, it is considered to be a form of ethical hacking. Unlike a vulnerability assessment that finds weaknesses in a system's security, a pen test exploits those weaknesses to determine the potential consequences if the system breaks or gets broken into by a threat actor. |

Kiểm **tra thâm nhập** hoặc kiểm tra bút là một cuộc tấn công mô phỏng giúp xác định các lỗ hổng trong hệ thống, mạng, trang web, ứng dụng và quy trình. Cuộc tấn công mô phỏng trong thử nghiệm bút bao gồm việc sử dụng các công cụ và kỹ thuật tương tự như các tác nhân độc hại để bắt chước một cuộc tấn công ngoài đời thực. Vì pentest là một cuộc tấn công được ủy quyền nên nó được coi là một hình thức hack có đạo đức. Không giống như đánh giá lỗ hổng nhằm tìm ra điểm yếu trong bảo mật của hệ thống, pen test khai thác những điểm yếu đó để xác định hậu quả tiềm ẩn nếu hệ thống bị hỏng hoặc bị kẻ đe dọa xâm nhập.

|  |
| --- |
| For example, the cybersecurity team at a financial company might simulate an attack on their banking app to determine if there are weaknesses that would allow an attacker to steal customer information or illegally transfer funds. If the pen test uncovers misconfigurations, the team can address them and improve the overall security of the app. |

Ví dụ: nhóm an ninh mạng tại một công ty tài chính có thể mô phỏng một cuộc tấn công vào ứng dụng ngân hàng của họ để xác định xem có điểm yếu nào cho phép kẻ tấn công đánh cắp thông tin khách hàng hoặc chuyển tiền bất hợp pháp hay không. Nếu quá trình kiểm tra bút phát hiện ra các cấu hình sai, nhóm có thể giải quyết chúng và cải thiện tính bảo mật tổng thể của ứng dụng.

|  |
| --- |
| **Note:** Organizations that are regulated by PCI DSS, HIPAA, or GDPR must routinely perform penetration testing to maintain compliance standards. |

**Lưu ý:** Các tổ chức được quản lý bởi PCI DSS, HIPAA hoặc GDPR phải thường xuyên thực hiện thử nghiệm thâm nhập để duy trì các tiêu chuẩn tuân thủ.

|  |
| --- |
| **Learning from varied perspectives** |

**Học từ nhiều góc độ khác nhau**

|  |
| --- |
| These authorized attacks are performed by pen testers who are skilled in programming and network architecture. Depending on their objectives, organizations might use a few different approaches to penetration testing:   * Red team tests *simulate attacks* to identify vulnerabilities in systems, networks, or applications. * Blue team tests focus on *defense* *and incident response* to validate an organization's existing security systems. * Purple team tests are *collaborative*, focusing on improving the security posture of the organization by combining elements of red and blue team exercises. |

Các cuộc tấn công được ủy quyền này được thực hiện bởi những người kiểm tra bút có kỹ năng lập trình và kiến ​​trúc mạng. Tùy thuộc vào mục tiêu của họ, các tổ chức có thể sử dụng một số cách tiếp cận khác nhau để thử nghiệm thâm nhập:

* Các thử nghiệm của đội đỏ *mô phỏng các cuộc tấn công* để xác định các lỗ hổng trong hệ thống, mạng hoặc ứng dụng.
* Các thử nghiệm của đội xanh tập trung vào *phòng thủ và ứng phó sự cố* để xác thực hệ thống bảo mật hiện có của tổ chức.
* Các bài kiểm tra của đội màu tím mang *tính hợp tác* , tập trung vào việc cải thiện tình hình bảo mật của tổ chức bằng cách kết hợp các yếu tố trong bài tập của đội đỏ và xanh.

|  |
| --- |
| Red team tests are commonly performed by independent pen testers who are hired to evaluate internal systems. Although, cybersecurity teams may also have their own pen testing experts. Regardless of the approach, penetration testers must make an important decision before simulating an attack: *How much access and information do I need?* |

Các bài kiểm tra của đội đỏ thường được thực hiện bởi những người kiểm tra bút độc lập được thuê để đánh giá hệ thống nội bộ. Mặc dù vậy, các nhóm an ninh mạng cũng có thể có chuyên gia kiểm tra bút của riêng họ. Bất kể cách tiếp cận nào, người kiểm tra thâm nhập đều phải đưa ra quyết định quan trọng trước khi mô phỏng một cuộc tấn công: *Tôi cần bao nhiêu quyền truy cập và thông tin?*

|  |
| --- |
| **Penetration testing strategies** |

**Chiến lược thử nghiệm thâm nhập**

|  |
| --- |
| There are three common penetration testing strategies:   * **Open-box testing** is when the tester has the same privileged access that an internal developer would have—information like system architecture, data flow, and network diagrams. This strategy goes by several different names, including internal, full knowledge, white-box, and clear-box penetration testing. * **Closed-box testing** is when the tester has little to no access to internal systems—similar to a malicious hacker. This strategy is sometimes referred to as external, black-box, or zero knowledge penetration testing. * **Partial knowledge testing** is when the tester has limited access and knowledge of an internal system—for example, a customer service representative. This strategy is also known as gray-box testing. |

Có ba chiến lược thử nghiệm thâm nhập phổ biến:

* **Thử nghiệm hộp mở** là khi người thử nghiệm có cùng quyền truy cập đặc quyền mà nhà phát triển nội bộ sẽ có—thông tin như kiến ​​trúc hệ thống, luồng dữ liệu và sơ đồ mạng. Chiến lược này có nhiều tên khác nhau, bao gồm thử nghiệm thâm nhập nội bộ, kiến ​​thức đầy đủ, hộp trắng và hộp rõ ràng.
* **Kiểm thử hộp kín** là khi người kiểm tra có ít hoặc không có quyền truy cập vào hệ thống nội bộ—tương tự như một hacker độc hại. Chiến lược này đôi khi được gọi là thử nghiệm thâm nhập bên ngoài, hộp đen hoặc không có kiến ​​thức.
* **Kiểm tra kiến ​​thức một phần** là khi người kiểm tra có quyền truy cập và kiến ​​thức hạn chế về hệ thống nội bộ—ví dụ: đại diện dịch vụ khách hàng. Chiến lược này còn được gọi là thử nghiệm hộp xám.

|  |
| --- |
| Closed box testers tend to produce the most accurate simulations of a real-world attack. Nevertheless, each strategy produces valuable results by demonstrating how an attacker might infiltrate a system and what information they could access. |

Những người thử nghiệm hộp kín có xu hướng tạo ra những mô phỏng chính xác nhất về một cuộc tấn công trong thế giới thực. Tuy nhiên, mỗi chiến lược đều tạo ra kết quả có giá trị bằng cách chứng minh cách kẻ tấn công có thể xâm nhập vào hệ thống và những thông tin chúng có thể truy cập.

|  |
| --- |
| **Becoming a penetration tester** |

**Trở thành người thử nghiệm thâm nhập**

|  |
| --- |
| Penetration testers are in-demand in the fast growing field of cybersecurity. All of the skills you’re learning in this program can help you advance towards a career in pen testing:   * Network and application security * Experience with operating systems, like Linux * Vulnerability analysis and threat modeling * Detection and response tools * Programming languages, like Python and BASH * Communication skills |

Người thử nghiệm thâm nhập đang có nhu cầu trong lĩnh vực an ninh mạng đang phát triển nhanh chóng. Tất cả các kỹ năng bạn đang học trong chương trình này có thể giúp bạn tiến tới sự nghiệp kiểm tra bút:

* Bảo mật mạng và ứng dụng
* Có kinh nghiệm làm việc với các hệ điều hành như Linux
* Phân tích lỗ hổng và mô hình hóa mối đe dọa
* Công cụ phát hiện và phản hồi
* Ngôn ngữ lập trình, như Python và BASH
* Kĩ năng giao tiếp

|  |
| --- |
| Programming skills are very helpful in penetration testing because it's often performed on software and IT systems. With enough practice and dedication, cybersecurity professionals at any level can develop the skills needed to be a pen tester. |

Kỹ năng lập trình rất hữu ích trong thử nghiệm thâm nhập vì nó thường được thực hiện trên phần mềm và hệ thống CNTT. Với đủ thực hành và cống hiến, các chuyên gia an ninh mạng ở mọi cấp độ đều có thể phát triển các kỹ năng cần thiết để trở thành người kiểm tra bút.

|  |
| --- |
| **Bug bounty programs** |

**Chương trình thưởng lỗi**

|  |
| --- |
| Organizations commonly run bug bounty programs which offer freelance pen testers financial rewards for finding and reporting vulnerabilities in their products. Bug bounties are great opportunities for amateur security professionals to participate and grow their skills. |

Các tổ chức thường chạy các chương trình tiền thưởng lỗi nhằm cung cấp phần thưởng tài chính cho những người thử nghiệm bút tự do để tìm và báo cáo các lỗ hổng trong sản phẩm của họ. Tiền thưởng lỗi là cơ hội tuyệt vời cho các chuyên gia bảo mật nghiệp dư tham gia và phát triển kỹ năng của họ.

|  |
| --- |
| **Pro tip:** [HackerOne](https://hackerone.com/bug-bounty-programs) is a community of ethical hackers where you can find active bug bounties to participate in. |

**Mẹo chuyên nghiệp:** [HackerOne](https://hackerone.com/bug-bounty-programs)là một cộng đồng các hacker có đạo đức, nơi bạn có thể tìm thấy các phần thưởng lỗi đang hoạt động để tham gia.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| A major risk for organizations is malicious hackers breaking into their systems. Penetration testing is another way for organizations to secure their systems. Security teams use these simulated attacks to get a clearer picture of weaknesses in their defenses. There’s a growing need for specialized security professionals in this field. Even if you start out assisting with these activities, there’s plenty of opportunities to grow and learn the skills to be a pen tester. |

Rủi ro lớn đối với các tổ chức là tin tặc độc hại xâm nhập vào hệ thống của họ. Kiểm tra thâm nhập là một cách khác để các tổ chức bảo mật hệ thống của họ. Các đội bảo mật sử dụng các cuộc tấn công mô phỏng này để có được bức tranh rõ ràng hơn về những điểm yếu trong hệ thống phòng thủ của họ. Nhu cầu về các chuyên gia bảo mật chuyên ngành trong lĩnh vực này ngày càng tăng. Ngay cả khi bạn bắt đầu hỗ trợ những hoạt động này, vẫn có rất nhiều cơ hội để phát triển và học hỏi các kỹ năng để trở thành người thử bút.

***2.6. Test your knowledge: Identify system vulnerabilities - Kiểm tra kiến ​​thức của bạn: Xác định lỗ hổng hệ thống***

***2.7. Portfolio Activity: Analyze a vulnerable system for a small business - Hoạt động danh mục đầu tư: Phân tích hệ thống dễ bị tổn thương cho một doanh nghiệp nhỏ***

|  |
| --- |
| **Activity Overview**  In this activity, you will conduct a vulnerability assessment for a small business. A vulnerability assessment is the internal review process of an organization’s security systems. You will evaluate the risks of a vulnerable information system and outline a remediation plan.  As a cybersecurity analyst, you might help with vulnerability assessments to prevent attacks in an organization. Later, you can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, review the [Create a cybersecurity portfolio](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/resources/U9Fja) topic.  Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ tiến hành đánh giá lỗ hổng cho một doanh nghiệp nhỏ. Đánh giá lỗ hổng bảo mật là quá trình xem xét nội bộ hệ thống bảo mật của một tổ chức. Bạn sẽ đánh giá rủi ro của một hệ thống thông tin dễ bị tấn công và vạch ra kế hoạch khắc phục.

Với tư cách là nhà phân tích an ninh mạng, bạn có thể trợ giúp đánh giá lỗ hổng bảo mật nhằm ngăn chặn các cuộc tấn công trong tổ chức. Sau đó, bạn có thể thêm tài liệu này vào danh mục an ninh mạng của mình để có thể chia sẻ tài liệu này với các nhà tuyển dụng hoặc nhà tuyển dụng tiềm năng. Để xem xét tầm quan trọng của việc xây dựng danh mục đầu tư chuyên nghiệp và các lựa chọn để tạo danh mục đầu tư của bạn, hãy xem lại[Tạo danh mục đầu tư an ninh mạng](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/resources/U9Fja)đề tài.

Hãy chắc chắn hoàn thành hoạt động này và trả lời các câu hỏi tiếp theo trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the following scenario. Then complete the step-by-step instructions.  You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.  You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured. |

**Kịch bản**

Xem lại tình huống sau. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn là nhà phân tích an ninh mạng mới được tuyển dụng cho một công ty thương mại điện tử. Công ty lưu trữ thông tin trên một máy chủ cơ sở dữ liệu từ xa vì nhiều nhân viên làm việc từ xa từ khắp nơi trên thế giới. Nhân viên của công ty thường xuyên truy vấn hoặc yêu cầu dữ liệu từ máy chủ để tìm kiếm khách hàng tiềm năng. Cơ sở dữ liệu đã được mở cho công chúng kể từ khi công ty ra mắt cách đây ba năm. Là một chuyên gia an ninh mạng, bạn nhận ra rằng việc để máy chủ cơ sở dữ liệu mở cho công chúng là một lỗ hổng nghiêm trọng.

Bạn được giao nhiệm vụ hoàn thành đánh giá tình huống dễ bị tổn thương để truyền đạt những rủi ro tiềm ẩn cho những người ra quyết định tại công ty. Bạn phải tạo một báo cáo bằng văn bản giải thích mức độ rủi ro của máy chủ dễ bị tấn công đối với hoạt động kinh doanh và cách bảo mật nó.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

Làm theo hướng dẫn để hoàn thành từng bước của hoạt động. Sau đó, trả lời 5 câu hỏi ở cuối hoạt động trước khi chuyển sang mục khóa học tiếp theo để so sánh bài làm của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Part 1 - Open a report template** |

**Phần 1 - Mở mẫu báo cáo**

|  |
| --- |
| **Step 1: Access the template**  Use the following template to construct your written report.  To use the template for this course item:   * Click the following link and select *Use Template*:  [Vulnerability assessment report](https://docs.google.com/document/d/1GYQchjHbuWYhl1VLb6jBuCJRsXSDjc9msoOAQPxq_wQ/template/preview?usp=sharing). |

**Bước 1: Truy cập mẫu**

Sử dụng mẫu sau để xây dựng báo cáo bằng văn bản của bạn.

Để sử dụng mẫu cho mục khóa học này:

* Nhấp vào liên kết sau và chọn *Sử dụng mẫu* :  [Báo cáo đánh giá lỗ hổng](https://docs.google.com/document/d/1GYQchjHbuWYhl1VLb6jBuCJRsXSDjc9msoOAQPxq_wQ/template/preview?usp=sharing).

|  |
| --- |
| **Step 2: Access supporting materials**  The following materials will help you complete this activity. Keep them open as you proceed to the next steps. You will use this resource in Part 2 of this activity.  To use the supporting materials for this course item:   * Click the following link and select *Use Template*: [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?resourcekey=0-3GRRWAd8HryVgof-Jc33yA). |

**Bước 2: Truy cập tài liệu hỗ trợ**

Các tài liệu sau đây sẽ giúp bạn hoàn thành hoạt động này. Giữ chúng mở khi bạn tiến hành các bước tiếp theo. Bạn sẽ sử dụng tài nguyên này trong Phần 2 của hoạt động này.

Để sử dụng các tài liệu hỗ trợ cho mục khóa học này:

* Nhấp vào liên kết sau và chọn *Sử dụng mẫu* :[NIST SP 800-30 Phiên bản 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?resourcekey=0-3GRRWAd8HryVgof-Jc33yA).

|  |
| --- |
| **Step 3: Review information about the vulnerable server**  In this activity, we have provided you with the **System Description** and **Scope** of the *Vulnerability assessment report* in the template provided. Vulnerability assessments include a description of the system being evaluated and the scope of the project.  Review the S**ystem Description** and **Scope** of the *Vulnerability assessment report*.  The **System Description** highlights the relevant components, architecture, and dependencies of the system being assessed. All of these parts and connections make up the attack surface of the vulnerable information system.  The **Scope** specifies the focus and boundaries of the assessment. For example, you might specify that the scope of this assessment only relates to the confidentiality, availability, and integrity of the data on the server — not the physical security of the server or its related IT systems. |

**Bước 3: Xem lại thông tin về máy chủ dễ bị tấn công**

Trong hoạt động này, chúng tôi đã cung cấp cho bạn Mô **tả hệ thống** và **Phạm vi** của *báo cáo đánh giá lỗ hổng bảo mật* theo mẫu được cung cấp. Đánh giá lỗ hổng bảo mật bao gồm mô tả về hệ thống đang được đánh giá và phạm vi của dự án.

Xem lại **Mô tả hệ thống** và **Phạm vi** của *báo cáo đánh giá Lỗ hổng* .

Mô **tả Hệ thống** nêu bật các thành phần, kiến ​​trúc và sự phụ thuộc có liên quan của hệ thống đang được đánh giá. Tất cả các bộ phận và kết nối này tạo nên bề mặt tấn công của hệ thống thông tin dễ bị tấn công.

Phạm **vi** xác định trọng tâm và ranh giới của việc đánh giá. Ví dụ: bạn có thể chỉ định rằng phạm vi đánh giá này chỉ liên quan đến tính bảo mật, tính khả dụng và tính toàn vẹn của dữ liệu trên máy chủ — không liên quan đến bảo mật vật lý của máy chủ hoặc các hệ thống CNTT liên quan của nó.

|  |
| --- |
| **Part 2 - Perform the risk assessment** |

**Phần 2 - Thực hiện đánh giá rủi ro**

|  |
| --- |
| **Step 1: Explain the purpose of the information system**  Use the [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg) resource to complete this activity.  Once you have reviewed  the  system description and scope, you will write  a purpose statement. The purpose section helps stakeholders understand the underlying objective and intended outcome of your analysis. A purpose statement also connects the technical objectives of your analysis with the organization's goals.  Consider what you know about the server:   * *How is the database server valuable to the business?* * *Why is it important for the business to secure the data on the server?* * *How might the server impact the business if it were disabled?*   In the **Purpose** section of the report, use the questions provided and write **3-5 sentences** (60-100 words) describing the reason(s) for conducting this vulnerability analysis. |

**Bước 1: Giải thích mục đích của hệ thống thông tin**

Sử dụng[NIST SP 800-30 Phiên bản 1](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg)nguồn lực để hoàn thành hoạt động này.

Khi bạn đã xem lại mô tả và phạm vi hệ thống, bạn sẽ viết một tuyên bố mục đích. Phần mục đích giúp các bên liên quan hiểu được mục tiêu cơ bản và kết quả dự kiến ​​của phân tích của bạn. Tuyên bố mục đích cũng kết nối các mục tiêu kỹ thuật trong phân tích của bạn với mục tiêu của tổ chức.

Hãy xem xét những gì bạn biết về máy chủ:

* *Máy chủ cơ sở dữ liệu có giá trị như thế nào đối với doanh nghiệp?*
* *Tại sao việc bảo mật dữ liệu trên máy chủ lại quan trọng với doanh nghiệp?*
* *Máy chủ có thể tác động đến doanh nghiệp như thế nào nếu nó bị vô hiệu hóa?*

Trong phần **Mục đích** của báo cáo, hãy sử dụng các câu hỏi được cung cấp và viết **3-5 câu** (60-100 từ) mô tả (các) lý do thực hiện phân tích lỗ hổng này.

|  |
| --- |
| **Step 2: Identify potential threat sources**  Explore the *Threat sources* section of the *NIST SP 800-30 Rev. 1* resource. Using what you know about the vulnerable database server, notice the threat types and examples described.  In the **Threat Source** column of the Risk Assessment table of your template, **identify three** potentialthreats. Choose the threats based on the information you have gathered from the system description, scope, purpose, and *NIST SP 800-30 Rev. 1* resource. |

**Bước 2: Xác định các nguồn đe dọa tiềm ẩn**

Khám phá phần *Nguồn đe dọa* của tài nguyên *NIST SP 800-30 Rev. 1* . Sử dụng những gì bạn biết về máy chủ cơ sở dữ liệu dễ bị tấn công, hãy chú ý đến các loại mối đe dọa và ví dụ được mô tả.

Trong cột **Nguồn đe dọa** của bảng Đánh giá rủi ro trong mẫu của bạn, **hãy xác định ba** mối đe dọa tiềm ẩn . Chọn các mối đe dọa dựa trên thông tin bạn đã thu thập từ mô tả hệ thống, phạm vi, mục đích và tài nguyên *NIST SP 800-30 Rev. 1* .

|  |
| --- |
| **Step 3: Identify potential threat events**  *NIST SP 800-30 Rev. 1* provides a comprehensive list of possible security events that could compromise a vulnerable information system — labeled *Threat events*. This list covers what attackers from different groups typically try to achieve and how good they are at it. For example, a business competitor might have the technical capabilities needed to conduct a denial of service attack.  Explore the *Threat events* section in the resource. Then, **identify three** threat events that could be initiated based on the threat sources you identified. Write the three threat events in the **Threat Event** column of the Risk Assessment table in your template. |

**Bước 3: Xác định các sự kiện đe dọa tiềm ẩn**

*NIST SP 800-30 Rev. 1* cung cấp danh sách đầy đủ các sự kiện bảo mật có thể xảy ra có thể làm tổn hại đến hệ thống thông tin dễ bị tấn công — được gắn nhãn *Sự kiện đe dọa* . Danh sách này bao gồm những gì những kẻ tấn công từ các nhóm khác nhau thường cố gắng đạt được và mức độ giỏi của chúng trong việc đó. Ví dụ: một đối thủ cạnh tranh kinh doanh có thể có khả năng kỹ thuật cần thiết để tiến hành một cuộc tấn công từ chối dịch vụ.

Khám phá phần *Sự kiện đe dọa* trong tài nguyên. Sau đó, **xác định ba** sự kiện đe dọa có thể được bắt đầu dựa trên các nguồn đe dọa mà bạn đã xác định. Viết ba sự kiện đe dọa vào cột **Sự kiện Đe dọa** của bảng Đánh giá Rủi ro trong mẫu của bạn.

|  |
| --- |
| **Step 4: Calculate the risk of potential threats**  You may recall from an earlier reading [about calculating risks](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/9wHgg/understand-risks-threats-and-vulnerabilities) that potential threats and vulnerabilities are important factors to think about when evaluating the security of an asset.  Refer to the likelihood and severity sections of the *NIST SP 800-30 Rev. 1* resource and ask yourself the following questions about each threat that you identified earlier:   * *How frequently could this happen?* * *Would critical business functions be impacted?* * *How might this affect the business and its customers?*   Then, estimate a **Likelihood** score (1-3) and **Severity** score (1-3) for each threat and add your scores to the corresponding columns of the Risk Assessment table in your template. After that, calculate an overall **Risk** score (1-9) for each threat using the formula (**likelihood x severity = risk**).  **Note:** The number of rows in a risk table can vary depending on the complexity and scope of the assessment. In general, it should provide stakeholders with a comprehensive overview of all significant risks. |

**Bước 4: Tính toán rủi ro của các mối đe dọa tiềm ẩn**

Bạn có thể nhớ lại từ bài đọc trước đó[về tính toán rủi ro](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/9wHgg/understand-risks-threats-and-vulnerabilities)rằng các mối đe dọa và lỗ hổng tiềm ẩn là những yếu tố quan trọng cần cân nhắc khi đánh giá tính bảo mật của tài sản.

Tham khảo phần khả năng xảy ra và mức độ nghiêm trọng của tài nguyên *NIST SP 800-30 Rev. 1* và tự hỏi bản thân những câu hỏi sau về từng mối đe dọa mà bạn đã xác định trước đó:

* *Điều này có thể xảy ra thường xuyên như thế nào?*
* *Các chức năng kinh doanh quan trọng có bị ảnh hưởng không?*
* *Điều này có thể ảnh hưởng đến doanh nghiệp và khách hàng như thế nào?*

Sau đó, ước tính điểm **Khả năng** (1-3) và điểm Mức **độ nghiêm trọng** (1-3) cho mỗi mối đe dọa và thêm điểm của bạn vào các cột tương ứng của bảng Đánh giá Rủi ro trong mẫu của bạn. Sau đó, tính điểm **Rủi ro** tổng thể (1-9) cho từng mối đe dọa bằng công thức ( **khả năng x mức độ nghiêm trọng = rủi ro** ).

**Lưu ý:** Số lượng hàng trong bảng rủi ro có thể khác nhau tùy thuộc vào mức độ phức tạp và phạm vi đánh giá. Nói chung, nó phải cung cấp cho các bên liên quan một cái nhìn tổng quan toàn diện về tất cả các rủi ro đáng kể.

|  |
| --- |
| **Part 3 - Propose security recommendations** |

**Phần 3 - Đề xuất các khuyến nghị bảo mật**

|  |
| --- |
| **Step 1: Explain your approach**  Another section that's commonly included in a vulnerability assessment is an explanation of your approach. This helps stakeholders understand your thought process of evaluating the risks you've identified — adding valuable context for stakeholders.  You are conducting a *qualitative* vulnerability assessment, which relies on subjective judgment to assess the likelihood and severity of risks. Your task here is to estimatehow bad attacks could be by judging theirchancesbased on your security knowledge. Qualitative vulnerability assessments are useful for identifying high-level risks facing an organization. This information helps organizations make informed decisions about resource allocation, project planning, and other aspects of their business operations.  In the **Approach** section of your template, write **3-5 sentences** (60-100 words) explaining why you selected the 3 specific threat sources/events you chose and why you think they're significant business risks. |

**Bước 1: Giải thích cách tiếp cận của bạn**

Một phần khác thường được đưa vào đánh giá lỗ hổng là phần giải thích về cách tiếp cận của bạn. Điều này giúp các bên liên quan hiểu được quá trình suy nghĩ của bạn khi đánh giá những rủi ro mà bạn đã xác định — bổ sung bối cảnh có giá trị cho các bên liên quan.

Bạn đang tiến hành đánh giá lỗ hổng *định tính* , dựa trên đánh giá chủ quan để đánh giá khả năng và mức độ nghiêm trọng của rủi ro. Nhiệm vụ của bạn ở đây là ước tính mức độ nghiêm trọng của các cuộc tấn công bằng cách đánh giá khả năng xảy ra của chúng dựa trên kiến ​​thức bảo mật của bạn. Đánh giá lỗ hổng định tính rất hữu ích trong việc xác định các rủi ro cấp cao mà tổ chức phải đối mặt. Thông tin này giúp các tổ chức đưa ra quyết định sáng suốt về phân bổ nguồn lực, lập kế hoạch dự án và các khía cạnh khác trong hoạt động kinh doanh của họ.

Trong phần **Cách tiếp cận** của mẫu, hãy viết **3-5 câu** (60-100 từ) giải thích lý do bạn chọn 3 nguồn/sự kiện mối đe dọa cụ thể mà bạn đã chọn và tại sao bạn cho rằng chúng là những rủi ro kinh doanh đáng kể.

|  |
| --- |
| **Step 2: Propose a remediation strategy**  After performing a vulnerability assessment, creating a well-defined remediation strategy is crucial for protecting your systems and data.  The remediation strategy should provide stakeholders with actionable steps that can be taken to remediate, or fix, vulnerabilities to avoid threats.  **Note:** Certain threats cannot be fixed. In those cases, it's equally important to consider a *mitigation strategy* — a plan to reduce the severity of a threat.  Think about the risks that could remediate and/or mitigate using security controls like:   * Principle of least privilege * Defense in depth * Multi-factor authentication (MFA) * Authentication, Authorization, Accounting (AAA) framework   In the **Remediation** section of the template, write **3-5 sentences** (60-100 words) summarizing specific security controls that could be implemented to remediate or mitigate the risks to the information system.  Align your suggestions with the risks you've assessed. For example, you might suggest public key infrastructure (PKI) to address exfiltration of sensitive information. |

**Bước 2: Đề xuất phương án khắc phục**

Sau khi thực hiện đánh giá lỗ hổng, việc tạo chiến lược khắc phục được xác định rõ ràng là rất quan trọng để bảo vệ hệ thống và dữ liệu của bạn. Chiến lược khắc phục phải cung cấp cho các bên liên quan các bước có thể thực hiện được để khắc phục hoặc khắc phục các lỗ hổng nhằm tránh các mối đe dọa.

**Lưu ý:** Một số mối đe dọa không thể khắc phục được. Trong những trường hợp đó, điều quan trọng không kém là phải xem xét *chiến lược giảm thiểu* - một kế hoạch nhằm giảm mức độ nghiêm trọng của mối đe dọa.

Hãy suy nghĩ về những rủi ro có thể khắc phục và/hoặc giảm thiểu bằng cách sử dụng các biện pháp kiểm soát bảo mật như:

* Nguyên tắc đặc quyền tối thiểu
* Phòng thủ có chiều sâu
* Xác thực đa yếu tố (MFA)
* Khung xác thực, ủy quyền, kế toán (AAA)

Trong phần **Khắc phục** của mẫu, viết **3-5 câu** (60-100 từ) tóm tắt các biện pháp kiểm soát bảo mật cụ thể có thể được thực hiện để khắc phục hoặc giảm thiểu rủi ro cho hệ thống thông tin.

Căn chỉnh các đề xuất của bạn với những rủi ro bạn đã đánh giá. Ví dụ: bạn có thể đề xuất cơ sở hạ tầng khóa công khai (PKI) để giải quyết vấn đề rò rỉ thông tin nhạy cảm.

|  |
| --- |
| **Pro Tip: Save the template**  Finally, be sure to save a copy of your completed activity. You can use it for your professional portfolio to demonstrate your knowledge and/or experience to potential employers. |

**Mẹo chuyên nghiệp: Lưu mẫu**

Cuối cùng, hãy nhớ lưu một bản sao của hoạt động đã hoàn thành của bạn. Bạn có thể sử dụng nó cho hồ sơ nghề nghiệp của mình để chứng minh kiến ​​thức và/hoặc kinh nghiệm của mình với các nhà tuyển dụng tiềm năng.

|  |
| --- |
| **What to Include in Your Response**  Be sure to address the following elements in your completed activity:   * 3-5 sentences describing the reasons for conducting the security analysis in the **Purpose** section * A completed **Risk Assessment** section * 3-5 sentences explaining your reasoning for the identified risks in the **Approach** section   3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the **Remediation** section |

**Những gì cần bao gồm trong phản hồi của bạn**

Hãy đảm bảo giải quyết các yếu tố sau trong hoạt động đã hoàn thành của bạn:

* 3-5 câu mô tả lý do tiến hành phân tích bảo mật trong phần **Mục đích**
* Phần **đánh giá rủi ro** đã hoàn thành
* 3-5 câu giải thích lý do của bạn về những rủi ro được xác định trong phần **Tiếp cận**

3-5 câu tóm tắt chiến lược *khắc phục* và/hoặc *giảm thiểu* trong phần **Khắc phục**

|  |
| --- |
| **Step 3: Assess your activity**  The following is a self-assessment for your *Vulnerability assessment report*. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your report.  There are a total of 5 points possible for this activity and each statement is worth 1 point. The items correspond to each step you completed for the activity.  To complete the self-assessment, first open your *Vulnerability assessment report*. Then, respond yes or no to each statement.  When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this activity is at least 80% (or 4/5 points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 4 points before continuing on to the next course item. |

**Bước 3: Đánh giá hoạt động của bạn**

Sau đây là phần tự đánh giá cho *báo cáo Đánh giá lỗ hổng bảo mật* của bạn . Bạn sẽ sử dụng những tuyên bố này để xem xét công việc của riêng bạn. Quá trình tự đánh giá là một phần quan trọng trong trải nghiệm học tập vì nó cho phép bạn đánh giá báo cáo của mình *một cách khách quan* .

Có tổng cộng 5 điểm cho hoạt động này và mỗi câu có giá trị 1 điểm. Các mục tương ứng với từng bước bạn đã hoàn thành cho hoạt động.

Để hoàn tất quá trình tự đánh giá, trước tiên hãy mở *báo cáo đánh giá Lỗ hổng bảo mật* của bạn . Sau đó, trả lời có hoặc không cho mỗi câu.

Khi bạn hoàn thành và gửi câu trả lời của mình, bạn sẽ nhận được điểm phần trăm. Điểm số này sẽ giúp bạn xác nhận xem bạn đã hoàn thành các bước yêu cầu của hoạt động hay chưa. Điểm đậu được đề xuất cho hoạt động này ít nhất là 80% (hoặc 4/5 điểm). Nếu muốn tăng điểm, bạn có thể sửa lại dự án của mình rồi gửi lại phản hồi để phản ánh bất kỳ thay đổi nào bạn đã thực hiện. Cố gắng đạt được ít nhất 4 điểm trước khi tiếp tục học bài tiếp theo.

***2.8. Portfolio Activity Exemplar: Analyze a vulnerable system for a small business - Ví dụ về hoạt động danh mục đầu tư: Phân tích hệ thống dễ bị tổn thương cho một doanh nghiệp nhỏ***

|  |
| --- |
| **Portfolio Activity Exemplar: Analyze a vulnerable system for a small business**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Ví dụ về hoạt động danh mục đầu tư: Phân tích hệ thống dễ bị tổn thương cho một doanh nghiệp nhỏ**

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the following link and select *Use Template*.  Link to exemplar:[Vulnerability assessment report](https://docs.google.com/document/d/1JoKelI2NE_Nunpwq9Tf6E4ox7XWKrZZdgYNM6S09870/template/preview?usp=sharing) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Báo cáo đánh giá lỗ hổng](https://docs.google.com/document/d/1JoKelI2NE_Nunpwq9Tf6E4ox7XWKrZZdgYNM6S09870/template/preview?usp=sharing)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course. |

**Đánh giá mẫu mực**

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong suốt khóa học.

|  |
| --- |
| ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your vulnerability assessment report includes each of the following elements: an explanation of the purpose of the assessment, a completed risk assessment table, an explanation of your approach to quantifying risk, and details of your remediation strategy that address the system's vulnerabilities.* |

***Lưu ý:*** *Ví dụ thể hiện một cách khả thi để hoàn thành hoạt động. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là báo cáo đánh giá lỗ hổng của bạn bao gồm từng yếu tố sau: giải thích về mục đích đánh giá, bảng đánh giá rủi ro hoàn chỉnh, giải thích về cách tiếp cận của bạn để định lượng rủi ro và chi tiết về chiến lược khắc phục nhằm giải quyết các lỗ hổng của hệ thống .*

|  |
| --- |
| The exemplar uses details from the given scenario and includes the following:   * 3-5 sentences describing the reasons for conducting the security analysis in the **Purpose** section * A completed **Risk Assessment** section * 3-5 sentences explaining the reasoning for the identified risks in the **Approach** section * 3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the **Remediation** section |

Ví dụ mẫu sử dụng các chi tiết từ tình huống đã cho và bao gồm những thông tin sau:

* 3-5 câu mô tả lý do tiến hành phân tích bảo mật trong phần **Mục đích**
* Phần **đánh giá rủi ro** đã hoàn thành
* 3-5 câu giải thích lý do cho các rủi ro được xác định trong phần **Tiếp cận**
* 3-5 câu tóm tắt chiến lược *khắc phục* và/hoặc *giảm thiểu* trong phần **Khắc phục**

|  |
| --- |
| **Overview**  The exemplar report contains a **Purpose** section that is an explanation of the information system that's being assessed—a publicly accessible database server. This statement describes the business function of the system. It also makes clear the reason for conducting the analysis.  The **Risk Assessment** section of the exemplar contains a completed table. The risk assessment identifies potential threat sources and threat events that could negatively impact the business. Both were determined by asking questions such as:   * Is the threat relevant to this system? * Is the threat internal or external? * What is the threat actor’s intent? * What are the threat actors’ technical capabilities?   The risk of each threat is quantified by multiplying its *likelihood* of occurring with the *severity* of its impact on the business. Then, an overall *risk* score is calculated that demonstrates to stakeholders both the seriousness of the risks to the database and how resources should be prioritized to address the most critical risks.  **Note:** The number of rows in a risk assessment table can vary depending on the complexity and scope of the assessment.  The **Approach** section of the exemplar is a statement following the risk assessment that explains why and how specific threats were evaluated.  Lastly, a plan for securing the vulnerable database server was outlined in the **Remediation** section of the report. |

**Tổng quan**

Báo cáo mẫu có chứa phần **Mục đích** giải thích về hệ thống thông tin đang được đánh giá—một máy chủ cơ sở dữ liệu có thể truy cập công khai. Tuyên bố này mô tả chức năng kinh doanh của hệ thống. Nó cũng làm rõ lý do tiến hành phân tích.

Phần **Đánh giá Rủi ro** của mẫu có chứa một bảng hoàn chỉnh. Đánh giá rủi ro xác định các nguồn đe dọa tiềm ẩn và các sự kiện đe dọa có thể tác động tiêu cực đến doanh nghiệp. Cả hai đều được xác định bằng cách đặt những câu hỏi như:

* Mối đe dọa có liên quan đến hệ thống này không?
* Mối đe dọa là bên trong hay bên ngoài?
* Mục đích của kẻ đe dọa là gì?
* Khả năng kỹ thuật của các tác nhân đe dọa là gì?

Rủi ro của mỗi mối đe dọa được định lượng bằng cách nhân *khả năng* xảy ra với *mức độ nghiêm trọng* của tác động đối với doanh nghiệp. Sau đó, điểm *rủi ro* tổng thể được tính toán để chứng minh cho các bên liên quan thấy cả mức độ nghiêm trọng của rủi ro đối với cơ sở dữ liệu và cách ưu tiên các nguồn lực để giải quyết các rủi ro nghiêm trọng nhất.

**Lưu ý:** Số lượng hàng trong bảng đánh giá rủi ro có thể khác nhau tùy thuộc vào mức độ phức tạp và phạm vi đánh giá.

Phần **Cách tiếp cận** của ví dụ mẫu là một tuyên bố sau khi đánh giá rủi ro giải thích lý do và cách thức đánh giá các mối đe dọa cụ thể.

Cuối cùng, kế hoạch bảo mật máy chủ cơ sở dữ liệu dễ bị tấn công đã được nêu trong phần **Khắc phục** của báo cáo.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| It's crucial for security analysts to develop risk assessment and reporting skills. These skills will enable you to identify potential risk within an organization's systems and escalate that information to the appropriate channels. This activity is intended as an opportunity for you to practice analyzing the risks of a vulnerable system. You can add this document to your cybersecurity portfolio. However, all systems have vulnerabilities. As such, you're encouraged to continue practicing these skills by applying them to other systems that are discussed in the program. |

Điều quan trọng đối với các nhà phân tích bảo mật là phát triển kỹ năng đánh giá và báo cáo rủi ro. Những kỹ năng này sẽ cho phép bạn xác định rủi ro tiềm ẩn trong hệ thống của tổ chức và chuyển thông tin đó đến các kênh thích hợp. Hoạt động này nhằm mục đích tạo cơ hội cho bạn thực hành phân tích rủi ro của một hệ thống dễ bị tổn thương. Bạn có thể thêm tài liệu này vào danh mục an ninh mạng của mình. Tuy nhiên, tất cả các hệ thống đều có lỗ hổng. Vì vậy, bạn được khuyến khích tiếp tục thực hành những kỹ năng này bằng cách áp dụng chúng vào các hệ thống khác được thảo luận trong chương trình.

**3. Cyber attacker mindset - Tư duy tấn công mạng**

***3.1. Protect all entry points – Bảo vệ tất cả các điểm vào***

|  |
| --- |
| There's a wide range of vulnerabilities in systems that need to be found. Assessing those weaknesses is a time-consuming process. To position themselves ahead of threats and make the most of their limited resources, companies start by understanding the environment surrounding their operations. An important part of this is getting a sense of their attack surface. |

Có rất nhiều lỗ hổng trong hệ thống cần được tìm ra.Đánh giá những điểm yếu đó là một quá trình tốn thời gian.Để định vị bản thân trước các mối đe dọa vàtận dụng tối đa nguồn lực hạn chế của mình, các công ty bắt đầu bằng cách hiểumôi trường xung quanh hoạt động của họ.Một phần quan trọng của việc này là phải nắm được bề mặt tấn công của chúng.

|  |
| --- |
| An attack surface is all the potential vulnerabilities that a threat actor could exploit. Analyzing the attack surface is usually the first thing security teams do. |

Bề mặt tấn công là tất cả các lỗ hổng tiềm ẩn mà tác nhân đe dọacó thể khai thác.Phân tích bề mặt tấn công thường là điều đầu tiên mà các nhóm bảo mật làm.

|  |
| --- |
| For example, imagine being part of a security team of an old castle. Your team would need to decide how to allocate resources to defenses. Giant walls, stone towers, and wooden gates are a few common security controls of these structures. While these are all designed to protect the assets inside from attacks, they don't exactly account for all the possibilities. What if the castle were near the ocean? If it were, these defenses would be vulnerable to long range attacks by ship. A proper understanding of the attack surface would mean your security team equipped the castle with catapults that could deal with these kinds of threats. |

Ví dụ, hãy tưởng tượng bạn là thành viên của đội an ninh của một lâu đài cổ.Nhóm của bạn sẽ cần quyết định cách phân bổ tài nguyên cho phòng thủ.Những bức tường khổng lồ, những tòa tháp đá vàCổng gỗ là một trong những biện pháp kiểm soát an ninh phổ biến của những công trình này.Mặc dù tất cả những điều này đều được thiết kế để bảo vệ tài sản bên trong khỏi các cuộc tấn công,chúng không thực sự tính đến tất cả các khả năng.Nếu lâu đài ở gần biển thì sao?Nếu vậy, hệ thống phòng thủ này sẽ dễ bị tổn thương trước các cuộc tấn công tầm xa bằng tàu.Hiểu đúng về bề mặt tấn công sẽ có nghĩa là nhóm bảo mật của bạntrang bị cho lâu đài những máy bắn đá có thể giải quyết được những mối đe dọa như thế này.

|  |
| --- |
| Modern organizations need to concern themselves with both a physical and digital attack surface. The physical attack surface is made up of people and their devices. This surface can be attacked from both inside and outside the organization, which makes it unique. |

Các tổ chức hiện đại cần quan tâm đến cả mặt vật chất vàbề mặt tấn công kỹ thuật số.Bề mặt tấn công vật lý bao gồm con người và thiết bị của họ.Bề mặt này có thể bị tấn công từ cả bên trong và bên ngoàibên ngoài tổ chức, điều này làm cho nó trở nên độc đáo.

|  |
| --- |
| For example, let's consider an unattended laptop in a public space, like a coffee shop. The person responsible for it walked away while sensitive company information was visible on the screen. This information is vulnerable to external threats, like a business competitor, who can easily record the information and exploit it. An internal threat of this attack surface, on the other hand, is often angry employees. These employees might share an organization's private information on purpose. |

Ví dụ,hãy xem xét một chiếc máy tính xách tay không có người trông coi ở nơi công cộng, như quán cà phê.Người chịu trách nhiệm chonó bỏ đi trong khi thông tin nhạy cảm của công ty vẫn hiển thị trên màn hình.Thông tin này dễ bị tổn thương trước các mối đe dọa bên ngoài,giống như một đối thủ cạnh tranh trong kinh doanh, người có thể dễ dàng ghi lại thông tin và khai thác nó.Mặt khác, mối đe dọa nội bộ của cuộc tấn công này xuất hiệnthường là những nhân viên tức giận.Những nhân viên này có thể chia sẻ thông tin riêng tư của một tổ chức trênmục đích.

|  |
| --- |
| In general, the physical attack surface should be filled with obstacles that deter attacks from happening. We call this process security hardening. Security hardening is the process of strengthening a system to reduce its vulnerabilities and attack surface. In other words, hardening is the act of minimizing the attack surface by limiting its points of entry. |

Nhìn chung, bề mặt tấn công vật lý phải được lấp đầy bằng các chướng ngại vậtngăn chặn các cuộc tấn công xảy ra.Chúng tôi gọi quá trình này là tăng cường bảo mật.Tăng cường bảo mật là quá trình tăng cường hệ thống đểgiảm thiểu lỗ hổng và bề mặt tấn công.Nói cách khác, làm cứng là hành độnggiảm thiểu bề mặt tấn công bằng cách hạn chế các điểm xâm nhập.

|  |
| --- |
| We do this a lot in security because the smaller the attack surface, the easier it is to protect. In fact, some security controls that we've explored previously, like organization policies and access controls, are common ways that organizations harden their physical attack surface. |

Chúng tôi thực hiện điều này rất nhiều trong bảo mật vì bề mặt tấn công càng nhỏ,thì việc bảo vệ càng dễ dàng hơn.Trên thực tế, một số biện pháp kiểm soát an ninh mà chúng tôi đã khám phá trước đây,giống như chính sách tổ chức và kiểm soát truy cập, là những cách phổ biến màcác tổ chức tăng cường bảo vệ bề mặt tấn công vật lý của mình.

|  |
| --- |
| The digital attack surface is a bit tougher to harden. The digital attack surface includes everything that's beyond our organization's firewall. In other words, it includes anything that connects to an organization online. |

Bề mặt tấn công kỹ thuật số khó bị tấn công hơn một chút.Bề mặt tấn công kỹ thuật số bao gồm mọi thứ nằm ngoài tầm hiểu biết của chúng tatường lửa của tổ chức.Nói cách khác, nó bao gồm mọi thứ kết nối trực tuyến với một tổ chức.

|  |
| --- |
| In the past, organizations stored their data in a single location. This mainly consisted of servers that were managed on-site. Accessing the information stored on those servers required connecting to the network the workplace managed. |

Trước đây, các tổ chức lưu trữ dữ liệu của mình ở một vị trí duy nhất.Điều này chủ yếu bao gồm các máy chủ được quản lý tại chỗ.Việc truy cập thông tin được lưu trữ trên các máy chủ đó yêu cầu phải kết nối vớimạng lưới nơi làm việc quản lý.

|  |
| --- |
| These days, information is accessed outside of an organization's network because it's stored in the cloud. Information can be accessed from anywhere in the world. A person can be in one part of the world, fly to another place, and continue working. All while outside of their organization's network. |

Ngày nay, thông tin được truy cập bên ngoài mạng lưới của một tổ chức vì nóđược lưu trữ trên đám mây.Có thể truy cập thông tin từ bất cứ nơi nào trên thế giới.Một người có thể ở một nơi nào đó trên thế giới, bay đến một nơi khác vàtiếp tục làm việc. Tất cả đều diễn ra bên ngoài mạng lưới của tổ chức họ.

|  |
| --- |
| Cloud computing has essentially expanded the digital attack surface. Quicker access to information is something we all benefit from, but it comes with a cost. Organizations of all sizes are under more pressure to defend against threats coming from different entry points. |

Điện toán đám mây về cơ bản đã mở rộng phạm vi tấn công kỹ thuật số.Truy cập thông tin nhanh hơn là điều mà tất cả chúng ta đều được hưởng lợi, nhưngnó đi kèm với một cái giá.Các tổ chức ở mọi quy mô đều chịu nhiều áp lực hơn trong việc bảo vệ chống lại các mối đe dọađến từ nhiều điểm vào khác nhau.

|  |
| --- |
| When we get together next time, we'll explore why this is such a challenge. |

Lần tới khi chúng ta gặp nhau, chúng ta sẽ cùng tìm hiểu xem tại sao đây lại là một thách thức lớn như vậy.

***3.2. Approach cybersecurity with an attacker mindset - Tiếp cận an ninh mạng với tư duy của kẻ tấn công***

|  |
| --- |
| **Approach cybersecurity with an attacker mindset** |

**Tiếp cận an ninh mạng với tư duy của kẻ tấn công**

|  |
| --- |
| Cybersecurity is a continuously changing field. It's a fast-paced environment where new threats and innovative technologies can disrupt your plans at a moment's notice. As a security professional, it’s up to you to be prepared by anticipating change. |

An ninh mạng là một lĩnh vực liên tục thay đổi. Đây là một môi trường phát triển nhanh, nơi các mối đe dọa mới và công nghệ tiên tiến có thể phá vỡ kế hoạch của bạn bất cứ lúc nào. Là một chuyên gia an ninh, bạn phải chuẩn bị bằng cách dự đoán sự thay đổi.

|  |
| --- |
| This all starts with identifying vulnerabilities. In a video, you learned about the importance of vulnerability assessments, the internal review process of an organization's security systems. In this reading, you will learn how you can use the findings of a vulnerability assessment proactively by analyzing them from the perspective of an attacker. |

Tất cả bắt đầu bằng việc xác định các lỗ hổng. Trong một video, bạn đã tìm hiểu về tầm quan trọng của **đánh giá lỗ hổng,** quy trình đánh giá nội bộ các hệ thống bảo mật của một tổ chức. Trong bài đọc này, bạn sẽ tìm hiểu cách sử dụng các phát hiện của đánh giá lỗ hổng một cách chủ động bằng cách phân tích chúng theo góc nhìn của kẻ tấn công.

|  |
| --- |
| **Being prepared for anything** |

**Chuẩn bị cho mọi thứ**

|  |
| --- |
| Having a plan should things go wrong is important. But how do you figure out what to plan for? In this field, teams often conduct simulations of things that can go wrong as part of their vulnerability management strategy. One way this is done is by applying an attacker mindset to the weaknesses they discover. |

Có một kế hoạch phòng trường hợp mọi thứ diễn ra không như mong đợi là điều quan trọng. Nhưng làm thế nào để bạn tìm ra kế hoạch cho những gì? Trong lĩnh vực này, các nhóm thường tiến hành mô phỏng những điều có thể diễn ra không như một phần của chiến lược quản lý lỗ hổng của họ. Một cách để thực hiện điều này là áp dụng tư duy của kẻ tấn công vào các điểm yếu mà họ phát hiện ra.

|  |
| --- |
| Applying an attacker mindset is a lot like conducting an experiment. It's about causing problems in a controlled environment and evaluating the outcome to gain insights. Adopting an attacker mindset is a beneficial skill in security because it offers a different perspective about the challenges you're trying to solve. The insights you gain can be valuable when it's time to establish a security plan or modify an existing one. |

Áp dụng tư duy của kẻ tấn công cũng giống như tiến hành một thí nghiệm. Đó là việc gây ra các vấn đề trong một môi trường được kiểm soát và đánh giá kết quả để có được hiểu biết sâu sắc. Áp dụng tư duy của kẻ tấn công là một kỹ năng có lợi trong bảo mật vì nó cung cấp một góc nhìn khác về những thách thức mà bạn đang cố gắng giải quyết. Những hiểu biết sâu sắc mà bạn có được có thể có giá trị khi đến lúc thiết lập một kế hoạch bảo mật hoặc sửa đổi một kế hoạch hiện có.

|  |
| --- |
| **Simulating threats** |

**Mô phỏng các mối đe dọa**

|  |
| --- |
| One method of applying an attacker mindset is using attack simulations. These activities are normally performed in one of two ways: *proactively* and *reactively*. Both approaches share a common goal, which is to make systems safer.   * *Proactive simulations* assume the role of an attacker by exploiting vulnerabilities and breaking through defenses. This is sometimes called a red team exercise. * *Reactive simulations* assume the role of a defender responding to an attack. This is sometimes called a blue team exercise. |

Một phương pháp áp dụng tư duy của kẻ tấn công là sử dụng mô phỏng tấn công. Các hoạt động này thường được thực hiện theo một trong hai cách: *chủ động* và *phản ứng* . Cả hai cách tiếp cận đều có chung một mục tiêu là làm cho hệ thống an toàn hơn.

* *Mô phỏng chủ động* đảm nhận vai trò của kẻ tấn công bằng cách khai thác lỗ hổng và phá vỡ hàng phòng thủ. Đôi khi điều này được gọi là bài tập nhóm đỏ.
* *Mô phỏng phản ứng* đảm nhận vai trò của người phòng thủ phản ứng lại một cuộc tấn công. Đôi khi điều này được gọi là bài tập đội xanh.

|  |
| --- |
| Each kind of simulation is a team effort that you might be involved with as an analyst. |

Mỗi loại mô phỏng là một nỗ lực của nhóm mà bạn có thể tham gia với tư cách là nhà phân tích.

|  |
| --- |
| Proactive teams tend to spend more time planning their attacks than performing them. If you find yourself engaged in one of these exercises, your team will likely deploy a range of tactics. For example, they might persuade staff into disclosing their login credentials using fictitious emails to evaluate security awareness at the company. |

Các nhóm chủ động có xu hướng dành nhiều thời gian hơn để lập kế hoạch tấn công hơn là thực hiện chúng. Nếu bạn thấy mình tham gia vào một trong những bài tập này, nhóm của bạn có thể sẽ triển khai một loạt các chiến thuật. Ví dụ, họ có thể thuyết phục nhân viên tiết lộ thông tin đăng nhập của họ bằng email giả để đánh giá nhận thức về bảo mật tại công ty.

|  |
| --- |
| On the other hand, reactive teams dedicate their efforts to gathering information about the assets they're protecting. This is commonly done with the assistance of vulnerability scanning tools. |

Mặt khác, các nhóm phản ứng dành nỗ lực của họ để thu thập thông tin về tài sản mà họ đang bảo vệ. Điều này thường được thực hiện với sự hỗ trợ của các công cụ quét lỗ hổng.

|  |
| --- |
| **Scanning for trouble** |

**Quét tìm sự cố**

|  |
| --- |
| You might recall that a **vulnerability scanner** is software that automatically compares existing common vulnerabilities and exposures against the technologies on the network. Vulnerability scanners are frequently used in the field. Security teams employ a variety of scanning techniques to uncover weaknesses in their defenses. Reactive simulations often rely on the results of a scan to weigh the risks and determine ways to remediate a problem. |

Bạn có thể nhớ rằng **máy quét lỗ hổng** là phần mềm tự động so sánh các lỗ hổng và sự phơi bày phổ biến hiện có với các công nghệ trên mạng. Máy quét lỗ hổng thường được sử dụng trong lĩnh vực này. Các nhóm bảo mật sử dụng nhiều kỹ thuật quét khác nhau để phát hiện ra điểm yếu trong hệ thống phòng thủ của họ. Mô phỏng phản ứng thường dựa vào kết quả quét để cân nhắc rủi ro và xác định cách khắc phục sự cố.

|  |
| --- |
| For example, a team conducting a reactive simulation might perform an external vulnerability scan of their network. The entire exercise might follow the steps you learned in a video about vulnerability assessments:   * **Identification:** A vulnerable server is flagged because it's running an outdated operating system (OS). * **Vulnerability analysis:** Research is done on the outdated OS and its vulnerabilities. * **Risk assessment:** After doing your due diligence, the severity of each vulnerability is scored and the impact of not fixing it is evaluated. * **Remediation**: Finally, the information that you’ve gathered can be used to address the issue. |

Ví dụ, một nhóm thực hiện mô phỏng phản ứng có thể thực hiện quét lỗ hổng bên ngoài mạng của họ. Toàn bộ bài tập có thể tuân theo các bước bạn đã học trong video về đánh giá lỗ hổng:

* **Nhận dạng:** Máy chủ dễ bị tấn công được đánh dấu vì đang chạy hệ điều hành (OS) lỗi thời.
* **Phân tích lỗ hổng:** Nghiên cứu được thực hiện trên hệ điều hành lỗi thời và các lỗ hổng của nó.
* **Đánh giá rủi ro:** Sau khi hoàn tất quá trình thẩm định, mức độ nghiêm trọng của từng lỗ hổng sẽ được chấm điểm và tác động của việc không khắc phục sẽ được đánh giá.
* **Biện pháp khắc phục** : Cuối cùng, thông tin bạn thu thập được có thể được sử dụng để giải quyết vấn đề.

|  |
| --- |
| During an activity like this, you’ll often produce a report of your findings. These can be brought to the attention of service providers or your supervisors. Clearly communicating the results of these exercises to others is an important skill to develop as a security professional. |

Trong một hoạt động như thế này, bạn thường sẽ tạo ra một báo cáo về những phát hiện của mình. Những phát hiện này có thể được báo cáo cho các nhà cung cấp dịch vụ hoặc người giám sát của bạn. Việc truyền đạt rõ ràng kết quả của các bài tập này cho người khác là một kỹ năng quan trọng cần phát triển với tư cách là một chuyên gia an ninh.

|  |
| --- |
| **Finding innovative solutions** |

**Tìm kiếm giải pháp sáng tạo**

|  |
| --- |
| Many security controls that you’ve learned about were created as a reactive response to risks. That’s because criminals are continually looking for ways to bypass existing defenses. Effectively applying an attacker mindset will require you to stay knowledgeable of security trends and emerging technologies. |

Nhiều biện pháp kiểm soát bảo mật mà bạn đã tìm hiểu được tạo ra như một phản ứng phản ứng với rủi ro. Đó là vì tội phạm liên tục tìm cách vượt qua các biện pháp phòng thủ hiện có. Áp dụng hiệu quả tư duy của kẻ tấn công sẽ đòi hỏi bạn phải luôn hiểu biết về các xu hướng bảo mật và công nghệ mới nổi.

|  |
| --- |
| **Pro tip:** Resources like [NISTs National Vulnerability Database (NVD)](https://nvd.nist.gov/) can help you remain current on common vulnerabilities. |

**Mẹo chuyên nghiệp:** Các nguồn tài nguyên như[Cơ sở dữ liệu lỗ hổng quốc gia của NIST (NVD)](https://nvd.nist.gov/)có thể giúp bạn cập nhật các lỗ hổng phổ biến.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Vulnerability assessments are an important part of security risk planning. As an analyst, you’ll likely participate in proactive and reactive simulations of these activities. Preparing yourself by researching common vulnerabilities only goes so far. It’s equally important that you stay informed about new technologies to be able to think with an innovative mindset. |

Đánh giá lỗ hổng là một phần quan trọng trong kế hoạch rủi ro bảo mật. Là một nhà phân tích, bạn có thể sẽ tham gia vào các mô phỏng chủ động và phản ứng của các hoạt động này. Việc chuẩn bị cho bản thân bằng cách nghiên cứu các lỗ hổng phổ biến chỉ có tác dụng đến một mức nào đó. Điều quan trọng không kém là bạn phải luôn cập nhật thông tin về các công nghệ mới để có thể suy nghĩ với tư duy sáng tạo.

***3.3. Types of threat actors - Các loại tác nhân đe dọa***

|  |
| --- |
| **Types of threat actors** |

**Các loại tác nhân đe dọa**

|  |
| --- |
| Anticipating attacks is an important skill you’ll need to be an effective security professional. Developing this skill requires you to have an open and flexible mindset about where attacks can come from. Previously, you learned about **attack surfaces**, which are all the potential vulnerabilities that a threat actor could exploit. |

Dự đoán các cuộc tấn công là một kỹ năng quan trọng mà bạn cần để trở thành một chuyên gia bảo mật hiệu quả. Phát triển kỹ năng này đòi hỏi bạn phải có tư duy cởi mở và linh hoạt về nơi các cuộc tấn công có thể đến. Trước đó, bạn đã tìm hiểu về **bề mặt tấn công** , tức là tất cả các lỗ hổng tiềm ẩn mà kẻ tấn công có thể khai thác.

|  |
| --- |
| Networks, servers, devices, and staff are examples of attack surfaces that can be exploited. Security teams of all sizes regularly find themselves defending these surfaces due to the expanding digital landscape. The key to defending any of them is to limit access to them. |

Mạng, máy chủ, thiết bị và nhân viên là những ví dụ về bề mặt tấn công có thể bị khai thác. Các nhóm bảo mật ở mọi quy mô thường xuyên thấy mình phải bảo vệ những bề mặt này do bối cảnh kỹ thuật số đang mở rộng. Chìa khóa để bảo vệ bất kỳ bề mặt nào trong số chúng là hạn chế quyền truy cập vào chúng.

|  |
| --- |
| In this reading, you’ll learn more about threat actors and the types of risks they pose. You’ll also explore the most common features of an attack surface that threat actors can exploit. |

Trong bài đọc này, bạn sẽ tìm hiểu thêm về tác nhân đe dọa và các loại rủi ro mà chúng gây ra. Bạn cũng sẽ khám phá các tính năng phổ biến nhất của bề mặt tấn công mà tác nhân đe dọa có thể khai thác.

|  |
| --- |
| **Threat actors** |

**Các tác nhân đe dọa**

|  |
| --- |
| A **threat actor** is any person or group who presents a security risk. This broad definition refers to people inside and outside an organization. It also includes individuals who intentionally pose a threat, and those that accidentally put assets at risk. That’s a wide range of people! |

Tác **nhân đe dọa** là bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro về an ninh. Định nghĩa rộng này đề cập đến những người bên trong và bên ngoài một tổ chức. Nó cũng bao gồm những cá nhân cố ý gây ra mối đe dọa và những người vô tình đặt tài sản vào tình trạng nguy hiểm. Đó là một phạm vi rộng lớn những người!

|  |
| --- |
| Threat actors are normally divided into five categories based on their motivations:   * **Competitors** refers to rival companies who pose a threat because they might benefit from leaked information. * **State actors** are government intelligence agencies. * **Criminal syndicates** refer to organized groups of people who make money from criminal activity. * **Insider threats** can be any individual who has or had authorized access to an organization’s resources. This includes employees who accidentally compromise assets or individuals who purposefully put them at risk for their own benefit. * **Shadow IT** refers to individuals who use technologies that lack IT governance. A common example is when an employee uses their personal email to send work-related communications. |

Các tác nhân đe dọa thường được chia thành năm loại dựa trên động cơ của họ:

* **Đối thủ cạnh tranh** là các công ty đối thủ gây ra mối đe dọa vì họ có thể hưởng lợi từ thông tin bị rò rỉ.
* **Các tác nhân nhà nước** là các cơ quan tình báo của chính phủ.
* **Các tổ chức tội phạm** là những nhóm người có tổ chức kiếm tiền từ hoạt động tội phạm.
* **Mối đe dọa nội gián** có thể là bất kỳ cá nhân nào có hoặc đã được phép truy cập vào tài nguyên của tổ chức. Điều này bao gồm nhân viên vô tình xâm phạm tài sản hoặc cá nhân cố tình đặt tài sản vào tình trạng nguy hiểm vì lợi ích của riêng họ.
* **Shadow IT** đề cập đến những cá nhân sử dụng công nghệ không có quản trị CNTT. Một ví dụ phổ biến là khi một nhân viên sử dụng email cá nhân của họ để gửi thông tin liên lạc liên quan đến công việc.

|  |
| --- |
| In the digital attack surface, these threat actors often gain unauthorized access by hacking into systems. By definition, a **hacker** is any person who uses computers to gain unauthorized access to computer systems, networks, or data. Similar to the term threat actor, hacker is also an umbrella term. When used alone, the term fails to capture a threat actor’s intentions. |

Trong bề mặt tấn công kỹ thuật số, những tác nhân đe dọa này thường có được quyền truy cập trái phép bằng cách hack vào hệ thống. Theo định nghĩa, **tin tặc** là bất kỳ người nào sử dụng máy tính để có được quyền truy cập trái phép vào hệ thống máy tính, mạng hoặc dữ liệu. Tương tự như thuật ngữ tác nhân đe dọa, tin tặc cũng là một thuật ngữ bao trùm. Khi được sử dụng riêng lẻ, thuật ngữ này không nắm bắt được ý định của tác nhân đe dọa.

|  |
| --- |
| **Types of hackers** |

**Các loại tin tặc**

|  |
| --- |
| Because the formal definition of a hacker is broad, the term can be a bit ambiguous. In security, it applies to three types of individuals based on their intent:   1. Unauthorized hackers 2. Authorized, or ethical, hackers 3. Semi-authorized hackers |

Vì định nghĩa chính thức của hacker khá rộng nên thuật ngữ này có thể hơi mơ hồ. Trong bảo mật, nó áp dụng cho ba loại cá nhân dựa trên mục đích của họ:

1. Tin tặc trái phép
2. Tin tặc được cấp phép hoặc có đạo đức
3. Tin tặc bán được ủy quyền

|  |
| --- |
| An unauthorized hacker, or unethical hacker, is an individual who uses their programming skills to commit crimes. Unauthorized hackers are also known as malicious hackers. Skill level ranges widely among this category of hacker. For example, there are hackers with limited skills who can’t write their own malicious software, sometimes called *script kiddies***.** Unauthorized hackers like this carry out attacks using pre-written code that they obtain from other, more skilled hackers. |

Một hacker trái phép, hay hacker phi đạo đức, là một cá nhân sử dụng các kỹ năng lập trình của mình để phạm tội. Hacker trái phép cũng được gọi là hacker độc hại. Mức độ kỹ năng dao động rộng rãi trong nhóm hacker này. Ví dụ, có những hacker có kỹ năng hạn chế không thể tự viết phần mềm độc hại, đôi khi được gọi là *script kiddies* **.** Những hacker trái phép như thế này thực hiện các cuộc tấn công bằng cách sử dụng mã được viết sẵn mà chúng lấy từ những hacker khác có kỹ năng cao hơn.

|  |
| --- |
| Authorized, or ethical, hackers refer to individuals who use their programming skills to improve an organization's overall security. These include internal members of a security team who are concerned with testing and evaluating systems to secure the attack surface. They also include external security vendors and freelance hackers that some companies incentivize to find and report vulnerabilities, a practice called **bug bounty** programs. |

Tin tặc được ủy quyền hoặc có đạo đức là những cá nhân sử dụng kỹ năng lập trình của mình để cải thiện bảo mật tổng thể của một tổ chức. Những người này bao gồm các thành viên nội bộ của nhóm bảo mật, những người quan tâm đến việc thử nghiệm và đánh giá các hệ thống để bảo vệ bề mặt tấn công. Họ cũng bao gồm các nhà cung cấp bảo mật bên ngoài và tin tặc tự do mà một số công ty khuyến khích tìm và báo cáo các lỗ hổng, một hoạt động được gọi là chương trình **tiền thưởng lỗi** .

|  |
| --- |
| Semi-authorized hackers typically refer to individuals who might violate ethical standards, but are not considered malicious. For example, a **hacktivist** is a person who might use their skills to achieve a political goal. One might exploit security vulnerabilities of a public utility company to spread awareness of their existence. The intentions of these types of threat actors is often to expose security risks that should be addressed before a malicious hacker finds them. |

Tin tặc bán được ủy quyền thường ám chỉ những cá nhân có thể vi phạm các tiêu chuẩn đạo đức, nhưng không bị coi là có ác ý. Ví dụ, một **hacker** là người có thể sử dụng các kỹ năng của mình để đạt được mục tiêu chính trị. Người ta có thể khai thác các lỗ hổng bảo mật của một công ty tiện ích công cộng để nâng cao nhận thức về sự tồn tại của họ. Mục đích của những tác nhân đe dọa này thường là để phơi bày các rủi ro bảo mật cần được giải quyết trước khi tin tặc độc hại tìm thấy chúng.

|  |
| --- |
| **Advanced persistent threats** |

**Các mối đe dọa dai dẳng nâng cao**

|  |
| --- |
| Many malicious hackers find their way into a system, cause trouble, and then leave. But on some occasions, threat actors stick around. These kinds of events are known as advanced persistent threats, or APTs. |

Nhiều tin tặc độc hại tìm đường vào hệ thống, gây rắc rối rồi bỏ đi. Nhưng đôi khi, những kẻ tấn công vẫn ở lại. Những sự kiện như vậy được gọi là các mối đe dọa dai dẳng nâng cao, hay APT.

|  |
| --- |
| An **advanced persistent threat (APT)** refers to instances when a threat actor maintains unauthorized access to a system for an extended period of time. The term is mostly associated with nation states and state-sponsored actors. Typically, an APT is concerned with surveilling a target to gather information. They then use the intel to manipulate government, defense, financial, and telecom services. |

Một **mối đe dọa dai dẳng nâng cao (APT)** đề cập đến các trường hợp khi một tác nhân đe dọa duy trì quyền truy cập trái phép vào một hệ thống trong một khoảng thời gian dài. Thuật ngữ này chủ yếu liên quan đến các quốc gia và các tác nhân được nhà nước bảo trợ. Thông thường, một APT liên quan đến việc giám sát mục tiêu để thu thập thông tin. Sau đó, chúng sử dụng thông tin tình báo để thao túng các dịch vụ chính phủ, quốc phòng, tài chính và viễn thông.

|  |
| --- |
| Just because the term is associated with state actors does not mean that private businesses are safe from APTs. These kinds of threat actors are stealthy because hacking into another government agency or utility is costly and time consuming. APTs will often target private organizations first as a step towards gaining access to larger entities. |

Chỉ vì thuật ngữ này liên quan đến các tác nhân nhà nước không có nghĩa là các doanh nghiệp tư nhân an toàn trước APT. Những tác nhân đe dọa này rất lén lút vì việc hack vào một cơ quan hoặc tiện ích chính phủ khác rất tốn kém và mất thời gian. APT thường nhắm mục tiêu vào các tổ chức tư nhân trước tiên như một bước để tiếp cận các thực thể lớn hơn.

|  |
| --- |
| **Access points** |

**Điểm truy cập**

|  |
| --- |
| Each threat actor has a unique motivation for targeting an organization's assets. Keeping them out takes more than knowing their intentions and capabilities. It’s also important to recognize the types of attack vectors they’ll use. |

Mỗi tác nhân đe dọa có động cơ riêng khi nhắm mục tiêu vào tài sản của tổ chức. Việc ngăn chặn chúng không chỉ đòi hỏi phải biết ý định và khả năng của chúng. Điều quan trọng nữa là phải nhận ra các loại vectơ tấn công mà chúng sẽ sử dụng.

|  |
| --- |
| For the most part, threat actors gain access through one of these attack vector categories:   * **Direct access**, referring to instances when they have physical access to a system * **Removable media**, which includes portable hardware, like USB flash drives * **Social media platforms** that are used for communication and content sharing * **Email**,includingboth personal and business accounts * **Wireless networks** on premises * **Cloud services** usually provided by third-party organizations * **Supply chains** like third-party vendors that can present a backdoor into systems |

Phần lớn, kẻ tấn công có thể truy cập thông qua một trong các loại hình tấn công sau:

* **Truy cập trực tiếp** , đề cập đến các trường hợp khi họ có quyền truy cập vật lý vào hệ thống
* **Phương tiện lưu trữ di động** , bao gồm phần cứng di động, như ổ đĩa flash USB
* **Nền tảng truyền thông xã hội** được sử dụng để giao tiếp và chia sẻ nội dung
* **Email** , bao gồm cả tài khoản cá nhân và doanh nghiệp
* **Mạng không dây** tại cơ sở
* **Dịch vụ đám mây** thường được cung cấp bởi các tổ chức bên thứ ba
* **Chuỗi cung ứng** như các nhà cung cấp bên thứ ba có thể tạo ra một cửa hậu vào hệ thống

|  |
| --- |
| Any of these attack vectors can provide access to a system. Recognizing a threat actor’s intentions can help you determine which access points they might target and what ultimate goals they could have. For example, remote workers are more likely to present a threat via email than a direct access threat. |

Bất kỳ vectơ tấn công nào trong số này đều có thể cung cấp quyền truy cập vào hệ thống. Nhận biết ý định của tác nhân đe dọa có thể giúp bạn xác định điểm truy cập nào mà chúng có thể nhắm tới và mục tiêu cuối cùng mà chúng có thể có. Ví dụ, những người làm việc từ xa có nhiều khả năng đưa ra mối đe dọa qua email hơn là mối đe dọa truy cập trực tiếp.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Defending an attack surface starts with thinking like a threat actor. As a security professional, it’s important to understand *why* someone would pose a threat to organizational assets. This includes recognizing that every threat actor isn’t intentionally out to cause harm. |

Bảo vệ bề mặt tấn công bắt đầu bằng cách suy nghĩ như một tác nhân đe dọa. Là một chuyên gia bảo mật, điều quan trọng là phải hiểu *tại sao* ai đó lại gây ra mối đe dọa cho tài sản của tổ chức. Điều này bao gồm việc nhận ra rằng không phải mọi tác nhân đe dọa đều cố ý gây hại.

|  |
| --- |
| It’s equally important to recognize the ways in which a threat actor might gain access to a system. Matching intentions with attack vectors is an invaluable skill as you continue to develop an attacker mindset. |

Điều quan trọng không kém là phải nhận ra những cách mà kẻ tấn công có thể truy cập vào hệ thống. Việc khớp ý định với các vectơ tấn công là một kỹ năng vô giá khi bạn tiếp tục phát triển tư duy của kẻ tấn công.

***3.4. Niru: Adopt an attacker mindset - Niru: Áp dụng tư duy tấn công***

|  |
| --- |
| [MUSIC] Hi, I'm Niru, and I lead the red team at Google. The red team at Google simulates attackers that are trying to hack into Google. They function as a sparring partner for the blue team, that is, the teams that build security controls, detection pipelines, or respond to incidents. So we help test all of those by simulating adversaries. So we hack into Google to make it harder to hack into Google. So it's like, hey, we found these issues with your system, now here are some recommendations we have, and how can we help you fix this? Thinking like an attacker is approaching a problem like an adversary. I generally have a predisposition to think like an attacker. [LAUGH]. It started when I was a kid and I used to play video games, and I used to ask, oh, do I have to beat the game in the way it's intended? Do I have to get the objective in the standard path? Looking at a system and asking the question, can I break into it? How do I break into it? What is likely to fail? If it fails, what does that give me? It's about taking apart systems and trying to understand it. Threat modeling is integral to almost anything a security professional does. It's about challenging assumptions. It's about approaching things from a different perspective. Rather than looking at the system from the perspective of a developer who is thinking about, how do I build the system in a way that works for people? You're putting on the hat of an attacker and saying, if I looked at the system, how would I break into it? It's important for all security professionals to think like an attacker because you code more defensively, you build things more defensively, and you break things more offensively. And what that means is you're building in this resilience into the system, and you're building in all these safeguards that are going to help protect the data, the systems, and the people. In order to build my attacker mindset, what I did is I would go pick people's brains. What that means is I can grab time with them and say, hey, how do you approach the system? What are the assumptions you're making? How do you build out the security safeguards that you're thinking about? My advice for people who are trying to build their own attacker mindset is go talk to people, be it in local meetups, in conferences, find yourself a CTF group and play these competitions with them. See how each person in the team approaches certain things and solves for it. Almost everything we do on a daily basis is online these days, like banking is online, grocery shopping is online, the electricity grid, the water supplies. All of this has happened in a short span of time, and now people are taking a step back and say, what does that mean for us? And cybersecurity folks are the ones who help make sure these systems are locked down and protected against these adversaries. If you're inquisitive, if you like taking things apart, if you like solving things, if you want to help make things secure, you should join cybersecurity. |

[ÂM NHẠC]Xin chào, tôi là Niru và tôi là trưởng nhóm đỏ tại Google.Nhóm đỏ tại Google mô phỏng những kẻ tấn công đang cố gắng xâm nhập vào Google.Họ hoạt động như một đối tác tập luyện cho đội xanh, tức là các độixây dựng các biện pháp kiểm soát an ninh, đường ống phát hiện hoặc ứng phó với sự cố.Vì vậy, chúng tôi giúp kiểm tra tất cả những điều đó bằng cách mô phỏng kẻ thù.Vì vậy, chúng tôi hack vào Google để khiến việc hack vào Google trở nên khó khăn hơn.Vì vậy, nó giống như, này, chúng tôi đã tìm thấy những vấn đề này với hệ thống của bạn,Sau đây là một số khuyến nghị của chúng tôi và làm sao chúng tôi có thể giúp bạn khắc phục điều này?Suy nghĩ như một kẻ tấn công là tiếp cận vấn đề như một kẻ thù.Tôi thường có khuynh hướng suy nghĩ như một kẻ tấn công.[CƯỜI].Nó bắt đầu khi tôi còn là một đứa trẻ và tôi thường chơi trò chơi điện tử, vàTôi từng tự hỏi, ôi, liệu tôi có phải thắng trò chơi theo đúng cách mà nó hướng dẫn không?Tôi có cần phải đạt được mục tiêu theo đường dẫn chuẩn không?Khi nhìn vào một hệ thống và đặt câu hỏi, liệu tôi có thể đột nhập vào đó không?Làm sao tôi có thể đột nhập vào đó?Điều gì có khả năng thất bại?Nếu thất bại thì tôi được lợi ích gì?Đó là việc tháo rời các hệ thống và cố gắng hiểu nó.Mô hình hóa mối đe dọa là một phần không thể thiếu trong hầu hết mọi việc mà một chuyên gia bảo mật thực hiện.Vấn đề là phải thách thức những giả định.Đó là cách tiếp cận mọi thứ theo một góc nhìn khác.Thay vì nhìn vào hệ thống từ góc nhìn của một nhà phát triểnsuy nghĩ về việc làm thế nào để xây dựng hệ thống theo cách có lợi cho mọi người?Bạn đang đội mũ của một kẻ tấn công và nói rằng, nếu tôi nhìn vào hệ thống,làm sao tôi có thể đột nhập vào đó?Điều quan trọng là tất cả các chuyên gia bảo mật phải suy nghĩ như một kẻ tấn côngbởi vì bạn mã hóa theo hướng phòng thủ hơn, bạn xây dựng mọi thứ theo hướng phòng thủ hơn vàbạn phá vỡ mọi thứ theo cách tấn công hơn.Và điều đó có nghĩa là bạn đang xây dựng khả năng phục hồi này vào hệ thống vàbạn đang xây dựng tất cả các biện pháp bảo vệ này để giúp bảo vệ dữ liệu,hệ thống và con người.Để xây dựng tư duy tấn công của tôi,điều tôi làm là đi moi não mọi người.Điều đó có nghĩa là tôi có thể dành thời gian cho họ và nói rằng,Này, bạn tiếp cận hệ thống như thế nào?Bạn đang đưa ra giả định gì?Bạn xây dựng các biện pháp bảo mật mà bạn đang nghĩ tới như thế nào?Lời khuyên của tôi dành cho những người đang cố gắng xây dựng tư duy tấn công của riêng mìnhlà nói chuyện với mọi người, có thể là trong các cuộc gặp gỡ địa phương, trong các hội nghị,tìm cho mình một nhóm CTF và tham gia các cuộc thi này cùng họ.Xem cách mỗi người trong nhóm tiếp cận và giải quyết một số vấn đề nhất định.Hầu như mọi thứ chúng ta làm hàng ngày đều trực tuyến ngày nay, giống như giao dịch ngân hàngtrực tuyến, mua sắm hàng tạp hóa trực tuyến, lưới điện, nguồn cung cấp nước.Tất cả những điều này đã xảy ra trong một khoảng thời gian ngắn, vàbây giờ mọi người đang lùi lại một bước và tự hỏi, điều đó có ý nghĩa gì với chúng ta?Và những người làm về an ninh mạng là những người giúp đảm bảo các hệ thống này được khóaxuống và được bảo vệ khỏi những kẻ thù này.Nếu bạn tò mò, nếu bạn thích tháo rời mọi thứ, nếu bạn thích giải quyết mọi thứ,nếu bạn muốn góp phần bảo mật mọi thứ, bạn nên tham gia an ninh mạng.

***3.5. Pathways through defenses - Con đường xuyên qua hàng phòng thủ***

|  |
| --- |
| To defend against attacks, organizations need to have more than just the understanding of the growing digital landscape around them. Positioning themselves ahead of a cyber threat also takes understanding the type of attacks that can be used against them. |

Để chống lại các cuộc tấn công,các tổ chức cần phải có nhiều hơnchỉ là sự hiểu biết vềbối cảnh kỹ thuật số đang phát triển xung quanh họ.Việc định vị bản thân trước mối đe dọa mạng cũng cầnhiểu loạicác cuộc tấn công có thể được sử dụng để chống lại họ.

|  |
| --- |
| Last time, we began exploring how the cloud has expanded the digital attack surface that organizations protect. As a result, cloud computing has led to an increase in the number attack vectors available. |

Lần trước, chúng ta đã bắt đầu khám phá cách đám mây đãmở rộng bề mặt tấn công kỹ thuật sốmà các tổ chức bảo vệ.Kết quả là, điện toán đám mây đã dẫn đếnsự gia tăng số lượng các phương tiện tấn công có sẵn.

|  |
| --- |
| Attack vectors refer to the pathways attackers use to penetrate security defenses. Like the doors and windows of a home, these pathways are the exploitable features of an attack surface. One example of an attack vector would be social media. Another would be removable media, like a USB drive. |

Các vectơ tấn công đề cập đến các con đườngkẻ tấn công sử dụng để xâm nhập vào hệ thống bảo mật.Giống như cửa ra vào và cửa sổ của một ngôi nhà,những con đường này là những đặc điểm có thể khai tháccủa một bề mặt tấn công.Một ví dụ về phương thức tấn công là mạng xã hội.Một cách khác là sử dụng phương tiện di động, như ổ USB.

|  |
| --- |
| Most people outside of security assume that cyber criminals are the only ones out there exploiting attack vectors. While attack vectors are used by malicious hackers to steal information, other groups use them too. For example, employees occasionally exploit attack vectors unintentionally. This happens a lot with social media platforms. Sometimes, employees post sensitive company news that shouldn't have been shared. At times, this same kind of thing happens on purpose. Social media platforms are also vectors that disgruntled employees use to intentionally share confidential information that can harm the company. |

Hầu hết mọi người bên ngoài an ninh đều cho rằngtội phạm mạng là những kẻ duy nhấtđang khai thác các hướng tấn công.Trong khi các vector tấn công được sử dụng bởitin tặc độc hại đánh cắp thông tin,các nhóm khác cũng sử dụng chúng.Ví dụ, nhân viênthỉnh thoảng khai thác các hướng tấn công một cách vô ý.Điều này thường xảy ra với các nền tảng truyền thông xã hội.Đôi khi, nhân viên đăng tin tức nhạy cảm của công tyđiều đó không nên được chia sẻ.Đôi khi, điều tương tự như thế này cũng xảy ra một cách có chủ đích.Các nền tảng truyền thông xã hội cũngcác vector khiến nhân viên bất mãnsử dụng để chia sẻ một cách có chủ ýthông tin bí mật có thể gây hại cho công ty.

|  |
| --- |
| We all treat attack vectors as critical risks to asset security. Attackers typically put forth a lot of effort planning their attacks before carrying them out. It's up to us as security professionals to put an even greater amount of effort into stopping them. |

Tất cả chúng ta đều coi các vectơ tấn công làrủi ro nghiêm trọng đối với an ninh tài sản.Những kẻ tấn công thường đưa ra rất nhiềunỗ lực lập kế hoạch tấn công trước khi thực hiện.Tùy thuộc vào chúng ta với tư cách là chuyên gia an ninhnỗ lực nhiều hơn nữa để ngăn chặn chúng.

|  |
| --- |
| Security teams do this by thinking of each vector with an attacker mindset. This starts with a simple question, "how would we exploit this vector?" We then go through a step-by-step process to answer our question. |

Các đội an ninh thực hiện điều này bằng cách nghĩ đếnmỗi vector có tư duy của kẻ tấn công.Điều này bắt đầu bằng một câu hỏi đơn giản,"Chúng ta có thể khai thác vectơ này như thế nào?"Sau đó chúng ta thực hiện theo từng bước mộtđể trả lời câu hỏi của chúng tôi.

|  |
| --- |
| First, when practicing an attacker mindset, we identify a target. This could be specific information, a system, a person, a group, or the organization itself. |

Đầu tiên, khi thực hành tư duy của kẻ tấn công,chúng tôi xác định mục tiêu.Đây có thể là thông tin cụ thể, một hệ thống,một người, một nhóm,hoặc chính tổ chức đó.

|  |
| --- |
| Next, we determine how the target can be accessed. What information is available that an attacker might take advantage of to reach the target? |

Tiếp theo, chúng ta xác định cách thức truy cập mục tiêu.Những thông tin nào có sẵn mà kẻ tấn công có thể biết?có thể tận dụng để đạt được mục tiêu?

|  |
| --- |
| Based on that information, the third step is to evaluate the attack vectors that can be exploited to gain entry. |

Dựa trên thông tin đó,bước thứ ba là đánh giácác phương thức tấn công có thể bị khai thác để xâm nhập.

|  |
| --- |
| And finally, we find the tools and methods of attack. What will the attackers use to carry this out? |

Và cuối cùng, chúng ta tìm ra các công cụ và phương pháp tấn công.Kẻ tấn công sẽ dùng gì để thực hiện hành động này?

|  |
| --- |
| Along the way, practicing an attacker mindset provides valuable insight into the best security controls to implement and the vulnerabilities that need to be monitored. Every organization has a long list of attack vectors to defend. While there are a lot of ways to protect them, there are a few common rules for doing this. |

Trên đường đi, thực hànhtư duy của kẻ tấn công cung cấp cái nhìn sâu sắc có giá trịvào các biện pháp kiểm soát an ninh tốt nhất để thực hiệnvà những lỗ hổng cần được giám sát.Mỗi tổ chức đều có một danh sách dàicủa các vectơ tấn công để phòng thủ.Mặc dù có rất nhiều cách để bảo vệ chúng,có một số quy tắc chung để thực hiện việc này.

|  |
| --- |
| One key to defending attack vectors is educating users about security vulnerabilities. These efforts are usually tied to an event. For example, advising them about a new phishing exploit that is targeting users in the organization. |

Một chìa khóa để bảo vệ các vectơ tấn công làgiáo dục người dùng về lỗ hổng bảo mật.Những nỗ lực này thường gắn liền với một sự kiện nào đó.Ví dụ, tư vấn cho họ vềmột khai thác lừa đảo mới đó lànhắm mục tiêu đến người dùng trong tổ chức.

|  |
| --- |
| Another rule is applying the principle of least privilege. We've explored least privilege earlier in this section. It's the idea that access rights should be limited to what's required to perform a task. Like we previously explored, this practice closes multiple security holes inside an organization's attack surface. |

Một quy tắc khác đang được áp dụngnguyên tắc đặc quyền tối thiểu.Chúng ta đã tìm hiểu về đặc quyền tối thiểu ở phần trước của phần này.Đó là ý tưởng rằng quyền truy cập nên đượcgiới hạn ở những gì cần thiết để thực hiện một nhiệm vụ.Như chúng ta đã khám phá trước đó,thực hành này đóng nhiều lỗ hổng bảo mậtbên trong bề mặt tấn công của một tổ chức.

|  |
| --- |
| Next, using the right security controls and tools can go a long way towards defending attack vectors. Even the most knowledgeable employees make security mistakes, like accidentally clicking on a malicious link in an email. Having the right security tools in place, like antivirus software, helps to defend attack vectors more efficiently and reduce the risk of human error. |

Tiếp theo, sử dụng các biện pháp kiểm soát bảo mật phù hợp vàcác công cụ có thể có tác dụng rất lớn trong việc bảo vệ các phương thức tấn công.Ngay cả những nhân viên hiểu biết nhấtmắc lỗi bảo mật,giống như vô tình nhấp vàomột liên kết độc hại trong email.Có các công cụ bảo mật phù hợp,giống như phần mềm diệt vi-rút,giúp bảo vệ các vectơ tấn công nhiều hơnhiệu quả và giảm thiểu nguy cơ sai sót của con người.

|  |
| --- |
| Last but not least, is building a diverse security team. This is one of the best ways to reduce the risk of attack vectors and prevent future attacks. |

Cuối cùng nhưng không kém phần quan trọng,đang xây dựng một đội ngũ an ninh đa dạng.Đây là một trong những cách tốt nhất để giảm nguy cơcác phương thức tấn công và ngăn chặn các cuộc tấn công trong tương lai.

|  |
| --- |
| Your own unique perspective can greatly improve the security team's ability to apply an attacker's mindset and stay one step ahead of potential threats. Keeping yourself informed is always important in this field. You're already off to a great start, so keep up the good work! |

Quan điểm độc đáo của riêng bạn có thểcải thiện đáng kể khả năng của đội an ninháp dụng tư duy của kẻ tấn công và ở lạiđi trước một bước so với các mối đe dọa tiềm tàng.Giữ cho mình được thông tin làluôn quan trọng trong lĩnh vực này.Bạn đã có một khởi đầu tuyệt vời rồi,vì vậy hãy tiếp tục làm việc tốt nhé!

***3.6. Self-reflection: Approach cybersecurity with an attacker mindset - Tự suy ngẫm: Tiếp cận an ninh mạng với tư duy của kẻ tấn công***

|  |
| --- |
| **Activity Overview**  Now that you've been introduced to attack surfaces and attack vectors, you can pause for a moment and think about what you are learning. In this self-reflection, you will think about how these factors can help identify threats and respond to brief questions.  You have learned many skills and concepts in this course. Completing this self-reflection will help you understand how you might use what you’ve learned for different tasks and roles in the security field. Answering and asking questions in this self-reflection will help to reinforce what you’ve learned, so it will be easier for you to remember it later. |

**Tổng quan hoạt động**

Bây giờ bạn đã được giới thiệu về bề mặt tấn công và các vector tấn công, bạn có thể dừng lại một chút và suy nghĩ về những gì bạn đang học. Trong phần tự phản ánh này, bạn sẽ nghĩ về cách các yếu tố này có thể giúp xác định các mối đe dọa và trả lời các câu hỏi ngắn.

Bạn đã học được nhiều kỹ năng và khái niệm trong khóa học này. Hoàn thành phần tự phản ánh này sẽ giúp bạn hiểu cách bạn có thể sử dụng những gì đã học cho các nhiệm vụ và vai trò khác nhau trong lĩnh vực an ninh. Trả lời và đặt câu hỏi trong phần tự phản ánh này sẽ giúp củng cố những gì bạn đã học, do đó, bạn sẽ dễ nhớ lại hơn sau này.

|  |
| --- |
| **Review the steps of applying an attacker mindset**  Previously, you learned that applying an attacker mindset to any situation starts by asking yourself, “How would I exploit this vector?” This will require you to consider two elements: the attack surface and its attack vectors.  Remember, an **attack surface** includes all the potential vulnerabilities that a threat actor could exploit. An **attack vector** is the pathway that an attacker uses to penetrate security defenses of an attack surface.  After considering these elements, you can then go through a step-by-step process to apply an attacker mindset:   * Identify a target * Determine how the target can be accessed * Evaluate attack vectors that can be exploited * Find the tools and methods of attack   For a refresher on the elements of an attacker mindset, you can review [the video on attack vectors](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/vRop4/pathways-through-defenses) and [the video on attack surfaces](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/iRZoR/digital-attack-surface-protecting-all-entry-points). |

**Xem lại các bước áp dụng tư duy của kẻ tấn công**

Trước đó, bạn đã học rằng việc áp dụng tư duy của kẻ tấn công vào bất kỳ tình huống nào đều bắt đầu bằng cách tự hỏi: "Tôi sẽ khai thác hướng tấn công này như thế nào?" Điều này đòi hỏi bạn phải xem xét hai yếu tố: bề mặt tấn công và các hướng tấn công của nó.

Hãy nhớ rằng, **bề mặt tấn công** bao gồm tất cả các lỗ hổng tiềm ẩn mà tác nhân đe dọa có thể khai thác. **Vectơ tấn công** là con đường mà kẻ tấn công sử dụng để xâm nhập vào các biện pháp phòng thủ bảo mật của bề mặt tấn công.

Sau khi xem xét các yếu tố này, bạn có thể thực hiện quy trình từng bước để áp dụng tư duy của kẻ tấn công:

* Xác định mục tiêu
* Xác định cách mục tiêu có thể được truy cập
* Đánh giá các vectơ tấn công có thể bị khai thác
* Tìm các công cụ và phương pháp tấn công

Để ôn lại các yếu tố trong tư duy của kẻ tấn công, bạn có thể xem lại[video về các vector tấn công](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/vRop4/pathways-through-defenses)Và[video về bề mặt tấn công](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/lecture/iRZoR/digital-attack-surface-protecting-all-entry-points).

|  |
| --- |
| **Reflection**  Consider what you reviewed about applying an attacker mindset in relation to securing your home environment:   * What are the attack surfaces of a home? Are they physical or digital? What are their vulnerabilities? Are they currently exposed to risk?   **1.**  Question 1  Now, write 2-3 sentences (40-60 words) that describe important characteristics about the attack surfaces of your home. Type your response in the text box.  Next, consider how an attacker might exploit the vulnerabilities of that surface.   * What are the attack vectors of this surface? Are there multiple entry points? How might the vulnerabilities be exploited? What defenses exist? Can new defenses be added?   **2.**  Question 2  Now, write 3-5 sentences (60-100 words) that explain what those attack vectors are and how you can apply the tools and/or strategies you’ve learned to protect your home. Type your response in the text box. |

**Sự phản xạ**

Hãy xem xét những gì bạn đã xem xét về việc áp dụng tư duy của kẻ tấn công liên quan đến việc bảo vệ môi trường gia đình của bạn:

* Bề mặt tấn công của một ngôi nhà là gì? Chúng là bề mặt vật lý hay kỹ thuật số? Điểm yếu của chúng là gì? Chúng hiện có đang phải đối mặt với rủi ro không?

**1 .**

Câu hỏi 1

Bây giờ, hãy viết 2-3 câu (40-60 từ) mô tả các đặc điểm quan trọng về bề mặt tấn công của ngôi nhà bạn. Nhập câu trả lời của bạn vào hộp văn bản.

Tiếp theo, hãy xem xét cách kẻ tấn công có thể khai thác lỗ hổng của bề mặt đó.

* Các vectơ tấn công của bề mặt này là gì? Có nhiều điểm vào không? Các lỗ hổng có thể bị khai thác như thế nào? Có những biện pháp phòng thủ nào? Có thể thêm biện pháp phòng thủ mới không?

Các bề mặt bị tấn công của ngôi nhà bao gồm tất cả các điểm xâm nhập tiềm ẩn để truy cập trái phép, chẳng hạn như cửa ra vào, cửa sổ và cửa gara. Đảm bảo những thứ này được an toàn bằng cách sử dụng ổ khóa chắc chắn, lắp đặt hệ thống an ninh và duy trì ánh sáng thích hợp có thể làm giảm đáng kể nguy cơ đột nhập⁴³. Thường xuyên kiểm tra và cập nhật các biện pháp này là rất quan trọng đối với an ninh gia đình.

|  |
| --- |
| Các bề mặt bị tấn công của ngôi nhà bao gồm tất cả các điểm xâm nhập tiềm ẩn để truy cập trái phép, chẳng hạn như cửa ra vào, cửa sổ và cửa gara. Đảm bảo những thứ này được an toàn bằng cách sử dụng ổ khóa chắc chắn, lắp đặt hệ thống an ninh và duy trì ánh sáng thích hợp có thể làm giảm đáng kể nguy cơ đột nhập⁴³. Thường xuyên kiểm tra và cập nhật các biện pháp này là rất quan trọng đối với an ninh gia đình. |

**2 .**

Câu hỏi 2

Bây giờ, hãy viết 3-5 câu (60-100 từ) giải thích các vectơ tấn công đó là gì và cách bạn có thể áp dụng các công cụ và/hoặc chiến lược đã học để bảo vệ ngôi nhà của mình. Nhập câu trả lời của bạn vào hộp văn bản.

|  |
| --- |
| Các vectơ tấn công là các phương pháp hoặc con đường mà tội phạm mạng sử dụng để có được quyền truy cập trái phép vào mạng gia đình và thiết bị của bạn. Các phương thức tấn công phổ biến bao gồm email lừa đảo, mạng Wi-Fi không bảo mật và phần mềm lỗi thời. Để bảo vệ ngôi nhà của mình, bạn có thể sử dụng mật khẩu mạnh, duy nhất cho tất cả các thiết bị và tài khoản, bật xác thực hai yếu tố, thường xuyên cập nhật phần mềm và bảo mật mạng Wi-Fi của mình bằng mật khẩu và mã hóa mạnh. Ngoài ra, việc thận trọng với các email và liên kết đáng ngờ có thể giúp ngăn chặn các cuộc tấn công lừa đảo. |

***3.7. Fortify against brute force cyber attacks - Tăng cường chống lại các cuộc tấn công mạng vũ phu***

|  |
| --- |
| **Fortify against brute force cyber attacks** |

**Tăng cường chống lại các cuộc tấn công mạng bằng vũ lực**

|  |
| --- |
| Usernames and passwords are one of the most common and important security controls in use today. They’re like the door lock that organizations use to restrict access to their networks, services, and data. But a major issue with relying on login credentials as a critical line of defense is that they’re vulnerable to being stolen and guessed by attackers. |

Tên người dùng và mật khẩu là một trong những biện pháp kiểm soát bảo mật phổ biến và quan trọng nhất hiện nay. Chúng giống như ổ khóa cửa mà các tổ chức sử dụng để hạn chế quyền truy cập vào mạng, dịch vụ và dữ liệu của họ. Nhưng một vấn đề lớn khi dựa vào thông tin đăng nhập như một tuyến phòng thủ quan trọng là chúng dễ bị đánh cắp và bị kẻ tấn công đoán ra.

|  |
| --- |
| In a video, you learned that **brute force attacks** are a trial-and-error process of discovering private information. In this reading, you’ll learn about the many tactics and tools used by threat actors to perform brute force attacks. You’ll also learn prevention strategies that organizations can use to defend against them. |

Trong video, bạn đã học được rằng **các cuộc tấn công brute force** là một quá trình thử và sai để khám phá thông tin riêng tư. Trong bài đọc này, bạn sẽ tìm hiểu về nhiều chiến thuật và công cụ mà các tác nhân đe dọa sử dụng để thực hiện các cuộc tấn công brute force. Bạn cũng sẽ tìm hiểu các chiến lược phòng ngừa mà các tổ chức có thể sử dụng để chống lại chúng.

|  |
| --- |
| **A matter of trial and error** |

**Một vấn đề thử nghiệm và sai sót**

|  |
| --- |
| One way of opening a closed lock is trying as many combinations as possible. Threat actors sometimes use similar tactics to gain access to an application or a network. |

Một cách để mở khóa đóng là thử càng nhiều kết hợp càng tốt. Kẻ tấn công đôi khi sử dụng các chiến thuật tương tự để truy cập vào ứng dụng hoặc mạng.

|  |
| --- |
| Attackers use a variety of tactics to find their way into a system:   * *Simple brute force attacks* are an approach in which attackers guess a user's login credentials. They might do this by entering any combination of username and password that they can think of until they find the one that works. * *Dictionary attacks* are a similar technique except in these instances attackers use a list of commonly used credentials to access a system. This list is similar to matching a definition to a word in a dictionary. * *Reverse brute force attacks* are similar to dictionary attacks, except they start with a single credential and try it in various systems until a match is found. * *Credential stuffing* is a tactic in which attackers use stolen login credentials from previous data breaches to access user accounts at another organization. A specialized type of credential stuffing is called *pass the hash*. These attacks reuse stolen, unsalted hashed credentials to trick an authentication system into creating a new authenticated user session on the network. |

Kẻ tấn công sử dụng nhiều chiến thuật khác nhau để tìm cách xâm nhập vào hệ thống:

* *Tấn công brute force đơn giản* là phương pháp mà kẻ tấn công đoán thông tin đăng nhập của người dùng. Chúng có thể thực hiện bằng cách nhập bất kỳ tổ hợp tên người dùng và mật khẩu nào mà chúng nghĩ ra được cho đến khi tìm ra tổ hợp phù hợp.
* *Tấn công từ điển* là một kỹ thuật tương tự, ngoại trừ trong những trường hợp này, kẻ tấn công sử dụng danh sách các thông tin xác thực thường dùng để truy cập hệ thống. Danh sách này tương tự như việc khớp định nghĩa với một từ trong từ điển.
* *Tấn công ngược bằng brute force* tương tự như tấn công từ điển, ngoại trừ việc chúng bắt đầu bằng một thông tin xác thực duy nhất và thử trên nhiều hệ thống khác nhau cho đến khi tìm thấy thông tin trùng khớp.
* *Nhồi thông tin xác thực* là một chiến thuật mà kẻ tấn công sử dụng thông tin đăng nhập bị đánh cắp từ các vụ vi phạm dữ liệu trước đó để truy cập vào tài khoản người dùng tại một tổ chức khác. Một loại nhồi thông tin xác thực chuyên biệt được gọi là *pass the hash* . Các cuộc tấn công này sử dụng lại thông tin xác thực đã băm không được đánh cắp để đánh lừa hệ thống xác thực tạo phiên người dùng đã xác thực mới trên mạng.

|  |
| --- |
| **Note:** Besides access credentials, encrypted information can sometimes be brute forced using a technique known as *exhaustive key search*. |

**Lưu ý:** Bên cạnh thông tin xác thực truy cập, thông tin được mã hóa đôi khi có thể bị tấn công bằng cách sử dụng một kỹ thuật được gọi là *tìm kiếm khóa toàn diện* .

|  |
| --- |
| Each of these methods involve a lot of guess work. Brute forcing your way into a system can be a tedious and time consuming process—especially when it’s done manually. That’s why threat actors often use tools to conduct their attacks. |

Mỗi phương pháp này đều đòi hỏi nhiều công sức để đoán. Việc tấn công brute force vào hệ thống có thể là một quá trình tẻ nhạt và tốn thời gian—đặc biệt là khi thực hiện thủ công. Đó là lý do tại sao những kẻ tấn công thường sử dụng các công cụ để thực hiện các cuộc tấn công của chúng.

|  |
| --- |
| **Tools of the trade** |

**Công cụ của nghề**

|  |
| --- |
| There are so many combinations that can be used to create a single set of login credentials. The number of characters, letters, and numbers that can be mixed together is truly incredible. When done manually, it could take someone years to try every possible combination. |

Có rất nhiều sự kết hợp có thể được sử dụng để tạo ra một bộ thông tin đăng nhập duy nhất. Số lượng ký tự, chữ cái và số có thể được kết hợp với nhau thực sự đáng kinh ngạc. Khi thực hiện thủ công, có thể mất nhiều năm để ai đó thử mọi sự kết hợp có thể.

|  |
| --- |
| Instead of dedicating the time to do this, attackers often use software to do the guess work for them. These are some common brute forcing tools:   * Aircrack-ng * Hashcat * John the Ripper * Ophcrack * THC Hydra |

Thay vì dành thời gian để làm điều này, kẻ tấn công thường sử dụng phần mềm để đoán công việc thay chúng. Sau đây là một số công cụ brute forcing phổ biến:

* Aircrack-ng
* Hashcat
* John the Ripper
* Ophcrack
* THC Hydra

|  |
| --- |
| Sometimes, security professionals use these tools to test and analyze their own systems. They each serve different purposes. For example, you might use Aircrack-ng to test a Wi-Fi network for vulnerabilities to brute force attack. |

Đôi khi, các chuyên gia bảo mật sử dụng các công cụ này để kiểm tra và phân tích hệ thống của riêng họ. Mỗi công cụ phục vụ các mục đích khác nhau. Ví dụ, bạn có thể sử dụng Aircrack-ng để kiểm tra mạng Wi-Fi để tìm lỗ hổng tấn công brute force.

|  |
| --- |
| **Prevention measures** |

**Biện pháp phòng ngừa**

|  |
| --- |
| Organizations defend against brute force attacks with a combination of technical and managerial controls. Each make cracking defense systems through brute force less likely:   * Hashing and salting * Multi-factor authentication (MFA) * CAPTCHA * Password policies |

Các tổ chức bảo vệ chống lại các cuộc tấn công bằng vũ lực bằng sự kết hợp giữa các biện pháp kiểm soát kỹ thuật và quản lý. Mỗi biện pháp làm cho khả năng bẻ khóa hệ thống phòng thủ bằng vũ lực ít xảy ra hơn:

* Băm nhỏ và ướp muối
* Xác thực đa yếu tố (MFA)
* Mã xác thực
* Chính sách mật khẩu

|  |
| --- |
| Technologies, like multi-factor authentication (MFA), reinforce each login attempt by requiring a second or third form of identification. Other important tools are CAPTCHA and effective password policies. |

Các công nghệ như xác thực đa yếu tố (MFA) củng cố mỗi lần đăng nhập bằng cách yêu cầu hình thức nhận dạng thứ hai hoặc thứ ba. Các công cụ quan trọng khác là CAPTCHA và chính sách mật khẩu hiệu quả.

|  |
| --- |
| **Hashing and salting** |

**Băm nhỏ và ướp muối**

|  |
| --- |
| Hashing converts information into a unique value that can then be used to determine its integrity. **Salting** is an additional safeguard that’s used to strengthen hash functions. It works by adding random characters to data, like passwords. This increases the length and complexity of hash values, making them harder to brute force and less susceptible to dictionary attacks. |

Băm chuyển đổi thông tin thành một giá trị duy nhất sau đó có thể được sử dụng để xác định tính toàn vẹn của nó. **Muối** là một biện pháp bảo vệ bổ sung được sử dụng để tăng cường các hàm băm. Nó hoạt động bằng cách thêm các ký tự ngẫu nhiên vào dữ liệu, như mật khẩu. Điều này làm tăng độ dài và độ phức tạp của các giá trị băm, khiến chúng khó bị tấn công bằng vũ lực và ít bị tấn công từ điển hơn.

|  |
| --- |
| **Multi-factor authentication (MFA)** |

**Xác thực đa yếu tố (MFA)**

|  |
| --- |
| **Multi-factor authentication** (MFA) is a security measure that requires a user to verify their identity in two or more ways to access a system or network. MFA is a layered approach to protecting information. MFA limits the chances of brute force attacks because unauthorized users are unlikely to meet each authentication requirement even if one credential becomes compromised. |

**Xác thực đa yếu tố** (MFA) là biện pháp bảo mật yêu cầu người dùng xác minh danh tính của họ theo hai hoặc nhiều cách để truy cập vào hệ thống hoặc mạng. MFA là phương pháp tiếp cận theo lớp để bảo vệ thông tin. MFA hạn chế khả năng xảy ra các cuộc tấn công bằng cách dùng vũ lực vì người dùng trái phép khó có thể đáp ứng từng yêu cầu xác thực ngay cả khi một thông tin xác thực bị xâm phạm.

|  |
| --- |
| **CAPTCHA** |

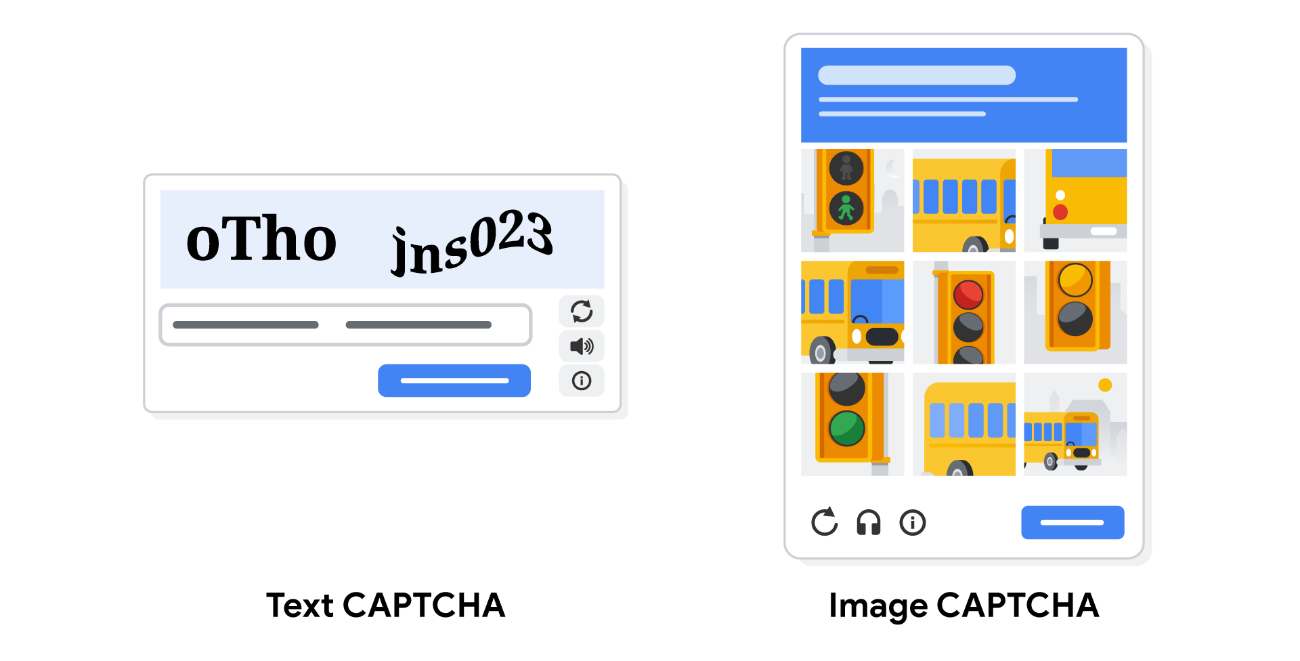
**Mã xác thực**

|  |
| --- |
| CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It is known as a challenge-response authentication system. CAPTCHA asks users to complete a simple test that proves they are human and not software that’s trying to brute force a password. |

CAPTCHA là viết tắt của Completely Automated Public Turing test to tell Computers and Humans Apart (Kiểm tra Turing công khai hoàn toàn tự động để phân biệt máy tính và con người). Nó được biết đến như một hệ thống xác thực thử thách-phản hồi. CAPTCHA yêu cầu người dùng hoàn thành một bài kiểm tra đơn giản để chứng minh rằng họ là con người chứ không phải phần mềm đang cố gắng tấn công mật khẩu.

|  |
| --- |
| Here are common CAPTCHA examples: |

Sau đây là một số ví dụ CAPTCHA phổ biến:



|  |
| --- |
| There are two types of CAPTCHA tests. One scrambles and distorts a randomly generated sequence of letters and/or numbers and asks users to enter them into a text box. The other test asks users to match images to a randomly generated word. You’ve likely had to pass a CAPTCHA test when accessing a web service that contains sensitive information, like an online bank account. |

Có hai loại kiểm tra CAPTCHA. Một loại xáo trộn và làm méo mó một chuỗi các chữ cái và/hoặc số được tạo ngẫu nhiên và yêu cầu người dùng nhập chúng vào hộp văn bản. Loại kiểm tra còn lại yêu cầu người dùng ghép hình ảnh với một từ được tạo ngẫu nhiên. Bạn có thể đã phải vượt qua bài kiểm tra CAPTCHA khi truy cập vào một dịch vụ web có chứa thông tin nhạy cảm, như tài khoản ngân hàng trực tuyến.

|  |
| --- |
| **Password policy** |

**Chính sách mật khẩu**

|  |
| --- |
| Organizations use these managerial controls to standardize good password practices across their business. For example, one of these policies might require users to create passwords that are at least 8 characters long and feature a letter, number, and symbol. Other common requirements can include password lockout policies. For example, a password lockout can limit the number of login attempts before access to an account is suspended and require users to create new, unique passwords after a certain amount of time. |

Các tổ chức sử dụng các biện pháp kiểm soát quản lý này để chuẩn hóa các thông lệ mật khẩu tốt trong toàn bộ doanh nghiệp của họ. Ví dụ, một trong những chính sách này có thể yêu cầu người dùng tạo mật khẩu dài ít nhất 8 ký tự và có chữ cái, số và ký hiệu. Các yêu cầu chung khác có thể bao gồm chính sách khóa mật khẩu. Ví dụ, khóa mật khẩu có thể giới hạn số lần đăng nhập trước khi quyền truy cập vào tài khoản bị đình chỉ và yêu cầu người dùng tạo mật khẩu mới, duy nhất sau một khoảng thời gian nhất định.

|  |
| --- |
| The purpose of each of these requirements is to create more possible password combinations. This lengthens the amount of time it takes an attacker to find one that will work. The [National Institute of Standards and Technology (NIST) Special Publication 800-63B](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf) provides detailed guidance that organizations can reference when creating their own password policies. |

Mục đích của mỗi yêu cầu này là tạo ra nhiều tổ hợp mật khẩu khả thi hơn. Điều này kéo dài thời gian kẻ tấn công tìm ra tổ hợp có thể hoạt động.[Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) Ấn phẩm đặc biệt 800-63B](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)cung cấp hướng dẫn chi tiết mà các tổ chức có thể tham khảo khi tạo chính sách mật khẩu của riêng mình.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Brute force attacks are simple yet reliable ways to gain unauthorized access to systems. Generally, the stronger a password is, the more resilient it is to being cracked. As a security professional, you might find yourself using the tools described above to test the security of your organization's systems. Recognizing the tactics and tools used to conduct a brute force attack is the first step towards stopping attackers. |

Tấn công bằng vũ lực là cách đơn giản nhưng đáng tin cậy để truy cập trái phép vào hệ thống. Nhìn chung, mật khẩu càng mạnh thì khả năng bị bẻ khóa càng cao. Là một chuyên gia bảo mật, bạn có thể thấy mình đang sử dụng các công cụ được mô tả ở trên để kiểm tra tính bảo mật của hệ thống tổ chức. Nhận biết các chiến thuật và công cụ được sử dụng để thực hiện tấn công bằng vũ lực là bước đầu tiên để ngăn chặn kẻ tấn công.

***3.8. Activity: Identify the attack vectors of a USB drive - Hoạt động: Xác định các vectơ tấn công của ổ USB***

|  |
| --- |
| **Activity Overview**  In this activity, you will assess the attack vectors of a USB drive. You will consider a scenario of finding a USB drive in a parking lot from both the perspective of an attacker and a target.  USBs, or flash drives, are commonly used for storing and transporting data. However, some characteristics of these small, convenient devices can also introduce security risks. Threat actors frequently use USBs to deliver malicious software, damage other hardware, or even take control of devices. **USB baiting** is an attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network. It relies on curious people to plug in an unfamiliar flash drive that they find.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan hoạt động**

Trong hoạt động này, bạn sẽ đánh giá các vectơ tấn công của ổ USB. Bạn sẽ xem xét một kịch bản tìm thấy ổ USB trong bãi đậu xe từ góc nhìn của cả kẻ tấn công và mục tiêu.

USB, hay ổ đĩa flash, thường được sử dụng để lưu trữ và vận chuyển dữ liệu. Tuy nhiên, một số đặc điểm của những thiết bị nhỏ, tiện lợi này cũng có thể gây ra rủi ro bảo mật. Những kẻ đe dọa thường sử dụng USB để phân phối phần mềm độc hại, làm hỏng phần cứng khác hoặc thậm chí kiểm soát các thiết bị. **USB baiting** là một cuộc tấn công trong đó kẻ đe dọa cố tình để lại một ổ USB chứa phần mềm độc hại để nhân viên tìm và cài đặt để vô tình lây nhiễm vào mạng. Nó dựa vào những người tò mò cắm một ổ đĩa flash lạ mà họ tìm thấy.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Mục tiếp theo của khóa học sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với bài làm của bạn.

|  |
| --- |
| **Scenario**  Review the following scenario. Then complete the step-by-step instructions.  You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There’s no one else around who might have dropped it, so you decide to pick it up out of curiosity.  You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it’s one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn’t connected to other files or networks, so the USB drive can’t affect other systems if it happens to be infected with malicious software. |

**Kịch bản**

Xem lại tình huống sau. Sau đó hoàn thành hướng dẫn từng bước.

Bạn là thành viên của đội an ninh tại Bệnh viện Rhetorical và đến làm việc vào một buổi sáng. Trên bãi đậu xe, bạn tìm thấy một ổ USB có in logo của bệnh viện. Không có ai khác xung quanh có thể làm rơi nó, vì vậy bạn quyết định nhặt nó lên vì tò mò.

Bạn mang ổ USB trở lại văn phòng nơi nhóm đã cài đặt phần mềm ảo hóa trên một máy trạm. Phần mềm ảo hóa có thể được sử dụng cho mục đích này vì đây là một trong những cách duy nhất để điều tra an toàn một ổ USB lạ. Phần mềm hoạt động bằng cách chạy một phiên bản mô phỏng của máy tính trên cùng một máy trạm. Mô phỏng này không được kết nối với các tệp hoặc mạng khác, do đó ổ USB không thể ảnh hưởng đến các hệ thống khác nếu nó bị nhiễm phần mềm độc hại.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions and answer the question below to complete the activity. |

**Hướng dẫn từng bước**

Làm theo hướng dẫn và trả lời câu hỏi bên dưới để hoàn thành hoạt động.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the link and select *Use Template*.  Link to template: [Parking lot USB exercise](https://docs.google.com/document/d/1jdI0FecPuabVB5ZI7na8C0Jm8J6bFlU76AEKD0T8dSw/template/preview?usp=sharing&resourcekey=0-BnHBngk9keuLxbaDs5koeQ) |

**Bước 1: Truy cập mẫu**

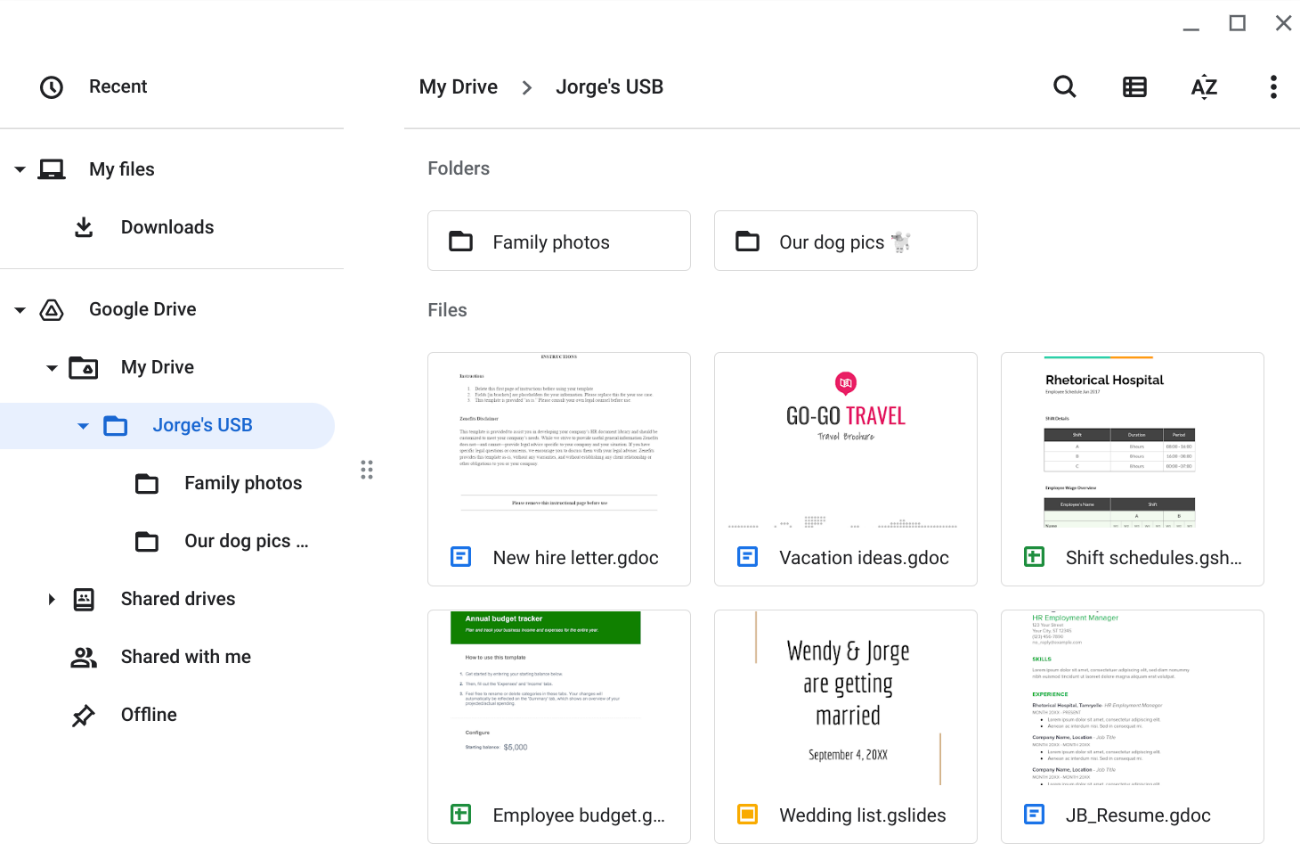
Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng mẫu* .

Liên kết đến mẫu: [Bài tập USB bãi đậu xe](https://docs.google.com/document/d/1jdI0FecPuabVB5ZI7na8C0Jm8J6bFlU76AEKD0T8dSw/template/preview?usp=sharing&resourcekey=0-BnHBngk9keuLxbaDs5koeQ)

|  |
| --- |
| **Step 2: Inspect the contents of the USB stick**  You create a virtual environment and plug the USB drive into the workstation. The contents of the device appear to belong to Jorge Bailey, the human resource manager at Rhetorical Hospital.  Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule.  Review the types of information that Jorge has stored on this device. Then, in the **Contents** row of the activity template, write **2-3 sentences** (40-60 words) about the type of information that's stored on the USB drive.  ***Note:*** *USB drives often contain an assortment of personally identifiable information (PII). Attackers can easily use this sensitive information to target the data owner or others around them.* |

**Bước 2: Kiểm tra nội dung của ổ USB**

Bạn tạo một môi trường ảo và cắm ổ USB vào máy trạm. Nội dung của thiết bị dường như thuộc về Jorge Bailey, giám đốc nhân sự tại Bệnh viện Rhetorical.



Ổ đĩa của Jorge chứa hỗn hợp các tệp cá nhân và liên quan đến công việc. Ví dụ, nó chứa các thư mục có vẻ như lưu trữ ảnh gia đình và thú cưng. Ngoài ra còn có một lá thư tuyển dụng mới và lịch làm việc của nhân viên.

Xem lại các loại thông tin mà Jorge đã lưu trữ trên thiết bị này. Sau đó, trong hàng **Nội dung** của mẫu hoạt động, hãy viết **2-3 câu** (40-60 từ) về loại thông tin được lưu trữ trên ổ USB.

***Lưu ý:*** *Ổ USB thường chứa nhiều loại thông tin nhận dạng cá nhân (PII). Kẻ tấn công có thể dễ dàng sử dụng thông tin nhạy cảm này để nhắm vào chủ sở hữu dữ liệu hoặc những người xung quanh.*

|  |
| --- |
| **Step 3: Apply an attacker mindset to the contents of the USB drive**  The flash drive appears to contain a mixture of personal and work-related files. Consider how an attacker might use this information if they obtained it. Also, consider whether this whole event was staged.  For example, an attacker could have placed these files on the USB drive as a distraction. They might have targeted Jorge or someone he knows, hoping they would find the device and plug it into their workstation. In doing so, the attacker could establish a backdoor into the company's systems while the unsuspecting target browsed through the files.  In the **Attacker mindset** row of the activity template, write **2-3 sentences** (40-60 words) about how this information could be used against Jorge or the hospital.  ***Pro tip:*** *The Cybersecurity and Infrastructure Security Agency (CISA) provides some* [*security tips on using caution with USB drives*](https://www.cisa.gov/news-events/news/using-caution-usb-drives)*, including keeping personal and business drives separate.* |

**Bước 3: Áp dụng tư duy của kẻ tấn công vào nội dung của ổ USB**

Ổ đĩa flash dường như chứa hỗn hợp các tệp cá nhân và liên quan đến công việc. Hãy xem xét cách kẻ tấn công có thể sử dụng thông tin này nếu chúng có được nó. Ngoài ra, hãy xem xét liệu toàn bộ sự kiện này có được dàn dựng hay không.

Ví dụ, kẻ tấn công có thể đã đặt những tập tin này vào ổ USB để đánh lạc hướng. Chúng có thể nhắm vào Jorge hoặc một người nào đó mà anh ta biết, hy vọng họ sẽ tìm thấy thiết bị và cắm nó vào máy trạm của họ. Khi làm như vậy, kẻ tấn công có thể thiết lập một cửa hậu vào hệ thống của công ty trong khi mục tiêu không nghi ngờ gì duyệt qua các tập tin.

Trong hàng **tư duy của kẻ tấn công** trong mẫu hoạt động, hãy viết **2-3 câu** (40-60 từ) về cách thông tin này có thể được sử dụng để chống lại Jorge hoặc bệnh viện.

***Mẹo chuyên nghiệp:*** *Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) cung cấp một số*[*mẹo bảo mật khi sử dụng ổ đĩa USB*](https://www.cisa.gov/news-events/news/using-caution-usb-drives)*, bao gồm việc tách biệt các ổ đĩa cá nhân và công việc.*

|  |
| --- |
| **Step 4: Analyze the risks of finding a parking lot USB**  You have *not* opened any of the files on the device, which is best practice.  Attackers sometimes conduct USB baiting attacks to deliver malicious code that they've crafted.  However, this USB drive was still a security risk even though it did not contain malicious code. It could have easily been found by an attacker who might have used its contents to plan a variety of attacks.  Consider some of the risks associated with USB baiting attacks:   * What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee? * What sensitive information could a threat actor find on a device like this? * How might that information be used against an individual or an organization?   In the **Risk analysis** row of the activity template, write **3 or 4 sentences** (60-80 words) describing any technical, operational, or managerial controls that could mitigate USB baiting attacks. |

**Bước 4: Phân tích rủi ro khi tìm bãi đậu xe USB**

Bạn *chưa* mở bất kỳ tệp nào trên thiết bị, đây là thông lệ tốt nhất.

Kẻ tấn công đôi khi thực hiện các cuộc tấn công mồi nhử USB để phát tán mã độc mà chúng đã tạo ra.

Tuy nhiên, ổ USB này vẫn là một rủi ro bảo mật mặc dù nó không chứa mã độc hại. Nó có thể dễ dàng bị kẻ tấn công tìm thấy và có thể sử dụng nội dung của nó để lên kế hoạch cho nhiều cuộc tấn công khác nhau.

Hãy xem xét một số rủi ro liên quan đến các cuộc tấn công mồi nhử USB:

* Những loại phần mềm độc hại nào có thể ẩn trong các thiết bị này? Điều gì có thể xảy ra nếu thiết bị bị nhiễm và bị một nhân viên khác phát hiện?
* Kẻ tấn công có thể tìm thấy thông tin nhạy cảm nào trên một thiết bị như thế này?
* Thông tin đó có thể được sử dụng để chống lại cá nhân hoặc tổ chức như thế nào?

Trong hàng **Phân tích rủi ro** của mẫu hoạt động, hãy viết **3 hoặc 4 câu** (60-80 từ) mô tả bất kỳ biện pháp kiểm soát kỹ thuật, vận hành hoặc quản lý nào có thể giảm thiểu các cuộc tấn công mồi nhử USB.

|  |
| --- |
| **What to Include in Your Response**  Be sure to address the following criteria in your completed activity:   * 2-3 sentences about the types of information stored on the USB drive * 2-3 sentences about how the information could be used against the owner and/or organization * 3-4 sentences analyzing the risks of USB baiting attacks |

**Những gì cần đưa vào phản hồi của bạn**

Hãy đảm bảo đáp ứng các tiêu chí sau trong hoạt động đã hoàn thành của bạn:

* 2-3 câu về các loại thông tin được lưu trữ trên ổ USB
* 2-3 câu về cách thông tin có thể được sử dụng để chống lại chủ sở hữu và/hoặc tổ chức
* 3-4 câu phân tích rủi ro của các cuộc tấn công mồi nhử USB

***3.9. Activity Exemplar: Identify the attack vectors of a USB drive - Ví dụ hoạt động: Xác định các vectơ tấn công của ổ USB***

|  |
| --- |
| **Activity Exemplar: Identify the attack vectors of a USB drive**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Ví dụ hoạt động: Xác định các vectơ tấn công của ổ USB**

Sau đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ này đáp ứng được kỳ vọng của hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link and select *Use Template*.  Link to exemplar:[Parking lot USB exercise](https://docs.google.com/document/d/11jmT2Czh0VgwhnI28MSF9bDROtPoctaM2qyaYR362_0/template/preview?usp=sharing) |

**Mẫu hoàn thành**

Để xem lại mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng mẫu* .

Liên kết đến ví dụ:[Bài tập USB bãi đậu xe](https://docs.google.com/document/d/11jmT2Czh0VgwhnI28MSF9bDROtPoctaM2qyaYR362_0/template/preview?usp=sharing)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.  ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your activity analyzes the types of information that can be found on a USB drive, how they can be exploited by a threat actor, and the types of attacks that can be hidden on these devices.* |

**Đánh giá mẫu**

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong khóa học.

***Lưu ý:*** *Ví dụ này thể hiện một cách có thể để hoàn thành hoạt động. Hoạt động của bạn có thể khác ở một số điểm. Điều quan trọng là hoạt động của bạn phân tích các loại thông tin có thể tìm thấy trên ổ USB, cách chúng có thể bị kẻ tấn công khai thác và các loại tấn công có thể ẩn trên các thiết bị này.*

|  |
| --- |
| The completed exemplar addresses the following criteria:   * 2-3 sentences about the types of information stored on the USB drive * 2-3 sentences about how the information could be used against the owner and/or organization * 3-4 sentences analyzing the risks of USB baiting attacks   Next, review the exemplar components:  **Contents:** The contents of the USB drive contain files that appear to belong to a specific person. It contains a mixture of personal and business-related information that should not be stored in the same place.  **Attacker mindset:** Any information that an attacker obtains can be used against someone. Information on a USB drive should be encrypted regardless of whether it’s personal or work-related.  **Risk analysis:** It’s unsafe to plug an unfamiliar USB drive into your computer because of the wide range of attacks that can be hidden on them. Promoting employee awareness of USB baiting attacks is a managerial control that can reduce the risks of a negative event. Routinely scanning for viruses is an example of an operational control that can be implemented. And disabling Autoplay on all PCs is a technical precaution that can be taken. |

Bản mẫu hoàn chỉnh đáp ứng các tiêu chí sau:

* 2-3 câu về các loại thông tin được lưu trữ trên ổ USB
* 2-3 câu về cách thông tin có thể được sử dụng để chống lại chủ sở hữu và/hoặc tổ chức
* 3-4 câu phân tích rủi ro của các cuộc tấn công mồi nhử USB

Tiếp theo, hãy xem lại các thành phần mẫu:

**Nội dung:** Nội dung của ổ USB chứa các tệp dường như thuộc về một người cụ thể. Nó chứa hỗn hợp thông tin cá nhân và thông tin liên quan đến công việc không nên được lưu trữ ở cùng một nơi.

**Tư duy của kẻ tấn công:** Bất kỳ thông tin nào mà kẻ tấn công có được đều có thể được sử dụng để chống lại ai đó. Thông tin trên ổ USB phải được mã hóa bất kể là thông tin cá nhân hay liên quan đến công việc.

**Phân tích rủi ro:** Không an toàn khi cắm ổ USB lạ vào máy tính của bạn vì có nhiều loại tấn công có thể ẩn trên đó. Thúc đẩy nhận thức của nhân viên về các cuộc tấn công mồi nhử USB là một biện pháp kiểm soát quản lý có thể giảm thiểu rủi ro của một sự kiện tiêu cực. Quét virus thường xuyên là một ví dụ về biện pháp kiểm soát hoạt động có thể được triển khai. Và vô hiệu hóa Tự động phát trên tất cả PC là một biện pháp phòng ngừa kỹ thuật có thể được thực hiện.

***3.10. Test your knowledge: Cyber attacker mindset - Kiểm tra kiến ​​thức của bạn: Tư duy tấn công mạng***

**4. Review: Vulnerabilities in systems - Đánh giá: Lỗ hổng trong hệ thống**

***4.1. Wrap-up – Tóm tắt***

|  |
| --- |
| Here we are at the end of this section! Can you believe it? I had so much fun exploring the world of vulnerabilities. I hope you felt the same. More importantly, I hope you got a better sense of how complex a landscape the digital world is. This environment is filled with gaps that attackers can use to gain unauthorized access to assets, making it a challenge to defend. |

Đây là chúng ta ở cuốiphần này! Bạn có tin được không?Tôi thực sự thích thú khi khám phá thế giới của những điểm yếu.Tôi hy vọng bạn cũng cảm thấy như vậy.Quan trọng hơn, tôi hy vọng bạn hiểu rõ hơnthế giới số phức tạp đến mức nào.Môi trường này chứa đầy những lỗ hổng mà kẻ tấn công có thểsử dụng để truy cập trái phép vào tài sản,khiến việc phòng thủ trở nên khó khăn.

|  |
| --- |
| We've explored a lot of information this time around, so let's quickly recap what we've covered. |

Lần này chúng tôi đã khám phá rất nhiều thông tin,vậy chúng ta hãy cùng tóm tắt lại những gì đã học nhé.

|  |
| --- |
| You learned about the vulnerability management process, starting with the defense-in-depth model. You learned about the layers of this security framework and how each of them work together to build a stronger defense. |

Bạn đã tìm hiểu về quy trình quản lý lỗ hổng,bắt đầu với mô hình phòng thủ theo chiều sâu.Bạn đã học về các lớp củakhuôn khổ bảo mật này vàcách mỗi người làm việc cùng nhauđể xây dựng một hàng phòng thủ vững chắc hơn.

|  |
| --- |
| You then learned about the CVE list that's used to find cataloged vulnerabilities. This is a great addition to your growing security toolbox. |

Sau đó bạn đã tìm hiểu về danh sách CVEđược sử dụng để tìm các lỗ hổng đã được lập danh mục.Đây là một bổ sung tuyệt vời chohộp công cụ bảo mật ngày càng mở rộng của bạn.

|  |
| --- |
| After that, you learned of the attack surfaces that businesses protect. We discussed physical and digital surfaces and the challenges of defending the cloud. |

Sau đó, bạn đã học đượccác bề mặt tấn công được doanh nghiệp bảo vệ.Chúng tôi thảo luận về bề mặt vật lý và kỹ thuật sốvà những thách thức trong việc bảo vệ đám mây.

|  |
| --- |
| We finished up by exploring common attack vectors, where you learned how security teams use an attacker mindset to identify the security gaps that cyber criminals try to exploit. |

Chúng tôi kết thúc bằng việc khám phá các vectơ tấn công phổ biến,nơi bạn học được cách các đội an ninhsử dụng tư duy của kẻ tấn công đểxác định các lỗ hổng bảo mậtmà tội phạm mạng đang cố gắng khai thác.

|  |
| --- |
| Every one of the vulnerabilities that we've discussed so far is faced with a number of threats. |

Mọi lỗ hổng mà chúng ta đã thảo luậncho đến nay vẫn phải đối mặt với một số mối đe dọa.

|  |
| --- |
| When we get back together, we're going to expand our attacker mindset even further by exploring specific type of attacks that cybercriminals commonly use. We'll look at things like malware and the techniques attackers use to compromise defense systems. By exploring how these tools and tactics work, you'll gain a clearer understanding of the threats they pose. We'll then wrap up by investigating how security teams stop these threats from damaging our organizations' operations, their reputation, and most importantly, their customers and employees. |

Khi chúng ta quay lại với nhau,chúng ta sẽ mở rộng tư duy tấn công của mìnhthậm chí xa hơn nữa bằngkhám phá loại tấn công cụ thểmà tội phạm mạng thường sử dụng.Chúng ta sẽ xem xét những thứ như phần mềm độc hại và các kỹ thuậtkẻ tấn công sử dụng để xâm nhập vào hệ thống phòng thủ.Bằng cách khám phá cách thức hoạt động của các công cụ và chiến thuật này,bạn sẽ hiểu rõ hơnvề những mối đe dọa mà chúng gây ra.Sau đó chúng tôi sẽ kết thúc bằng cách điều tra cách các nhóm bảo mậtngăn chặn những mối đe dọa này từgây tổn hại đến hoạt động của tổ chức chúng tôi,danh tiếng của họ, và quan trọng nhất là,khách hàng và nhân viên của họ.

|  |
| --- |
| You've done a fantastic job getting to this point. When you're ready, let's finish the journey together. I'm looking forward to being back with you again. |

Bạn đã làm rất tốt để đạt tới được thành quả này.Khi bạn đã sẵn sàng, chúng ta hãy cùng nhau hoàn thành chuyến đi.Tôi rất mong được gặp lại bạn lần nữa.

***4.2. Glossary terms from module 3 - Thuật ngữ trong học phần***

|  |
| --- |
| **Glossary terms from module 3** |

**Thuật ngữ trong mô-đun 3**

|  |
| --- |
| **Terms and definitions from Course 5, Module 3** |

**Các thuật ngữ và định nghĩa từ Khóa học 5, Mô -đun 3**

|  |
| --- |
| **Advanced persistent threat (APT):** An instance when a threat actor maintains unauthorized access to a system for an extended period of time |

**Mối đe dọa dai dẳng nâng cao (APT):** Trường hợp kẻ tấn công duy trì quyền truy cập trái phép vào hệ thống trong thời gian dài

|  |
| --- |
| **Attack surface:** All the potential vulnerabilities that a threat actor could exploit |

**Bề mặt tấn công:** Tất cả các lỗ hổng tiềm ẩn mà kẻ tấn công có thể khai thác

|  |
| --- |
| **Attack tree:** A diagram that maps threats to assets |

**Cây tấn công:** Sơ đồ ánh xạ các mối đe dọa đến tài sản

|  |
| --- |
| **Attack vector:** The pathways attackers use to penetrate security defenses |

**Vectơ tấn công:** Các con đường kẻ tấn công sử dụng để xâm nhập vào hệ thống phòng thủ an ninh

|  |
| --- |
| **Bug bounty:** Programs that encourage freelance hackers to find and report vulnerabilities |

**Tiền thưởng cho lỗi:** Chương trình khuyến khích tin tặc tự do tìm và báo cáo lỗ hổng

|  |
| --- |
| **Common Vulnerabilities and Exposures (CVE®) list:** An openly accessible dictionary of known vulnerabilities and exposures |

**Danh sách các lỗ hổng và điểm yếu phổ biến (CVE®):** Từ điển có thể truy cập công khai về các lỗ hổng và điểm yếu đã biết

|  |
| --- |
| **Common Vulnerability Scoring System (CVSS):** A measurement system that scores the severity of a vulnerability |

**Hệ thống chấm điểm lỗ hổng chung (CVSS):** Một hệ thống đo lường chấm điểm mức độ nghiêm trọng của lỗ hổng

|  |
| --- |
| **CVE Numbering Authority (CNA):** An organization that volunteers to analyze and distribute information on eligible CVEs |

**Cơ quan đánh số CVE (CNA):** Một tổ chức tình nguyện phân tích và phân phối thông tin về các CVE đủ điều kiện

|  |
| --- |
| **Defense in depth:** A layered approach to vulnerability management that reduces risk |

**Phòng thủ chuyên sâu:** Một cách tiếp cận theo từng lớp để quản lý lỗ hổng giúp giảm thiểu rủi ro

|  |
| --- |
| **Exploit:** A way of taking advantage of a vulnerability |

**Khai thác:** Một cách lợi dụng lỗ hổng

|  |
| --- |
| **Exposure:** A mistake that can be exploited by a threat |

**Phơi bày:** Một sai lầm có thể bị lợi dụng bởi mối đe dọa

|  |
| --- |
| **Hacker:** Any person who uses computers to gain access to computer systems, networks, or data |

**Hacker:** Bất kỳ người nào sử dụng máy tính để truy cập vào hệ thống máy tính, mạng hoặc dữ liệu

|  |
| --- |
| **MITRE:** A collection of non-profit research and development centers |

**MITRE:** Một tập hợp các trung tâm nghiên cứu và phát triển phi lợi nhuận

|  |
| --- |
| **Security hardening:** The process of strengthening a system to reduce its vulnerability and attack surface |

**Tăng cường bảo mật:** Quá trình tăng cường hệ thống để giảm thiểu lỗ hổng và bề mặt tấn công

|  |
| --- |
| **Threat actor:** Any person or group who presents a security risk |

**Tác nhân đe dọa:** Bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro về an ninh

|  |
| --- |
| **Vulnerability:** A weakness that can be exploited by a threat |

**Điểm yếu:** Điểm yếu có thể bị khai thác bởi mối đe dọa

|  |
| --- |
| **Vulnerability assessment:** The internal review process of a company’s security systems |

**Đánh giá lỗ hổng:** Quá trình xem xét nội bộ các hệ thống bảo mật của công ty

|  |
| --- |
| **Vulnerability management:** The process of finding and patching vulnerabilities |

**Quản lý lỗ hổng:** Quá trình tìm và vá lỗ hổng

|  |
| --- |
| **Vulnerability scanner:** Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network |

**Máy quét lỗ hổng:** Phần mềm tự động so sánh các lỗ hổng và nguy cơ phổ biến hiện có với các công nghệ trên mạng

|  |
| --- |
| **Zero-day:** An exploit that was previously unknown |

**Zero-day:** Một khai thác trước đây chưa được biết đến

***4.3. Module 3 challenge - Thử thách mô-đun 3***

# **Module 4: Threats to asset security – Các mối đe dọa đối với bảo mật tài sản**

|  |
| --- |
| You will explore common types of threats to digital asset security. You'll also examine the tools and techniques used by cybercriminals to target assets. In addition, you'll be introduced to the threat modeling process and learn ways security professionals stay ahead of security breaches. |

Bạn sẽ khám phá các loại mối đe dọa phổ biến đối với bảo mật tài sản kỹ thuật số. Bạn cũng sẽ xem xét các công cụ và kỹ thuật mà tội phạm mạng sử dụng để nhắm mục tiêu vào tài sản. Ngoài ra, bạn sẽ được giới thiệu về quy trình mô hình hóa mối đe dọa và tìm hiểu cách các chuyên gia bảo mật luôn đi trước các vi phạm bảo mật.

|  |
| --- |
| **Learning Objectives**   * Identify forms of social engineering. * Identify different types of malware. * Identify forms of web-based exploits. * Summarize the threat modeling process. |

**Mục tiêu học tập**

* Xác định các hình thức kỹ thuật xã hội.
* Xác định các loại phần mềm độc hại khác nhau.
* Xác định các hình thức khai thác trên web.
* Tóm tắt quá trình lập mô hình mối đe dọa.

**1. Social engineering – Kỹ thuật xã hội**

***1.1. Welcome to module 4 - Chào mừng đến với mô-đun 4***

|  |
| --- |
| Here we are! The final section of the course. What are amazing job you've done so far! Putting in the time, dedication, and hard work to get to this point is definitely something to celebrate. But we're not through yet. As we near the end of this course, now's the time to focus and finish strong. Let's turn our attention to threats. |

Đây rồi! Phần cuối cùng của khóa học.Bạn đã làm được những công việc tuyệt vời như thế nào cho đến giờ?Đưa vào thời gian,sự cống hiến và làm việc chăm chỉ để đạt đượcđây chắc chắn là điều đáng mừng.Nhưng chúng ta vẫn chưa xong đâu.Khi chúng ta gần kết thúc khóa học này,Bây giờ là lúc tập trung và hoàn thành tốt.Chúng ta hãy chú ý đến các mối đe dọa.

|  |
| --- |
| We've already explored assets, vulnerabilities, and the controls used to protect both. A common theme between those two topics has been the wide range of assets and vulnerabilities out there. The world of threats is no different. |

Chúng tôi đã khám phá tài sản,lỗ hổng bảo mật và các biện pháp kiểm soát được sử dụng để bảo vệ cả hai.Một chủ đề chung giữa hai chủ đề đó làđã có nhiều loại tài sảnvà những lỗ hổng ngoài kia.Thế giới của những mối đe dọa cũng không có gì khác biệt.

|  |
| --- |
| If you recall, threats are any circumstance or event that can negatively impact assets. In this part of the course, you're going to expand your security mindset by getting a high-level view of the most dangerous threats facing organizations today. |

Nếu bạn nhớ lại, mối đe dọa là bất kỳ hoàn cảnh nàohoặc sự kiện có thể tác động tiêu cực đến tài sản.Trong phần này của khóa học,bạn sẽ mở rộng tư duy bảo mật của mình bằng cách nhận đượcmột cái nhìn cấp cao vềnhững mối đe dọa nguy hiểm nhất mà các tổ chức phải đối mặt hiện nay.

|  |
| --- |
| First, we're going to begin by exploring social engineering tactics, psychological tricks that attackers use to gain unauthorized access to assets. |

Đầu tiên, chúng ta sẽ bắt đầu bằngkhám phá các chiến thuật kỹ thuật xã hội,thủ đoạn tâm lý mà kẻ tấn công sử dụng đểcó quyền truy cập trái phép vào tài sản.

|  |
| --- |
| Next, we'll explore a common type of threat that's been around since the start of personal computers, malware. We're going to spend some time investigating the major types of malware. |

Tiếp theo, chúng ta sẽ khám phá một loại mối đe dọa phổ biến đã đượckể từ khi máy tính cá nhân ra đời, phần mềm độc hại.Chúng ta sẽ dành chút thời gianđiều tra các loại phần mềm độc hại chính.

|  |
| --- |
| After that, we'll turn our attention to web-based exploits. Most organizations these days operate in a digital space, and many of them are new to it. In this section of the course, you're going to learn about some of the most common threats that organizations face online. |

Sau đó, chúng ta sẽ quay lạisự chú ý của chúng tôi tới các hoạt động khai thác trên web.Hầu hết các tổ chức ngày nay hoạt động trong không gian kỹ thuật số,và nhiều người trong số họ còn mới mẻ với việc này.Trong phần này của khóa học,bạn sẽ học về một sốnhững mối đe dọa phổ biến nhất mà các tổ chức phải đối mặt trực tuyến.

|  |
| --- |
| Finally, after exploring common threats that organizations deal with, we're going to wrap up by exploring the threat modeling process. |

Cuối cùng, sau khi khám phácác mối đe dọa phổ biến mà các tổ chức phải đối mặt,chúng ta sẽ kết thúc bằng việc khám pháquá trình mô hình hóa mối đe dọa.

|  |
| --- |
| Understanding threats is essential for a security analyst, and there's a lot to cover. So, let's get started! |

Hiểu được các mối đe dọa là điều cần thiết chomột nhà phân tích bảo mật và có rất nhiều thứ cần phải đề cập.Vậy thì, chúng ta hãy bắt đầu nhé!

***1.2. The criminal art of persuasion - Nghệ thuật thuyết phục tội phạm***

|  |
| --- |
| When you hear the word "cybercriminal", what comes to mind? You may imagine a hacker hunched over a computer in a dark room. If this is what came to mind, you're not alone. In fact, this is what most people outside of security think of. But online criminals aren't always that different from those operating in the real world. |

Khi bạn nghe từ "tội phạm mạng",bạn nghĩ tới điều gì?Bạn có thể tưởng tượng một hackercúi gằm mặt trên máy tính trong phòng tối.Nếu đây là điều bạn nghĩ tới thì bạn không phải là người duy nhất.Trên thực tế, đây chính là điềuhầu hết mọi người bên ngoài ngành an ninh đều nghĩ đến.Nhưng tội phạm trực tuyến không phải lúc nào cũng như vậykhác với những hoạt động trong thế giới thực.

|  |
| --- |
| Malicious hackers are just one type of online criminal. They are a specific kind that relies on sophisticated computer programming skills to pull off their attacks. There are other ways to commit crimes that don't require programming skills. Sometimes, criminals rely on a more traditional approach, manipulation. |

Tin tặc độc hại chỉ là một loại tội phạm trực tuyến.Chúng là một loại cụ thể dựa vàokỹ năng lập trình máy tính tinh viđể thực hiện các cuộc tấn công của họ.Có nhiều cách khác để phạm tộikhông yêu cầu kỹ năng lập trình.Đôi khi, tội phạm dựa vàomột cách tiếp cận truyền thống hơn, đó là thao túng.

|  |
| --- |
| Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. |

Kỹ thuật xã hội làmột kỹ thuật thao túng khai tháclỗi của con người để đạt đượcthông tin cá nhân, quyền truy cập hoặc đồ vật có giá trị.

|  |
| --- |
| These tactics trick people into breaking normal security procedures on the attacker's behalf. This can lead to data exposures, widespread malware infections, or unauthorized access to restricted systems. Social engineering attacks can happen anywhere. They happen online, in-person, and through other interactions. Threat actors use many different tactics to carry out their attacks. |

Những chiến thuật này lừa mọi người phá vỡcác thủ tục bảo mật thông thường thay mặt cho kẻ tấn công.Điều này có thể dẫn đến việc lộ dữ liệu,nhiễm phần mềm độc hại lan rộng, hoặctruy cập trái phép vào các hệ thống bị hạn chế.Các cuộc tấn công kỹ thuật xã hội có thể xảy ra ở bất cứ đâu.Chúng xảy ra trực tuyến, trực tiếp,và thông qua các tương tác khác.Những kẻ đe dọa sử dụng nhiều chiến thuật khác nhauđể thực hiện các cuộc tấn công của họ.

|  |
| --- |
| Some attacks can take a matter of seconds to perform. For example, someone impersonating tech support asks an employee for their password to fix their computer. Other attacks can take months or longer, such as threat actors monitoring an employee's social media. The employee might post a comment saying they've gotten a temporary position in a new role at the company. An attacker might use an opportunity like this to target the temporary worker, who is likely to be less knowledgeable about security procedures. |

Một số cuộc tấn công có thể mất vài giây để thực hiện.Ví dụ, một người nào đó mạo danhhỗ trợ kỹ thuật hỏi một nhân viênđể có mật khẩu sửa máy tính của họ.Các cuộc tấn công khác có thể mất nhiều tháng hoặc lâu hơn,chẳng hạn như các tác nhân đe dọatheo dõi phương tiện truyền thông xã hội của nhân viên.Nhân viên có thể đăng bình luận nói rằng họ đã nhận đượcmột vị trí tạm thời trong vai trò mới tại công ty.Kẻ tấn công có thể sử dụng cơ hội như thế này để nhắm mục tiêungười lao động tạm thời, người có khả năng làít hiểu biết về các thủ tục bảo mật.

|  |
| --- |
| Regardless of the timeframe, knowing what to look for can help you quickly identify and stop an attack in its tracks. |

Bất kể khung thời gian,biết những gì cần tìm có thể giúp bạn nhanh chóngxác định và ngăn chặn cuộc tấn công ngay từ đầu.

|  |
| --- |
| There are multiple stages of social engineering attacks. The first is usually to prepare. At this stage, attackers gather information about their target. Using the intel, they'll determine the best way to exploit them. |

Có nhiều giai đoạn của cuộc tấn công kỹ thuật xã hội.Đầu tiên thường là chuẩn bị.Ở giai đoạn này, những kẻ tấn côngthu thập thông tin về mục tiêu của họ.Sử dụng thông tin tình báo, họ sẽxác định cách tốt nhất để khai thác chúng.

|  |
| --- |
| In the next stage, attackers establish trust. This is often referred to as pretexting. Here, attackers use the information they gathered earlier to open a line of communication. They'll typically disguise themselves to trick their target into a false sense of trust. |

Ở giai đoạn tiếp theo, kẻ tấn công sẽ thiết lập lòng tin.Điều này thường được gọi là ngụy biện.Ở đây, kẻ tấn công sử dụng thông tin họđã tập hợp trước đó để mở đường liên lạc.Họ thường cải trang để lừa gạtmục tiêu của họ vào một cảm giác tin tưởng sai lầm.

|  |
| --- |
| After that, attackers use persuasion tactics. This stage is where the earlier preparation really matters. This is when the attacker manipulates their target into volunteering information. Sometimes they do this by using specific vocabulary that makes them sound like a member of the organization. |

Sau đó, kẻ tấn công sử dụng chiến thuật thuyết phục.Giai đoạn này là nơi chuẩn bị trước đóthực sự quan trọng.Đây là lúc kẻ tấn công thao túngmục tiêu của họ vào thông tin tình nguyện.Đôi khi họ làm điều này bằng cách sử dụng từ vựng cụ thểđiều đó khiến họ nghe giống như một thành viên của tổ chức.

|  |
| --- |
| The final stage of the process is to disconnect from the target. After they collect the information they want, attackers break communication with their target. They disappear to cover their tracks. |

Giai đoạn cuối cùng của quá trìnhlà ngắt kết nối với mục tiêu.Sau khi họ thu thập được thông tin họ muốn,kẻ tấn công cắt đứt liên lạc với mục tiêu của mình.Họ biến mất để che giấu dấu vết.

|  |
| --- |
| Criminals who use social engineering are stealthy. The digital world has expanded their capabilities. It's also created more ways for them to go unnoticed. Still, there are ways that we can prevent their attacks. |

Những tên tội phạm sử dụng kỹ thuật xã hội rất tinh vi.Thế giới số đã mở rộng khả năng của họ.Nó cũng tạo ra nhiều cách hơn để chúng không bị chú ý.Tuy nhiên, vẫn có cách để chúng ta có thể ngăn chặn các cuộc tấn công của chúng.

|  |
| --- |
| Implementing managerial controls like policies, standards, and procedures, are one of the first lines of defense. For example, businesses often follow the patch management standard defined in NIST Special Publication 800-40. These standards are used to create procedures for updating operating systems, applications, and firmware that can be exploited. |

Thực hiện các biện pháp kiểm soát quản lý như chính sách,tiêu chuẩn và thủ tục,là một trong những tuyến phòng thủ đầu tiên.Ví dụ, các doanh nghiệp thường theo dõitiêu chuẩn quản lý bản vá được xác định trongẤn phẩm đặc biệt 800-40 của NIST.Các tiêu chuẩn này được sử dụng để tạo racác thủ tục cập nhật hệ điều hành,các ứng dụng và chương trình cơ sở có thể bị khai thác.

|  |
| --- |
| Staying informed of trends is also a major priority for any security professional. An even better defense against social engineering attacks is sharing what you know with others. Attackers play on our natural curiosity and desire to help one another. Their hope is that targets won't think too hard about what's going on. Teaching the signs of attack to others goes a long way towards preventing threats. |

Việc cập nhật thông tin về xu hướng cũng làlà ưu tiên hàng đầu của bất kỳ chuyên gia an ninh nào.Một sự phòng thủ thậm chí còn tốt hơn chống lạitấn công kỹ thuật xã hội làchia sẻ những gì bạn biết với người khác.Những kẻ tấn công lợi dụng sự tò mò tự nhiên của chúng tavà mong muốn giúp đỡ lẫn nhau.Hy vọng của họ là mục tiêu sẽ không nghĩquá khó khăn về những gì đang diễn ra.Dạy những dấu hiệu tấn công cho người kháccó tác dụng to lớn trong việc ngăn ngừa các mối đe dọa.

|  |
| --- |
| Social engineering is a threat to the assets and privacy of both individuals and organizations. Malicious attackers use a variety of tactics to confuse and manipulate their targets. When we get back together next time, we're going to explore one of the most commonly used techniques that's a major problem for organizations of all sizes. |

Kỹ thuật xã hội là mối đe dọa đối với tài sản vàquyền riêng tư của cả cá nhân và tổ chức.Những kẻ tấn công độc hại sử dụng nhiều loạichiến thuật để gây nhầm lẫn và thao túng mục tiêu.Khi chúng ta quay lại với nhau lần sau,chúng ta sẽ khám phá một trongcác kỹ thuật được sử dụng phổ biến nhấtđó là một vấn đề lớn đối với các tổ chức ở mọi quy mô.

***1.3. Social engineering tactics - Nghệ thuật thuyết phục tội phạm***

|  |
| --- |
| **Social engineering tactics** |

**Chiến thuật kỹ thuật xã hội**

|  |
| --- |
| Social engineering attacks are a popular choice among threat actors. That’s because it’s often easier to trick people into providing them with access, information, or money than it is to exploit a software or network vulnerability. |

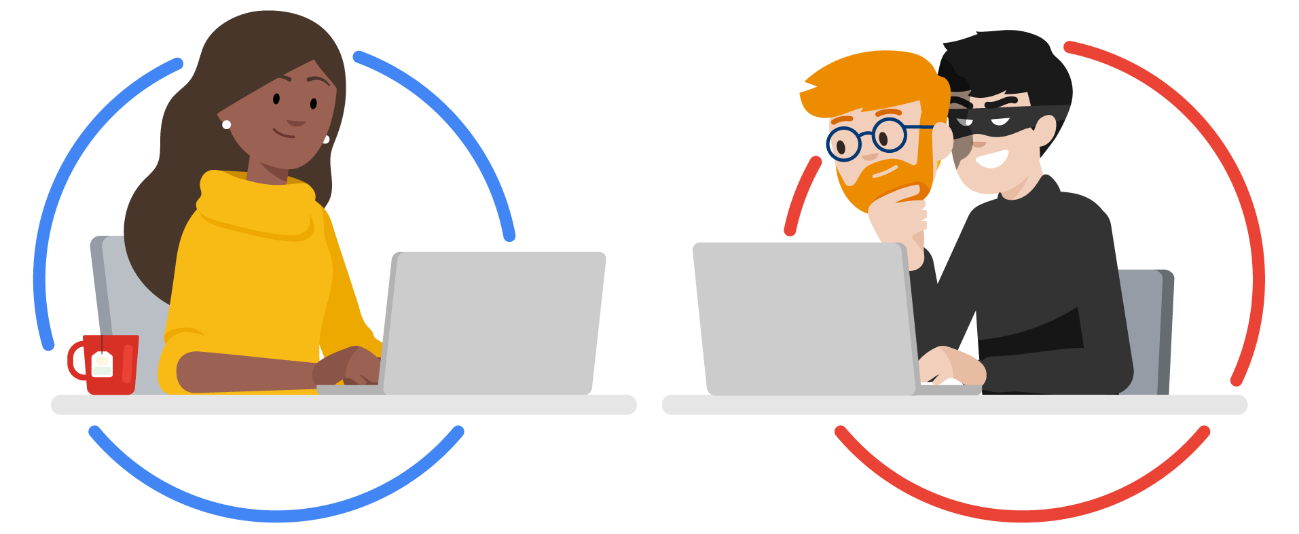
Tấn công kỹ thuật xã hội là lựa chọn phổ biến của những kẻ đe dọa. Đó là vì thường dễ lừa người khác cung cấp cho chúng quyền truy cập, thông tin hoặc tiền hơn là khai thác lỗ hổng phần mềm hoặc mạng.

|  |
| --- |
| As you might recall, **social engineering** is a manipulation technique that exploits human error to gain private information, access, or valuables. It's an umbrella term that can apply to a broad range of attacks. Each technique is designed to capitalize on the trusting nature of people and their willingness to help. In this reading, you will learn about specific social engineering tactics to watch out for. You’ll also learn ways that organizations counter these threats. |

Như bạn có thể nhớ lại, **kỹ thuật xã hội** là một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin riêng tư, quyền truy cập hoặc đồ vật có giá trị. Đây là một thuật ngữ chung có thể áp dụng cho nhiều loại tấn công. Mỗi kỹ thuật được thiết kế để tận dụng bản chất tin tưởng của mọi người và sự sẵn lòng giúp đỡ của họ. Trong bài đọc này, bạn sẽ tìm hiểu về các chiến thuật kỹ thuật xã hội cụ thể cần chú ý. Bạn cũng sẽ tìm hiểu cách các tổ chức chống lại các mối đe dọa này.

|  |
| --- |
| **Social engineering risks** |

**Rủi ro kỹ thuật xã hội**



|  |
| --- |
| Social engineering is a form of deception that takes advantage of the way people think. It preys on people’s natural feelings of curiosity, generosity, and excitement. Threat actors turn those feelings against their targets by affecting their better judgment. Social engineering attacks can be incredibly harmful because of how easy they can be to accomplish. |

Kỹ thuật xã hội là một hình thức lừa dối lợi dụng cách suy nghĩ của mọi người. Nó lợi dụng cảm giác tò mò, hào phóng và phấn khích tự nhiên của mọi người. Những kẻ đe dọa biến những cảm xúc đó thành hành động chống lại mục tiêu của chúng bằng cách tác động đến khả năng phán đoán tốt hơn của chúng. Các cuộc tấn công kỹ thuật xã hội có thể cực kỳ nguy hiểm vì chúng có thể dễ dàng thực hiện.

|  |
| --- |
| One of the highest-profile social engineering attacks that occurred in recent years was the [*Twitter Hack* *of 2020*](https://www.dfs.ny.gov/Twitter_Report). During that incident, a group of hackers made phone calls to Twitter employees pretending to be from the IT department. Using this basic scam, the group managed to gain access to the organization’s network and internal tools. This allowed them to take over the accounts of high-profile users, including politicians, celebrities, and entrepreneurs. |

Một trong những cuộc tấn công kỹ thuật xã hội có mức độ nghiêm trọng cao nhất xảy ra trong những năm gần đây là[*Tấn công Twitter* *của năm 2020*](https://www.dfs.ny.gov/Twitter_Report). Trong sự cố đó, một nhóm tin tặc đã gọi điện thoại đến các nhân viên Twitter giả vờ là nhân viên bộ phận CNTT. Sử dụng trò lừa đảo cơ bản này, nhóm đã truy cập được vào mạng lưới và các công cụ nội bộ của tổ chức. Điều này cho phép chúng chiếm đoạt tài khoản của những người dùng có địa vị cao, bao gồm các chính trị gia, người nổi tiếng và doanh nhân.

|  |
| --- |
| Attacks like this are just one example of the chaos threat actors can create using basic social engineering techniques. These attacks present serious risks because they don’t require sophisticated computer skills to perform. Defending against them requires a multi-layered approach that combines technological controls with user awareness. |

Các cuộc tấn công như thế này chỉ là một ví dụ về sự hỗn loạn mà các tác nhân đe dọa có thể tạo ra bằng cách sử dụng các kỹ thuật kỹ thuật xã hội cơ bản. Các cuộc tấn công này gây ra rủi ro nghiêm trọng vì chúng không yêu cầu các kỹ năng máy tính phức tạp để thực hiện. Việc phòng thủ chống lại chúng đòi hỏi một phương pháp tiếp cận nhiều lớp kết hợp các biện pháp kiểm soát công nghệ với nhận thức của người dùng.

|  |
| --- |
| **Signs of an attack** |

**Dấu hiệu của một cuộc tấn công**

|  |
| --- |
| Oftentimes, people are unable to tell that an attack is happening until it's too late. Social engineering is such a dangerous threat because it typically allows attackers to bypass technological defenses that are in their way. Although these threats are difficult to prevent, recognizing the signs of social engineering is a key to reducing the likelihood of a successful attack. |

Thông thường, mọi người không thể biết rằng một cuộc tấn công đang diễn ra cho đến khi quá muộn. Kỹ thuật xã hội là một mối đe dọa nguy hiểm vì nó thường cho phép kẻ tấn công vượt qua các biện pháp phòng thủ công nghệ cản đường chúng. Mặc dù những mối đe dọa này khó ngăn chặn, nhưng việc nhận ra các dấu hiệu của kỹ thuật xã hội là chìa khóa để giảm khả năng xảy ra một cuộc tấn công thành công.

|  |
| --- |
| These are common types of social engineering to watch out for:   * **Baiting** is a social engineering tactic that tempts people into compromising their security. A common example is USB baiting that relies on someone finding an infected USB drive and plugging it into their device. * **Phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. It is one of the most common forms of social engineering, typically performed via email. * **Quid pro quo** is a type of baiting used to trick someone into believing that they’ll be rewarded in return for sharing access, information, or money. For example, an attacker might impersonate a loan officer at a bank and call customers offering them a lower interest rate on their credit card. They'll tell the customers that they simply need to provide their account details to claim the deal. * **Tailgating** is a social engineering tactic in which unauthorized people follow an authorized person into a restricted area. This technique is also sometimes referred to as piggybacking. * **Watering hole** is a type of attack when a threat actor compromises a website frequently visited by a specific group of users. Oftentimes, these watering hole sites are infected with malicious software. An example is the *Holy Water attack of 2020* that infected various religious, charity, and volunteer websites. |

Sau đây là những loại kỹ thuật xã hội phổ biến mà bạn cần cảnh giác:

* **Baiting** là một chiến thuật kỹ thuật xã hội dụ dỗ mọi người xâm phạm bảo mật của họ. Một ví dụ phổ biến là USB baiting dựa trên việc ai đó tìm thấy ổ USB bị nhiễm và cắm vào thiết bị của họ.
* **Lừa đảo** là việc sử dụng các phương tiện truyền thông kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại. Đây là một trong những hình thức kỹ thuật xã hội phổ biến nhất, thường được thực hiện qua email.
* **Quid pro quo** là một loại mồi nhử được sử dụng để lừa ai đó tin rằng họ sẽ được thưởng khi chia sẻ quyền truy cập, thông tin hoặc tiền. Ví dụ, kẻ tấn công có thể mạo danh nhân viên tín dụng tại một ngân hàng và gọi điện cho khách hàng để cung cấp cho họ mức lãi suất thấp hơn trên thẻ tín dụng của họ. Chúng sẽ nói với khách hàng rằng họ chỉ cần cung cấp thông tin chi tiết về tài khoản của mình để yêu cầu giao dịch.
* **Tailgating** là một chiến thuật kỹ thuật xã hội trong đó những người không được phép đi theo một người được phép vào một khu vực hạn chế. Kỹ thuật này đôi khi cũng được gọi là piggybacking.
* **Watering hole** là một loại tấn công khi tác nhân đe dọa xâm nhập vào một trang web thường xuyên được một nhóm người dùng cụ thể truy cập. Thông thường, các trang web watering hole này bị nhiễm phần mềm độc hại. Một ví dụ là cuộc *tấn công Holy Water năm 2020* đã lây nhiễm nhiều trang web tôn giáo, từ thiện và tình nguyện.

|  |
| --- |
| Attackers might use any of these techniques to gain unauthorized access to an organization. Everyone is vulnerable to them, from entry-level employees to senior executives. However, you can reduce the risks of social engineering attacks at any business by teaching others what to expect. |

Kẻ tấn công có thể sử dụng bất kỳ kỹ thuật nào trong số này để truy cập trái phép vào một tổ chức. Mọi người đều có thể bị tấn công, từ nhân viên mới vào nghề đến giám đốc điều hành cấp cao. Tuy nhiên, bạn có thể giảm thiểu rủi ro của các cuộc tấn công kỹ thuật xã hội tại bất kỳ doanh nghiệp nào bằng cách hướng dẫn người khác những gì cần chuẩn bị.

|  |
| --- |
| **Encouraging caution** |

**Khuyến khích thận trọng**

|  |
| --- |
| Spreading awareness usually starts with comprehensive security training. When it comes to social engineering, there are three main areas to focus on when teaching others:   * **Stay alert** of suspicious communications and unknown people, especially when it comes to email. For example, look out for spelling errors and double-check the sender's name and email address. * **Be cautious** about sharing information, especially over social media. Threat actors often search these platforms for any information they can use to their advantage. * **Control curiosity** when something seems too good to be true. This can include wanting to click on attachments or links in emails and advertisements. |

Việc truyền bá nhận thức thường bắt đầu bằng đào tạo an ninh toàn diện. Khi nói đến kỹ thuật xã hội, có ba lĩnh vực chính cần tập trung vào khi dạy người khác:

* **Hãy cảnh giác** với các thông tin liên lạc đáng ngờ và những người lạ, đặc biệt là khi nói đến email. Ví dụ, hãy chú ý đến lỗi chính tả và kiểm tra lại tên và địa chỉ email của người gửi.
* **Hãy thận trọng** khi chia sẻ thông tin, đặc biệt là trên mạng xã hội. Những kẻ đe dọa thường tìm kiếm thông tin trên các nền tảng này để có thể sử dụng cho mục đích có lợi cho chúng.
* **Kiểm soát sự tò mò** khi có điều gì đó có vẻ quá tốt để trở thành sự thật. Điều này có thể bao gồm việc muốn nhấp vào tệp đính kèm hoặc liên kết trong email và quảng cáo.

|  |
| --- |
| **Pro tip:** Implementing technologies like firewalls, multi-factor authentication (MFA), block lists, email filtering, and others helps layers the defenses should someone make a mistake. |

**Mẹo chuyên nghiệp:** Việc triển khai các công nghệ như tường lửa, xác thực đa yếu tố (MFA), danh sách chặn, lọc email và các công nghệ khác giúp tăng cường khả năng phòng thủ trong trường hợp có người mắc lỗi.

|  |
| --- |
| Ideally, security training extends beyond employees. Educating customers about social engineering threats is also a key to mitigating these threats. And security analysts play an important part in promoting safe practices. For example, a big part of an analyst's job is testing systems and documenting best practices for others at an organization to follow. |

Về mặt lý tưởng, đào tạo bảo mật mở rộng ra ngoài phạm vi nhân viên. Giáo dục khách hàng về các mối đe dọa kỹ thuật xã hội cũng là chìa khóa để giảm thiểu các mối đe dọa này. Và các nhà phân tích bảo mật đóng vai trò quan trọng trong việc thúc đẩy các hoạt động an toàn. Ví dụ, một phần lớn công việc của nhà phân tích là kiểm tra hệ thống và ghi lại các hoạt động thực hành tốt nhất để những người khác trong tổ chức làm theo.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| People’s willingness to help one another and their trusting nature is what makes social engineering such an appealing tactic for criminals. It just takes one act of kindness or a momentary lapse in judgment for an attack to work. Criminals go to great lengths to make their attacks difficult to detect. They rely on a variety of manipulation techniques to trick their targets into granting them access. For that reason, implementing effective controls and recognizing the signs of an attack go a long way towards preventing threats. |

Sự sẵn lòng giúp đỡ lẫn nhau và bản chất tin tưởng của mọi người là những gì khiến cho kỹ thuật xã hội trở thành một chiến thuật hấp dẫn đối với tội phạm. Chỉ cần một hành động tử tế hoặc một khoảnh khắc mất bình tĩnh trong phán đoán là có thể thực hiện được một cuộc tấn công. Tội phạm sẽ làm mọi cách để khiến các cuộc tấn công của họ khó bị phát hiện. Họ dựa vào nhiều kỹ thuật thao túng khác nhau để lừa mục tiêu cấp cho họ quyền truy cập. Vì lý do đó, việc thực hiện các biện pháp kiểm soát hiệu quả và nhận ra các dấu hiệu của một cuộc tấn công sẽ giúp ngăn chặn các mối đe dọa.

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| Here are two additional resources to review that will help you continue developing your understanding of social engineering trends and security practices:   * [OUCH!](https://www.sans.org/newsletters/ouch/) is a free monthly newsletter from the SANS Institute that reports on social engineering trends and other security topics. * [Scamwatch](https://www.scamwatch.gov.au/) is a resource for news and tools for recognizing, avoiding, and reporting social engineering scams. |

Sau đây là hai nguồn tài nguyên bổ sung để bạn tham khảo nhằm giúp bạn tiếp tục phát triển hiểu biết của mình về các xu hướng kỹ thuật xã hội và các hoạt động bảo mật:

* [ÁI ỐI!](https://www.sans.org/newsletters/ouch/)là bản tin hàng tháng miễn phí từ Viện SANS, báo cáo về các xu hướng kỹ thuật xã hội và các chủ đề bảo mật khác.
* [Đồng hồ lừa đảo](https://www.scamwatch.gov.au/)là nguồn tin tức và công cụ giúp nhận biết, tránh xa và báo cáo các vụ lừa đảo kỹ thuật xã hội.

***1.4. Phishing for information - Lừa đảo để lấy thông tin***

|  |
| --- |
| Cybercriminals prefer attacks that do the most amount of damage with the least amount of effort. One of the most popular forms of social engineering that meets this description is phishing. |

Tội phạm mạng thích các cuộc tấn công gây ra nhiều thiệt hại nhất với ít nhấtlượng nỗ lực.Một trong những hình thức tấn công xã hội phổ biến nhất đáp ứng được mô tả này là lừa đảo qua mạng.

|  |
| --- |
| Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. Phishing leverages many communication technologies, but the term is mainly used to describe attacks that arrive by email. |

Lừa đảo là việc sử dụng các phương tiện truyền thông kỹ thuật số để lừa mọi ngườitiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.Lừa đảo tận dụng nhiều công nghệ truyền thông, nhưngThuật ngữ này chủ yếu được dùng để mô tả các cuộc tấn công đến qua email.

|  |
| --- |
| Phishing attacks don't just affect individuals. They are also harmful to organizations. A single employee that falls for one of these tricks can give malicious attackers access to systems. Once inside, attackers can exploit sensitive data like customer names and product secrets. |

Các cuộc tấn công lừa đảo không chỉ ảnh hưởng đến cá nhân.Chúng cũng có hại cho các tổ chức.Một nhân viên duy nhất mắc phải một trong những mánh khóe này có thể gây ra hậu quả xấukẻ tấn công truy cập vào hệ thống.Một khi đã vào bên trong, kẻ tấn công có thể khai thác dữ liệu nhạy cảm như tên khách hàng vàbí mật sản phẩm.

|  |
| --- |
| Attackers who carry out these attacks commonly use phishing kits. A phishing kit is a collection of software tools needed to launch a phishing campaign. People with little technical background can use one of these kits. |

Những kẻ tấn công thực hiện các cuộc tấn công này thường sử dụng bộ công cụ lừa đảo.Bộ công cụ lừa đảo là tập hợp các công cụ phần mềm cần thiết để khởi chạymột chiến dịch lừa đảo.Những người có ít kiến ​​thức chuyên môn cũng có thể sử dụng một trong những bộ dụng cụ này.

|  |
| --- |
| Each of the tools inside are designed to avoid detection. As a security professional, you should be aware of the three main tools inside a phishing kit, so that you can quickly identify when they're being used and put a stop to it. |

Mỗi dụng cụ bên trong đều được thiết kế để tránh bị phát hiện.Là một chuyên gia an ninh,bạn nên biết ba công cụ chính bên trong một bộ công cụ lừa đảo, vì vậyđể bạn có thể nhanh chóng xác định khi nào chúng đang được sử dụng và ngăn chặn nó.

|  |
| --- |
| The first is malicious attachments. These are files that are infected and can cause harm to the organization's systems. |

Đầu tiên là các tệp đính kèm độc hại.Đây là những tệp bị nhiễm và có thể gây hại cho hệ thống của tổ chức.

|  |
| --- |
| Phishing kits also include fake-data collection forms. These forms look like legitimate forms, like a survey. Unlike a real survey, they ask for sensitive information that isn't normally asked for in an email. |

Bộ công cụ lừa đảo cũng bao gồm các biểu mẫu thu thập dữ liệu giả.Những mẫu đơn này trông giống như những mẫu đơn hợp pháp, như một cuộc khảo sát.Không giống như một cuộc khảo sát thực tế,chúng yêu cầu những thông tin nhạy cảm mà thông thường không được yêu cầu trong email.

|  |
| --- |
| The third resource they include are fraudulent web links. These open to malicious web pages that are designed to look like trusted brands. Unlike actual websites, these fraudulent sites are built to steal information, like login credentials. |

Nguồn thứ ba họ đưa vào là các liên kết web lừa đảo.Những trang web này sẽ dẫn đến các trang web độc hại được thiết kế trông giống như các thương hiệu đáng tin cậy.Không giống như các trang web thực tế,các trang web lừa đảo này được xây dựng để đánh cắp thông tin, như thông tin đăng nhập.

|  |
| --- |
| Cybercriminals can use these tools to launch a phishing attack in many forms. The most common is through malicious emails. However, they can use them in other forms of communication too. Most recently, cybercriminals are using smishing and vishing to trick people into revealing private information. |

Tội phạm mạng có thể sử dụng những công cụ này để thực hiện tấn công lừa đảo dưới nhiều hình thức.Phổ biến nhất là thông qua email độc hại.Tuy nhiên, họ cũng có thể sử dụng chúng trong các hình thức giao tiếp khác.Gần đây nhất, tội phạm mạng đang sử dụng smishing vàlừa đảo để lừa mọi người tiết lộ thông tin riêng tư.

|  |
| --- |
| Smishing is the use of text messages to obtain sensitive information or to impersonate a known source. You've probably received these types of messages before. Not only are smishing messages annoying to receive, they're also difficult to prevent. That's why some attackers send them. Some smishing messages are easy to detect. They might show signs of being malicious like promising a cash reward for clicking an attached link that shouldn't be clicked. Other times, smishing is hard to spot. Attackers sometimes use local area codes to appear legitimate. Some hackers can even send messages disguised as friends and families of their target to fool them into disclosing sensitive information. |

Smishing là việc sử dụng tin nhắn văn bản để lấy thông tin nhạy cảm hoặcđể mạo danh một nguồn tin đã biết.Có lẽ bạn đã từng nhận được những tin nhắn kiểu này trước đây.Không chỉ tin nhắn smishing gây khó chịu khi nhận,chúng cũng khó ngăn chặn. Đó là lý do tại sao một số kẻ tấn công gửi chúng.Một số tin nhắn smishing rất dễ bị phát hiện.Họ có thể biểu hiện dấu hiệu độc hại như hứa thưởng tiền mặt chonhấp vào liên kết đính kèm không nên nhấp vào.Những lần khác, việc đập vỡ rất khó phát hiện.Kẻ tấn công đôi khi sử dụng mã vùng địa phương để tỏ ra hợp pháp.Một số tin tặc thậm chí có thể gửi tin nhắn được ngụy trang thành bạn bè vàgia đình mục tiêu để lừa họ tiết lộ thông tin nhạy cảm.

|  |
| --- |
| Vishing is the exploitation of electronic voice communication to obtain sensitive information or impersonate a known source. During vishing attacks, criminals pretend to be someone they're not. For example, attackers might call pretending to be a company representative. They might claim that there's a problem with your account. And they can offer to fix it if you provide them with sensitive information. |

Vishing là việc khai thác thông tin liên lạc bằng giọng nói điện tử để có đượcthông tin nhạy cảm hoặc mạo danh một nguồn tin đã biết.Trong các cuộc tấn công vishing, tội phạm sẽ giả vờ là một người nào đó mà chúng không phải.Ví dụ, kẻ tấn công có thể gọi điện giả vờ là đại diện của công ty.Họ có thể khẳng định rằng tài khoản của bạn có vấn đề.Và họ có thể đề nghị sửa lỗi nếu bạn cung cấp cho họ thông tin nhạy cảm.

|  |
| --- |
| Most organizations use a few basic security measures to prevent these and any other types of phishing attacks from becoming a problem. For example, anti-phishing policies spread awareness and encourage users to follow data security procedures correctly. Employee training resources also help inform employees about things to look for when an email looks suspicious. |

Hầu hết các tổ chức sử dụng một số biện pháp bảo mật cơ bản để ngăn chặn những điều này vàbất kỳ loại tấn công lừa đảo nào khác trở thành vấn đề.Ví dụ, các chính sách chống lừa đảo nâng cao nhận thức vàkhuyến khích người dùng thực hiện đúng các quy trình bảo mật dữ liệu.Các nguồn đào tạo nhân viên cũng giúp thông báo cho nhân viên về những điều cần tìm kiếmkhi một email có vẻ đáng ngờ.

|  |
| --- |
| Another line of defense against phishing is securing email inboxes. Email filters are commonly used to keep harmful messages from reaching users. For example, specific email addresses can be blocked using a blocklist. Organizations often use other filters, like allowlists, to specify IP addresses that are approved to send mail within the company. |

Một biện pháp phòng thủ khác chống lại lừa đảo là bảo mật hộp thư đến email.Bộ lọc email thường được sử dụng để ngăn những tin nhắn có hại đến được người dùng.Ví dụ, các địa chỉ email cụ thể có thể bị chặn bằng danh sách chặn.Các tổ chức thường sử dụng các bộ lọc khác, như danh sách cho phép, để chỉ định địa chỉ IPđược chấp thuận gửi thư trong công ty.

|  |
| --- |
| Organizations also use intrusion prevention systems to look for unusual patterns in email traffic. Security analysts use monitoring tools like this to spot suspicious emails, quarantine them, and produce a log of events. |

Các tổ chức cũng sử dụng hệ thống phòng chống xâm nhập để tìm kiếmcác mô hình bất thường trong lưu lượng email.Các nhà phân tích bảo mật sử dụng các công cụ giám sát như thế này để phát hiện các email đáng ngờ,cách ly họ và lập nhật ký các sự kiện.

|  |
| --- |
| Phishing campaigns are popular and dangerous forms of social engineering that organizations of all sizes need to deal with. Just a single compromised password that an attacker can get their hands on can lead to a costly data breach. Now that you're familiar with the tools these attackers use, you're better equipped to spot phishing and prevent it. |

Các chiến dịch lừa đảo là những hình thức kỹ thuật xã hội phổ biến và nguy hiểmcác tổ chức ở mọi quy mô đều cần phải giải quyết.Chỉ cần một mật khẩu bị xâm phạm mà kẻ tấn công có thể lấy được có thể dẫn đếnđến một vụ vi phạm dữ liệu tốn kém.Bây giờ bạn đã quen thuộc với các công cụ mà những kẻ tấn công này sử dụng,bạn sẽ được trang bị tốt hơn để phát hiện lừa đảo và ngăn chặn nó.

***1.5. Types of phishing - Lừa đảo để lấy thông tin***

|  |
| --- |
| **Types of phishing** |

**Các loại lừa đảo**

|  |
| --- |
| Phishing is one of the most common types of **social engineering**, which are manipulation techniques that exploit human error to gain private information, access, or valuables. Previously, you learned how **phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. |

Lừa đảo qua mạng là một trong những loại **kỹ thuật xã hội** phổ biến nhất , là các kỹ thuật thao túng lợi dụng lỗi của con người để lấy thông tin riêng tư, quyền truy cập hoặc đồ vật có giá trị. Trước đây, bạn đã học cách **lừa đảo qua mạng** là sử dụng phương tiện truyền thông kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.

|  |
| --- |
| Sometimes, phishing attacks appear to come from a trusted person or business. This can lead unsuspecting recipients into acting against their better judgment, causing them to break security procedures. In this reading, you’ll learn about common phishing tactics used by attackers today. |

Đôi khi, các cuộc tấn công lừa đảo có vẻ như đến từ một người hoặc doanh nghiệp đáng tin cậy. Điều này có thể khiến những người nhận không nghi ngờ hành động trái với phán đoán của họ, khiến họ vi phạm các quy trình bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu về các chiến thuật lừa đảo phổ biến mà những kẻ tấn công sử dụng hiện nay.

|  |
| --- |
| **The origins of phishing** |

**Nguồn gốc của lừa đảo**

|  |
| --- |
| Phishing has been around since the early days of the internet. It can be traced back to the 1990s. At the time, people across the world were coming online for the first time. As the internet became more accessible it began to attract the attention of malicious actors. These malicious actors realized that the internet gave them a level of anonymity to commit their crimes. |

Lừa đảo trực tuyến đã xuất hiện từ những ngày đầu của Internet. Nó có thể bắt nguồn từ những năm 1990. Vào thời điểm đó, mọi người trên khắp thế giới lần đầu tiên trực tuyến. Khi Internet trở nên dễ tiếp cận hơn, nó bắt đầu thu hút sự chú ý của những kẻ xấu. Những kẻ xấu này nhận ra rằng Internet mang lại cho chúng một mức độ ẩn danh để thực hiện tội ác của mình.

|  |
| --- |
| **Early persuasion tactics** |

**Chiến thuật thuyết phục sớm**

|  |
| --- |
| One of the earliest instances of phishing was aimed at a popular chat service called AOL Instant Messenger (AIM). Users of the service began receiving emails asking them to verify their accounts or provide personal billing information. The users were unaware that these messages were sent by malicious actors pretending to be service providers. |

Một trong những trường hợp lừa đảo sớm nhất nhắm vào một dịch vụ trò chuyện phổ biến có tên là AOL Instant Messenger (AIM). Người dùng dịch vụ bắt đầu nhận được email yêu cầu họ xác minh tài khoản hoặc cung cấp thông tin thanh toán cá nhân. Người dùng không biết rằng những tin nhắn này được gửi bởi những kẻ xấu giả danh là nhà cung cấp dịch vụ.

|  |
| --- |
| This was one of the first examples of mass phishing, which describesattacks that send malicious emails out to a large number of people, increasing the likelihood of baiting someone into the trap. |

Đây là một trong những ví dụ đầu tiên về lừa đảo hàng loạt, mô tả các cuộc tấn công gửi email độc hại đến nhiều người, làm tăng khả năng dụ ai đó vào bẫy.

|  |
| --- |
| During the AIM attacks, malicious actors carefully crafted emails that appeared to come directly from AOL. The messages used official logos, colors, and fonts to trick unsuspecting users into sharing their information and account details. |

Trong các cuộc tấn công AIM, những kẻ xấu đã cẩn thận tạo ra các email có vẻ như đến trực tiếp từ AOL. Các tin nhắn sử dụng logo, màu sắc và phông chữ chính thức để lừa người dùng không nghi ngờ chia sẻ thông tin và chi tiết tài khoản của họ.

|  |
| --- |
| Attackers used the stolen information to create fraudulent AOL accounts they could use to carry out other crimes anonymously. AOL was forced to adapt their security policies to address these threats. The chat service began including messages on their platforms to warn users about phishing attacks. |

Những kẻ tấn công đã sử dụng thông tin bị đánh cắp để tạo ra các tài khoản AOL gian lận mà chúng có thể sử dụng để thực hiện các tội phạm khác một cách ẩn danh. AOL đã buộc phải điều chỉnh chính sách bảo mật của mình để giải quyết các mối đe dọa này. Dịch vụ trò chuyện bắt đầu bao gồm các tin nhắn trên nền tảng của họ để cảnh báo người dùng về các cuộc tấn công lừa đảo.

|  |
| --- |
| **How phishing has evolved** |

**Lừa đảo trực tuyến đã phát triển như thế nào**

|  |
| --- |
| Phishing continued evolving at the turn of the century as businesses and newer technologies began entering the digital landscape. In the early 2000s, e-commerce and online payment systems started to become popular alternatives to traditional marketplaces. The introduction of online transactions presented new opportunities for attackers to commit crimes. |

Lừa đảo trực tuyến tiếp tục phát triển vào đầu thế kỷ khi các doanh nghiệp và công nghệ mới hơn bắt đầu thâm nhập vào bối cảnh kỹ thuật số. Vào đầu những năm 2000, thương mại điện tử và hệ thống thanh toán trực tuyến bắt đầu trở thành những lựa chọn thay thế phổ biến cho các thị trường truyền thống. Sự ra đời của các giao dịch trực tuyến đã tạo ra những cơ hội mới cho những kẻ tấn công thực hiện tội phạm.

|  |
| --- |
| A number of techniques began to appear around this time period, many of which are still used today. There are five common types of phishing that every security analyst should know:   * **Email phishing** is a type of attack sent via email in which threat actors send messages pretending to be a trusted person or entity. * **Smishing** is a type of phishing that uses Short Message Service (SMS), a technology that powers text messaging. Smishing covers all forms of text messaging services, including Apple’s iMessages, WhatsApp, and other chat mediums on phones. * **Vishing** refers to the use of voice calls or voice messages to trick targets into providing personal information over the phone. * **Spear phishing** is a subset of email phishing in which specific people are purposefully targeted, such as the accountants of a small business. * **Whaling** refers to a category of spear phishing attempts that are aimed at high-ranking executives in an organization. |

Một số kỹ thuật bắt đầu xuất hiện vào khoảng thời gian này, nhiều trong số đó vẫn được sử dụng cho đến ngày nay. Có năm loại lừa đảo phổ biến mà mọi nhà phân tích bảo mật nên biết:

* **Lừa đảo qua email** là một loại tấn công được gửi qua email trong đó kẻ tấn công gửi tin nhắn giả mạo là người hoặc tổ chức đáng tin cậy.
* **Smishing** là một loại lừa đảo sử dụng Dịch vụ tin nhắn ngắn (SMS), một công nghệ hỗ trợ nhắn tin văn bản. Smishing bao gồm tất cả các hình thức dịch vụ nhắn tin văn bản, bao gồm iMessages của Apple, WhatsApp và các phương tiện trò chuyện khác trên điện thoại.
* **Vishing** là việc sử dụng các cuộc gọi thoại hoặc tin nhắn thoại để lừa mục tiêu cung cấp thông tin cá nhân qua điện thoại.
* **Lừa đảo qua email** là một dạng lừa đảo qua email trong đó mục tiêu cụ thể là những người cụ thể, chẳng hạn như kế toán của một doanh nghiệp nhỏ.
* **Whaling** là một loại hình lừa đảo trực tuyến nhắm vào các giám đốc điều hành cấp cao trong một tổ chức.

|  |
| --- |
| Since the early days of phishing, email attacks remain the most common types that are used. While they were originally used to trick people into sharing access credentials and credit card information, email phishing became a popular method to infect computer systems and networks with malicious software. |

Kể từ những ngày đầu của lừa đảo trực tuyến, các cuộc tấn công qua email vẫn là loại phổ biến nhất được sử dụng. Mặc dù ban đầu chúng được sử dụng để lừa mọi người chia sẻ thông tin đăng nhập và thông tin thẻ tín dụng, lừa đảo qua email đã trở thành phương pháp phổ biến để lây nhiễm phần mềm độc hại vào hệ thống máy tính và mạng.

|  |
| --- |
| In late 2003, attackers around the world created fraudulent websites that resembled businesses like eBay and PayPal™. Mass phishing campaigns to distribute malicious programs were also launched against e-commerce and banking sites. |

Vào cuối năm 2003, những kẻ tấn công trên khắp thế giới đã tạo ra các trang web gian lận giống với các doanh nghiệp như eBay và PayPal™. Các chiến dịch lừa đảo hàng loạt để phân phối các chương trình độc hại cũng được phát động nhằm vào các trang web thương mại điện tử và ngân hàng.

|  |
| --- |
| **Recent trends** |

**Xu hướng gần đây**

|  |
| --- |
| Starting in the 2010s, attackers began to shift away from mass phishing attempts that relied on baiting unsuspecting people into a trap. Leveraging new technologies, criminals began carrying out what’s known astargeted phishing attempts. Targeted phishing describes attacks that are sent to specific targets using highly customized methods to create a strong sense of familiarity. |

Bắt đầu từ những năm 2010, những kẻ tấn công bắt đầu chuyển hướng khỏi các nỗ lực lừa đảo hàng loạt dựa trên việc dụ những người không nghi ngờ vào bẫy. Tận dụng các công nghệ mới, tội phạm bắt đầu thực hiện những gì được gọi là các nỗ lực lừa đảo có mục tiêu. Lừa đảo có mục tiêu mô tả các cuộc tấn công được gửi đến các mục tiêu cụ thể bằng các phương pháp được tùy chỉnh cao để tạo ra cảm giác quen thuộc mạnh mẽ.

|  |
| --- |
| A type of targeted phishing that evolved in the 2010s is angler phishing. **Angler phishing** is a technique where attackers impersonate customer service representatives on social media. This tactic evolved from people’s tendency to complain about businesses online. Threat actors intercept complaints from places like message boards or comment sections and contact the angry customer via social media. Like the AIM attacks of the 1990s, they use fraudulent accounts that appear similar to those of actual businesses. They then trick the angry customers into sharing sensitive information with the promise of fixing their problem. |

Một loại lừa đảo có mục tiêu phát triển vào những năm 2010 là lừa đảo câu cá. **Lừa đảo câu cá** là một kỹ thuật mà kẻ tấn công mạo danh đại diện dịch vụ khách hàng trên phương tiện truyền thông xã hội. Chiến thuật này phát triển từ xu hướng phàn nàn về các doanh nghiệp trực tuyến của mọi người. Các tác nhân đe dọa chặn các khiếu nại từ những nơi như bảng tin hoặc phần bình luận và liên hệ với khách hàng tức giận qua phương tiện truyền thông xã hội. Giống như các cuộc tấn công AIM của những năm 1990, chúng sử dụng các tài khoản gian lận trông giống với tài khoản của các doanh nghiệp thực tế. Sau đó, chúng lừa những khách hàng tức giận chia sẻ thông tin nhạy cảm với lời hứa sẽ khắc phục sự cố của họ.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Phishing tactics have become very sophisticated over the years. Unfortunately, there isn't a perfect solution that prevents these attacks from happening. Tactics, like email phishing that started in the last century, remain an effective and profitable method of attack for criminals online today. |

Các chiến thuật lừa đảo qua email đã trở nên rất tinh vi trong những năm qua. Thật không may, không có giải pháp hoàn hảo nào có thể ngăn chặn các cuộc tấn công này xảy ra. Các chiến thuật như lừa đảo qua email bắt đầu từ thế kỷ trước vẫn là phương pháp tấn công hiệu quả và có lợi nhuận đối với tội phạm trực tuyến hiện nay.

|  |
| --- |
| There isn’t a technological solution to prevent phishing entirely. However, there are many ways to reduce the damage from these attacks when they happen. One way is to spread awareness and inform others. As a security professional, you may be responsible for helping others identify forms of social engineering, like phishing. For example, you might create training programs that educate employees about topics like phishing. Sharing your knowledge with others is an important responsibility that helps build a culture of security. |

Không có giải pháp công nghệ nào có thể ngăn chặn hoàn toàn việc lừa đảo qua mạng. Tuy nhiên, có nhiều cách để giảm thiểu thiệt hại do các cuộc tấn công này gây ra khi chúng xảy ra. Một cách là nâng cao nhận thức và thông báo cho người khác. Là một chuyên gia bảo mật, bạn có thể chịu trách nhiệm giúp người khác xác định các hình thức kỹ thuật xã hội, như lừa đảo qua mạng. Ví dụ, bạn có thể tạo các chương trình đào tạo để giáo dục nhân viên về các chủ đề như lừa đảo qua mạng. Chia sẻ kiến ​​thức của bạn với người khác là một trách nhiệm quan trọng giúp xây dựng văn hóa bảo mật.

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| Staying up-to-date on phishing threats is one of the best things you can do to educate yourself and help your organization make smarter security decisions.   * [Google’s phishing quiz](https://phishingquiz.withgoogle.com/) is a tool that you can use or share that illustrates just how difficult it can be to identify these attacks. * [Phishing.org](https://www.phishing.org/) reports on the latest phishing trends and shares free resources that can help reduce phishing attacks. * The [Anti-Phishing Working Group (APWG)](https://apwg.org/) is a non-profit group of multidisciplinary security experts that publishes a quarterly report on phishing trends. |

Luôn cập nhật thông tin về các mối đe dọa lừa đảo là một trong những điều tốt nhất bạn có thể làm để nâng cao kiến ​​thức và giúp tổ chức của bạn đưa ra các quyết định bảo mật thông minh hơn.

* [Bài kiểm tra lừa đảo của Google](https://phishingquiz.withgoogle.com/)là một công cụ mà bạn có thể sử dụng hoặc chia sẻ để minh họa mức độ khó khăn khi xác định các cuộc tấn công này.
* [Phishing.org](https://www.phishing.org/)báo cáo về các xu hướng lừa đảo mới nhất và chia sẻ các tài nguyên miễn phí có thể giúp giảm các cuộc tấn công lừa đảo.
* Các[Nhóm công tác chống lừa đảo (APWG)](https://apwg.org/)là một nhóm phi lợi nhuận gồm các chuyên gia bảo mật đa ngành, chuyên xuất bản báo cáo hàng quý về xu hướng lừa đảo qua mạng.

***1.6. Test your knowledge: Social engineering - Kiểm tra kiến thức của bạn: Kỹ thuật xã hội***

***1.7. Activity: Filter malicious emails - Hoạt động: Lọc email độc hại***

|  |
| --- |
| **Activity Overview**  In this activity, you will analyze a suspicious email and identify signs of a phishing attack. Then, you will determine whether the email should be allowed or quarantined.  Phishing is one of the most common and dangerous forms of social engineering that you’ll encounter in the field. Identifying phishing attempts will help you prevent threats and find ways to improve security procedures. |

**Tổng quan hoạt động**

Trong hoạt động này, bạn sẽ phân tích một email đáng ngờ và xác định các dấu hiệu của một cuộc tấn công lừa đảo. Sau đó, bạn sẽ xác định xem email đó có nên được phép hay bị cách ly.

Lừa đảo là một trong những hình thức kỹ thuật xã hội phổ biến và nguy hiểm nhất mà bạn sẽ gặp phải trong lĩnh vực này. Việc xác định các nỗ lực lừa đảo sẽ giúp bạn ngăn chặn các mối đe dọa và tìm cách cải thiện các quy trình bảo mật.

|  |
| --- |
| **Scenario**  Review the scenario below. Then complete the step-by-step instructions.  You’re a security analyst at an investment firm called Imaginary Bank. An executive at the firm recently received a spear phishing email that appears to come from the board of Imaginary Bank. **Spear phishing** is a malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source. In this case, the executive is being asked to install new collaboration software, ExecuTalk.  The executive suspects this email might be a phishing attempt because ExecuTalk was never mentioned during the last board meeting. They've forwarded the message to your team to verify if it’s legitimate. Your supervisor has tasked you with investigating the message and determining whether it should be quarantined. |

**Kịch bản**

Xem lại tình huống bên dưới. Sau đó hoàn thành hướng dẫn từng bước.

Bạn là một nhà phân tích bảo mật tại một công ty đầu tư có tên là Imaginary Bank. Một giám đốc điều hành tại công ty này gần đây đã nhận được một email lừa đảo có vẻ như đến từ hội đồng quản trị của Imaginary Bank. **Lừa đảo có chủ đích** là một cuộc tấn công email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể, có vẻ như bắt nguồn từ một nguồn đáng tin cậy. Trong trường hợp này, giám đốc điều hành được yêu cầu cài đặt phần mềm cộng tác mới, ExecuTalk.

Giám đốc điều hành nghi ngờ email này có thể là một nỗ lực lừa đảo vì ExecuTalk chưa bao giờ được nhắc đến trong cuộc họp hội đồng quản trị gần đây nhất. Họ đã chuyển tiếp tin nhắn cho nhóm của bạn để xác minh xem nó có hợp lệ không. Giám sát viên của bạn đã giao cho bạn nhiệm vụ điều tra tin nhắn và xác định xem nó có nên bị cách ly hay không.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions and answer the questions below to complete the activity. |

**Hướng dẫn từng bước**

Làm theo hướng dẫn và trả lời các câu hỏi bên dưới để hoàn thành hoạt động.

Bước 1: Phân tích email đáng ngờ

|  |
| --- |
| **Step 1: Analyze the suspicious email**  Previously, you learned that phishing is a type of social engineering. Threat actors who send malicious emails rely on deception and manipulation techniques to trick their targets. When investigating suspicious emails like this, it's a good idea to note the threat actor's tactics. You can use that information to alert others at your organization about similar messages they might receive and what to watch out for. |

Trước đây, bạn đã biết rằng lừa đảo là một loại kỹ thuật xã hội. Những kẻ đe dọa gửi email độc hại dựa vào các kỹ thuật lừa dối và thao túng để đánh lừa mục tiêu của chúng. Khi điều tra các email đáng ngờ như thế này, bạn nên lưu ý các chiến thuật của kẻ đe dọa. Bạn có thể sử dụng thông tin đó để cảnh báo những người khác trong tổ chức của mình về các tin nhắn tương tự mà họ có thể nhận được và những điều cần chú ý.

|  |
| --- |
| Start your investigation by analyzing the suspicious message. Try to identify clues that this is a phishing attack against this executive at Imaginary Bank:  ***From:*** *imaginarybank@gmail.org*  ***Sent:*** *Saturday, December 21, 2019  15:05:05*  ***To:*** *cfo@imaginarybank.com*  ***Subject:*** *RE: You are been added to an ecsecutiv's groups*  *Conglaturations! You have been added to a collaboration group ‘Execs.’*  *Downlode ExecuTalk to your computer.*  ***Mac®*** *|* ***Windows®*** *|* ***Android™***  *You're team needs you! This invitation will expire in 48 hours so act quickly.*  *Sincerely,*  ***ExecuTalk©***  *All rights reserved.* |

Bắt đầu cuộc điều tra của bạn bằng cách phân tích tin nhắn đáng ngờ. Cố gắng xác định manh mối cho thấy đây là cuộc tấn công lừa đảo nhắm vào giám đốc điều hành này tại Imaginary Bank:

***Từ:*** *imaginarybank@gmail.org*

***Đã gửi:*** *Thứ bảy, ngày 21 tháng 12 năm 2019 15:05:05*

***Đến:*** *cfo@imaginarybank.com*

***Tiêu đề:*** *RE: Bạn đã được thêm vào nhóm của một giám đốc điều hành*

*Xin chúc mừng! Bạn đã được thêm vào nhóm cộng tác 'Execs'.*

*Tải ExecuTalk về máy tính của bạn.*

***Mac®*** *|* ***Windows®*** *|* ***Android™***

*Nhóm của bạn cần bạn! Lời mời này sẽ hết hạn sau 48 giờ nên hãy hành động nhanh chóng.*

*Trân trọng,*

***Thực hiện©***

*Mọi quyền được bảo lưu.*

|  |
| --- |
| **Step 2: Examine the sender's information**  Next, examine the major parts of this message in closer detail starting with the email header. You can often find clues in the message header that indicate you are dealing with a phishing attack.  Examine the email header of this suspicious message:  ***From:*** *imaginarybank@gmail.org*  ***Sent:*** *Saturday, December 21, 2019  15:05:05*  ***To:*** *cfo@imaginarybank.com*  ***Subject:*** *RE: You are been added to an ecsecutiv's groups* |

**Bước 2: Kiểm tra thông tin người gửi**

Tiếp theo, hãy kiểm tra các phần chính của tin nhắn này chi tiết hơn, bắt đầu từ tiêu đề email. Bạn thường có thể tìm thấy manh mối trong tiêu đề tin nhắn cho biết bạn đang phải đối mặt với một cuộc tấn công lừa đảo.

Kiểm tra tiêu đề email của tin nhắn đáng ngờ này:

***Từ:*** *imaginarybank@gmail.org*

***Đã gửi:*** *Thứ bảy, ngày 21 tháng 12 năm 2019 15:05:05*

***Đến:*** *cfo@imaginarybank.com*

***Tiêu đề:*** *RE: Bạn đã được thêm vào nhóm của một giám đốc điều hành*

|  |
| --- |
| **Pro tip:** Always check the domain name that comes after the @ symbol. Requests for sensitive information or asking you to download files should not come from personal accounts, like *@gmail.com, @icloud, @yahoo.com* or others. |

**Mẹo chuyên nghiệp:** Luôn kiểm tra tên miền theo sau ký hiệu @. Yêu cầu thông tin nhạy cảm hoặc yêu cầu bạn tải xuống tệp không nên đến từ tài khoản cá nhân, như *@gmail.com, @icloud, @yahoo.com* hoặc các tài khoản khác.

|  |
| --- |
| **Step 3: Review the message body for clues**  Next, review the body of the message received by the executive at Imaginary Bank. Try to identify three ways this threat actor tried to disguise their message as a legitimate email.  **Note:** This message is strictly meant to illustrate an example of an email that contains malicious download options.  *Conglaturations! You have been added to a collaboration group ‘Execs.’*  *Downlode ExecuTalk to your computer.*  ***Mac®*** *|* ***Windows®*** *|* ***Android™***  *You're team needs you! This invitation will expire in 48 hours so act quickly.*  *Sincerely,*  ***ExecuTalk©***  *All rights reserved.* |

**Bước 3: Xem lại nội dung tin nhắn để tìm manh mối**

Tiếp theo, hãy xem lại nội dung tin nhắn mà giám đốc điều hành tại Imaginary Bank nhận được. Cố gắng xác định ba cách mà kẻ tấn công này đã cố gắng ngụy trang tin nhắn của họ thành một email hợp pháp.

**Lưu ý:** Tin nhắn này chỉ nhằm mục đích minh họa ví dụ về email có chứa tùy chọn tải xuống độc hại.

*Xin chúc mừng! Bạn đã được thêm vào nhóm cộng tác 'Execs'.*

*Tải ExecuTalk về máy tính của bạn.*

***Mac®*** *|* ***Windows®*** *|* ***Android™***

*Nhóm của bạn cần bạn! Lời mời này sẽ hết hạn sau 48 giờ nên hãy hành động nhanh chóng.*

*Trân trọng,*

***Thực hiện©***

*Mọi quyền được bảo lưu.*

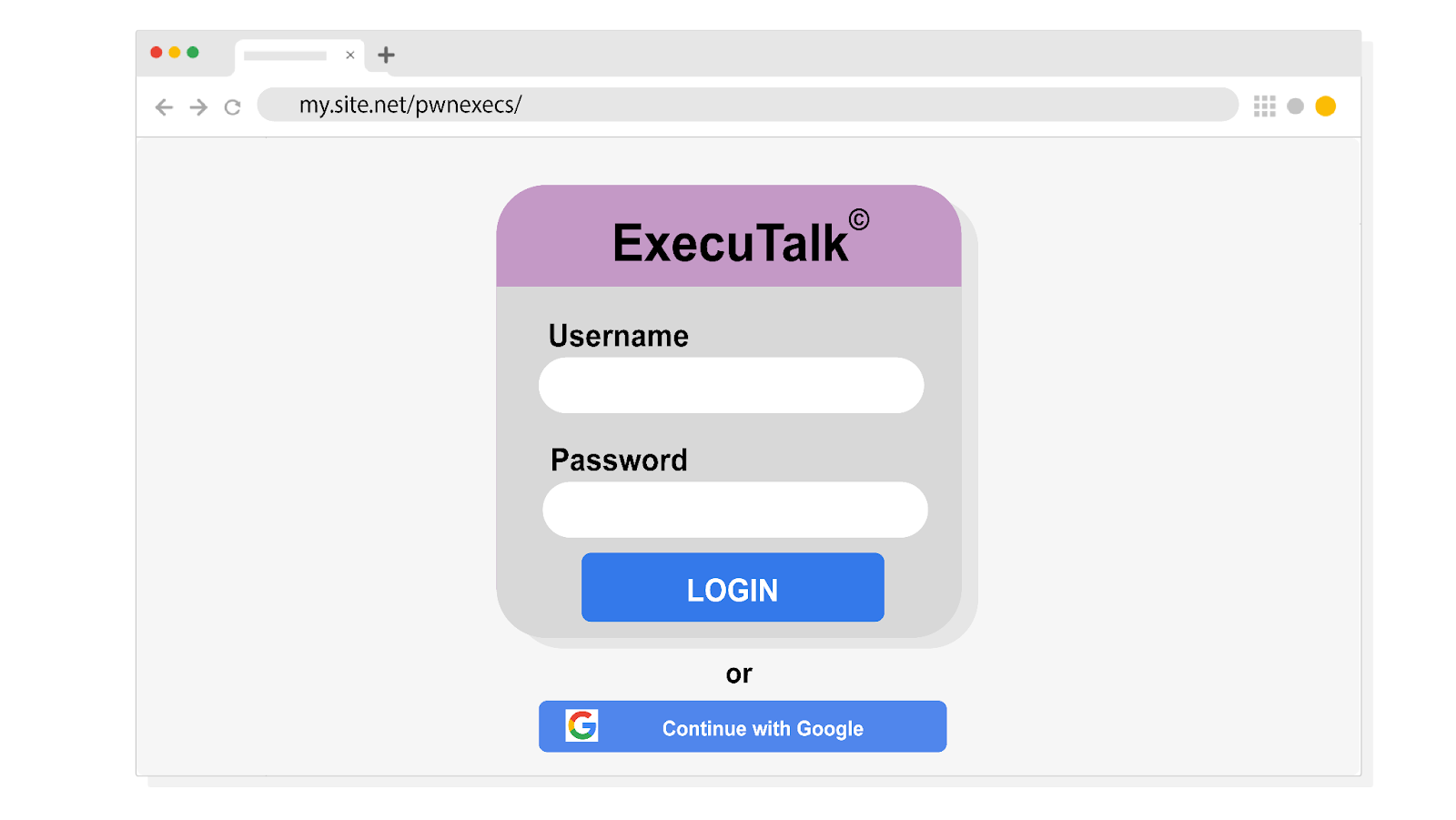
|  |
| --- |
| **Step 4: Investigate the download options**  Phishing emails often contain links that redirect to malicious sites or trigger malware downloads.  **Pro tip:** When investigating suspicious emails, hovering your mouse cursor over buttons will reveal the URL they redirect to without having to click them. This is the safest way to check if it will take you to a suspicious domain or if it links to an http:// URL that isn’t secure.  In this case, the message contains three download options. Each of them opens this login form: |

**Bước 4: Tìm hiểu các tùy chọn tải xuống**

Email lừa đảo thường chứa các liên kết chuyển hướng đến các trang web độc hại hoặc kích hoạt tải xuống phần mềm độc hại.

**Mẹo chuyên nghiệp:** Khi điều tra email đáng ngờ, hãy di con trỏ chuột qua các nút sẽ hiển thị URL mà chúng chuyển hướng đến mà không cần phải nhấp vào chúng. Đây là cách an toàn nhất để kiểm tra xem nó có đưa bạn đến một tên miền đáng ngờ hay liên kết đến một URL http:// không an toàn không.

Trong trường hợp này, tin nhắn chứa ba tùy chọn tải xuống. Mỗi tùy chọn mở biểu mẫu đăng nhập này:



**2. Malware – Phần mềm độc hại**

***2.1. Malicious software - Phần mềm độc hại***

|  |
| --- |
| People and computers are very different from one another. There's one way that we're alike. You know how? We're both vulnerable to getting an infection. While humans can be infected by a virus that causes a cold or flu, computers can be infected by malware. |

Con người và máy tính rất khác nhau.Có một điểm khiến chúng ta giống nhau.Bạn biết không? Cả hai chúng ta đềudễ bị nhiễm trùng.Trong khi con người có thể bị nhiễm vi-rútgây ra cảm lạnh hoặc cúm,máy tính có thể bị nhiễm phần mềm độc hại.

|  |
| --- |
| Malware is software designed to harm devices or networks. Malware, which is short for malicious software, can be spread in many ways. For example, it can be spread through an infected USB drive. Or also commonly spread between computers online. |

Phần mềm độc hại là phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng.Phần mềm độc hại, viết tắt của phần mềm độc hại,có thể lây lan theo nhiều cách.Ví dụ, nó có thể làlây lan qua ổ USB bị nhiễm virus.Hoặc cũng thường lây lan giữa các máy tính trực tuyến.

|  |
| --- |
| Devices and systems that are connected to the internet are especially vulnerable to infection. When a device becomes infected, malware interferes with its normal operations. Attackers use malware to take control of the infected system without the user's knowledge or permission. Malware has been a threat to people and organizations for a long time. Attackers have created many different strains of malware. They all vary in how they're spread. |

Các thiết bị và hệ thống được kết nối vớiInternet đặc biệt dễ bị nhiễm virus.Khi một thiết bị bị nhiễm virus,phần mềm độc hại can thiệp vào hoạt động bình thường của nó.Kẻ tấn công sử dụng phần mềm độc hại để kiểm soáthệ thống bị nhiễm mà không cósự hiểu biết hoặc sự cho phép của người dùng.Phần mềm độc hại đã trở thành mối đe dọa đối với con người vàcác tổ chức trong một thời gian dài.Những kẻ tấn công đã tạo ra nhiều loại phần mềm độc hại khác nhau.Mỗi loại đều có cách lây lan khác nhau.

|  |
| --- |
| Five of the most common types of malware are a virus, worm, trojan, ransomware, and spyware. Let's take a look at how each of them work. |

Năm loại phần mềm độc hại phổ biến nhất là vi-rút,sâu, trojan, phần mềm tống tiền và phần mềm gián điệp.Chúng ta hãy cùng xem xét cách thức hoạt động của từng loại.

|  |
| --- |
| A virus is malicious code written to interfere with computer operations and cause damage to data and software. Viruses typically hide inside of trusted applications. When the infected program is launched, the virus clones itself and spreads to other files on the device. An important characteristic of viruses is that they have to be activated by the user to start the infection. |

Một loại virus là mã độc được viết ra để can thiệp vàohoạt động máy tính và nguyên nhânthiệt hại cho dữ liệu và phần mềm.Virus thường ẩn náu bên trong các ứng dụng đáng tin cậy.Khi chương trình bị nhiễm được khởi chạy,virus tự nhân bản vàlây lan sang các tập tin khác trên thiết bị.Một đặc điểm quan trọng củavirus là chúng phảiđược người dùng kích hoạt để bắt đầu lây nhiễm.

|  |
| --- |
| The next kind of malware doesn't have this limitation. A worm is malware that can duplicate and spread itself across systems on its own. While viruses require users to perform an action like opening a file to duplicate, worms use an infected device as a host. They scan the connected network for other devices. Worms then infect everything on the network without requiring an action to trigger the spread. |

Loại phần mềm độc hại tiếp theo không có hạn chế này.Một con sâu là phần mềm độc hại có thểtự nhân đôi và lây lan trên khắp các hệ thống.Trong khi virus yêu cầu người dùng phải thực hiệnmột hành động như mở một tập tin để sao chép,sâu sử dụng thiết bị bị nhiễm làm vật chủ.Họ quét mạng được kết nối để tìm các thiết bị khác.Sau đó, sâu sẽ lây nhiễm mọi thứ trên mạngmà không cần thực hiện hành động nào để kích hoạt sự lây lan.

|  |
| --- |
| Viruses and worms are delivered through phishing emails and other methods before they infect a device. Making sure you click links only from trusted sources is one way to avoid these types of infection. However, attackers have designed another form of malware that can get past this precaution. |

Virus và sâu được đưa quaemail lừa đảo và các phương pháp kháctrước khi chúng lây nhiễm vào thiết bị.Đảm bảo bạn chỉ nhấp vào liên kết từnguồn đáng tin cậy là một cáchđể tránh những loại nhiễm trùng này.Tuy nhiên, những kẻ tấn công đã thiết kếmột dạng phần mềm độc hại kháccó thể vượt qua biện pháp phòng ngừa này.

|  |
| --- |
| A trojan, or Trojan horse, is malware that looks like a legitimate file or program. The name is a reference to an ancient Greek legend that's set in the city of Troy. In Troy, a group of soldiers hid inside a giant wooden horse that was presented as a gift to their enemies. It was accepted and brought inside the city walls. Later that evening, the soldiers inside of the horse climbed out and attacked the city. Like this ancient tale, attackers design trojans to appear harmless. This type of malware is typically disguised as files or useful applications to trick their target into installing them. |

Một con ngựa thành Troy, hay còn gọi là Trojan,là phần mềm độc hại trông giống như một tệp hoặc chương trình hợp pháp.Tên là một tham chiếu đếnmột truyền thuyết Hy Lạp cổ đại lấy bối cảnh ở thành phố Troy.Ở thành Troy, một nhóm lính ẩn núp bên trongmột con ngựa gỗ khổng lồđược tặng như một món quà cho kẻ thù của họ.Nó đã được chấp nhận và mang vào bên trong tường thành phố.Tối hôm đó, những người lính bên trongcủa con ngựa trèo ra và tấn công thành phố.Giống như câu chuyện cổ xưa này,Kẻ tấn công thiết kế trojan trông có vẻ vô hại.Loại phần mềm độc hại này thường được ngụy trang dưới dạng tệp hoặcứng dụng hữu ích để lừamục tiêu của họ là cài đặt chúng.

|  |
| --- |
| Attackers often use trojans to gain access and install another kind of malware called ransomware. Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. These kind of attacks have become very common these days. A unique feature of ransomware attacks is that they make themselves known to their targets. Without doing this, they couldn't collect the money they demand. Normally, they decrypt the hidden data as soon as the sum of money is paid. Unfortunately, there's no guarantee they won't return to demand more. |

Những kẻ tấn công thường sử dụng trojan để truy cập vàcài đặt một loại phần mềm độc hại khác gọi là ransomware.Ransomware là một loại tấn công độc hại mà kẻ tấn côngmã hóa dữ liệu của một tổ chức vàyêu cầu thanh toán để khôi phục quyền truy cập.Những kiểu tấn công này đã trở nên rất phổ biến hiện nay.Một tính năng độc đáo củacác cuộc tấn công ransomware là họđể mục tiêu của họ biết đến mình.Nếu không làm điều này, họkhông thể thu được số tiền họ yêu cầu.Thông thường, họ giải mã dữ liệu ẩnngay sau khi số tiền được thanh toán.Thật không may, không có sự đảm bảo nàohọ sẽ không quay lại để đòi hỏi thêm nữa.

|  |
| --- |
| The last type of malware I want to mention is spyware. Spyware is malware that's used to gather and sell information without consent. Consent is a keyword in this case. |

Loại phần mềm độc hại cuối cùng tôi muốn đề cập là phần mềm gián điệp.Phần mềm gián điệp là phần mềm độc hại được sử dụng đểthu thập và bán thông tin mà không có sự đồng ý.Sự đồng ý là từ khóa trong trường hợp này.

|  |
| --- |
| Organizations also collect information about their customers, like their browsing habits and purchase history. However, they always give their customers the ability to opt out. Cybercriminals, on the other hand, use spyware to steal information. They use spyware attacks to collect data like login credentials, account PINs, and other types of sensitive information for their own personal gain. |

Các tổ chức cũngthu thập thông tin về khách hàng của họ,như thói quen duyệt web và lịch sử mua hàng của họ.Tuy nhiên, họ luôn luôn đưa racho khách hàng của họ khả năng lựa chọn không tham gia.Mặt khác, tội phạm mạngsử dụng phần mềm gián điệp để đánh cắp thông tin.Họ sử dụng các cuộc tấn công phần mềm gián điệp đểthu thập dữ liệu như thông tin đăng nhập,mã PIN tài khoản và các loại khácthông tin nhạy cảm để phục vụ lợi ích cá nhân.

|  |
| --- |
| There are many other types of malware besides these and new forms are always evolving. They all pose a serious risk to individuals and organizations. Next time, we'll explore how security teams detect and remove these kinds of threats. |

Ngoài ra còn có nhiều loại phần mềm độc hại khácnhững hình thức này và những hình thức mới luôn luôn phát triển.Tất cả chúng đều gây ra rủi ro nghiêm trọngcho cá nhân và tổ chức.Lần tới, chúng ta sẽ khám phá cáchnhóm an ninh phát hiện và loại bỏ những mối đe dọa như thế này.

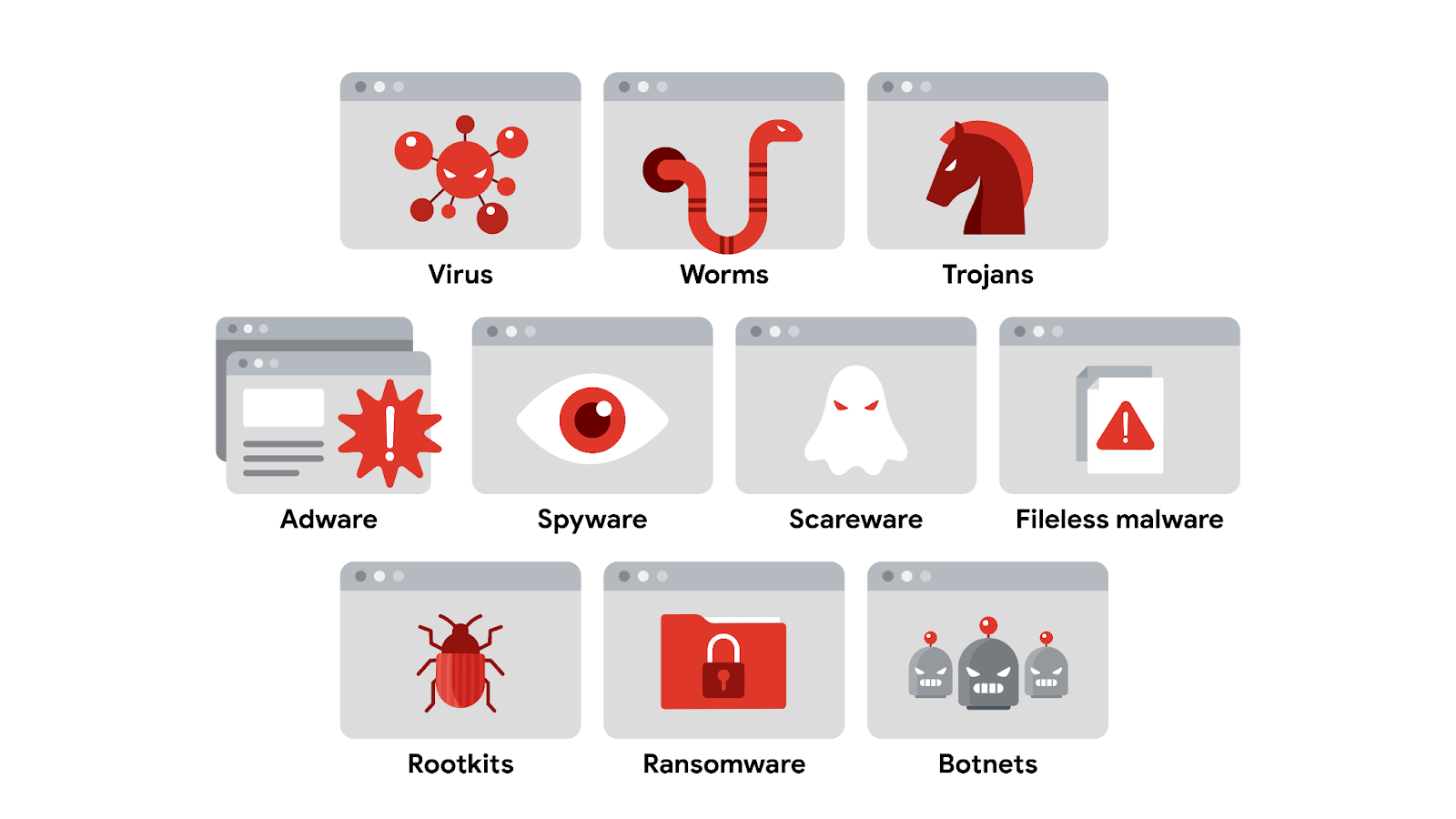
***2.2. An introduction to malware - Giới thiệu về phần mềm độc hại***

|  |
| --- |
| **An introduction to malware** |

**Giới thiệu về phần mềm độc hại**

|  |
| --- |
| Previously, you learned that malware is software designed to harm devices or networks. Since its first appearance on personal computers decades ago, malware has developed into a variety of strains. Being able to identify different types of malware and understand the ways in which they are spread will help you stay alert and be informed as a security professional. |

Trước đây, bạn đã biết rằng **phần mềm độc hại** là phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng. Kể từ lần đầu tiên xuất hiện trên máy tính cá nhân cách đây nhiều thập kỷ, phần mềm độc hại đã phát triển thành nhiều loại khác nhau. Có thể xác định các loại phần mềm độc hại khác nhau và hiểu cách chúng lây lan sẽ giúp bạn luôn cảnh giác và được thông báo với tư cách là một chuyên gia bảo mật.



|  |
| --- |
| **Virus** |

**Vi-rút**

|  |
| --- |
| A **virus** is malicious code written to interfere with computer operations and cause damage to data and software. This type of malware must be installed by the target user before it can spread itself and cause damage. One of the many ways that viruses are spread is through phishing campaigns where malicious links are hidden within links or attachments. |

Virus là mã độc được viết ra để can thiệp vào hoạt động của máy tính và gây thiệt hại cho dữ liệu và phần mềm. Loại phần mềm độc hại này phải được người dùng mục tiêu **cài** đặt trước khi nó có thể tự lây lan và gây thiệt hại. Một trong nhiều cách mà virus lây lan là thông qua các chiến dịch lừa đảo, trong đó các liên kết độc hại được ẩn trong các liên kết hoặc tệp đính kèm.

|  |
| --- |
| **Worm** |

**Sâu**

|  |
| --- |
| A **worm** is malware that can duplicate and spread itself across systems on its own. Similar to a virus, a worm must be installed by the target user and can also be spread with tactics like malicious email. Given a worm's ability to spread on its own, attackers sometimes target devices, drives, or files that have shared access over a network. |

Sâu là **phần** mềm độc hại có thể tự nhân bản và tự lây lan trên các hệ thống. Tương tự như vi-rút, sâu phải được người dùng mục tiêu cài đặt và cũng có thể lây lan bằng các chiến thuật như email độc hại. Với khả năng tự lây lan của sâu, kẻ tấn công đôi khi nhắm vào các thiết bị, ổ đĩa hoặc tệp có quyền truy cập được chia sẻ qua mạng.

|  |
| --- |
| A well known example is the Blaster worm, also known as Lovesan, Lovsan, or MSBlast. In the early 2000s, this worm spread itself on computers running Windows XP and Windows 2000 operating systems. It would force devices into a continuous loop of shutting down and restarting. Although it did not damage the infected devices, it was able to spread itself to hundreds of thousands of users around the world. Many variants of the Blaster worm have been deployed since the original and can infect modern computers. |

Một ví dụ nổi tiếng là sâu Blaster, còn được gọi là Lovesan, Lovsan hoặc MSBlast. Vào đầu những năm 2000, sâu này đã tự lây lan trên các máy tính chạy hệ điều hành Windows XP và Windows 2000. Nó sẽ buộc các thiết bị vào một vòng lặp liên tục tắt máy và khởi động lại. Mặc dù nó không làm hỏng các thiết bị bị nhiễm, nhưng nó có thể tự lây lan sang hàng trăm nghìn người dùng trên toàn thế giới. Nhiều biến thể của sâu Blaster đã được triển khai kể từ bản gốc và có thể lây nhiễm các máy tính hiện đại.

|  |
| --- |
| **Note:** Worms were very popular attacks in the mid 2000s but are less frequently used in recent years. |

**Lưu ý:** Sâu máy tính là loại tấn công rất phổ biến vào giữa những năm 2000 nhưng ít được sử dụng hơn trong những năm gần đây.

|  |
| --- |
| **Trojan** |

**Trojan**

|  |
| --- |
| A trojan, also called a **Trojan horse**, is malware that looks like a legitimate file or program. This characteristic relates to how trojans are spread. Similar to viruses, attackers deliver this type of malware hidden in file and application downloads. Attackers rely on tricking unsuspecting users into believing they’re downloading a harmless file, when they’re actually infecting their own device with malware that can be used to spy on them, grant access to other devices, and more. |

Trojan, còn được gọi là **Trojan horse** , là phần mềm độc hại trông giống như một tệp hoặc chương trình hợp pháp. Đặc điểm này liên quan đến cách trojan lây lan. Tương tự như vi-rút, kẻ tấn công phân phối loại phần mềm độc hại này ẩn trong tệp và ứng dụng tải xuống. Kẻ tấn công dựa vào việc lừa người dùng không nghi ngờ tin rằng họ đang tải xuống một tệp vô hại, trong khi thực tế là chúng đang lây nhiễm phần mềm độc hại vào thiết bị của chính mình để có thể theo dõi họ, cấp quyền truy cập vào các thiết bị khác, v.v.

|  |
| --- |
| **Adware** |

**Phần mềm quảng cáo**

|  |
| --- |
| Advertising-supported software, or **adware**, is a type of legitimate software that is sometimes used to display digital advertisements in applications. Software developers often use adware as a way to lower their production costs or to make their products free to the public—also known as freeware or shareware. In these instances, developers monetize their product through ad revenue rather than at the expense of their users. |

Phần mềm được hỗ trợ quảng cáo, hay **phần mềm quảng cáo** , là một loại phần mềm hợp pháp đôi khi được sử dụng để hiển thị quảng cáo kỹ thuật số trong các ứng dụng. Các nhà phát triển phần mềm thường sử dụng phần mềm quảng cáo như một cách để giảm chi phí sản xuất hoặc để sản phẩm của họ miễn phí cho công chúng—còn được gọi là phần mềm miễn phí hoặc phần mềm chia sẻ. Trong những trường hợp này, các nhà phát triển kiếm tiền từ sản phẩm của họ thông qua doanh thu quảng cáo thay vì bằng chi phí của người dùng.

|  |
| --- |
| Malicious adware falls into a sub-category of malware known as a **potentially unwanted application (PUA)**. A PUA is a type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software. Attackers sometimes hide this type of malware in freeware with insecure design to monetize ads for themselves instead of the developer. This works even when the user has declined to receive ads. |

Phần mềm quảng cáo độc hại thuộc một tiểu thể loại phần mềm độc hại được gọi là **ứng dụng có khả năng không mong muốn (PUA)** . PUA là một loại phần mềm không mong muốn được đóng gói cùng với các chương trình hợp pháp có thể hiển thị quảng cáo, làm chậm thiết bị hoặc cài đặt phần mềm khác. Kẻ tấn công đôi khi ẩn loại phần mềm độc hại này trong phần mềm miễn phí với thiết kế không an toàn để kiếm tiền từ quảng cáo cho chính chúng thay vì nhà phát triển. Điều này vẫn hiệu quả ngay cả khi người dùng đã từ chối nhận quảng cáo.

|  |
| --- |
| **Spyware** |

**Phần mềm gián điệp**

|  |
| --- |
| **Spyware** is malware that's used to gather and sell information without consent. It's also considered a PUA. Spyware is commonly hidden in *bundleware*, additional software that is sometimes packaged with other applications. PUAs like spyware have become a serious challenge in the open-source software development ecosystem. That’s because developers tend to overlook how their software could be misused or abused by others. |

**Spyware** là phần mềm độc hại được sử dụng để thu thập và bán thông tin mà không có sự đồng ý. Nó cũng được coi là PUA. Spyware thường ẩn trong *bundleware* , phần mềm bổ sung đôi khi được đóng gói cùng với các ứng dụng khác. PUA như spyware đã trở thành một thách thức nghiêm trọng trong hệ sinh thái phát triển phần mềm nguồn mở. Đó là vì các nhà phát triển có xu hướng bỏ qua cách phần mềm của họ có thể bị người khác sử dụng sai hoặc lạm dụng.

|  |
| --- |
| **Scareware** |

**Phần mềm hù dọa**

|  |
| --- |
| Another type of PUA is **scareware**. This type of malware employs tactics to frighten users into infecting their own device. Scareware tricks users by displaying fake warnings that appear to come from legitimate companies. Email and pop-ups are just a couple of ways scareware is spread. Both can be used to deliver phony warnings with false claims about the user's files or data being at risk. |

Một loại PUA khác là **scareware** . Loại phần mềm độc hại này sử dụng các chiến thuật để dọa người dùng lây nhiễm vào thiết bị của chính họ. Scareware lừa người dùng bằng cách hiển thị các cảnh báo giả mạo có vẻ như đến từ các công ty hợp pháp. Email và cửa sổ bật lên chỉ là một vài cách mà scareware lây lan. Cả hai đều có thể được sử dụng để đưa ra các cảnh báo giả mạo với các tuyên bố sai sự thật về việc tệp hoặc dữ liệu của người dùng đang gặp rủi ro.

|  |
| --- |
| **Fileless malware** |

**Phần mềm độc hại không có tệp**

|  |
| --- |
| **Fileless malware** does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer. This type of infection resides in memory where the malware never touches the hard drive. This is unlike the other types of malware, which are stored within a file on disk. Instead, these stealthy infections get into the operating system or hide within trusted applications. |

**Phần mềm độc hại không có tệp** không cần người dùng cài đặt vì nó sử dụng các chương trình hợp lệ đã được cài đặt để lây nhiễm máy tính. Loại nhiễm trùng này nằm trong bộ nhớ nơi phần mềm độc hại không bao giờ chạm vào ổ cứng. Điều này không giống như các loại phần mềm độc hại khác, được lưu trữ trong một tệp trên đĩa. Thay vào đó, các loại nhiễm trùng lén lút này xâm nhập vào hệ điều hành hoặc ẩn trong các ứng dụng đáng tin cậy.

|  |
| --- |
| **Pro tip:** Fileless malware is detected by performing memory analysis, which requires experience with operating systems. |

**Mẹo chuyên nghiệp:** Phần mềm độc hại không có tệp được phát hiện bằng cách thực hiện phân tích bộ nhớ, đòi hỏi kinh nghiệm với hệ điều hành.

|  |
| --- |
| **Rootkits** |

**Rootkits**

|  |
| --- |
| A **rootkit** is malware that provides remote, administrative access to a computer. Most attackers use rootkits to open a backdoor to systems, allowing them to install other forms of malware or to conduct network security attacks. |

Rootkit là **phần** mềm độc hại cung cấp quyền truy cập quản trị từ xa vào máy tính. Hầu hết kẻ tấn công sử dụng rootkit để mở cửa hậu vào hệ thống, cho phép chúng cài đặt các dạng phần mềm độc hại khác hoặc thực hiện các cuộc tấn công bảo mật mạng.

|  |
| --- |
| This kind of malware is often spread by a combination of two components: a dropper and a loader. A **dropper** is a type of malware that comes packed with malicious code which is delivered and installed onto a target system. For example, a dropper is often disguised as a legitimate file, such as a document, an image, or an executable to deceive its target into opening, or dropping it, onto their device. If the user opens the dropper program, its malicious code is executed and it hides itself on the target system. |

Loại phần mềm độc hại này thường được phát tán bằng sự kết hợp của hai thành phần: dropper và loader. Dropper **là** một loại phần mềm độc hại đi kèm với mã độc được phân phối và cài đặt vào hệ thống mục tiêu. Ví dụ, dropper thường được ngụy trang thành một tệp hợp lệ, chẳng hạn như tài liệu, hình ảnh hoặc tệp thực thi để đánh lừa mục tiêu mở hoặc thả tệp đó vào thiết bị của họ. Nếu người dùng mở chương trình dropper, mã độc của nó sẽ được thực thi và ẩn mình trên hệ thống mục tiêu.

|  |
| --- |
| Multi-staged malware attacks, where multiple packets of malicious code are deployed, commonly use a variation called a loader. A **loader** is a type of malware that downloads strains of malicious code from an external source and installs them onto a target system. Attackers might use loaders for different purposes, such as to set up another type of malware---a botnet. |

Các cuộc tấn công phần mềm độc hại nhiều giai đoạn, trong đó nhiều gói mã độc hại được triển khai, thường sử dụng một biến thể gọi là trình tải. **Trình tải** là một loại phần mềm độc hại tải xuống các chủng mã độc hại từ nguồn bên ngoài và cài đặt chúng vào hệ thống mục tiêu. Kẻ tấn công có thể sử dụng trình tải cho các mục đích khác nhau, chẳng hạn như thiết lập một loại phần mềm độc hại khác --- botnet.

|  |
| --- |
| **Botnet** |

**Mạng lưới bot**

|  |
| --- |
| A **botnet**, short for “robot network,” is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder.” Viruses, worms, and trojans are often used to spread the initial infection and turn the devices into a bot for the bot-herder. The attacker then uses file sharing, email, or social media application protocols to create new bots and grow the botnet. When a target unknowingly opens the malicious file, the computer, or bot, reports the information back to the bot-herder, who can execute commands on the infected computer. |

Botnet , viết tắt của “robot network”, là một tập hợp các máy tính bị nhiễm **phần** mềm độc hại nằm dưới sự kiểm soát của một tác nhân đe dọa duy nhất, được gọi là “bot-herder”. Virus, sâu và trojan thường được sử dụng để phát tán sự lây nhiễm ban đầu và biến các thiết bị thành bot cho bot-herder. Sau đó, kẻ tấn công sử dụng các giao thức ứng dụng chia sẻ tệp, email hoặc phương tiện truyền thông xã hội để tạo bot mới và phát triển botnet. Khi mục tiêu vô tình mở tệp độc hại, máy tính hoặc bot sẽ báo cáo thông tin trở lại bot-herder, người có thể thực hiện các lệnh trên máy tính bị nhiễm.

|  |
| --- |
| **Ransomware** |

**Phần mềm tống tiền**

|  |
| --- |
| Ransomware describes a malicious attack where threat actors encrypt an organization's data and demand payment to restore access. According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware crimes are on the rise and becoming increasingly sophisticated. Ransomware infections can cause significant damage to an organization and its customers. An example is the [WannaCry](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) attack that encrypts a victim's computer until a ransom payment of cryptocurrency is paid. |

Ransomware mô tả một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của một tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập. Theo Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA), tội phạm ransomware đang gia tăng và ngày càng tinh vi. Nhiễm ransomware có thể gây ra thiệt hại đáng kể cho một tổ chức và khách hàng của tổ chức đó. Một ví dụ là[Muốn Khóc](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)cuộc tấn công mã hóa máy tính của nạn nhân cho đến khi khoản tiền chuộc bằng tiền điện tử được trả.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| The variety of malware is astounding. The number of ways that it’s spread is even more staggering. Malware is a complex threat that can require its own specialization in cybersecurity. One place to learn more about malware analysis is [INFOSEC's introductory course on malware analysis](https://www.infosecinstitute.com/skills/courses/malware-analysis-introduction/). Even without specializing in malware analysis, recognizing the types of malware and how they’re spread is an important part of defending against these attacks as a security analyst. |

Sự đa dạng của phần mềm độc hại thật đáng kinh ngạc. Số lượng cách mà nó lây lan thậm chí còn đáng kinh ngạc hơn. Phần mềm độc hại là một mối đe dọa phức tạp có thể đòi hỏi chuyên môn riêng về an ninh mạng. Một nơi để tìm hiểu thêm về phân tích phần mềm độc hại là[Khóa học giới thiệu về phân tích phần mềm độc hại của INFOSEC](https://www.infosecinstitute.com/skills/courses/malware-analysis-introduction/). Ngay cả khi không chuyên về phân tích phần mềm độc hại, việc nhận biết các loại phần mềm độc hại và cách chúng lây lan cũng là một phần quan trọng trong việc phòng thủ chống lại các cuộc tấn công này với tư cách là một nhà phân tích bảo mật.

***2.3. The rise of cryptojacking - Sự gia tăng của cryptojacking***

|  |
| --- |
| Malware has been around nearly as long as computers. In its earliest forms, it was used by troublemakers as a form of digital vandalism. In today's digital world, malware has become a profitable crime that attackers use for their own financial gain. |

Phần mềm độc hại đã tồn tại gần như lâu đời như máy tính.Ở dạng ban đầu của nó,nó được sử dụng bởi những kẻ gây rốinhư một hình thức phá hoại kỹ thuật số.Trong thế giới kỹ thuật số ngày nay,phần mềm độc hại đã trở thành một tội phạm có lợi nhuậnmà kẻ tấn công sử dụng để kiếm lợi nhuận cho riêng mình.

|  |
| --- |
| As a security professional, it's important that you remain aware of the latest evolutions. Let's take a closer look at one way malware has evolved. We'll then use this example to consider how malware can be spotted and how you can proactively protect against malware. Ransomware is one of the types of malware attackers use to steal money. |

Là một chuyên gia an ninh,điều quan trọng là bạn phải duy trìbiết về những diễn biến mới nhất.Chúng ta hãy cùng xem xét kỹ hơn cách phần mềm độc hại đã phát triển.Sau đó chúng ta sẽ sử dụng ví dụ nàyđể xem xét phần mềm độc hại có thể như thế nàophát hiện và làm thế nào bạn có thểchủ động bảo vệ chống lại phần mềm độc hại.Ransomware là một trong những loạikẻ tấn công sử dụng phần mềm độc hại để đánh cắp tiền.

|  |
| --- |
| Another more recent type of malware is cryptojacking. Cryptojacking is a form of malware that installs software to illegally mine cryptocurrencies. You may be familiar with cryptocurrency from the news. If you're new to the topic, cryptocurrencies are a form of digital money that have real-world value. Like physical forms of currency, there are many different types. For the most part, they're referred to as coins or tokens. |

Một loại phần mềm độc hại mới hơn là cryptojacking.Cryptojacking là một dạng phần mềm độc hại được cài đặtphần mềm khai thác tiền điện tử trái phép.Bạn có thể đã biết đến tiền điện tử qua tin tức.Nếu bạn mới biết đến chủ đề này,tiền điện tử là một hình thức tiền kỹ thuật số cógiá trị thực tế. Giống như các hình thức tiền tệ vật lý,có nhiều loại khác nhau.Phần lớn,chúng được gọi là tiền xu hoặc token.

|  |
| --- |
| In simple terms, crypto mining is a process used to obtain new coins. Crypto mining is similar to the process for mining for other resources, like gold. Mining for something like gold involves machinery, such as trucks and bulldozers, that can dig through the Earth. Crypto coins, on the other hand, use computers instead. Rather than digging through the Earth, the computers run software that dig through billions of lines of encrypted code. When enough code is processed, a crypto coin can be found. |

Nói một cách đơn giản, khai thác tiền điện tử làmột quá trình được sử dụng để có được tiền xu mới.Khai thác tiền điện tử tương tự như quá trìnhđể khai thác các nguồn tài nguyên khác, như vàng.Khai thác thứ gì đó như vàng liên quan đến máy móc, chẳng hạn nhưgiống như xe tải và xe ủi đất, có thể đào xuyên qua Trái Đất.Mặt khác, tiền điện tửsử dụng máy tính thay thế. Thay vào đóhơn là đào xuyên qua Trái Đất,các máy tính chạy phần mềm đàothông qua hàng tỷ dòng mã được mã hóa.Khi xử lý đủ mã, một đồng tiền điện tử có thể được tìm thấy.

|  |
| --- |
| Generally, more computers mining for coins mean more cryptocurrency can be discovered. Criminals unfortunately figured this out. Beginning in 2017, cryptojacking malware started being used to gain unauthorized control of personal computers to mine cryptocurrency. |

Nói chung, nhiều máy tính khai thác hơntiền xu có nghĩa là có thể khám phá thêm nhiều loại tiền điện tử hơn.Thật không may là bọn tội phạm đã phát hiện ra điều này.Bắt đầu từ năm 2017, cryptojackingphần mềm độc hại bắt đầu được sử dụng để giành quyền kiểm soát trái phépcủa máy tính cá nhân để khai thác tiền điện tử.

|  |
| --- |
| Since that time, cryptojacking techniques have become more sophisticated. Criminals now regularly target vulnerable servers to spread their mining software. Devices that communicate with the infected server become infected themselves. The malicious code then runs in the background, mining for coins unknown to anyone. |

Kể từ thời điểm đó,Các kỹ thuật đào tiền điện tử đã trở nên tinh vi hơn.Tội phạm hiện nay thường xuyên nhắm mục tiêumáy chủ dễ bị tấn công để phát tán phần mềm khai thác.Các thiết bị giao tiếp vớimáy chủ bị nhiễm cũng sẽ bị nhiễm.Sau đó, mã độc sẽ chạy ẩn trong nền,khai thác những đồng tiền mà không ai biết đến.

|  |
| --- |
| Cryptojacking software is hard to detect. Luckily, security professionals have sophisticated tools that can help. An intrusion detection system, or IDS, is an application that monitors system activity and alerts some possible intrusions. When abnormal activity is detected like, malware mining for coins, the IDS alerts security personnel. |

Phần mềm đào tiền điện tử rất khó phát hiện.May mắn thay, các chuyên gia an ninhcó những công cụ tinh vi có thể giúp ích.Hệ thống phát hiện xâm nhập, hay IDS, là một ứng dụnggiám sát hoạt động của hệ thốngvà cảnh báo một số khả năng xâm nhập.Khi phát hiện hoạt động bất thường như phần mềm độc hạikhai thác tiền điện tử, IDS sẽ cảnh báo nhân viên an ninh.

|  |
| --- |
| Despite their usefulness, detection systems have a major drawback. New forms of malware can remain undetected. Fortunately, there are subtle signs that indicate a device is infected with cryptojacking software or other forms of malware. |

Mặc dù chúng hữu ích,hệ thống phát hiện có một nhược điểm lớn.Các dạng phần mềm độc hại mới có thể không bị phát hiện.May mắn thay, códấu hiệu tinh tế cho thấy một thiết bị làbị nhiễm phần mềm đào tiền mã hóahoặc các dạng phần mềm độc hại khác.

|  |
| --- |
| By far the most telling sign of a cryptojacking infection is slowdown. Other signs include increased CPU usage, sudden system crashes, and fast draining batteries. Another sign is unusually high electricity costs related to the resource- intensive process of crypto mining. |

Dấu hiệu rõ ràng nhất cho đến nayNhiễm trùng cryptojacking làm chậm quá trình.Các dấu hiệu khác bao gồm việc sử dụng CPU tăng lên,Hệ thống đột ngột bị sập và pin nhanh hết.Một dấu hiệu khác là chi phí điện cao bất thườngliên quan đến quá trình sử dụng nhiều tài nguyêncủa khai thác tiền điện tử.

|  |
| --- |
| It's also good to know that there are certain measures you can take to reduce the likelihood of experiencing a malware attack like cryptojacking. These defenses include things like using browser extensions designed to block malware, using ad blockers, disabling JavaScript, and staying alert on the latest trends. Security analysts can also educate others in their organizations on malware attacks. |

Cũng tốt khi biết rằng cómột số biện pháp bạn có thể thực hiện đểgiảm khả năng gặp phảimột cuộc tấn công bằng phần mềm độc hại như cryptojacking.Những biện pháp phòng thủ này bao gồm những thứ như sử dụngtiện ích mở rộng trình duyệt được thiết kế để chặn phần mềm độc hại,sử dụng trình chặn quảng cáo, vô hiệu hóaJavaScript và luôn cập nhật những xu hướng mới nhất.Các nhà phân tích an ninh cũng có thể giáo dục những người kháctổ chức của họ về các cuộc tấn công phần mềm độc hại.

|  |
| --- |
| While cryptojacking is still relatively new, attacks are becoming more common. The type of malicious code cybercriminals spread is continually evolving. It takes many years of experience to analyze new forms of malware. Nevertheless, you're well on your way towards helping defend against these threats. |

Mặc dù cryptojacking vẫn còn tương đối mới,các cuộc tấn công đang trở nên phổ biến hơn.Loại mã độc hạiTội phạm mạng đang không ngừng phát triển và lây lan.Phải mất nhiều năm kinh nghiệmđể phân tích các dạng phần mềm độc hại mới.Tuy nhiên, bạn vẫn ổncách giúp bạn bảo vệ bản thân khỏi những mối đe dọa này.

***2.4. Test your knowledge: Malware - Kiểm tra kiến thức của bạn: Phần mềm độc hại***

**3. Web-based exploits – Khai thác dựa trên web**

***3.1. Cross-site scripting (XSS) - Kịch bản chéo trang web (XSS)***

|  |
| --- |
| Previously, we explored a few types of malware. Whether it's installed on an individual computer or a network server, all malicious software needs to be delivered to the target before it can work. Phishing and other social engineering techniques are common ways for malware to be delivered. Another way it's spread is using a broad class of threats known as web based exploits. |

Trước đây, chúng ta đã tìm hiểu một số loại phần mềm độc hại.Cho dù nó được cài đặt trên một cá nhânmáy tính hoặc máy chủ mạng, tất cả phần mềm độc hại cần phải đượcđược chuyển đến mục tiêu trước khi nó có thể hoạt động.Lừa đảo và các kỹ thuật xã hội kháckỹ thuật là cách phổ biến để phát tán phần mềm độc hại.Một cách khác để lan truyền nó là sử dụng một cách rộng rãilớp mối đe dọa được gọi là khai thác dựa trên web.

|  |
| --- |
| Web-based exploits are malicious code or behavior that's used to take advantage of coding flaws in a web application. Cybercriminals target web-based exploits to obtain sensitive personal information. Attacks occur because web applications interact with multiple users across multiple networks. Malicious hackers commonly exploit this high level of interaction using injection attacks. |

Các khai thác dựa trên web là mã độc hại hoặc hành viđược sử dụng để lợi dụng các lỗi mã hóa trong ứng dụng web.Tội phạm mạng nhắm vào các lỗ hổng trên web để lấy cắp thông tin cá nhân nhạy cảm.Các cuộc tấn công xảy ra vì các ứng dụng webtương tác với nhiều người dùng trên nhiều mạng lưới.Những tin tặc độc hại thường khai thác điều nàymức độ tương tác cao sử dụng các cuộc tấn công tiêm nhiễm.

|  |
| --- |
| An injection attack is malicious code inserted into a vulnerable application. The infected application often appears to work normally. That's because the injected code runs in the background, unknown to the user. Applications are vulnerable to injection attacks because they are programmed to receive data inputs. This could be something the user types, clicks, or something one program is sharing with another. When coded correctly, applications should be able to interpret and handle user inputs. |

Tấn công tiêm mã độc là chèn mã độc vào một ứng dụng dễ bị tấn công.Ứng dụng bị nhiễm thường có vẻ hoạt động bình thường.Đó là vì mã được chèn chạy ngầm mà người dùng không biết.Các ứng dụng dễ bị tấn côngtấn công vì chúng được lập trình để tiếp nhận dữ liệu đầu vào.Đây có thể là thứ mà người dùng nhập,nhấp chuột hoặc thứ gì đó mà một chương trình đang chia sẻ với chương trình khác.Khi được mã hóa chính xác,các ứng dụng phải có khả năng diễn giải và xử lý thông tin đầu vào của người dùng.

|  |
| --- |
| For example, let's say an application is expecting the user to enter a phone number. This application should validate the input from the user to make sure the data is all numbers and not more than ten digits. If the input from the user doesn't meet these requirements, the application should know how to handle it. Web apps interact with multiple users across many platforms. They also have a lot of interactive objects like images and buttons. This makes it challenging for developers to think of all the ways they should sanitize their input. |

Ví dụ, giả sử một ứng dụng làyêu cầu người dùng nhập số điện thoại.Ứng dụng này sẽ xác thực đầu vàotừ người dùng để đảm bảo dữ liệu chỉ là số và không quá mười chữ số.Nếu đầu vào từ người dùng không đáp ứngnhững yêu cầu này, ứng dụng phải biết cách xử lý.Ứng dụng web tương tác với nhiều người dùng trên nhiều nền tảng.Chúng cũng có rất nhiều đối tượng tương tác như hình ảnh và nút bấm.Điều này gây khó khăn cho các nhà phát triểnnghĩ về mọi cách để họ có thể khử trùng thông tin đầu vào của mình.

|  |
| --- |
| A common and dangerous type of injection attack that's a threat to web apps is cross-site scripting. Cross site scripting, or XSS, is an injection attack that inserts code into a vulnerable website or web application. These attacks are often delivered by exploiting the two languages used by most websites, HTML and JavaScript. Both can give cybercriminals access to everything that loads on the infected web page. This can include session cookies, geolocation, and even webcams and microphones. |

Một loại tiêm phổ biến và nguy hiểmCuộc tấn công đe dọa các ứng dụng web là tấn công xuyên trang web.Cross site scripting, hay XSS, là một cuộc tấn công chèn mãvào một trang web hoặc ứng dụng web dễ bị tấn công.Những cuộc tấn công này thường được thực hiệnbằng cách khai thác hai ngôn ngữ được sử dụng bởi hầu hết các trang web là HTML và JavaScript.Cả hai đều có thể cung cấp cho tội phạm mạng quyền truy cậpmọi thứ tải trên trang web bị nhiễm.Điều này có thể bao gồm cookie phiên,định vị địa lý, thậm chí cả webcam và micrô.

|  |
| --- |
| There are three main types of cross-site scripting attacks reflected, stored, and DOM-based. |

Có ba loại tấn công mã lệnh chéo trang chínhphản ánh, lưu trữ và dựa trên DOM.

|  |
| --- |
| A reflected XSS attack is an instance where a malicious script is sent to the server and activated during the server's response. A common example of this is the search bar of a website. In a reflected XSS attack, criminals send their target a web link that appears to go to a trusted site. When they click the link, it sends a HTTP request to the vulnerable site server. The attacker script is then returned or reflected back to the innocent user's browser. Here, the browser loads the malicious script because it trusts the server's response. With the script loaded, information like session cookies are sent back to the attacker. |

Một cuộc tấn công XSS phản ánh là trường hợp một tập lệnh độc hại được gửiđến máy chủ và được kích hoạt trong quá trình phản hồi của máy chủ.Một ví dụ phổ biến về điều này là thanh tìm kiếm của một trang web.Trong một cuộc tấn công XSS phản xạ,Tội phạm gửi cho mục tiêu một liên kết web có vẻ như dẫn đến một trang web đáng tin cậy.Khi họ nhấp vào liên kết, nó sẽ gửi một yêu cầu HTTP đến máy chủ trang web dễ bị tấn công.Sau đó, tập lệnh của kẻ tấn công được trả về hoặcphản chiếu lại trình duyệt của người dùng vô tội.Ở đây, trình duyệt tải phần mềm độc hạiscript vì nó tin tưởng vào phản hồi của máy chủ.Với tập lệnh được tải,thông tin như cookie phiên được gửi lại cho kẻ tấn công.

|  |
| --- |
| In a stored XSS attack, the malicious script isn't hidden in a link that needs to be sent to the server. Instead a stored XSS attack is an instance when malicious script is injected directly on the server. Here, attackers target elements of a site that are served to the user. This could be things like images and buttons that load when the site is visited. Infected elements activate the malicious code when a user simply visits the site. Stored XSS attacks can be damaging because the user has no way of knowing the site is infected beforehand. |

Trong một cuộc tấn công XSS được lưu trữ,mã độc không được ẩn trong liên kết cần được gửi đến máy chủ.Thay vào đó, một cuộc tấn công XSS được lưu trữ là một trường hợpkhi mã độc được đưa trực tiếp vào máy chủ.Ở đây, kẻ tấn công nhắm vào các thành phần của trang web được cung cấp cho người dùng.Điều này có thể là những thứ như hình ảnhvà các nút tải khi trang web được truy cập.Các thành phần bị nhiễm sẽ kích hoạt mã độc khi người dùng truy cập vào trang web.Các cuộc tấn công XSS được lưu trữ có thể gây hại vìngười dùng không có cách nào biết trước được trang web có bị nhiễm hay không.

|  |
| --- |
| Finally there's DOM-based XSS. DOM stands for Document Object Model, which is basically the source code of a website. A DOM-based XSS attack is an instance when malicious script exists in the web page a browser loads. Unlike reflected XSS, these attacks don't need to be sent to the server to activate. |

Cuối cùng là XSS dựa trên DOM. DOM là viết tắt củađối với Mô hình đối tượng tài liệu, về cơ bản là mã nguồn của một trang web.Một cuộc tấn công XSS dựa trên DOM là một trường hợpkhi có tập lệnh độc hại trong trang webtrình duyệt tải. Không giống như XSS phản ánh,những cuộc tấn công này không cần phải được gửi đến máy chủ để kích hoạt.

|  |
| --- |
| In a DOM-based attack, a malicious script can be seen in the URL. In this example, the website's URL contains parameter values. The parameter values reflect input from the user. Here, the site allows users to select color themes. When the user makes a selection, it appears as part of the URL. In a DOM-based attack, criminals change the parameter that's expecting an input. For example, they could hide malicious JavaScript in the HTML tags. The browser would process the HTML and execute the JavaScript. |

Trong cuộc tấn công dựa trên DOM, có thể thấy một tập lệnh độc hại trong URL.Trong ví dụ này, URL của trang web chứa các giá trị tham số.Các giá trị tham số phản ánh thông tin đầu vào từ người dùng.Tại đây, trang web cho phép người dùng chọn chủ đề màu sắc.Khi người dùng thực hiện lựa chọn, lựa chọn đó sẽ xuất hiện như một phần của URL.Trong cuộc tấn công dựa trên DOM, tội phạm sẽ thay đổi tham số đang chờ dữ liệu đầu vào.Ví dụ, họ có thể ẩn mã JavaScript độc hại trong thẻ HTML.Trình duyệt sẽ xử lý HTML và thực thi JavaScript.

|  |
| --- |
| Hackers use these methods of cross-site scripting to steal sensitive information. Security analysts should be familiar with this group of injection attacks. However, they're not the only ones, as we'll discover next time. |

Tin tặc sử dụng các phương pháp tấn công chéo trang này để đánh cắp thông tin nhạy cảm.Các nhà phân tích bảo mật hẳn phải quen thuộc với nhóm tấn công tiêm nhiễm này.Tuy nhiên, chúng không phải là những thứ duy nhất, chúng ta sẽ khám phá ở phần sau.

***3.2. Exploitable gaps in databases - Các lỗ hồng có thể khai thác trong cơ sở dữ liệu***

|  |
| --- |
| Let's keep exploring injection and attacks by investigating another common type of web based exploit. The next one we're going to discuss exploits the way websites access information from databases. Early in the program, you may have learned about SQL. You may recall, SQL is a programming language used to create, interact with, and request information from a database. |

Chúng ta hãy tiếp tục khám phá tiêm vàtấn công bằng cách điều tra một loại khai thác phổ biến khác trên web.Tiếp theo chúng ta sẽ thảo luận về cách khai thác các trang web truy cậpthông tin từ cơ sở dữ liệu.Vào giai đoạn đầu của chương trình, bạn có thể đã học về SQL.Bạn có thể nhớ lại, SQL là một ngôn ngữ lập trình được sử dụng để tạo,tương tác và yêu cầu thông tin từ cơ sở dữ liệu.

|  |
| --- |
| SQL is used by most web applications. For example, shopping websites use it a lot. Imagine the databases of an online clothing store It likely contains a full inventory of all the items the company sells. Websites don't normally make users enter the SQL queries manually. Instead, they use things like menus, images, and buttons to show users information in a meaningful way. For example, when an online shopper clicks a button to add a sweater to their cart, it triggers a SQL query. The query runs in the background where no one can see it. |

SQL được sử dụng bởi hầu hết các ứng dụng web. Ví dụ, các trang web mua sắm sử dụng nó rất nhiều.Hãy tưởng tượng cơ sở dữ liệu của một cửa hàng quần áo trực tuyếnCó khả năng nó chứa toàn bộ hàng tồn kho của tất cả các mặt hàng mà công ty bán.Các trang web thường không yêu cầu người dùng nhập truy vấn SQL theo cách thủ công.Thay vào đó, họ sử dụng những thứ như menu, hình ảnh vàcác nút để hiển thị thông tin cho người dùng theo cách có ý nghĩa.Ví dụ, khi người mua sắm trực tuyến nhấp vào nút để thêm áo len vào giỏ hàng của họ,nó kích hoạt một truy vấn SQL. Truy vấn chạy ở chế độ nền nơi không ai có thể nhìn thấy.

|  |
| --- |
| You'd never know from using the menus and buttons of a website, but sometimes those backend queries are vulnerable to injection attacks. |

Bạn sẽ không bao giờ biết được khi sử dụng các menu và nút của một trang web, nhưngđôi khi những truy vấn phụ trợ này dễ bị tấn công bằng mã độc.

|  |
| --- |
| A SQL injection is an attack that executes unexpected queries on a database. Like cross-site scripting, SQL injection occurs due to a lack of sanitized input. The injections take place in the area of the website that are designed to accept user input. A common example is the login form to access a site. One of these forms might trigger a backend SQL statement like this when a user enters their credentials. Web forms, like this one, are designed to copy user input into the statement exactly as they're written. |

SQL injection là một cuộc tấn công thực hiện các truy vấn không mong muốn trên cơ sở dữ liệu.Giống như tấn công xuyên trang, tấn công SQL xảy ra do thiếu dữ liệu đầu vào đã được khử trùng.Các mũi tiêm được thực hiện tại khu vực của trang web được thiết kế đểchấp nhận thông tin đầu vào của người dùng. Một ví dụ phổ biến là biểu mẫu đăng nhập để truy cập vào một trang web.Một trong những biểu mẫu này có thể kích hoạt một câu lệnh SQL ở phía saunhư thế này khi người dùng nhập thông tin đăng nhập của họ.Các biểu mẫu web, như biểu mẫu này, được thiết kế để sao chép dữ liệu đầu vào của người dùng vào báo cáochính xác như những gì đã viết.

|  |
| --- |
| The statement then sends a request to the server, which runs the query. Websites that are vulnerable to SQL injection insert the user's input exactly as it's entered before running the code. |

Sau đó, câu lệnh sẽ gửi yêu cầu đến máy chủ để chạy truy vấn.Các trang web dễ bị tấn công SQL injection sẽ chèn chính xác dữ liệu đầu vào của người dùngkhi được nhập trước khi chạy mã.

|  |
| --- |
| Unfortunately, this is a serious design flaw. It commonly happens because web developers expect people to use these inputs correctly. They don't anticipate attackers exploiting them. For example, an attacker might insert additional SQL code. This could cause the server to run a harmful query of code that it wasn't expecting. Malicious hackers can target these attack vectors to obtain sensitive information, modify tables and even gain administrative rights to the database. |

Thật không may, đây là một lỗi thiết kế nghiêm trọng.Điều này thường xảy ra vì các nhà phát triển web mong đợi mọi người sử dụng các đầu vào nàymột cách chính xác.Họ không lường trước được những kẻ tấn công sẽ lợi dụng họ. Ví dụ,kẻ tấn công có thể chèn thêm mã SQL.Điều này có thể khiến máy chủ chạy một truy vấn mã có hại mà nó không phảimong đợi.Những tin tặc độc hại có thể nhắm vào các vectơ tấn công này để lấy thông tin nhạy cảm,sửa đổi bảng và thậm chí giành được quyền quản trị cơ sở dữ liệu.

|  |
| --- |
| The best way to defend against SQL injection is code that will sanitize the input. Developers can write code to search for specific SQL characters. This gives the server a clearer idea of what inputs to expect. One way this is done is with prepared statements. |

Cách tốt nhất để chống lại SQL injection là mã sẽ khử trùngđầu vào.Các nhà phát triển có thể viết mã để tìm kiếm các ký tự SQL cụ thể.Điều này giúp máy chủ hiểu rõ hơn về những dữ liệu đầu vào cần mong đợi.Một cách để thực hiện điều này là sử dụng các câu lệnh đã chuẩn bị sẵn.

|  |
| --- |
| A prepared statement is a coding technique that executes SQL statements before passing them on to the database. When the user's input is unknown, the best practice is to use these prepared statements. With just a few extra lines of code, a prepared statement executes the code before passing it on to the server. This means the code can be validated before performing the query. |

Một câu lệnh đã chuẩn bị là một kỹ thuật mã hóa thực thiCác câu lệnh SQL trước khi chuyển chúng vào cơ sở dữ liệu.Khi đầu vào của người dùng không xác định,cách tốt nhất là sử dụng những câu lệnh đã chuẩn bị sẵn này.Chỉ với một vài dòng mã bổ sung,một câu lệnh đã chuẩn bị sẽ thực thi mã trước khi chuyển nó tới máy chủ.Điều này có nghĩa là mã có thể được xác thực trước khi thực hiện truy vấn.

|  |
| --- |
| Having well written code is one of the keys to preventing SQL injection. |

Viết code tốt là một trong những chìa khóa để ngăn chặn tấn công SQL injection.

|  |
| --- |
| Security teams work with program developers to test applications for these sort of vulnerabilities. Like a lot of security tasks, it's a team effort. Injection attacks are just one of many types of web-based exploits that security teams deal with. We're going to explore how security teams prepare for injection attacks and other kinds of threats. |

Các nhóm bảo mật làm việc với các nhà phát triển chương trình để kiểm tra các ứng dụngnhững loại lỗ hổng này.Giống như nhiều nhiệm vụ bảo mật khác, đây là nỗ lực của cả nhóm.Các cuộc tấn công tiêm mã chỉ là một trong nhiều loại khai thác dựa trên web mà bảo mậtcác đội phải giải quyết.Chúng ta sẽ khám phá cách các nhóm bảo mật chuẩn bị cho các cuộc tấn công tiêm nhiễm vàcác loại đe dọa khác.

***3.3. Prevent injection attacks - Ngăn chặn các cuộc tấn công tiêm***

|  |
| --- |
| **Prevent injection attacks** |

**Ngăn chặn các cuộc tấn công tiêm**

|  |
| --- |
| Previously, you learned that **Structured Query Language** (SQL) is a programming language used to create, interact with, and request information from a database. SQL is one of the most common programming languages used to interact with databases because it is widely supported by a range of database products. |

Trước đó, bạn đã học rằng **Ngôn ngữ truy vấn có cấu trúc** (SQL) là ngôn ngữ lập trình được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu. SQL là một trong những ngôn ngữ lập trình phổ biến nhất được sử dụng để tương tác với cơ sở dữ liệu vì nó được hỗ trợ rộng rãi bởi nhiều sản phẩm cơ sở dữ liệu.

|  |
| --- |
| As you might recall, malicious **SQL injection** is a type of attack that executes unexpected queries on a database. Threat actors perform SQL injections to modify, delete, or steal information from databases. A SQL injection is a common attack vector that is used to gain unauthorized access to web applications. Due to the language's popularity with developers, SQL injections are regularly listed in the OWASP® Top 10 because developers tend to focus on making their applications work correctly rather than protecting their products from injection. |

Như bạn có thể nhớ lại, **SQL injection** độc hại là một loại tấn công thực hiện các truy vấn không mong muốn trên cơ sở dữ liệu. Các tác nhân đe dọa thực hiện SQL injection để sửa đổi, xóa hoặc đánh cắp thông tin từ cơ sở dữ liệu. SQL injection là một vectơ tấn công phổ biến được sử dụng để có được quyền truy cập trái phép vào các ứng dụng web. Do ngôn ngữ này phổ biến với các nhà phát triển, SQL injection thường được liệt kê trong OWASP® Top 10 vì các nhà phát triển có xu hướng tập trung vào việc làm cho các ứng dụng của họ hoạt động chính xác hơn là bảo vệ sản phẩm của họ khỏi bị tiêm.

|  |
| --- |
| In this reading, you'll learn about SQL queries and how they are used to request information from a database. You will also learn about the three classes of SQL injection attacks used to manipulate vulnerable queries. You will also learn ways to identify when websites are vulnerable and ways to address those gaps. |

Trong bài đọc này, bạn sẽ tìm hiểu về các truy vấn SQL và cách chúng được sử dụng để yêu cầu thông tin từ cơ sở dữ liệu. Bạn cũng sẽ tìm hiểu về ba lớp tấn công SQL injection được sử dụng để thao túng các truy vấn dễ bị tấn công. Bạn cũng sẽ tìm hiểu các cách xác định khi nào các trang web dễ bị tấn công và cách giải quyết các lỗ hổng đó.

|  |
| --- |
| **SQL queries** |

**Truy vấn SQL**

|  |
| --- |
| Every bit of information that’s accessed online is stored in a database. A **database** is an organized collection of information or data in one place. A database can include data such as an organization's employee directory or customer payment methods. In SQL, database information is organized in tables. SQL is commonly used for retrieving, inserting, updating, or deleting information in tables using queries. |

Mọi bit thông tin được truy cập trực tuyến đều được lưu trữ trong cơ sở dữ liệu. **Cơ sở dữ liệu** là tập hợp thông tin hoặc dữ liệu được tổ chức tại một nơi. Cơ sở dữ liệu có thể bao gồm dữ liệu như danh bạ nhân viên của tổ chức hoặc phương thức thanh toán của khách hàng. Trong SQL, thông tin cơ sở dữ liệu được tổ chức trong các bảng. SQL thường được sử dụng để truy xuất, chèn, cập nhật hoặc xóa thông tin trong các bảng bằng truy vấn.

|  |
| --- |
| A *SQL query* is a request for data from a database. For example, a SQL query can request data from an organization's employee directory such as employee IDs, names, and job titles. A human resources application can accept an input that queries a SQL table to filter the data and locate a specific person. SQL injections can occur anywhere within a vulnerable application that can accept a SQL query. |

*Truy vấn SQL* là yêu cầu dữ liệu từ cơ sở dữ liệu. Ví dụ, truy vấn SQL có thể yêu cầu dữ liệu từ danh bạ nhân viên của tổ chức như ID nhân viên, tên và chức danh công việc. Ứng dụng nguồn nhân lực có thể chấp nhận đầu vào truy vấn bảng SQL để lọc dữ liệu và định vị một người cụ thể. SQL injection có thể xảy ra ở bất kỳ đâu trong ứng dụng dễ bị tấn công có thể chấp nhận truy vấn SQL.

|  |
| --- |
| Queries are usually initiated in places where users can input information into an application or a website via an input field. Input fields include features that accept text input such as login forms, search bars, or comment submission boxes. A SQL injection occurs when an attacker exploits input fields that aren't programmed to filter out unwanted text. SQL injections can be used to manipulate databases, steal sensitive data, or even take control of vulnerable applications. |

Truy vấn thường được khởi tạo ở những nơi mà người dùng có thể nhập thông tin vào ứng dụng hoặc trang web thông qua trường nhập. Trường nhập bao gồm các tính năng chấp nhận nhập văn bản như biểu mẫu đăng nhập, thanh tìm kiếm hoặc hộp gửi bình luận. SQL injection xảy ra khi kẻ tấn công khai thác các trường nhập không được lập trình để lọc văn bản không mong muốn. SQL injection có thể được sử dụng để thao túng cơ sở dữ liệu, đánh cắp dữ liệu nhạy cảm hoặc thậm chí kiểm soát các ứng dụng dễ bị tấn công.

|  |
| --- |
| **SQL injection categories** |

**Các loại tiêm SQL**

|  |
| --- |
| There are three main categories of SQL injection:   * In-band * Out-of-band * Inferential |

Có ba loại chính của SQL injection:

* Trong băng tần
* Ngoài băng tần
* Suy luận

|  |
| --- |
| In the following sections, you'll learn that each type describes how a SQL injection is initiated and how it returns the results of the attack. |

Trong các phần sau, bạn sẽ tìm hiểu về từng loại mô tả cách khởi tạo tấn công SQL và cách trả về kết quả của cuộc tấn công.

|  |
| --- |
| **In-band SQL injection** |

**Tiêm SQL trong băng tần**

|  |
| --- |
| In-band, or classic, SQL injection is the most common type. An in-band injection is one that uses the *same communication channel* to launch the attack and gather the results. |

In-band, hay còn gọi là SQL injection cổ điển, là loại phổ biến nhất. In-band injection là loại sử dụng *cùng một kênh truyền thông* để khởi chạy cuộc tấn công và thu thập kết quả.

|  |
| --- |
| For example, this might occur in the search box of a retailer's website that lets customers find products to buy. If the search box is vulnerable to injection, an attacker could enter a malicious query that would be executed in the database, causing it to return sensitive information like user passwords. The data that's returned is displayed back in the search box where the attack was initiated. |

Ví dụ, điều này có thể xảy ra trong hộp tìm kiếm của trang web của nhà bán lẻ cho phép khách hàng tìm sản phẩm để mua. Nếu hộp tìm kiếm dễ bị tấn công, kẻ tấn công có thể nhập truy vấn độc hại sẽ được thực thi trong cơ sở dữ liệu, khiến nó trả về thông tin nhạy cảm như mật khẩu người dùng. Dữ liệu được trả về sẽ được hiển thị trở lại trong hộp tìm kiếm nơi cuộc tấn công bắt đầu.

|  |
| --- |
| **Out-of-band SQL injection** |

**Tiêm SQL ngoài băng tần**

|  |
| --- |
| An out-of-band injection is one that uses a *different communication channel*  to launch the attack and gather the results. |

Tấn công ngoài băng tần là tấn công sử dụng *kênh truyền thông khác*  để phát động cuộc tấn công và thu thập kết quả.

|  |
| --- |
| For example, an attacker could use a malicious query to create a connection between a vulnerable website and a database they control. This separate channel would allow them to bypass any security controls that are in place on the website's server, allowing them to steal sensitive data |

Ví dụ, kẻ tấn công có thể sử dụng truy vấn độc hại để tạo kết nối giữa một trang web dễ bị tấn công và cơ sở dữ liệu mà chúng kiểm soát. Kênh riêng biệt này sẽ cho phép chúng bỏ qua mọi biện pháp kiểm soát bảo mật có trên máy chủ của trang web, cho phép chúng đánh cắp dữ liệu nhạy cảm

|  |
| --- |
| **Note:** Out-of-band injection attacks are very uncommon because they'll only work when certain features are enabled on the target server. |

**Lưu ý:** Các cuộc tấn công tiêm mã độc ngoài băng thông rất hiếm khi xảy ra vì chúng chỉ có tác dụng khi một số tính năng nhất định được bật trên máy chủ mục tiêu.

|  |
| --- |
| **Inferential SQL injection** |

**Tiêm SQL suy luận**

|  |
| --- |
| Inferential SQL injection occurs when an attacker is unable to directly see the results of their attack. Instead, they can interpret the results by analyzing the *behavior* of the system. |

Tiêm SQL suy luận xảy ra khi kẻ tấn công không thể trực tiếp nhìn thấy kết quả của cuộc tấn công. Thay vào đó, chúng có thể diễn giải kết quả bằng cách phân tích *hành vi* của hệ thống.

|  |
| --- |
| For example, an attacker might perform a SQL injection attack on the login form of a website that causes the system to respond with an error message. Although sensitive data is not returned, the attacker can figure out the database's structure based on the error. They can then use this information to craft attacks that will give them access to sensitive data or to take control of the system. |

Ví dụ, kẻ tấn công có thể thực hiện một cuộc tấn công SQL injection vào biểu mẫu đăng nhập của một trang web khiến hệ thống phản hồi bằng một thông báo lỗi. Mặc dù dữ liệu nhạy cảm không được trả về, kẻ tấn công có thể tìm ra cấu trúc của cơ sở dữ liệu dựa trên lỗi. Sau đó, chúng có thể sử dụng thông tin này để tạo ra các cuộc tấn công cho phép chúng truy cập vào dữ liệu nhạy cảm hoặc kiểm soát hệ thống.

|  |
| --- |
| **Injection Prevention** |

**Phòng ngừa tiêm chích**

|  |
| --- |
| SQL queries are often programmed with the assumption that users will only input relevant information. For example, a login form that expects users to input their email address assumes the input will be formatted a certain way, such as *jdoe@domain.com*. Unfortunately, this isn’t always the case. |

Các truy vấn SQL thường được lập trình với giả định rằng người dùng sẽ chỉ nhập thông tin có liên quan. Ví dụ, một biểu mẫu đăng nhập yêu cầu người dùng nhập địa chỉ email của họ sẽ giả định rằng thông tin đầu vào sẽ được định dạng theo một cách nhất định, chẳng hạn như *jdoe@domain.com* . Thật không may, điều này không phải lúc nào cũng đúng.

|  |
| --- |
| A key to preventing SQL injection attacks is to *escape* *user inputs*—preventing someone from inserting any code that a program isn't expecting. |

Chìa khóa để ngăn chặn các cuộc tấn công tiêm SQL là *tránh các dữ liệu đầu vào của người dùng* —ngăn chặn ai đó chèn bất kỳ mã nào mà chương trình không mong đợi.

|  |
| --- |
| There are several ways to escape user inputs:   * **Prepared statements**: a coding technique that executes SQL statements before passing them on to a database * **Input sanitization**: programming that removes user input which could be interpreted as code. * **Input validation**: programming that ensures user input meets a system's expectations. |

Có một số cách để thoát khỏi dữ liệu đầu vào của người dùng:

* **Các câu lệnh đã chuẩn bị** : một kỹ thuật mã hóa thực thi các câu lệnh SQL trước khi chuyển chúng vào cơ sở dữ liệu
* **Khử trùng đầu vào** : lập trình loại bỏ dữ liệu đầu vào của người dùng có thể được hiểu là mã.
* **Xác thực đầu vào** : lập trình đảm bảo dữ liệu đầu vào của người dùng đáp ứng được kỳ vọng của hệ thống.

|  |
| --- |
| Using a combination of these techniques can help prevent SQL injection attacks. In the security field, you might need to work closely with application developers to address vulnerabilities that can lead to SQL injections. [OWASP's SQL injection detection techniques](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection) is a useful resource if you're interested in investigating SQL injection vulnerabilities on your own. |

Sử dụng kết hợp các kỹ thuật này có thể giúp ngăn chặn các cuộc tấn công SQL injection. Trong lĩnh vực bảo mật, bạn có thể cần phải làm việc chặt chẽ với các nhà phát triển ứng dụng để giải quyết các lỗ hổng có thể dẫn đến SQL injection.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Many web applications retrieve data from databases using SQL, and injection attacks are quite common due to the popularity of the language. As is the case with other kinds of injection attacks, SQL injections are a result of unexpected user input. It's important to collaborate with app developers to help prevent these kinds of attacks by sharing your understanding of SQL injection techniques and the defenses that should be put in place. |

Nhiều ứng dụng web lấy dữ liệu từ cơ sở dữ liệu bằng SQL và các cuộc tấn công tiêm mã khá phổ biến do tính phổ biến của ngôn ngữ này. Giống như các loại tấn công tiêm mã khác, tiêm mã SQL là kết quả của dữ liệu đầu vào bất ngờ của người dùng. Điều quan trọng là phải hợp tác với các nhà phát triển ứng dụng để giúp ngăn chặn các loại tấn công này bằng cách chia sẻ hiểu biết của bạn về các kỹ thuật tiêm mã SQL và các biện pháp phòng thủ cần áp dụng.

***3.4. The upward trend of cyber crime - Xu hướng gia tăng của tội phạm mạng***

***3.5. Test your knowledge: Web-based exploits - Kiểm tra kiến thức của bạn: Khai thác dựa trên web***

**4. Threat modeling – Mô hình hóa môi đe dọa**

***4.1. A proactive approach to security - Một cách tiếp cận chủ động đối với an ninh***

|  |
| --- |
| Preparing for attacks is an important job that the entire security team is responsible for. Threat actors have many tools they can use depending on their target. For example, attacking a small business can be different from attacking a public utility. Each have different assets and specific defenses to keep them safe. In all cases, anticipating attacks is the key to preparing for them. In security, we do that by performing an activity known as threat modeling. |

Chuẩn bị chotấn công là công việc quan trọng mà toàn bộ nhóm an ninh phải chịu trách nhiệm.Kẻ tấn công có nhiều công cụ có thể sử dụng tùy thuộc vào mục tiêu của chúng.Ví dụ,tấn công một doanh nghiệp nhỏ có thể khác với tấn công một công ty tiện ích công cộng.Mỗi loại đều có tài sản khác nhau và biện pháp phòng thủ cụ thể để giữ an toàn.Trong mọi trường hợp, việc dự đoán các cuộc tấn công chính là chìa khóa để chuẩn bị ứng phó.Trong bảo mật, chúng tôi thực hiện điều đó bằng cách thực hiện một hoạt động được gọi là mô hình hóa mối đe dọa.

|  |
| --- |
| Threat modeling is a process of identifying assets, their vulnerabilities, and how each is exposed to threats. We apply threat modeling to everything we protect. Entire systems, applications, or business processes all get examined from this security-related perspective. |

Mô hình hóa mối đe dọa là một quá trình xác định tài sản,điểm yếu của họ và cách mỗi người tiếp xúc với các mối đe dọa.Chúng tôi áp dụng mô hình đe dọa vào mọi thứchúng tôi bảo vệ. Toàn bộ hệ thống, ứng dụng hoặc quy trình kinh doanhtất cả đều được xem xét từ góc độ liên quan đến bảo mật.

|  |
| --- |
| Creating threat models is a lengthy and detailed activity. They're normally performed by a collection of individuals with years of experience in the field. Because of that, it's considered to be an advanced skill in security. However, that doesn't mean you won't be involved. |

Việc tạo ra các mô hình mối đe dọa là một hoạt động dài và chi tiết.Chúng thường được thực hiện bởi một nhóm cá nhân có nhiều năm kinh nghiệm trongcánh đồng.Vì thế, nó được coi là một kỹ năng nâng cao trong lĩnh vực bảo mật.Tuy nhiên, điều đó không có nghĩa là bạn sẽ không tham gia.

|  |
| --- |
| There are several threat modeling frameworks used in the field. Some are better suited for network security. Others are better for things like information security, or application development. |

Có một số khuôn khổ mô hình hóa mối đe dọa được sử dụng trong lĩnh vực này.Một số phù hợp hơn cho bảo mật mạng. Những cái khác phù hợp hơn chonhững thứ như bảo mật thông tin hoặc phát triển ứng dụng.

|  |
| --- |
| In general, there are six steps of a threat model. The first is to define the scope of the model. At this stage, the team determines what they're building by creating an inventory of assets and classifying them. |

Nhìn chung, mô hình mối đe dọa có sáu bước.Đầu tiên là xác định phạm vi của mô hình.Ở giai đoạn này, nhóm xác định những gì họ đang xây dựng bằng cách tạo rakiểm kê tài sản và phân loại chúng.

|  |
| --- |
| The second step is to identify threats. Here, the team defines all potential threat actors. A threat actor is any person or group who presents a security risk. Threat actors are characterized as being internal or external. For example, an internal threat actor could be an employee who intentionally expose an asset to harm. An example of an external threat actor could be a malicious hacker, or a competing business. |

Bước thứ hai là xác định mối đe dọa.Tại đây, nhóm sẽ xác định tất cả các tác nhân đe dọa tiềm ẩn.Tác nhân đe dọa là bất kỳ cá nhân hoặc nhóm người nào có nguy cơ gây ra rủi ro về an ninh.Tác nhân đe dọa được phân loại thành tác nhân bên trong hoặc bên ngoài.Ví dụ, một tác nhân đe dọa nội bộ có thể là một nhân viênngười cố ý làm tổn hại đến tài sản.Một ví dụ về tác nhân đe dọa bên ngoài có thể là một tin tặc độc hại hoặcmột doanh nghiệp cạnh tranh.

|  |
| --- |
| After threat actors have been identified, the team puts together what's known as an attack tree. An attack tree is a diagram that maps threats to assets. The team tries to be as detailed as possible when constructing this diagram before moving on. |

Sau khi các tác nhân đe dọa đã được xác định,nhóm đã xây dựng nên cái gọi là cây tấn công.Cây tấn công là sơ đồ lập bản đồ các mối đe dọa đối với tài sản.Nhóm cố gắng chi tiết nhất có thể khi xây dựngsơ đồ này trước khi tiếp tục.

|  |
| --- |
| Step three of the threat modeling process is to characterize the environment. Here, the team applies an attacker mindset to the business. They consider how the customers and employees interact with the environment. Other factors they consider are external partners and third party vendors. |

Bước thứ ba của quá trình lập mô hình mối đe dọa là mô tả môi trường.Ở đây, nhóm áp dụng tư duy của kẻ tấn công vào doanh nghiệp.Họ xem xét cách khách hàng và nhân viên tương tác với môi trường.Những yếu tố khác mà họ cân nhắc là các đối tác bên ngoài và nhà cung cấp bên thứ ba.

|  |
| --- |
| At step four, their objective is to analyze threats. Here, the team works together to examine existing protections and identify gaps. They then rank threats according to their risk score that they assign. |

Ở bước thứ tư, mục tiêu của họ là phân tích các mối đe dọa.Tại đây, nhóm sẽ cùng nhau kiểm tra các biện pháp bảo vệ hiện có và xác định những lỗ hổng.Sau đó, họ xếp hạng các mối đe dọa theo điểm rủi ro mà họ chỉ định.

|  |
| --- |
| During step five, the team decides how to mitigate risk. At this point, the group creates their plan for defending against threats. The choices here are to avoid risk, transfer it, reduce it, or accept it. |

Ở bước thứ năm, nhóm sẽ quyết định cách giảm thiểu rủi ro.Vào thời điểm này, nhóm sẽ lập kế hoạch phòng thủ chống lại các mối đe dọa.Các lựa chọn ở đây là tránh rủi ro, chuyển giao, giảm thiểu hoặc chấp nhận rủi ro.

|  |
| --- |
| The sixth and final step is to evaluate findings. At this stage, everything that was done during the exercise is documented, fixes are applied, and the team makes note of any successes they had. They also record any lessons learned, so they can inform how they approach future threat models. |

Bước thứ sáu và cũng là bước cuối cùng là đánh giá những phát hiện.Ở giai đoạn này, mọi thứ đã được thực hiện trong quá trình thực hiện đều được ghi lại.các bản sửa lỗi được áp dụng và nhóm sẽ ghi nhận mọi thành công mà họ đạt được.Họ cũng ghi lại bất kỳ bài học kinh nghiệm nào, vì vậyhọ có thể thông báo cách tiếp cận các mô hình mối đe dọa trong tương lai.

|  |
| --- |
| That's an overview of the general threat modeling process. What we've explored was just one of many methods that exist. |

Đó là tổng quan về quy trình lập mô hình mối đe dọa chung.Những gì chúng tôi khám phá chỉ là một trong nhiều phương pháp hiện có.

***4.2. Identify: Steps of the threat model process - Xác định: Các bước của quy trình mô hình mối đe dọa***

|  |
| --- |
| **Identify: Steps of the threat model process** |

|  |  |
| --- | --- |
| Step 1: | Define the scope |
| Step 2: | Identify threats |
| Step 3: | Characterize the environment |
| Step 4: | Analyze threats |
| Step 5: | Mitigate risks |
| Step 6: | Evaluate findings |

|  |  |
| --- | --- |
| Step 1: | Xác định phạm vi |
| Step 2: | Xác định các mối đe dọa |
| Step 3: | Nêu đặc điểm môi trường |
| Step 4: | Phân tích các mối đe dọa |
| Step 5: | Giảm thiểu rủi ro |
| Step 6: | Đánh giá kết quả |

***4.3. Chantelle: The value of diversity in cybersecurity - Chantelle: Giá trị của sự đa dạng trong an ninh mạng***

|  |
| --- |
| My name is Chantelle. I'm a Security Engineer here at Google, and I am part of the security and implement, and scaling team. We secure and monitor systems that contain sensitive information. My background, initially I was going to be a heart surgeon and then I took chemistry, I took chem 1, and I was like, no that's not happening. My interest in cybersecurity came from a TV show called Mr. Robot. It's about a vigilante hacker trying to save the world. And from there, that kind of piqued my interest in security, and so that's a great foundation. Valuing diversity in security is important because we're exposed to a broad range of thinking. That helps to inspire a lot of creative ideas and different perspectives and different ways of tackling a problem and that kind of leads us forward into being better security engineers. Our Manager, Laureen always steps in to tell us, "Don't be so quick to find a solution. Don't be so quick to solve the problems yourselves." We have a wide range of security engineers and connections to our disposal, and she encourages us to go out and seek them out, and then to come back and then have us settle in and brainstorm all of these ideas that we've collected after we've went out and tried to find it. We've ultimately almost always come up with the best possible outcome that we can ever come up with. My advice for people to get into the industry is get out there and be proactive. I definitely recommend joining up the security community on Twitter. There's a huge security community on Twitter right now. That shares a bunch of resources, opportunities, job positions, and are definitely open to talking to anyone that's interested in getting into the field but just don't know how. I recommend security as a career. Definitely, I think that for me personally, I was able to tap into my rebel side a lot in security. I found I was able to express myself a bit more in security. It's just a whole ball of goodness. |

Tên tôi là Chantelle.Tôi là Kỹ sư an ninh tại Google,và tôi là một phần củanhóm bảo mật, triển khai và mở rộng quy mô.Chúng tôi bảo mật và giám sáthệ thống chứa thông tin nhạy cảm.Bối cảnh của tôi, ban đầu tôi địnhlà một bác sĩ phẫu thuật tim và sau đó tôi học hóa học,Tôi đã học môn Hóa 1 và tôi nghĩ rằng,Không, điều đó không xảy ra.Sự quan tâm của tôi đến an ninh mạngxuất phát từ một chương trình truyền hình có tên là Mr.Robot. Nó nói về một hacker cảnh giáccố gắng cứu thế giới.Và từ đó, điều đó đã khơi dậy sự quan tâm của tôi đối với vấn đề an ninh,và đó là một nền tảng tuyệt vời.Đánh giá cao sự đa dạng trong an ninh là điều quan trọngvì chúng ta được tiếp xúc với nhiều luồng suy nghĩ khác nhau.Điều đó giúp truyền cảm hứng cho rất nhiều ý tưởng sáng tạo vànhững góc nhìn khác nhau và những cách khác nhaucủa việc giải quyết một vấn đề vàđiều đó dẫn chúng ta tiến về phía trướcđể trở thành kỹ sư an ninh giỏi hơn.Người quản lý của chúng tôi, Laureen luôn bước vào để nói với chúng tôi,"Đừng vội tìm ra giải pháp.Đừng vội vàng tự mình giải quyết vấn đề."Chúng tôi có nhiều loạikỹ sư an ninh và các kết nối theo ý của chúng tôi,và cô ấy khuyến khích chúng ta đi ra ngoài và tìm kiếm chúng,và sau đó quay lại và sau đó để chúng tôi ổn định vàhãy động não tất cả những ý tưởng mà chúng ta đã cóđược thu thập sau khi chúng tôi ra ngoài và cố gắng tìm kiếm nó.Cuối cùng chúng tôi hầu như luôn luôn xuất hiệnvới kết quả tốt nhất có thểmà chúng ta có thể nghĩ ra.Lời khuyên của tôi cho mọi người để có được vàongành công nghiệp này phải đi ra ngoài và chủ động.Tôi chắc chắn khuyên bạn nên tham gianâng cao cộng đồng bảo mật trên Twitter.Hiện nay có một cộng đồng bảo mật rất lớn trên Twitter.Chia sẻ một loạt các tài nguyên,cơ hội, vị trí công việc,và chắc chắn là sẵn sàng nói chuyện vớibất kỳ ai quan tâm đến việc tham gia vào lĩnh vực nàynhưng không biết làm thế nào. Tôi khuyên bạn nên theo đuổi nghề an ninh.Chắc chắn, tôi nghĩ rằng đối với cá nhân tôi,Tôi có thể khai thác bản tính nổi loạn của mình rất nhiều trong công tác an ninh.Tôi thấy mình có thể diễn đạtbản thân tôi an toàn hơn một chút.Nó chỉ là một quả bóng đầy sự tốt lành.

***4.4. PASTA: The Process for Attack Simulation and Threat Analysis - PASTA: Quy trình mô phỏng tấn công và phân tích mối đe dọa***

|  |
| --- |
| Let's finish exploring threat modeling by taking a look at real-world scenarios. This time, we'll use a standard threat modeling process called PASTA. |

Chúng ta hãy kết thúc việc khám phá mô hình mối đe dọa bằng cách xem xét các tình huống thực tế.Lần này, chúng ta sẽ sử dụng quy trình mô hình hóa mối đe dọa tiêu chuẩn có tên là PASTA.

|  |
| --- |
| Imagine that a fitness company is getting ready to launch their first mobile app. Before we can go live, the company asks their security team to ensure the app will protect customer data. The team decides to perform a threat model using the PASTA framework. |

Hãy tưởng tượng rằng một công ty thể hình đang chuẩn bị ra mắt ứng dụng di động đầu tiên của họ.Trước khi chúng ta có thể phát trực tiếp,công ty yêu cầu nhóm bảo mật của mình đảm bảo ứng dụng sẽ bảo vệ dữ liệu khách hàng.Nhóm quyết định thực hiện mô hình mối đe dọa bằng cách sử dụng khuôn khổ PASTA.

|  |
| --- |
| PASTA is a popular threat modeling framework that's used across many industries. PASTA is short for Process for Attack Simulation and Threat Analysis. There are seven stages of the PASTA framework. Let's go through each of them to help this fitness company get their app ready. |

PASTA là một khuôn khổ mô hình hóa mối đe dọa phổ biến được sử dụng trên nhiềucác ngành công nghiệp.PASTA là viết tắt của Quy trình mô phỏng tấn công và phân tích mối đe dọa.Khung PASTA có bảy giai đoạn.Chúng ta hãy cùng xem xét từng mục để giúp công ty thể hình này chuẩn bị ứng dụng của họ.

|  |
| --- |
| Stage one of the PASTA threat model framework is to define business and security objectives. Before starting the threat model, the team needs to decide what their goals are. The main objective in our example with the fitness company app is protecting customer data. The team starts by asking a lot of questions at this stage. They'll need to understand things like how personally identifiable information is handled. Answering these questions is a key to evaluate the impact of threats that they'll find along the way. |

Giai đoạn một của khuôn khổ mô hình mối đe dọa PASTA là xác định doanh nghiệp vàmục tiêu an ninh.Trước khi bắt đầu mô hình mối đe dọa, nhóm cần quyết định mục tiêu của họ là gì.Mục tiêu chính trong ví dụ của chúng tôi với ứng dụng công ty thể hình làbảo vệ dữ liệu khách hàng.Nhóm bắt đầu bằng cách đặt ra rất nhiều câu hỏi ở giai đoạn này.Họ sẽ cần phải hiểu những điều như thế nào về mặt cá nhânthông tin có thể nhận dạng được được xử lý.Trả lời những câu hỏi này là chìa khóa để đánh giá tác độngcủa những mối đe dọa mà họ sẽ gặp phải trên đường đi.

|  |
| --- |
| Stage two of the PASTA framework is to define the technical scope. Here, the team's focus is to identify the application components that must be evaluated. This is what we discussed earlier as the attack surface. For a mobile app, this will include technology that's involved while data is at rest and in use. This includes network protocols, security controls, and other data interactions. |

Giai đoạn thứ hai của khuôn khổ PASTA là xác định phạm vi kỹ thuật.Ở đây, trọng tâm của nhóm là xác định các thành phần ứng dụng phải cóđược đánh giá.Đây chính là điều chúng ta đã thảo luận trước đó về bề mặt tấn công.Đối với ứng dụng di động,điều này sẽ bao gồm công nghệ liên quan khi dữ liệu đang ở trạng thái nghỉ và đang được sử dụng.Điều này bao gồm các giao thức mạng, kiểm soát bảo mật và các tương tác dữ liệu khác.

|  |
| --- |
| At stage three of PASTA, the team's job is to decompose the application. In other words, we need to identify the existing controls that will protect user data from threats. This normally means working with the application developers to produce a data flow diagram. A diagram like this will show how data gets from a user's device to the company's database. It would also identify the controls in place to protect this data along the way. |

Ở giai đoạn ba của PASTA, nhiệm vụ của nhóm là phân tích ứng dụng.Nói cách khác,chúng ta cần xác định các biện pháp kiểm soát hiện có để bảo vệ dữ liệu người dùng khỏi các mối đe dọa.Điều này thường có nghĩa là làm việc với các nhà phát triển ứng dụng để tạo ra dữ liệusơ đồ dòng chảy.Một sơ đồ như thế này sẽ cho thấy dữ liệu được truyền từ thiết bị của người dùng đến công ty như thế nàocơ sở dữ liệu.Nó cũng sẽ xác định các biện pháp kiểm soát được áp dụng để bảo vệ dữ liệu này trong suốt quá trình.

|  |
| --- |
| Stage four of PASTA is next. The focus here is to perform a threat analysis. This is where the team gets into their attacker mindset. Here, research is done to collect the most up-to-date information on the type of attacks being used. Like other technologies, mobile apps have many attack vectors. These change regularly, so the team would reference resources to stay up-to-date. |

Tiếp theo là giai đoạn thứ tư của PASTA.Trọng tâm ở đây là thực hiện phân tích mối đe dọa.Đây là lúc đội bóng bước vào tư duy tấn công.Ở đây, nghiên cứu được thực hiện để thu thập thông tin mới nhất về loạicác cuộc tấn công đang được sử dụng.Giống như các công nghệ khác, ứng dụng di động có nhiều phương thức tấn công.Những thông tin này thay đổi thường xuyên nên nhóm sẽ tham khảo tài nguyên để cập nhật thông tin.

|  |
| --- |
| Stage five of PASTA is performing a vulnerability analysis. In this stage, the team more deeply investigates potential vulnerabilities by considering the root of the problem. |

Giai đoạn năm của PASTA là thực hiện phân tích lỗ hổng.Trong giai đoạn này, nhóm nghiên cứu sẽ điều tra sâu hơncác lỗ hổng tiềm ẩn bằng cách xem xét gốc rễ của vấn đề.

|  |
| --- |
| Next is stage six of PASTA, where the team conducts attack modeling. This is where the team tests the vulnerabilities that were analyzed in stage five by simulating attacks. The team does this by creating an attack tree, which looks like a flow chart. For example, an attack tree for our mobile app might look like this. Customer information, like user names and passwords, is a target. This data is normally stored in a database. We've learned that databases are vulnerable to attacks like SQL injection. So we will add this attack vector to our attack tree. A threat actor might exploit vulnerabilities caused by unsanitized inputs to attack this vector. The security team uses attack trees like this to identify attack vectors that need to be tested to validate threats. This is just one branch of this attack tree. An application, like a fitness app, typically has lots of branches with a number of other attack vectors. |

Tiếp theo là giai đoạn thứ sáu của PASTA, nơi nhóm thực hiện mô hình tấn công.Đây là nơi nhóm kiểm tra các lỗ hổng đã được phân tíchở giai đoạn năm bằng cách mô phỏng các cuộc tấn công.Nhóm thực hiện điều này bằng cách tạo ra một cây tấn công trông giống như sơ đồ luồng.Ví dụ, sơ đồ tấn công cho ứng dụng di động của chúng tôi có thể trông như thế này.Thông tin khách hàng, như tên người dùng và mật khẩu, là mục tiêu.Dữ liệu này thường được lưu trữ trong cơ sở dữ liệu.Chúng ta đã biết rằng cơ sở dữ liệu dễ bị tấn công bằng các cuộc tấn công như SQL injection.Vì vậy, chúng ta sẽ thêm vector tấn công này vào cây tấn công của mình.Một tác nhân đe dọa có thể khai thác các lỗ hổng do không được khử trùngđầu vào để tấn công vào vector này.Nhóm bảo mật sử dụng các cây tấn công như thế này để xác định các vectơ tấn côngcần phải được thử nghiệm để xác thực các mối đe dọa.Đây chỉ là một nhánh của phương pháp tấn công này.Một ứng dụng, như ứng dụng thể dục, thường có nhiều nhánh vớimột số phương thức tấn công khác.

|  |
| --- |
| Stage seven of PASTA is to analyze risk and impact. Here, the team assembles all the information they've collected in stages one through six. By this stage, the team is in position to make informed risk management recommendations to business stakeholders that align with their goals. |

Giai đoạn thứ bảy của PASTA là phân tích rủi ro và tác động.Ở đây, nhóm tập hợp tất cả thông tin họ đã thu thập được tronggiai đoạn một đến giai đoạn sáu.Đến giai đoạn này, nhóm đã ở vị trí có thể đưa ra quyết định rủi ro sáng suốtđưa ra các khuyến nghị của ban quản lý cho các bên liên quan trong doanh nghiệp phù hợp với mục tiêu của họ.

|  |
| --- |
| And with that, we made it all the way through a threat modeling exercise based on the PASTA framework! |

Và với điều đó, chúng tôi đã thực hiện được tất cả các bước trong bài tập mô hình hóa mối đe dọa dựa trênvề khuôn khổ PASTA!

***4.5. Traits of an effective threat model - Đặc điểm của một mô hình đe dọa hiệu quả***

|  |
| --- |
| **Traits of an effective threat model** |

**Đặc điểm của một mô hình đe dọa hiệu quả**

|  |
| --- |
| **Threat modeling** is the process of identifying assets, their vulnerabilities, and how each is exposed to threats. It is a strategic approach that combines various security activities, such as vulnerability management, threat analysis, and incident response. Security teams commonly perform these exercises to ensure their systems are adequately protected. Another use of threat modeling is to proactively find ways of reducing risks to any system or business process. |

**Mô hình hóa mối đe dọa** là quá trình xác định tài sản, lỗ hổng của chúng và cách từng tài sản tiếp xúc với các mối đe dọa. Đây là một phương pháp tiếp cận chiến lược kết hợp nhiều hoạt động bảo mật khác nhau, chẳng hạn như quản lý lỗ hổng, phân tích mối đe dọa và phản ứng sự cố. Các nhóm bảo mật thường thực hiện các bài tập này để đảm bảo hệ thống của họ được bảo vệ đầy đủ. Một ứng dụng khác của mô hình hóa mối đe dọa là chủ động tìm cách giảm thiểu rủi ro cho bất kỳ hệ thống hoặc quy trình kinh doanh nào.

|  |
| --- |
| Traditionally, threat modeling is associated with the field of application development. In this reading, you will learn about common threat modeling frameworks that are used to design software that can withstand attacks. You'll also learn about the growing need for application security and ways that you can participate. |

Theo truyền thống, mô hình hóa mối đe dọa gắn liền với lĩnh vực phát triển ứng dụng. Trong bài đọc này, bạn sẽ tìm hiểu về các khuôn khổ mô hình hóa mối đe dọa phổ biến được sử dụng để thiết kế phần mềm có thể chống lại các cuộc tấn công. Bạn cũng sẽ tìm hiểu về nhu cầu ngày càng tăng đối với bảo mật ứng dụng và các cách bạn có thể tham gia.

|  |
| --- |
| **Why application security matters** |

**Tại sao bảo mật ứng dụng lại quan trọng**

|  |
| --- |
| Applications have become an essential part of many organizations' success. For example, web-based applications allow customers from anywhere in the world to connect with businesses, their partners, and other customers. |

Ứng dụng đã trở thành một phần thiết yếu trong thành công của nhiều tổ chức. Ví dụ, các ứng dụng dựa trên web cho phép khách hàng từ mọi nơi trên thế giới kết nối với doanh nghiệp, đối tác của họ và các khách hàng khác.

|  |
| --- |
| Mobile applications have also changed the way people access the digital world. Smartphones are often the main way that data is exchanged between users and a business. The volume of data being processed by applications makes securing them a key to reducing risk for everyone who’s connected. |

Các ứng dụng di động cũng đã thay đổi cách mọi người truy cập vào thế giới kỹ thuật số. Điện thoại thông minh thường là cách chính để trao đổi dữ liệu giữa người dùng và doanh nghiệp. Khối lượng dữ liệu được xử lý bởi các ứng dụng khiến việc bảo mật chúng trở thành chìa khóa để giảm rủi ro cho mọi người được kết nối.

|  |
| --- |
| For example, say an application uses Java-based logging libraries with the Log4Shell vulnerability ([CVE-2021-44228](https://nvd.nist.gov/vuln/detail/CVE-2021-44228)). If it's not patched, this vulnerability can allow remote code execution that an attacker can use to gain full access to your system from anywhere in the world. If exploited, a critical vulnerability like this can impact millions of devices. |

Ví dụ, giả sử một ứng dụng sử dụng thư viện ghi nhật ký dựa trên Java với lỗ hổng Log4Shell ([CVE-2021-44228](https://nvd.nist.gov/vuln/detail/CVE-2021-44228)). Nếu không được vá, lỗ hổng này có thể cho phép thực thi mã từ xa mà kẻ tấn công có thể sử dụng để có quyền truy cập đầy đủ vào hệ thống của bạn từ bất kỳ đâu trên thế giới. Nếu bị khai thác, một lỗ hổng nghiêm trọng như thế này có thể ảnh hưởng đến hàng triệu thiết bị.

|  |
| --- |
| **Defending the application layer** |

**Bảo vệ lớp ứng dụng**

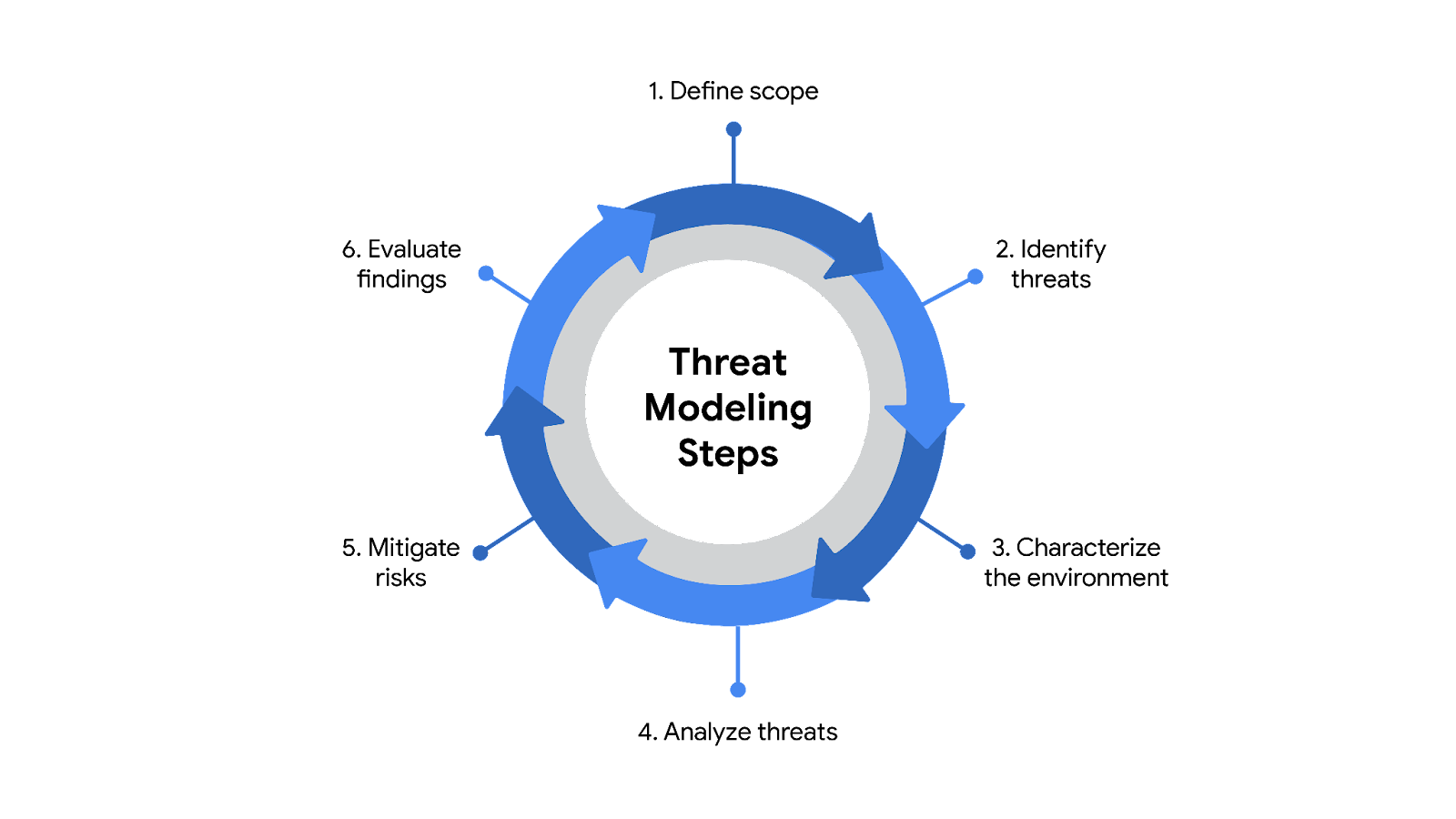
|  |
| --- |
| Defending the application layer requires proper testing to uncover weaknesses that can lead to risk. Threat modeling is one of the primary ways to ensure that an application meets security requirements. A DevSecOps team, which stands for development, security, and operations, usually performs these analyses. |

Bảo vệ lớp ứng dụng đòi hỏi phải thử nghiệm đúng cách để phát hiện ra các điểm yếu có thể dẫn đến rủi ro. Mô hình hóa mối đe dọa là một trong những cách chính để đảm bảo rằng ứng dụng đáp ứng các yêu cầu bảo mật. Nhóm DevSecOps, viết tắt của phát triển, bảo mật và vận hành, thường thực hiện các phân tích này.

|  |
| --- |
| A typical threat modeling process is performed in a cycle:   * Define the scope * Identify threats * Characterize the environment * Analyze threats * Mitigate risks * Evaluate findings |

Một quy trình mô hình hóa mối đe dọa điển hình được thực hiện theo một chu kỳ:

* Xác định phạm vi
* Xác định các mối đe dọa
* Đặc điểm môi trường
* Phân tích các mối đe dọa
* Giảm thiểu rủi ro
* Đánh giá các phát hiện



|  |
| --- |
| Ideally, threat modeling should be performed before, during, and after an application is developed. However, conducting a thorough software analysis takes time and resources. Everything from the application's architecture to its business purposes should be evaluated. As a result, a number of threat-modeling frameworks have been developed over the years to make the process smoother. |

Về lý tưởng, mô hình hóa mối đe dọa nên được thực hiện trước, trong và sau khi ứng dụng được phát triển. Tuy nhiên, việc tiến hành phân tích phần mềm kỹ lưỡng cần có thời gian và nguồn lực. Mọi thứ từ kiến ​​trúc của ứng dụng đến mục đích kinh doanh của ứng dụng đều phải được đánh giá. Do đó, một số khuôn khổ mô hình hóa mối đe dọa đã được phát triển trong nhiều năm để giúp quá trình này diễn ra suôn sẻ hơn.

|  |
| --- |
| **Note:** Threat modeling should be incorporated at every stage of the software development lifecycle, or SDLC. |

**Lưu ý:** Mô hình hóa mối đe dọa phải được kết hợp ở mọi giai đoạn của vòng đời phát triển phần mềm (SDLC).

|  |
| --- |
| **Common frameworks** |

**Khung chung**

|  |
| --- |
| When performing threat modeling, there are multiple methods that can be used, such as:   * STRIDE * PASTA * Trike * VAST |

Khi thực hiện mô hình hóa mối đe dọa, có nhiều phương pháp có thể được sử dụng, chẳng hạn như:

* STRIDE
* PASTA
* Trike
* VAST

|  |
| --- |
| Organizations might use any one of these to gather intelligence and make decisions to improve their security posture. Ultimately, the “right” model depends on the situation and the types of risks an application might face. |

Các tổ chức có thể sử dụng bất kỳ mô hình nào trong số này để thu thập thông tin tình báo và đưa ra quyết định nhằm cải thiện tình hình bảo mật của mình. Cuối cùng, mô hình "đúng" phụ thuộc vào tình huống và loại rủi ro mà ứng dụng có thể gặp phải.

|  |
| --- |
| **STRIDE** |

**STRIDE**

|  |
| --- |
| STRIDE is a threat-modeling framework developed by Microsoft. It’s commonly used to identify vulnerabilities in six specific attack vectors. The acronym represents each of these vectors: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. |

STRIDE là một khuôn khổ mô hình hóa mối đe dọa do Microsoft phát triển. Nó thường được sử dụng để xác định các lỗ hổng trong sáu vectơ tấn công cụ thể. Từ viết tắt đại diện cho từng vectơ này: giả mạo, giả mạo, từ chối, tiết lộ thông tin, từ chối dịch vụ và nâng cao đặc quyền.

|  |
| --- |
| **PASTA** |

**PASTA**

|  |
| --- |
| The **Process of Attack Simulation and Threat Analysis** (PASTA) is a risk-centric threat modeling process developed by two OWASP leaders and supported by a cybersecurity firm called VerSprite. Its main focus is to discover evidence of viable threats and represent this information as a model. PASTA's evidence-based design can be applied when threat modeling an application or the environment that supports that application. Its seven stage process consists of various activities that incorporate relevant security artifacts of the environment, like vulnerability assessment reports. |

Quá **trình mô phỏng tấn công và phân tích mối đe dọa** (PASTA) là một quy trình mô hình hóa mối đe dọa tập trung vào rủi ro do hai nhà lãnh đạo của OWASP phát triển và được hỗ trợ bởi một công ty an ninh mạng có tên là VerSprite. Trọng tâm chính của quy trình này là phát hiện bằng chứng về các mối đe dọa khả thi và biểu diễn thông tin này dưới dạng một mô hình. Thiết kế dựa trên bằng chứng của PASTA có thể được áp dụng khi mô hình hóa mối đe dọa cho một ứng dụng hoặc môi trường hỗ trợ ứng dụng đó. Quy trình bảy giai đoạn của quy trình này bao gồm nhiều hoạt động khác nhau kết hợp các hiện vật bảo mật có liên quan của môi trường, như báo cáo đánh giá lỗ hổng.

|  |
| --- |
| **Trike** |

**Trike**

|  |
| --- |
| Trike is an open source methodology and tool that takes a security-centric approach to threat modeling. It's commonly used to focus on security permissions, application use cases, privilege models, and other elements that support a secure environment. |

Trike là một phương pháp và công cụ nguồn mở áp dụng phương pháp tiếp cận tập trung vào bảo mật để mô hình hóa mối đe dọa. Nó thường được sử dụng để tập trung vào quyền bảo mật, trường hợp sử dụng ứng dụng, mô hình đặc quyền và các yếu tố khác hỗ trợ môi trường an toàn.

|  |
| --- |
| **VAST** |

**VAST**

|  |
| --- |
| The Visual, Agile, and Simple Threat (VAST) Modeling framework is part of an automated threat-modeling platform called ThreatModeler®. Many security teams opt to use VAST as a way of automating and streamlining their threat modeling assessments. |

Khung mô hình hóa mối đe dọa trực quan, linh hoạt và đơn giản (VAST) là một phần của nền tảng mô hình hóa mối đe dọa tự động có tên là ThreatModeler®. Nhiều nhóm bảo mật lựa chọn sử dụng VAST như một cách tự động hóa và hợp lý hóa các đánh giá mô hình hóa mối đe dọa của họ.

|  |
| --- |
| **Participating in threat modeling** |

**Tham gia vào mô hình hóa mối đe dọa**

|  |
| --- |
| Threat modeling is often performed by experienced security professionals, but it’s almost never done alone. This is especially true when it comes to securing applications. Programs are complex systems responsible for handling a lot of data and processing  a variety of commands from users and other systems. |

Mô hình hóa mối đe dọa thường được thực hiện bởi các chuyên gia bảo mật giàu kinh nghiệm, nhưng hầu như không bao giờ được thực hiện một mình. Điều này đặc biệt đúng khi nói đến việc bảo mật các ứng dụng. Các chương trình là các hệ thống phức tạp chịu trách nhiệm xử lý nhiều dữ liệu và xử lý nhiều lệnh khác nhau từ người dùng và các hệ thống khác.

|  |
| --- |
| One of the keys to threat modeling is asking the right questions:   * What are we working on? * What kinds of things can go wrong? * What are we doing about it? * Have we addressed everything? * Did we do a good job? |

Một trong những chìa khóa của mô hình hóa mối đe dọa là đặt câu hỏi đúng:

* Chúng tôi đang làm gì?
* Những chuyện gì có thể xảy ra không ổn?
* Chúng ta đang làm gì về vấn đề này?
* Chúng ta đã giải quyết hết mọi vấn đề chưa?
* Chúng ta đã làm tốt chưa?

|  |
| --- |
| It takes time and practice to learn how to work with things like data flow diagrams and attack trees. However, anyone can learn to be an effective threat modeler. Regardless of your level of experience, participating in one of these exercises always starts with simply asking the right questions. |

Cần có thời gian và thực hành để học cách làm việc với những thứ như sơ đồ luồng dữ liệu và cây tấn công. Tuy nhiên, bất kỳ ai cũng có thể học cách trở thành người lập mô hình mối đe dọa hiệu quả. Bất kể trình độ kinh nghiệm của bạn như thế nào, việc tham gia một trong những bài tập này luôn bắt đầu bằng cách chỉ cần đặt câu hỏi đúng.

|  |
| --- |
| **Key takeaways** |

**Những điểm chính**

|  |
| --- |
| Many people rely on software applications in their day to day lives. Securing the applications that people use has never been more important. Threat modeling is one of the main ways to determine whether security controls are in place to protect data privacy. Building the skills required to lead a threat modeling activity is a matter of practice. However, even a security analyst with little experience can be a valuable contributor to the process. It all starts with applying an attacker mindset and thinking critically about how data is handled. |

Nhiều người dựa vào các ứng dụng phần mềm trong cuộc sống hàng ngày của họ. Việc bảo mật các ứng dụng mà mọi người sử dụng chưa bao giờ quan trọng hơn thế. Mô hình hóa mối đe dọa là một trong những cách chính để xác định xem các biện pháp kiểm soát bảo mật có được áp dụng để bảo vệ quyền riêng tư dữ liệu hay không. Việc xây dựng các kỹ năng cần thiết để lãnh đạo hoạt động mô hình hóa mối đe dọa là vấn đề thực hành. Tuy nhiên, ngay cả một nhà phân tích bảo mật có ít kinh nghiệm cũng có thể là người đóng góp có giá trị cho quá trình này. Tất cả bắt đầu bằng việc áp dụng tư duy của kẻ tấn công và suy nghĩ nghiêm túc về cách xử lý dữ liệu.

***4.6. Explore: Apply PASTA to an application's threat model - Khám phá: Áp dụng PASTA vào mô hình mối đe dọa của ứng dụng***

|  |
| --- |
| **Explore: Apply PASTA to an application's threat model** |

**Khám phá: Áp dụng PASTA vào mô hình mối đe dọa của ứng dụng**

|  |
| --- |
| A designer clothing store has a new shopping app to drive sales. Improve the security of the app by performing a threat analysis using the PASTA framework. |

|  |
| --- |
| Một cửa hàng quần áo thiết kế có ứng dụng mua sắm mới để tăng doanh số bán hàng. Cải thiện tính bảo mật của ứng dụng bằng cách thực hiện phân tích mối đe dọa bằng khung PASTA. |

|  |  |
| --- | --- |
| **PASTA framework** | |
| **Stage 1: Define business and security objectives** | The team determines the retailer wants their app to protect customer data. |
| **Stage 2: Define the technical scope** | The team identifies the application components that must be evaluated. |
| **Stage 3: Decompose the application** | The team identifies existing controls that will protect user data from attackers. |
| **Stage 4: Perform a threat analysis** | The team gathers up-to-date intelligence on types of mobile-app attacks. |
| **Stage 5: Perform a vulnerability analysis** | The team more deeply investigates potential vulnerabilities related to the app. |
| **Stage 6: Conduct attack modeling** | The team creates an attack tree and maps vulnerabilities to attack vectors. |
| **Stage 7: Analyze risk and impact** | The team analyzes all collected data and makes risk management recommendations. |

|  |  |
| --- | --- |
| **PASTA framework** | |
| **Giai đoạn 1: Xác định mục tiêu kinh doanh và bảo mật** | Nhóm xác định nhà bán lẻ muốn ứng dụng của họ bảo vệ dữ liệu khách hàng. |
| **Giai đoạn 2: Xác định phạm vi kỹ thuật** | Nhóm xác định các thành phần ứng dụng phải được đánh giá. |
| **Giai đoạn 3: Phân tách ứng dụng** | Nhóm xác định các biện pháp kiểm soát hiện có sẽ bảo vệ dữ liệu người dùng khỏi những kẻ tấn công. |
| **Giai đoạn 4: Thực hiện phân tích mối đe dọa** | Nhóm thu thập thông tin tình báo cập nhật về các loại tấn công ứng dụng di động. |
| **Giai đoạn 5: Thực hiện phân tích lỗ hổng** | Nhóm điều tra sâu hơn các lỗ hổng tiềm ẩn liên quan đến ứng dụng. |
| **Giai đoạn 6: Tiến hành mô hình tấn công** | Nhóm tạo ra một cây tấn công và ánh xạ các lỗ hổng tới các vectơ tấn công. |
| **Giai đoạn 7: Phân tích rủi ro và tác động** | Nhóm phân tích tất cả dữ liệu thu thập được và đưa ra khuyến nghị quản lý rủi ro. |

***4.7. Activity: Apply the PASTA threat model framework - Hoạt động: Áp dụng khuôn khổ mô hình mối đe dọa PASTA***

|  |
| --- |
| **Activity Overview**  In this activity, you will practice using the Process of Attack Simulation and Threat Analysis (PASTA) threat model framework. You will determine whether a new shopping app is safe to launch.  Threat modeling is an important part of secure software development. Security teams typically perform threat models to identify vulnerabilities before malicious actors do. PASTA is a commonly used framework for assessing the risk profile of new applications. |

**Tổng quan hoạt động**

Trong hoạt động này, bạn sẽ thực hành sử dụng khuôn khổ mô hình mối đe dọa Phân tích mối đe dọa và Mô phỏng quá trình tấn công (PASTA). Bạn sẽ xác định xem ứng dụng mua sắm mới có an toàn để ra mắt hay không.

Mô hình hóa mối đe dọa là một phần quan trọng của quá trình phát triển phần mềm an toàn. Các nhóm bảo mật thường thực hiện mô hình mối đe dọa để xác định lỗ hổng trước khi các tác nhân độc hại thực hiện. PASTA là một khuôn khổ thường được sử dụng để đánh giá hồ sơ rủi ro của các ứng dụng mới.

|  |
| --- |
| **Scenario**  Review the following scenario. Then complete the step-by-step instructions.  You’re part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.  You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app. |

**Kịch bản**

Xem lại tình huống sau. Sau đó hoàn thành hướng dẫn từng bước.

Bạn là thành viên của nhóm bảo mật đang phát triển tại một công ty dành cho những người đam mê và sưu tập giày thể thao. Doanh nghiệp đang chuẩn bị ra mắt ứng dụng di động giúp khách hàng dễ dàng mua và bán giày.

Bạn đang thực hiện mô hình mối đe dọa của ứng dụng bằng cách sử dụng khuôn khổ PASTA. Bạn sẽ trải qua từng giai đoạn trong bảy giai đoạn của khuôn khổ để xác định các yêu cầu bảo mật cho ứng dụng công ty giày thể thao mới.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions and answer the included questions to complete the activity. |

**Hướng dẫn từng bước**

Thực hiện theo hướng dẫn và trả lời các câu hỏi kèm theo để hoàn thành hoạt động.

|  |
| --- |
| **Part 1 - Access the resources** |

**Phần 1 - Truy cập tài nguyên**

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the following link and select *Use Template*.  Link to template: [PASTA worksheet](https://docs.google.com/document/d/1u3aU6ZnWfcjzwZt79OdIwJ27dcyCZYDtmEEMivey3Os/template/preview?resourcekey=0-TAMA_2t0BCj5-BL9wG23Ng) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng mẫu* .

Liên kết đến mẫu:[Phiếu bài tập PASTA](https://docs.google.com/document/d/1u3aU6ZnWfcjzwZt79OdIwJ27dcyCZYDtmEEMivey3Os/template/preview?resourcekey=0-TAMA_2t0BCj5-BL9wG23Ng)

|  |
| --- |
| **Step 2: Access supporting materials**  The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.  To use the supporting materials for this course item, click the following link and select *Use Template*.  Link to supporting materials:   * [PASTA data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) * [PASTA attack tree](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?resourcekey=0-zYPY7AhPJdcClXamlAfOag#slide=id.p) |

**Bước 2: Truy cập tài liệu hỗ trợ**

Các tài liệu hỗ trợ sau đây sẽ giúp bạn hoàn thành hoạt động này. Hãy giữ chúng mở khi bạn tiến hành các bước tiếp theo.

Để sử dụng tài liệu hỗ trợ cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng mẫu* .

Liên kết tới tài liệu hỗ trợ:

* [Sơ đồ luồng dữ liệu PASTA](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)
* [Cây tấn công PASTA](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?resourcekey=0-zYPY7AhPJdcClXamlAfOag#slide=id.p)

|  |
| --- |
| **Part 2 - Complete the PASTA stages** |

**Phần 2 - Hoàn thành các giai đoạn PASTA**

|  |
| --- |
| **Step 1: Identify the mobile app’s business objectives**  The main goal of Stage I of the PASTA framework is to understand why the application was developed and what it is expected to do.  ***Note:*** *Stage I typically requires gathering input from many individuals at a business.*  First, review the following description of why the sneaker company decided to develop this new app:  **Description:** Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we’re being responsible with their information.  Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.  In the **Stage 1** row of the **PASTA worksheet,** make **2-3 notes** ofbusiness objectives that you’ve identified from the description. |

**Bước 1: Xác định mục tiêu kinh doanh của ứng dụng di động**

Mục tiêu chính của Giai đoạn I trong khuôn khổ PASTA là hiểu lý do tại sao ứng dụng được phát triển và ứng dụng được kỳ vọng sẽ thực hiện những gì.

***Lưu ý:*** *Giai đoạn I thường yêu cầu thu thập ý kiến ​​đóng góp từ nhiều cá nhân trong một doanh nghiệp.*

Trước tiên, hãy xem lại phần mô tả sau đây về lý do tại sao công ty giày thể thao quyết định phát triển ứng dụng mới này:

**Mô tả:** Ứng dụng của chúng tôi phải kết nối người bán và người mua một cách liền mạch. Người dùng phải dễ dàng đăng ký, đăng nhập và quản lý tài khoản của mình. Quyền riêng tư dữ liệu là mối quan tâm lớn của chúng tôi. Chúng tôi muốn người dùng cảm thấy tự tin rằng chúng tôi đang chịu trách nhiệm với thông tin của họ.

Người mua nên có thể nhắn tin trực tiếp cho người bán để hỏi. Họ cũng nên có khả năng đánh giá người bán để khuyến khích dịch vụ tốt. Bán hàng nên rõ ràng và xử lý nhanh chóng. Người dùng nên có nhiều tùy chọn thanh toán để quá trình thanh toán diễn ra suôn sẻ. Xử lý thanh toán đúng cách thực sự quan trọng vì chúng tôi muốn tránh các vấn đề pháp lý.

Trong hàng Giai **đoạn 1** của **bảng tính PASTA,** hãy ghi ra **2-3 ghi chú** về các mục tiêu kinh doanh mà bạn đã xác định được từ phần mô tả.

|  |
| --- |
| **Step 2: Evaluate the apps components**  In Stage II, the technological scope of the project is defined. Normally, the application development team is involved in this stage because they have the most knowledge about the code base and application logic. Your responsibility as a security professional would be to evaluate the application's architecture for security risks.  For example, the app will be exchanging and storing a lot of user data. These are some of the technologies that it uses:   * **Application programming interface (API):** An API is a set of rules that define how software components interact with each other. In application development, third-party APIs are commonly used to add functionality without having to program it from scratch. * **Public key infrastructure (PKI):** PKI is an encryption framework that secures the exchange of online information. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and a user's device. * **SHA-256:** SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. The sneaker app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers. * **Structured query language (SQL):** SQL is a programming language used to create, interact with, and request information from a database. For example, the mobile app uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also  uses SQL to access that data during a purchase.   Consider what you've learned about these technologies:   * *Which of these technologies would you evaluate first? How might they present risks from a security perspective?*   In the **Stage II** row of the **PASTA worksheet**, write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. |

**Bước 2: Đánh giá các thành phần của ứng dụng**

Ở Giai đoạn II, phạm vi công nghệ của dự án được xác định. Thông thường, nhóm phát triển ứng dụng tham gia vào giai đoạn này vì họ có nhiều kiến ​​thức nhất về cơ sở mã và logic ứng dụng. Trách nhiệm của bạn với tư cách là một chuyên gia bảo mật là đánh giá kiến ​​trúc ứng dụng để tìm rủi ro bảo mật.

Ví dụ, ứng dụng sẽ trao đổi và lưu trữ rất nhiều dữ liệu người dùng. Đây là một số công nghệ mà ứng dụng sử dụng:

* **Giao diện lập trình ứng dụng (API):** API là một tập hợp các quy tắc xác định cách các thành phần phần mềm tương tác với nhau. Trong phát triển ứng dụng, API của bên thứ ba thường được sử dụng để thêm chức năng mà không cần phải lập trình từ đầu.
* **Cơ sở hạ tầng khóa công khai (PKI):** PKI là một khuôn khổ mã hóa bảo mật việc trao đổi thông tin trực tuyến. Ứng dụng di động sử dụng kết hợp các thuật toán mã hóa đối xứng và không đối xứng: AES và RSA. Mã hóa AES được sử dụng để mã hóa dữ liệu nhạy cảm, chẳng hạn như thông tin thẻ tín dụng. Mã hóa RSA được sử dụng để trao đổi khóa giữa ứng dụng và thiết bị của người dùng.
* **SHA-256:** SHA-256 là hàm băm thường dùng, lấy dữ liệu đầu vào có độ dài bất kỳ và tạo ra bản tóm tắt 256 bit. Ứng dụng sneaker sẽ sử dụng SHA-256 để bảo vệ dữ liệu người dùng nhạy cảm, như mật khẩu và số thẻ tín dụng.
* **Ngôn ngữ truy vấn có cấu trúc (SQL):** SQL là ngôn ngữ lập trình được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu. Ví dụ, ứng dụng di động sử dụng SQL để lưu trữ thông tin về giày thể thao đang được bán cũng như người bán đang bán chúng. Nó cũng sử dụng SQL để truy cập dữ liệu đó trong quá trình mua hàng.

Hãy xem xét những gì bạn đã học được về các công nghệ này:

* *Bạn sẽ đánh giá công nghệ nào trong số này trước? Chúng có thể gây ra rủi ro như thế nào theo quan điểm bảo mật?*

Trong hàng Giai **đoạn II** của **phiếu bài tập PASTA** , hãy viết **2-3 câu** (40-60 từ) mô tả lý do tại sao bạn chọn ưu tiên công nghệ đó hơn các công nghệ khác.

|  |
| --- |
| **Step 3: Review a data flow diagram**  During Stage III of PASTA, the objective is to analyze how the application is handling information. Here, each process is broken down.  For example, one of the app's processes might be to allow buyers to search the database for shoes that are for sale.  Open the **PASTA data flow diagram** resource. Review the diagram and consider how the technologies you evaluated relate to protecting user data in this process.  ***Note:*** *Software developers usually have detailed data flow diagrams available for security teams to use and verify that information is being processed securely.* |

**Bước 3: Xem lại sơ đồ luồng dữ liệu**

Trong Giai đoạn III của PASTA, mục tiêu là phân tích cách ứng dụng xử lý thông tin. Ở đây, mỗi quy trình được chia nhỏ.

Ví dụ, một trong những quy trình của ứng dụng có thể là cho phép người mua tìm kiếm trong cơ sở dữ liệu những đôi giày đang được bán.

Mở tài nguyên **sơ đồ luồng dữ liệu PASTA** . Xem lại sơ đồ và cân nhắc cách các công nghệ bạn đã đánh giá liên quan đến việc bảo vệ dữ liệu người dùng trong quy trình này.

***Lưu ý:*** *Các nhà phát triển phần mềm thường có sơ đồ luồng dữ liệu chi tiết để nhóm bảo mật sử dụng và xác minh rằng thông tin đang được xử lý an toàn.*

|  |
| --- |
| **Step 4: Use an attacker mindset to analyze potential threats**  Stage IV is about identifying potential threats to the application. This includes threats to the technologies you listed in Stage II. It also concerns the processes of your data flow diagram from Stage III.  For example, the apps authentication system could be attacked with a virus. Authentication could also be attacked if a threat actor social engineers an employee.  In the **Stage IV** row of the PASTA worksheet, list **2 types** of threats that are risks to the information being handled by the sneaker company's app.  ***Pro tip:*** *Internal system logs that you will use as a security analyst are good sources of threat intel* |

**Bước 4: Sử dụng tư duy của kẻ tấn công để phân tích các mối đe dọa tiềm ẩn**

Giai đoạn IV là về việc xác định các mối đe dọa tiềm ẩn đối với ứng dụng. Điều này bao gồm các mối đe dọa đối với các công nghệ bạn đã liệt kê trong Giai đoạn II. Nó cũng liên quan đến các quy trình của sơ đồ luồng dữ liệu của bạn từ Giai đoạn III.

Ví dụ, hệ thống xác thực ứng dụng có thể bị tấn công bằng vi-rút. Xác thực cũng có thể bị tấn công nếu kẻ tấn công sử dụng kỹ thuật xã hội để tấn công nhân viên.

Trong hàng Giai **đoạn IV** của bảng tính PASTA, hãy liệt kê **2 loại** mối đe dọa gây rủi ro cho thông tin mà ứng dụng của công ty giày thể thao đang xử lý.

***Mẹo chuyên nghiệp:*** *Nhật ký hệ thống nội bộ mà bạn sẽ sử dụng với tư cách là nhà phân tích bảo mật là nguồn thông tin tình báo về mối đe dọa tốt*

|  |
| --- |
| **Step 5: List vulnerabilities that can be exploited by those threats**  Stage V of PASTA is the vulnerability analysis. Here, you need to consider the attack surface of the technologies listed in Stage II.  For example, the app will use a payment system. The form used to collect credit card information might be vulnerable if it fails to encrypt data.  In **Stage V** of the **PASTA worksheet**, list **2 types** of vulnerabilities that could be exploited.  ***Pro tip:*** *Resources like the* [*CVE® list*](https://cve.mitre.org/cve/search_cve_list.html) *and* [*OWASP*](https://owasp.org/www-community/vulnerabilities/) *are useful for finding common software vulnerabilities.* |

**Bước 5: Liệt kê các lỗ hổng có thể bị khai thác bởi các mối đe dọa đó**

Giai đoạn V của PASTA là phân tích lỗ hổng. Ở đây, bạn cần xem xét bề mặt tấn công của các công nghệ được liệt kê trong Giai đoạn II.

Ví dụ, ứng dụng sẽ sử dụng hệ thống thanh toán. Biểu mẫu được sử dụng để thu thập thông tin thẻ tín dụng có thể dễ bị tấn công nếu không mã hóa dữ liệu.

Trong **Giai đoạn V** của **bảng tính PASTA** , hãy liệt kê **2 loại** lỗ hổng có thể bị khai thác.

***Mẹo chuyên nghiệp:*** *Các nguồn tài nguyên như*[*Danh sách CVE®*](https://cve.mitre.org/cve/search_cve_list.html)*Và*[*OWASP*](https://owasp.org/www-community/vulnerabilities/)*hữu ích trong việc tìm ra các lỗ hổng phần mềm phổ biến.*

|  |
| --- |
| **Step 6: Map assets, threats, and vulnerabilities to an attack tree**  In Stage VI of PASTA, the information gathered in the previous two steps are used to build an attack tree.  Open the **PASTA attack tree** resource. Review the diagram and consider how threat actors can potentially exploit these attack vectors.  **Note:** Applications like this normally have large, complex attack trees with many branches. |

**Bước 6: Ánh xạ tài sản, mối đe dọa và lỗ hổng vào cây tấn công**

Ở Giai đoạn VI của PASTA, thông tin thu thập được ở hai bước trước sẽ được sử dụng để xây dựng cây tấn công.

Mở tài nguyên **cây tấn công PASTA** . Xem lại sơ đồ và xem xét cách các tác nhân đe dọa có thể khai thác các vectơ tấn công này.

**Lưu ý:** Các ứng dụng như thế này thường có cây tấn công lớn, phức tạp với nhiều nhánh.

|  |
| --- |
| **Step 7: Identify new security controls that can reduce risk**  PASTA threat modeling is commonly used to reduce the likelihood of security risks. In Stage VII, the final goal is to implement defenses and safeguards that mitigate threats.  In **Stage VII** of the **PASTA worksheet**, list **4 security controls** that you have learned about that can reduce the chances of a security incident, like a data breach. |

**Bước 7: Xác định các biện pháp kiểm soát bảo mật mới có thể giảm thiểu rủi ro**

Mô hình hóa mối đe dọa PASTA thường được sử dụng để giảm khả năng xảy ra rủi ro bảo mật. Ở Giai đoạn VII, mục tiêu cuối cùng là triển khai các biện pháp phòng thủ và bảo vệ để giảm thiểu các mối đe dọa.

Trong **Giai đoạn VII** của **bảng tính PASTA** , hãy liệt kê **4 biện pháp kiểm soát bảo mật** mà bạn đã tìm hiểu có thể giúp giảm nguy cơ xảy ra sự cố bảo mật, chẳng hạn như vi phạm dữ liệu.

|  |
| --- |
| **What to Include in Your Response**  Be sure to address the following elements in your completed activity:   * **2-3** business objectives * **2-3** technology requirements * **2** potential threats * **2** system vulnerabilities * **4** defenses that limit risk |

**Những gì cần đưa vào phản hồi của bạn**

Hãy đảm bảo giải quyết các yếu tố sau trong hoạt động đã hoàn thành của bạn:

* **2-3** mục tiêu kinh doanh
* **2-3** yêu cầu về công nghệ
* **2** mối đe dọa tiềm tàng
* **2** lỗ hổng hệ thống
* **4** biện pháp phòng thủ hạn chế rủi ro

***4.8. Activity Exemplar: Apply the PASTA threat model framework - Ví dụ hoạt động: Áp dụng khuôn khổ mô hình mối đe dọa PASTA***

|  |
| --- |
| **Activity Exemplar: Apply the PASTA threat model framework**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Ví dụ hoạt động: Áp dụng khuôn khổ mô hình mối đe dọa PASTA**

Sau đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ này đáp ứng được kỳ vọng của hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link and select *Use Template*.  Link to exemplar: [PASTA worksheet exemplar](https://docs.google.com/document/d/1AKtzaOKIPDGaq3yV9asSkdCsW_q2UYuS_6VQz6NWZsc/template/preview#heading=h.7nlk2ynsm6vx) |

**Mẫu hoàn thành**

Để xem lại mẫu cho mục khóa học này, hãy nhấp vào liên kết và chọn *Sử dụng mẫu* .

Liên kết đến ví dụ:[Mẫu bài tập PASTA](https://docs.google.com/document/d/1AKtzaOKIPDGaq3yV9asSkdCsW_q2UYuS_6VQz6NWZsc/template/preview#heading=h.7nlk2ynsm6vx)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.  ***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your activity includes information at each stage of the process. Threat modeling is an advanced practice in cybersecurity. It normally requires experience in the field, deep knowledge of computer technology, and many different people to participate.*  Let’s review each stage of this PASTA threat modeling exercise:  **Stage I: Define business and security objectives**  **Summary:** These objectives are defined early by asking broad questions about the purpose of the application. For example, how does the app make the business money? Understanding the answer to these questions helps guide the detailed work that will follow.  **Recommendations:** A shopping application like this will need to process payments. Based on this description, we know certain technologies are required to keep information private and secure and that everything will need to be compliant with PCI-DSS.  **Stage II: Define the technical scope**  **Summary:** The objective here is to understand the attack surface by identifying the technologies being used by the application and understanding their dependencies.  **Recommendations:** APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there’s a larger attack surface.  **Stage III: Decompose the application**  **Summary:** Stage three builds upon the previous stage by investigating how the application's components communicate together. The objective here is to review how the application works and how security controls are currently implemented.  **Recommendations:** The sample data flow diagram shows how a typical search request passes through multiple layers. One thing you might review here would be to ensure the MySQL database is using prepared statements when queries are input.  **Stage IV: Threat analysis**  **Summary:** The main objective of stage four is to consider the types of threats that might affect your application. This relates to the technologies you've already scoped. Another thing to consider is the types of data your application will be processing.  **Recommendations:** Injection attacks are common for SQL databases. Session hijacking is possible because the app communicates cookies between multiple layers.  It's important to consider your technological attack surface and any relevant threats to your product to effectively implement your information security responsibilities.  **Stage V: Vulnerability analysis**  **Summary:** Stage five is about associating asset vulnerabilities with potential threats. The objective here is to identify what is wrong with the design of the app or its codebase based on your security testing.  **Recommendations:**  A lack of prepared statements can make our SQL database vulnerable to injection attacks. And session hijacking is possible if cookies are mishandled between input and output sources.  **Stage VI: Attack modeling**  **Summary:** In this stage, the objective is to link the threats and vulnerabilities identified in the previous steps using attack trees. The purpose of using attack trees here is to show that the potential threats that you've identified are actually viable.  Resources like MITRE ATT&CK and the CVE® list are useful references to find evidence that validates the information that you've modeled in your attack tree.  **Recommendations:** This sample attack tree models how user data is vulnerable to the attacks that were identified earlier. Like the sample data flow diagram, an actual attack tree for a mobile application would be much more complex than this.  **Stage VII: Risk analysis and impact**  **Summary:** The objective of the final stage of PASTA is to identify ways to mitigate the risks that were identified from stages IV - VI and plan for any remaining risks that can't be remediated.  **Recommendations:** SHA-256, incident response procedures, password policy, and principle of least privilege are a few examples of technical, operational, and managerial controls that can be implemented before launch to reduce risk. |

**Đánh giá mẫu**

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để hướng dẫn bạn khi bạn tiếp tục tiến bộ trong khóa học.

***Lưu ý:*** *Ví dụ này thể hiện một cách có thể để hoàn thành hoạt động. Hoạt động của bạn có thể khác ở một số điểm. Điều quan trọng là hoạt động của bạn bao gồm thông tin ở từng giai đoạn của quy trình. Mô hình hóa mối đe dọa là một hoạt động nâng cao trong an ninh mạng. Hoạt động này thường đòi hỏi kinh nghiệm trong lĩnh vực này, kiến ​​thức sâu rộng về công nghệ máy tính và nhiều người khác nhau để tham gia.*

Hãy cùng xem xét từng giai đoạn của bài tập mô hình hóa mối đe dọa PASTA này:

**Giai đoạn I: Xác định mục tiêu kinh doanh và bảo mật**

**Tóm tắt:** Các mục tiêu này được xác định sớm bằng cách đặt câu hỏi chung về mục đích của ứng dụng. Ví dụ, ứng dụng kiếm tiền cho doanh nghiệp như thế nào? Hiểu câu trả lời cho những câu hỏi này giúp định hướng công việc chi tiết tiếp theo.

**Khuyến nghị:** Một ứng dụng mua sắm như thế này sẽ cần xử lý thanh toán. Dựa trên mô tả này, chúng tôi biết một số công nghệ nhất định là cần thiết để giữ thông tin riêng tư và an toàn và mọi thứ sẽ cần phải tuân thủ PCI-DSS.

**Giai đoạn II: Xác định phạm vi kỹ thuật**

**Tóm tắt:** Mục tiêu ở đây là hiểu bề mặt tấn công bằng cách xác định các công nghệ đang được ứng dụng sử dụng và hiểu sự phụ thuộc của chúng.

**Khuyến nghị:** API tạo điều kiện thuận lợi cho việc trao đổi dữ liệu giữa khách hàng, đối tác và nhân viên, do đó chúng cần được ưu tiên. Chúng xử lý rất nhiều dữ liệu nhạy cảm trong khi kết nối nhiều người dùng và hệ thống với nhau. Tuy nhiên, cần cân nhắc các chi tiết như API nào đang được sử dụng trước khi ưu tiên công nghệ này hơn công nghệ khác. Do đó, chúng có thể dễ bị lỗ hổng bảo mật hơn vì có bề mặt tấn công lớn hơn.

**Giai đoạn III: Phân tích ứng dụng**

**Tóm tắt:** Giai đoạn ba xây dựng dựa trên giai đoạn trước bằng cách điều tra cách các thành phần của ứng dụng giao tiếp với nhau. Mục tiêu ở đây là xem xét cách ứng dụng hoạt động và cách kiểm soát bảo mật hiện đang được triển khai.

**Khuyến nghị:** Sơ đồ luồng dữ liệu mẫu cho thấy cách một yêu cầu tìm kiếm thông thường đi qua nhiều lớp. Một điều bạn có thể xem xét ở đây là đảm bảo cơ sở dữ liệu MySQL đang sử dụng các câu lệnh đã chuẩn bị khi các truy vấn được nhập.

**Giai đoạn IV: Phân tích mối đe dọa**

**Tóm tắt:** Mục tiêu chính của giai đoạn bốn là xem xét các loại mối đe dọa có thể ảnh hưởng đến ứng dụng của bạn. Điều này liên quan đến các công nghệ bạn đã xác định phạm vi. Một điều khác cần xem xét là các loại dữ liệu mà ứng dụng của bạn sẽ xử lý.

**Khuyến nghị:** Các cuộc tấn công tiêm mã là phổ biến đối với cơ sở dữ liệu SQL. Có thể chiếm đoạt phiên vì ứng dụng truyền cookie giữa nhiều lớp. Điều quan trọng là phải xem xét bề mặt tấn công công nghệ của bạn và bất kỳ mối đe dọa nào có liên quan đến sản phẩm của bạn để thực hiện hiệu quả các trách nhiệm bảo mật thông tin của bạn.

**Giai đoạn V: Phân tích lỗ hổng**

**Tóm tắt:** Giai đoạn năm là về việc liên kết các lỗ hổng tài sản với các mối đe dọa tiềm ẩn. Mục tiêu ở đây là xác định lỗi trong thiết kế ứng dụng hoặc cơ sở mã của ứng dụng dựa trên thử nghiệm bảo mật của bạn.

**Khuyến nghị:**   Việc thiếu các câu lệnh chuẩn bị có thể khiến cơ sở dữ liệu SQL của chúng ta dễ bị tấn công tiêm nhiễm. Và việc chiếm đoạt phiên có thể xảy ra nếu cookie bị xử lý sai giữa các nguồn đầu vào và đầu ra.

**Giai đoạn VI: Mô hình tấn công**

**Tóm tắt:** Ở giai đoạn này, mục tiêu là liên kết các mối đe dọa và lỗ hổng được xác định trong các bước trước bằng cách sử dụng cây tấn công. Mục đích của việc sử dụng cây tấn công ở đây là để chứng minh rằng các mối đe dọa tiềm ẩn mà bạn đã xác định thực sự khả thi. Các nguồn như MITRE ATT&CK và danh sách CVE® là những tài liệu tham khảo hữu ích để tìm bằng chứng xác thực thông tin mà bạn đã mô hình hóa trong cây tấn công của mình.

**Khuyến nghị:** Mẫu cây tấn công này mô hình hóa cách dữ liệu người dùng dễ bị tấn công đã được xác định trước đó. Giống như sơ đồ luồng dữ liệu mẫu, một cây tấn công thực tế cho ứng dụng di động sẽ phức tạp hơn nhiều so với sơ đồ này.

**Giai đoạn VII: Phân tích rủi ro và tác động**

**Tóm tắt:** Mục tiêu của giai đoạn cuối cùng của PASTA là xác định các cách giảm thiểu rủi ro đã được xác định từ giai đoạn IV - VI và lập kế hoạch ứng phó với mọi rủi ro còn lại không thể khắc phục được.

**Khuyến nghị:** SHA-256, quy trình ứng phó sự cố, chính sách mật khẩu và nguyên tắc đặc quyền tối thiểu là một số ví dụ về các biện pháp kiểm soát kỹ thuật, vận hành và quản lý có thể được triển khai trước khi ra mắt để giảm thiểu rủi ro.

***4.9. Test your knowledge: Threat modeling - Kiểm tra kiến thức của bạn: Mô hình hóa mối đe dọa***

**5. Review: Threats in cybersecurity – Đánh giá: Các mối đe dọa trong an ninh mạng**

***5.1. Wrap-up - Tóm tắt***

|  |
| --- |
| Managing threats is a major part of what security professionals do. In this part of the course, we've explored some common types of cyber threats that you'll likely encounter in the field. Let's review. |

Quản lý các mối đe dọa là một phần quan trọngnhững gì các chuyên gia an ninh làm.Trong phần này của khóa học,chúng tôi đã khám phá một số loại phổ biếncủa các mối đe dọa mạng mà bạn sẽcó thể gặp phải trong thực tế. Chúng ta hãy cùng xem lại.

|  |
| --- |
| We started off discussing social engineering. You learned that attackers have a variety of ways to trick their targets into sharing private information. Social engineering techniques rely on exploiting people's trust and willingness to help. Phishing attacks are one of the most common ways that attackers go about manipulating their targets. |

Chúng tôi bắt đầu thảo luận về kỹ thuật xã hội.Bạn đã biết rằng những kẻ tấn công có nhiều cách khác nhau đểlừa mục tiêu chia sẻ thông tin riêng tư.Kỹ thuật kỹ thuật xã hội dựa vàolợi dụng lòng tin và thiện chí giúp đỡ của mọi người.Tấn công lừa đảo là một trong những cách phổ biến nhấtrằng kẻ tấn công sẽ tìm cách thao túng mục tiêu của chúng.

|  |
| --- |
| Next, we explored malware. Here, we discussed the major classes of malware, like viruses, trojans, and worms. You learned how to spot signs of infection. You also learned how malware has evolved and become more sophisticated over the years. |

Tiếp theo, chúng ta khám phá phần mềm độc hại.Ở đây, chúng tôi thảo luận về các lớp phần mềm độc hại chính,giống như virus, trojan và sâu.Bạn đã học cách phát hiện các dấu hiệu nhiễm trùng.Bạn cũng đã học được cách phần mềm độc hại đãđã phát triển và trở nên tinh vi hơn theo thời gian.

|  |
| --- |
| After that, we turned our attention to web-based exploits, specifically injection attacks. You learned about cross-site scripting and SQL injection, two of the most common types of attacks facing organizations online. We discussed how each of these attacks are carried out. You also learned about how web applications can be protected from malicious code. Finally, we explored the threat modeling process. You learned the process that security teams use to perform these exercises. |

Sau đó, chúng tôi chuyển sự chú ý của mình sangkhai thác dựa trên web, đặc biệt là các cuộc tấn công tiêm nhiễm.Bạn đã học về cross-site scriptingvà tiêm SQL,hai trong số những loại phổ biến nhấtcác cuộc tấn công mà các tổ chức phải đối mặt trực tuyến.Chúng tôi đã thảo luận về cách thực hiện từng cuộc tấn công này.Bạn cũng đã học được về cáchcác ứng dụng web có thể được bảo vệ khỏi mã độc.Cuối cùng, chúng tôi đã khám phá quá trình mô hình hóa mối đe dọa.Bạn đã học được quy trình mà các nhóm bảo mậtsử dụng để thực hiện các bài tập này.

|  |
| --- |
| Unfortunately, cyberattacks and security breaches are a reality that we're challenged with on a regular basis. However, being aware of the type of threats that exist and the threat modeling process provides an important foundation for your work as a security analyst. |

Thật không may, các cuộc tấn công mạng vàvi phạm an ninh là một thực tếchúng ta thường xuyên phải đối mặt với thử thách này.Tuy nhiên, nhận thức đượcloại mối đe dọa hiện hữu vàquá trình mô hình hóa mối đe dọa cung cấpmột nền tảng quan trọng chocông việc của bạn với tư cách là nhà phân tích bảo mật.

***5.2. Glossary terms from module 4 - Thuật ngữ trong mô-đun 4***

|  |
| --- |
| **Glossary terms from module 4** |

**Thuật ngữ trong mô-đun 4**

|  |
| --- |
| **Terms and definitions from Course 5, Module 4** |

**Các thuật ngữ và định nghĩa từ Khóa học 5, Mô-đun 4**

|  |
| --- |
| **Angler phishing:** A technique where attackers impersonate customer service representatives on social media |

**Lừa đảo qua mạng:** Một kỹ thuật mà kẻ tấn công mạo danh nhân viên dịch vụ khách hàng trên mạng xã hội

|  |
| --- |
| **Advanced persistent threat (APT):** Instances when a threat actor maintains unauthorized access to a system for an extended period of time |

**Mối đe dọa dai dẳng nâng cao (APT):** Các trường hợp khi tác nhân đe dọa duy trì quyền truy cập trái phép vào hệ thống trong một thời gian dài

|  |
| --- |
| **Adware:** A type of legitimate software that is sometimes used to display digital advertisements in applications |

**Phần mềm quảng cáo:** Một loại phần mềm hợp pháp đôi khi được sử dụng để hiển thị quảng cáo kỹ thuật số trong các ứng dụng

|  |
| --- |
| **Attack tree:** A diagram that maps threats to assets |

**Cây tấn công:** Sơ đồ ánh xạ các mối đe dọa đến tài sản

|  |
| --- |
| **Baiting:** A social engineering tactic that tempts people into compromising their security |

**Mồi nhử:** Một chiến thuật kỹ thuật xã hội dụ dỗ mọi người xâm phạm an ninh của họ

|  |
| --- |
| **Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder" |

**Botnet:** Một tập hợp các máy tính bị nhiễm phần mềm độc hại nằm dưới sự kiểm soát của một tác nhân đe dọa duy nhất, được gọi là "bot-herder"

|  |
| --- |
| **Cross-site scripting (XSS):** An injection attack that inserts code into a vulnerable website or web application |

**Tấn công mã hóa chéo trang web (XSS):** Một cuộc tấn công chèn mã vào một trang web hoặc ứng dụng web dễ bị tấn công

|  |
| --- |
| **Cryptojacking:** A form of malware that installs software to illegally mine cryptocurrencies |

**Cryptojacking:** Một dạng phần mềm độc hại cài đặt phần mềm để khai thác tiền điện tử bất hợp pháp

|  |
| --- |
| **DOM-based XSS attack:** An instance when malicious script exists in the webpage a browser loads |

**Tấn công XSS dựa trên DOM:** Trường hợp tập lệnh độc hại tồn tại trong trang web mà trình duyệt tải

|  |
| --- |
| **Dropper:** A type of malware that comes packed with malicious code which is delivered and installed onto a target system |

**Dropper:** Một loại phần mềm độc hại đi kèm với mã độc được phân phối và cài đặt vào hệ thống mục tiêu

|  |
| --- |
| **Fileless malware:** Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer |

**Phần mềm độc hại không có tệp:** Phần mềm độc hại không cần người dùng cài đặt vì nó sử dụng các chương trình hợp pháp đã được cài đặt để lây nhiễm vào máy tính

|  |
| --- |
| **Hacker:** Any person or group who uses computers to gain unauthorized access to data |

**Hacker:** Bất kỳ cá nhân hoặc nhóm nào sử dụng máy tính để truy cập trái phép vào dữ liệu

|  |
| --- |
| **Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment |

**Quản lý danh tính và truy cập (IAM):** Một tập hợp các quy trình và công nghệ giúp các tổ chức quản lý danh tính kỹ thuật số trong môi trường của họ

|  |
| --- |
| **Injection attack:** Malicious code inserted into a vulnerable application |

**Tấn công tiêm:** Mã độc được chèn vào ứng dụng dễ bị tấn công

|  |
| --- |
| **Input validation:** Programming that validates inputs from users and other programs |

**Xác thực đầu vào:** Lập trình xác thực đầu vào từ người dùng và các chương trình khác

|  |
| --- |
| **Intrusion detection system (IDS):** An application that monitors system activity and alerts on possible intrusions |

**Hệ thống phát hiện xâm nhập (IDS):** Một ứng dụng giám sát hoạt động của hệ thống và cảnh báo về các cuộc xâm nhập có thể xảy ra

|  |
| --- |
| **Loader:** A type of malware that downloads strains of malicious code from an external source and installs them onto a target system |

**Trình tải:** Một loại phần mềm độc hại tải xuống các loại mã độc hại từ nguồn bên ngoài và cài đặt chúng vào hệ thống mục tiêu

|  |
| --- |
| **Malware:** Software designed to harm devices or networks |

**Phần mềm độc hại:** Phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng

|  |
| --- |
| **Process of Attack Simulation and Threat Analysis (PASTA):** A popular threat modeling framework that’s used across many industries |

**Quy trình mô phỏng tấn công và phân tích mối đe dọa (PASTA):** Một khuôn khổ mô hình hóa mối đe dọa phổ biến được sử dụng trong nhiều ngành công nghiệp

|  |
| --- |
| **Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software |

**Lừa đảo:** Sử dụng phương tiện truyền thông kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại

|  |
| --- |
| **Phishing kit:** A collection of software tools needed to launch a phishing campaign |

**Bộ công cụ lừa đảo:** Một bộ sưu tập các công cụ phần mềm cần thiết để khởi chạy một chiến dịch lừa đảo

|  |
| --- |
| **Prepared statement:** A coding technique that executes SQL statements before passing them onto the database |

**Câu lệnh đã chuẩn bị:** Một kỹ thuật mã hóa thực thi các câu lệnh SQL trước khi chuyển chúng vào cơ sở dữ liệu

|  |
| --- |
| **Potentially unwanted application (PUA):** A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software |

**Ứng dụng có khả năng không mong muốn (PUA):** Một loại phần mềm không mong muốn được đóng gói cùng với các chương trình hợp pháp có thể hiển thị quảng cáo, làm chậm thiết bị hoặc cài đặt phần mềm khác

|  |
| --- |
| **Quid pro quo:** A type of baiting used to trick someone into believing that they’ll be rewarded in return for sharing access, information, or money |

**Quid pro quo:** Một loại mồi nhử được sử dụng để lừa ai đó tin rằng họ sẽ được thưởng khi chia sẻ quyền truy cập, thông tin hoặc tiền bạc

|  |
| --- |
| **Ransomware:** Type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access |

**Ransomware:** Loại tấn công độc hại trong đó kẻ tấn công mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập

|  |
| --- |
| **Reflected XSS attack:** An instance when malicious script is sent to a server and activated during the server’s response |

**Tấn công XSS phản ánh:** Trường hợp tập lệnh độc hại được gửi đến máy chủ và được kích hoạt trong quá trình phản hồi của máy chủ

|  |
| --- |
| **Rootkit:** Malware that provides remote, administrative access to a computer |

**Rootkit:** Phần mềm độc hại cung cấp quyền truy cập quản trị từ xa vào máy tính

|  |
| --- |
| **Scareware:** Malware that employs tactics to frighten users into infecting their device |

**Scareware:** Phần mềm độc hại sử dụng các chiến thuật để dọa người dùng lây nhiễm thiết bị của họ

|  |
| --- |
| **Smishing**: The use of text messages to trick users to obtain sensitive information or to impersonate a known source |

**Smishing** : Việc sử dụng tin nhắn văn bản để lừa người dùng lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết

|  |
| --- |
| **Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables |

**Kỹ thuật xã hội:** Một kỹ thuật thao túng lợi dụng lỗi của con người để lấy thông tin riêng tư, quyền truy cập hoặc đồ vật có giá trị

|  |
| --- |
| **Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source |

**Lừa đảo qua email:** Một cuộc tấn công email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể, có vẻ như xuất phát từ một nguồn đáng tin cậy

|  |
| --- |
| **Spyware:** Malware that’s used to gather and sell information without consent |

**Phần mềm gián điệp:** Phần mềm độc hại được sử dụng để thu thập và bán thông tin mà không được sự đồng ý

|  |
| --- |
| **SQL (Structured Query Language):** A programming language used to create, interact with, and request information from a database |

**SQL (Ngôn ngữ truy vấn có cấu trúc):** Một ngôn ngữ lập trình được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu

|  |
| --- |
| **SQL injection:** An attack that executes unexpected queries on a database |

**SQL injection:** Một cuộc tấn công thực hiện các truy vấn không mong muốn trên cơ sở dữ liệu

|  |
| --- |
| **Stored XSS attack:** An instance when malicious script is injected directly on the server |

**Tấn công Stored XSS:** Trường hợp tập lệnh độc hại được đưa trực tiếp vào máy chủ

|  |
| --- |
| **Tailgating:** A social engineering tactic in which unauthorized people follow an authorized person into a restricted area |

**Đi theo đuôi:** Một chiến thuật kỹ thuật xã hội trong đó những người không được phép đi theo một người được phép vào khu vực hạn chế

|  |
| --- |
| **Threat:** Any circumstance or event that can negatively impact assets |

**Mối đe dọa:** Bất kỳ hoàn cảnh hoặc sự kiện nào có thể tác động tiêu cực đến tài sản

|  |
| --- |
| **Threat actor:** Any person or group who presents a security risk |

**Tác nhân đe dọa:** Bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro về an ninh

|  |
| --- |
| **Threat modeling:** The process of identifying assets, their vulnerabilities, and how each is exposed to threats |

**Mô hình hóa mối đe dọa:** Quá trình xác định tài sản, lỗ hổng của chúng và cách từng tài sản bị ảnh hưởng bởi các mối đe dọa

|  |
| --- |
| **Trojan horse:** Malware that looks like a legitimate file or program |

**Trojan horse:** Phần mềm độc hại trông giống như một tập tin hoặc chương trình hợp pháp

|  |
| --- |
| **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source |

**Vishing:** Việc khai thác thông tin liên lạc bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết

|  |
| --- |
| **Watering hole attack**: A type of attack when a threat actor compromises a website frequently visited by a specific group of users |

**Tấn công Watering hole** : Một loại tấn công khi kẻ tấn công xâm nhập vào một trang web thường xuyên được một nhóm người dùng cụ thể truy cập

|  |
| --- |
| **Whaling:** A category of spear phishing attempts that are aimed at high-ranking executives in an organization |

**Whaling:** Một loại hình lừa đảo trực tuyến nhắm vào các giám đốc điều hành cấp cao trong một tổ chức

|  |
| --- |
| **Web-based exploits:** Malicious code or behavior that’s used to take advantage of coding flaws in a web application |

**Khai thác dựa trên web:** Mã độc hại hoặc hành vi được sử dụng để lợi dụng các lỗi mã hóa trong ứng dụng web

***5.3. Module 4 challenge - Thử thách Module 4***

**6. Congratulations on completing course 5 – Xin chúc mừng bạn đã hoàn thành khóa học 5**

***6.1. Course wrap-up - Tổng kết khóa học***

|  |
| --- |
| Congratulations on making it through the end of this course! I can hardly believe our time together is over. Before moving on in the certificate program, I'd like to reflect on all the amazing progress you've made. |

Xin chúc mừng vì đã hoàn thành khóa học này!Tôi khó có thể tin rằng thời gian chúng ta bên nhau đã kết thúc.Trước khi chuyển sang chương trình cấp chứng chỉ,Tôi muốn suy ngẫm về tất cả những tiến bộ đáng kinh ngạc mà bạn đã đạt được.

|  |
| --- |
| When we started, you were introduced to a wide range of assets organizations protect. Our primary focus was information security, specifically digital information. |

Khi chúng tôi bắt đầu, bạn đã được giới thiệu đến nhiều loại tài sảntổ chức bảo vệ.Trọng tâm chính của chúng tôi là bảo mật thông tin, cụ thể làthông tin kỹ thuật số.

|  |
| --- |
| Here, you learned how asset classification helps security teams focus their efforts and prioritize resources. We explored digital assets in the three states of data. We also learned how policies, standards, and procedures can mitigate organizational risk. Our focus on the NIST cybersecurity framework introduced you to a commonly used framework for managing risk. |

Tại đây, bạn đã học được cách phân loại tài sản giúp các nhóm an ninh tập trungnỗ lực của họ và ưu tiên nguồn lực.Chúng tôi đã khám phá tài sản kỹ thuật số ở ba trạng thái dữ liệu.Chúng tôi cũng đã học được cách các chính sách, tiêu chuẩn vàcác thủ tục có thể giảm thiểu rủi ro của tổ chức.Tập trung của chúng tôi vào khuôn khổ an ninh mạng NIST đã giới thiệu cho bạn mộtkhuôn khổ để quản lý rủi ro.

|  |
| --- |
| Afterwards, you learned about fundamental security systems and controls. |

Sau đó, bạn sẽ được học về các hệ thống an ninh và biện pháp kiểm soát cơ bản.

|  |
| --- |
| You got to explore technology, like encryption, that's used to protect data in all its states. You also learned how technologies like public key infrastructure and digital certificates are used to maintain the confidentiality, integrity, and availability of information online. And you also explored access controls that make up the authentication, authorization, and accounting framework. |

Bạn phải khám phá công nghệ, như mã hóa, được sử dụng để bảo vệ dữ liệutrong mọi trạng thái của nó.Bạn cũng đã học được cách các công nghệ như cơ sở hạ tầng khóa công khai vàchứng chỉ số được sử dụng để duy trì tính bảo mật,tính toàn vẹn và tính khả dụng của thông tin trực tuyến.Và bạn cũng đã khám phá các biện pháp kiểm soát truy cập tạo nên xác thực,thẩm quyền và khuôn khổ kế toán.

|  |
| --- |
| Next, we explored common vulnerabilities and systems. During this part of the course, you got an inside look into how security teams position themselves ahead of attacks. |

Tiếp theo, chúng tôi khám phá các lỗ hổng và hệ thống phổ biến.Trong phần này của khóa học, bạn sẽ có cái nhìn sâu sắc về cách các nhóm an ninhtự định vị mình trước các cuộc tấn công.

|  |
| --- |
| We explored the defense in depth strategy that's applied to protect information as it's exchanged between parties online. You also learned about the common vulnerability and exposures list, the vulnerability assessment process, and attack surfaces and attack vectors. |

Chúng tôi đã khám phá chiến lược phòng thủ chuyên sâu được áp dụng để bảo vệ thông tin nhưnó được trao đổi giữa các bên trực tuyến.Bạn cũng đã tìm hiểu về danh sách các lỗ hổng và nguy cơ phổ biến,quá trình đánh giá lỗ hổng, bề mặt tấn công và các hướng tấn công.

|  |
| --- |
| We then explored the major threats to asset security, like social engineering, malware, and web-based exploits. |

Sau đó, chúng tôi đã khám phá những mối đe dọa lớn đối với an ninh tài sản,như kỹ thuật xã hội, phần mềm độc hại và khai thác trên web.

|  |
| --- |
| Together, we discussed how these attacks are carried out and the way security teams prevent them from doing damage. We then finished up by exploring the process of threat modeling. |

Chúng tôi cùng nhau thảo luận về cách thức thực hiện các cuộc tấn công này vàcách các đội an ninh ngăn chặn chúng gây ra thiệt hại.Sau đó chúng tôi kết thúc bằng việc khám phá quá trình lập mô hình mối đe dọa.

|  |
| --- |
| We covered so much! I really appreciate your effort throughout it all. When I first started my career in security, my goal was to learn, network, and embrace any opportunity. I was able to attend security conferences, receive job tips, earned references, and volunteered to gain experience. At that time, I would have never imagined that I'd be here teaching what I've learned to others. |

Chúng ta đã đề cập đến rất nhiều điều!Tôi thực sự đánh giá cao nỗ lực của bạn trong suốt quá trình này.Khi tôi mới bắt đầu sự nghiệp an ninh, mục tiêu của tôi là học hỏi, kết nối vànắm bắt mọi cơ hội.Tôi đã có thể tham dự các hội nghị về an ninh, nhận được các mẹo tìm việc,đã kiếm được nhiều tài liệu tham khảo và tình nguyện tích lũy kinh nghiệm.Vào thời điểm đó,Tôi không bao giờ nghĩ rằng mình sẽ ở đây để truyền đạt những gì mình đã học cho người khác.

|  |
| --- |
| That just goes to show you, your security journey is only just beginning. While our time together is over, we covered a lot of complex topics, many of which are areas of specialization in security. With the foundation you've built here, you have a wide range of possibilities to continue growing in the field. |

Điều đó chứng tỏ hành trình bảo mật của bạn chỉ mới bắt đầu.Trong khi thời gian chúng ta bên nhau đã kết thúc, chúng ta đã đề cập đến rất nhiều chủ đề phức tạp,nhiều trong số đó là các lĩnh vực chuyên môn về an ninh.Với nền tảng bạn đã xây dựng ở đây,bạn có nhiều cơ hội để tiếp tục phát triển trong lĩnh vực này.

|  |
| --- |
| I'm so glad to have played a part in this step along your journey into the world of security. And I wish you all the best as you continue forward along your path. |

Tôi rất vui khi được đóng góp một phần vào bước tiến này trong hành trình của bạn vào thế giớibảo vệ.Và tôi chúc bạn mọi điều tốt đẹp nhất trên con đường bạn đi.

***6.2. Course 5 glossary - Từ điển khóa học 5***

|  |
| --- |
| **Course 5 glossary** |

**Từ điển khóa học 5**

|  |
| --- |
| We’ve covered a lot of terms—some of which you may have already known, and some of which are new. To make it easy to remember what a word means, we created this glossary of terms and definitions.  To use the glossary for this course item, click the link below and select “Use Template.”  Link to glossary: [Course 5 Glossary](https://docs.google.com/document/d/1i3IbpcZHIoSL_CoRR7sLwIyTN5Aj_TcYBwMn44eVRvE/template/preview?usp=sharing&resourcekey=0-986ppWjHBYBOLbKNxqqMTA) |

Chúng tôi đã đề cập đến rất nhiều thuật ngữ—một số trong đó bạn có thể đã biết và một số thì mới. Để giúp bạn dễ nhớ nghĩa của một từ, chúng tôi đã tạo ra bảng thuật ngữ và định nghĩa này.

Để sử dụng thuật ngữ cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn “Sử dụng mẫu”.

Liên kết đến thuật ngữ:[Từ vựng khóa học 5](https://docs.google.com/document/d/1i3IbpcZHIoSL_CoRR7sLwIyTN5Aj_TcYBwMn44eVRvE/template/preview?usp=sharing&resourcekey=0-986ppWjHBYBOLbKNxqqMTA)

***6.3. Your Course 5 learning journey - Hành trình học tập Khóa học 5 của bạn***

|  |
| --- |
| **Get started on the next course** |

**Bắt đầu khóa học tiếp theo**

|  |
| --- |
| Congratulations on completing Course 5 of the Google Cybersecurity Certificate: **Assets, Threats, and Vulnerabilities**! In this part of the program, you learned about assets and how they are protected. You also developed an attacker mindset by exploring the common security controls used to mitigate vulnerabilities and defend against threats. |

Xin chúc mừng bạn đã hoàn thành Khóa học 5 của Chứng chỉ An ninh mạng của Google: **Tài sản, Mối đe dọa và Lỗ hổng** ! Trong phần này của chương trình, bạn đã tìm hiểu về tài sản và cách chúng được bảo vệ. Bạn cũng đã phát triển tư duy của kẻ tấn công bằng cách khám phá các biện pháp kiểm soát bảo mật phổ biến được sử dụng để giảm thiểu lỗ hổng và bảo vệ chống lại các mối đe dọa.

|  |
| --- |
| The Google Cybersecurity Certificate has eight courses: |

Chứng chỉ An ninh mạng của Google có tám khóa học:



|  |
| --- |
| 1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities. 2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. 3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks. 4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL. 5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities. *(This is the course you just completed. Well done!)* 6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents. 7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks. 8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.   Now that you have completed this course, you’re ready to move on to the next course: [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1). |

1. **Nền tảng của An ninh mạng** — Khám phá nghề an ninh mạng, bao gồm các sự kiện quan trọng dẫn đến sự phát triển của lĩnh vực an ninh mạng và tầm quan trọng liên tục của nó đối với hoạt động của tổ chức. Tìm hiểu về các vai trò và trách nhiệm an ninh mạng cấp đầu vào.
2. **Chơi an toàn: Quản lý rủi ro bảo mật** — Xác định cách các chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh và khám phá các công cụ an ninh mạng phổ biến.
3. **Kết nối và Bảo vệ: Mạng và Bảo mật mạng** — Tìm hiểu về các lỗ hổng cấp độ mạng và cách bảo mật mạng.
4. **Công cụ chuyên dụng: Linux và SQL** — Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
5. **Tài sản, Mối đe dọa và Lỗ hổng** — Tìm hiểu về tầm quan trọng của các biện pháp kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và phòng thủ tài sản của tổ chức khỏi nhiều mối đe dọa, rủi ro và lỗ hổng khác nhau. *(Đây là khóa học bạn vừa hoàn thành. Làm tốt lắm!)*
6. **Báo động: Phát hiện và ứng phó** — Hiểu vòng đời ứng phó sự cố và thực hành sử dụng các công cụ để phát hiện và ứng phó với các sự cố an ninh mạng.
7. **Tự động hóa các tác vụ an ninh mạng bằng Python** — Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. **Đưa vào hoạt động: Chuẩn bị cho công việc an ninh mạng** — Tìm hiểu về phân loại sự cố, leo thang và cách giao tiếp với các bên liên quan. Khóa học này kết thúc chương trình bằng các mẹo về cách tham gia cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

Bây giờ bạn đã hoàn thành khóa học này, bạn đã sẵn sàng chuyển sang khóa học tiếp theo:[**Báo động: Phát hiện và ứng phó**](https://www.coursera.org/learn/detection-and-response/home/week/1).

***6.4. Get started on the next course - Bắt đầu khóa học tiếp theo***