Khoá học 2 — An toàn là bạn: Quản lý rủi ro an ninh

Trong khóa học này, học viên sẽ đi sâu tìm hiểu các khái niệm đã làm quen ở khoá học đầu tiên, chú trọng vào cách chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh. Cụ thể, học viên sẽ xác định các bước quản lý rủi ro và tìm hiểu những mối đe dọa, rủi ro và lỗ hổng thường gặp. Ngoài ra, học viên cũng sẽ tìm hiểu dữ liệu Quản lý sự kiện và thông tin bảo mật (SIEM) và sử dụng cẩm nang hướng dẫn để ứng phó với các mối đe dọa, rủi ro và lỗ hổng đã phát hiện. Cuối cùng, họ sẽ thực hành kiểm tra bảo mật, một bước quan trọng để đến gần hơn với mục tiêu trở thành chuyên gia an ninh mạng.

Đến hết khóa học này, học viên sẽ:

- Xác định các mối đe dọa, rủi ro và lỗ hổng thường gặp.
- Hiểu được những mối đe dọa, rủi ro và lỗ hổng mà chuyên gia phân tích an ninh mạng mới vào nghề phải tập trung vào nhất.
- Hiểu được mục đích của khuôn khổ và các biện pháp kiểm soát bảo mật.
- Mô tả được tam giác CIA: confidentiality, integrity, availability (bí mật, toàn vẹn, sẵn sàng).
- Giải thích được khuôn khổ của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST).
- Tìm hiểu và thực hành kiểm tra bảo mật.
- Sử dụng cẩm nang hướng dẫn để ứng phó với mối đe doạ, rủi ro và lỗ hổng.

Hoạt động đưa vào hồ sơ: Trong khoá học 2, học viên sẽ hoàn thành kiểm tra bảo mật để đưa vào hồ sơ.

KỸ NĂNG THU ĐƯỢC:

- ❑ Tam giác CIA
- ❑ Khuôn khổ An ninh mạng (CSF) của NIST
- ❑ Khuôn khổ Quản lý rủi ro (RMF) của NIST
- ❑ Kiểm tra bảo mật
- ❑ Cẩm nang hướng dẫn ứng phó sự cố
- ❑ Kỹ năng công sở như phân tích và tư duy phản biện

CHỦ ĐỀ:

- ★ Lĩnh vực bảo mật
- ★ Khuôn khổ và biện pháp kiểm soát bảo mật
- ★ Khám phá công cụ bảo mật
- ★ Sử dụng cẩm nang để ứng phó sự cố

SỐ LIỆU VỀ NỘI DUNG:

35	Video
19	Bài đọc
14	Bài kiểm tra
8	Hoạt động thực hành

Course 2: Play It Safe: Manage Security Risks
Khóa 2: Thận trọng: Quản lý rủi ro bảo mật

Contents

Course 2: Play It Safe: Manage Security Risks
Khóa 2: Thận trọng: Quản lý rủi ro bảo mật

Module 1: Security domains
Phần 1: Miền bảo mật

Module 1: Security domains – Miền bảo mật

You will gain understanding of the CISSP's eight security domains. Then, you'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, you'll explore the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) and the steps of risk management.

Bạn sẽ hiểu rõ hơn về tám lĩnh vực bảo mật của CISSP. Sau đó, bạn sẽ tìm hiểu về các mối đe dọa, rủi ro và lỗ hổng chính đối với hoạt động kinh doanh. Ngoài ra, bạn sẽ khám phá Khung quản lý rủi ro (RMF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) và các bước quản lý rủi ro.

Learning Objectives

- Recognize and explain the focus of CISSP's eight security domains.
- Identify and define the primary threats, risks, and vulnerabilities to business operations.
- Describe the threats, risks, and vulnerabilities that entry-level security analysts are most focused on.
- Determine how threats, risks, and vulnerabilities impact business operations.
- Identify the steps of risk management.

Mục tiêu học tập

- Nhận biết và giải thích trọng tâm của tám lĩnh vực bảo mật của CISSP.
- Xác định và xác định các mối đe dọa, rủi ro và lỗ hổng chính đối với hoạt động kinh doanh.
- Mô tả các mối đe dọa, rủi ro và lỗ hổng bảo mật mà các nhà phân tích bảo mật cấp mới tập trung vào nhất.
- Xác định các mối đe dọa, rủi ro và lỗ hổng ảnh hưởng đến hoạt động kinh doanh như thế nào.
- Xác định các bước quản lý rủi ro.

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

1.1. Introduction to Course 2 – Giới thiệu khóa học 2

My name is Ashley, and I'm a Customer Engineering Enablement Lead for Security Operation Sales at Google. I'm excited to be your instructor for this course.

Tên tôi là Ashley và tôi là Trưởng nhóm hỗ trợ kỹ thuật khách hàng choBán hàng hoạt động bảo mật tại Google.Tôi rất vui mừng được trở thành người hướng dẫn của bạn cho khóa học này.

Module 1: Security domains
Phần 1: Miền bảo mật

Let's start by quickly reviewing what we've covered so far. Earlier, we defined security and explored some common job responsibilities for entry-level analysts. We also discussed core skills and knowledge that analysts need to develop. Then, we shared some key events like the LoveLetter and Morris attacks that led to the development and ongoing evolution of the security field. We also introduced you to frameworks, controls, and the CIA triad, which are all used to reduce risk.

Hãy bắt đầu bằng cách xem lại nhanh những gì chúng ta đã trình bày cho đến nay.Trước đó, chúng ta đã xác định tính bảo mật vàkhám phá một số trách nhiệm công việc chung của các nhà phân tích cấp đầu vào.Chúng tôi cũng thảo luận về các kỹ năng và kiến thức cốt lõi mà các nhà phân tích cần phát triển.Sau đó, chúng tôi chia sẻ một số sự kiện quan trọng như cuộc tấn công LoveLetter và Morrisđã dẫn tới sự phát triển và tiến hóa không ngừng của lĩnh vực an ninh.Chúng tôi cũng đã giới thiệu cho bạn các khuôn khổ, điều khiển vàbộ ba CIA, tất cả đều được sử dụng để giảm thiểu rủi ro.

In this course, we'll discuss the focus of Certified Information Systems Security Professional's, or CISSP's, eight security domains. We'll also cover security frameworks and controls in more detail, with a focus on NIST's Risk Management Framework. Additionally, we'll explore security audits, including common elements of internal audits. Then, we'll introduce some basic security tools, and you'll have a chance to explore how to use security tools to protect assets and data from threats, risks, and vulnerabilities.

Trong khóa học này, chúng ta sẽ thảo luận trọng tâm của Chuyên gia bảo mật hệ thống thông tin được chứng nhận,hoặc CISSP's, tám miền bảo mật.Chúng tôi cũng sẽ đề cập đến các khung bảo mật và kiểm soát chi tiết hơn,tập trung vào Khung quản lý rủi ro của NIST.Ngoài ra, chúng ta sẽ khám phá các hoạt động kiểm tra bảo mật, bao gồm các hoạt động kiểm tra chungcác yếu tố của kiểm toán nội bộ.Sau đó, chúng tôi sẽ giới thiệu một số công cụ bảo mật cơ bản vàbạn sẽ có cơ hội khám phá cách sử dụng các công cụ bảo mật để bảo vệ tài sản và dữ liệukhỏi các mối đe dọa, rủi ro và điểm yếu.

Securing an organization and its assets from threats, risks, and vulnerabilities is an important step in maintaining business operations. In my experience as a security analyst, I helped respond to a severe breach that cost the organization nearly $250,000. So, I hope you're feeling motivated to continue your security journey. I know I'm excited. Let's get started!

Bảo vệ tổ chức và tài sản của tổ chức khỏi các mối đe dọa, rủi ro vàlỗ hổng là một bước quan trọng trong việc duy trì hoạt động kinh doanh.Theo kinh nghiệm của tôi với tư cách là nhà phân tích chứng khoán, tôi đã giúp giải quyết các vấn đềmột vi phạm nghiêm trọng khiến tổ chức này thiệt hại gần 250.000 USD.Vì vậy, tôi hy vọng bạn cảm thấy có động lực để tiếp tục hành trình bảo mật của mình.Tôi biết tôi rất vui mừng.Bắt đầu nào!

1.2. Course 2 overview – Tổng quan khóa 2

Module 1: Security domains
Phần 1: Miền bảo mật

Hello, and welcome to **Play It Safe: Manage Security Risks**, the second course in the Google Cybersecurity Certificate. You're on an exciting journey!

Xin chào và chào mừng bạn đến với **Chơi an toàn: Quản lý rủi ro bảo mật** , khóa học thứ hai trong Chứng chỉ an ninh mạng của Google. Bạn đang trên một hành trình thú vị!

By the end of this course, you will develop a greater understanding of the eight Certified Information Systems Security Professional (CISSP) security domains, as well as specific security frameworks and controls. You'll also be introduced to how to use security tools and audits to help protect assets and data. These are key concepts in the cybersecurity field, and understanding them will help you keep organizations, and the people they serve, safe from threats, risks, and vulnerabilities.

Đến cuối khóa học này, bạn sẽ hiểu rõ hơn về tám miền bảo mật của Chuyên gia bảo mật hệ thống thông tin được chứng nhận (CISSP), cũng như các khung và biện pháp kiểm soát bảo mật cụ thể. Bạn cũng sẽ được giới thiệu cách sử dụng các công cụ bảo mật và kiểm tra để giúp bảo vệ tài sản và dữ liệu. Đây là những khái niệm chính trong lĩnh vực an ninh mạng và việc hiểu chúng sẽ giúp bạn giữ cho các tổ chức và những người mà họ phục vụ được an toàn trước các mối đe dọa, rủi ro và lỗ hổng bảo mật.

Certificate program progress

Tiến độ chương trình chứng chỉ

The Google Cybersecurity Certificate program has eight courses. **Play It Safe: Manage Security Risks** is the second course.

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. **Chơi an toàn: Quản lý rủi ro bảo mật** là khóa học thứ hai.

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.

Module 1: Security domains
Phần 1: Miền bảo mật

2. **Play It Safe: Manage Security Risks** — *(current course)* 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.

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.

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 vai trò và trách nhiệm an ninh mạng cấp cơ bản.

2. **Chơi an toàn: Quản lý rủi ro bảo mật** — *(khóa học hiện tại)* Xác định cách các chuyên gia an ninh mạng sử dụng các 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** - Hiểu biết về các lỗ hổng ở cấp độ mạng và cách bảo mật mạng.

4. **Công cụ giao dịch: 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 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. **Âm thanh báo động: Phát hiện và phản hồi** — 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.

Module 1: Security domains
Phần 1: Miền bảo mật

7. **Tự động hóa các tác vụ an ninh mạng với Python** — 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** — 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 2 content

Nội dung khóa 2

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.

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

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.

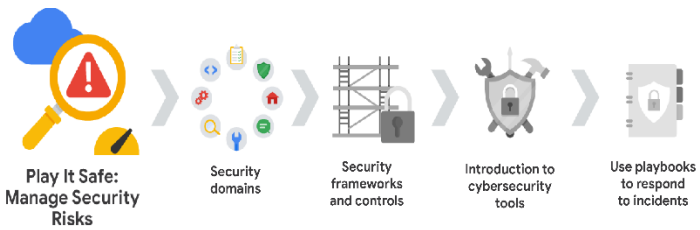
Điều gì sẽ đến? Dưới đây là tổng quan nhanh về các kỹ năng bạn sẽ học trong mỗi mô-đun của khóa học này.

Module 1: Security domains

You will gain understanding of the CISSP's eight security domains. Then, you'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, you'll explore the National Institute of Standards and Technology's (NIST) Risk Management Framework and the steps of risk management.

Mô-đun 1: Miền bảo mật

Bạn sẽ hiểu rõ hơn về tám lĩnh vực bảo mật của CISSP. Sau đó, bạn sẽ tìm hiểu về các mối đe dọa, rủi ro và lỗ hổng chính đối với hoạt động kinh doanh. Ngoài ra, bạn sẽ khám phá Khung quản lý rủi ro của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) và các bước quản lý rủi ro.



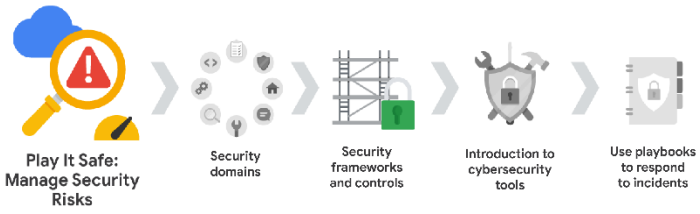
Module 1: Security domains
Phần 1: Miền bảo mật

Module 2: Security frameworks and controls

You will focus on security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. You'll learn about Open Web Application Security Project (OWASP) security principles and security audits.

Mô-đun 2: Khung bảo mật và kiểm soát

Bạn sẽ tập trung vào các khuôn khổ và biện pháp kiểm soát bảo mật, cùng với các thành phần cốt lõi của bộ ba bảo mật, tính toàn vẹn và tính khả dụng (CIA). Bạn sẽ tìm hiểu về các nguyên tắc bảo mật và kiểm tra bảo mật của Dự án bảo mật ứng dụng web mở (OWASP).

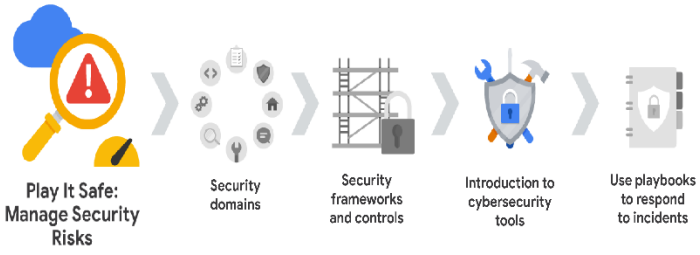


Module 3: Introduction to cybersecurity tools

You will explore industry leading security information and event management (SIEM) tools that are used by security professionals to protect business operations. You'll learn how entry-level security analysts use SIEM dashboards as part of their every day work.

Mô-đun 3: Giới thiệu các công cụ an ninh mạng

Bạn sẽ khám phá các công cụ quản lý sự kiện và thông tin bảo mật (SIEM) hàng đầu trong ngành được các chuyên gia bảo mật sử dụng để bảo vệ hoạt động kinh doanh. Bạn sẽ tìm hiểu cách các nhà phân tích bảo mật cấp đầu vào sử dụng bảng thông tin SIEM như một phần công việc hàng ngày của họ.



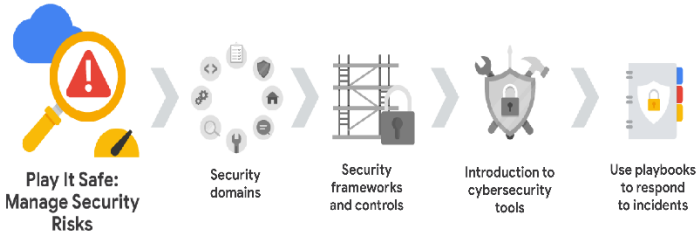
Module 4: Use playbooks to respond to incidents

Module 1: Security domains
Phần 1: Miền bảo mật

You'll learn about the purposes and common uses of playbooks. You'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

Mô-đun 4: Sử dụng cẩm nang để ứng phó với sự cố

Bạn sẽ tìm hiểu về mục đích và cách sử dụng phổ biến của playbook. Bạn cũng sẽ khám phá cách các chuyên gia an ninh mạng sử dụng cẩm nang để ứng phó với các mối đe dọa, rủi ro và lỗ hổng đã xác định.



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**.**
- **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 kiến với những người học khác trong khóa học.diễn đàn thảo luận**.**
- **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 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 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 trongTài nguyênchuyển 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 theoQuy tắc ứng xử của Courserađể 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.

Course completion to obtain a certificate

Hoàn thành khóa học để được cấp chứng chỉ

To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:

- Pay the course certificate fee or apply and be approved for a Coursera scholarship.
- Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course.

Để gửi bài tập đã chấm điểm và đủ điều kiện nhận Chứng chỉ an ninh mạng của Google, bạn phải:

- Tralệ phí cấp chứng chỉ khóa họchoặc đăng ký và được chấp thuận tham gia Courserahọc bổng.
- Vượt qua tất cả các câu hỏi được chấm điểm trong tám khóa học với số điểm ít nhất là 80%. Mỗi bài kiểm tra được chấm điểm trong một khóa học là một phần của điểm tích lũy cho khóa học đó.

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:

- **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.

Module 1: Security domains
Phần 1: Miền bảo mật

- **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 to ask for help from other learners taking this program. You can also visit Coursera's Global Online Community. Other important things to know while learning with others can be found in the Coursera Honor Code and Code of Conduct.

- **Update your profile:** Consider updating your 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.

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:

- **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 được 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 dụngdiễn đàn thảo luậnđể yêu cầu sự giúp đỡ từ những người học khác tham gia chương trình này. Bạn cũng có thể ghé thăm Coursera'sCộng đồng trực tuyến toàn cầu. Những điều quan trọng khác cần biết khi học cùng người khác có thể được tìm thấy trongMã danh dự CourseraVàQuy tắc ứng xử.

- **Cập nhật hồ sơ của bạn:** Hãy xem xétcập nhật hồ sơ của bantrên 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:

- Microsoft Word: Help and learning: Microsoft Support page for Word
- Google Docs: Help Center page for Google Docs
- Microsoft Excel: Help and learning: Microsoft Support page for Excel
- Google Sheets: Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning: Microsoft Support page for PowerPoint
- How to use Google Slides: Help Center page for Google Slides
- Common problems with labs: Troubleshooting help for Qwiklabs activities

Module 1: Security domains
Phần 1: Miền bảo mật

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: Trợ giúp và học tập: Trang hỗ trợ của Microsoft dành cho Word
- Google Tài liệu: Trang Trung tâm trợ giúp dành cho Google Documents
- Microsoft Excel: Trợ giúp và học tập: Trang hỗ trợ của Microsoft dành cho Excel
- Google Trang tính: Trang Trung tâm trợ giúp dành cho Google Trang tính
- Microsoft PowerPoint: Trợ giúp và học tập: Trang hỗ trợ của Microsoft dành cho PowerPoint
- Cách sử dụng Google Trang trình bày: Trang Trung tâm trợ giúp dành cho Google Trang trình bày
- Các vấn đề thường gặp với phòng thí nghiệm: 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:

- **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.

Module 1: Security domains
Phần 1: Miền bảo mật

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 section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.

- Cybersecurity Certificate glossary

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:

- **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 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.

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 nguyênphần. 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

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.

- Click **thumbs-up** for materials you find helpful.

Module 1: Security domains
Phần 1: Miền bảo mật

- Click **thumbs-down** for materials that you do not find helpful.

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.

For technical help, visit the Learner Help Center.

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.

- Hãy **nhấp vào biểu tượng thích** đối với những tài liệu bạn thấy hữu ích.
- Hãy **nhấp vào biểu tượng không thích** đối với những tài liệu mà bạn thấy không hữu ích.

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.

Để được trợ giúp kỹ thuật, hãy truy cậpTrung tâm trợ giúp người học.

1.4. Connect with your classmates – Kết nối với các bạn cùng lớp của bạn

2. More about the CISSP security domains – Tìm hiểu thêm về các miền bảo mật CISSP

2.1. Welcome to module 1 – Chào mừng đến với module 1

The world of security, which we also refer to as cybersecurity throughout this program, is vast. So making sure that you have the knowledge, skills, and tools to successfully navigate this world is why we're here.

Thế giới an ninh, mà chúng tôi còn gọi làan ninh mạng trong suốt chương trình này là rất lớn.Vì vậy, hãy chắc chắn rằng bạn có kiến thức, kỹ năng vàcông cụ để định hướng thành công thế giới này là lý do chúng tôi có mặt ở đây.

In the following videos, you'll learn about the focus of CISSP's eight security domains. Then, we'll discuss threats, risks, and vulnerabilities in more detail. We'll

also introduce you to the three layers of the web and share some examples to help you understand the different types of attacks that we'll discuss throughout the program. Finally, we'll examine how to manage risks by using the National Institute of Standards and Technology's Risk Management Framework, known as the NIST RMF.

Trong các video tiếp theo,bạn sẽ tìm hiểu về trọng tâm của tám miền bảo mật của CISSP.Sau đó, chúng ta sẽ thảo luận chi tiết hơn về các mối đe dọa, rủi ro và lỗ hổng.Chúng tôi cũng sẽ giới thiệu cho bạn ba lớp của web vàchia sẻ một số ví dụ để giúp bạn hiểu các loại tấn công khác nhau mà chúng tôi sẽthảo luận xuyên suốt chương trình.Cuối cùng, chúng ta sẽ xem xét cách quản lý rủi ro bằng cách sử dụng Viện Nghiên cứu Quốc gia vềKhung quản lý rủi ro của Tiêu chuẩn và Công nghệ, được gọi là NIST RMF.

Because these topics and related technical skills are considered core knowledge in the security field, continuing to build your understanding of them will help you mitigate and manage the risks and threats that organizations face on a daily basis.

Bởi vì những chủ đề này vàkỹ năng kỹ thuật liên quan được coi là kiến thức cốt lõi trong lĩnh vực an ninh,tiếp tục xây dựng sự hiểu biết của bạn về chúng sẽ giúp bạn giảm thiểu vàquản lý các rủi ro và mối đe dọa mà các tổ chức phải đối mặt hàng ngày.

In the next video, we'll further discuss the focus of the eight security domains introduced in the first course.

Trong video tiếp theo, chúng ta sẽ thảo luận sâu hơn về trọng tâm của tám biện pháp bảo mậttên miền được giới thiệu trong khóa học đầu tiên.

2.2. Explore the CISSP security domains, Part 1 – Khám phá các miền bảo mật CISSP, Phần 1

Welcome back! You might remember from course one that there are eight security domains, or categories, identified by CISSP. Security teams use them to organize daily tasks and identify gaps in security that could cause negative consequences for an organization, and to establish their security posture. Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

Module 1: Security domains
Phần 1: Miền bảo mật

Chào mừng trở lại!Bạn có thể nhớ từ khóa học thứ nhất rằng có tám lĩnh vực hoặc danh mục bảo mật,được xác định bởi CISSP.Đội ngũ an ninh sử dụng chúng để tổ chức các công việc hàng ngày vàxác định các lỗ hổng bảo mật có thể gây ra hậu quả tiêu cực chomột tổ chức và để thiết lập tình trạng an ninh của họ.Tình trạng an ninh đề cập đến khả năng của một tổ chức để quản lýnó bảo vệ các tài sản và dữ liệu quan trọng và phản ứng với sự thay đổi.

In this video, we'll discuss the focus of the first four domains: security and risk management, asset security, security architecture and engineering, and communication and network security.

Trong video này, chúng ta sẽ thảo luận trọng tâm của bốn lĩnh vực đầu tiên:an ninh và quản lý rủi ro, bảo mật tài sản,kiến trúc và kỹ thuật an ninh, an ninh mạng và truyền thông.

The first domain is security and risk management. There are several areas of focus for this domain: defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations. Let's discuss each area of focus in more detail.

Lĩnh vực đầu tiên là bảo mật và quản lý rủi ro.Có một số lĩnh vực trọng tâm cho miền này:xác định các mục tiêu và mục tiêu an ninh, giảm thiểu rủi ro,tuân thủ, tính liên tục trong kinh doanh và các quy định pháp luật.Hãy thảo luận chi tiết hơn về từng lĩnh vực trọng tâm.

By defining security goals and objectives, organizations can reduce risks to critical assets and data like PII, or personally identifiable information. Risk mitigation means having the right procedures and rules in place to quickly reduce the impact of a risk like a breach. Compliance is the primary method used to develop an organization's internal security policies, regulatory requirements, and independent standards. Business continuity relates to an organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

Bằng cách xác định các mục tiêu và mục tiêu an ninh,tổ chức có thể giảm thiểu rủi ro đối với tài sản và dữ liệu quan trọngnhư PII hoặc thông tin nhận dạng cá nhân.Giảm thiểu rủi ro có nghĩa là có các quy trình và quy tắc phù hợptại chỗ để nhanh chóng giảm

thiểu tác động của rủi ro như vi phạm.Tuân thủ là phương pháp chính được sử dụng để phát triển nội bộ của một tổ chứcchính sách bảo mật, các yêu cầu pháp lý và các tiêu chuẩn độc lập.Tính liên tục trong kinh doanh liên quan đến khả năng của tổ chức trong việc duy trìnăng suất hàng ngày của họ bằng cách thiết lập các kế hoạch khắc phục rủi ro sau thảm họa.

And finally, while laws related to security and risk management are different worldwide, the overall goals are similar. As a security professional, this means following rules and expectations for ethical behavior to minimize negligence, abuse, or fraud.

Và cuối cùng, trong khi các luật liên quan đến an ninh vàquản lý rủi ro là khác nhau trên toàn thế giới, các mục tiêu tổng thể là tương tự nhau.Là một chuyên gia bảo mật, điều này có nghĩa là tuân theo các quy tắc và kỳ vọng đối vớihành vi đạo đức để giảm thiểu sự cẩu thả, lạm dụng hoặc gian lận.

The next domain is asset security. The asset security domain is focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. This means that assets such as PII or SPII should be securely handled and protected, whether stored on a computer, transferred over a network like the internet, or even physically collected. Organizations also need to have policies and procedures that ensure data is properly stored, maintained, retained, and destroyed. Knowing what data you have and who has access to it is necessary for having a strong security posture that mitigates risk to critical assets and data.

Lĩnh vực tiếp theo là bảo mật tài sản.Miền bảo mật tài sản tập trung vào việc bảo mật tài sản vật lý và kỹ thuật số.Nó cũng liên quan đến việc lưu trữ, bảo trì,lưu giữ và hủy bỏ dữ liệu.Điều này có nghĩa là các tài sản như PII hoặc SPII phải được xử lý an toàn vàđược bảo vệ, cho dù được lưu trữ trên máy tính, được truyền quamột mạng như internet, hoặc thậm chí được thu thập về mặt vật lý.Các tổ chức cũng cần có các chính sách và thủ tục để đảm bảodữ liệu được lưu trữ, duy trì, giữ lại và hủy đúng cách.Biết dữ liệu nào bạn có và ai có quyền truy cập vào dữ liệu đó là cần thiết để cómột tư thế bảo mật mạnh mẽ giúp giảm thiểu rủi ro đối với các tài sản và dữ liệu quan trọng.

Previously, we provided a few examples that touched on the disposal of data. For example, an organization might have you, as a security analyst, oversee the destruction of hard drives to make sure that they're properly disposed of. This ensures that private data stored on those drives can't be accessed by threat actors.

Module 1: Security domains
Phần 1: Miền bảo mật

Trước đây, chúng tôi đã cung cấp một số ví dụ liên quan đến việc xử lý dữ liệu.Ví dụ: một tổ chức có thể yêu cầu bạn, với tư cách là nhà phân tích bảo mật, giám sátviệc tiêu hủy các ổ đĩa cứng để đảm bảo rằng chúng được xử lý đúng cách.Điều này đảm bảo rằng dữ liệu riêng tư được lưu trữ trên các ổ đĩa đó không thể bị truy cập bởi tác nhân đe dọa.

The third domain is security architecture and engineering. This domain is focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data. One of the core concepts of secure design architecture is shared responsibility. Shared responsibility means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security. By having policies that encourage users to recognize and report security concerns, many issues can be handled quickly and effectively.

Lĩnh vực thứ ba là kiến trúc và kỹ thuật bảo mật.Miền này tập trung vào việc tối ưu hóa bảo mật dữ liệu bằng cách đảm bảo các công cụ hiệu quả,các hệ thống và quy trình được áp dụng để bảo vệ tài sản và dữ liệu của tổ chức.Một trong những khái niệm cốt lõi của kiến trúc thiết kế an toàn là trách nhiệm được chia sẻ.Trách nhiệm chung có nghĩa là tất cả các cá nhân trongmột tổ chức đóng vai trò tích cực trong việc giảm thiểu rủi ro vàduy trì cả an ninh vật lý và ảo.Bằng việc có các chính sách khuyến khích người dùng nhận biết vàbáo cáo những lo ngại về bảo mật, nhiều vấn đề có thể được xử lý nhanh chóng và hiệu quả.

The fourth domain is communication and network security, which is mainly focused on managing and securing physical networks and wireless communications. Secure networks keep an organization's data and communications safe whether on-site, or in the cloud, or when connecting to services remotely.

Lĩnh vực thứ tư là truyền thông và an ninh mạng, chủ yếu làtập trung vào việc quản lý và bảo mật mạng vật lý và truyền thông không dây.Mạng an toàn giữ cho dữ liệu và thông tin liên lạc của tổ chức được an toàndù tại chỗ hay trên đám mây hay khi kết nối với các dịch vụ từ xa.

For example, employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public wifi hotspots. By having security team members remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be exploited by threat actors.

Ví dụ, nhân viên làm việc từ xa trong không gian công cộng cần phảiđược bảo vệ khỏi các lỗ hổng có thể xảy ra khi họ sử dụngkết nối bluetooth không an toàn hoặc các điểm truy cập wifi công cộng.Bằng cách yêu cầu các thành viên nhóm bảo mật loại bỏ quyền truy cập vào các loại thông tin liên lạc đócác kênh ở cấp độ tổ chức, nhân viên có thể nản lòngthực hành hành vi không an toàn có thể bị các tác nhân đe dọa khai thác.

Now that we've reviewed the focus of our first four domains, let's discuss the last four domains.

Bây giờ chúng ta đã xem xét trọng tâm của bốn miền đầu tiên,hãy thảo luận về bốn lĩnh vực cuối cùng.

2.3. Explore the CISSP security domains, Part 2 – Khám phá các miền bảo mật CISSP, Phần 2

In this video, we'll cover the last four domains: identity and access management, security assessment and testing, security operations, and software development security.

Trong video này, chúng tôi sẽ đề cập đến bốn miền cuối cùng:quản lý danh tính và quyền truy cập, đánh giá và kiểm tra bảo mật,hoạt động bảo mật và bảo mật phát triển phần mềm.

The fifth domain is identity and access management, or IAM. And it's focused on access and authorization to keep data secure by making sure users follow established policies to control and manage assets. As an entry-level analyst, it's essential to keep an organization's systems and data as secure as possible by ensuring user access is limited to what employees need. Basically, the goal of IAM is to reduce the overall risk to systems and data.

Miền thứ năm là quản lý danh tính và quyền truy cập, hay IAM.Và nó tập trung vào quyền truy cập và ủy quyền để giữ an toàn cho dữ liệu bằngđảm bảo người dùng tuân theo các chính sách đã thiết lập để kiểm soát và quản lý tài sản.Là một nhà phân tích cấp độ đầu vào, điều cần thiết là giữ cho hệ thống và dữ liệu của tổ chức luôn hoạt động tốt.an toàn nhất có thể bằng cách đảm bảo quyền truy cập của người dùng được giới hạn ở những gì nhân viên cần.Về cơ bản, mục tiêu của IAM là giảm rủi ro tổng thể đối với hệ thống và dữ liệu.

For example, if everyone at a company is using the same administrator login, there is no way to track who has access to what data. In the event of a breach, separating valid user activity from the threat actor would be impossible.

Ví dụ: nếu mọi người trong công ty đang sử dụng cùng một thông tin đăng nhập của quản trị viên,không có cách nào để theo dõi ai có quyền truy cập vào dữ liệu nào.Trong trường hợp vi phạm,việc tách hoạt động hợp lệ của người dùng khỏi tác nhân đe dọa là không thể.

There are four main components to IAM. Identification is when a user verifies who they are by providing a user name, an access card, or biometric data such as a fingerprint. Authentication is the verification process to prove a person's identity, such as entering a password or PIN. Authorization takes place after a user's identity has been confirmed and relates to their level of access, which depends on the role in the organization. Accountability refers to monitoring and recording user actions, like login attempts, to prove systems and data are used properly.

Có bốn thành phần chính của IAM.Nhận dạng là khi người dùng xác minh họ là ai bằng cách cung cấp tên người dùng,thẻ truy cập hoặc dữ liệu sinh trắc học như dấu vân tay.Xác thực là quá trình xác minh để chứng minh thông tin của một ngườidanh tính, chẳng hạn như nhập mật khẩu hoặc mã PIN.Việc ủy quyền diễn ra sau khi danh tính của người dùng đã được xác nhận vàliên quan đến mức độ tiếp cận của họ, điều này phụ thuộc vào vai trò trong tổ chức.Trách nhiệm đề cập đến việc giám sát và ghi lại hành động của người dùng,như các lần đăng nhập, để chứng minh hệ thống và dữ liệu được sử dụng đúng cách.

The sixth security domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security control testing can help an organization identify new and better ways to mitigate threats, risks, and vulnerabilities. This involves examining organizational goals and objectives, and evaluating if the controls being used actually achieve those goals. Collecting and analyzing security data regularly also helps prevent threats and risks to the organization.

Lĩnh vực bảo mật thứ sáu là đánh giá và kiểm tra bảo mật.Miền này tập trung vào việc tiến hành kiểm tra kiểm soát bảo mật,thu thập và phân tích dữ liệu, đồng thời tiến hành kiểm tra bảo mật để giám sátrủi ro, mối đe dọa và điểm yếu.Kiểm tra kiểm soát an ninh có thể giúp tổ chức xác định cáccách tốt hơn để giảm thiểu các mối đe dọa, rủi ro và lỗ hổng.Điều này liên quan đến việc kiểm tra các mục tiêu và mục tiêu của tổ chức,

vàđánh giá xem các biện pháp kiểm soát đang được sử dụng có thực sự đạt được các mục tiêu đó hay không.Việc thu thập và phân tích dữ liệu bảo mật thường xuyên cũng giúp ngăn ngừa các mối đe dọa vàrủi ro cho tổ chức.

Analysts might use security control testing evaluations and security assessment reports to improve existing controls or implement new controls. An example of implementing a new control could be requiring the use of multi-factor authentication to better protect the organization from potential threats and risks.

Các nhà phân tích có thể sử dụng các đánh giá kiểm tra kiểm soát an ninh và cácbáo cáo đánh giá để cải thiện các biện pháp kiểm soát hiện có hoặc triển khai các biện pháp kiểm soát mới.Một ví dụ về việc triển khai một biện pháp kiểm soát mới có thể yêu cầu sử dụng phương pháp phân tích đa yếu tốxác thực để bảo vệ tổ chức tốt hơn khỏi các mối đe dọa và rủi ro tiềm ẩn.

Next, let's discuss security operations. The security operations domain is focused on conducting investigations and implementing preventative measures. Investigations begin once a security incident has been identified. This process requires a heightened sense of urgency in order to minimize potential risks to the organization. If there is an active attack, mitigating the attack and preventing it from escalating further is essential for ensuring that private information is protected from threat actors.

Tiếp theo, hãy thảo luận về các hoạt động bảo mật.Lĩnh vực hoạt động an ninh tập trung vào việc tiến hành điều tra vàthực hiện các biện pháp phòng ngừa.Các cuộc điều tra bắt đầu khi một sự cố an ninh đã được xác định.Quá trình này đòi hỏi tính cấp bách cao độ để giảm thiểunhững rủi ro tiềm ẩn đối với tổ chức.Nếu có một cuộc tấn công đang diễn ra, việc giảm nhẹ cuộc tấn công vàngăn chặn nó leo thang hơn nữa là điều cần thiết chođảm bảo rằng thông tin cá nhân được bảo vệ khỏi các tác nhân đe dọa.

Once the threat has been neutralized, the collection of digital and physical evidence to conduct a forensic investigation will begin. A digital forensic investigation must take place to identify when, how, and why the breach occurred. This helps security teams determine areas for improvement and preventative measures that can be taken to mitigate future attacks.

Khi mối đe dọa đã được vô hiệu hóa, việc thu thập dữ liệu vật lý và kỹ thuật số sẽbằng chứng để tiến hành điều tra pháp y sẽ bắt đầu.Một cuộc điều tra pháp y kỹ thuật số phải được thực hiện để xác địnhkhi nào, như thế nào và tại sao vi phạm xảy ra.Điều này giúp

các nhóm bảo mật xác định các khu vực cần cải thiện vàcác biện pháp phòng ngừa có thể được thực hiện để giảm thiểu các cuộc tấn công trong tương lai.

The eighth and final security domain is software development security. This domain focuses on using secure coding practices. As you may remember, secure coding practices are recommended guidelines that are used to create secure applications and services. The software development lifecycle is an efficient process used by teams to quickly build software products and features. In this process, security is an additional step. By ensuring that each phase of the software development lifecycle undergoes security reviews, security can be fully integrated into the software product.

Lĩnh vực bảo mật thứ tám và cuối cùng là bảo mật phát triển phần mềm.Miền này tập trung vào việc sử dụng các phương pháp mã hóa an toàn.Như bạn có thể nhớ, các phương pháp mã hóa an toàn là những nguyên tắc được khuyến nghịđược sử dụng để tạo ra các ứng dụng và dịch vụ an toàn.Vòng đời phát triển phần mềm là một quy trình hiệu quả được các nhóm sử dụng đểnhanh chóng xây dựng các sản phẩm và tính năng phần mềm.Trong quá trình này, bảo mật là một bước bổ sung.Bằng cách đảm bảo rằng mỗi giai đoạn của vòng đời phát triển phần mềm đều trải quađánh giá bảo mật, bảo mật có thể được tích hợp hoàn toàn vào sản phẩm phần mềm.

For example, performing a secure design review during the design phase, secure code reviews during the development and testing phases, and penetration testing during the deployment and implementation phase ensures that security is embedded into the software product at every step. This keeps software secure and sensitive data protected, and mitigates unnecessary risk to an organization.

Ví dụ: thực hiện đánh giá thiết kế an toàn trong giai đoạn thiết kế,đánh giá mã an toàn trong giai đoạn phát triển và thử nghiệm,và thử nghiệm thâm nhập trong giai đoạn triển khai và triển khaiđảm bảo rằng tính bảo mật được nhúng vào sản phẩm phần mềm ở mọi bước.Điều này giúp phần mềm được an toàn và bảo vệ dữ liệu nhạy cảm, đồng thờigiảm thiểu rủi ro không cần thiết cho tổ chức.

Being familiar with these domains can help you better understand how they're used to improve the overall security of an organization and the critical role security teams play. Next, we'll discuss security threats, risks, and vulnerabilities, including ransomware, and introduce you to the three layers of the web.

Làm quen với những miền này có thể giúp bạn hiểu rõ hơn về cách chúng hoạt độngđược sử dụng để cải thiện an ninh tổng thể của một tổ chức vàvai trò quan trọng

của đội an ninh.Tiếp theo, chúng ta sẽ thảo luận về các mối đe dọa, rủi ro và lỗ hổng bảo mật,bao gồm cả ransomware và giới thiệu cho bạn ba lớp của web.

2.4. Security domains cybersecurity analysts need to know – Các lĩnh vực bảo mật mà nhà phân tích an ninh mạng cần biết

Security domains cybersecurity analysts need to know

Các lĩnh vực bảo mật mà nhà phân tích an ninh mạng cần biết

As an analyst, you can explore various areas of cybersecurity that interest you. One way to explore those areas is by understanding different security domains and how they're used to organize the work of security professionals. In this reading you will learn more about CISSP's eight security domains and how they relate to the work you'll do as a security analyst.

Với tư cách là nhà phân tích, bạn có thể khám phá nhiều lĩnh vực an ninh mạng khác nhau mà bạn quan tâm. Một cách để khám phá những lĩnh vực đó là tìm hiểu các lĩnh vực bảo mật khác nhau và cách chúng được sử dụng để tổ chức công việc của các chuyên gia bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu thêm về tám lĩnh vực bảo mật của CISSP và cách chúng liên quan đến công việc bạn sẽ làm với tư cách là nhà phân tích bảo mật.

Domain one: Security and risk management

Module 1: Security domains
Phần 1: Miền bảo mật

Tên miền một: Bảo mật và quản lý rủi ro

All organizations must develop their security posture. Security posture is an organization’s ability to manage its defense of critical assets and data and react to change. Elements of the security and risk management domain that impact an organization's security posture include:

- Security goals and objectives
- Risk mitigation processes
- Compliance
- Business continuity plans
- Legal regulations
- Professional and organizational ethics

Information security, or InfoSec, is also related to this domain and refers to a set of processes established to secure information. An organization may use playbooks and implement training as a part of their security and risk management program, based on their needs and perceived risk. There are many InfoSec design processes, such as:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

As an example, a security team may need to alter how personally identifiable information (PII) is treated in order to adhere to the European Union's General Data Protection Regulation (GDPR).

Tất cả các tổ chức phải phát triển tư thế bảo mật của mình. Tình trạng bảo mật là khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi. Các yếu tố của miền quản lý rủi ro và bảo mật ảnh hưởng đến trạng thái bảo mật của tổ chức bao gồm:

- Mục đích và mục tiêu an ninh
- Quy trình giảm thiểu rủi ro

- Sự tuân thủ
- Kế hoạch kinh doanh liên tục
- Quy định pháp luật
- Đạo đức nghề nghiệp và tổ chức

Bảo mật thông tin, hay InfoSec, cũng liên quan đến lĩnh vực này và đề cập đến một tập hợp các quy trình được thiết lập để bảo mật thông tin. Một tổ chức có thể sử dụng cẩm nang và triển khai đào tạo như một phần của chương trình quản lý rủi ro và bảo mật của họ, dựa trên nhu cầu và rủi ro nhận thấy của họ. Có nhiều quy trình thiết kế InfoSec, chẳng hạn như:

- Ứng phó sự cố
- Quản lý lỗ hổng
- Bảo mật ứng dụng
- Bảo mật đám mây
- An ninh cơ sở hạ tầng

Ví dụ: nhóm bảo mật có thể cần thay đổi cách xử lý thông tin nhận dạng cá nhân (PII) để tuân thủ Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu (GDPR).

Domain two: Asset security

Lĩnh vực thứ hai: Bảo đảm tài sản

Asset security involves managing the cybersecurity processes of organizational assets, including the storage, maintenance, retention, and destruction of physical and virtual data. Because the loss or theft of assets can expose an organization and increase the level of risk, keeping track of assets and the data they hold is essential. Conducting a security impact analysis, establishing a recovery plan, and managing data exposure will depend on the level of risk associated with each asset. Security analysts may need to store, maintain, and retain data by creating backups to ensure they are able to restore the environment if a security incident places the organization’s data at risk.

Bảo mật tài sản liên quan đến việc quản lý các quy trình an ninh mạng của tài sản tổ chức, bao gồm lưu trữ, bảo trì, lưu giữ và tiêu hủy dữ liệu vật lý và ảo. Bởi vì việc mất mát hoặc trộm cắp tài sản có thể khiến tổ chức bị lộ và làm tăng mức độ rủi ro nên việc

theo dõi tài sản và dữ liệu chúng nắm giữ là điều cần thiết. Việc tiến hành phân tích tác động bảo mật, thiết lập kế hoạch khôi phục và quản lý việc tiếp xúc với dữ liệu sẽ tùy thuộc vào mức độ rủi ro liên quan đến từng tài sản. Các nhà phân tích bảo mật có thể cần lưu trữ, duy trì và giữ lại dữ liệu bằng cách tạo bản sao lưu để đảm bảo họ có thể khôi phục môi trường nếu sự cố bảo mật khiến dữ liệu của tổ chức gặp rủi ro.

Domain three: Security architecture and engineering

Miền thứ ba: Kiến trúc và kỹ thuật bảo mật

This domain focuses on managing data security. Ensuring effective tools, systems, and processes are in place helps protect an organization’s assets and data. Security architects and engineers create these processes.

One important aspect of this domain is the concept of shared responsibility. Shared responsibility means all individuals involved take an active role in lowering risk during the design of a security system. Additional design principles related to this domain, which are discussed later in the program, include:

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

An example of managing data is the use of a security information and event management (SIEM) tool to monitor for flags related to unusual login or user activity that could indicate a threat actor is attempting to access private data.

Miền này tập trung vào việc quản lý bảo mật dữ liệu. Việc đảm bảo có sẵn các công cụ, hệ thống và quy trình hiệu quả sẽ giúp bảo vệ tài sản và dữ liệu của tổ chức. Các kiến trúc sư và kỹ sư bảo mật tạo ra các quy trình này.

Module 1: Security domains
Phần 1: Miền bảo mật

Một khía cạnh quan trọng của lĩnh vực này là khái niệm về trách nhiệm chung. Trách nhiệm chung có nghĩa là tất cả các cá nhân liên quan đều đóng vai trò tích cực trong việc giảm thiểu rủi ro trong quá trình thiết kế hệ thống bảo mật. Các nguyên tắc thiết kế bổ sung liên quan đến lĩnh vực này, sẽ được thảo luận sau trong chương trình, bao gồm:

- Mô hình hóa mối đe dọa
- Đặc quyền nhất
- Phòng thủ có chiều sâu
- Thất bại một cách an toàn
- Tách biệt nhiệm vụ
- Giữ nó đơn giản
- Không tin tưởng
- Tin tưởng nhưng xác minh

Một ví dụ về quản lý dữ liệu là việc sử dụng công cụ quản lý sự kiện và thông tin bảo mật (SIEM) để theo dõi các cờ liên quan đến hoạt động đăng nhập hoặc hoạt động của người dùng bất thường có thể cho thấy tác nhân đe dọa đang cố truy cập dữ liệu riêng tư.

Domain four: Communication and network security

Lĩnh vực 4: Truyền thông và an ninh mạng

This domain focuses on managing and securing physical networks and wireless communications. This includes on-site, remote, and cloud communications.

Organizations with remote, hybrid, and on-site work environments must ensure data remains secure, but managing external connections to make certain that remote workers are securely accessing an organization’s networks is a challenge. Designing network security controls—such as restricted network access—can help protect users and ensure an organization’s network remains secure when employees travel or work outside of the main office.

Miền này tập trung vào việc quản lý và bảo mật mạng vật lý và truyền thông không dây. Điều này bao gồm thông tin liên lạc tại chỗ, từ xa và đám mây.

Module 1: Security domains
Phần 1: Miền bảo mật

Các tổ chức có môi trường làm việc từ xa, kết hợp và tại chỗ phải đảm bảo dữ liệu được an toàn, nhưng việc quản lý các kết nối bên ngoài để đảm bảo rằng nhân viên từ xa truy cập an toàn vào mạng của tổ chức là một thách thức. Thiết kế các biện pháp kiểm soát bảo mật mạng—chẳng hạn như quyền truy cập mạng bị hạn chế—có thể giúp bảo vệ người dùng và đảm bảo mạng của tổ chức vẫn an toàn khi nhân viên đi du lịch hoặc làm việc bên ngoài văn phòng chính.

Domain five: Identity and access management

Miền năm: Quản lý danh tính và quyền truy cập

The identity and access management (IAM) domain focuses on keeping data secure. It does this by ensuring user identities are trusted and authenticated and that access to physical and logical assets is authorized. This helps prevent unauthorized users, while allowing authorized users to perform their tasks.

Essentially, IAM uses what is referred to as the principle of least privilege, which is the concept of granting only the minimal access and authorization required to complete a task. As an example, a cybersecurity analyst might be asked to ensure that customer service representatives can only view the private data of a customer, such as their phone number, while working to resolve the customer's issue; then remove access when the customer's issue is resolved.

Miền quản lý danh tính và truy cập (IAM) tập trung vào việc giữ an toàn cho dữ liệu. Nó thực hiện điều này bằng cách đảm bảo danh tính người dùng được tin cậy và xác thực cũng như quyền truy cập vào các tài sản vật lý và logic được cấp phép. Điều này giúp ngăn chặn những người dùng trái phép, đồng thời cho phép người dùng được ủy quyền thực hiện nhiệm vụ của mình.

Về cơ bản, IAM sử dụng nguyên tắc được gọi là nguyên tắc đặc quyền tối thiểu, tức là khái niệm chỉ cấp quyền truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ. Ví dụ: nhà phân tích an ninh mạng có thể được yêu cầu đảm bảo rằng đại diện dịch vụ khách hàng chỉ có thể xem dữ liệu riêng tư của khách hàng, chẳng hạn như số điện thoại của họ, trong khi làm việc để giải quyết vấn đề của khách hàng; sau đó xóa quyền truy cập khi vấn đề của khách hàng được giải quyết.

Domain six: Security assessment and testing

Lĩnh vực thứ sáu: Đánh giá và kiểm tra bảo mật

Module 1: Security domains
Phần 1: Miền bảo mật

The security assessment and testing domain focuses on identifying and mitigating risks, threats, and vulnerabilities. Security assessments help organizations determine whether their internal systems are secure or at risk. Organizations might employ penetration testers, often referred to as “pen testers,” to find vulnerabilities that could be exploited by a threat actor.

This domain suggests that organizations conduct security control testing, as well as collect and analyze data. Additionally, it emphasizes the importance of conducting security audits to monitor for and reduce the probability of a data breach. To contribute to these types of tasks, cybersecurity professionals may be tasked with auditing user permissions to validate that users have the correct levels of access to internal systems.

Miền đánh giá và kiểm tra bảo mật tập trung vào việc xác định và giảm thiểu rủi ro, mối đe dọa và lỗ hổng. Đánh giá bảo mật giúp các tổ chức xác định xem hệ thống nội bộ của họ có an toàn hay đang gặp rủi ro hay không. Các tổ chức có thể sử dụng người kiểm tra thâm nhập, thường được gọi là “người kiểm tra bút”, để tìm ra các lỗ hổng có thể bị kẻ đe dọa khai thác.

Miền này đề xuất các tổ chức tiến hành kiểm tra kiểm soát bảo mật cũng như thu thập và phân tích dữ liệu. Ngoài ra, nó nhấn mạnh tầm quan trọng của việc tiến hành kiểm tra bảo mật để giám sát và giảm khả năng vi phạm dữ liệu. Để đóng góp vào các loại nhiệm vụ này, các chuyên gia an ninh mạng có thể được giao nhiệm vụ kiểm tra quyền của người dùng để xác thực rằng người dùng có cấp độ truy cập chính xác vào hệ thống nội bộ.

Domain seven: Security operations

Lĩnh vực thứ bảy: Hoạt động an ninh

The security operations domain focuses on the investigation of a potential data breach and the implementation of preventative measures after a security incident has occurred. This includes using strategies, processes, and tools such as:

- Training and awareness
- Reporting and documentation
- Intrusion detection and prevention
- SIEM tools

- Log management
- Incident management
- Playbooks
- Post-breach forensics
- Reflecting on lessons learned

The cybersecurity professionals involved in this domain work as a team to manage, prevent, and investigate threats, risks, and vulnerabilities. These individuals are trained to handle active attacks, such as large amounts of data being accessed from an organization's internal network, outside of normal working hours. Once a threat is identified, the team works diligently to keep private data and information safe from threat actors.

Miền hoạt động bảo mật tập trung vào việc điều tra vi phạm dữ liệu tiềm ẩn và thực hiện các biện pháp phòng ngừa sau khi xảy ra sự cố bảo mật. Điều này bao gồm việc sử dụng các chiến lược, quy trình và công cụ như:

- Đào tạo và nhận thức
- Báo cáo và tài liệu
- Phát hiện và ngăn chặn xâm nhập
- công cụ SIEM
- Quản lý nhật ký
- Quản lý sự cố
- Sách chơi
- Pháp y sau vi phạm
- Suy ngẫm về bài học kinh nghiệm

Các chuyên gia an ninh mạng tham gia vào lĩnh vực này làm việc như một nhóm để quản lý, ngăn chặn và điều tra các mối đe dọa, rủi ro và lỗ hổng bảo mật. Những cá nhân này được đào tạo để xử lý các cuộc tấn công đang hoạt động, chẳng hạn như một lượng lớn dữ liệu được truy cập từ mạng nội bộ của tổ chức, ngoài giờ làm việc bình thường. Sau khi xác định được mối đe dọa, nhóm sẽ nỗ lực làm việc để giữ an toàn cho dữ liệu và thông tin riêng tư khỏi các tác nhân đe dọa.

Domain eight: Software development security

Module 1: Security domains
Phần 1: Miền bảo mật

Miền thứ tám: Bảo mật phát triển phần mềm

The software development security domain is focused on using secure programming practices and guidelines to create secure applications. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users.

Security must be incorporated into each element of the software development life cycle, from design and development to testing and release. To achieve security, the software development process must have security in mind at each step. Security cannot be an afterthought.

Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly. Having a system in place to test the programming conventions, software executables, and security measures embedded in the software is necessary. Having quality assurance and pen tester professionals ensure the software has met security and performance standards is also an essential part of the software development process. For example, an entry-level analyst working for a pharmaceutical company might be asked to make sure encryption is properly configured for a new medical device that will store private patient data.

Lĩnh vực bảo mật phát triển phần mềm tập trung vào việc sử dụng các hướng dẫn và thực tiễn lập trình an toàn để tạo ra các ứng dụng an toàn. Việc sở hữu các ứng dụng bảo mật sẽ giúp cung cấp các dịch vụ an toàn và đáng tin cậy, giúp bảo vệ các tổ chức và người dùng của họ.

Bảo mật phải được tích hợp vào từng yếu tố của vòng đời phát triển phần mềm, từ thiết kế và phát triển đến thử nghiệm và phát hành. Để đạt được bảo mật, quy trình phát triển phần mềm phải lưu ý đến bảo mật ở mỗi bước. An ninh không thể là một suy nghĩ lại.

Thực hiện kiểm tra bảo mật ứng dụng có thể giúp đảm bảo các lỗ hổng được xác định và giảm thiểu tương ứng. Cần có một hệ thống để kiểm tra các quy ước lập trình, khả năng thực thi phần mềm và các biện pháp bảo mật được nhúng trong phần mềm. Việc có các chuyên gia kiểm tra bút và đảm bảo chất lượng đảm bảo phần mềm đáp ứng các tiêu chuẩn về hiệu suất và bảo mật cũng là một phần thiết yếu của quá trình phát triển phần mềm. Ví dụ: một nhà phân tích cấp đầu vào làm việc cho một công ty dược phẩm có thể được yêu cầu đảm bảo mã hóa được cấu hình đúng cách cho một thiết bị y tế mới sẽ lưu trữ dữ liệu riêng tư của bệnh nhân.

Key takeaways

Module 1: Security domains
Phần 1: Miền bảo mật

Bài học chính

In this reading, you learned more about the focus areas of the eight CISSP security domains. In addition, you learned about InfoSec and the principle of least privilege. Being familiar with these security domains and related concepts will help you gain insight into the field of cybersecurity.

Trong bài đọc này, bạn đã tìm hiểu thêm về các lĩnh vực trọng tâm của tám miền bảo mật CISSP. Ngoài ra, bạn đã tìm hiểu về InfoSec và nguyên tắc đặc quyền tối thiểu. Làm quen với các lĩnh vực bảo mật này và các khái niệm liên quan sẽ giúp bạn hiểu rõ hơn về lĩnh vực an ninh mạng.

2.5. Ashley: My path to cybersecurity – Ashley: Con đường đến với an ninh mạng của tôi

My name is Ashley and my role at Google is CE Enablement Lead for SecOps sales. All that means is I help set up training for customer engineers that support our products. Grew up with a computer, loved the Internet. I have one of the earliest AOL screen names in history and I'm very proud of that. My dad is an engineer and I think there was always an interest in tech. But when I got out of high school, there wasn't a clear path to get there. It wasn't a linear path at all. I was a knucklehead growing up. I gave up in 10th grade and I just didn't care for a long time and I was getting in trouble a lot and I pretty much told myself if I don't join the military and get out of here, I will probably not be here in about 2-3 years if I continue down this path. I joined the army right out of high school, graduated in June, and four days later I was at bootcamp at Fort Jackson, South Carolina as a trumpet player, believe it or not, I come back and had to get a job and was not even tracking on tech jobs or anything like that. I was pulling in carts for a big hardware store, selling video games, retail, box slinger for a freight company. All of that stuff has happened before I even figured out that tech was an option. The military was kind enough to retrain me in IT, and that's kind of how I actually got the official first wave of schooling to be able to actually say, hey, I have the skills to at least be a PC technician. I went back to community college and I actually did find a cybersecurity associates degree program, worked on some certifications. I went to my first DEFCON, which is a big hacking conference, and that set off a light bulb, I think to actually get that clarity on what the path could look like. I landed my first security analyst job back in 2017 and I went to a Veterans Training Program at my last company that was free for vets and ended up getting hired out of the training. I was with that company for almost five years before I came to Google. If you're new and you're just coming in, you have to know how to work with a team. I think a lot of us learned that in customer service settings. Some of the skills I learned working in retail, dealing with hard customers, learning how to even talk to people or diffuse a situation if people are upset about things, just learning how to talk to people. In IT we need that. It's no longer just the tech skills we need, the more T-shaped which they're soft skills, there's people skills, and there's technical skills. You have to have good analysis skills, and again, it doesn't even have to be

technical analysis, if you can read a book and pick apart the rhetorical devices of that story, you can do analysis work. I didn't have to be a software engineer to work in this field. For many of us, there's like a math fear, programming is a big hurdle, but we work with people, we work with processes, and you don't necessarily need to have that coding knowledge to understand people or processes. There's so many ways to break in, so do not get discouraged and don't be scared to think outside of the box to get your foot in the door.

Tên tôi là Ashley và vai trò của tôi tại Googlelà Trưởng nhóm hỗ trợ CE cho hoạt động bán hàng SecOps.Tất cả điều đó có nghĩa là tôi giúp thiết lập chương trình đào tạodành cho các kỹ sư khách hàng hỗ trợ sản phẩm của chúng tôi.Lớn lên với máy tính, yêu thích Internet.Tôi có một trong những tên màn hình AOL sớm nhấttrong lịch sử và tôi rất tự hào về điều đó.Bố tôi là một kỹ sư vàTôi nghĩ luôn có sự quan tâm đến công nghệ.Nhưng khi tôi tốt nghiệp trung học,không có một con đường rõ ràng để đạt được điều đó.Đó hoàn toàn không phải là một con đường tuyến tính.Tôi là một kẻ ngu ngốc khi lớn lên.Tôi đã bỏ cuộc vào năm lớp 10 và tôi đã không làm vậyquan tâm trong một thời gian dài và tôi đã nhận đượcgặp rắc rối rất nhiều và tôi đã nói khá nhiềubản thân tôi nếu tôi không gia nhập quân đội và rời khỏi đây,Có lẽ tôi sẽ không ở đâykhoảng 2-3 năm nếu tôi tiếp tục đi theo con đường này.Tôi gia nhập quân đội ngay từtrung học, tốt nghiệp vào tháng 6,và bốn ngày sau tôi tham gia chương trình đào tạo ở Fort Jackson,Nam Carolina với tư cách là người chơi kèn,tin hay không thì tùy, tôi quay lại và phải lấymột công việc và không phảithậm chí theo dõi các công việc kỹ thuật hoặc bất cứ điều gì tương tự.Tôi đang kéo xe cho một cửa hàng kim khí lớn,bán trò chơi điện tử, bán lẻ,hộp slinger cho một công ty vận chuyển hàng hóa.Tất cả những điều đó đã xảy ratrước khi tôi nhận ra rằng công nghệ là một lựa chọn.Quân đội đã rất tốt bụng khi đào tạo lại tôi về CNTT,và đó là cách tôi thực sự có đượclàn sóng đầu tiên chính thứcvề việc đi học để có thể thực sự nói,này, tôi có đủ kỹ năng để trở thành một kỹ thuật viên PC.Tôi quay lại trường cao đẳng cộng đồng và tôi thực sựđã tìm thấy một chương trình cấp bằng cao đẳng an ninh mạng,đã làm việc trên một số chứng chỉ.Tôi đã tham dự DEFCON đầu tiên của mình,đó là một hội nghị hack lớn,và điều đó làm bật lên một bóng đèn,Tôi nghĩ để thực sự có đượcsự rõ ràng về con đường có thể trông như thế nào.Tôi đã có được công việc phân tích bảo mật đầu tiên của mìnhtrở lại năm 2017 và tôi đã đi đếnChương trình đào tạo cựu chiến binh ở công ty gần đây nhất của tôinó miễn phí cho bác sĩ thú y và cuối cùngđược tuyển dụng ra khỏi khóa đào tạo.Tôi đã làm việc với công ty đó tronggần năm năm trước khi tôi đến với Google.Nếu bạn là người mới và vừa mới gia nhập,bạn phải biết cách làm việc với một nhóm.Tôi nghĩ nhiều người trong chúng ta đã học được điều đótrong cài đặt dịch vụ khách hàng.Một số kỹ năng tôi học được khi làm việc trong lĩnh vực bán lẻ,đối phó với những khách hàng khó tính,học cách nói chuyện với mọi người hoặc khuếch tánmột tình huống khi mọi người khó chịu về một điều gì đó,chỉ đang học cách nói chuyện với mọi người.Trong CNTT chúng tôi cần điều đó.Chúng ta không chỉ cần những kỹ năng công nghệ nữa,kỹ năng mềm càng có hình chữ T,có kỹ năng con người và có kỹ năng kỹ thuật.Bạn phải có kỹ năng phân tích tốt,và một lần nữa, nó thậm chí khôngphải là phân tích kỹ thuật,nếu bạn có thể đọc một cuốn sách và chọnngoài những biện pháp tu từ của câu chuyện đó,bạn có thể làm công việc phân tích.Tôi không cần phải như vậymột kỹ sư phần mềm làm việc trong lĩnh vực này.Đối với nhiều người trong chúng ta, nó giống như nỗi sợ toán học,lập trình là một trở ngại lớn,nhưng chúng tôi làm việc với mọi người,chúng tôi làm việc với các quy trình,và bạn không nhất thiết phải cókiến thức mã hóa đó để hiểu con người hoặc

quy trình.Có rất nhiều cách để đột nhập,vì vậy đừng nản lòng và đừng sợ hãihãy suy nghĩ sáng tạo để đặt chân vào cửa.

2.6. Identify: CISSP's eight security domains – Xác định: tám miền bảo mật của CISSP

Area of focus	CISSP security domain
Securing assets; storage, maintenance, retention, and destruction of data	Asset security
Managing and securing physical networks and wireless communications	Communication and network security
Security goals and objectives, risk mitigation, compliance, business continuity, and the law	Security and risk management
Optimizing data security by using effective tools, systems, and processes	Security architecture and engineering
Using secure coding practices to create secure applications and services	Software development security
Conducting security control testing and audits, collecting and analyzing data	Security assessment and testing
Using access, authorization, and established policies to secure data and manage assets	Identity and access management
Conducting investigations and implementing preventative measures	Security operations

2.7. Test your knowledge: More about the CISSP security domains – Kiểm tra kiến thức của bạn: Tìm hiểu thêm về các miền bảo mật CISSP

3. Navigate threats, risks, and vulnerabilities – Điều hướng các mối đe dọa, rủi ro và lỗ hổng

3.1. Threats, risks, and vulnerabilities – Các mối đe dọa, rủi ro và lỗ hổng

As an entry-level security analyst, one of your many roles will be to handle an organization's digital and physical assets. As a reminder, an asset is an item perceived as having value to an organization. During their lifespan, organizations acquire all types of assets, including physical office spaces, computers, customers' PII,

intellectual property, such as patents or copyrighted data, and so much more. Unfortunately, organizations operate in an environment that presents multiple security threats, risks, and vulnerabilities to their assets. Let's review what threats, risks, and vulnerabilities are and discuss some common examples of each.

Với tư cách là nhà phân tích bảo mật cấp mới vào, một trong nhiều vai trò của bạn sẽ là xử lýtài sản vật lý và kỹ thuật số của một tổ chức.Như một lời nhắc nhở,một tài sản là một vật phẩm được coi là có giá trị đối với một tổ chức.Trong suốt vòng đời của mình, các tổ chức có được tất cả các loại tài sản, bao gồm cảkhông gian văn phòng vật lý, máy tính, PII của khách hàng, sở hữu trí tuệ,chẳng hạn như bằng sáng chế hoặc dữ liệu có bản quyền, v.v.Thật không may, các tổ chức hoạt động trong một môi trường có nhiềunhiều mối đe dọa, rủi ro và lỗ hổng bảo mật đối với tài sản của họ.Hãy xem xét các mối đe dọa, rủi ro và lỗ hổng là gì vàthảo luận về một số ví dụ phổ biến của mỗi.

A threat is any circumstance or event that can negatively impact assets. One example of a threat is a social engineering attack. Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Malicious links in email messages that look like they're from legitimate companies or people is one method of social engineering known as phishing. As a reminder, phishing is a technique that is used to acquire sensitive data, such as user names, passwords, or banking information.

Mối đe dọa là bất kỳ tình huống hoặc sự kiện nào có thể tác động tiêu cực đến tài sản.Một ví dụ về mối đe dọa là một cuộc tấn công kỹ thuật xã hội.Kỹ thuật xã hội là một kỹ thuật thao túng khai thác lỗi của con ngườiđể có được thông tin cá nhân, quyền truy cập hoặc vật có giá trị.Các liên kết độc hại trong email trông giống như từ các công ty hợp pháphoặc con người là một phương pháp kỹ thuật xã hội được gọi là lừa đảo.Xin nhắc lại, lừa đảo là một kỹ thuật được sử dụng để thu thập dữ liệu nhạy cảm,chẳng hạn như tên người dùng, mật khẩu hoặc thông tin ngân hàng.

Risks are different from threats. A risk is anything that can impact the confidentiality, integrity, or availability of an asset. Think of a risk as the likelihood of a threat occurring. An example of a risk to an organization might be the lack of backup protocols for making sure its stored information can be recovered in the event of an accident or security incident. Organizations tend to rate risks at different levels: low, medium, and high, depending on possible threats and the value of an asset.

Rủi ro khác với đe dọa.Rủi ro là bất cứ điều gì có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn,hoặc sự sẵn có của một tài sản.Hãy coi rủi ro là khả năng xảy ra mối đe dọa.Một ví dụ về rủi ro đối với tổ chức có thể là việc thiếu các giao thức dự phòng chođảm bảo thông tin được lưu trữ có thể được phục hồi trong trường hợp xảy ra tai nạn

hoặcsự cố an ninh.Các tổ chức có xu hướng đánh giá rủi ro ở các mức độ khác nhau: thấp, trung bình,và cao, tùy thuộc vào các mối đe dọa có thể xảy ra và giá trị của tài sản.

A low-risk asset is information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised. This includes public information such as website content, or published research data.

Tài sản có rủi ro thấp là thông tin không gây tổn hại đến danh tiếng của tổ chức hoặchoạt động đang diễn ra và sẽ không gây ra thiệt hại tài chính nếu bị xâm phạm.Điều này bao gồm thông tin công khai như nội dung trang web hoặcdữ liệu nghiên cứu được công bố.

A medium-risk asset might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations. For example, the early release of a company's quarterly earnings could impact the value of their stock.

Tài sản có rủi ro trung bình có thể bao gồm thông tin không có sẵncho công chúng và có thể gây ra một số thiệt hại cho tài chính của tổ chức,danh tiếng hoặc các hoạt động đang diễn ra.Ví dụ: việc công bố sớm thu nhập hàng quý của công ty có thể ảnh hưởng đếngiá trị cổ phiếu của họ.

A high-risk asset is any information protected by regulations or laws, which if compromised, would have a severe negative impact on an organization's finances, ongoing operations, or reputation. This could include leaked assets with SPII, PII, or intellectual property.

Tài sản có rủi ro cao là bất kỳ thông tin nào được bảo vệ bởi các quy định hoặc pháp luật,mà nếu bị xâm phạm sẽ có tác động tiêu cực nghiêm trọng đếntài chính, hoạt động đang diễn ra hoặc danh tiếng của một tổ chức.Điều này có thể bao gồm các tài sản bị rò rỉ với SPII, PII,hoặc sở hữu trí tuệ.

Now, let's discuss vulnerabilities. A vulnerability is a weakness that can be exploited by a threat. And it's worth noting that both a vulnerability and threat must be present for there to be a risk. Examples of vulnerabilities include: an outdated firewall, software, or application; weak passwords; or unprotected confidential data. People can also be considered a vulnerability. People's actions can significantly affect an

organization's internal network. Whether it's a client, external vendor, or employee, maintaining security must be a united effort.

Bây giờ, hãy thảo luận về các lỗ hổng.Lỗ hổng là điểm yếu có thể bị khai thác bởi mối đe dọa.Và điều đáng chú ý là cả lỗ hổng vàmối đe dọa phải hiện diện thì mới có rủi ro.Ví dụ về các lỗ hổng bảo mật bao gồm: tường lửa, phần mềm hoặcứng dụng; mật khẩu yếu; hoặc dữ liệu bí mật không được bảo vệ.Con người cũng có thể được coi là một điểm dễ bị tổn thương.Hành động của mọi người có thể ảnh hưởng đáng kể đến mạng nội bộ của tổ chức.Cho dù đó là khách hàng, nhà cung cấp bên ngoài hay nhân viên,duy trì an ninh phải là một nỗ lực thống nhất.

So entry-level analysts need to educate and empower people to be more security conscious. For example, educating people on how to identify a phishing email is a great starting point. Using access cards to grant employee access to physical spaces while restricting outside visitors is another good security measure. Organizations must continually improve their efforts when it comes to identifying and mitigating vulnerabilities to minimize threats and risks. Entry-level analysts can support this goal by encouraging employees to report suspicious activity and actively monitoring and documenting employees' access to critical assets.

Vì vậy, các nhà phân tích cấp đầu vào cần phải đào tạo vàtrao quyền cho mọi người có ý thức bảo mật hơn.Ví dụ: hướng dẫn mọi người cách xác định email lừa đảo là điểm khởi đầu tuyệt vời.Sử dụng thẻ ra vào để cấp cho nhân viên quyền truy cập vào các không gian vật lý trong khihạn chế du khách bên ngoài là một biện pháp an ninh tốt khác.Các tổ chức phải liên tục cải thiện những nỗ lực của mình khi nói đếnxác định và giảm thiểu các lỗ hổng để giảm thiểu các mối đe dọa và rủi ro.Các nhà phân tích cấp mới vào có thể hỗ trợ mục tiêu này bằng cách khuyến khích nhân viênbáo cáo hoạt động đáng ngờ và tích cực theo dõi vàghi lại quyền truy cập của nhân viên vào các tài sản quan trọng.

Now that you're familiar with some of the threats, risks, and vulnerabilities analysts frequently encounter, coming up, we'll discuss how they impact business operations.

Bây giờ bạn đã quen với một số mối đe dọa, rủi ro vàcác nhà phân tích lỗ hổng thường gặp phải,sắp tới, chúng ta sẽ thảo luận về cách chúng tác động đến hoạt động kinh doanh.

3.2. Key impacts of threats, risks, and vulnerabilities – Tác động chính của các mối đe dọa, rủi ro và lỗ hổng

Module 1: Security domains
Phần 1: Miền bảo mật

In this video, we'll discuss an expensive type of malware called ransomware. Then we'll cover three key impacts of threats, risks, and vulnerabilities on organizational operations.

Trong video này, chúng ta sẽ thảo luận về một loại phần mềm độc hại đắt tiền có tên là ransomware.Sau đó chúng ta sẽ đề cập đến ba tác động chính của các mối đe dọa, rủi ro vànhững lỗ hổng trong hoạt động của tổ chức.

Ransomware is a malicious attack where threat actors encrypt an organization's data then demand payment to restore access. Once ransomware is deployed by an attacker, it can freeze network systems, leave devices unusable, and encrypt, or lock confidential data, making devices inaccessible. The threat actor then demands a ransom before providing a decryption key to allow organizations to return to their normal business operations. Think of a decryption key as a password provided to regain access to your data. Note that when ransom negotiations occur or data is leaked by threat actors, these events can occur through the dark web.

Ransomware là một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóadữ liệu của tổ chức sau đó yêu cầu thanh toán để khôi phục quyền truy cập.Khi ransomware được kẻ tấn công triển khai,nó có thể đóng băng hệ thống mạng, khiến các thiết bị không thể sử dụng được vàmã hóa hoặc khóa dữ liệu bí mật, khiến thiết bị không thể truy cập được.Sau đó, kẻ đe dọa sẽ yêu cầu một khoản tiền chuộc trước khi cung cấp khóa giải mãđể cho phép các tổ chức trở lại hoạt động kinh doanh bình thường của họ.Hãy coi khóa giải mã như một mật khẩu được cung cấp để lấy lại quyền truy cập vào dữ liệu của bạn.Lưu ý rằng khi các cuộc đàm phán về tiền chuộc diễn ra hoặc dữ liệu bị rò rỉ bởi các tác nhân đe dọa,những sự kiện này có thể xảy ra thông qua web đen.

While many people use search engines to navigate to their social media accounts or to shop online, this is only a small part of what the web really is. The web is actually an interlinked network of online content that's made up of three layers: the surface web, the deep web, and the dark web.

Trong khi nhiều người sử dụng công cụ tìm kiếm để điều hướng đến tài khoản truyền thông xã hội của họ hoặcđể mua sắm trực tuyến, đây chỉ là một phần nhỏ trong bản chất thực sự của web.Web thực sự là một mạng lưới nội dung trực tuyến được liên kết với nhauđược tạo thành từ ba lớp: web bề mặt, web sâu và web tối.

Module 1: Security domains
Phần 1: Miền bảo mật

The surface web is the layer that most people use. It contains content that can be accessed using a web browser.

Surface web là lớp được nhiều người sử dụng nhất.Nó chứa nội dung có thể được truy cập bằng trình duyệt web.

The deep web generally requires authorization to access it. An organization's intranet is an example of the deep web, since it can only be accessed by employees or others who have been granted access.

Deep web thường yêu cầu ủy quyền để truy cập nó.Mạng nội bộ của một tổ chức là một ví dụ về deep web,vì nó chỉ có thể được truy cập bởi nhân viên hoặc những người khác đã được cấp quyền truy cập.

Lastly, the dark web can only be accessed by using special software. The dark web generally carries a negative connotation since it is the preferred web layer for criminals because of the secrecy that it provides.

Cuối cùng, trang web tối chỉ có thể được truy cập bằng phần mềm đặc biệt.Trang web tối thường mang ý nghĩa tiêu cực vì nó được ưa thíchlớp web dành cho tội phạm vì tính bí mật mà nó cung cấp.

Now, let's discuss three key impacts of threats, risks, and vulnerabilities. The first impact we'll discuss is financial impact. When an organization's assets are compromised by an attack, such as the use of malware, the financial consequences can be significant for a variety of reasons. These can include interrupted production and services, the cost to correct the issue, and fines if assets are compromised because of non-compliance with laws and regulations.

Bây giờ, hãy thảo luận về ba tác động chính của các mối đe dọa, rủi ro và lỗ hổng.Tác động đầu tiên chúng ta sẽ thảo luận là tác động tài chính.Khi tài sản của tổ chức bị xâm phạm bởi một cuộc tấn công, chẳng hạn như việc sử dụngcủa phần mềm độc hại, hậu quả tài chính có thể rất lớn vì nhiều lý do.Chúng có thể bao gồm việc sản xuất và dịch vụ bị gián đoạn,chi phí để khắc phục vấn đề và tiền phạt nếu tài sản bị xâm phạmvì không tuân thủ pháp luật và các quy định.

The second impact is identity theft. Organizations must decide whether to store private customer, employee, and outside vendor data, and for how long. Storing any type of sensitive data presents a risk to the organization. Sensitive data can include personally identifiable information, or PII, which can be sold or leaked through the dark web. That's because the dark web provides a sense of secrecy and threat actors may have the ability to sell data there without facing legal consequences.

Tác động thứ hai là đánh cắp danh tính.Các tổ chức phải quyết định có nên lưu trữ thông tin khách hàng cá nhân,dữ liệu về nhân viên và nhà cung cấp bên ngoài cũng như trong bao lâu.Việc lưu trữ bất kỳ loại dữ liệu nhạy cảm nào đều gây rủi ro cho tổ chức.Dữ liệu nhạy cảm có thể bao gồm thông tin nhận dạng cá nhân hoặcPII, có thể được bán hoặc rò rỉ qua web đen.Đó là bởi vì web đen mang lại cảm giác bí mật và những kẻ đe dọa có thểcó khả năng bán dữ liệu ở đó mà không phải đối mặt với hậu quả pháp lý.

The last impact we'll discuss is damage to an organization's reputation. A solid customer base supports an organization's mission, vision, and financial goals. An exploited vulnerability can lead customers to seek new business relationships with competitors or create bad press that causes permanent damage to an organization's reputation. The loss of customer data doesn't only affect an organization's reputation and financials, it may also result in legal penalties and fines. Organizations are strongly encouraged to take proper security measures and follow certain protocols to prevent the significant impact of threats, risks, and vulnerabilities. By using all the tools in their toolkit, security teams are better prepared to handle an event such as a ransomware attack.

Tác động cuối cùng mà chúng ta sẽ thảo luận là tổn hại đến danh tiếng của tổ chức.Cơ sở khách hàng vững chắc hỗ trợ sứ mệnh của tổ chức,tầm nhìn và mục tiêu tài chính.Một lỗ hổng bị khai thác có thể khiến khách hàng tìm kiếm hoạt động kinh doanh mớimối quan hệ với đối thủ cạnh tranh hoặctạo ra những tin tức xấu gây tổn hại vĩnh viễn đến danh tiếng của tổ chức.Việc mất dữ liệu khách hàng không chỉ ảnh hưởng đến uy tín của tổ chức vàtài chính, nó cũng có thể dẫn đến hình phạt và tiền phạt pháp lý.Các tổ chức được khuyến khích thực hiện các biện pháp an ninh thích hợp vàtuân theo các giao thức nhất định để ngăn chặn tác động đáng kể của các mối đe dọa,rủi ro và tình trạng dễ bị tổn thương.Bằng cách sử dụng tất cả các công cụ trong bộ công cụ của mình, các nhóm bảo mật sẽ hoạt động tốt hơnsẵn sàng xử lý một sự kiện như một cuộc tấn công bằng ransomware.

Coming up, we'll cover the NIST risk management framework's seven steps for managing risk.

Sắp tới, chúng tôi sẽ đề cập đến khung quản lý rủi ro của NISTbảy bước để quản lý rủi ro.

3.3. Herbert: Manage threats, risks, and vulnerabilities – Herbert: Quản lý các mối đe dọa, rủi ro và lỗ hổng

My name is Herbert and I am a Security Engineer at Google. I think I've always been interested in security, in high school our school gave us these huge Dell laptops. There wasn't a whole lot of security within those computers. So, many of my friends would have cracked versions of like video games like Halo, that's really where I learned how to start manipulating computers to kind of do what I want. I guess [LAUGH] my day to day consists of analyzing security risks and providing solutions to those risks. A typical task for cybersecurity analysts would usually be something like exceptions requests. Analyzing if someone needs to have special access to a device or document based on the role that the person has or the project that they're working on. One of the more common threats that we come across is misconfigurations or requesting access for something that you don't really need. For example, I recently had a case where a vendor we were working with had changed their OAuth scope requests. And basically that means that they were requesting more permissions to use Google services than they had before in the past. We weren't sure really how to go about that because that wasn't a situation we've come across before. So it's still ongoing, but we're working with partner teams to kind of develop a solution for that. I think another thing that we've seen is outdated systems, machines that need to be patched. That sounds like an IT issue, but it's also definitely a cybersecurity issue. Having outdated machines, not having proper device management policies, working with a team or many teams is a huge part of the job. In order to get really anything done, you need to communicate with not just the team that you're a part of, but with other teams. Ten years ago I was working at a pizza joint and ten years later, here I am, at Google as a Security Engineer. If I told my 16 year old self that I would be here, I wouldn't have believed myself, but it is possible.

Tên tôi là Herbert và tôi là Kỹ sư bảo mật tại Google.Tôi nghĩ tôi luôn quan tâm đến vấn đề an ninh,ở trường trung học, trường chúng tôi đã cho chúng tôi những chiếc máy tính xách tay Dell khổng lồ này.Không có nhiều biện pháp bảo mật trong những máy tính đó.Vì vậy, nhiều người bạn của tôi chắc hẳn đã có phiên bản bẻ khóa của các trò chơi điện tử như Halo,đó thực sự là nơi tôi học cách bắt đầu thao tác với máy tính để làm những việcTôi muốn.Tôi đoán [CƯỜI] công việc hàng ngày của tôi bao gồm việc phân tích các rủi ro bảo mật vàđưa ra giải pháp khắc phục những rủi ro đó.Một nhiệm vụ điển hình chocác nhà phân tích an ninh mạng thường sẽ đưa ra những yêu cầu giống như ngoại lệ.Phân tích xem ai đó có cần quyền truy cập đặc biệt vào thiết bị hoặc tài liệu khôngdựa trên vai trò của người đó hoặc dự án mà họ đang thực hiện.Một trong những mối đe dọa phổ biến nhất mà chúng tôi gặp phải là cấu hình sai hoặcyêu cầu quyền truy cập vào thứ gì đó mà bạn không thực sự cần.Ví dụ: gần đây tôi gặp trường hợp một nhà cung cấp mà chúng tôiđang làm việc đã thay đổi yêu cầu phạm vi OAuth của họ.Và về cơ bản điều đó có nghĩa là họ đang yêu cầu nhiều quyền hơn để sử dụng Googledịch vụ hơn những gì họ đã có trước đây.Chúng tôi thực sự không chắc chắn về

cách thực hiện điều đó bởi vì đó không phải làmột tình huống mà chúng tôi đã gặp phải trước đây.Vì vậy, nó vẫn đang tiếp diễn, nhưngchúng tôi đang làm việc với các nhóm đối tác để phát triển giải pháp cho vấn đề đó.Tôi nghĩ một điều khác mà chúng ta đã thấy là các hệ thống lỗi thời,những máy cần được vá lỗi.Nghe có vẻ giống như một vấn đề về CNTT nhưng chắc chắn đây cũng là một vấn đề về an ninh mạng.Máy móc lạc hậu, không có chính sách quản lý thiết bị phù hợp,làm việc với một nhóm hoặc nhiều nhóm là một phần quan trọng của công việc.Để thực sự hoàn thành được mọi việc, bạn cần giao tiếp không chỉ với nhómmà bạn là thành viên nhưng với các nhóm khác.Mười năm trước tôi đang làm việc tại một cửa hàng pizza và mười năm sau,tôi ở đây, tại Google với tư cách là Kỹ sư bảo mật.Nếu tôi nói với bản thân mình lúc 16 tuổi rằng tôi sẽ ở đây,Tôi sẽ không tin bản thân mình, nhưng điều đó là có thể.

3.4. NIST's Risk Management Framework – Khung quản lý rủi ro của NIST

As you might remember from earlier in the program, the National Institute of Standards and Technology, NIST, provides many frameworks that are used by security professionals to manage risks, threats, and vulnerabilities.

Như bạn có thể nhớ ở phần trước của chương trình,Viện Tiêu chuẩn và Công nghệ Quốc gia,NIST, cung cấp nhiều khung công tác được sử dụng bởicác chuyên gia bảo mật để quản lýrủi ro, mối đe dọa và điểm yếu.

In this video, we're going to focus on NIST's Risk Management Framework or RMF. As an entry-level analyst, you may not engage in all of these steps, but it's important to be familiar with this framework. Having a solid foundational understanding of how to mitigate and manage risks can set yourself apart from other candidates as you begin your job search in the field of security.

Trong video này, chúng ta sẽ tập trung vàoKhung quản lý rủi ro của NIST hoặc RMF.Là một nhà phân tích cấp đầu vào,bạn có thể không tham gia vào tất cả các bước này,nhưng điều quan trọng là phải làm quen với khuôn khổ này.Có nền tảng hiểu biết vững chắcvề cách giảm thiểu và quản lý rủi ro có thểtạo sự khác biệt với các ứng viên khác khi bạnbắt đầu tìm kiếm việc làm của bạn trong lĩnh vực an ninh.

There are seven steps in the RMF: prepare, categorize, select, implement, assess, authorize, and monitor.

Có bảy bước trong RMF: chuẩn bị, phân loại,lựa chọn, thực hiện, đánh giá, ủy quyền và giám sát.

Module 1: Security domains
Phần 1: Miền bảo mật

Let's start with Step one, prepare. Prepare refers to activities that are necessary to manage security and privacy risks before a breach occurs. As an entry-level analyst, you'll likely use this step to monitor for risks and identify controls that can be used to reduce those risks.

Hãy bắt đầu với Bước một, chuẩn bị.Chuẩn bị đề cập đến các hoạt động cần thiết để quản lýrủi ro về bảo mật và quyền riêng tư trước khi vi phạm xảy ra.Là một nhà phân tích cấp đầu vào,bạn có thể sẽ sử dụng bước này để theo dõi rủi ro vàxác định các biện pháp kiểm soát có thể được sử dụng để giảm thiểu những rủi ro đó.

Step two is categorize, which is used to develop risk management processes and tasks. Security professionals then use those processes and develop tasks by thinking about how the confidentiality, integrity, and availability of systems and information can be impacted by risk. As an entry-level analyst, you'll need to be able to understand how to follow the processes established by your organization to reduce risks to critical assets, such as private customer information.

Bước hai là phân loại,được sử dụng để phát triểnquy trình và nhiệm vụ quản lý rủi ro.Các chuyên gia bảo mật sau đó sử dụng các quy trình đó vàphát triển các nhiệm vụ bằng cách suy nghĩ về cách thức bảo mật,tính toàn vẹn và tính sẵn có củahệ thống và thông tin có thể bị ảnh hưởng bởi rủi ro.Là một nhà phân tích cấp đầu vào,bạn sẽ cần có khả năng hiểu làm thế nàotuân theo các quy trình đã được thiết lậpbởi tổ chức của bạn để giảm thiểu rủi ro đối vớitài sản quan trọng, chẳng hạn như thông tin khách hàng cá nhân.

Step three is select. Select means to choose, customize, and capture documentation of the controls that protect an organization. An example of the select step would be keeping a playbook up-to-date or helping to manage other documentation that allows you and your team to address issues more efficiently.

Bước ba là chọn.Select có nghĩa là lựa chọn, tùy chỉnh,và nắm bắt tài liệu củacác biện pháp kiểm soát để bảo vệ một tổ chức.Một ví dụ về bước chọn sẽ được giữmột cẩm nang được cập nhật hoặc giúp đỡquản lý các tài liệu khác cho phép bạn vànhóm của bạn để giải quyết vấn đề hiệu quả hơn.

Step four is to implement security and privacy plans for the organization. Having good plans in place is essential for minimizing the impact of ongoing security risks.

For example, if you notice a pattern of employees constantly needing password resets, implementing a change to password requirements may help solve this issue.

Bước bốn là thực hiệnkế hoạch bảo mật và quyền riêng tư cho tổ chức.Có kế hoạch tốt là điều cần thiết chogiảm thiểu tác động của các rủi ro bảo mật đang diễn ra.Ví dụ: nếu bạn nhận thấy một mô hìnhnhân viên liên tục cần đặt lại mật khẩu,thực hiện một sự thay đổi đối vớiyêu cầu mật khẩu có thể giúp giải quyết vấn đề này.

Step five is assess. Assess means to determine if established controls are implemented correctly. An organization always wants to operate as efficiently as possible. So it's essential to take the time to analyze whether the implemented protocols, procedures, and controls that are in place are meeting organizational needs. During this step, analysts identify potential weaknesses and determine whether the organization's tools, procedures, controls, and protocols should be changed to better manage potential risks.

Bước năm là đánh giá.Đánh giá có nghĩa là để xác định xemcác biện pháp kiểm soát đã thiết lập được thực hiện một cách chính xác.Một tổ chức luôn mong muốnđể hoạt động hiệu quả nhất có thể.Vì vậy, điều cần thiết là phải dành thời gian đểphân tích xem các giao thức được triển khai,các thủ tục và biện pháp kiểm soát có trongnơi đang đáp ứng nhu cầu tổ chức.Trong bước này, nhà phân tích xác địnhnhững điểm yếu tiềm ẩn và xác địnhliệu các công cụ của tổ chức,thủ tục, kiểm soát,và các giao thức nên đượcthay đổi để quản lý tốt hơn các rủi ro tiềm ẩn.

Step six is authorize. Authorize means being accountable for the security and privacy risks that may exist in an organization. As an analyst, the authorization step could involve generating reports, developing plans of action, and establishing project milestones that are aligned to your organization's security goals.

Bước sáu là ủy quyền.Ủy quyền có nghĩa là chịu trách nhiệm vềnhững rủi ro về bảo mật và quyền riêng tư màcó thể tồn tại trong một tổ chức.Với tư cách là một nhà phân tích,bước ủy quyền có thể liên quan đến việc tạo báo cáo,xây dựng các kế hoạch hành động,và thiết lập các mốc quan trọng của dự ánphù hợp với mục tiêu bảo mật của tổ chức bạn.

Step seven is monitor. Monitor means to be aware of how systems are operating. Assessing and maintaining technical operations are tasks that analysts complete daily. Part of maintaining a low level of risk for an organization is knowing how the current

systems support the organization's security goals. If the systems in place don't meet those goals, changes may be needed.

Bước bảy là giám sát.Giám sát có nghĩa là để biết hệ thống đang hoạt động như thế nào.Đánh giá và duy trì hoạt động kỹ thuậtlà những nhiệm vụ mà các nhà phân tích hoàn thành hàng ngày.Một phần của việc duy trì mức độ thấprủi ro đối với một tổ chức làbiết hệ thống hiện tại hỗ trợ như thế nàomục tiêu an ninh của tổ chức.Nếu hệ thống hiện có không đáp ứng được những mục tiêu đó,những thay đổi có thể cần thiết.

Although it may not be your job to establish these procedures, you will need to make sure they're working as intended so that risks to the organization itself, and the people it serves, are minimized.

Mặc dù nó có thể khôngcông việc của bạn là thiết lập các thủ tục này,bạn sẽ cần phải chắc chắnhọ đang làm việc như dự định nênrủi ro cho bản thân tổ chức,và những người mà nó phục vụ được giảm thiểu.

3.5. Manage common threats, risks, and vulnerabilities – Khung quản lý rủi ro của NIST

Manage common threats, risks, and vulnerabilities

Quản lý các mối đe dọa, rủi ro và lỗ hổng phổ biến

Previously, you learned that security involves protecting organizations and people from threats, risks, and vulnerabilities. Understanding the current threat landscapes gives organizations the ability to create policies and processes designed to help prevent and mitigate these types of security issues. In this reading, you will further explore how to manage risk and some common threat actor tactics and techniques, so you are better prepared to protect organizations and the people they serve when you enter the cybersecurity field.

Trước đây, bạn đã biết rằng bảo mật bao gồm việc bảo vệ các tổ chức và con người khỏi các mối đe dọa, rủi ro và lỗ hổng bảo mật. Hiểu được bối cảnh mối đe dọa hiện tại mang lại cho các tổ chức khả năng tạo ra các chính sách và quy trình được thiết kế để giúp ngăn chặn và giảm thiểu các loại vấn đề bảo mật này. Trong bài đọc này, bạn sẽ khám phá thêm cách quản lý rủi ro cũng như một số chiến thuật và kỹ thuật của tác nhân đe dọa phổ biến, để bạn có sự chuẩn bị tốt hơn để bảo vệ các tổ chức và những người mà họ phục vụ khi bạn tham gia vào lĩnh vực an ninh mạng.

Risk management

Quản lý rủi ro

A primary goal of organizations is to protect assets. An **asset** is an item perceived as having value to an organization. Assets can be digital or physical. Examples of digital assets include the personal information of employees, clients, or vendors, such as:

- Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
- Dates of birth
- Bank account numbers
- Mailing addresses

Examples of physical assets include:

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

Some common strategies used to manage risks include:

- **Acceptance**: Accepting a risk to avoid disrupting business continuity
- **Avoidance**: Creating a plan to avoid the risk altogether
- **Transference**: Transferring risk to a third party to manage
- **Mitigation**: Lessening the impact of a known risk

Additionally, organizations implement risk management processes based on widely accepted frameworks to help protect digital and physical assets from various threats, risks, and vulnerabilities. Examples of frameworks commonly used in the cybersecurity industry include the National Institute of Standards and Technology Risk Management Framework (NIST RMF) and Health Information Trust Alliance (HITRUST).

Following are some common types of threats, risks, and vulnerabilities you'll help organizations manage as a security professional.

Module 1: Security domains
Phần 1: Miền bảo mật

Mục tiêu chính của các tổ chức là bảo vệ tài sản. Tài **sản** là một vật phẩm được coi là có giá trị đối với một tổ chức. Tài sản có thể là kỹ thuật số hoặc vật lý. Ví dụ về tài sản kỹ thuật số bao gồm thông tin cá nhân của nhân viên, khách hàng hoặc nhà cung cấp, chẳng hạn như:

- Số An sinh Xã hội (SSN) hoặc số nhận dạng quốc gia duy nhất được cấp cho cá nhân
- Ngày sinh
- Số tài khoản ngân hàng
- Địa chỉ gửi thư

Ví dụ về tài sản vật chất bao gồm:

- Kiosk thanh toán
- May chủ
- Máy tính để bàn
- Không gian văn phòng

Một số chiến lược phổ biến được sử dụng để quản lý rủi ro bao gồm:

- **Chấp nhận** : Chấp nhận rủi ro để tránh làm gián đoạn hoạt động kinh doanh liên tục
- **Phòng tránh** : Lập kế hoạch để tránh hoàn toàn rủi ro
- **Chuyển giao** : Chuyển rủi ro cho bên thứ ba quản lý
- **Giảm nhẹ** : Giảm bớt tác động của một rủi ro đã biết

Ngoài ra, các tổ chức triển khai các quy trình quản lý rủi ro dựa trên các khuôn khổ được chấp nhận rộng rãi để giúp bảo vệ tài sản vật lý và kỹ thuật số khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau. Ví dụ về các khung thường được sử dụng trong ngành an ninh mạng bao gồm Khung quản lý rủi ro công nghệ và tiêu chuẩn quốc gia (NIST RMF) và Liên minh tin cậy thông tin y tế (HITRUST).

Sau đây là một số loại mối đe dọa, rủi ro và lỗ hổng phổ biến mà bạn sẽ giúp các tổ chức quản lý với tư cách là chuyên gia bảo mật.

Today’s most common threats, risks, and vulnerabilities

Các mối đe dọa, rủi ro và lỗ hổng phổ biến nhất hiện nay

Module 1: Security domains
Phần 1: Miền bảo mật

Threats

Các mối đe dọa

A **threat** is any circumstance or event that can negatively impact assets. As an entry-level security analyst, your job is to help defend the organization's assets from inside and outside threats. Therefore, understanding common types of threats is important to an analyst's daily work. As a reminder, common threats include:

- **Insider threats:** Staff members or vendors abuse their authorized access to obtain data that may harm an organization.
- **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

Mối **đe dọa** là bất kỳ tình huống hoặc sự kiện nào có thể tác động tiêu cực đến tài sản. Là nhà phân tích bảo mật cấp mới vào, công việc của bạn là giúp bảo vệ tài sản của tổ chức khỏi các mối đe dọa bên trong và bên ngoài. Do đó, việc hiểu các loại mối đe dọa phổ biến là điều quan trọng đối với công việc hàng ngày của nhà phân tích. Xin nhắc lại, các mối đe dọa phổ biến bao gồm:

- **Mối đe dọa từ nội bộ:** Nhân viên hoặc nhà cung cấp lạm dụng quyền truy cập được ủy quyền của họ để lấy dữ liệu có thể gây hại cho tổ chức.
- **Các mối đe dọa liên tục nâng cao (APT):** Tác nhân đe dọa duy trì quyền truy cập trái phép vào hệ thống trong một khoảng thời gian dài.

Risks

Rủi ro

A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. One way to think about this is that a risk is being late to work and threats are traffic, an accident, a flat tire, etc.

There are different factors that can affect the likelihood of a risk to an organization's assets, including:

- **External risk:** Anything outside the organization that has the potential to harm organizational assets, such as threat actors attempting to gain access to private information
- **Internal risk:** A current or former employee, vendor, or trusted partner who poses a security risk
- **Legacy systems:** Old systems that might not be accounted for or updated, but can still impact assets, such as workstations or old mainframe systems. For example, an organization might have an old vending machine that takes credit card payments or a workstation that is still connected to the legacy accounting system.
- **Multiparty risk:** Outsourcing work to third-party vendors can give them access to intellectual property, such as trade secrets, software designs, and inventions.
- **Software compliance/licensing:** Software that is not updated or in compliance, or patches that are not installed in a timely manner

There are many resources, such as the NIST, that provide lists of cybersecurity risks. Additionally, the Open Web Application Security Project (OWASP) publishes a standard awareness document about the top 10 most critical security risks to web applications, which is updated regularly.

Rủi **ro** là bất cứ điều gì có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của tài sản. Công thức cơ bản để xác định mức độ rủi ro là rủi ro bằng khả năng xảy ra mối đe dọa. Một cách để nghĩ về điều này là nguy cơ đi làm muộn và các mối đe dọa là giao thông, tai nạn, xẹp lốp, v.v.

Có nhiều yếu tố khác nhau có thể ảnh hưởng đến khả năng xảy ra rủi ro đối với tài sản của tổ chức, bao gồm:

- **Rủi ro bên ngoài:** Bất cứ điều gì bên ngoài tổ chức có khả năng gây tổn hại đến tài sản của tổ chức, chẳng hạn như các tác nhân đe dọa cố gắng truy cập thông tin cá nhân
- **Rủi ro nội bộ:** Nhân viên, nhà cung cấp hoặc đối tác đáng tin cậy hiện tại hoặc trước đây có nguy cơ bảo mật
- **Hệ thống kế thừa:** Các hệ thống cũ có thể không được tính toán hoặc cập nhật nhưng vẫn có thể ảnh hưởng đến tài sản, chẳng hạn như máy trạm hoặc hệ thống máy tính lớn cũ. Ví dụ: một tổ chức có thể có một máy bán hàng tự động cũ nhận thanh toán bằng thẻ tín dụng hoặc một máy trạm vẫn được kết nối với hệ thống kế toán cũ.

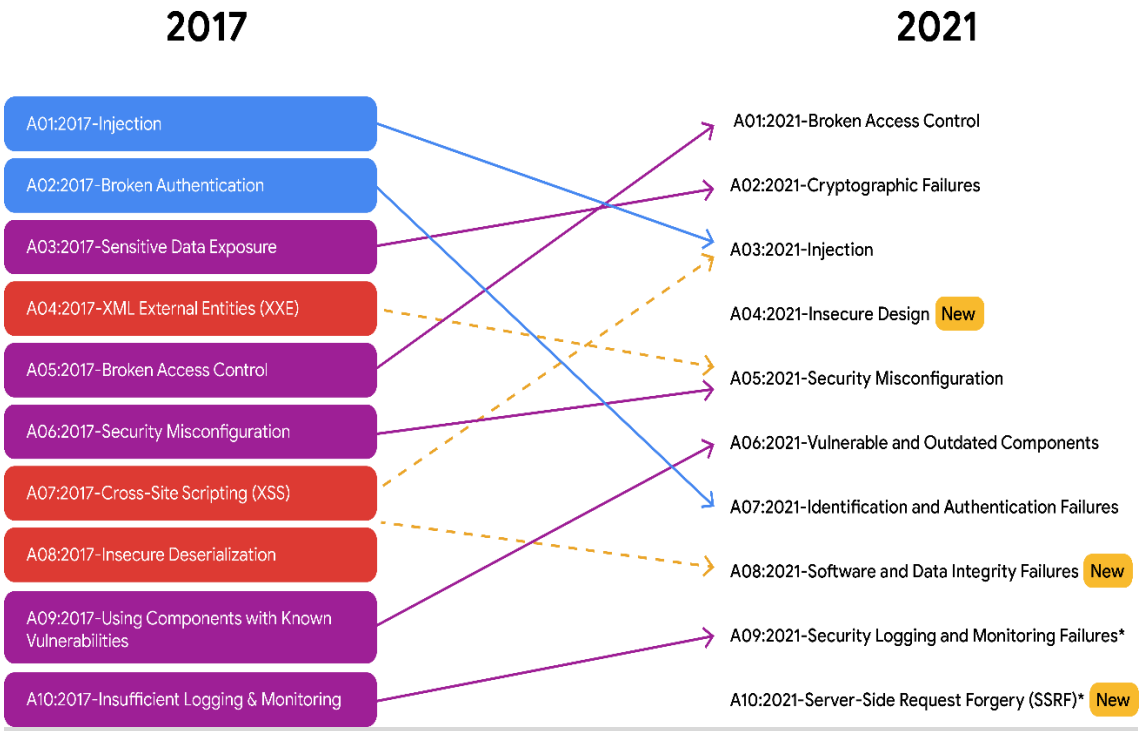
- **Rủi ro từ nhiều bên:** Gia công phần mềm cho các nhà cung cấp bên thứ ba có thể giúp họ tiếp cận với tài sản trí tuệ, chẳng hạn như bí mật thương mại, thiết kế phần mềm và phát minh.

- **Tuân thủ/cấp phép phần mềm:** Phần mềm không được cập nhật hoặc không tuân thủ hoặc các bản vá không được cài đặt kịp thời

Có nhiều tài nguyên, chẳng hạn như NIST, cung cấp danh sách cácrủi ro an ninh mạng. Ngoài ra, Dự án Bảo mật Ứng dụng Web Mở (OWASP) xuất bản một tài liệu nhận thức tiêu chuẩn về10 rủi ro bảo mật nghiêm trọng nhấtvào các ứng dụng web được cập nhật thường xuyên.

Note: The OWASP's common attack types list contains three new risks for the years 2017 to 2021: insecure design, software and data integrity failures, and server-side request forgery. This update emphasizes the fact that security is a constantly evolving field. It also demonstrates the importance of staying up to date on current threat actor tactics and techniques, so you can be better prepared to manage these types of risks.

Lưu ý: Danh sách các loại tấn công phổ biến của OWASP chứa ba rủi ro mới trong giai đoạn 2017 đến 2021: thiết kế không an toàn, lỗi về tính toàn vẹn của phần mềm và dữ liệu cũng như giả mạo yêu cầu phía máy chủ. Bản cập nhật này nhấn mạnh thực tế rằng bảo mật là một lĩnh vực không ngừng phát triển. Nó cũng cho thấy tầm quan trọng của việc luôn cập nhật các chiến thuật và kỹ thuật của tác nhân đe dọa hiện tại, để bạn có thể chuẩn bị tốt hơn để quản lý các loại rủi ro này.



Vulnerabilities

Lỗ hổng

A **vulnerability** is a weakness that can be exploited by a threat. Therefore, organizations need to regularly inspect for vulnerabilities within their systems. Some vulnerabilities include:

- **ProxyLogon:** A pre-authenticated vulnerability that affects the Microsoft Exchange server. This means a threat actor can complete a user authentication process to deploy malicious code from a remote location.
- **ZeroLogon:** A vulnerability in Microsoft's Netlogon authentication protocol. An authentication protocol is a way to verify a person's identity. Netlogon is a service that ensures a user's identity before allowing access to a website's location.
- **Log4Shell:** Allows attackers to run Java code on someone else's computer or leak sensitive information. It does this by enabling a remote attacker to take control of devices connected to the internet and run malicious code.
- **PetitPotam:** Affects Windows New Technology Local Area Network (LAN) Manager (NTLM). It is a theft technique that allows a LAN-based attacker to initiate an authentication request.
- **Security logging and monitoring failures:** Insufficient logging and monitoring capabilities that result in attackers exploiting vulnerabilities without the organization knowing it
- **Server-side request forgery:** Allows attackers to manipulate a server-side application into accessing and updating backend resources. It can also allow threat actors to steal data.

As an entry-level security analyst, you might work in vulnerability management, which is monitoring a system to identify and mitigate vulnerabilities. Although patches and updates may exist, if they are not applied, intrusions can still occur. For this reason, constant monitoring is important. The sooner an organization identifies a vulnerability and addresses it by patching it or updating their systems, the sooner it can be mitigated, reducing the organization's exposure to the vulnerability.

Lỗ hổng là điểm yếu có thể bị khai thác bởi mối đe dọa. Do đó, các tổ chức cần thường xuyên kiểm tra các lỗ hổng trong hệ thống của mình. Một số lỗ hổng bao gồm:

- **ProxyLogon:** Một lỗ hổng được xác thực trước ảnh hưởng đến máy chủ Microsoft Exchange. Điều này có nghĩa là kẻ đe dọa có thể hoàn tất quy trình xác thực người dùng để triển khai mã độc từ một địa điểm từ xa.

- **ZeroLogon:** Một lỗ hổng trong giao thức xác thực Netlogon của Microsoft. Giao thức xác thực là một cách để xác minh danh tính của một người. Netlogon là dịch vụ đảm bảo danh tính của người dùng trước khi cho phép truy cập vào vị trí của trang web.

- **Log4Shell:** Cho phép kẻ tấn công chạy mã Java trên máy tính của người khác hoặc rò rỉ thông tin nhạy cảm. Nó thực hiện điều này bằng cách cho phép kẻ tấn công từ xa chiếm quyền kiểm soát các thiết bị được kết nối với internet và chạy mã độc.

- **PetitPotam:** Ảnh hưởng đến Trình quản lý Mạng cục bộ (LAN) Công nghệ mới của Windows (NTLM). Đây là một kỹ thuật đánh cắp cho phép kẻ tấn công dựa trên mạng LAN bắt đầu yêu cầu xác thực.

- **Lỗi giám sát và ghi nhật ký bảo mật:** Khả năng ghi nhật ký và giám sát không đủ dẫn đến kẻ tấn công khai thác lỗ hổng mà tổ chức không hề hay biết

- **Giả mạo yêu cầu phía máy chủ:** Cho phép kẻ tấn công thao túng ứng dụng phía máy chủ truy cập và cập nhật tài nguyên phụ trợ. Nó cũng có thể cho phép các tác nhân đe dọa đánh cắp dữ liệu.

Với tư cách là nhà phân tích bảo mật cấp đầu vào, bạn có thể làm việc trong lĩnh vực quản lý lỗ hổng, tức là giám sát hệ thống để xác định và giảm thiểu lỗ hổng. Mặc dù các bản vá và bản cập nhật có thể tồn tại nhưng nếu không được áp dụng, các hành vi xâm nhập vẫn có thể xảy ra. Vì lý do này, việc theo dõi liên tục là rất quan trọng. Tổ chức xác định lỗ hổng bảo mật càng sớm và giải quyết lỗ hổng đó bằng cách vá lỗ hổng hoặc cập nhật hệ thống của họ thì lỗ hổng đó có thể được giảm thiểu càng sớm, giảm khả năng tiếp xúc với lỗ hổng bảo mật của tổ chức.

To learn more about the vulnerabilities explained in this section of the reading, as well as other vulnerabilities, explore the NIST National Vulnerability Database and CISA Known Exploited Vulnerabilities Catalog.

Để tìm hiểu thêm về các lỗ hổng được giải thích trong phần đọc này, cũng như các lỗ hổng khác, hãy khám phá phầnCơ sở dữ liệu về lỗ hổng bảo mật quốc gia của NISTVàDanh mục lỗ hổng bị khai thác đã biết của CISA.

Key takeaways

Bài học chính

In this reading, you learned about some risk management strategies and frameworks that can be used to develop organization-wide policies and processes to mitigate threats, risks, and vulnerabilities. You also learned about some of today's most common threats, risks, and vulnerabilities to business operations. Understanding these concepts can better prepare you to not only protect against, but also mitigate, the types of security-related issues that can harm organizations and people alike.

Trong bài đọc này, bạn đã tìm hiểu về một số chiến lược và khuôn khổ quản lý rủi ro có thể được sử dụng để phát triển các chính sách và quy trình trong toàn tổ chức nhằm giảm thiểu các mối đe dọa, rủi ro và lỗ hổng. Bạn cũng đã tìm hiểu về một số mối đe dọa, rủi ro và lỗ hổng phổ biến nhất hiện nay đối với hoạt động kinh doanh. Hiểu những khái niệm này có thể giúp bạn chuẩn bị tốt hơn để không chỉ bảo vệ mà còn giảm thiểu các loại vấn đề liên quan đến bảo mật có thể gây hại cho tổ chức cũng như mọi người.

Resources for more information

Tài nguyên để biết thêm thông tin

To learn more, click the linked terms in this reading. Also, consider exploring the following sites:

- OWASP Top Ten
- NIST RMF
-

Để tìm hiểu thêm, hãy nhấp vào các thuật ngữ được liên kết trong bài đọc này. Ngoài ra, hãy xem xét khám phá các trang web sau:

- Top 10 của OWASP
- NIST RMF

3.6. Test your knowledge: Navigate threats, risks, and vulnerabilities – Kiểm tra kiến thức của bạn: Điều hướng các mối đe dọa, rủi ro và lỗ hổng

4. Review: Security domains – Đánh giá: Miền bảo mật

4.1. Wrap-up – Gói lại

Module 1: Security domains
Phần 1: Miền bảo mật

You've now completed the first section of this course! Let's review what we've discussed so far.

Bây giờ bạn đã hoàn thành phần đầu tiên của khóa học này!Hãy xem lại những gì chúng ta đã thảo luận cho đến nay.

We started out by exploring the focus of CISSP's eight security domains. Then, we discussed threats, risks, and vulnerabilities, and how they can impact organizations. This included a close examination of ransomware and an introduction to the three layers of the web.

Chúng tôi bắt đầu bằng việc khám phá trọng tâm của tám lĩnh vực bảo mật của CISSP.Sau đó, chúng tôi thảo luận về các mối đe dọa, rủi ro vàcác lỗ hổng và cách chúng có thể tác động đến các tổ chức.Điều này bao gồm việc kiểm tra chặt chẽ ransomware vàgiới thiệu về ba lớp của web.

Finally, we focused on seven steps of the NIST Risk Management Framework, also called the RMF.

Cuối cùng, chúng tôi tập trung vào bảy bước của Quy trình Rủi ro NISTKhung quản lý, còn được gọi là RMF.

You did a fantastic job adding new knowledge to your security analyst toolkit. In upcoming videos, we'll go into more detail about some common tools used by entry-level security analysts. Then, you'll have an opportunity to analyze data generated by those tools to identify risks, threats, or vulnerabilities. You'll also have a chance to use a playbook to respond to incidents. That's all for now. Keep up the great work!

Bạn đã làm rất tốt việc bổ sung kiến thức mới cho nhà phân tích bảo mật của mìnhbộ công cụ.Trong các video sắp tới, chúng ta sẽ đi vào chi tiết hơn vềmột số công cụ phổ biến được sử dụng bởi các nhà phân tích bảo mật cấp đầu vào.Sau đó, bạn sẽ có cơ hội phân tích dữ liệu được tạo bởi nhữngcông cụ để xác định rủi ro, mối đe dọa hoặc lỗ hổng.Bạn cũng sẽ có cơ hội sử dụng cẩm nang để ứng phó với các sự cố.Đó là tất cả cho bây giờ.Kịp các công việc tuyệt vời!

Module 1: Security domains
Phần 1: Miền bảo mật

4.2. Glossary terms from module 1 – Thuật ngữ module 1

Glossary terms from module 1

Thuật ngữ thuật ngữ từ mô-đun 1

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Đánh giá: Bước thứ năm của NIST RMF có nghĩa là xác định xem các biện pháp kiểm soát đã thiết lập có được triển khai chính xác hay không

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization

Ủy quyền: Bước thứ sáu của NIST RMF đề cập đến việc chịu trách nhiệm về các rủi ro bảo mật và quyền riêng tư có thể tồn tại trong một tổ chức

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Tính liên tục trong kinh doanh: Khả năng của tổ chức trong việc duy trì năng suất hàng ngày bằng cách thiết lập các kế hoạch khắc phục rủi ro sau thảm họa

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

Phân loại: Bước thứ hai của NIST RMF được sử dụng để phát triển các quy trình và nhiệm vụ quản lý rủi ro

External threat: Anything outside the organization that has the potential to harm organizational assets

Mối đe dọa bên ngoài: Bất cứ điều gì bên ngoài tổ chức có khả năng gây tổn hại đến tài sản của tổ chức

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

Mối đe dọa bên ngoài: Bất cứ điều gì bên ngoài tổ chức có khả năng gây tổn hại đến tài sản của tổ chức

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Mối đe dọa nội bộ: Nhân viên hiện tại hoặc cựu nhân viên, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy gây ra rủi ro bảo mật

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

Giám sát : Bước thứ bảy của NIST RMF có nghĩa là nhận thức được cách các hệ thống đang vận hành

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Chuẩn bị: Bước đầu tiên của NIST RMF liên quan đến các hoạt động cần thiết để quản lý rủi ro về bảo mật và quyền riêng tư trước khi xảy ra vi phạm

Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access

Module 1: Security domains
Phần 1: Miền bảo mật

Ransomware: Một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập

Risk: Anything that can impact the 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

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

Giảm thiểu rủi ro: Quá trình áp dụng các quy trình và quy tắc phù hợp để nhanh chóng giảm thiểu tác động của rủi ro như vi phạm

Security posture: An organization's ability to manage its defense of critical assets and data and react to change

Tình trạng bảo mật: Khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Chọn : Bước thứ ba của NIST RMF có nghĩa là chọn, tùy chỉnh và thu thập tài liệu về các biện pháp kiểm soát nhằm bảo vệ tổ chức

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Trách nhiệm chung: Ý tưởng rằng tất cả các cá nhân trong một tổ chức có vai trò tích cực trong việc giảm thiểu rủi ro và duy trì cả an ninh vật lý và ảo

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 khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc tài sản có giá trị

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

4.3. Module 1 challenge – Thử thách module 1

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Module 2: Security framework and controls – Khung bảo mật và kiểm soát

You will focus on security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. You'll learn about Open Web Application Security Project (OWASP) security principles and security audits.

Bạn sẽ tập trung vào các khuôn khổ và biện pháp kiểm soát bảo mật, cùng với các thành phần cốt lõi của bộ ba bảo mật, tính toàn vẹn và tính khả dụng (CIA). Bạn sẽ tìm hiểu về các nguyên tắc bảo mật và kiểm tra bảo mật của Dự án bảo mật ứng dụng web mở (OWASP).

Learning Objectives

- Define and describe the purpose of security frameworks and controls.
- Describe the CIA triad.
- Explain the National Institute of Standards and Technology (NIST) frameworks.
- Identify security principles.
- Examine how businesses use security frameworks and controls to protect business operations.
- Define security audits.
- Explore common elements of internal security audits.

Mục tiêu học tập

- Xác định và mô tả mục đích của các khung và biện pháp kiểm soát bảo mật.
- Mô tả bộ ba CIA.
- Giải thích khuôn khổ của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST).
- Xác định các nguyên tắc bảo mật.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

- Kiểm tra cách doanh nghiệp sử dụng các khung bảo mật và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh.
- Xác định kiểm tra an ninh.
- Khám phá các yếu tố chung của kiểm toán an ninh nội bộ.

1. More about frameworks and controls – Tìm hiểu thêm về frameworks và controls

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

Welcome back! As a security analyst, your job isn't just keeping organizations safe. Your role is much more important. You're also helping to keep people safe. Breaches that affect customers', vendors', and employees' data can cause significant damage to people's financial stability and their reputations. As an analyst, your day-to-day work will help keep people and organizations safe.

Chào mừng trở lại! Là một nhà phân tích chứng khoán,công việc của bạn không chỉ là giữ an toàn cho tổ chức.Vai trò của bạn quan trọng hơn nhiều.Bạn cũng đang giúp giữ an toàn cho mọi người.Những vi phạm ảnh hưởng đến khách hàng, nhà cung cấp,và dữ liệu của nhân viên có thể gây ra thiệt hại đáng kể chosự ổn định tài chính của mọi người và danh tiếng của họ.Là một nhà phân tích, công việc hàng ngày của bạnsẽ giúp giữ an toàn cho mọi người và tổ chức.

In this section of the course, we'll discuss security frameworks, controls, and design principles in more detail, and how they can be applied to security audits to help protect organizations and people.

Trong phần này của khóa học,chúng ta sẽ thảo luận về các khuôn khổ bảo mật, các biện pháp kiểm soát,và các nguyên tắc thiết kế chi tiết hơn cũng như cách chúng có thể được thực hiệnáp dụng cho kiểm tra an ninh để giúpbảo vệ tổ chức và con người.

Keeping customer information confidential is a crucial part of my daily work at Google. The NIST Cybersecurity Framework plays a large part in this. The framework ensures the protection and compliance of customer tools and personal work devices through the use of security controls.

Bảo mật thông tin khách hàng làmột phần quan trọng trong công việc hàng ngày của tôi tại Google.Khung an ninh mạng NISTđóng một vai trò lớn trong việc này.Khuôn khổ

này đảm bảo việc bảo vệ và tuân thủ cáccông cụ khách hàng và thiết bị làm việc cá nhânthông qua việc sử dụng các biện pháp kiểm soát an ninh.

Welcome to the world of security frameworks and controls. Let's get started!

Chào mừng đến với thế giới của các khuôn khổ và biện pháp kiểm soát bảo mật.Bắt đầu nào!

1.2. Frameworks – Frameworks

In an organization, plans are put in place to protect against a variety of threats, risks, and vulnerabilities. However, the requirements used to protect organizations and people often overlap. Because of this, organizations use security frameworks as a starting point to create their own security policies and processes.

Trong một tổ chức, các kế hoạch được đưa ra để bảo vệchống lại nhiều mối đe dọa, rủi ro và điểm yếu.Tuy nhiên, các yêu cầu được sử dụng để bảo vệtổ chức và con người thường chồng chéo lên nhau.Vì điều này, các tổ chức sử dụng các khuôn khổ bảo mật nhưđiểm khởi đầu để tạo rachính sách và quy trình bảo mật của riêng họ.

Let's start by quickly reviewing what frameworks are. Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware. Security involves more than just the virtual space. It also includes the physical, which is why many organizations have plans to maintain safety in the work environment. For example, access to a building may require using a key card or badge.

Hãy bắt đầu bằng cách xem xét nhanh framework là gì.Khung bảo mật là các hướng dẫn được sử dụng để xây dựngkế hoạch giúp giảm thiểu rủi ro vàcác mối đe dọa đối với dữ liệu và quyền riêng tư,chẳng hạn như các cuộc tấn công kỹ thuật xã hội và ransomware.Bảo mật không chỉ liên quan đến không gian ảo.Nó cũng bao gồm cả thể chất,đó là lý do tại sao nhiều tổ chức cókế hoạch duy trì an toàn trong môi trường làm việc.Ví dụ: truy cập vào một tòa nhàcó thể yêu cầu sử dụng thẻ chìa khóa hoặc huy hiệu.

Other security frameworks provide guidance for how to prevent, detect, and respond to security breaches. This is particularly important when trying to protect an organization from social engineering attacks like phishing that target their employees.

Các khung bảo mật khác cung cấphướng dẫn cách phòng ngừa,phát hiện và xử lý các vi phạm an ninh.Điều này đặc biệt quan trọngkhi cố gắng bảo vệ một tổ chức khỏicác cuộc tấn công kỹ thuật xã hội nhưlừa đảo nhắm vào nhân viên của họ.

Remember, people are the biggest threat to security. So frameworks can be used to create plans that increase employee awareness and educate them about how they can protect the organization, their co-workers, and themselves. Educating employees about existing security challenges is essential for minimizing the possibility of a breach.

Hãy nhớ rằng, con người là mối đe dọa lớn nhất đối với an ninh.Vì vậy, các khung có thể được sử dụng để tạo ra các kế hoạch làm tăngnhận thức của nhân viên và giáo dục họ vềcách họ có thể bảo vệ tổ chức,đồng nghiệp và bản thân họ.Giáo dục nhân viên về những thách thức an ninh hiện tại làcần thiết để giảm thiểu khả năng vi phạm.

Providing employee training about how to recognize red flags, or potential threats, is essential, along with having plans in place to quickly report and address security issues. As an analyst, it will be important for you to understand and implement the plans your organization has in place to keep the organization, its employees, and the people it serves safe from social engineering attacks, breaches, and other harmful security incidents.

Đào tạo nhân viên về cách thực hiệnnhận ra những lá cờ đỏ hoặc những mối đe dọa tiềm ẩn làcần thiết, cùng với việc có sẵn kế hoạchđể nhanh chóng báo cáo và giải quyết các vấn đề bảo mật.Với tư cách là một nhà phân tích, nó sẽĐiều quan trọng là bạn phải hiểu vàthực hiện các kế hoạch tổ chức của bạncó sẵn để duy trì tổ chức,nhân viên của nó và những người ở đóphục vụ an toàn trước các cuộc tấn công kỹ thuật xã hội,vi phạm và các sự cố an ninh có hại khác.

Coming up, we'll review and discuss security controls, which are used alongside frameworks to achieve an organization's security goals.

Sắp tới, chúng tôi sẽ xem xét vàthảo luận về các biện pháp kiểm soát bảo mật được sử dụngbên cạnh các khuôn khổ để đạt đượcmục tiêu an ninh của một tổ chức.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

1.3. Controls – Controls

While frameworks are used to create plans to address security risks, threats, and vulnerabilities, controls are used to reduce specific risks. If proper controls are not in place, an organization could face significant financial impacts and damage to their reputation because of exposure to risks including trespassing, creating fake employee accounts, or providing free benefits.

Trong khi các framework được sử dụng để tạokế hoạch giải quyết các rủi ro an ninh,các mối đe dọa và điểm yếu,kiểm soát được sử dụng để giảm thiểu rủi ro cụ thể.Nếu không có biện pháp kiểm soát thích hợp,một tổ chức có thể phải đối mặt với những tác động tài chính đáng kểvà tổn hại đến danh tiếng của họvì phải đối mặt với rủi robao gồm xâm nhập trái phép, tạo tài khoản nhân viên giả,hoặc cung cấp các lợi ích miễn phí.

Let's review the definition of controls. Security controls are safeguards designed to reduce specific security risks. In this video, we'll discuss three common types of controls: encryption, authentication, and authorization.

Hãy xem lại định nghĩa của điều khiển.Kiểm soát an ninh là biện pháp bảo vệđược thiết kế để giảm thiểu rủi ro bảo mật cụ thể.Trong video này, chúng ta sẽ thảo luận về ba loại phổ biếncủa các điều khiển: mã hóa,xác thực và ủy quyền.

Encryption is the process of converting data from a readable format to an encoded format. Typically, encryption involves converting data from plaintext to ciphertext. Ciphertext is the raw, encoded message that's unreadable to humans and computers. Ciphertext data cannot be read until it's been decrypted into its original plaintext form. Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.

Mã hóa là quá trình chuyển đổi dữ liệutừ định dạng có thể đọc được sang định dạng được mã hóa.Thông thường, mã hóa bao gồm việc chuyển đổidữ liệu từ bản rõ sang bản mã.Bản mã là thông điệp thô, được mã hóacon người và máy tính không thể đọc được.Dữ liệu văn bản mã hóa không thể được đọc cho đến khi nó đượcđược giải mã thành dạng bản rõ ban đầu.Mã hóa được sử dụng để đảm bảobảo mật dữ liệu nhạy cảm,chẳng hạn như thông tin tài khoản của khách hànghoặc số an sinh xã hội.

Another control that can be used to protect sensitive data is authentication. Authentication is the process of verifying who someone or something is. A real-world

example of authentication is logging into a website with your username and password. This basic form of authentication proves that you know the username and password and should be allowed to access the website. More advanced methods of authentication, such as multi-factor authentication, or MFA, challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometrics, such as a fingerprint, voice, or face scan.

Một điều khiển khác có thể được sử dụng để bảo vệdữ liệu nhạy cảm là xác thực.Xác thực là quá trìnhxác minh ai đó hoặc một cái gì đó làMột ví dụ thực tế về xác thực làđăng nhập vào một trang web bằng tên người dùng và mật khẩu của bạn.Hình thức xác thực cơ bản này chứng minh rằng bạnbiết tên người dùng và mật khẩuvà phải được phép truy cập vào trang web.Các phương pháp xác thực nâng cao hơn,chẳng hạn như xác thực đa yếu tố hoặc MFA,thách thức người dùngchứng minh rằng họ là người mà họ tuyên bốbằng cách yêu cầu cả mật khẩuvà một hình thức xác thực bổ sung,như mã bảo mật hoặc sinh trắc học,chẳng hạn như dấu vân tay,quét giọng nói hoặc khuôn mặt.

Biometrics are unique physical characteristics that can be used to verify a person's identity. Examples of biometrics are a fingerprint, an eye scan, or a palm scan. One example of a social engineering attack that can exploit biometrics is vishing. Vishing is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source. For example, vishing could be used to impersonate a person's voice to steal their identity and then commit a crime.

Sinh trắc học là những đặc điểm vật lý độc đáocó thể được sử dụng để xác minh danh tính của một người.Ví dụ về sinh trắc học là dấu vân tay,quét mắt hoặc quét lòng bàn tay.Một ví dụ về cuộc tấn công kỹ thuật xã hộicó thể khai thác sinh trắc học là vishing.Vishing là việc khai thácthông tin liên lạc bằng giọng nói điện tử đểcó được thông tin nhạy cảm hoặcđể mạo danh một nguồn đã biết.Ví dụ: vishing có thể được sử dụng để mạo danhgiọng nói của một người để ăn cắpdanh tính của họ và sau đó phạm tội.

Another very important security control is authorization. Authorization refers to the concept of granting access to specific resources within a system. Essentially, authorization is used to verify that a person has permission to access a resource. As an example, if you're working as an entry-level security analyst for the federal government, you could have permission to access data through the deep web or other internal data that is only accessible if you're a federal employee.

Một biện pháp kiểm soát bảo mật rất quan trọng khác là ủy quyền.Sự ủy quyền đề cập đến khái niệmcấp quyền truy cập vào các tài nguyên cụ thể trong một hệ thống.Về cơ

bản, ủy quyền được sử dụng để xác minhrằng một người có quyền truy cập vào một tài nguyên.Ví dụ: nếu bạn đang làm việc nhưmột nhà phân tích bảo mật cấp đầu vàocho chính phủ liên bang,bạn có thể có quyền truy cậpdữ liệu thông qua web sâu hoặcdữ liệu nội bộ khác chỉcó thể truy cập nếu bạn là nhân viên liên bang.

The security controls we discussed today are only one element of a core security model known as the CIA triad. Coming up, we'll talk more about this model and how security teams use it to protect their organizations.

Các biện pháp kiểm soát bảo mật mà chúng ta đã thảo luậnngày hôm nay chỉ là một phần tử củamột mô hình an ninh cốt lõi được gọi là bộ ba CIA.Sắp tới, chúng ta sẽ nói nhiều hơn về mô hình này và cáchđội bảo mật sử dụng nó để bảo vệ tổ chức của họ.

1.4. The relationship between frameworks and controls – Mối quan hệ giữa khuôn khổ và kiểm soát

The relationship between frameworks and controls

Mối quan hệ giữa khuôn khổ và kiểm soát

Previously, you learned how organizations use security frameworks and controls to protect against threats, risks, and vulnerabilities. This included discussions about the National Institute of Standards and Technology's (NIST's) Risk Management Framework (RMF) and Cybersecurity Framework (CSF), as well as the confidentiality, integrity, and availability (CIA) triad. In this reading, you will further explore security frameworks and controls and how they are used together to help mitigate organizational risk.

Trước đây, bạn đã tìm hiểu cách các tổ chức sử dụng khung bảo mật và biện pháp kiểm soát để bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng bảo mật. Điều này bao gồm các cuộc thảo luận về Khung quản lý rủi ro (RMF) và Khung an ninh mạng (CSF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), cũng như bộ ba bảo mật, toàn vẹn và sẵn sàng (CIA). Trong bài đọc này, bạn sẽ khám phá thêm các khung và biện pháp kiểm soát bảo mật cũng như cách chúng được sử dụng cùng nhau để giúp giảm thiểu rủi ro cho tổ chức.

Frameworks and controls

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Khung và điều khiển

Security frameworks are guidelines used for building plans to help mitigate risk and threats to data and privacy. Frameworks support organizations' ability to adhere to compliance laws and regulations. For example, the healthcare industry uses frameworks to comply with the United States' Health Insurance Portability and Accountability Act (HIPAA), which requires that medical professionals keep patient information safe.

Khung bảo mật là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và các mối đe dọa đối với dữ liệu và quyền riêng tư. Các khuôn khổ hỗ trợ khả năng của tổ chức trong việc tuân thủ luật pháp và quy định. Ví dụ: ngành chăm sóc sức khỏe sử dụng các khuôn khổ để tuân thủ Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA) của Hoa Kỳ, trong đó yêu cầu các chuyên gia y tế phải giữ an toàn thông tin bệnh nhân.

Security controls are safeguards designed to reduce *specific* security risks. Security controls are the measures organizations use to lower risk and threats to data and privacy. For example, a control that can be used alongside frameworks to ensure a hospital remains compliant with HIPAA is requiring that patients use multi-factor authentication (MFA) to access their medical records. Using a measure like MFA to validate someone's identity is one way to help mitigate potential risks and threats to private data.

Kiểm soát bảo mật là các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật *cụ thể* . Kiểm soát bảo mật là các biện pháp mà các tổ chức sử dụng để giảm rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư. Ví dụ: một biện pháp kiểm soát có thể được sử dụng cùng với các khuôn khổ để đảm bảo bệnh viện vẫn tuân thủ HIPAA đang yêu cầu bệnh nhân sử dụng xác thực đa yếu tố (MFA) để truy cập hồ sơ y tế của họ. Sử dụng biện pháp như MFA để xác thực danh tính của ai đó là một cách giúp giảm thiểu rủi ro và mối đe dọa tiềm ẩn đối với dữ liệu riêng tư.

Specific frameworks and controls

Các khuôn khổ và biện pháp kiểm soát cụ thể

There are many different frameworks and controls that organizations can use to remain compliant with regulations and achieve their security goals. Frameworks

covered in this reading are the Cyber Threat Framework (CTF) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Several common security controls, used alongside these types of frameworks, are also explained.

Có nhiều khuôn khổ và biện pháp kiểm soát khác nhau mà các tổ chức có thể sử dụng để duy trì tuân thủ các quy định và đạt được mục tiêu bảo mật của mình. Các khung được đề cập trong bài đọc này là Khung đe dọa mạng (CTF) và Tổ chức tiêu chuẩn quốc tế/Ủy ban kỹ thuật điện quốc tế (ISO/IEC) 27001. Một số biện pháp kiểm soát bảo mật phổ biến, được sử dụng cùng với các loại khung này, cũng được giải thích.

Cyber Threat Framework (CTF)

Khung đe dọa mạng (CTF)

According to the Office of the Director of National Intelligence, the CTF was developed by the U.S. government to provide “a common language for describing and communicating information about cyber threat activity.” By providing a common language to communicate information about threat activity, the CTF helps cybersecurity professionals analyze and share information more efficiently. This allows organizations to improve their response to the constantly evolving cybersecurity landscape and threat actors' many tactics and techniques.

Theo Văn phòng Giám đốc Tình báo Quốc gia, CTF được chính phủ Hoa Kỳ phát triển để cung cấp “ngôn ngữ chung để mô tả và truyền đạt thông tin về hoạt động đe dọa mạng”. Bằng cách cung cấp một ngôn ngữ chung để truyền đạt thông tin về hoạt động đe dọa, CTF giúp các chuyên gia an ninh mạng phân tích và chia sẻ thông tin hiệu quả hơn. Điều này cho phép các tổ chức cải thiện phản ứng của họ trước bối cảnh an ninh mạng không ngừng phát triển cũng như nhiều chiến thuật và kỹ thuật của các tác nhân đe dọa.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001

Tổ chức Tiêu chuẩn hóa Quốc tế/Ủy ban Kỹ thuật Điện Quốc tế (ISO/IEC) 27001

An internationally recognized and used framework is ISO/IEC 27001. The ISO 27000 family of standards enables organizations of all sectors and sizes to manage the

security of assets, such as financial information, intellectual property, employee data, and information entrusted to third parties. This framework outlines requirements for an information security management system, best practices, and controls that support an organization's ability to manage risks. Although the ISO/IEC 27001 framework does not require the use of specific controls, it does provide a collection of controls that organizations can use to improve their security posture.

Khuôn khổ được quốc tế công nhận và sử dụng là ISO/IEC 27001. Nhóm tiêu chuẩn ISO 27000 cho phép các tổ chức thuộc mọi lĩnh vực và quy mô quản lý tính bảo mật của tài sản, chẳng hạn như thông tin tài chính, sở hữu trí tuệ, dữ liệu nhân viên và thông tin được ủy thác cho bên thứ ba. Khung này phác thảo các yêu cầu đối với hệ thống quản lý bảo mật thông tin, các biện pháp thực hành tốt nhất và các biện pháp kiểm soát hỗ trợ khả năng quản lý rủi ro của tổ chức. Mặc dù khuôn khổ ISO/IEC 27001 không yêu cầu sử dụng các biện pháp kiểm soát cụ thể nhưng nó cung cấp một tập hợp các biện pháp kiểm soát mà các tổ chức có thể sử dụng để cải thiện tình trạng bảo mật của mình.

Controls

Điều khiển

Controls are used alongside frameworks to reduce the possibility and impact of a security threat, risk, or vulnerability. Controls can be physical, technical, and administrative and are typically used to prevent, detect, or correct security issues.

Các biện pháp kiểm soát được sử dụng cùng với các khuôn khổ để giảm khả năng và tác động của mối đe dọa, rủi ro hoặc lỗ hổng bảo mật. Các biện pháp kiểm soát có thể là vật lý, kỹ thuật và hành chính và thường được sử dụng để ngăn chặn, phát hiện hoặc khắc phục các vấn đề bảo mật.

Examples of physical controls:

- Gates, fences, and locks
- Security guards
- Closed-circuit television (CCTV), surveillance cameras, and motion detectors
- Access cards or badges to enter office spaces

Ví dụ về điều khiển vật lý:

- Cổng, hàng rào và ổ khóa
- Nhân viên bảo vệ
- Truyền hình mạch kín (CCTV), camera giám sát và máy dò chuyển động
- Thẻ truy cập hoặc huy hiệu để vào không gian văn phòng

Examples of technical controls:

- Firewalls
- MFA
- Antivirus software

Ví dụ về kiểm soát kỹ thuật:

- Tường lửa
- MFA
- Phần mềm diệt virus

Examples of administrative controls:

- Separation of duties
- Authorization
- Asset classification

Ví dụ về kiểm soát hành chính:

- Tách biệt nhiệm vụ
- Ủy quyền
- Phân loại tài sản

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

To learn more about controls, particularly those used to protect health-related assets from a variety of threat types, review the U.S. Department of Health and Human Services' Physical Access Control presentation.

Để tìm hiểu thêm về các biện pháp kiểm soát, đặc biệt là các biện pháp được sử dụng để bảo vệ tài sản liên quan đến sức khỏe khỏi nhiều loại mối đe dọa khác nhau, hãy xem lại Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ'Bản trình bày Kiểm soát truy cập vật lý.

Key takeaways

Bài học chính

Cybersecurity frameworks and controls are used together to establish an organization's security posture. They also support an organization's ability to meet security goals and comply with laws and regulations. Although these frameworks and controls are typically voluntary, organizations are strongly encouraged to implement and use them to help ensure the safety of critical assets.

Các khuôn khổ và biện pháp kiểm soát an ninh mạng được sử dụng cùng nhau để thiết lập tình trạng bảo mật của tổ chức. Chúng cũng hỗ trợ khả năng của tổ chức trong việc đáp ứng các mục tiêu bảo mật và tuân thủ luật pháp và quy định. Mặc dù các khuôn khổ và biện pháp kiểm soát này thường mang tính tự nguyện nhưng các tổ chức được khuyến khích triển khai và sử dụng chúng để giúp đảm bảo an toàn cho các tài sản quan trọng.

1.5. Test your knowledge: More about frameworks and controls – Kiểm tra kiến thức của bạn: Tìm hiểu thêm về các khuôn khổ và biện pháp kiểm soát

2. The CIA triad: Confidentiality, integrity, and availability – Bộ ba CIA: Bảo mật, toàn vẹn và sẵn sàng

2.1. Explore the CIA triad – Khám phá bộ ba CIA

Great to see you again! While working as an entry-level security analyst, your main responsibility is to help protect your organization's sensitive assets and data from threat actors. The CIA triad is a core security model that will help you do that.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Thật tuyệt khi được gặp lại bạn!Khi làm việc với tư cách là nhà phân tích bảo mật cấp độ đầu vào, trách nhiệm chính của bạn làgiúp bảo vệ tài sản và dữ liệu nhạy cảm của tổ chức bạn khỏi các tác nhân đe dọa.Bộ ba CIA là mô hình bảo mật cốt lõi sẽ giúp bạn thực hiện điều đó.

In this video, we'll explore the CIA triad and discuss the importance of each component for keeping an organization safe from threats, risks, and vulnerabilities. Let's get started!

Trong video này, chúng ta sẽ khám phá bộ ba CIA và thảo luận về tầm quan trọng của từng bộ ba.thành phần để giữ cho tổ chức an toàn trước các mối đe dọa, rủi ro và lỗ hổng.Bắt đầu nào!

The CIA triad is a model that helps inform how organizations consider risk when setting up systems and security policies. As a reminder, the three letters in the CIA triad stand for confidentiality, integrity, and availability. As an entry-level analyst, you'll find yourself constantly referring to these three core principles as you work to protect your organization and the people it serves.

Bộ ba CIA là một mô hình giúp thông báo cách các tổ chứcxem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật.Xin nhắc lại, ba chữ cái trong bộ ba CIA tượng trưng chotính bảo mật, tính toàn vẹn và tính sẵn sàng.Là một nhà phân tích cấp độ đầu vào, bạn sẽ thấy mình liên tục đề cập đếnba nguyên tắc cốt lõi này khi bạn làm việc để bảo vệ tổ chức của mình và mọi ngườinó phục vụ.

Confidentiality means that only authorized users can access specific assets or data. Sensitive data should be available on a "need to know" basis, so that only the people who are authorized to handle certain assets or data have access.

Tính bảo mật có nghĩa là chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài sản hoặc dữ liệu cụ thể.Dữ liệu nhạy cảm phải có sẵn trên cơ sở "cần biết", vì vậyrằng chỉ những người được ủy quyền xử lý một số tài sản hoặc dữ liệu nhất định mới có quyền truy cập.

Integrity means that the data is correct, authentic, and reliable. Determining the integrity of data and analyzing how it's used will help you, as a security professional, decide whether the data can or cannot be trusted.

Tính toàn vẹn có nghĩa là dữ liệu chính xác, xác thực và đáng tin cậy.Việc xác định tính toàn vẹn của dữ liệu và phân tích cách dữ liệu được sử dụng sẽ giúp ích cho bạn, cũng nhưmột chuyên gia bảo mật, quyết định xem dữ liệu có thể hoặc không thể tin cậy được.

Availability means that the data is accessible to those who are authorized to access it. Inaccessible data isn't useful and can prevent people from being able to do their jobs. As a security professional, ensuring that systems, networks, and applications are functioning properly to allow for timely and reliable access, may be a part of your everyday work responsibilities.

Tính sẵn sàng có nghĩa là dữ liệu có thể được truy cập bởi những ngườiđược phép truy cập vào nó.Dữ liệu không thể truy cập không hữu ích vàcó thể cản trở mọi người thực hiện công việc của mình.Là một chuyên gia bảo mật, đảm bảo rằng các hệ thống, mạng vàcác ứng dụng đang hoạt động bình thường để cho phép thực hiện kịp thời vàtruy cập đáng tin cậy, có thể là một phần trách nhiệm công việc hàng ngày của bạn.

Now that we've defined the CIA triad and its components, let's explore how you might use the CIA triad to protect an organization. If you work for an organization that has large amounts of private data like a bank, the principle of confidentiality is essential because the bank must keep people's personal and financial information safe.

Bây giờ chúng ta đã xác định được bộ ba CIA và các thành phần của nó,hãy khám phá cách bạn có thể sử dụng bộ ba CIA để bảo vệ một tổ chức.Nếu bạn làm việc cho một tổ chức có lượng lớn dữ liệu riêng tư như ngân hàng,nguyên tắc bảo mật là cần thiết bởi vìngân hàng phải giữ an toàn thông tin cá nhân và tài chính của mọi người.

The principle of integrity is also a priority. For example, if a person's spending habits or purchasing locations change dramatically, the bank will likely disable access to the account until they can verify that the account owner, not a threat actor, is actually the one making purchases.

Nguyên tắc liêm chính cũng là một ưu tiên.Ví dụ: nếu thói quen chi tiêu của một người hoặcđịa điểm mua hàng thay đổi đáng kể, ngân hàng có thể sẽ vô hiệu hóatruy cập vào tài khoản cho đến khi họ có thể xác minh rằng chủ sở hữu tài khoản,không phải là kẻ đe dọa, thực ra là người thực hiện mua hàng.

The availability principle is also critical. Banks put a lot of effort into making sure that people can access their account information easily on the web. And to make sure that information is protected from threat actors, banks use a validation process to help minimize damage if they suspect that customer accounts have been compromised.

Nguyên tắc sẵn có cũng rất quan trọng.Các ngân hàng đã nỗ lực rất nhiều để đảm bảo rằng mọi ngườicó thể truy cập thông tin tài khoản của họ một cách dễ dàng trên web.Và để đảm bảo rằng thông tin được bảo vệ khỏi các tác nhân đe dọa, các ngân hàngsử dụng quy trình xác nhận để giúp giảm thiểu thiệt hại nếu họ nghi ngờ rằngtài khoản của khách hàng đã bị xâm phạm.

As an analyst, you'll regularly use each component of the triad to help protect your organization and the people it serves. And having the CIA triad constantly in mind, will help you keep sensitive data and assets safe from a variety of threats, risks, and vulnerabilities including the social engineering attacks, malware, and data theft we discussed earlier.

Là một nhà phân tích, bạn sẽ thường xuyên sử dụng từng thành phần củabộ ba để giúp bảo vệ tổ chức của bạn và những người mà tổ chức đó phục vụ.Và luôn nghĩ tới bộ ba CIA,sẽ giúp bạn giữ an toàn cho dữ liệu và tài sản nhạy cảm trước nhiều mối đe dọa khác nhau,rủi ro và lỗ hổng bao gồm các cuộc tấn công kỹ thuật xã hội,phần mềm độc hại và đánh cắp dữ liệu mà chúng ta đã thảo luận trước đó.

Coming up, we'll explore specific frameworks and principles that will also help you protect your organization from threats, risks, and vulnerabilities. See you soon!

Sắp tới, chúng ta sẽ khám phá các khuôn khổ và nguyên tắc cụ thể cũng sẽgiúp bạn bảo vệ tổ chức của mình khỏi các mối đe dọa, rủi ro và lỗ hổng.Hẹn sớm gặp lại!

2.2. Use the CIA triad to protect organizations – Sử dụng bộ ba CIA để bảo vệ các tổ chức

Use the CIA triad to protect organizations

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Sử dụng bộ ba CIA để bảo vệ các tổ chức

Previously, you were introduced to the confidentiality, integrity, and availability (CIA) triad and how it helps organizations consider and mitigate risk. In this reading, you will learn how cybersecurity analysts use the CIA triad in the workplace.

Trước đây, bạn đã được giới thiệu về bộ ba bảo mật, tính toàn vẹn và tính khả dụng (CIA) cũng như cách bộ ba này giúp các tổ chức xem xét và giảm thiểu rủi ro. Trong bài đọc này, bạn sẽ tìm hiểu cách các nhà phân tích an ninh mạng sử dụng bộ ba CIA tại nơi làm việc.

The CIA triad for analysts

Bộ ba CIA dành cho các nhà phân tích

The **CIA triad** is a model that helps inform how organizations consider risk when setting up systems and security policies. It is made up of three elements that cybersecurity analysts and organizations work toward upholding: confidentiality, integrity, and availability. Maintaining an acceptable level of risk and ensuring systems and policies are designed with these elements in mind helps establish a successful **security posture**, which refers to an organization's ability to manage its defense of critical assets and data and react to change.

Bộ **ba CIA** là một mô hình giúp thông báo cách các tổ chức xem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật. Nó được tạo thành từ ba yếu tố mà các nhà phân tích và tổ chức an ninh mạng nỗ lực duy trì: tính bảo mật, tính toàn vẹn và tính sẵn sàng. Việc duy trì mức độ rủi ro có thể chấp nhận được và đảm bảo các hệ thống và chính sách được thiết kế có tính đến các yếu tố này sẽ giúp thiết lập một **trạng thái bảo mật** thành công , đề cập đến khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với sự thay đổi.

Confidentiality

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Bảo mật

Confidentiality is the idea that only authorized users can access specific assets or data. In an organization, confidentiality can be enhanced through the implementation of design principles, such as the principle of least privilege. The principle of least privilege limits users' access to only the information they need to complete work-related tasks. Limiting access is one way of maintaining the confidentiality and security of private data.

Tính bảo mật là ý tưởng mà chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài sản hoặc dữ liệu cụ thể. Trong một tổ chức, tính bảo mật có thể được tăng cường thông qua việc thực hiện các nguyên tắc thiết kế, chẳng hạn như nguyên tắc đặc quyền tối thiểu. Nguyên tắc đặc quyền tối thiểu giới hạn quyền truy cập của người dùng chỉ vào thông tin họ cần để hoàn thành các nhiệm vụ liên quan đến công việc. Hạn chế quyền truy cập là một cách để duy trì tính bảo mật và bảo mật của dữ liệu riêng tư.

Integrity

Toàn vẹn

Integrity is the idea that the data is verifiably correct, authentic, and reliable. Having protocols in place to verify the authenticity of data is essential. One way to verify data integrity is through cryptography, which is used to transform data so unauthorized parties cannot read or tamper with it (NIST, 2022). Another example of how an organization might implement integrity is by enabling encryption, which is the process of converting data from a readable format to an encoded format. Encryption can be used to prevent access and ensure data, such as messages on an organization's internal chat platform, cannot be tampered with.

Tính toàn vẹn là ý tưởng rằng dữ liệu là chính xác, xác thực và đáng tin cậy. Việc có sẵn các giao thức để xác minh tính xác thực của dữ liệu là điều cần thiết. Một cách để xác minh tính toàn vẹn dữ liệu là thông qua mật mã, được sử dụng để chuyển đổi dữ liệu để các bên trái phép không thể đọc hoặc giả mạo dữ liệu đó (NIST, 2022). Một ví dụ khác về cách một tổ chức có thể triển khai tính toàn vẹn là kích hoạt mã hóa, đó là quá trình chuyển đổi dữ liệu từ định dạng có thể đọc được sang định dạng được mã hóa. Mã hóa có thể được sử dụng để ngăn chặn quyền truy cập và đảm bảo dữ liệu, chẳng hạn như tin nhắn trên nền tảng trò chuyện nội bộ của tổ chức, không thể bị giả mạo.

Availability

Khả dụng

Availability is the idea that data is accessible to those who are authorized to use it. When a system adheres to both availability and confidentiality principles, data can be used when needed. In the workplace, this could mean that the organization allows remote employees to access its internal network to perform their jobs. It's worth noting that access to data on the internal network is still limited, depending on what type of access employees need to do their jobs. If, for example, an employee works in the organization's accounting department, they might need access to corporate accounts but not data related to ongoing development projects.

Tính khả dụng là ý tưởng rằng dữ liệu có thể truy cập được đối với những người được phép sử dụng nó. Khi một hệ thống tuân thủ cả nguyên tắc sẵn có và bảo mật, dữ liệu có thể được sử dụng khi cần thiết. Tại nơi làm việc, điều này có thể có nghĩa là tổ chức cho phép nhân viên từ xa truy cập mạng nội bộ để thực hiện công việc của họ. Điều đáng chú ý là quyền truy cập vào dữ liệu trên mạng nội bộ vẫn còn hạn chế, tùy thuộc vào loại quyền truy cập mà nhân viên cần để thực hiện công việc của mình. Ví dụ: nếu một nhân viên làm việc trong bộ phận kế toán của tổ chức, họ có thể cần quyền truy cập vào tài khoản công ty nhưng không cần dữ liệu liên quan đến các dự án phát triển đang diễn ra.

Key takeaways

Bài học chính

The CIA triad is essential for establishing an organization's security posture. Knowing what it is and how it's applied can help you better understand how security teams work to protect organizations and the people they serve.

Bộ ba CIA rất cần thiết để thiết lập thế trận an ninh của một tổ chức. Biết nó là gì và cách áp dụng nó có thể giúp bạn hiểu rõ hơn cách các nhóm bảo mật hoạt động để bảo vệ các tổ chức và những người mà họ phục vụ.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

2.3. Practice: Use the CIA triad in workplace situations – Thực hành: Sử dụng bộ ba CIA trong các tình huống tại nơi làm việc

Scenario	CIA triad component
You recently shopped at Store Y and verify you were charged correctly.	Integrity
You frequently sign into your bank account to check your balances.	Availability
You must use two-factor authentication before signing into an employee portal.	Confidentiality

Kịch bản	Thành phần bộ ba CIA
Gần đây bạn đã mua sắm tại Cửa hàng Y và xác minh rằng bạn đã được tính phí chính xác.	Chính trực
Bạn thường xuyên đăng nhập vào tài khoản ngân hàng để kiểm tra số dư của mình.	khả dụng
Bạn phải sử dụng xác thực hai yếu tố trước khi đăng nhập vào cổng thông tin nhân viên.	Bảo mật

2.4. Test your knowledge: The CIA triad – Kiểm tra kiến thức của bạn: Bộ ba CIA

3. NIST frameworks – NIST frameworks

3.1. NIST frameworks – NIST frameworks

Welcome back. Before we get started, let's quickly review the purpose of frameworks. Organizations use frameworks as a starting point to develop plans that mitigate risks, threats, and vulnerabilities to sensitive data and assets. Fortunately, there are organizations worldwide that create frameworks security professionals can use to develop those plans.

Chào mừng trở lại. Trước khi chúng ta bắt đầu,Hãy nhanh chóng xem lại mục đích của các framework.Các tổ chức sử dụng các khuôn khổ nhưđiểm khởi đầu để phát triển các kế hoạch giảm thiểu rủi ro,các mối đe dọa và điểm yếu đối vớidữ liệu và tài sản nhạy

cảm.May mắn thay, có những tổ chức trên toàn thế giớitạo các chuyên gia bảo mật khuôn khổcó thể sử dụng để phát triển những kế hoạch đó.

In this video, we'll discuss two of the National Institute of Standards and Technology, or NIST's frameworks that can support ongoing security efforts for all types of organizations, including for profit and nonprofit businesses, as well as government agencies. While NIST is a US based organization, the guidance it provides can help analysts all over the world understand how to implement essential cybersecurity practices. One NIST framework that we'll discuss throughout the program is the NIST Cybersecurity Framework, or CSF.

Trong video này, chúng ta sẽ thảo luận về hai trong sốViện Tiêu chuẩn và Công nghệ Quốc gia,hoặc các khuôn khổ của NIST có thể hỗ trợnỗ lực bảo mật liên tục cho tất cả các loại hình tổ chức,bao gồm cả các hoạt động kinh doanh vì lợi nhuận và phi lợi nhuận,cũng như các cơ quan chính phủ.Mặc dù NIST là một tổ chức có trụ sở tại Hoa Kỳ,hướng dẫn mà nó cung cấp có thể giúp các nhà phân tích trên toànthế giới hiểu làm thế nào đểthực hiện các biện pháp an ninh mạng thiết yếu.Một khuôn khổ NIST mà chúng tôi sẽthảo luận xuyên suốt chương trìnhKhung bảo mật không gian mạng NIST hoặc CSF.

The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. This framework is widely respected and essential for maintaining security regardless of the organization you work for. The CSF consists of five important core functions, identify, protect, detect, respond, and recover, which we'll discuss in detail in a future video. For now, we'll focus on how the CSF benefits organizations and how it can be used to protect against threats, risks, and vulnerabilities by providing a workplace example.

CSF là một khuôn khổ tự nguyệnbao gồm các tiêu chuẩn,hướng dẫn và thực tiễn tốt nhấtđể quản lý rủi ro an ninh mạng.Khuôn khổ này được tôn trọng rộng rãi và cần thiết choduy trì an ninh bất kểtổ chức mà bạn làm việc.CSF bao gồmnăm chức năng cốt lõi quan trọng, xác định,bảo vệ, phát hiện, phản hồi và phục hồi,mà chúng ta sẽ thảo luận chi tiết trong video sau.Hiện tại, chúng ta sẽ tập trung vàoCSF mang lại lợi ích như thế nào cho các tổ chứcvà cách nó có thể được sử dụng để bảo vệ khỏi các mối đe dọa,rủi ro và tình trạng dễ bị tổn thương bởicung cấp một ví dụ về nơi làm việc

Imagine that one morning you receive a high-risk notification that a workstation has been compromised. You identify the workstation, and discover that there's an unknown device plugged into it. You block the unknown device remotely to stop any potential threat and protect the organization. Then you remove the infected workstation to prevent the spread of the damage and use tools to detect any additional

threat actor behavior and identify the unknown device. You respond by investigating the incident to determine who used the unknown device, how the threat occurred, what was affected, and where the attack originated.

Hãy tưởng tượng rằng một buổi sáng bạn nhận đượcmột thông báo có nguy cơ cao rằngmột máy trạm đã bị xâm phạm.Bạn xác định máy trạm,và khám phá ra rằng cómột thiết bị không xác định được cắm vào nó.Bạn chặn thiết bị không xác định từ xa để dừngbất kỳ mối đe dọa tiềm tàng nào và bảo vệ tổ chức.Sau đó bạn loại bỏ máy trạm bị nhiễm bệnhđể ngăn chặn sự lây lan của thiệt hại và sử dụngcông cụ để phát hiện thêm bất kỳ hành vi nào của tác nhân đe dọavà xác định thiết bị không xác định.Bạn phản ứng bằng cách điều trasự cố để xác định ai đã sử dụng thiết bị không xác định,mối đe dọa xảy ra như thế nào,những gì bị ảnh hưởng và cuộc tấn công bắt nguồn từ đâu.

In this case, you discover that an employee was charging their infected phone using a USB port on their work laptop. Finally, you do your best to recover any files or data that were affected and correct any damage the threat caused to the workstation itself.

Trong trường hợp này, bạn phát hiện ra rằng một nhân viên đang tính phíđiện thoại bị nhiễm bệnh của họ đang sử dụngmột cổng USB trên máy tính xách tay làm việc của họ.Cuối cùng, bạn cố gắng hết sức đểkhôi phục bất kỳ tập tin hoặc dữ liệu nàobị ảnh hưởng và khắc phục mọi hư hỏngmối đe dọa gây ra cho chính máy trạm.

As demonstrated by the previous example, the core functions of the NIST CSF provide specific guidance and direction for security professionals. This framework is used to develop plans to handle an incident appropriately and quickly to lower risk, protect an organization against a threat, and mitigate any potential vulnerabilities. The NIST CSF also expands into the protection of the United States federal government with NIST special publication, or SP 800-53. It provides a unified framework for protecting the security of information systems within the federal government, including the systems provided by private companies for federal government use.

Như đã được chứng minh bằng ví dụ trước,các chức năng cốt lõi của NIST CSF cung cấphướng dẫn cụ thể vàđịnh hướng cho các chuyên gia an ninh.Khung này được sử dụng để phát triển các kế hoạch xử lýxử lý sự cố một cách thích hợp và nhanh chóng để giảm thiểu rủi ro,bảo vệ một tổ chức chống lại một mối đe dọa,và giảm thiểu mọi lỗ hổng tiềm ẩn.NIST CSF cũng mở rộng sang việc bảo vệchính phủ liên bang Hoa Kỳ vớiẤn phẩm đặc biệt của NIST, hoặc SP 800-53.Nó cung cấp một khuôn khổ thống nhất để bảo vệsự an toàn của hệ thống thông tintrong chính phủ liên bang,bao gồm các hệ thống được cung cấp bởicác công ty tư nhân để chính phủ liên bang sử dụng.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

The security controls provided by this framework are used to maintain the CIA triad for those systems used by the government. Isn't it amazing how all of these frameworks and controls work together. We've discussed some really important security topics in this video that will be very useful for you as you continue your security journey. Because they're core elements of the security profession, the NIST CSF is a useful framework that most security professionals are familiar with, and having an understanding of the NIST, SP 800-53 is crucial if you have an interest in working for the US federal government. Coming up, we'll continue to explore the five NIST CSF functions and how organizations use them to protect assets and data.

Các biện pháp kiểm soát an ninh được cung cấp bởikhuôn khổ này được sử dụng để duy trìbộ ba CIA cho những hệ thống được chính phủ sử dụng.Thật tuyệt vời phải không khi tất cảcác khuôn khổ và điều khiển này hoạt động cùng nhau.Chúng ta đã thảo luận về một số chủ đề bảo mật thực sự quan trọngtrong video này sẽrất hữu ích cho bạnkhi bạn tiếp tục hành trình bảo mật của mình.Bởi vì chúng là những yếu tố cốt lõi của ngành an ninh,NIST CSF làmột khuôn khổ hữu íchhầu hết các chuyên gia bảo mật đều quen thuộc với,và có sự hiểu biết về NIST,SP 800-53 rất quan trọngnếu bạn có hứng thú vớilàm việc cho chính phủ liên bang Hoa Kỳ.Sắp tới chúng ta sẽ tiếp tục khám phánăm chức năng NIST CSF vàcách các tổ chức sử dụng chúng để bảo vệ tài sản và dữ liệu.

3.2. Explore the five functions of the NIST Cybersecurity Framework – Khám phá năm chức năng của Khung an ninh mạng NIST

Hello again! I'm excited you're here. We have so much to discuss. Previously, we covered the uses and benefits of the NIST CSF. In this video, we'll focus specifically on the five core functions of the NIST CSF framework. Let's get started.

Xin chào lần nữa! Tôi rất vui vì bạn ở đây.Chúng ta có rất nhiều điều để thảo luận.Trước đây chúng ta đã đề cập đến việc sử dụngvà lợi ích của NIST CSF.Trong video này, chúng tôi sẽ tập trung cụ thể vàonăm chức năng cốt lõi của khung NIST CSF.Bắt đầu nào.

NIST CSF focuses on five core functions: identify, protect, detect, respond, and recover. These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Basically, when it comes to security operations, NIST CSF functions are key for making sure an organization is protected against potential threats, risks, and vulnerabilities. So let's take a little time to explore how each function can be used to improve an organization's security.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

NIST CSF tập trung vào năm chức năng cốt lõi: xác định,bảo vệ, phát hiện, phản hồi và phục hồi.Những chức năng cốt lõi này giúptổ chức quản lý rủi ro an ninh mạng,thực hiện các chiến lược quản lý rủi ro,và học hỏi từ những sai lầm trước đó.Về cơ bản, khi nói đến hoạt động bảo mật,Các hàm NIST CSF làchìa khóa để đảm bảo một tổ chứcđược bảo vệ chống lại các mối đe dọa tiềm tàng,rủi ro và tình trạng dễ bị tổn thương.Vì vậy chúng ta hãy dành chút thời gian để khám phá cáchmỗi chức năng có thể được sử dụng đểcải thiện an ninh của một tổ chức.

The first core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. For example, as a security analyst, you may be asked to monitor systems and devices in your organization's internal network to identify potential security issues

Chức năng cốt lõi đầu tiên làxác định, có liên quan đến việc quản lýRủi ro an ninh mạng và ảnh hưởng của nó tớicon người và tài sản của một tổ chức.Ví dụ, với tư cách là một nhà phân tích chứng khoán,bạn có thể được yêu cầu giám sát các hệ thống và thiết bị trongmạng nội bộ của tổ chức bạn để xác địnhvấn đề bảo mật tiềm ẩn

The second core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.

Chức năng cốt lõi thứ hai là bảo vệ, đó là chiến lượcđược sử dụng để bảo vệ một tổ chứcthông qua việc thực hiện các chính sáchquy trình, đào tạo,và các công cụ giúp giảm thiểu các mối đe dọa an ninh mạng.

For example, as a security analyst, you and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.

Ví dụ, với tư cách là một nhà phân tích chứng khoán,bạn và nhóm của bạn có thể gặp phảicác mối đe dọa và tấn công mới và lạ.Vì vậy, việc nghiên cứu các dữ liệu lịch sử vàcải thiện chính sáchvà thủ tục là cần thiết.

The third core function is detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections. For example, as an analyst, you might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the

security team about any potential threats or incidents. The fourth function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

Chức năng cốt lõi thứ ba là phát hiện,có nghĩa là xác định các sự cố bảo mật tiềm ẩnvà nâng cao khả năng giám sát đểtăng tốc độ và hiệu quả của việc phát hiện.Ví dụ, với tư cách là một nhà phân tích,bạn có thể được yêu cầu xem lạithiết lập công cụ bảo mật mới để đảm bảo nó được gắn cờ ở mức thấp,rủi ro trung bình hoặc cao,và sau đó cảnh báo đội an ninh vềbất kỳ mối đe dọa hoặc sự cố tiềm ẩn nào.Chức năng thứ tư là phản hồi, có nghĩa là thực hiệnđảm bảo rằng các thủ tục thích hợp được sử dụng để ngăn chặn,trung hòa,và phân tích các sự cố bảo mật, vàthực hiện các cải tiến đối với quy trình bảo mật.

As an analyst, you could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.

Là một nhà phân tích, bạn có thểlàm việc với một nhóm để thu thập vàtổ chức dữ liệu để ghi lại một sự cố và đề xuấtcải tiến các quy trình đểngăn chặn sự việc xảy ra lần nữa.

The fifth core function is recover, which is the process of returning affected systems back to normal operation.

Chức năng cốt lõi thứ năm làphục hồi, đó là quá trìnhđưa các hệ thống bị ảnh hưởng trở lại hoạt động bình thường.

For example, as an entry-level security analyst, you might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

Ví dụ, với tư cách là một nhà phân tích bảo mật cấp đầu vào,bạn có thể làm việc với nhóm bảo mật của mìnhđể khôi phục hệ thống,dữ liệu và tài sản, chẳng hạn nhưhồ sơ tài chính hoặc pháp lý, cóbị ảnh hưởng bởi một sự cố như vi phạm.

We've covered a lot of information in this video. Hopefully, it helped you understand the value of learning about the NIST CSF and its five core functions.

Chúng tôi đã đề cập đến rất nhiều thông tin trong video này.Hy vọng nó đã giúp được bạnhiểu giá trị của việc học vềNIST CSF và năm chức năng cốt lõi của nó.

From proactive to reactive measures, all five functions are essential for making sure that an organization has effective security strategies in place.

Từ biện pháp chủ động đến biện pháp phản ứng, cả năm chức năng đều được thực hiệncần thiết để đảm bảo rằng một tổ chứccó chiến lược bảo mật hiệu quả tại chỗ.

Security incidents are going to happen, but an organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk.

Sự cố an ninh sẽ xảy ra,nhưng một tổ chức phải cókhả năng phục hồi nhanh chóng saubất kỳ thiệt hại nào do sự cố gây radể giảm thiểu mức độ rủi ro của họ.

Coming up, we'll discuss security principles that work hand-in-hand with NIST frameworks and the CIA triad to help protect critical data and assets.

Sắp tới chúng ta sẽ thảo luậnnguyên tắc bảo mật phối hợp chặt chẽ vớiKhuôn khổ NIST và bộ ba CIAđể giúp bảo vệ dữ liệu và tài sản quan trọng.

3.3. Test your knowledge: NIST frameworks – Kiểm tra kiến thức của bạn: khung NIST

4. OWASP principles and security audits – Nguyên tắc OWASP và kiểm tra bảo mật

4.1. OWASP security principles – Nguyên tắc bảo mật OWASP

It's important to understand how to protect an organization's data and assets because that will be part of your role as a security analyst. Fortunately, there are principles and guidelines that can be used, along with NIST frameworks and the CIA triad, to help security teams minimize threats and risks.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Điều quan trọng là phải hiểu cách bảo vệdữ liệu và tài sản của một tổ chứcbởi vì đó sẽ là một phần củavai trò của bạn là một nhà phân tích bảo mật.May mắn thay, có những nguyên tắc vàhướng dẫn có thể được sử dụng, cùng vớikhuôn khổ NIST và bộ ba CIA, đểgiúp các nhóm bảo mật giảm thiểu các mối đe dọa và rủi ro.

In this video, we'll explore some Open Web Application Security Project, or OWASP, security principles that are useful to know as an entry-level analyst.

Trong video này, chúng ta sẽ khám phá một số tính năng MởDự án bảo mật ứng dụng web hoặc OWASP,nguyên tắc bảo mật đượchữu ích khi biết với tư cách là một nhà phân tích cấp đầu vào.

The first OWASP principle is to minimize the attack surface area. An attack surface refers to all the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses. Examples of common attack vectors are phishing emails and weak passwords. To minimize the attack surface and avoid incidents from these types of vectors, security teams might disable software features, restrict who can access certain assets, or establish more complex password requirements.

Nguyên tắc OWASP đầu tiên làgiảm thiểu diện tích bề mặt tấn công.Một bề mặt tấn công đề cập đếntất cả các lỗ hổng tiềm ẩnmà kẻ đe dọa có thể khai thác,giống như các vectơ tấn công, là những con đườngkẻ tấn công sử dụng để xâm nhập vào hệ thống phòng thủ an ninh.Ví dụ về các vectơ tấn công phổ biến làemail lừa đảo và mật khẩu yếu.Để giảm thiểu bề mặt tấn côngvà tránh những sự cố từ những loại nàyvectơ, đội bảo mật có thể vô hiệu hóa các tính năng của phần mềm,hạn chế người có thể truy cập vào một số tài sản nhất định hoặcthiết lập các yêu cầu mật khẩu phức tạp hơn.

The principle of least privilege means making sure that users have the least amount of access required to perform their everyday tasks. The main reason for limiting access to organizational information and resources is to reduce the amount of damage a security breach could cause. For example, as an entry-level analyst, you may have access to log data, but may not have access to change user permissions. Therefore, if a threat actor compromises your credentials, they'll only be able to gain limited access to digital or physical assets, which may not be enough for them to deploy their intended attack.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Nguyên tắc đặc quyền tối thiểucó nghĩa là đảm bảo rằng người dùng cólượng truy cập ít nhấtcần thiết để thực hiện các công việc hàng ngày của họ.Nguyên nhân chính của việc hạn chế truy cậpđến thông tin tổ chức vànguồn lực là giảm số lượngthiệt hại mà vi phạm an ninh có thể gây ra.Ví dụ, với tư cách là một nhà phân tích cấp đầu vào,bạn có thể có quyền truy cập vào dữ liệu nhật ký,nhưng có thể không có quyền truy cập để thay đổi quyền của người dùng.Vì vậy, nếukẻ đe dọa xâm phạm thông tin đăng nhập của bạn,họ sẽ chỉ có thể đạt đượcquyền truy cập hạn chế vào tài sản kỹ thuật số hoặc vật chất,điều đó có thể không đủ để họtriển khai cuộc tấn công dự định của họ.

The next principle we'll discuss is defense in depth. Defense in depth means that an organization should have multiple security controls that address risks and threats in different ways. One example of a security control is multi-factor authentication, or MFA, which requires users to take an additional step beyond simply entering their username and password to gain access to an application. Other controls include firewalls, intrusion detection systems, and permission settings that can be used to create multiple points of defense, a threat actor must get through to breach an organization.

Nguyên tắc tiếp theo chúng ta sẽ thảo luận là phòng thủ theo chiều sâu.Phòng thủ theo chiều sâu có nghĩa là một tổ chức cần phải cónhiều biện pháp kiểm soát bảo mậtgiải quyết các rủi ro và mối đe dọa theo những cách khác nhau.Một ví dụ về kiểm soát an ninh làxác thực đa yếu tố hoặc MFA,đòi hỏi người dùng phải thực hiệnmột bước bổ sung ngoài việc đơn giảnnhập tên người dùng của họ vàmật khẩu để truy cập vào một ứng dụng.Các biện pháp kiểm soát khác bao gồm tường lửa,hệ thống phát hiện xâm nhập,và cài đặt quyền có thểđược sử dụng để tạo ra nhiều điểm phòng thủ,kẻ đe dọa phải vượt quađể xâm phạm một tổ chức.

Another principle is separation of duties, which can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system. For example, the person in a company who signs the paychecks shouldn't also be the person who prepares them.

Một nguyên tắc khác là phân chia nhiệm vụ,có thể được sử dụng để ngăn chặn các cá nhân khỏithực hiện các hoạt động gian lận hoặc bất hợp pháp.Nguyên tắc này có nghĩa là không ai được giaonhiều đặc quyền đến mức họ có thể lạm dụng hệ thống.Ví dụ, một người trong công ty kýtiền lương cũng không nênhãy là người chuẩn bị chúng.

Only two more principles to go! You're doing great. Keep security simple is the next principle. As the name suggests, when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable. The more complex the security controls are, the harder it is for people to work collaboratively.

Chỉ còn hai nguyên tắc nữa thôi! Bạn đang làm rất tốt.Giữ an ninh đơn giản lànguyên tắc tiếp theo. Đúng như tên gọi,khi thực hiện các biện pháp kiểm soát an ninh,những giải pháp phức tạp không cần thiết nêntránh được vì chúng có thể trở nên không thể quản lý được.Việc kiểm soát an ninh càng phức tạp thìmọi người càng khó hợp tác làm việc.

The last principle is to fix security issues correctly. Technology is a great tool, but can also present challenges. When a security incident occurs, security professionals are expected to identify the root cause quickly. From there, it's important to correct any identified vulnerabilities and conduct tests to ensure that repairs are successful.

Nguyên tắc cuối cùng là khắc phục vấn đề bảo mật một cách chính xác.Công nghệ là một công cụ tuyệt vời,nhưng cũng có thể đưa ra những thách thức.Khi xảy ra sự cố an ninh,các chuyên gia bảo mật dự kiến sẽxác định nguyên nhân gốc rễ một cách nhanh chóng.Từ đó, điều quan trọng là phải sửabất kỳ lỗ hổng nào được xác định vàtiến hành kiểm tra để đảm bảo rằng việc sửa chữa thành công.

An example of an issue is a weak password to access an organization's wifi because it could lead to a breach. To fix this type of security issue, stricter password policies could be put in place.

Một ví dụ về vấn đề là mật khẩu yếu đểtruy cập wifi của tổ chứcvì nó có thể dẫn đến vi phạm.Để khắc phục loại vấn đề bảo mật này,chính sách mật khẩu chặt chẽ hơn có thể được đưa ra.

I know we've covered a lot, but understanding these principles increases your overall security knowledge and can help you stand out as a security professional.

Tôi biết chúng ta đã đề cập rất nhiều,nhưng việc hiểu những nguyên tắc này sẽ tăng lênkiến thức bảo mật tổng thể của bạnvà có thể giúp bạn nổi bật như một chuyên gia bảo mật.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

4.2. More about OWASP security principles – Tìm hiểu thêm về nguyên tắc bảo mật OWASP

More about OWASP security principles

Tìm hiểu thêm về nguyên tắc bảo mật OWASP

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

Trước đây, bạn đã biết rằng các nhà phân tích an ninh mạng giúp giữ an toàn cho dữ liệu và giảm thiểu rủi ro cho tổ chức bằng cách sử dụng nhiều khung bảo mật, biện pháp kiểm soát và nguyên tắc bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu thêm về 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), các nguyên tắc bảo mật và cách các nhà phân tích cấp đầu vào sử dụng chúng.

Security principles

Nguyên tắc bảo mật

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event management (SIEM) dashboard, or using a vulnerability scanner, you will use these principles in some way.

Tại nơi làm việc, các nguyên tắc bảo mật được đưa vào công việc hàng ngày của bạn. Cho dù bạn đang phân tích nhật ký, giám sát bảng thông tin bảo mật và quản lý sự kiện (SIEM) hay sử dụngmáy quét lỗ hổng, bạn sẽ sử dụng những nguyên tắc này theo một cách nào đó.

Previously, you were introduced to several OWASP security principles. These included:

- **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
- **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
- **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.
- **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
- **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
- **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

Trước đây, bạn đã được giới thiệu một số nguyên tắc bảo mật của OWASP. Những điều đó được bao gồm:

- **Giảm thiểu diện tích bề mặt tấn công** : Bề mặt tấn công đề cập đến tất cả các lỗ hổng tiềm ẩn mà tác nhân đe dọa có thể khai thác.
- **Nguyên tắc đặc quyền tối thiểu** : Người dùng có ít quyền truy cập cần thiết nhất để thực hiện các công việc hàng ngày của mình.
- **Phòng thủ theo chiều sâu** : Các tổ chức nên có các biện pháp kiểm soát bảo mật khác nhau để giảm thiểu rủi ro và mối đe dọa.
- **Phân chia nhiệm vụ** : Các hoạt động quan trọng phải dựa vào nhiều người, mỗi người tuân theo nguyên tắc ít đặc quyền nhất.
- **Giữ an ninh đơn giản** : Tránh các giải pháp phức tạp không cần thiết. Sự phức tạp làm cho việc bảo mật trở nên khó khăn.
- **Khắc phục sự cố bảo mật một cách chính xác** : Khi xảy ra sự cố bảo mật, hãy xác định nguyên nhân gốc rễ, ngăn chặn tác động, xác định lỗ hổng và tiến hành kiểm tra để đảm bảo việc khắc phục thành công.

Additional OWASP security principles

Nguyên tắc bảo mật OWASP bổ sung

Next, you'll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

Tiếp theo, bạn sẽ tìm hiểu về bốn nguyên tắc bảo mật OWASP bổ sung mà các nhà phân tích an ninh mạng và nhóm của họ sử dụng để giữ an toàn cho hoạt động của tổ chức và mọi người.

Establish secure defaults

Thiết lập mặc định an toàn

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

Nguyên tắc này có nghĩa là trạng thái bảo mật tối ưu của ứng dụng cũng là trạng thái mặc định của ứng dụng đó đối với người dùng; sẽ phải mất thêm công sức để làm cho ứng dụng không an toàn.

Fail securely

Thất bại một cách an toàn

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

Thất bại một cách an toàn có nghĩa là khi một điều khiển bị lỗi hoặc dừng, nó sẽ thực hiện điều đó bằng cách đặt mặc định thành tùy chọn an toàn nhất. Ví dụ: khi tường lửa bị lỗi, nó chỉ cần đóng tất cả các kết nối và chặn tất cả các kết nối mới thay vì bắt đầu chấp nhận mọi kết nối.

Don't trust services

Đừng tin tưởng vào dịch vụ

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn't explicitly trust that their partners' systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

Nhiều tổ chức làm việc với các đối tác bên thứ ba. Những đối tác bên ngoài này thường có các chính sách bảo mật khác với tổ chức. Và tổ chức không nên tin tưởng một cách rõ ràng rằng hệ thống của đối tác của họ được an toàn. Ví dụ: nếu nhà cung cấp bên thứ ba theo dõi điểm thưởng cho khách hàng của hãng hàng không thì hãng hàng không phải đảm bảo rằng số dư là chính xác trước khi chia sẻ thông tin đó với khách hàng của họ.

Avoid security by obscurity

Tránh bảo mật bằng cách tối nghĩa

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):

Tính bảo mật của các hệ thống quan trọng không nên dựa vào việc giấu kín các chi tiết. Hãy xem xét ví dụ sau từ OWASP (2016):

The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

Tính bảo mật của ứng dụng không nên dựa vào việc giữ bí mật mã nguồn. Tính bảo mật của nó phải dựa vào nhiều yếu tố khác, bao gồm chính sách mật khẩu hợp lý, bảo vệ chuyên sâu, giới hạn giao dịch kinh doanh, kiến trúc mạng vững chắc cũng như kiểm soát gian lận và kiểm toán.

Key takeaways

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Bài học chính

Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.

Các chuyên gia an ninh mạng không ngừng áp dụng các nguyên tắc bảo mật để bảo vệ các tổ chức và những người mà họ phục vụ. Với tư cách là nhà phân tích bảo mật cấp độ đầu vào, bạn có thể sử dụng các nguyên tắc bảo mật này để thúc đẩy các phương pháp phát triển an toàn nhằm giảm thiểu rủi ro cho cả công ty và người dùng.

4.3. Wajih: Stay up-to-date on the latest cybersecurity threats – Wajih: Luôn cập nhật các mối đe dọa an ninh mạng mới nhất

My name is Wajih and I'm a security engineer at Google working in the digital forensics department. Do you need a background in cybersecurity? No you don't. My past experiences is working at a water park as a snow cone machine guy. I worked at a movie theater selling popcorn in concession stands. During my undergrad, I was a bio major at first like my freshman year. I met someone in a bus who was mentioning about this cool cybersecurity startup that just sounded really cool. Some strategies I leveraged to keep up to date on the latest cybersecurity trends is going on online forums such as Medium to research different security trends and topics. I personally use Medium a lot as I could filter by the tag of like I want to find articles related to cybersecurity and or I want to find articles related to cloud security. Based off their filtering algorithm, I just go on and see like what other people are talking about and then that's what helps me keep up to date. If it's more of like networking that you're looking forward to, then I highly recommend just going out to those like conferences. My advice for people wanting to get into cybersecurity is don't be too overwhelmed with trying to understand every single specialization within cybersecurity. There's so much going on within the cybersecurity field in terms of trends and it's nice to stay up to date with all of those but sometimes you need to take a step back and prioritize what subjects within cybersecurity you are staying most up to date like on. I love this job. I love the challenges. I feel like there is a shortage in cybersecurity professionals out there from just past experiences, hearing from other friends in computer science fields. Most of them say that oh it's too hard, too complicated to get in. Don't listen to those people. I encourage you to push through. It's definitely well worth it. First just get the fundamentals down and be persistent.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Tên tôi là Wajih vàTôi là kỹ sư bảo mật tại Google làm việc trong bộ phận điều tra kỹ thuật số.Bạn có cần kiến thức nền tảng về an ninh mạng không?Không, bạn không.Kinh nghiệm trước đây của tôi là làm việc tại công viên nước với tư cách là một người làm máy tạo nón tuyết.Tôi làm việc tại một rạp chiếu phim bán bỏng ngô ở các quầy nhượng quyền.Trong thời gian học đại học, ban đầu tôi học chuyên ngành sinh học giống như năm thứ nhất.Tôi gặp một người trên xe buýt và người đó đang nhắc đến điều thú vị nàycông ty khởi nghiệp về an ninh mạng nghe có vẻ rất thú vị.Một số chiến lược tôi đã tận dụng để cập nhật thông tin mới nhấtxu hướng an ninh mạng đang diễn ra trên các diễn đàn trực tuyến như Medium tớinghiên cứu các xu hướng và chủ đề bảo mật khác nhau.Cá nhân tôi sử dụng Medium rất nhiều vì tôi có thể lọc theo thểnhư tôi muốn tìm những bài viết liên quan đến an ninh mạng vàhoặc tôi muốn tìm các bài viết liên quan đến bảo mật đám mây.Dựa trên thuật toán lọc của họ, tôi chỉ cần tiếp tục và xem những gì người khác làmđang nói đến và đó là điều giúp tôi cập nhật.Nếu nó giống với việc kết nối mạng hơn mà bạn mong đợi,thì tôi thực sự khuyên bạn chỉ nên đến những nơi như hội nghị.Lời khuyên của tôi dành cho những người muốn tham gia vào lĩnh vực an ninh mạng là đừng quá choáng ngợpvới việc cố gắng hiểu mọi chuyên môn trong lĩnh vực an ninh mạng.Có rất nhiều điều đang diễn ra trong lĩnh vực an ninh mạng về các xu hướng vàthật tuyệt khi được cập nhật tất cả những điều đó nhưngđôi khi bạn cần lùi lại một bước và ưu tiên những môn học nàotrong lĩnh vực an ninh mạng, bạn luôn cập nhật nhất như trên.Tôi yêu công việc này.Tôi yêu những thử thách.Tôi cảm thấy hiện nay đang có sự thiếu hụt chuyên gia an ninh mạng từchỉ là những kinh nghiệm đã qua, nghe được từ những người bạn khác trong lĩnh vực khoa học máy tính.Hầu hết họ đều nói rằng ôi nó quá khó, quá phức tạp để vào được.Đừng nghe những người đó.Tôi khuyến khích bạn vượt qua.Nó chắc chắn rất có giá trị.Đầu tiên chỉ cần nắm vững những nguyên tắc cơ bản và kiên trì.

4.4. Plan a security audit – Lập kế hoạch kiểm tra an ninh

Now that we've covered different frameworks, controls, security principles, and compliance regulations, the question is: How do they all work together?

Bây giờ chúng ta đã đề cập đến các framework khác nhau,kiểm soát, nguyên tắc bảo mật,và các quy định tuân thủ, câu hỏi đặt ra là:Làm thế nào để tất cả họ làm việc cùng nhau?

The answer to that question is by conducting security audits. A security audit is a review of an organization's security controls, policies, and procedures against a set of expectations.

Câu trả lời cho câu hỏi đó làbằng cách tiến hành kiểm tra an ninh.Kiểm toán an ninh là việc xem xétkiểm soát an ninh của một tổ chức,các chính sách và thủ tục đi ngược lại với một loạt các kỳ vọng.

There are two main types of security audits: external and internal. We'll focus on internal security audits because those are the types of audits that entry-level analysts might be asked to contribute to.

Có hai loại chínhkiểm tra an ninh: bên ngoài và nội bộ.Chúng tôi sẽ tập trung vào kiểm tra an ninh nội bộvì đó là những loạicác cuộc kiểm toán mà các nhà phân tích cấp đầu vàocó thể được yêu cầu đóng góp.

An internal security audit is typically conducted by a team of people that might include an organization's compliance officer, security manager, and other security team members. Internal security audits are used to help improve an organization's security posture and help organizations avoid fines from governing agencies due to a lack of compliance. Internal security audits help security teams identify organizational risk, assess controls, and correct compliance issues.

Kiểm toán an ninh nội bộ làthường được thực hiện bởi một nhómnhững người có thể bao gồmnhân viên tuân thủ của một tổ chức,người quản lý bảo mật và các thành viên khác trong nhóm bảo mật.Kiểm toán an ninh nội bộ được sử dụng để giúp cải thiệntình hình an ninh của một tổ chức và giúp đỡ các tổ chứctránh bị phạt từ chính quyềncơ quan do thiếu sự tuân thủ.Trợ giúp kiểm tra an ninh nội bộđội bảo mật xác định rủi ro tổ chức,đánh giá các biện pháp kiểm soát và khắc phục các vấn đề tuân thủ.

Now that we've discussed the purposes of internal audits, let's cover some common elements of internal audits. These include establishing the scope and goals of the audit, conducting a risk assessment of the organization's assets, completing a controls assessment, assessing compliance, and communicating results to stakeholders.

Bây giờ chúng ta đã thảo luận về mục đích của kiểm toán nội bộ,chúng ta hãy đề cập đến một số yếu tố phổ biến của kiểm toán nội bộ.Chúng bao gồm việc thiết lập phạm vivà mục tiêu của cuộc kiểm toán,tiến hành đánh giá rủi rovề tài sản của tổ chức,hoàn thành đánh giá kiểm soát,đánh giá sự tuân thủ,và thông báo kết quả cho các bên liên quan.

In this video, we'll cover the first two elements, which are a part of the audit planning process: establishing the scope and goals, then completing a risk assessment.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Trong video này, chúng tôi sẽ đề cập đếnhai phần tử đầu tiên, đó làMột phần của quá trình lập kế hoạch kiểm toán:thiết lập phạm vi và mục tiêu,sau đó hoàn thành việc đánh giá rủi ro.

Scope refers to the specific criteria of an internal security audit. Scope requires organizations to identify people, assets, policies, procedures, and technologies that might impact an organization's security posture. Goals are an outline of the organization's security objectives, or what they want to achieve in order to improve their security posture.

Phạm vi đề cập đến các tiêu chí cụ thểcủa một cuộc kiểm toán an ninh nội bộ.Phạm vi yêu cầu tổ chức xác định con người, tài sản,Chính sách & Thủ tục,và những công nghệ có thểtác động đến tình hình an ninh của tổ chức.Mục tiêu là một phác thảo củamục tiêu an ninh của tổ chức,hoặc những gì họ muốn đạt đượcnhằm cải thiện tình hình an ninh của họ.

Although more senior-level security team members and other stakeholders usually establish the scope and goals of the audit, entry-level analysts might be asked to review and understand the scope and goals in order to complete other elements of the audit.

Mặc dù có nhiều thành viên nhóm bảo mật cấp cao hơn vàcác bên liên quan khác thường thiết lậpphạm vi và mục tiêu của cuộc kiểm toán,các nhà phân tích cấp đầu vào có thểyêu cầu xem xét và hiểuphạm vi và mục tiêu đểhoàn thiện các phần khác của cuộc kiểm toán.

As an example, the scope of this audit involves assessing user permissions; identifying existing controls, policies, and procedures; and accounting for the technology currently in use by the organization. The goals outlined include implementing core functions of frameworks, like the NIST CSF; establishing policies and procedures to ensure compliance; and strengthening system controls.

Ví dụ, phạm vi củaquá trình kiểm tra này liên quan đến việc đánh giá quyền của người dùng;xác định các biện pháp kiểm soát, chính sách hiện có,và thủ tục; và hạch toáncông nghệ hiện đang được tổ chức sử dụng.Các mục tiêu được nêu ra bao gồmthực hiện các chức năng cốt lõi của framework,như NIST CSF;thiết lập các chính sách và thủ tục để đảm bảoTuân thủ; và tăng cường kiểm soát hệ thống.

The next element is conducting a risk assessment, which is focused on identifying potential threats, risks, and vulnerabilities. This helps organizations consider what security measures should be implemented and monitored to ensure the safety of assets. Similar to establishing the scope and goals, a risk assessment is oftentimes completed by managers or other stakeholders. However, you might be asked to analyze details provided in the risk assessment to consider what types of controls and compliance regulations need to be in place to help improve the organization's security posture.

Yếu tố tiếp theo là tiến hành đánh giá rủi ro,tập trung vào việc xác địnhcác mối đe dọa, rủi ro và điểm yếu tiềm ẩn.Điều này giúp các tổ chức xem xétnhững biện pháp an ninh nênđược thực hiện và giám sátđể đảm bảo an toàn cho tài sản.Tương tự như việc thiết lập phạm vi và mục tiêu,việc đánh giá rủi ro đôi khi làđược hoàn thành bởi các nhà quản lý hoặc các bên liên quan khác.Tuy nhiên, bạn có thể được yêu cầu phân tíchchi tiết được cung cấp trong đánh giá rủi rođể xem xét những loạiquy định kiểm soát và tuân thủcần phải có mặt để giúp đỡcải thiện tình hình an ninh của tổ chức.

For example, this risk assessment highlights that there are inadequate controls, processes, and procedures in place to protect the organization's assets. Specifically, there is a lack of proper management of physical and digital assets, including employee equipment. The equipment used to store data is not properly secured. And access to private information stored in the organization's internal network likely needs more robust controls in place. Now that we've discussed the initial planning elements of an internal security audit, coming up, we'll focus on the last three elements.

Ví dụ, việc đánh giá rủi ro nàynhấn mạnh rằng có sự kiểm soát không đầy đủ,quy trình, thủ tục trongnơi bảo vệ tài sản của tổ chức.Đặc biệt là thiếu sự quản lý phù hợptài sản vật chất và kỹ thuật số,bao gồm cả thiết bị của nhân viên.Thiết bị dùng đểlưu trữ dữ liệu không được bảo mật đúng cách.Và quyền truy cập vào thông tin cá nhân được lưu trữ trongmạng nội bộ của tổ chứccó thể cần có những biện pháp kiểm soát mạnh mẽ hơn.Bây giờ chúng ta đã thảo luậncác yếu tố lập kế hoạch ban đầucủa kiểm toán an ninh nội bộ,sắp tới, chúng ta sẽ tập trung vào ba yếu tố cuối cùng.

4.5. Complete a security audit – Hoàn thành kiểm tra bảo mật

Previously, we discussed the initial planning elements of an internal security audit. In this video, we'll cover the final elements that an entry-level analyst might be asked to complete.

Trước đây, chúng ta đã thảo luận về các yếu tố lập kế hoạch ban đầu của mộtKiểm toán an ninh.Trong video này, chúng tôi sẽ đề cập đến các yếu tố cuối cùng mà một nhà phân tích cấp mới bắt đầucó thể được yêu cầu hoàn thành.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

As a reminder, the planning elements of internal security audits include establishing the scope and goals, then conducting a risk assessment. The remaining elements are completing a controls assessment, assessing compliance, and communicating results. Before completing these last three elements, you'll need to review the scope and goals, as well as the risk assessment, and ask yourself some questions. For example: What is the audit meant to achieve? Which assets are most at risk? Are current controls sufficient to protect those assets? If not, what controls and compliance regulations need to be implemented? Considering questions like these can support your ability to complete the next element: a controls assessment.

Xin nhắc lại, các yếu tố lập kế hoạch của kiểm tra an ninh nội bộ bao gồmthiết lập phạm vi và mục tiêu, sau đó tiến hành đánh giá rủi ro.Các yếu tố còn lại đang hoàn thiện đánh giá kiểm soát,đánh giá sự tuân thủ và thông báo kết quả.Trước khi hoàn thành ba yếu tố cuối cùng này, bạn cần xem lại phạm vi và mục tiêu,cũng như đánh giá rủi ro và tự hỏi mình một số câu hỏi.Ví dụ: Kiểm toán nhằm đạt được mục đích gì? Những tài sản nào có nguy cơ cao nhất?Các biện pháp kiểm soát hiện tại có đủ để bảo vệ những tài sản đó không?Nếu không, những biện pháp kiểm soát và quy định tuân thủ nào cần được thực hiện?Việc xem xét những câu hỏi như thế này có thể hỗ trợ khả năng của bạnđể hoàn thành yếu tố tiếp theo: đánh giá các biện pháp kiểm soát.

A controls assessment involves closely reviewing an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective. To do this, entry-level analysts might be tasked with classifying controls into the following categories: administrative controls, technical controls, and physical controls.

Đánh giá các biện pháp kiểm soát bao gồm việc xem xét chặt chẽ các hoạt động hiện tại của tổ chức.tài sản, sau đó đánh giá rủi ro tiềm ẩn đối với tài sản đó,để đảm bảo các quy trình và kiểm soát nội bộ có hiệu quả.Để làm điều này, các nhà phân tích cấp đầu vào có thể được giao nhiệm vụ phân loạikiểm soát thành các loại sau: kiểm soát hành chính,kiểm soát kỹ thuật và kiểm soát vật lý.

Administrative controls are related to the human component of cybersecurity. They include policies and procedures that define how an organization manages data, such as the implementation of password policies.

Kiểm soát hành chính có liên quan đến thành phần con người của an ninh mạng.Chúng bao gồm các chính sách và thủ tục xác định cách thức một tổ chứcquản lý dữ liệu, chẳng hạn như việc thực hiện các chính sách mật khẩu.

Technical controls are hardware and software solutions used to protect assets, such as the use of intrusion detection systems, or IDS's, and encryption.

Kiểm soát kỹ thuật là các giải pháp phần cứng và phần mềm được sử dụng để bảo vệ tài sản, chẳng hạn nhưnhư việc sử dụng các hệ thống phát hiện xâm nhập hoặc IDS và mã hóa.

Physical controls refer to measures put in place to prevent physical access to protected assets, such as surveillance cameras and locks.

Kiểm soát vật lý đề cập đến các biện pháp được đưa ra để ngăn ngừatruy cập vào các tài sản được bảo vệ, chẳng hạn như camera giám sát và ổ khóa.

The next element is determining whether or not the organization is adhering to necessary compliance regulations. As a reminder, compliance regulations are laws that organizations must follow to ensure private data remains secure. In this example, the organization conducts business in the European Union and accepts credit card payments. So they need to adhere to the GDPR and Payment Card Industry Data Security Standard, or PCI DSS.

Yếu tố tiếp theo là xác định liệutổ chức không tuân thủ các quy định tuân thủ cần thiết.Xin nhắc lại, các quy định về tuân thủ là các luật quy địnhcác tổ chức phải tuân theo để đảm bảo dữ liệu riêng tư được an toàn.Trong ví dụ này, tổ chức tiến hành kinh doanh ở Liên minh Châu Âu vàchấp nhận thanh toán bằng thẻ tín dụng.Vì vậy, họ cần tuân thủ GDPR vàTiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán hoặc PCI DSS.

The final common element of an internal security audit is communication. Once the internal security audit is complete, results and recommendations need to be communicated to stakeholders. In general, this type of communication summarizes the scope and goals of the audit. Then, it lists existing risks and notes how quickly those risks need to be addressed. Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture.

Yếu tố chung cuối cùng của kiểm tra an ninh nội bộ là giao tiếp.Khi quá trình kiểm tra an ninh nội bộ hoàn tất, kết quả vàkhuyến nghị cần được truyền đạt tới các bên liên

quan.Nhìn chung, kiểu giao tiếp này tóm tắt phạm vi vàmục tiêu của cuộc kiểm toán.Sau đó, nó liệt kê các rủi ro hiện có và ghi chú mức độ nhanh chóng mà những rủi ro đó cần được giải quyết.Ngoài ra, nó xác định các quy định tuân thủtổ chức cần tuân thủ và đưa ra các khuyến nghị chocải thiện tình hình an ninh của tổ chức.

Internal audits are a great way to identify gaps within an organization. When I worked at a previous company, my team and I conducted an internal password audit and found that many of the passwords were weak. Once we identified this issue, the compliance team took the lead and began enforcing stricter password policies. Audits are an opportunity to determine what security measures an organization has in place and what areas need to be improved to achieve the organization's desired security posture.

Kiểm toán nội bộ là một cách tuyệt vời để xác định những lỗ hổng trong một tổ chức.Khi tôi làm việc ở công ty trước đây, nhóm của tôi và tôi đã tiến hành một cuộc khảo sát nội bộkiểm tra mật khẩu và phát hiện ra rằng nhiều mật khẩu yếu.Sau khi chúng tôi xác định được vấn đề này, nhóm tuân thủ sẽ dẫn đầu vàbắt đầu thực thi các chính sách mật khẩu chặt chẽ hơn.Kiểm toán là cơ hội để xác định những biện pháp an ninh nàotổ chức đã sẵn sàng và những lĩnh vực nào cần được cải thiện đểđạt được trạng thái bảo mật mong muốn của tổ chức.

Security audits are quite involved, yet of extreme value to organizations. Later in the course, you'll have an opportunity to complete elements of an internal security audit for a fictional company, which you can include in your professional portfolio.

Kiểm toán bảo mật khá phức tạp nhưng lại có giá trị cực kỳ lớn đối với các tổ chức.Sau này trong khóa học,bạn sẽ có cơ hội hoàn thành các phần của cuộc kiểm tra bảo mật nội bộ chomột công ty hư cấu mà bạn có thể đưa vào danh mục đầu tư chuyên nghiệp của mình.

4.6. More about security audits – Tìm hiểu thêm về kiểm tra bảo mật

More about security audits

Tìm hiểu thêm về kiểm tra bảo mật

Previously, you were introduced to how to plan and complete an internal security audit. In this reading, you will learn more about security audits, including the goals and objectives of audits.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Trước đây, bạn đã được giới thiệu cách lập kế hoạch và hoàn thành kiểm tra bảo mật nội bộ. Trong bài đọc này, bạn sẽ tìm hiểu thêm về kiểm tra bảo mật, bao gồm các mục tiêu và mục tiêu của kiểm tra.

Security audits

Kiểm tra an ninh

A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations. Audits are independent reviews that evaluate whether an organization is meeting internal and external criteria. Internal criteria include outlined policies, procedures, and best practices. External criteria include regulatory compliance, laws, and federal regulations.

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. Kiểm toán là các đánh giá độc lập nhằm đánh giá liệu một tổ chức có đáp ứng các tiêu chí bên trong và bên ngoài hay không. Tiêu chí nội bộ bao gồm các chính sách, thủ tục và phương pháp thực hành tốt nhất được nêu ra. Tiêu chí bên ngoài bao gồm tuân thủ quy định, luật pháp và các quy định của liên bang.

Additionally, a security audit can be used to assess an organization's established security controls. As a reminder, **security controls** are safeguards designed to reduce specific security risks.

Ngoài ra, kiểm tra bảo mật có thể được sử dụng để đánh giá các biện pháp kiểm soát bảo mật đã được thiết lập của tổ chức. Xin nhắc lại, **kiểm soát bảo mật** là các biện pháp bảo vệ được thiết kế để giảm các rủi ro bảo mật cụ thể.

Audits help ensure that security checks are made (i.e., daily monitoring of security information and event management dashboards), to identify threats, risks, and vulnerabilities. This helps maintain an organization’s security posture. And, if there are security issues, a remediation process must be in place.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Kiểm tra giúp đảm bảo thực hiện kiểm tra bảo mật (tức là giám sát hàng ngày thông tin bảo mật và bảng điều khiển quản lý sự kiện), để xác định các mối đe dọa, rủi ro và lỗ hổng. Điều này giúp duy trì tình trạng an ninh của tổ chức. Và nếu có vấn đề về bảo mật thì phải có quy trình khắc phục.

Goals and objectives of an audit

Mục tiêu và mục tiêu của cuộc kiểm toán

The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. The objective is to identify and address areas of remediation and growth. Audits provide direction and clarity by identifying what the current failures are and developing a plan to correct them.

Mục tiêu của kiểm toán là đảm bảo các hoạt động công nghệ thông tin (CNTT) của tổ chức đáp ứng các tiêu chuẩn của ngành và tổ chức. Mục tiêu là xác định và giải quyết các lĩnh vực cần khắc phục và tăng trưởng. Kiểm toán cung cấp định hướng và sự rõ ràng bằng cách xác định những sai sót hiện tại là gì và xây dựng kế hoạch khắc phục chúng.

Security audits must be performed to safeguard data and avoid penalties and fines from governmental agencies. The frequency of audits is dependent on local laws and federal compliance regulations.

Kiểm toán bảo mật phải được thực hiện để bảo vệ dữ liệu và tránh các hình phạt và tiền phạt từ các cơ quan chính phủ. Tần suất kiểm tra phụ thuộc vào luật pháp địa phương và các quy định tuân thủ của liên bang.

Factors that affect audits

Các yếu tố ảnh hưởng đến kiểm toán

Factors that determine the types of audits an organization implements include:

- Industry type
- Organization size
- Ties to the applicable government regulations
- A business's geographical location
- A business decision to adhere to a specific regulatory compliance

To review common compliance regulations that different organizations need to adhere to, refer to the reading about controls, frameworks, and compliance.

Các yếu tố xác định loại hình đánh giá mà tổ chức thực hiện bao gồm:

- Loại công nghiệp
- Quy mô tổ chức
- Mối quan hệ với các quy định hiện hành của chính phủ
- Vị trí địa lý của một doanh nghiệp
- Một quyết định kinh doanh để tuân thủ một quy định cụ thể

Để xem xét các quy định tuân thủ chung mà các tổ chức khác nhau cần tuân thủ, hãy tham khảođọc về các biện pháp kiểm soát, khuôn khổ và sự tuân thủ.

The role of frameworks and controls in audits

Vai trò của khuôn khổ và biện pháp kiểm soát trong kiểm toán

Along with compliance, it's important to mention the role of frameworks and controls in security audits. Frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the international standard for information security (ISO 27000) series are designed to help organizations prepare for regulatory compliance security audits. By adhering to these and other relevant frameworks, organizations can save time when conducting external and internal audits. Additionally, frameworks, when used alongside controls, can support organizations' ability to align with regulatory compliance requirements and standards.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Cùng với việc tuân thủ, điều quan trọng là phải đề cập đến vai trò của các khuôn khổ và biện pháp kiểm soát trong kiểm tra bảo mật. Các khuôn khổ như Khung An ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST CSF) và loạt tiêu chuẩn quốc tế về bảo mật thông tin (ISO 27000) được thiết kế để giúp các tổ chức chuẩn bị cho hoạt động kiểm tra bảo mật tuân thủ quy định. Bằng cách tuân thủ các khuôn khổ này và các khuôn khổ liên quan khác, tổ chức có thể tiết kiệm thời gian khi tiến hành đánh giá bên ngoài và nội bộ. Ngoài ra, các khuôn khổ, khi được sử dụng cùng với các biện pháp kiểm soát, có thể hỗ trợ khả năng của tổ chức trong việc điều chỉnh các yêu cầu và tiêu chuẩn tuân thủ quy định.

There are three main categories of controls to review during an audit, which are administrative and/or managerial, technical, and physical controls. To learn more about specific controls related to each category, click the following link and select "Use Template."

Link to template: Control categories

Có ba loại biện pháp kiểm soát chính cần xem xét trong quá trình kiểm toán, đó là các biện pháp kiểm soát hành chính và/hoặc quản lý, kỹ thuật và vật lý. Để tìm hiểu thêm về các điều khiển cụ thể liên quan đến từng danh mục, hãy nhấp vào liên kết sau và chọn "Sử dụng mẫu".

Liên kết đến mẫu:Danh mục kiểm soát

Audit checklist

Danh sách kiểm tra kiểm tra

It's necessary to create an audit checklist before conducting an audit. A checklist is generally made up of the following areas of focus:

Cần phải tạo danh sách kiểm tra kiểm toán trước khi tiến hành kiểm toán. Danh sách kiểm tra thường bao gồm các lĩnh vực trọng tâm sau:

Identify the scope of the audit

- The audit should:

- List assets that will be assessed (e.g., firewalls are configured correctly, PII is secure, physical assets are locked, etc.)
- Note how the audit will help the organization achieve its desired goals
- Indicate how often an audit should be performed
- Include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees

Xác định phạm vi kiểm toán

- Cuộc kiểm toán nên:
  - Liệt kê các tài sản sẽ được đánh giá (ví dụ: tường lửa được cấu hình đúng, PII được bảo mật, tài sản vật chất bị khóa, v.v.)
  - Lưu ý cách kiểm toán sẽ giúp tổ chức đạt được mục tiêu mong muốn
  - Cho biết tần suất thực hiện kiểm toán
  - Bao gồm việc đánh giá các chính sách, giao thức và thủ tục của tổ chức để đảm bảo chúng hoạt động như dự định và được nhân viên thực hiện

Complete a risk assessment

- A risk assessment is used to evaluate identified organizational risks related to budget, controls, internal processes, and external standards (i.e., regulations).

Hoàn thành đánh giá rủi ro

- Đánh giá rủi ro được sử dụng để đánh giá các rủi ro đã được xác định của tổ chức liên quan đến ngân sách, kiểm soát, quy trình nội bộ và các tiêu chuẩn bên ngoài (tức là các quy định).

Conduct the audit

- When conducting an internal audit, you will assess the security of the identified assets listed in the audit scope.

Tiến hành kiểm toán

- Khi tiến hành kiểm toán nội bộ, bạn sẽ đánh giá tính bảo mật của các tài sản được xác định được liệt kê trong phạm vi kiểm toán.

Create a mitigation plan

- A mitigation plan is a strategy established to lower the level of risk and potential costs, penalties, or other issues that can negatively affect the organization’s security posture.

Tạo một kế hoạch giảm nhẹ

- Kế hoạch giảm thiểu là một chiến lược được thiết lập để giảm mức độ rủi ro và chi phí tiềm ẩn, hình phạt hoặc các vấn đề khác có thể ảnh hưởng tiêu cực đến tình hình bảo mật của tổ chức.

Communicate results to stakeholders

- The end result of this process is providing a detailed report of findings, suggested improvements needed to lower the organization's level of risk, and compliance regulations and standards the organization needs to adhere to.

Truyền đạt kết quả cho các bên liên quan

- Kết quả cuối cùng của quá trình này là cung cấp một báo cáo chi tiết về các phát hiện, những cải tiến được đề xuất cần thiết để giảm mức độ rủi ro của tổ chức cũng như các quy định và tiêu chuẩn tuân thủ mà tổ chức cần tuân thủ.

Key takeaways

Bài học chính

In this reading you learned more about security audits, including what they are; why they’re conducted; and the role of frameworks, controls, and compliance in audits.

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

Trong bài đọc này, bạn đã tìm hiểu thêm về kiểm tra bảo mật, bao gồm cả nội dung của chúng; tại sao chúng được tiến hành; và vai trò của các khuôn khổ, biện pháp kiểm soát và tính tuân thủ trong kiểm toán.

Although there is much more to learn about security audits, this introduction is meant to support your ability to complete an audit of your own for a self-reflection portfolio activity later in this course.

Mặc dù còn nhiều điều cần tìm hiểu về kiểm tra bảo mật, nhưng phần giới thiệu này nhằm hỗ trợ khả năng của bạn để hoàn thành việc kiểm tra của riêng bạn cho hoạt động danh mục tự phản ánh sau này trong khóa học này.

Resources for more information

Tài nguyên để biết thêm thông tin

Resources that you can explore to further develop your understanding of audits in the cybersecurity space are:

- Assessment and Auditing Resources
- IT Disaster Recovery Plan

Các tài nguyên mà bạn có thể khám phá để phát triển hơn nữa hiểu biết của mình về hoạt động kiểm tra trong lĩnh vực an ninh mạng là:

- Nguồn lực đánh giá và kiểm toán
- Kế hoạch khắc phục thảm họa CNTT

4.7. Test your knowledge: OWASP principles and security audits – Kiểm tra kiến thức của bạn: Nguyên tắc OWASP và kiểm tra bảo mật

4.8. Portfolio Activity: Conduct a security audit – Hoạt động danh mục đầu tư: Tiến hành kiểm tra bảo mật

4.9. Portfolio Activity Exemplar: Conduct a security audit – Ví dụ về hoạt động danh mục đầu tư: Tiến hành kiểm tra bảo mật

Module 2: Security framework and controls
Phần 2: Khung bảo mật và kiểm soát

5. Review: Security frameworks and controls – Đánh giá: Khung bảo mật và biện pháp kiểm soát

5.1. Wrap-up – Gói lại

Great job! Now you've had an opportunity to learn more about security concepts that can help an organization protect data and assets. We've covered quite a bit, but it will all be valuable knowledge for you as you continue along your journey into the security profession.

Bạn đã làm rất tốt! Bây giờ bạn đã cómột cơ hội để tìm hiểu thêm vềkhái niệm bảo mật có thể giúpmột tổ chức bảo vệ dữ liệu và tài sản.Chúng tôi đã đề cập khá nhiều,nhưng tất cả sẽ là những kiến thức quý giá cho bạn khi bạntiếp tục cuộc hành trình của bạn vào nghề an ninh.

We started by defining what security frameworks are, and how they help organizations protect critical information. We also explored security controls and the important role they play in protecting against risks, threats, and vulnerabilities. This included a discussion of the CIA triad, which is a core security model, and two NIST frameworks: the CSF and S.P. 800-53. Then, we covered some of OWASP's secure design principles.

Chúng tôi bắt đầu bằng việc xác định khung bảo mật là gì,và cách chúng giúp đỡ các tổ chứcbảo vệ thông tin quan trọng.Chúng tôi cũng đã khám phá các biện pháp kiểm soát bảo mậtvà vai trò quan trọng của chúngchơi để bảo vệ chống lạirủi ro, mối đe dọa và điểm yếu.Điều này bao gồm một cuộc thảo luận về bộ ba CIA,đây là mô hình bảo mật cốt lõi và hai khung NIST:CSF và SP 800-53.Sau đó, chúng tôi đề cập đến một số nguyên tắc thiết kế an toàn của OWASP.

We ended by introducing security audits with a focus on the elements of an internal audit that you may be asked to complete or contribute to.

Chúng tôi đã kết thúc bằng việc giới thiệu các biện pháp kiểm tra bảo mật tập trung vàocác yếu tố của kiểm toán nội bộ mà bạncó thể được yêu cầu hoàn thành hoặc đóng góp.

Security professionals use the concepts we discussed to help protect organizations' assets, data, systems, and people. As you continue along your journey into the security profession, a lot of these concepts will come up repeatedly. What we're doing

now is giving you a foundational understanding of security practices and topics that will help you along the way.

Các chuyên gia bảo mật sử dụng các khái niệm chúng ta đã thảo luậnđể giúp bảo vệ tài sản của tổ chức,dữ liệu, hệ thống và con người.Khi bạn tiếp tụchành trình của bạn vào nghề an ninh,rất nhiều khái niệm trong số này sẽ xuất hiện nhiều lần.Những gì chúng tôi đang làm bây giờ là mang lại cho bạnmột sự hiểu biết cơ bản vềcác chủ đề và thực hành bảo mậtđiều đó sẽ giúp bạn trên đường đi.

In the next section of the course, we'll discuss specific security tools you may one day use as an analyst. We'll cover how they're used to improve an organization's security posture and how they can help you achieve your goal of keeping organizations and people safe. I'm excited to continue this journey with you. See you soon!

Trong phần tiếp theo của khóa học,chúng ta sẽ thảo luận về các công cụ bảo mật cụ thểmột ngày nào đó bạn có thể sử dụng nó như một nhà phân tích.Chúng tôi sẽ đề cập đến cách chúng được sử dụng để cải thiệntình hình an ninh của một tổ chứcvà cách họ có thể giúp bạn đạt được mục tiêuđảm bảo an toàn cho tổ chức và con người.Tôi rất hào hứng để tiếp tụccuộc hành trình này với bạn. Hẹn sớm gặp lại!

5.2. 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 2, Module 2

Các thuật ngữ và định nghĩa trong Khóa 2, Học phần 2

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

Attack vectors: The pathways attackers use to penetrate security defenses

Các vectơ tấn công: Con đường mà kẻ tấn công sử dụng để xâm nhập vào hệ thống phòng thủ an ninh

Authentication: The process of verifying who someone is

Xác thực: Quá trình xác minh ai đó là ai

Authorization: The concept of granting access to specific resources in a system

Ủy quyền: Khái niệm cấp quyền truy cập vào các tài nguyên cụ thể trong hệ thống

Availability: The idea that data is accessible to those who are authorized to access it

Tính sẵn có: Ý tưởng rằng dữ liệu có thể truy cập được đối với những người được phép truy cập nó

Biometrics: The unique physical characteristics that can be used to verify a person's identity

Sinh trắc học: Các đặc điểm vật lý duy nhất có thể được sử dụng để xác minh danh tính của một người

Confidentiality: The idea that only authorized users can access specific assets or data

Tính bảo mật: Ý tưởng rằng chỉ những người dùng được ủy quyền mới có thể truy cập các tài sản hoặc dữ liệu cụ thể

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Bộ ba bí mật, toàn vẹn, sẵn có (CIA): Một mô hình giúp thông báo cách các tổ chức xem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật

Detect: A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

Phát hiện: Chức năng cốt lõi của NIST liên quan đến việc xác định các sự cố bảo mật tiềm ẩn và cải thiện khả năng giám sát để tăng tốc độ và hiệu quả phát hiện

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

Identify: A NIST core function related to management of cybersecurity risk and its effect on an organization’s people and assets

Xác định : Chức năng cốt lõi của NIST liên quan đến quản lý rủi ro an ninh mạng và ảnh hưởng của nó đối với con người và tài sản của tổ chức

Integrity: The idea that the data is correct, authentic, and reliable

Tính toàn vẹn: Ý tưởng rằng dữ liệu là chính xác, xác thực và đáng tin cậy

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

National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) Ấn bản Đặc biệt (SP) 800-53: Khuôn khổ thống nhất để bảo vệ an ninh hệ thống thông tin trong chính phủ liên bang Hoa Kỳ

Open Web Application Security Project/Open Worldwide Application Security Project (OWASP): A non-profit organization focused on improving software security

Dự án bảo mật ứng dụng web mở/Dự án bảo mật ứng dụng toàn cầu mở (OWASP): Một tổ chức phi lợi nhuận tập trung vào việc cải thiện bảo mật phần mềm

Protect: A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

Bảo vệ: Chức năng cốt lõi của NIST được sử dụng để bảo vệ tổ chức thông qua việc triển khai các chính sách, quy trình, đào tạo và công cụ giúp giảm thiểu các mối đe dọa an ninh mạng

Recover: A NIST core function related to returning affected systems back to normal operation

Khôi phục: Chức năng cốt lõi của NIST liên quan đến việc đưa các hệ thống bị ảnh hưởng trở lại hoạt động bình thường

Respond: A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

Phản hồi: Chức năng cốt lõi của NIST liên quan đến việc đảm bảo rằng các quy trình thích hợp được sử dụng để ngăn chặn, vô hiệu hóa và phân tích các sự cố bảo mật cũng như thực hiện các cải tiến đối với quy trình bảo mật

Risk: Anything that can impact the 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

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

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Khung bảo mật: Nguyên tắc dùng để xây dựng kế hoạch giúp giảm thiểu rủi ro và các mối đe dọa đối với dữ liệu và quyền riêng tư

Security posture: An organization’s ability to manage its defense of critical assets and data and react to change

Tình trạng bảo mật: Khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi

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

5.3. Module 2 challenge – Thử thách mô-đun 2

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Module 3: Introduction to cybersecurity tools – Giới thiệu các công cụ an ninh mạng

You will explore industry leading security information and event management (SIEM) tools that are used by security professionals to protect business operations. You'll learn how entry-level security analysts use SIEM dashboards as part of their every day work.

Bạn sẽ khám phá các công cụ quản lý sự kiện và thông tin bảo mật (SIEM) hàng đầu trong ngành được các chuyên gia bảo mật sử dụng để bảo vệ hoạt động kinh doanh. Bạn sẽ tìm hiểu cách các nhà phân tích bảo mật cấp đầu vào sử dụng bảng thông tin SIEM như một phần công việc hàng ngày của họ.

Learning Objectives

- Identify and define commonly used Security Information and Event Management (SIEM) tools.
- Describe how SIEM tools are used to protect business operations.
- Explain how entry-level security analysts use SIEM dashboards.

Mục tiêu học tập

- Xác định và xác định các công cụ Quản lý sự kiện và thông tin bảo mật (SIEM) thường được sử dụng.
- Mô tả cách sử dụng các công cụ SIEM để bảo vệ hoạt động kinh doanh.
- Giải thích cách các nhà phân tích bảo mật cấp đầu vào sử dụng bảng thông tin SIEM.

1. Security information and event management (SIEM) dashboards – Bảng thông tin quản lý sự kiện và thông tin bảo mật (SIEM)

1.1. Welcome to module 3 – Chào mừng đến với mô-đun 3

Welcome back! Previously, we discussed security frameworks, controls, and design principles, and how security professionals apply these to security audits.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Chào mừng trở lại!Trước đây, chúng ta đã thảo luận về các khung bảo mật, biện pháp kiểm soát và thiết kếnguyên tắc và cách các chuyên gia bảo mật áp dụng những nguyên tắc này vào kiểm tra bảo mật.

In this section, we'll continue to explore security tools and how they can help you keep organizations and the people they serve safe. Security professionals often use a variety of tools to address specific security challenges, such as collecting security data, detecting and analyzing threats, or automating tasks. Security tools help organizations achieve a more comprehensive security posture.

Trong phần này, chúng ta sẽ tiếp tục khám phá các công cụ bảo mật vàcách họ có thể giúp bạn giữ an toàn cho các tổ chức và những người mà họ phục vụ.Các chuyên gia bảo mật thường sử dụng nhiều công cụ khác nhau để giải quyếtnhững thách thức bảo mật cụ thể, chẳng hạn như thu thập dữ liệu bảo mật,phát hiện và phân tích các mối đe dọa hoặc tự động hóa các nhiệm vụ.Các công cụ bảo mật giúp các tổ chức đạt được trạng thái bảo mật toàn diện hơn.

We'll begin by covering different types of logs, what they track, and how they're used.

Chúng ta sẽ bắt đầu bằng cách đề cập đến các loại nhật ký khác nhau,những gì họ theo dõi và cách chúng được sử dụng.

Then we'll explore security information and event management, otherwise known as SIEM, dashboards. Finally, we'll discuss some common SIEM tools used in the security industry. Let's get started!

Sau đó chúng ta sẽ khám phá thông tin bảo mật và quản lý sự kiện,còn được gọi là SIEM, bảng điều khiển.Cuối cùng, chúng ta sẽ thảo luận về một số công cụ SIEM phổ biến được sử dụng trong ngành bảo mật.Bắt đầu nào!

1.2. Logs and SIEM tools – Logs và công cụ SIEM

As a security analyst, one of your responsibilities might include analyzing log data to mitigate and manage threats, risks, and vulnerabilities. As a reminder, a log is a record of events that occur within an organization's systems and networks. Security

analysts access a variety of logs from different sources. Three common log sources include firewall logs, network logs, and server logs. Let's explore each of these log sources in more detail.

Là một nhà phân tích chứng khoán,một trong những trách nhiệm của bạn có thể bao gồm việc phân tíchghi dữ liệu để giảm thiểu và quản lýmối đe dọa, rủi ro và điểm yếu.Xin nhắc lại, nhật ký là bản ghi lại các sự kiệnxảy ra trong hệ thống và mạng lưới của một tổ chức.Các nhà phân tích bảo mật truy cập vào nhiều loạinhật ký từ các nguồn khác nhau.Ba nguồn nhật ký phổ biến bao gồm nhật ký tường lửa,nhật ký mạng và nhật ký máy chủ.Hãy cùng khám phá từng nguồn nhật ký này một cách chi tiết hơn.

A firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

Nhật ký tường lửa là bản ghi các nỗ lực hoặckết nối được thiết lập cholưu lượng truy cập đến từ internet.Nó cũng bao gồm các yêu cầu gửi đivào internet từ bên trong mạng.

A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

Nhật ký mạng là bản ghi củatất cả các máy tính và thiết bịvào và ra khỏi mạng.Nó cũng ghi lại các kết nối giữacác thiết bị và dịch vụ trên mạng.

Finally, a server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

Cuối cùng, nhật ký máy chủ là bản ghi củacác sự kiện liên quan đến các dịch vụ như trang web,email hoặc chia sẻ tập tin.Nó bao gồm các hành động như đăng nhập,yêu cầu mật khẩu và tên người dùng.

By monitoring logs, like the one shown here, security teams can identify vulnerabilities and potential data breaches. Understanding logs is important because SIEM tools rely on logs to monitor systems and detect security threats.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Bằng cách theo dõi nhật ký, giống như nhật ký hiển thị ở đây,đội an ninh có thể xác địnhcác lỗ hổng và nguy cơ vi phạm dữ liệu.Hiểu nhật ký là quan trọngvì các công cụ SIEM dựa vàonhật ký để giám sát hệ thống và phát hiện các mối đe dọa bảo mật.

A security information and event management, or SIEM, tool is an application that collects and analyzes log data to monitor critical activities in an organization. It provides real-time visibility, event monitoring and analysis, and automated alerts. It also stores all log data in a centralized location.

Một công cụ quản lý sự kiện và thông tin bảo mật hoặc SIEMlà một ứng dụngthu thập và phân tích dữ liệu nhật ký đểgiám sát các hoạt động quan trọng trong một tổ chức.Nó cung cấp khả năng hiển thị theo thời gian thực,giám sát và phân tích sự kiện cũng như cảnh báo tự động.Nó cũng lưu trữ tất cả dữ liệu nhật ký ở một vị trí tập trung.

Because SIEM tools index and minimize the number of logs a security professional must manually review and analyze, they increase efficiency and save time.

Bởi vì các công cụ SIEM lập chỉ mục và giảm thiểu số lượng nhật kýmột chuyên gia bảo mật phảixem xét và phân tích thủ công,chúng làm tăng hiệu quả và tiết kiệm thời gian.

But, SIEM tools must be configured and customized to meet each organization's unique security needs. As new threats and vulnerabilities emerge, organizations must continually customize their SIEM tools to ensure that threats are detected and quickly addressed.

Tuy nhiên, các công cụ SIEM phải được cấu hình và tùy chỉnh đểđáp ứng nhu cầu bảo mật riêng biệt của mỗi tổ chức.Khi các mối đe dọa và lỗ hổng mới xuất hiện,các tổ chức phải liên tục tùy chỉnhcông cụ SIEM của họ để đảm bảo rằngcác mối đe dọa được phát hiện và giải quyết nhanh chóng.

Later in the certificate program, you'll have a chance to practice using different SIEM tools to identify potential security incidents.

Sau đó trong chương trình chứng chỉ,bạn sẽ có cơ hội thực hành sử dụngcác công cụ SIEM khác nhau đểxác định các sự cố an ninh tiềm ẩn.

Coming up, we'll explore SIEM dashboards and how cybersecurity professionals use them to monitor for threats, risks, and vulnerabilities.

Sắp tới chúng ta sẽ khám pháBảng điều khiển SIEM và cách thức bảo mật mạngcác chuyên gia sử dụng chúng để theo dõimối đe dọa, rủi ro và điểm yếu.

1.3. SIEM dashboards – Bảng điều khiển SIEM

We've explored how SIEM tools are used to collect and analyze log data. However, this is just one of the many ways SIEM tools are used in cybersecurity.

Chúng tôi đã khám phá cách sử dụng các công cụ SIEMđể thu thập và phân tích dữ liệu nhật ký.Tuy nhiên, đây chỉ là một trongnhiều cách sử dụng công cụ SIEM trong an ninh mạng.

SIEM tools can also be used to create dashboards. You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

Các công cụ SIEM cũng có thể được sử dụng để tạo bảng thông tin.Bạn có thể đã gặp phải bảng điều khiểntrong một ứng dụng trên điện thoại hoặc thiết bị khác của bạn.Họ trình bày thông tin về tài khoản của bạn hoặcvị trí ở định dạng dễ hiểu.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

Ví dụ,ứng dụng thời tiết hiển thị dữ liệu như nhiệt độ,sự kết tủa,tốc độ gió và dự báo bằng biểu đồ,đồ thị và các yếu tố trực quan khác.Định dạng này giúp bạn dễ dàng nhanh chóngxác định các kiểu và xu hướng thời tiết,để bạn có thể chuẩn bị và lên kế hoạch cho ngày của mình cho phù hợp.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

Giống như các ứng dụng thời tiết giúp mọi người thực hiệnquyết định nhanh chóng và sáng suốt dựa trên dữ liệu,Bảng điều khiển SIEM giúp các nhà phân tích bảo mậttruy cập nhanh chóng và dễ dàngthông tin bảo mật của tổ chức của họ nhưbiểu đồ, đồ thị hoặc bảng.

For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

Ví dụ, một nhà phân tích chứng khoánnhận được cảnh báo về một nỗ lực đăng nhập đáng ngờ.Nhà phân tích truy cập bảng điều khiển SIEM của họđể thu thập thông tin về cảnh báo này.Sử dụng bảng điều khiển,nhà phân tích phát hiện ra rằng đã có500 lần đăng nhập của Ymaratài khoản trong khoảng thời gian năm phút.Họ cũng phát hiện ra rằng những nỗ lực đăng nhập đã xảy ra từvị trí địa lý bên ngoài Ymara'sđịa điểm thông thường và ngoài giờ làm việc thông thường của cô ấy.Bằng cách sử dụng một bảng điều khiển,nhà phân tích bảo mật đã có thể nhanh chóng xem xétbiểu diễn trực quan của dòng thời giancủa những lần thử đăng nhập,địa điểm và thời gian chính xác của hoạt động,sau đó xác định rằng hoạt động đó là đáng ngờ.

In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

Ngoài việc cung cấpmột bản tóm tắt toàn diện về dữ liệu liên quan đến bảo mật,Bảng điều khiển SIEM cũng cung cấpcác bên liên quan với các số liệu khác nhau.Số liệu là thuộc tính kỹ thuật quan trọngchẳng hạn như thời gian phản hồi,tính sẵn có và tỷ lệ thất bại,được sử dụng để đánh giáhiệu suất của một ứng dụng phần mềm.

SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

Bảng điều khiển SIEM có thểđược tùy chỉnh để hiển thị số liệu cụ thểhoặc dữ liệu khác có liên quancho các thành viên khác nhau trong một tổ chức.Ví dụ: nhà phân tích bảo mật có thể tạo bảng điều khiểnhiển thị số liệu chogiám sát hoạt động kinh doanh hàng ngày,như khối lượng lưu lượng mạng đến và đi.

We've examined how security analysts use SIEM dashboards to help organizations maintain their security posture. Well done!

Chúng tôi đã kiểm tra cách các nhà phân tích bảo mật sử dụngBảng điều khiển SIEM để trợ giúpcác tổ chức duy trì tình trạng an ninh của họ.Làm tốt!

Coming up, we'll discuss some common SIEM tools used in the cybersecurity industry. Meet you there.

Sắp tới, chúng ta sẽ thảo luận về một số công cụ SIEM phổ biếnđược sử dụng trong ngành an ninh mạng. Gặp bạn ở đó.

1.4. The future of SIEM tools – Tương lai của các công cụ SIEM

The future of SIEM tools

Tương lai của các công cụ SIEM

Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Trước đây, bạn đã được giới thiệu về các công cụ quản lý sự kiện và thông tin bảo mật (SIEM), cùng với một số ví dụ về các công cụ SIEM. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cách sử dụng các công cụ SIEM để bảo vệ hoạt động của tổ chức. Bạn cũng sẽ hiểu rõ hơn về cách thức và lý do tại sao các công cụ SIEM đang thay đổi để giúp bảo vệ các tổ chức và những người mà họ phục vụ khỏi các chiến thuật và kỹ thuật ngày càng phát triển của tác nhân đe dọa.

Current SIEM solutions

Các giải pháp SIEM hiện tại

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

Công cụ **SIEM** là một ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng trong một tổ chức. Các công cụ SIEM cung cấp khả năng giám sát và theo dõi nhật ký sự kiện bảo mật theo thời gian thực. Sau đó, dữ liệu được sử dụng để tiến hành phân tích kỹ lưỡng về mọi mối đe dọa, rủi ro hoặc lỗ hổng bảo mật tiềm ẩn được xác định. Công cụ SIEM có nhiều tùy chọn bảng điều khiển. Mỗi tùy chọn bảng điều khiển giúp các thành viên nhóm an ninh mạng quản lý và giám sát dữ liệu của tổ chức. Tuy nhiên, hiện tại, các công cụ SIEM yêu cầu sự tương tác của con người để phân tích các sự kiện bảo mật.

The future of SIEM tools

Tương lai của các công cụ SIEM

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for

organizations that don’t want to invest in creating and maintaining their own infrastructure.

Khi an ninh mạng tiếp tục phát triển, nhu cầu về chức năng đám mây cũng tăng lên. Các công cụ SIEM đã và đang tiếp tục phát triển để hoạt động trong môi trường được lưu trữ trên nền tảng đám mây và trên nền tảng đám mây. Các công cụ SIEM được lưu trữ trên nền tảng đám mây được vận hành bởi các nhà cung cấp chịu trách nhiệm duy trì và quản lý cơ sở hạ tầng cần thiết để sử dụng các công cụ này. Các công cụ được lưu trữ trên đám mây có thể truy cập đơn giản thông qua internet và là giải pháp lý tưởng cho các tổ chức không muốn đầu tư vào việc tạo và duy trì cơ sở hạ tầng của riêng họ.

Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

Tương tự như các công cụ SIEM được lưu trữ trên đám mây, các công cụ SIEM gốc trên nền tảng đám mây cũng được các nhà cung cấp duy trì và quản lý hoàn toàn cũng như được truy cập qua internet. Tuy nhiên, các công cụ dựa trên nền tảng đám mây được thiết kế để tận dụng tối đa khả năng của điện toán đám mây, chẳng hạn như tính khả dụng, tính linh hoạt và khả năng mở rộng.

Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage functionality.

Tuy nhiên, sự phát triển của các công cụ SIEM dự kiến sẽ tiếp tục để phù hợp với bản chất đang thay đổi của công nghệ cũng như các chiến thuật và kỹ thuật mới của tác nhân đe dọa. Ví dụ: hãy xem xét sự phát triển hiện tại của các thiết bị được kết nối với nhau có quyền truy cập vào Internet, được gọi là Internet of Things (IoT). Càng có nhiều thiết bị được kết nối với nhau thì bề mặt tấn công an ninh mạng càng lớn và lượng dữ liệu mà các tác nhân đe dọa có thể khai thác càng lớn. Sự đa dạng của các cuộc tấn công và dữ liệu cần được chú ý đặc biệt dự kiến sẽ tăng lên đáng kể. Ngoài ra, khi công nghệ trí tuệ nhân tạo (AI) và máy học (ML) tiếp tục phát triển, các khả năng của SIEM sẽ được

nâng cao để xác định tốt hơn các thuật ngữ liên quan đến mối đe dọa, trực quan hóa bảng điều khiển và chức năng lưu trữ dữ liệu.

The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response. **Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can't be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

Việc triển khai tự động hóa cũng sẽ giúp đội ngũ bảo mật ứng phó nhanh hơn với các sự cố có thể xảy ra, thực hiện nhiều hành động mà không cần chờ phản hồi của con người. **Điều phối, tự động hóa và phản hồi bảo mật (SOAR)** là tập hợp các ứng dụng, công cụ và quy trình làm việc sử dụng tự động hóa để phản hồi các sự kiện bảo mật. Về cơ bản, điều này có nghĩa là việc xử lý các sự cố thường gặp liên quan đến bảo mật bằng cách sử dụng các công cụ SIEM dự kiến sẽ trở thành một quy trình hợp lý hơn, đòi hỏi ít sự can thiệp thủ công hơn. Điều này giúp các nhà phân tích bảo mật rảnh tay để xử lý các sự cố phức tạp và hiếm gặp hơn, do đó, không thể tự động hóa bằng SOAR. Tuy nhiên, kỳ vọng là các nền tảng liên quan đến an ninh mạng sẽ giao tiếp và tương tác với nhau. Mặc dù công nghệ cho phép các hệ thống và thiết bị được kết nối với nhau giao tiếp với nhau đã tồn tại nhưng nó vẫn đang trong quá trình hoàn thiện.

Key takeaways

Bài học chính

SIEM tools play a major role in monitoring an organization's data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Các công cụ SIEM đóng vai trò chính trong việc giám sát dữ liệu của tổ chức. Với tư cách là nhà phân tích bảo mật cấp đầu vào, bạn có thể giám sát bảng thông tin SIEM như một phần công việc hàng ngày của mình. Thường xuyên nghiên cứu những phát triển mới trong công nghệ SIEM sẽ giúp bạn phát triển và thích ứng với những thay đổi trong lĩnh vực an ninh mạng. Điện toán đám mây, tích hợp ứng dụng SIEM và tự động hóa chỉ là một số tiến bộ mà các chuyên gia bảo mật có thể mong đợi trong quá trình phát triển các công cụ SIEM trong tương lai.

1.5. Parisa: The parallels of accessibility and security – Parisa: Sự tương đồng giữa khả năng tiếp cận và bảo mật

My name is Parisa and I'm a vice president of engineering and lead the Chrome Team. So as General manager of the Chrome Team, I lead a team of engineers and product managers and designers around the world who actually build Chrome and keep all of our users safe. I think accessibility is important to all aspects of technology, and when we think about its relevance for cybersecurity, you know, we ultimately want to keep everybody safe. I think of accessibility as making information, activities, or even environments meaningful, sensible, usable to as many people as possible. And when we're talking about this in a technology standpoint, it's usually about making information or services available to people with disabilities. Decisions we make based on our own abilities to enhance security can actually be ineffective. For example, you'll sometimes see the color red used for indication of a warning. Well, for somebody who's colorblind, like that is going to be ineffective. And so really thinking about accessibility when we're trying to keep people safe is super important for them to be effective. I've worked in the space of security for a really long time. And I do see some parallels between the spaces. I've really been able to see innovation driven when you're trying to solve a very specific security problem or a specific accessibility problem. Closed Captioning was originally designed and built to help people with hearing impairments, but it ends up helping everybody. For people who are new to the field of cybersecurity, it's just really important to remember that there's a range of abilities that you are wanting to serve. It's so important to get user research and feedback and a range of abilities in terms of testing the effectiveness of your security mitigations. I know it was scary for me early on. I didn't look like everybody else. I really struggled with whether I belonged. Finding people who could be mentors, having the courage to ask questions and recognize that you're rarely the only person with that question. And just sort of persevering through, sometimes hard moments can lead to breakthroughs and also just growing confidence. And one of the things I've learned is me having a different background than other people in this space was my own superpower. Instead of focusing on the delta between what I was and what the norm was in the room, I should feel a lot of pride in what made me unique and what unique skills and perspective I brought to the table.

Tên tôi là Parisa và tôi là phó chủ tịch kỹ thuật và lãnh đạo Nhóm Chrome.Vì vậy, với tư cách là Tổng giám đốc của Nhóm Chrome, tôi lãnh đạo một nhóm kỹ sư vàcác nhà quản lý sản phẩm và nhà thiết kế trên toàn thế giới, những người thực sựxây dựng Chrome và giữ an toàn cho tất cả người dùng của chúng tôi.Tôi nghĩ khả năng tiếp cận

là quan trọng đối với tất cả các khía cạnh của công nghệ vàkhi chúng tôi nghĩ về sự liên quan của nó đối vớian ninh mạng, bạn biết đấy, cuối cùng chúng tôi muốn giữ an toàn cho mọi người.Tôi nghĩ khả năng tiếp cận có nghĩa là tạo ra thông tin, hoạt động hoặcngay cả những môi trường có ý nghĩa, hợp lý, có thể sử dụng được cho càng nhiều người càng tốt.Và khi chúng ta nói về vấn đề này dưới góc độ công nghệ, thường làvề việc cung cấp thông tin hoặc dịch vụ cho người khuyết tật.Những quyết định chúng ta đưa ra dựa trên khả năng của chính mình để tăng cường bảo mật có thểthực tế là không hiệu quả.Ví dụ: đôi khi bạn sẽ thấy màu đỏ được sử dụng chodấu hiệu của một cảnh báo.Chà, đối với người mù màu, cách đó sẽ không hiệu quả.Và vì vậy, việc thực sự nghĩ đến khả năng tiếp cận khi chúng tôi cố gắng giữ an toàn cho mọi người làcực kỳ quan trọng để chúng có hiệu quả.Tôi đã làm việc trong lĩnh vực an ninh trong một thời gian dài.Và tôi thấy một số điểm tương đồng giữa các không gian.Tôi thực sự có thể thấy sự đổi mới được thúc đẩy khi bạn cố gắng giải quyếtmột vấn đề bảo mật rất cụ thể hoặc một vấn đề về khả năng truy cập cụ thể.Phụ đề chi tiết ban đầu được thiết kế và xây dựng để giúp mọi ngườivới người khiếm thính, nhưng cuối cùng nó lại giúp ích được cho mọi người.Đối với những người mới làm quen với lĩnh vực an ninh mạng, điều này thực sự quan trọnghãy nhớ rằng có nhiều khả năng mà bạn muốn phục vụ.Điều quan trọng là nhận được nghiên cứu và phản hồi của người dùng cũng như một loạt các khả năngvề mặt kiểm tra tính hiệu quả của các biện pháp giảm thiểu bảo mật của bạn.Tôi biết điều đó thật đáng sợ đối với tôi từ rất sớm.Tôi trông không giống những người khác.Tôi thực sự đấu tranh với việc liệu tôi có thuộc về hay không.Tìm những người có thể làm cố vấn, có can đảm đặt câu hỏi vànhận ra rằng bạn hiếm khi là người duy nhất có câu hỏi đó.Và chỉ cần kiên trì vượt qua, đôi khi những khoảnh khắc khó khăn có thểdẫn đến những đột phá và cũng chỉ làm tăng thêm sự tự tin.Và một trong những điều tôi học được là tôi có một quan điểm khácnền tảng hơn những người khác trong không gian này là siêu năng lực của riêng tôi.Thay vì tập trung vào sự khác biệt giữa bản chất của tôi và chuẩn mựccăn phòng, tôi sẽ cảm thấy rất tự hào về điều khiến tôi trở nên độc đáo vànhững kỹ năng và quan điểm độc đáo mà tôi đã mang đến.

1.6. Test your knowledge: Security information and event management (SIEM) dashboards – Kiểm tra kiến thức của bạn: Bảng thông tin quản lý sự kiện và thông tin bảo mật (SIEM)

2. Explore security information and event management (SIEM) tools – Khám phá các công cụ quản lý sự kiện và thông tin bảo mật (SIEM)

2.1. Explore common SIEM tools – Khám phá các công cụ SIEM phổ biến

Hello again! Previously, we discussed how SIEM tools help security analysts monitor systems and detect security threats.

Xin chào lần nữa!Trước đây, chúng ta đã thảo luận về cách các công cụ SIEM giúp các nhà phân tích bảo mật giám sát hệ thống vàphát hiện các mối đe dọa an ninh.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

In this video, we'll cover some industry leading SIEM tools that you'll likely encounter as a security analyst. First, let's discuss the different types of SIEM tools that organizations can choose from, based on their unique security needs.

Trong video này, chúng tôi sẽ đề cập đến một số công cụ SIEM hàng đầu trong ngành mà bạn sẽcó thể gặp phải với tư cách là một nhà phân tích bảo mật.Trước tiên, hãy thảo luận về các loại công cụ SIEM khác nhaucác tổ chức có thể lựa chọn, dựa trên nhu cầu bảo mật riêng của họ.

Self-hosted SIEM tools require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity. These applications are then managed and maintained by the organization's IT department, rather than a third party vendor. Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data.

Các công cụ SIEM tự lưu trữ yêu cầu các tổ chức phải cài đặt, vận hành vàduy trì công cụ bằng cơ sở hạ tầng vật lý của riêng họ, chẳng hạn như dung lượng máy chủ.Các ứng dụng này sau đó được quản lý và duy trì bởibộ phận CNTT của tổ chức chứ không phải là nhà cung cấp bên thứ ba.Các công cụ SIEM tự lưu trữ rất lý tưởng khi một tổ chứccần thiết để duy trì sự kiểm soát vật lý đối với dữ liệu bí mật.

Alternatively, cloud-hosted SIEM tools are maintained and managed by the SIEM providers, making them accessible through the internet. Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure.

Ngoài ra, các công cụ SIEM được lưu trữ trên đám mây được duy trì vàđược quản lý bởi các nhà cung cấp SIEM, giúp họ có thể truy cập được thông qua internet.Các công cụ SIEM được lưu trữ trên đám mây rất lý tưởng cho các tổ chức không muốnđầu tư vào việc tạo ra và duy trì cơ sở hạ tầng của riêng họ.

Or, an organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools, known as a hybrid solution. Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.

Hoặc, một tổ chức có thể chọn sử dụng kết hợp cả máy chủ tự lưu trữ vàCác công cụ SIEM được lưu trữ trên đám mây, được gọi là giải pháp kết hợp.Các tổ chức có thể chọn giải pháp SIEM lai để tận dụng lợi ích củađám mây đồng thời duy trì quyền kiểm soát vật lý đối với dữ liệu bí mật.

Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems. Let's begin by discussing Splunk.

Splunk Enterprise, Splunk Cloud và Chronicle là phổ biếnCác công cụ SIEM được nhiều tổ chức sử dụng để giúp bảo vệ dữ liệu và hệ thống của họ.Hãy bắt đầu bằng việc thảo luận về Splunk.

Splunk is a data analysis platform and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time. Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data. Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

Splunk là nền tảng phân tích dữ liệu và Splunk Enterprise cung cấp giải pháp SIEM.Splunk Enterprise là một công cụ tự lưu trữ được sử dụng để lưu giữ, phân tích và tìm kiếmdữ liệu nhật ký của tổ chức để cung cấp thông tin bảo mật và cảnh báo theo thời gian thực.Splunk Cloud là một công cụ lưu trữ trên đám mây được sử dụng để thu thập, tìm kiếm và giám sát dữ liệu nhật ký.Splunk Cloud rất hữu ích cho các tổ chức chạy môi trường kết hợp hoặc chỉ có đám mây,nơi một số hoặc tất cả các dịch vụ của tổ chức nằm trên đám mây.

Finally, there's Google's Chronicle. Chronicle is a cloud-native tool designed to retain, analyze, and search data. Chronicle provides log monitoring, data analysis, and data collection. Like cloud-hosted tools, cloud-native tools are also fully maintained and managed by the vendor. But cloud-native tools are specifically designed to take full advantage of cloud computing capabilities such as availability, flexibility, and scalability.

Cuối cùng là Chronicle của Google.Chronicle là một công cụ dựa trên đám mây được thiết kế để lưu giữ, phân tích và tìm kiếm dữ liệu.Chronicle cung cấp tính năng giám sát nhật ký, phân tích dữ liệu và thu thập dữ liệu.Giống như các công cụ được lưu trữ trên đám mây,Các công cụ dựa trên nền tảng đám mây cũng được nhà cung cấp duy trì và

quản lý đầy đủ.Tuy nhiên, các công cụ dựa trên nền tảng đám mây được thiết kế đặc biệt để tận dụng tối đalợi thế của khả năng điện toán đám mây như tính sẵn có,tính linh hoạt và khả năng mở rộng.

Because threat actors are frequently improving their strategies to compromise the confidentiality, integrity, and availability of their targets, it's important for organizations to use a variety of security tools to help defend against attacks. The SIEM tools we just discussed are only a few examples of the tools available for security teams to use to help defend their organizations. And later in the certificate program, you'll have the exciting opportunity to practice using Splunk Cloud and Chronicle.

Bởi vì các tác nhân đe dọa thường xuyên cải tiến chiến lược của họ đểlàm tổn hại đến tính bí mật, tính toàn vẹn vàsự sẵn có của các mục tiêu của họ, điều quan trọng đối vớicác tổ chức sử dụng nhiều công cụ bảo mật khác nhau để giúp chống lại các cuộc tấn công.Các công cụ SIEM mà chúng ta vừa thảo luận chỉ là một vài ví dụ về các công cụ có sẵn chođội bảo mật sử dụng để giúp bảo vệ tổ chức của họ.Và sau này trong chương trình chứng chỉ,bạn sẽ có cơ hội thú vị để thực hành sử dụng Splunk Cloud và Chronicle.

2.2. More about cybersecurity tools – Tìm hiểu thêm về các công cụ an ninh mạng

More about cybersecurity tools

Tìm hiểu thêm về các công cụ an ninh mạng

Previously, you learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, you'll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

Trước đây, bạn đã tìm hiểu về một số công cụ được các thành viên nhóm an ninh mạng sử dụng để giám sát và xác định các mối đe dọa, rủi ro và lỗ hổng bảo mật tiềm ẩn. Trong bài đọc này, bạn sẽ tìm hiểu thêm về các công cụ an ninh mạng độc quyền và nguồn mở phổ biến mà bạn có thể sử dụng với tư cách là chuyên gia an ninh mạng.

Open-source tools

Công cụ nguồn mở

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.

Các công cụ nguồn mở thường miễn phí sử dụng và có thể thân thiện với người dùng. Mục tiêu của các công cụ nguồn mở là cung cấp cho người dùng phần mềm được công chúng xây dựng theo cách hợp tác, điều này có thể giúp phần mềm trở nên an toàn hơn. Ngoài ra, các công cụ nguồn mở cho phép người dùng tùy chỉnh nhiều hơn, dẫn đến nhiều dịch vụ mới được xây dựng từ cùng một gói phần mềm nguồn mở.

Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

Các kỹ sư phần mềm tạo ra các dự án nguồn mở để cải tiến phần mềm và cung cấp phần mềm cho mọi người sử dụng, miễn là giấy phép quy định được tôn trọng. Mã nguồn của các dự án nguồn mở luôn sẵn có cho người dùng cũng như tài liệu đào tạo đi kèm với chúng. Việc có sẵn những nguồn này cho phép người dùng sửa đổi và cải thiện tài liệu dự án.

Proprietary tools

Công cụ độc quyền

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a

limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

Các công cụ độc quyền được phát triển và sở hữu bởi một cá nhân hoặc công ty và người dùng thường phải trả phí cho việc sử dụng và đào tạo. Chủ sở hữu các công cụ độc quyền là những người duy nhất có thể truy cập và sửa đổi mã nguồn. Điều này có nghĩa là người dùng thường phải chờ cập nhật phần mềm và đôi khi họ có thể phải trả phí cho những cập nhật đó. Phần mềm độc quyền thường cho phép người dùng sửa đổi một số tính năng hạn chế để đáp ứng nhu cầu cá nhân và tổ chức. Ví dụ về các công cụ độc quyền bao gồm công cụ Splunk® và Chronicle SIEM.

Common misconceptions

Quan niệm sai lầm phổ biến

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they’re identified.

Có một quan niệm sai lầm phổ biến rằng các công cụ nguồn mở kém hiệu quả hơn và không an toàn khi sử dụng như các công cụ độc quyền. Tuy nhiên, các nhà phát triển đã tạo ra các tài liệu nguồn mở trong nhiều năm và đã trở thành tiêu chuẩn của ngành. Mặc dù sự thật là các tác nhân đe dọa đã cố gắng thao túng các công cụ nguồn mở, nhưng vì những công cụ này là nguồn mở nên những người có mục đích xấu thực sự khó gây tổn hại thành công hơn. Khả năng tiếp xúc rộng rãi và khả năng truy cập ngay vào mã nguồn của những người dùng cũng như chuyên gia có thiện chí và được thông tin đầy đủ sẽ giúp ít có khả năng xảy ra sự cố hơn vì họ có thể khắc phục sự cố ngay khi chúng được xác định.

Examples of open-source tools

Ví dụ về các công cụ nguồn mở

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

Trong lĩnh vực bảo mật, có nhiều công cụ có nguồn mở và phổ biến được sử dụng. Hai ví dụ là Linux và Suricata.

Linux

Linux

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It's used to communicate with the hardware of a computer and manage software applications.

Linux là một hệ điều hành mã nguồn mở được sử dụng rộng rãi. Nó cho phép bạn điều chỉnh hệ điều hành theo nhu cầu của mình bằng giao diện dòng lệnh. Hệ **điều hành** là giao diện giữa phần cứng máy tính và người dùng. Nó được sử dụng để giao tiếp với phần cứng của máy tính và quản lý các ứng dụng phần mềm.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

Có nhiều phiên bản Linux tồn tại để thực hiện các nhiệm vụ cụ thể. Linux và giao diện dòng lệnh của nó sẽ được thảo luận chi tiết ở phần sau trong chương trình chứng chỉ.

Suricata

Suricata

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Suricata is an open-source network analysis and threat detection software. Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata là một phần mềm phân tích mạng và phát hiện mối đe dọa nguồn mở. Phần mềm phân tích mạng và phát hiện mối đe dọa được sử dụng để kiểm tra lưu lượng mạng nhằm xác định hành vi đáng ngờ và tạo nhật ký dữ liệu mạng. Phần mềm phát hiện tìm thấy hoạt động trên người dùng, máy tính hoặc địa chỉ Giao thức Internet (IP) để giúp phát hiện các mối đe dọa, rủi ro hoặc lỗ hổng tiềm ẩn.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it’s free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

Suricata được phát triển bởi Tổ chức bảo mật thông tin mở (OISF). OISF tận tâm duy trì việc sử dụng nguồn mở của dự án Suricata để đảm bảo nó miễn phí và có sẵn công khai. Suricata được sử dụng rộng rãi trong khu vực công và tư nhân, đồng thời tích hợp với nhiều công cụ SIEM và các công cụ bảo mật khác. Suricata cũng sẽ được thảo luận chi tiết hơn ở phần sau của chương trình.

Key takeaways

Bài học chính

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and proprietary tools in more depth.

Các công cụ nguồn mở được sử dụng rộng rãi trong ngành an ninh mạng. Trong suốt chương trình chứng chỉ, bạn sẽ có nhiều cơ hội để tìm hiểu và khám phá sâu hơn cả công cụ nguồn mở và công cụ độc quyền.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

2.3. Talya: Myths about the cybersecurity field – Talya: Những lầm tưởng về lĩnh vực an ninh mạng

I'm Talya, and I'm an engineer within privacy, safety and security at Google. So there are a lot of myths in the cybersecurity space. One big one is, you must know how to code, or you must know how to hack, or you must be a math wiz. I don't know how to code, although I have learned how to read code over time. I'm not a hacker. I'm not on the red team site of security, I'm more on like the blue team. I'm not a math wiz. I definitely took the business route, but I'm not a mathematician. That wasn't really the path. A lot of my strength really lies in my ability to build relationships, learn quickly on the job, doing, conducting research, asking all the right questions. I think those have been my strongest strength. Another big myth, is that, you are required to have a cybersecurity degree. I actually went to school for business, an advanced degree is not required. Even though I did later on go back, That was my preference. You do not need to pursue that in order for you to be considered a great candidate for cybersecurity. Another big one is you work in isolation within cybersecurity. It really depends on the path that you choose. But I found that to be one of the most that couldn't be further from the truth. My biggest advice for anyone who's interested in cybersecurity is, be okay with creating your own path. The path looks different for everyone. If you were to talk to five different people, their journeys are all different. So own your journey, and identify people who can support you. Let them know that you're sitting for the certificate, and see what support that you can get as you start your journey.

Tôi là Talya và tôi là kỹ sư về quyền riêng tư,an toàn và bảo mật tại Google.Vì vậy, có rất nhiều huyền thoại trong lĩnh vực an ninh mạng.Một cái lớn là,bạn phải biết cách viết mã,hoặc bạn phải biết cách hack,hoặc bạn phải là một phù thủy toán học.Tôi không biết cách viết mã,mặc dù tôi đã học được cách đọc mã theo thời gian.Tôi không phải là hacker.Tôi không ở khu vực an ninh của đội đỏ,Tôi giống đội xanh hơn.Tôi không phải là một phù thủy toán học.Tôi chắc chắn đã chọn con đường kinh doanh,nhưng tôi không phải là nhà toán học.Đó thực sự không phải là con đường.Rất nhiều sức mạnh của tôi thực sự nằmtrong khả năng của tôi để xây dựng các mối quan hệ,học hỏi nhanh trong công việclàm, tiến hành nghiên cứu, đặt tất cả các câu hỏi đúng.Tôi nghĩ đó là sức mạnh mạnh nhất của tôi.Một huyền thoại lớn khác, đó là,bạn được yêu cầu phải có bằng cấp về an ninh mạng.Thực ra tôi đã đi học kinh doanh,bằng cấp cao là không cần thiết.Mặc dù sau đó tôi đã quay trở lại,Đó là sở thích của tôi.Bạn không cần phải theo đuổi điều đó đểbạn được coi là ứng cử viên sáng giá cho lĩnh vực an ninh mạng.Một vấn đề lớn nữa là bạn làm việcbiệt lập trong an ninh mạng.Nó thực sự phụ thuộc vào con đường bạn chọn.Nhưng tôi thấy đó là một trong những điều tuyệt vời nhấtđiều đó không thể xa hơn sự thật.Lời khuyên lớn nhất của tôi dành cho bất cứ aingười quan tâm đến an ninh mạng là,được rồi với việc tạo ra con đường của riêng bạn.Con đường có vẻ khác nhau đối với mọi người.Nếu bạn nói chuyện với năm người khác nhau,cuộc hành trình của họ đều khác nhau.Vì vậy, hãy sở hữu hành trình của bạn,và xác định những người có thể hỗ trợ bạn.Hãy cho họ biết rằng bạn đang thi lấy chứng chỉ,và xem bạn có thể hỗ trợ những gìnhận được khi bạn bắt đầu cuộc hành trình của mình.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

2.4. Use SIEM tools to protect organizations – Sử dụng công cụ SIEM để bảo vệ tổ chức

Use SIEM tools to protect organizations

Sử dụng công cụ SIEM để bảo vệ tổ chức

Previously, you were introduced to security information and event management (SIEM) tools and a few SIEM dashboards. You also learned about different threats, risks, and vulnerabilities an organization may experience. In this reading, you will learn more about SIEM dashboard data and how cybersecurity professionals use that data to identify a potential threat, risk, or vulnerability.

Trước đây, bạn đã được giới thiệu về các công cụ quản lý sự kiện và thông tin bảo mật (SIEM) cũng như một số bảng thông tin SIEM. Bạn cũng đã tìm hiểu về các mối đe dọa, rủi ro và lỗ hổng khác nhau mà một tổ chức có thể gặp phải. Trong bài đọc này, bạn sẽ tìm hiểu thêm về dữ liệu bảng điều khiển SIEM và cách các chuyên gia an ninh mạng sử dụng dữ liệu đó để xác định mối đe dọa, rủi ro hoặc lỗ hổng tiềm ẩn.

Splunk

Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization’s everyday operations.

Splunk cung cấp các tùy chọn công cụ SIEM khác nhau: Splunk® Enterprise và Splunk® Cloud. Cả hai đều cho phép bạn xem lại dữ liệu của tổ chức trên trang tổng quan. Điều này giúp các chuyên gia bảo mật quản lý cơ sở hạ tầng nội bộ của tổ chức bằng cách thu thập, tìm kiếm, giám sát và phân tích dữ liệu nhật ký từ nhiều nguồn để có được cái nhìn đầy đủ về hoạt động hàng ngày của tổ chức.

Review the following Splunk dashboards and their purposes:

Xem lại các bảng thông tin Splunk sau đây và mục đích của chúng:

Security posture dashboard

Bảng điều khiển tình trạng bảo mật

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization's notable security-related events and trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

Bảng thông tin về trạng thái bảo mật được thiết kế cho các trung tâm hoạt động bảo mật (SOC). Nó hiển thị 24 giờ qua về các sự kiện và xu hướng liên quan đến bảo mật đáng chú ý của tổ chức, đồng thời cho phép các chuyên gia bảo mật xác định xem cơ sở hạ tầng và chính sách bảo mật có hoạt động như thiết kế hay không. Các nhà phân tích bảo mật có thể sử dụng bảng thông tin này để giám sát và điều tra các mối đe dọa tiềm ẩn trong thời gian thực, chẳng hạn như hoạt động mạng đáng ngờ bắt nguồn từ một địa chỉ IP cụ thể.

Executive summary dashboard

Bảng điều khiển tóm tắt điều hành

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

Bảng thông tin tóm tắt điều hành phân tích và theo dõi tình trạng tổng thể của tổ chức theo thời gian. Điều này giúp các nhóm bảo mật cải thiện các biện pháp bảo mật giúp giảm thiểu rủi ro. Các nhà phân tích bảo mật có thể sử dụng bảng thông tin này để cung cấp thông tin chi tiết cấp cao cho các bên liên quan, chẳng hạn như tạo bản tóm tắt về các sự cố và xu hướng bảo mật trong một khoảng thời gian cụ thể.

Incident review dashboard

Bảng điều khiển đánh giá sự cố

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

Bảng điều khiển đánh giá sự cố cho phép các nhà phân tích xác định các mô hình đáng ngờ có thể xảy ra trong trường hợp xảy ra sự cố. Nó hỗ trợ bằng cách làm nổi bật các mục có rủi ro cao hơn cần được nhà phân tích xem xét ngay lập tức. Bảng thông tin này có thể rất hữu ích vì nó cung cấp dòng thời gian trực quan về các sự kiện dẫn đến sự cố.

Risk analysis dashboard

Bảng điều khiển phân tích rủi ro

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

Bảng thông tin phân tích rủi ro giúp các nhà phân tích xác định rủi ro cho từng đối tượng rủi ro (ví dụ: một người dùng cụ thể, máy tính hoặc địa chỉ IP). Nó cho thấy những thay đổi trong hoạt động hoặc hành vi liên quan đến rủi ro, chẳng hạn như người dùng đăng nhập ngoài giờ làm việc bình thường hoặc lưu lượng truy cập mạng cao bất thường từ một máy tính cụ thể. Nhà phân tích bảo mật có thể sử dụng bảng thông tin

này để phân tích tác động tiềm ẩn của các lỗ hổng trong các tài sản quan trọng, giúp các nhà phân tích ưu tiên các nỗ lực giảm thiểu rủi ro của họ.

Chronicle

Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user
- An IP address

Chronicle là một công cụ SIEM dựa trên đám mây của Google giúp lưu giữ, phân tích và tìm kiếm dữ liệu nhật ký để xác định các mối đe dọa, rủi ro và lỗ hổng bảo mật tiềm ẩn. Chronicle cho phép bạn thu thập và phân tích dữ liệu nhật ký theo:

- Một tài sản cụ thể
- Một tên miền
- Một người dùng
- Một địa chỉ IP

Chronicle provides multiple dashboards that help analysts monitor an organization's logs, create filters and alerts, and track suspicious domain names.

Chronicle cung cấp nhiều trang tổng quan giúp các nhà phân tích theo dõi nhật ký của tổ chức, tạo bộ lọc và cảnh báo cũng như theo dõi các tên miền đáng ngờ.

Review the following Chronicle dashboards and their purposes:

Xem lại các trang tổng quan Chronicle sau đây và mục đích của chúng:

Enterprise insights dashboard

Bảng thông tin chuyên sâu về doanh nghiệp

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

Bảng thông tin chuyên sâu về doanh nghiệp nêu bật các cảnh báo gần đây. Nó xác định các tên miền đáng ngờ trong nhật ký, được gọi là dấu hiệu xâm phạm (IOC). Mỗi kết quả được gắn nhãn với điểm tin cậy để cho biết khả năng xảy ra mối đe dọa. Nó cũng cung cấp mức độ nghiêm trọng cho thấy tầm quan trọng của từng mối đe dọa đối với tổ chức. Nhà phân tích bảo mật có thể sử dụng trang tổng quan này để giám sát các nỗ lực đăng nhập hoặc truy cập dữ liệu liên quan đến tài sản quan trọng—như ứng dụng hoặc hệ thống—từ các vị trí hoặc thiết bị bất thường.

Data ingestion and health dashboard

Trang tổng quan về tình trạng và nhập dữ liệu

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Trang tổng quan về tình trạng và quá trình nhập dữ liệu hiển thị số lượng nhật ký sự kiện, nguồn nhật ký và tỷ lệ thành công của dữ liệu được xử lý vào Chronicle. Nhà phân tích bảo mật có thể sử dụng bảng thông tin này để đảm bảo rằng nguồn nhật ký được đặt cấu hình chính xác và nhật ký được nhận mà không có lỗi. Điều này giúp đảm bảo rằng các vấn đề liên quan đến nhật ký được giải quyết để nhóm bảo mật có quyền truy cập vào dữ liệu nhật ký mà họ cần.

IOC matches dashboard

Bảng điều khiển trận đấu của IOC

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team's focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

Bảng điều khiển đối sánh IOC chỉ ra các mối đe dọa, rủi ro và lỗ hổng hàng đầu đối với tổ chức. Các chuyên gia bảo mật sử dụng bảng thông tin này để quan sát tên miền, địa chỉ IP và IOC của thiết bị theo thời gian nhằm xác định xu hướng. Thông tin này sau đó được sử dụng để hướng sự tập trung của nhóm bảo mật vào các mối đe dọa có mức độ ưu tiên cao nhất. Ví dụ: các nhà phân tích bảo mật có thể sử dụng trang tổng quan này để tìm kiếm hoạt động bổ sung liên quan đến cảnh báo, chẳng hạn như thông tin đăng nhập của người dùng đáng ngờ từ một vị trí địa lý bất thường.

Main dashboard

Bảng điều khiển chính

The main dashboard displays a high-level summary of information related to the organization's data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Trang tổng quan chính hiển thị bản tóm tắt thông tin cấp cao liên quan đến hoạt động nhập dữ liệu, cảnh báo và sự kiện của tổ chức theo thời gian. Các chuyên gia bảo mật có thể sử dụng bảng thông tin này để truy cập dòng thời gian của các sự kiện bảo mật—chẳng hạn như số lần đăng nhập không thành công tăng đột biến—để xác định xu hướng mối đe dọa trên các nguồn nhật ký, thiết bị, địa chỉ IP và vị trí thực tế.

Rule detections dashboard

Trang tổng quan phát hiện quy tắc

The rule detections dashboard provides statistics related to incidents with the highest occurrences, severities, and detections over time. Security analysts can use this dashboard to access a list of all the alerts triggered by a specific detection rule, such as a rule designed to alert whenever a user opens a known malicious attachment from an email. Analysts then use those statistics to help manage recurring incidents and establish mitigation tactics to reduce an organization's level of risk.

Trang tổng quan phát hiện quy tắc cung cấp số liệu thống kê liên quan đến các sự cố có số lần xuất hiện, mức độ nghiêm trọng và số lần phát hiện cao nhất theo thời gian. Các nhà phân tích bảo mật có thể sử dụng trang tổng quan này để truy cập danh sách tất cả các cảnh báo được kích hoạt bởi một quy tắc phát hiện cụ thể, chẳng hạn như quy tắc được thiết kế để cảnh báo bất cứ khi nào người dùng mở tệp đính kèm độc hại đã biết từ email. Sau đó, các nhà phân tích sử dụng những số liệu thống kê đó để giúp quản lý các sự cố tái diễn và thiết lập các chiến thuật giảm thiểu nhằm giảm mức độ rủi ro của tổ chức.

User sign in overview dashboard

Bảng điều khiển tổng quan về đăng nhập của người dùng

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization’s applications.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Trang tổng quan về đăng nhập của người dùng cung cấp thông tin về hành vi truy cập của người dùng trong toàn tổ chức. Các nhà phân tích bảo mật có thể sử dụng trang tổng quan này để truy cập danh sách tất cả các sự kiện đăng nhập của người dùng nhằm xác định hoạt động bất thường của người dùng, chẳng hạn như người dùng đăng nhập từ nhiều vị trí cùng một lúc. Thông tin này sau đó được sử dụng để giúp giảm thiểu các mối đe dọa, rủi ro và lỗ hổng đối với tài khoản người dùng và ứng dụng của tổ chức.

Key takeaways

Bài học chính

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you'll have an opportunity to practice using various SIEM tool features and commands for search queries.

Các công cụ SIEM cung cấp bảng thông tin giúp các chuyên gia bảo mật tổ chức và tập trung nỗ lực bảo mật của họ. Điều này rất quan trọng vì nó cho phép các nhà phân tích giảm thiểu rủi ro bằng cách xác định, phân tích và khắc phục kịp thời các mục có mức độ ưu tiên cao nhất. Ở phần sau của chương trình, bạn sẽ có cơ hội thực hành sử dụng các tính năng và lệnh khác nhau của công cụ SIEM cho các truy vấn tìm kiếm.

2.5. Test your knowledge: Identify threats and vulnerabilities with SIEM tools – Kiểm tra kiến thức của bạn: Xác định các mối đe dọa và lỗ hổng bằng các công cụ SIEM

3. Review: Introduction to cybersecurity tools – Review: Giới thiệu các công cụ an ninh mạng

3.1. Wrap-up – Gói lại

Let's quickly review what we covered in this section of the course. We started by discussing the importance of logs and cybersecurity, and we explored different log types, like firewall, network, and server logs. Next, we explored SIEM dashboards and how they use visual representations to provide security teams with quick and clear insights into the security posture of an organization.

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

Hãy nhanh chóng xem lại những gì chúng ta đã đề cập trong phần này của khóa học.Chúng tôi bắt đầu bằng việc thảo luận về tầm quan trọng của nhật ký và an ninh mạng,và chúng tôi đã khám phá các loại nhật ký khác nhau, như nhật ký tường lửa, mạng và máy chủ.Tiếp theo, chúng tôi khám phá bảng thông tin SIEM vàcách họ sử dụng các hình thức trình bày trực quan để cung cấp cho các nhóm bảo mật thông tin nhanh chóng vànhững hiểu biết rõ ràng về tình hình an ninh của một tổ chức.

Finally, we introduced common SIEM tools used in the cybersecurity industry, including Splunk and Chronicle.

Cuối cùng, chúng tôi đã giới thiệu các công cụ SIEM phổ biến được sử dụng trong an ninh mạngngành công nghiệp, bao gồm cả Splunk và Chronicle.

We'll be exploring even more security tools later in the program, and you'll have opportunities to practice using them. Coming up, we'll discuss playbooks and how they help security professionals respond appropriately to identify threats, risks, and vulnerabilities. Meet you there.

Chúng tôi sẽ khám phá nhiều công cụ bảo mật hơn nữa sau này trong chương trình vàbạn sẽ có cơ hội thực hành sử dụng chúng.Sắp tới, chúng ta sẽ thảo luận về các cẩm nang và cách chúng trợ giúp các chuyên gia bảo mậtphản ứng thích hợp để xác định các mối đe dọa, rủi ro và điểm yếu.Gặp bạn ở đó.

3.2. Glossary terms from module 3 – Thuật ngữ trong học phần 3

Glossary terms from module 3

Thuật ngữ trong học phần 3

Terms and definitions from Course 2, Module 3

Các thuật ngữ và định nghĩa trong Khóa 2, Học phần 3

Chronicle: A cloud-native tool designed to retain, analyze, and search data

Chronicle: Một công cụ dựa trên đám mây được thiết kế để lưu giữ, phân tích và tìm kiếm dữ liệu

Incident response: An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Phản ứng sự cố: Nỗ lực nhanh chóng của tổ chức nhằm xác định cuộc tấn công, ngăn chặn thiệt hại và khắc phục hậu quả của vi phạm an ninh

Log: A record of events that occur within an organization's systems

Nhật ký: Bản ghi các sự kiện xảy ra trong hệ thống của tổ chức

Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

Số liệu: Các thuộc tính kỹ thuật chính như thời gian phản hồi, tính khả dụng và tỷ lệ lỗi, được sử dụng để đánh giá hiệu suất của ứng dụng phần mềm

Operating system (OS): The interface between computer hardware and the user

Hệ điều hành (OS): Giao diện giữa phần cứng máy tính và người dùng

Playbook: A manual that provides details about any operational action

Playbook: Sách hướng dẫn cung cấp thông tin chi tiết về bất kỳ hành động vận hành nào

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Quản lý sự kiện và thông tin bảo mật (SIEM): Một ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng trong một tổ chức

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events

Điều phối, tự động hóa và phản hồi bảo mật (SOAR): Tập hợp các ứng dụng, công cụ và quy trình làm việc sử dụng tự động hóa để phản hồi các sự kiện bảo mật

SIEM tools: A software platform that collects, analyzes, and correlates security data from various sources across your IT infrastructure that helps identify and respond to security threats in real-time, investigate security incidents, and comply with security regulations

Công cụ SIEM: Nền tảng phần mềm thu thập, phân tích và tương quan dữ liệu bảo mật từ nhiều nguồn khác nhau trên cơ sở hạ tầng CNTT của bạn, giúp xác định và ứng phó với các mối đe dọa bảo mật trong thời gian thực, điều tra các sự cố bảo mật và tuân thủ các quy định bảo mật

Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data

Splunk Cloud: Một công cụ lưu trữ trên đám mây được sử dụng để thu thập, tìm kiếm và giám sát dữ liệu nhật ký

Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

Splunk Enterprise: Một công cụ tự lưu trữ được sử dụng để lưu giữ, phân tích và tìm kiếm dữ liệu nhật ký của tổ chức nhằm cung cấp thông tin và cảnh báo bảo mật trong thời gian thực

Module 3: Introduction to cybersecurity tools
Phần 3: Giới thiệu các công cụ an ninh mạng

3.3. Module 3 challenge – Thử thách mô-đun 3

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Module 4: Use playbooks to respond to incidents – Sử dụng playbook để ứng phó với sự cố

You'll learn about the purposes and common uses of playbooks. You'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

Bạn sẽ tìm hiểu về mục đích và cách sử dụng phổ biến của playbook. Bạn cũng sẽ khám phá cách các chuyên gia an ninh mạng sử dụng cẩm nang để ứng phó với các mối đe dọa, rủi ro và lỗ hổng đã xác định.

Learning Objectives

- Define and describe the purpose of a playbook.
- Use a playbook to respond to identified threats, risks, or vulnerabilities.

Mục tiêu học tập

- Xác định và mô tả mục đích của một playbook.
- Sử dụng cẩm nang để ứng phó với các mối đe dọa, rủi ro hoặc lỗ hổng đã xác định.

1. Phases of incident response playbooks – Các giai đoạn của cẩm nang ứng phó sự cố

1.1. Welcome to module 4 – Chào mừng đến với mô-đun 4

Hello and welcome back. You've reached the final section of this course! Previously, we discussed security information and event management, or SIEM tools, and how they can be used to help organizations improve their security posture.

Xin chào và chào mừng trở lại.Bạn đã đến phần cuối cùng của khóa học này!Trước đây, chúng ta đã thảo luận về thông tin bảo mật vàquản lý sự kiện hoặc các công cụ SIEM

vàcách chúng có thể được sử dụng để giúp các tổ chức cải thiện tình trạng bảo mật của họ.

Let's continue our security journey by exploring another tool security professionals use: playbooks. In this section, we'll explore how playbooks help security teams respond to threats, risks, or vulnerabilities identified by SIEM tools.

Hãy tiếp tục hành trình bảo mật của chúng tôi bằng cách khám phá một công cụ khácác chuyên gia bảo mật sử dụng: playbooks.Trong phần này, chúng ta sẽ khám phá cách sách hướng dẫn giúp nhóm bảo mật phản hồitrước các mối đe dọa, rủi ro hoặc lỗ hổng được xác định bởi các công cụ SIEM.

Then, we'll discuss the six phases of incident response. Let's get started!

Sau đó, chúng ta sẽ thảo luận về sáu giai đoạn ứng phó sự cố.Bắt đầu nào!

1.2. Phases of an incident response playbook – Các giai đoạn của cẩm nang ứng phó sự cố

Previously, we discussed how SIEM tools are used to help protect an organization's critical assets and data. In this video, we'll introduce another important tool for maintaining an organization's security, known as a playbook.

Trước đây, chúng ta đã thảo luận về cách sử dụng các công cụ SIEM đểgiúp bảo vệ tài sản và dữ liệu quan trọng của tổ chức.Trong video này chúng tôi sẽ giới thiệumột công cụ quan trọng khác đểduy trì an ninh của một tổ chức,được biết đến như một vở kịch.

A playbook is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident. In the security field, playbooks are essential.

Urgency, efficiency, and accuracy are necessary to quickly identify and mitigate a security threat to reduce potential risk. Playbooks ensure that people follow a

consistent list of actions in a prescribed way, regardless of who is working on the case.

Tính cấp bách, hiệu quả và chính xác là cần thiết đểnhanh chóng xác định và giảm thiểumột mối đe dọa an ninh để giảm thiểu rủi ro tiềm ẩn.Playbook đảm bảo rằng mọi người làm theomột danh sách nhất quán các hành động theo cách quy định,bất kể ai đang giải quyết vụ án.

Different types of playbooks are used. These include playbooks for incident response, security alerts, teams-specific, and product-specific purposes.

Các loại playbook khác nhau được sử dụng.Chúng bao gồm các cẩm nang ứng phó sự cố,cảnh báo an ninh,mục đích cụ thể của nhóm và sản phẩm cụ thể.

Here, we'll focus on a playbook that's commonly used in cybersecurity, called an incident response playbook. Incident response is an organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach. An incident response playbook is a guide with six phases used to help mitigate and manage security incidents from beginning to end. Let's discuss each phase.

Ở đây, chúng ta sẽ tập trung vào một cẩm nang thường được sử dụng trongan ninh mạng, được gọi là cẩm nang ứng phó sự cố.Ứng phó sự cố là việc của một tổ chứcnỗ lực nhanh chóng để xác định một cuộc tấn công,chứa đựng thiệt hại vàkhắc phục hậu quả của sự vi phạm an ninh.Cẩm nang ứng phó sự cố là một hướng dẫn cósáu giai đoạn được sử dụng để giúp giảm thiểu vàquản lý sự cố an ninh từ đầu đến cuối.Hãy thảo luận về từng giai đoạn.

The first phase is preparation. Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users. Preparation sets the foundation for successful incident response. For example, organizations can create incident response plans and procedures that outline the roles and responsibilities of each security team member.

Giai đoạn đầu tiên là chuẩn bị.Các tổ chức phải chuẩn bigiảm thiểu khả năng, rủi ro,và tác động củamột sự cố an ninh bằng cách ghi lại các thủ tục,thiết lập kế hoạch nhân sự và giáo dục người dùng.Sự chuẩn bị đặt nền tảngđể ứng phó sự cố thành công.Ví dụ,

các tổ chứccó thể tạo ra các kế hoạch ứng phó sự cố vàcác thủ tục phác thảo các vai trò vàtrách nhiệm của từng thành viên trong đội an ninh.

The second phase is detection and analysis. The objective of this phase is to detect and analyze events using defined processes and technology. Using appropriate tools and strategies during this phase helps security analysts determine whether a breach has occurred and analyze its possible magnitude.

Giai đoạn thứ hai là phát hiện và phân tích.Mục tiêu của giai đoạn này là phát hiện và phân tíchsự kiện sử dụng các quy trình và công nghệ xác định.Sử dụng các công cụ thích hợp vàchiến lược trong giai đoạn này giúpcác nhà phân tích bảo mật xác định liệu một vi phạm cóxảy ra và phân tích mức độ có thể xảy ra của nó.

The third phase is containment. The goal of containment is to prevent further damage and reduce the immediate impact of a security incident. During this phase, security professionals take actions to contain an incident and minimize damage. Containment is a high priority for organizations because it helps prevent ongoing risks to critical assets and data.

Giai đoạn thứ ba là ngăn chặn.Mục đích của việc ngăn chặn là ngăn chặnthiệt hại thêm và giảmtác động ngay lập tức của một sự cố an ninh.Trong giai đoạn này, các chuyên gia bảo mật sẽ thực hiệnhành động nhằm ngăn chặn sự cố và giảm thiểu thiệt hại.Ngăn chặn là ưu tiên hàng đầu của các tổ chứcvì nó giúp ngăn ngừarủi ro liên tục đối với tài sản và dữ liệu quan trọng.

The fourth phase in an incident response playbook is eradication and recovery. This phase involves the complete removal of an incident's artifacts so that an organization can return to normal operations. During this phase, security professionals eliminate artifacts of the incident by removing malicious code and mitigating vulnerabilities. Once they've exercised due diligence, they can begin to restore the affected environment to a secure state. This is also known as IT restoration.

Giai đoạn thứ tư trong ứng phó sự cốplaybook là diệt trừ và phục hồi.Giai đoạn này liên quan đến việc loại bỏ hoàn toàn sự cốtạo tác để một tổ chứccó thể trở lại hoạt động bình thường.Trong giai đoạn này,các chuyên gia bảo mật loại bỏ các tạo tác củasự việc bằng cách loại bỏmã độc hại và giảm thiểu các lỗ hổng.Một khi họ đã thực hiện sự siêng năng cần thiết,họ có thể bắt đầu khôi phụcmôi trường bị ảnh hưởng sang trạng thái an toàn.Điều này còn được gọi là khôi phục CNTT.

The fifth phase is post-incident activity. This phase includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure

that an organization is better prepared to handle future incidents. Depending on the severity of the incident, organizations can conduct a full-scale incident analysis to determine the root cause of the incident and implement various updates or improvements to enhance its overall security posture.

Giai đoạn thứ năm là hoạt động sau sự cố.Giai đoạn này bao gồm việc ghi lại sự việc,thông báo cho lãnh đạo tổ chức,và áp dụng các bài học kinh nghiệm để đảm bảo rằngmột tổ chức tốt hơnsẵn sàng xử lý các sự cố trong tương lai.Tùy theo mức độ nghiêm trọng của sự việc,các tổ chức có thể tiến hành phân tích sự cố toàn diệnđể xác định nguyên nhân gốc rễvề sự cố và thực hiện các cập nhật khác nhauhoặc cải tiến để nâng cao tình trạng bảo mật tổng thể của nó.

The sixth and final phase in an incident response playbook is coordination. Coordination involves reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards. Coordination is important for many reasons. It ensures that organizations meet compliance requirements and it allows for coordinated response and resolution.

Giai đoạn thứ sáu và cuối cùng trongmột cẩm nang ứng phó sự cố là sự phối hợp.Phối hợp liên quan đến việc báo cáo sự cốvà chia sẻ thông tin, xuyên suốtquá trình ứng phó sự cố, dựa trêntrên các tiêu chuẩn đã được thiết lập của tổ chức.Sự phối hợp rất quan trọng vì nhiều lý do.Nó đảm bảo rằng các tổ chức đáp ứngyêu cầu tuân thủ và nócho phép phối hợp phản ứng và giải quyết.

There are many ways security professionals may be alerted to an incident. You recently learned about SIEM tools and how they collect and analyze data. They use this data to detect threats and generate alerts, which can inform the security team of a potential incident. Then, when a security analyst receives a SIEM alert, they can use the appropriate playbook to guide the response process. SIEM tools and playbooks work together to provide a structured and efficient way of responding to potential security incidents.

Có rất nhiều cáchcác chuyên gia an ninh có thể được cảnh báo về một sự cố.Gần đây bạn đã biết vềCác công cụ SIEM và cách chúng thu thập và phân tích dữ liệu.Họ sử dụng dữ liệu này để phát hiện các mối đe dọa và tạo racảnh báo, có thể thông báođội an ninh của một sự cố tiềm ẩn.Sau đó, khi nhà phân tích bảo mật nhận được cảnh báo SIEM,họ có thể sử dụng cẩm nang thích hợpđể hướng dẫn quá trình phản hồi.Các công cụ và sách hướng dẫn của SIEM phối hợp với nhau để cung cấpmột cách có cấu trúc và hiệu quảứng phó với các sự cố an ninh có thể xảy ra.

Throughout the program, you'll have opportunities to continue to build your understanding of these important concepts.

Xuyên suốt chương trình,bạn sẽ có cơ hội để tiếp tục xây dựngsự hiểu biết của bạn về những khái niệm quan trọng này.

1.3. More about playbooks – Tìm hiểu thêm về playbooks

More about playbooks

Tìm hiểu thêm về playbooks

Previously, you learned that playbooks are tools used by cybersecurity professionals to identify and respond to security issues. In this reading, you'll learn more about playbooks and their purpose in the field of cybersecurity.

Trước đây, bạn đã biết rằng cẩm nang là công cụ được các chuyên gia an ninh mạng sử dụng để xác định và ứng phó với các vấn đề bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cẩm nang và mục đích của chúng trong lĩnh vực an ninh mạng.

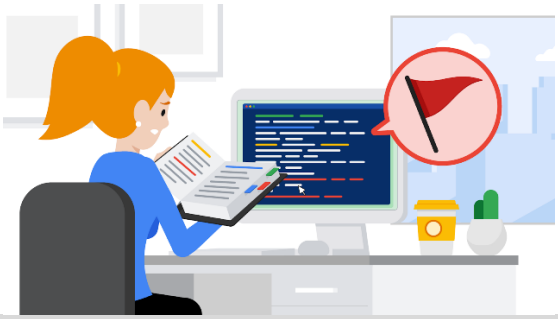
Playbook overview

Tổng quan về playbooks

A **playbook** is a manual that provides details about any operational action. Essentially, a playbook provides a predefined and up-to-date list of steps to perform when responding to an incident.

Playbook là một sổ tay hướng dẫn cung cấp thông tin chi tiết về bất kỳ hành động vận hành nào. Về cơ bản, cẩm nang cung cấp danh sách các bước được xác định trước và cập nhật để thực hiện khi ứng phó với một sự cố.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố



Playbooks are accompanied by a strategy. The strategy outlines expectations of team members who are assigned a task, and some playbooks also list the individuals responsible. The outlined expectations are accompanied by a plan. The plan dictates how the specific task outlined in the playbook must be completed.

Playbook được đi kèm với một chiến lược. Chiến lược nêu ra những kỳ vọng của các thành viên trong nhóm được giao nhiệm vụ và một số sách hướng dẫn cũng liệt kê những cá nhân chịu trách nhiệm. Những mong đợi được vạch ra sẽ đi kèm với một kế hoạch. Kế hoạch chỉ ra cách thức hoàn thành nhiệm vụ cụ thể được nêu trong sổ tay.

Playbooks should be treated as living documents, which means that they are frequently updated by security team members to address industry changes and new threats. Playbooks are generally managed as a collaborative effort, since security team members have different levels of expertise.

Playbook phải được coi như tài liệu sống, nghĩa là chúng được các thành viên nhóm bảo mật cập nhật thường xuyên để giải quyết những thay đổi trong ngành và các mối đe dọa mới. Playbook thường được quản lý như một nỗ lực hợp tác vì các thành viên nhóm bảo mật có trình độ chuyên môn khác nhau.

Updates are often made if:

- A failure is identified, such as an oversight in the outlined policies and procedures, or in the playbook itself.
- There is a change in industry standards, such as changes in laws or regulatory compliance.
- The cybersecurity landscape changes due to evolving threat actor tactics and techniques.

Cập nhật thường được thực hiện nếu:

- Một sai sót được xác định, chẳng hạn như sơ suất trong các chính sách và thủ tục đã vạch ra hoặc trong chính cẩm nang.
- Có sự thay đổi trong các tiêu chuẩn ngành, chẳng hạn như những thay đổi về luật pháp hoặc việc tuân thủ quy định.
- Bối cảnh an ninh mạng thay đổi do các chiến thuật và kỹ thuật của tác nhân đe dọa ngày càng phát triển.

Types of playbooks

Các loại playbook

Playbooks sometimes cover specific incidents and vulnerabilities. These might include ransomware, vishing, business email compromise (BEC), and other attacks previously discussed. Incident and vulnerability response playbooks are very common, but they are not the only types of playbooks organizations develop.

Playbook đôi khi bao gồm các sự cố và lỗ hổng cụ thể. Chúng có thể bao gồm ransomware, vishing, xâm phạm email doanh nghiệp (BEC) và các cuộc tấn công khác đã được thảo luận trước đây. Các cẩm nang ứng phó sự cố và lỗ hổng rất phổ biến, nhưng chúng không phải là loại cẩm nang duy nhất mà các tổ chức phát triển.

Each organization has a different set of playbook tools, methodologies, protocols, and procedures that they adhere to, and different individuals are involved at each step of the response process, depending on the country they are in. For example, incident notification requirements from government-imposed laws and regulations, along with compliance standards, affect the content in the playbooks. These requirements are subject to change based on where the incident originated and the type of data affected.

Mỗi tổ chức có một bộ công cụ, phương pháp, giao thức và quy trình trong cẩm nang khác nhau mà họ tuân thủ và các cá nhân khác nhau tham gia vào từng bước của quy trình ứng phó, tùy thuộc vào quốc gia họ sinh sống. Ví dụ: các yêu cầu thông báo sự cố từ chính phủ -luật và quy định được áp dụng, cùng với các tiêu chuẩn tuân thủ, ảnh hưởng đến nội dung trong cẩm nang. Các yêu cầu này có thể thay đổi tùy theo nơi xảy ra sự cố và loại dữ liệu bị ảnh hưởng.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Incident and vulnerability response playbooks

Sách hướng dẫn ứng phó sự cố và lỗ hổng

Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan. A business continuity plan is an established path forward allowing a business to recover and continue to operate as normal, despite a disruption like a security breach.

Sách hướng dẫn ứng phó sự cố và lỗ hổng thường được các chuyên gia an ninh mạng cấp thấp sử dụng. Chúng được phát triển dựa trên các mục tiêu được nêu trong kế hoạch kinh doanh liên tục của tổ chức. Kế hoạch kinh doanh liên tục là một lộ trình được thiết lập về phía trước cho phép doanh nghiệp phục hồi và tiếp tục hoạt động như bình thường, bất chấp sự gián đoạn như vi phạm an ninh.

These two types of playbooks are similar in that they both contain predefined and up-to-date lists of steps to perform when responding to an incident. Following these steps is necessary to ensure that you, as a security professional, are adhering to legal and organizational standards and protocols. These playbooks also help minimize errors and ensure that important actions are performed within a specific timeframe.

Hai loại cẩm nang này giống nhau ở chỗ đều chứa danh sách các bước được xác định trước và cập nhật để thực hiện khi ứng phó với sự cố. Việc làm theo các bước này là cần thiết để đảm bảo rằng bạn, với tư cách là một chuyên gia bảo mật, đang tuân thủ các tiêu chuẩn và giao thức pháp lý và tổ chức. Những cẩm nang này cũng giúp giảm thiểu sai sót và đảm bảo rằng các hành động quan trọng được thực hiện trong một khung thời gian cụ thể.

When an incident, threat, or vulnerability occurs or is identified, the level of risk to the organization depends on the potential damage to its assets. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. For this reason, a sense of urgency is essential. Following the steps outlined in playbooks is also important if any forensic task is being carried out. Mishandling data can easily compromise forensic data, rendering it unusable.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Khi một sự cố, mối đe dọa hoặc điểm yếu xảy ra hoặc được xác định, mức độ rủi ro đối với tổ chức phụ thuộc vào thiệt hại tiềm ẩn đối với tài sản của tổ chức. Công thức cơ bản để xác định mức độ rủi ro là rủi ro bằng khả năng xảy ra mối đe dọa. Vì lý do này, cảm giác cấp bách là điều cần thiết. Việc làm theo các bước được nêu trong sách hướng dẫn cũng rất quan trọng nếu bất kỳ nhiệm vụ pháp lý nào đang được thực hiện. Việc xử lý sai dữ liệu có thể dễ dàng làm tổn hại đến dữ liệu điều tra, khiến dữ liệu đó không thể sử dụng được.

Common steps included in incident and vulnerability playbooks include:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery from an incident

Các bước phổ biến có trong sổ tay sự cố và lỗ hổng bảo mật bao gồm:

- Sự chuẩn bị
- Phát hiện
- Phân tích
- ngăn chặn
- Diệt trừ
- Phục hồi từ sự cố

Additional steps include performing post-incident activities, and a coordination of efforts throughout the investigation and incident and vulnerability response stages.

Các bước bổ sung bao gồm thực hiện các hoạt động sau sự cố và phối hợp các nỗ lực trong suốt giai đoạn điều tra, giai đoạn ứng phó sự cố và lỗ hổng.

Key takeaways

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Bài học chính

It is essential to refine processes and procedures outlined in a playbook. With every documented incident, cybersecurity teams need to consider what was learned from the incident and what improvements should be made to handle incidents more effectively in the future. Playbooks create structure and ensure compliance with the law.

Điều cần thiết là phải tinh chỉnh các quy trình và thủ tục được nêu trong sổ tay. Với mỗi sự cố được ghi lại, các nhóm an ninh mạng cần xem xét những bài học rút ra được từ sự cố đó và những cải tiến nào cần thực hiện để xử lý sự cố hiệu quả hơn trong tương lai. Playbooks tạo ra cấu trúc và đảm bảo tuân thủ pháp luật.

Resources for more information

Tài nguyên để biết thêm thông tin

Incident and vulnerability response playbooks are only two examples of the many playbooks that an organization uses. If you plan to work as a cybersecurity professional outside of the U.S., you may want to explore the following resources:

- United Kingdom, National Cyber Security Center (NCSC) - Incident Management
- Australian Government - Cyber Incident Response Plan
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) - Vulnerability Handling and related guidelines
- Government of Canada - Ransomware Playbook
- Scottish Government - Playbook Templates

Cẩm nang ứng phó sự cố và lỗ hổng chỉ là hai ví dụ trong số rất nhiều cẩm nang mà một tổ chức sử dụng. Nếu dự định làm chuyên gia an ninh mạng bên ngoài Hoa Kỳ, bạn có thể muốn khám phá các tài nguyên sau:

- Vương quốc Anh, Trung tâm An ninh Mạng Quốc gia (NCSC) - Quản lý Sự cố

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

- Chính phủ Úc - Kế hoạch ứng phó sự cố mạng
- Trung tâm điều phối nhóm ứng phó khẩn cấp máy tính Nhật Bản (JPCERT/CC) - Xử lý lỗ hổng bảo mật và các hướng dẫn liên quan
- Chính phủ Canada - Cẩm nang về ransomware
- Chính phủ Scotland - Mẫu Playbook

1.4. Identify: Phases of an incident response playbook – Xác định: Các giai đoạn của cẩm nang ứng phó sự cố

Phase	Description
Preparation	Before incidents occur, mitigate potential impacts on the organization by documenting, establishing staffing plans, and educating users.
Detection and analysis	Detect and analyze events by implementing defined processes and appropriate technology.
Containment	Prevent further damage and reduce immediate impact of incidents.
Eradication and recovery	Completely remove artifacts of the incident so that an organization can return to normal operations.
Post-incident activity	Document the incident, inform organizational leadership, and apply lessons learned.
Coordination	Report incidents and share information throughout the response process, based on established standards.

Giai đoạn	Miêu tả
Sự chuẩn bị	Trước khi sự cố xảy ra, hãy giảm thiểu tác động tiềm ẩn đối với tổ chức bằng cách ghi chép, thiết lập kế hoạch nhân sự và giáo dục người dùng.
Phát hiện và phân tích	Phát hiện và phân tích các sự kiện bằng cách thực hiện các quy trình xác định và công nghệ phù hợp.

Ngăn chặn	Ngăn chặn thiệt hại thêm và giảm tác động ngay lập tức của sự cố.
Loại bỏ và phục hồi	Loại bỏ hoàn toàn các dấu vết của sự cố để tổ chức có thể trở lại hoạt động bình thường.
Hoạt động sau sự cố	Ghi lại sự việc, thông báo cho lãnh đạo tổ chức và áp dụng các bài học kinh nghiệm.
Phối hợp	Báo cáo sự cố và chia sẻ thông tin trong suốt quá trình ứng phó, dựa trên các tiêu chuẩn đã được thiết lập.

1.5. Zack: Incident response and the value of playbooks – Zack: Ứng phó sự cố và giá trị của cẩm nang

My name is Zack. I'm a Software Engineer on the security team in Google Workspace. I have non-traditional background. When I graduated college, I originally thought that I would pursue law, but I was accepted and I decided not to go. Instead, I joined Google in recruiting. Through that work, I did a little bit of strategy work where I taught myself web scraping and I really liked it, so I took one of Google's internal training courses that helped me move from recruiting to software engineering. Processes and playbooks are documentation that software engineers and other people at Google use to determine how we can respond to things that happen. Whether that's a security or privacy incident, whether that's an active attack, we have sets of guidelines or algorithms that we use to determine the best course of action to make sure that we manage people's data and security well. I'm relatively new to cybersecurity. I've been a software engineer here for about two years, and I don't have enough knowledge to be able to respond to every single thing that could possibly come my way when I'm on call or when I'm helping resolve a vulnerability. The playbooks are super important to people like me and other folks who are joining the industry new because they allow you to solve the problem with the experience of a much more experienced person, basically decades of experience in your own resolution because you can rely on this playbook and other people's advice. The kind of things that we use playbooks for our open attacks, privacy incidents, data leaks, denial of service attacks, service alerts, and others. When I first started out at Google, my first task on the security team was to fix an externally reported vulnerability. That means some security researcher out in the wild was playing with our app and found something that could potentially leak our user's data. When I received that, it was my first task on the team. Looking back on it, it's a relatively easy thing to solve, but it felt really overwhelming at the time. But when we receive a vulnerability report, it comes with remediation guidance. There were steps in the bug that was sent to me saying this is the things that we think that you should do. The things that I would say to somebody who's interested in starting out in cybersecurity is talk to as many people in the industry as you can. You'll learn about what the job is like. You'll learn about the skills that you need to get yourself there. If that's something that you're interested

in, you'll learn about open jobs and roles, what it's like to work at different companies. I wish people had told me when I graduated college that what these jobs are really like. I thought that coding would be heads down, typing away at a computer and a dark office for 12 hours a day. But it's not like that at all. 50% is communicating with other people and reviewing designs and talking about ideas. That's really compelling and I think if somebody had said that to me at the beginning of my career would have been totally different. Some teams come in and out of fashion, but security is ever-present. It's really important now it's only getting more important. There's a certain amount of security that comes with being in a security team. Definitely, a good place to be.

Tên tôi là Zack. Tôi là Kỹ sư phần mềm trênnhóm bảo mật trong Google Workspace.Tôi có nền tảng phi truyền thống.Khi tôi tốt nghiệp đại học, ban đầu tôinghĩ rằng tôi sẽ theo đuổi ngành luật,nhưng tôi đã được chấp nhận và tôi quyết định không đi.Thay vào đó, tôi tham gia tuyển dụng tại Google.Thông qua công việc đó tôi đã làm được một chútcông việc về chiến lược nơi tôi đã tự dạy mìnhquét web và tôi thực sự thích nó, vì vậyTôi lấy một trongCác khóa đào tạo nội bộ của Google đã giúp tôichuyển từ tuyển dụng sang công nghệ phần mềm.Các quy trình và sách hướng dẫn đượctài liệu mà các kỹ sư phần mềm và những người khác tạiGoogle sử dụng để xác định cách chúng tôi có thểphản ứng với những điều xảy ra.Cho dù đó là sự cố về bảo mật hay quyền riêng tư,cho dù đó là một cuộc tấn công tích cực,chúng tôi có bộ hướng dẫn hoặcthuật toán mà chúng tôi sử dụng để xác địnhcách hành động tốt nhất để đảm bảo rằng chúng ta quản lýdữ liệu của mọi người và bảo mật tốt.Tôi còn khá mới với an ninh mạng.Tôi đã làm kỹ sư phần mềm ở đây được khoảng hai năm,và tôi không có đủ kiến thứcđể có thể đáp ứngmọi thứ có thểcó thể sẽ đến với tôi khi tôi đang ở trêngọi điện hoặc khi tôi đang giúp giải quyết một lỗ hổng.Playbook cực kỳ quan trọngvới những người như tôi và những người khácgia nhập ngành mới vì chúng cho phép bạn giải quyếtvấn đề với kinh nghiệmcủa một người có nhiều kinh nghiệm hơn,về cơ bản hàng thập kỷ kinh nghiệm trongcách giải quyết của riêng bạn bởi vì bạn có thểhãy dựa vào cẩm nang này và lời khuyên của người khác.Những thứ mà chúng tôi sử dụng sách hướng dẫn cho các cuộc tấn công mở,sự cố về quyền riêng tư, rò rỉ dữ liệu,sự từ chối của dịch vụ tấn công,cảnh báo dịch vụ và những cảnh báo khác.Khi tôi mới bắt đầu làm việc tại Google,nhiệm vụ đầu tiên của tôi trong đội an ninhlà để khắc phục một lỗ hổng được báo cáo bên ngoài.Điều đó có nghĩa là một số nhà nghiên cứu bảo mậtngoài thiên nhiên đang chơi đùa vớiứng dụng của chúng tôi và tìm thấy thứ gì đó có thểcó khả năng rò rỉ dữ liệu người dùng của chúng tôi.Khi tôi nhận được điều đó,đó là nhiệm vụ đầu tiên của tôi trong đội.Nhìn lại thì đó làmột điều tương đối dễ dàng để giải quyết,nhưng lúc đó nó thực sự cảm thấy choáng ngợp.Nhưng khi chúng tôi nhận được báo cáo về lỗ hổng,nó đi kèm với hướng dẫn khắc phục.Có các bước trong lỗi đã được gửivới tôi nói điều nàylà những điều chúng tôi nghĩ bạn nên làm.Những điều mà tôi sẽ nói vớiai đó quan tâm đến việc bắt đầuan ninh mạng được gọi lànhiều người trong ngành nhất có thể.Bạn sẽ tìm hiểu về công việc đó như thế nào.Bạn sẽ tìm hiểu về những kỹ năng mà bạncần phải tự mình đến đó.Nếu đó là điều bạn quan tâm,bạn sẽ tìm hiểu về các công việc và vai trò đang mở,cảm giác làm việc ở các công ty khác nhau như thế nào.Tôi ước mọi người đã nói với tôi khi tôi tốt nghiệpđại học rằng những công việc này thực sự như thế nào.Tôi đã nghĩ rằng việc viết mã sẽ rất khó khăn,gõ phím trên máy tính vàmột văn phòng tối tăm trong 12 giờ một ngày.Nhưng nó không hề như thế chút nào.50% đang liên lạc vớingười khác và xem xétthiết kế và nói về ý tưởng.Điều đó thực sự hấp dẫn và tôinghĩ xem nếu ai đó đã nói điều đóvới tôi vào lúc bắt đầusự nghiệp sẽ hoàn toàn khác.Một số đội đến rồi lại lỗi thời,nhưng an ninh luôn hiện diện.Bây giờ nó thực sự

quan trọngchỉ trở nên quan trọng hơn.Có một mức độ bảo mật nhất định đi kèmvới việc ở trong một đội an ninh.Chắc chắn, một nơi tốt để được.

1.6. Test your knowledge: Incident response – Kiểm tra kiến thức của bạn: Ứng phó sự cố

2. Explore incident response – Khám phá ứng phó sự cố

2.1. Use a playbook to respond to threats, risks, or vulnerabilities – Sử dụng cẩm nang để ứng phó với các mối đe dọa, rủi ro hoặc lỗ hổng bảo mật

Welcome back! In this video, we're going to revisit SIEM tools and how they're used alongside playbooks to reduce organizational threats, risks, and vulnerabilities.

Chào mừng trở lại!Trong video này,chúng ta sẽ xem lạiCác công cụ SIEM và cách sử dụng chúngcẩm nang để giảm thiểu các mối đe dọa của tổ chức,rủi ro và tình trạng dễ bị tổn thương.

An incident response playbook is a guide that helps security professionals mitigate issues with a heightened sense of urgency, while maintaining accuracy. Playbooks create structure, ensure compliance, and outline processes for communication and documentation. Organizations may use different types of incident response playbooks depending on the situation. For example, an organization may have specific playbooks for addressing different types of attacks, such as ransomware, malware, distributed denial of service, and more.

Một cẩm nang ứng phó sự cố làhướng dẫn giúp các chuyên gia bảo mậtgiảm thiểu các vấn đề với ý thức cao hơn vềtính cấp bách mà vẫn đảm bảo tính chính xác.Playbooks tạo ra cấu trúc, đảm bảo sự tuân thủ,và phác thảo các quy trình chogiao tiếp và tài liệu.Các tổ chức có thể sử dụng các loạisách hướng dẫn ứng phó sự cố tùy theo tình huống.Ví dụ, một tổ chức có thể cósách hướng dẫn cụ thể để giải quyếtcác kiểu tấn công khác nhau,chẳng hạn như ransomware, phần mềm độc hại,từ chối dịch vụ phân tán, và nhiều hơn nữa.

To start, let's discuss how a security analyst might use a playbook to address a SIEM alert, like a potential malware attack. In this situation, a playbook is invaluable for guiding an analyst through the necessary actions to properly address the alert.

Để bắt đầu, hãy thảo luận về cách một nhà phân tích bảo mật có thể sử dụngmột cẩm nang để giải quyết cảnh báo SIEM, chẳng hạn như một cuộc tấn công phần mềm độc hại

tiềm ẩn.Trong tình huống này, một cuốn cẩm nang là vô giá đối vớihướng dẫn một nhà phân tích thông quacác hành động cần thiết để giải quyết đúng cảnh báo.

The first action in the playbook is to assess the alert. This means determining if the alert is actually valid by identifying why the alert was generated by the SIEM. This can be done by analyzing log data and related metrics.

Hành động đầu tiên trong cẩm nang là đánh giá cảnh báo.Điều này có nghĩa là xác định xem cảnh báo có thực sựhợp lệ bằng cách xác định lý do tại saocảnh báo được tạo ra bởi SIEM.Điều này có thể được thực hiện bằng cách phân tíchdữ liệu nhật ký và các số liệu liên quan.

Next, the playbook outlines the actions and tools to use to contain the malware and reduce further damage. For example, this playbook instructs the analyst to isolate, or disconnect, the infected network system to prevent the malware from spreading into other parts of the network.

Tiếp theo, cẩm nang phác thảo các hành động và công cụ đểsử dụng để chứa phần mềm độc hại và giảm thiệt hại thêm.Ví dụ: cẩm nang này hướng dẫnnhà phân tích có thể cô lập hoặc ngắt kết nối,hệ thống mạng bị nhiễm để ngăn chặnphần mềm độc hại lây lanvào các phần khác của mạng.

After containing the incident, step three of the playbook describes ways to eliminate all traces of the incident and restore the affected systems back to normal operations. For example, the playbook might instruct the analyst to restore the impacted operating system, then restore the affected data using a clean backup, created before the malware outbreak.

Sau khi khống chế được sự việc,bước ba của cẩm nang mô tảcách xóa bỏ mọi dấu vết của sự việcvà khôi phục các hệ thống bị ảnh hưởngtrở lại hoạt động bình thường.Ví dụ: playbook có thể hướng dẫnnhà phân tích để khôi phục hệ điều hành bị ảnh hưởng,sau đó khôi phục dữ liệu bị ảnh hưởng bằng cách sử dụngmột bản sao lưu sạch, được tạo trước khi phần mềm độc hại bùng phát.

Finally, once the incident has been resolved, step four of the playbook instructs the analyst to perform various post-incident activities and coordination efforts with the security team. Some actions include creating a final report to communicate the security incident to stakeholders, or reporting the incident to the appropriate

authorities, like the U.S. Federal Bureau of Investigations or other agencies that investigate cyber crimes.

Cuối cùng, khi sự việc đã được giải quyết,bước bốn của cẩm nang hướng dẫn nhà phân tích thực hiệncác hoạt động khác nhau sau sự cốvà nỗ lực phối hợp với đội an ninh.Một số hành động bao gồm tạo báo cáo cuối cùng chotruyền đạt sự cố an ninh tới các bên liên quan,hoặc báo cáo vụ việc cho cơ quan có thẩm quyền,như Cục Điều tra Liên bang Hoa Kỳhoặc các cơ quan khác điều tra tội phạm mạng.

This is just one example of how you might follow the steps in a playbook, since organizations develop their own internal procedures for addressing security incidents. What's most important to understand is that playbooks provide a consistent process for security professionals to follow.

Đây chỉ là một ví dụ về cáchbạn có thể làm theo các bước trong cẩm nang,vì các tổ chức phát triển các thủ tục nội bộ của riêng họđể giải quyết các sự cố an ninh.Điều quan trọng nhất cần hiểu là các vở kịchcung cấp một quy trình nhất quánđể các chuyên gia bảo mật theo dõi.

Note that playbooks are living documents, meaning the security team will make frequent changes, updates, and improvements to address new threats and vulnerabilities. In addition, organizations learn from past security incidents to improve their security posture, refine policies and procedures, and reduce the likelihood and impact of future incidents. Then, they update their playbooks accordingly.

Lưu ý rằng playbook là tài liệu sống,nghĩa là đội an ninh sẽ thực hiện những thay đổi thường xuyên,cập nhật và cải tiến đối vớigiải quyết các mối đe dọa và lỗ hổng mới.Ngoài ra, các tổ chức còn học hỏi từsự cố an ninh trong quá khứ đểcải thiện tình hình an ninh của họ,hoàn thiện các chính sách và thủ tục,và giảm thiểu khả năng cũng như tác động của các sự cố trong tương lai.Sau đó, họ cập nhật playbook của mình cho phù hợp.

As an entry-level security analyst, you may be required to use playbooks frequently, especially when monitoring networks and responding to incidents. Having an understanding of why playbooks are important and how they can help you achieve your working objectives will help ensure your success within this field.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Là một nhà phân tích bảo mật cấp đầu vào,bạn có thể phải sử dụng playbook thường xuyên,đặc biệt là khi giám sát mạngvà ứng phó với các sự cố.Có sự hiểu biết về lý do tại saocẩm nang rất quan trọng và chúng có thể giúp bạn như thế nàođạt được mục tiêu làm việc của bạn sẽgiúp đảm bảo sự thành công của bạn trong lĩnh vực này.

2.2. Erin: The importance of diversity of perspective on a security team – Erin: Tầm quan trọng của sự đa dạng về quan điểm trong nhóm bảo mật

Hi everyone. My name is Erin and I am a privacy engineer at Google. I work on speculative and emerging technology. So think of things that don't exist in the world, and that are coming within the next two to five years. My role is basically to take a look at all of the things that we are creating in terms of technology, and making sure that privacy is embedded in that. I am thinking for users before they even touch the product, making sure that when they utilize them, they'll have some form of trust in the engagement with that product. As well as knowing that we are protecting their privacy, things that they don't want to share or broadcast, and making sure that they're informed before they even touch the product. I always talk about soft skills being the most important thing over the technical skills. Because we can teach you anything but we can't teach you how to relate to people. That is something that you bring to the table. Diversity of thought and diversity of perspectives are very useful in understanding the world that we exist in. Because if we are designing products for everyday people, we need everyday people to basically help us understand those perspectives. Because I may look at something one way, but my colleague may see it another way based on their own experiences. And so, when you work together and come from different environments, you actually bring more equity and more depth to the things that you're looking at. And the perspective that you bring is the essential voice that is required in order to make a product better. When you look at people who work in journalism, or people who, like myself, worked in entertainment, they are bringing a different perspective for how they would tackle something. Or if we have a product where we are trying to convince a product team that maybe we shouldn't do this, it's always helpful to say, from someone who worked in journalism, do we really want this to end up in The Times? Probably not, right? And that is a way to come at people that, on the ground floor, they understand what that looks like. All of the experiences that you have had from the time you were born to now, they have been your experience. And you have to think about that in terms of where we're going with technology. When we're developing for a wide array of people, your experience may be someone else's experience. And so if we don't have you in the room, then we are missing the opportunity to actually bring something beautiful, I would say, to the equation. Which is why I encourage people, please come work with us in terms of technology. Get involved in STEM because the equity across product security, privacy, you name it, whether it be software engineering, everything requires a different voice. And it actually requires your voice.

Chào mọi người. Tên tôi là Erin vàTôi là kỹ sư về quyền riêng tư tại Google.Tôi làm việc về công nghệ đầu cơ và mới nổi.Vì vậy, hãy nghĩ về những thứ không tồn tại trên thế giới vàsẽ đến trong vòng hai đến năm năm tới.Vai trò của tôi về cơ bản là xem xét tất cả những thứ chúng tôi đang tạo ravề mặt công nghệ và đảm bảo rằng quyền riêng tư được lồng ghép vào đó.Tôi đang nghĩ cho người dùng thậm chí trước khi họ chạm vào

sản phẩm,đảm bảo rằng khi họ sử dụng chúng,họ sẽ có một số hình thức tin tưởng khi tương tác với sản phẩm đó.Cũng như biết rằng chúng tôi đang bảo vệ quyền riêng tư của họ,những thứ mà họ không muốn chia sẻ hoặc phát sóng, vàđảm bảo rằng họ được thông báo trước khi chạm vào sản phẩm.Tôi luôn nói về kỹ năng mềm là điều quan trọng nhất so với kỹ năng kỹ thuật.kỹ năng.Bởi vì chúng tôi có thể dạy bạn bất cứ điều gì nhưng chúng tôi không thể dạy bạn cách liên hệ với mọi người.Đó là thứ mà bạn mang lên bàn.Sự đa dạng trong suy nghĩ và sự đa dạng về quan điểm rất hữu ích tronghiểu thế giới mà chúng ta đang tồn tại.Bởi vì nếu chúng ta thiết kế sản phẩm cho người thường,về cơ bản chúng ta cần những người bình thường giúp chúng ta hiểu những quan điểm đó.Bởi vì tôi có thể nhìn sự việc theo một cách, nhưngđồng nghiệp của tôi có thể nhìn nhận nó theo cách khác dựa trên kinh nghiệm của chính họ.Và vì vậy, khi bạn làm việc cùng nhau và đến từ những môi trường khác nhau, bạn thực sựmang lại sự công bằng hơn và chiều sâu hơn cho những thứ bạn đang xem.Và quan điểm mà bạn mang lại chính là tiếng nói thiết yếucần thiết để làm cho sản phẩm tốt hơn.Khi bạn nhìn vào những người làm việc trong ngành báo chí, hay những người như tôi,hoạt động trong lĩnh vực giải trí, họ đang mang đến một góc nhìn khác chohọ sẽ giải quyết một việc gì đó như thế nào.Hoặc nếu chúng tôi có một sản phẩm mà chúng tôi đang cố gắng thuyết phục nhóm sản phẩm rằngcó lẽ chúng ta không nên làm điều này, điều này luôn hữu ích khi nói từ một người từng làm việc ởbáo chí, chúng ta có thực sự muốn chuyện này được đăng trên tờ The Times không?Có lẽ là không, phải không?Và đó là cách để tiếp cận những người ở tầng trệt,họ hiểu điều đó trông như thế nào.Tất cả những trải nghiệm mà bạn đã có từ khi bạn sinh ra cho đến bây giờ,họ đã từng là kinh nghiệm của bạn.Và bạn phải suy nghĩ về điều đó về việc chúng ta sẽ đi đâu với công nghệ.Khi chúng tôi phát triển cho nhiều đối tượng,kinh nghiệm của bạn có thể là kinh nghiệm của người khác.Và vì vậy nếu không có bạn trong phòng thì chúng tôi sẽ bỏ lỡ cơ hội đểtôi có thể nói là thực sự mang lại điều gì đó đẹp đẽ cho phương trình.Đó là lý do tại sao tôi khuyến khích mọi người hãy đến làm việc với chúng tôi về mặt công nghệ.Hãy tham gia vào STEM vì sự công bằng trong bảo mật sản phẩm,quyền riêng tư, bạn đặt tên cho nó, cho dù đó là công nghệ phần mềm,mọi thứ đều đòi hỏi một giọng nói khác.Và nó thực sự đòi hỏi giọng nói của bạn.

2.3. Playbooks, SIEM tools, and SOAR tools – Playbook, công cụ SIEM và công cụ SOAR

Playbooks, SIEM tools, and SOAR tools

Playbook, công cụ SIEM và công cụ SOAR

Previously, you learned that security teams encounter threats, risks, vulnerabilities, and incidents on a regular basis and that they follow playbooks to address security-related issues. In this reading, you will learn more about playbooks, including how they are used in security information and event management (SIEM) and security orchestration, automation, and response (SOAR).

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Trước đây, bạn đã biết rằng các nhóm bảo mật thường xuyên gặp phải các mối đe dọa, rủi ro, lỗ hổng và sự cố và họ tuân theo các hướng dẫn để giải quyết các vấn đề liên quan đến bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cẩm nang, bao gồm cách chúng được sử dụng trong thông tin bảo mật và quản lý sự kiện (SIEM) cũng như điều phối, tự động hóa và phản hồi bảo mật (SOAR).

Playbooks and SIEM tools

Playbook và công cụ SIEM

Playbooks are used by cybersecurity teams in the event of an incident. Playbooks help security teams respond to incidents by ensuring that a consistent list of actions are followed in a prescribed way, regardless of who is working on the case. Playbooks can be very detailed and may include flow charts and tables to clarify what actions to take and in which order. Playbooks are also used for recovery procedures in the event of a ransomware attack. Different types of security incidents have their own playbooks that detail who should take what action and when.

Playbook được các nhóm an ninh mạng sử dụng trong trường hợp xảy ra sự cố. Sách hướng dẫn giúp các nhóm bảo mật ứng phó với sự cố bằng cách đảm bảo rằng danh sách hành động nhất quán được tuân thủ theo cách quy định, bất kể ai đang xử lý vụ việc. Playbook có thể rất chi tiết và có thể bao gồm các biểu đồ và bảng để làm rõ những hành động cần thực hiện và theo thứ tự. Playbook cũng được sử dụng cho các quy trình khôi phục trong trường hợp bị tấn công bằng ransomware. Các loại sự cố bảo mật khác nhau có cẩm nang riêng nêu chi tiết ai sẽ thực hiện hành động nào và khi nào.

Playbooks are generally used alongside SIEM tools. If, for example, unusual user behavior is flagged by a SIEM tool, a playbook provides analysts with instructions about how to address the issue.

Playbook thường được sử dụng cùng với các công cụ SIEM. Ví dụ: nếu hành vi bất thường của người dùng bị công cụ SIEM gắn cờ, thì một cẩm nang sẽ cung cấp cho các nhà phân tích hướng dẫn về cách giải quyết vấn đề.

Playbooks and SOAR tools

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Playbook và công cụ SOAR

Playbooks are also used with SOAR tools. SOAR tools are similar to SIEM tools in that they are used for threat monitoring. SOAR is a piece of software used to automate repetitive tasks generated by tools such as a SIEM or managed detection and response (MDR). For example, if a user attempts to log into their computer too many times with the wrong password, a SOAR would automatically block their account to stop a possible intrusion. Then, analysts would refer to a playbook to take steps to resolve the issue.

Playbook cũng được sử dụng với các công cụ SOAR. Các công cụ SOAR tương tự như các công cụ SIEM ở chỗ chúng được sử dụng để theo dõi mối đe dọa. SOAR là một phần mềm được sử dụng để tự động hóa các tác vụ lặp đi lặp lại được tạo bởi các công cụ như SIEM hoặc phát hiện và phản hồi được quản lý (MDR). Ví dụ: nếu người dùng cố gắng đăng nhập vào máy tính của họ quá nhiều lần bằng mật khẩu sai, SOAR sẽ tự động chặn tài khoản của họ để ngăn chặn hành vi xâm nhập có thể xảy ra. Sau đó, các nhà phân tích sẽ tham khảo một cẩm nang để thực hiện các bước giải quyết vấn đề.

Key takeaways

Bài học chính

What is most important to know is that playbooks, also sometimes referred to as runbooks, provide detailed actions for security teams to take in the event of an incident. Knowing exactly who needs to do what and when can help reduce the impact of an incident and reduce the risk of damage to an organization’s critical assets.

Điều quan trọng nhất cần biết là cẩm nang, đôi khi còn được gọi là sổ tay hướng dẫn, cung cấp các hành động chi tiết để các nhóm bảo mật thực hiện trong trường hợp xảy ra sự cố. Biết chính xác ai cần làm gì và khi nào có thể giúp giảm tác động của sự cố và giảm nguy cơ thiệt hại đối với tài sản quan trọng của tổ chức.

2.4. Practice: Respond to a SIEM alert – Thực hành: Phản hồi cảnh báo SIEM

Incident	Playbook response

You're monitoring a SIEM dashboard and receive an alert about a suspicious file download. What's the first thing you should do?	Assess the alert by gathering more information
You determine that the suspicious file download alert is valid, so you follow the steps in your organization's playbook to contain and eliminate traces of the incident. What should you do next?	Restore affected systems
After you've taken all the necessary steps outlined in your organization's playbook to resolve the incident, what should you do?	Communicate the incident to stakeholders

Sự cố	Phản hồi của Playbook
Bạn đang theo dõi bảng điều khiển SIEM và nhận được cảnh báo về việc tải xuống tệp đáng ngờ. Điều đầu tiên bạn nên làm là gì?	Đánh giá cảnh báo bằng cách thu thập thêm thông tin
Bạn xác định rằng cảnh báo tải xuống tệp đáng ngờ là hợp lệ, vì vậy, bạn làm theo các bước trong sổ tay của tổ chức mình để ngăn chặn và loại bỏ dấu vết của vụ việc. Bạn nên làm gì tiếp theo?	Khôi phục hệ thống bị ảnh hưởng
Sau khi thực hiện tất cả các bước cần thiết được nêu trong cẩm nang của tổ chức để giải quyết sự cố, bạn nên làm gì?	Thông báo sự việc cho các bên liên quan

2.5. Test your knowledge: Use a playbook to respond to an incident – Kiểm tra kiến thức của bạn: Sử dụng cẩm nang để ứng phó với một sự cố

3. Review: Use playbooks to respond to incidents – Đánh giá: Sử dụng cẩm nang để ứng phó với sự cố

3.1. Wrap-up – Gói lại

Let's review what we covered in this section. We began by discussing the purpose of playbooks.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Hãy xem lại những gì chúng tôi đã đề cập trong phần này.Chúng tôi bắt đầu bằng việc thảo luận về mục đích của playbook.

Then, we examined the six phases of an incident response playbook, including an example of how a playbook might be used to address an incident.

Sau đó, chúng tôi xem xét sáu giai đoạn của cẩm nang ứng phó sự cố,bao gồm ví dụ về cách sử dụng cẩm nang để giải quyết một sự cố.

Playbooks are just one of the essential tools you'll use as a security analyst. They provide a structured, consistent approach to handling security incidents and can help you respond to security incidents quickly.

Playbook chỉ là một trong những công cụ thiết yếu mà bạn sẽ sử dụng với tư cách là nhà phân tích bảo mật.Họ cung cấp một cách tiếp cận có cấu trúc, nhất quán để xử lý các sự cố bảo mậtvà có thể giúp bạn ứng phó với các sự cố bảo mật một cách nhanh chóng.

Knowing how and when to use a playbook, will allow you to make informed decisions about how to respond to a security incident when it occurs and help to minimize the impact and damage it may cause your organization and the people it serves.

Biết cách thức và thời điểm sử dụng cẩm nang sẽ cho phép bạn đưa ra những quyết định sáng suốtquyết định về cách ứng phó với sự cố an ninh khi nó xảy ravà giúp giảm thiểu tác động vàthiệt hại mà nó có thể gây ra cho tổ chức của bạn và những người mà nó phục vụ.

Following the steps of the playbook and communicating appropriately with your team, will ensure your effectiveness as a security professional.

Làm theo các bước trong cẩm nang và giao tiếp phù hợp với nhóm của bạn,sẽ đảm bảo tính hiệu quả của bạn với tư cách là một chuyên gia bảo mật.

3.2. Glossary terms from module 4 – Thuật ngữ trong học phần 4

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Glossary terms from module 4

Thuật ngữ trong học phần 4

Terms and definitions from Course 2, Module 4

Các thuật ngữ và định nghĩa trong Khóa 2, Học phần 4

Incident response: An organization’s quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Phản ứng sự cố: Nỗ lực nhanh chóng của tổ chức nhằm xác định cuộc tấn công, ngăn chặn thiệt hại và khắc phục hậu quả của vi phạm an ninh

Playbook: A manual that provides details about any operational action

Playbook: Sách hướng dẫn cung cấp thông tin chi tiết về bất kỳ hành động vận hành nào

3.3. Module 4 challenge – Thử thách mô-đun 4

4. Congratulations on completing Course 2! – Chúc mừng bạn đã hoàn thành Khóa 2!

4.1. Course wrap-up – Tóm tắt khóa học

Congratulations on completing this course! Let's recap what we've covered so far. First, we reviewed CISSP's eight security domains and focused on threats, risks, and vulnerabilities to business operations.

Chúc mừng bạn đã hoàn thành khóa học này!Hãy tóm tắt lại những gì chúng ta đã trình bày cho đến nay.Đầu tiên, chúng tôi xem xét tám miền bảo mật của CISSP vàtập trung vào các mối đe dọa, rủi ro và điểm yếu đối với hoạt động kinh doanh.

Then, we explored security frameworks and controls, and how they're a starting point for creating policies and processes for security management. This included a discussion of the CIA triad, NIST frameworks, and security design principles, and how they benefit the security community as a whole. This was followed by a discussion about how frameworks, controls, and principles are related to security audits.

Sau đó, chúng tôi khám phá các khuôn khổ và biện pháp kiểm soát bảo mật cũng như cách chúng bắt đầuđiểm tạo ra các chính sách và quy trình để quản lý bảo mật.Điều này bao gồm một cuộc thảo luận về bộ ba CIA, các khuôn khổ của NIST vànguyên tắc thiết kế bảo mật và cách chúng mang lại lợi ích cho cộng đồng bảo mật nói chung.Tiếp theo đó là cuộc thảo luận về cách thức các khuôn khổ, biện pháp kiểm soát vànguyên tắc liên quan đến kiểm toán an ninh.

We also explored basic security tools, such as SIEM dashboards, and how they are used to protect business operations. And finally, we covered how to protect assets and data by using playbooks.

Chúng tôi cũng đã khám phá các công cụ bảo mật cơ bản, chẳng hạn như bảng thông tin SIEM vàchúng được sử dụng như thế nào để bảo vệ hoạt động kinh doanh.Và cuối cùng, chúng tôi đã đề cập đến cách bảo vệ tài sản và dữ liệu bằng cách sử dụng cẩm nang.

As a security analyst, you may be working on multiple tasks at once. Understanding the tools you have at your disposal, and how to use them, will elevate your knowledge in the field while helping you successfully accomplish your everyday tasks.

Là một nhà phân tích bảo mật, bạn có thể phải làm nhiều nhiệm vụ cùng một lúc.Hiểu các công cụ bạn có thể sử dụng vàcách sử dụng chúng, sẽ nâng cao kiến thức của bạn trong lĩnh vực này đồng thời giúp bạnhoàn thành tốt công việc hàng ngày của bạn.

Coming up next in the program, my colleague, Chris, will provide more details about topics covered in this course and introduce you to some new core security concepts. I've enjoyed sharing this journey with you.

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Phần tiếp theo của chương trình, đồng nghiệp của tôi, Chris,sẽ cung cấp thêm chi tiết về các chủ đề được đề cập trong khóa học này vàgiới thiệu cho bạn một số khái niệm bảo mật cốt lõi mới.Tôi rất vui khi được chia sẻ hành trình này với bạn.

4.2. Course 2 glossary – Thuật ngữ khóa 2

Course 2 glossary

Thuật ngữ khóa 2

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.

Chúng tôi đã đề cập đến rất nhiều thuật ngữ—một số thuật ngữ có thể bạn đã biết và một số thuật ngữ mới. Để giúp bạn dễ dàng nhớ nghĩa của một từ, chúng tôi đã tạo ra bảng chú giải các thuật ngữ và định nghĩa này.

To use the glossary for this course item, click the link below and select "Use Template."

Link to glossary: Course 2 glossary

Để sử dụng bảng thuật ngữ cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn "Sử dụng mẫu".

Liên kết đến bảng thuật ngữ:Thuật ngữ khóa 2

4.3. Your Course 2 learning journey – Hành trình học tập Khóa 2 của bạn

4.4. Get started on the next course – Bắt đầu khóa học tiếp theo

Get started on the next course

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

Bắt đầu khóa học tiếp theo

Congratulations on completing Course 2 of the Google Cybersecurity Certificate: **Play It Safe: Manage Security Risks**! In this part of the program, you learned about the focus of the eight Certified Information Systems Security Professional (CISSP) security domains. You also learned more about threats, risks, and vulnerabilities, as well as common security controls and frameworks. Additionally, you explored how to use the National Institute of Standards and Technology Risk Management Framework (NIST RMF), security information and event management (SIEM) technology, and playbooks to identify and help prevent security issues that can harm organizations and the people they serve.

Chúc mừng bạn đã hoàn thành Khóa 2 của Chứng chỉ an ninh mạng của Google: **Chơi an toàn: Quản lý rủi ro bảo mật** ! Trong phần này của chương trình, bạn đã tìm hiểu về trọng tâm của tám miền bảo mật Chuyên gia bảo mật hệ thống thông tin được chứng nhận (CISSP). Bạn cũng đã tìm hiểu thêm về các mối đe dọa, rủi ro và lỗ hổng bảo mật cũng như các khuôn khổ và kiểm soát bảo mật phổ biến. Ngoài ra, bạn đã khám phá cách sử dụng Khung quản lý rủi ro công nghệ và tiêu chuẩn quốc gia (NIST RMF), công nghệ quản lý sự kiện và thông tin bảo mật (SIEM) cũng như sách hướng dẫn để xác định và giúp ngăn chặn các vấn đề bảo mật có thể gây hại cho tổ chức và những người mà họ phục vụ. .

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. *(This is the course you just completed. Well done!)*

Module 4: Use playbooks to respond to incidents
Phần 4: Sử dụng playbook để ứng phó với sự cố

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.

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.

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 vai trò và trách nhiệm an ninh mạng cấp cơ bản.

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 cũng như khám phá các công cụ an ninh mạng phổ biến. *(Đây là khóa học bạn vừa hoàn thành. Làm tốt lắm!)*

3. **Kết nối và bảo vệ: Mạng và bảo mật mạng** - Hiểu biết về các lỗ hổng cấp độ mạng và cách bảo mật mạng.

4. **Công cụ giao dịch: 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 bảo mật** - 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. **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 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 nó vào hoạt động: Chuẩn bị cho các công việc về an ninh mạng** — Tìm hiểu về phân loại sự cố, leo thang 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.

Now that you have completed this course, you're ready to move on to the next course: **Connect and Protect: Networks and Network Security**.

Bây giờ bạn đã hoàn thành khóa học này, bạn đã sẵn sàng chuyển sang khóa học tiếp theo:**Kết nối và bảo vệ: Mạng và an ninh mạng**.

Keep up the great work!

Kịp các công việc tuyệt vời!