**Module 1: Introduction to detection and incident response - giới thiệu về phát hiện và ứng phó sự cố**

|  |
| --- |
| Detection and incident response are an important part of a cybersecurity analyst’s work. You'll explore how cybersecurity professionals verify and respond to malicious threats and become familiar with the steps involved in incident response. |

Phát hiện và ứng phó sự cố là một phần quan trọng trong công việc của một nhà phân tích an ninh mạng. Bạn sẽ khám phá cách các chuyên gia an ninh mạng xác minh và ứng phó với các mối đe dọa độc hại và làm quen với các bước liên quan đến ứng phó sự cố.

|  |
| --- |
| **Learning Objectives**   * Explain the lifecycle of an incident. * Determine the roles and responsibilities of incident response teams. * Describe the tools used in the documentation, detection, and management of incidents. |

**Mục tiêu học tập**

* Giải thích vòng đời của một sự cố.
* Xác định vai trò và trách nhiệm của các nhóm ứng phó sự cố.
* Mô tả các công cụ được sử dụng trong việc ghi chép, phát hiện và quản lý sự cố.

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

***1.1. Introduction to Course 6 - Giới thiệu về Khóa học 6***

|  |
| --- |
| Security attacks are on the rise, and new vulnerabilities are exploited and discovered every week. No matter how prepared an organization may be in the event of a security attack, at some point something goes wrong. Whether it's a data breach, ransomware, or a simple mistake made by an employee, incidents happen. And it's up to security professionals like you to effectively respond to security incidents. |

Các cuộc tấn công an ninh đang gia tăng vàlỗ hổng mới đang được khai thácvà được phát hiện mỗi tuần.Bất kể một tổ chức được chuẩn bị như thế nàocó thể xảy ra trong trường hợp xảy ra tấn công an ninh,đến một lúc nào đó có điều gì đó không ổn.Cho dù đó là vi phạm dữ liệu, phần mềm tống tiền,hoặc một lỗi đơn giản do một nhân viên mắc phải,sự cố xảy ra. Và nó phụ thuộc vàocác chuyên gia an ninh như bạnứng phó hiệu quả với các sự cố an ninh.

|  |
| --- |
| Hello and welcome to the course! I'm Dave, and I'm a Principal Security Strategist for Google Cloud. I have 20 years of experience as a security practitioner and leader. Over the past eight years, I've worked at industry-leading security vendors like Fortinet, Splunk, and Google, where I developed a specialty in security analytics. I have a passion for helping analysts develop the skills necessary to succeed in their careers. |

Xin chào và chào mừng đến với khóa học!Tôi là Dave và tôi là Hiệu trưởngChuyên gia chiến lược bảo mật cho Google Cloud.Tôi có 20 năm kinh nghiệmvới tư cách là người thực hành và lãnh đạo về an ninh.Trong tám năm qua,Tôi đã làm việc tại một công ty hàng đầu trong ngànhcác nhà cung cấp bảo mật như Fortinet,Splunk và Google, nơi tôi phát triểnchuyên ngành phân tích bảo mật.Tôi có niềm đam mê giúp các nhà phân tích phát triểnnhững kỹ năng cần thiết để thành công trong sự nghiệp.

|  |
| --- |
| I'm so happy you're here. You've done a great job so far. You've learned a lot about security concepts, best practices, and types of security attacks. Now in this course, we'll focus on incident detection, analysis, and response. You'll have the opportunity to apply your learning using tools such as tcpdump, Wireshark, Suricata, Splunk, and Chronicle. By the end of this course, you'll have an in-depth understanding of incident response. |

Tôi rất vui vì bạn ở đây.Cho đến giờ bạn đã làm rất tốt.Bạn đã học được rất nhiều về các khái niệm bảo mật,các biện pháp thực hành tốt nhất và các loại tấn công bảo mật.Bây giờ trong khóa học này, chúng ta sẽ tập trung vào phát hiện sự cố,phân tích và phản hồi.Bạn sẽ có cơ hội để áp dụngviệc học của bạn bằng cách sử dụng các công cụ như tcpdump,Wireshark, Suricata, Splunk và Chronicle.Đến cuối khóa học này,bạn sẽ có sự hiểu biết sâu sắccủa phản ứng sự cố.

|  |
| --- |
| First, you'll learn about the incident response lifecycle and how incident response teams work together. You'll also learn about the types of tools used in detection and response, including documentation. You'll also be given your own incident handler's journal that you'll use during your investigations. |

Đầu tiên, bạn sẽ tìm hiểu vềvòng đời phản ứng sự cố và cách thứccác đội ứng phó sự cố làm việc cùng nhau.Bạn cũng sẽ tìm hiểu về các loại công cụ được sử dụng trongphát hiện và phản hồi, bao gồm cả ghi chép.Bạn cũng sẽ được cung cấp nhật ký xử lý sự cố của riêng bạnmà bạn sẽ sử dụng trong quá trình điều tra của mình.

|  |
| --- |
| Next, you'll apply your knowledge and networking in Linux to monitor and analyze network traffic using packet sniffers like Wireshark and tcpdump to capture and analyze packets for potential indicators of security incidents. |

Tiếp theo, bạn sẽ áp dụng kiến ​​thức của mình vàmạng lưới trong Linux để giám sát và phân tíchlưu lượng mạng sử dụng packet sniffergiống như Wireshark và tcpdumpđể nắm bắt và phân tích các gói tincác chỉ số tiềm ẩn của sự cố an ninh.

|  |
| --- |
| Then, you'll become familiar with the common processes and procedures used during incident detection and response. You'll learn how to use investigative tools to analyze and verify incidents and produce documentation. |

Sau đó, bạn sẽ trở nên quen thuộc với các quy trình chung vàcác quy trình được sử dụng trong quá trình phát hiện và ứng phó sự cố.Bạn sẽ học cách sử dụng các công cụ điều tra đểphân tích và xác minh sự cố và lập tài liệu.

|  |
| --- |
| Finally, you'll learn how to interpret logs and alerts. You'll learn how detection tools produce logs and how these logs are analyzed in security information and event management tools. |

Cuối cùng, bạn sẽ học cách diễn giải nhật ký và cảnh báo.Bạn sẽ học cách sử dụng các công cụ phát hiệntạo ra các bản ghi và cách các bản ghi nàyđược phân tích trong an ninhcông cụ quản lý thông tin và sự kiện.

|  |
| --- |
| Ready to begin? Let's get started! |

Bạn đã sẵn sàng chưa? Hãy bắt đầu thôi!

***1.2.Course 6 overview - Tổng quan về khóa học 6***

|  |
| --- |
| **Course 6 overview** |

**Tổng quan về khóa học 6**



|  |
| --- |
| Hello, and welcome to **Sound the Alarm: Detection and Response**, the sixth course in the Google Cybersecurity Certificate. You’re on an exciting journey! |

Xin chào và chào mừng bạn đến với **Sound the Alarm: Detection and Response** , khóa học thứ sáu trong Chứng chỉ An ninh mạng của Google. Bạn đang trên một hành trình thú vị!

|  |
| --- |
| By the end of the course, you will have hands-on practice using resources like network protocol analyzers, intrusion detection systems (IDS), and security information event management (SIEM) tools to capture network packets and analyze log data. |

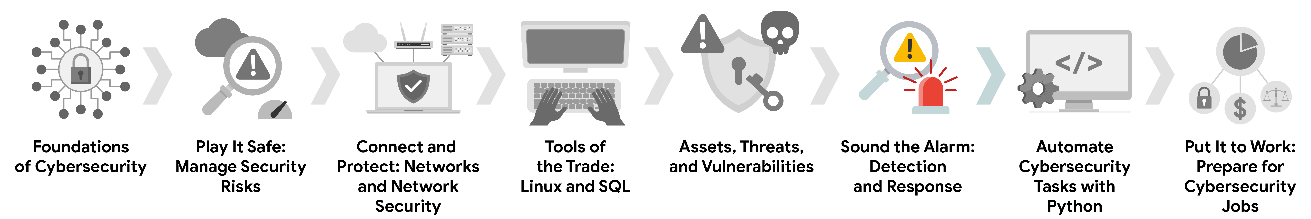
Đến cuối khóa học, bạn sẽ có cơ hội thực hành sử dụng các tài nguyên như trình phân tích giao thức mạng, hệ thống phát hiện xâm nhập (IDS) và công cụ quản lý sự kiện thông tin bảo mật (SIEM) để thu thập các gói tin mạng và phân tích dữ liệu nhật ký.

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

**Tiến độ chương trình cấp chứng chỉ**

|  |
| --- |
| The Google Cybersecurity Certificate program has eight courses. **Sound the Alarm: Detection and Response** is the sixth course. |

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. **Sound the Alarm: Detection and Response** là khóa học thứ sáu.



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

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

|  |
| --- |
| **Course 6 content** |

**Nội dung khóa học 6**

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

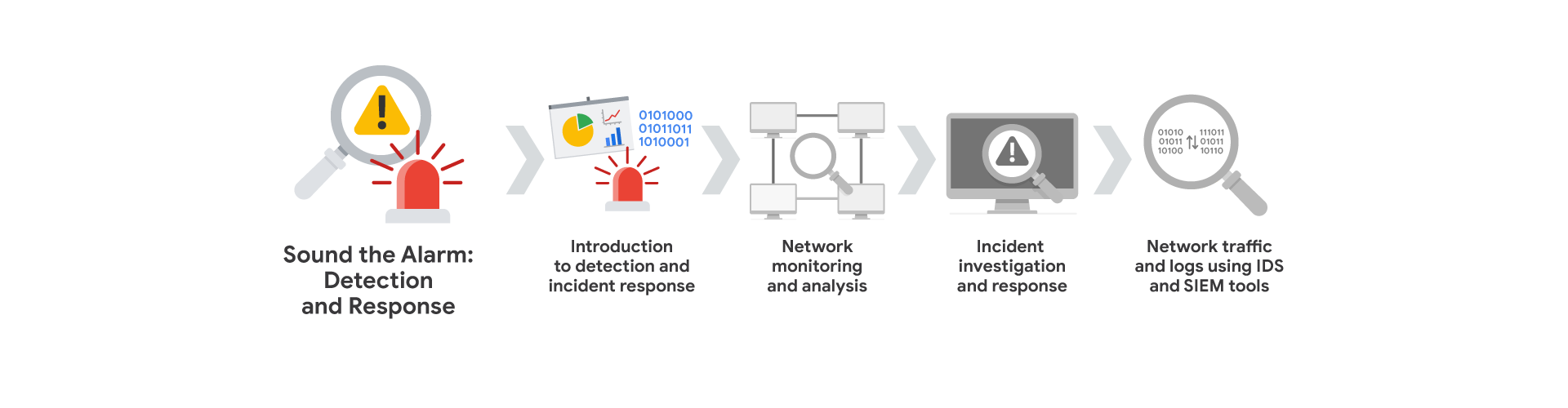
Mỗi khóa học của chương trình cấp chứng chỉ này được chia thành các mô-đun. Bạn có thể hoàn thành các khóa học theo tốc độ của riêng mình, nhưng các phân tích mô-đun được thiết kế để giúp bạn hoàn thành toàn bộ Chứng chỉ An ninh mạng của Google trong khoảng sáu tháng.

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

Sắp tới sẽ có gì? Sau đây là bản tóm tắt nhanh về các kỹ năng bạn sẽ học được trong từng mô-đun của khóa học này.

|  |
| --- |
| **Module 1: Introduction to detection and incident response** |

**Mô-đun 1: Giới thiệu về phát hiện và ứng phó sự cố**

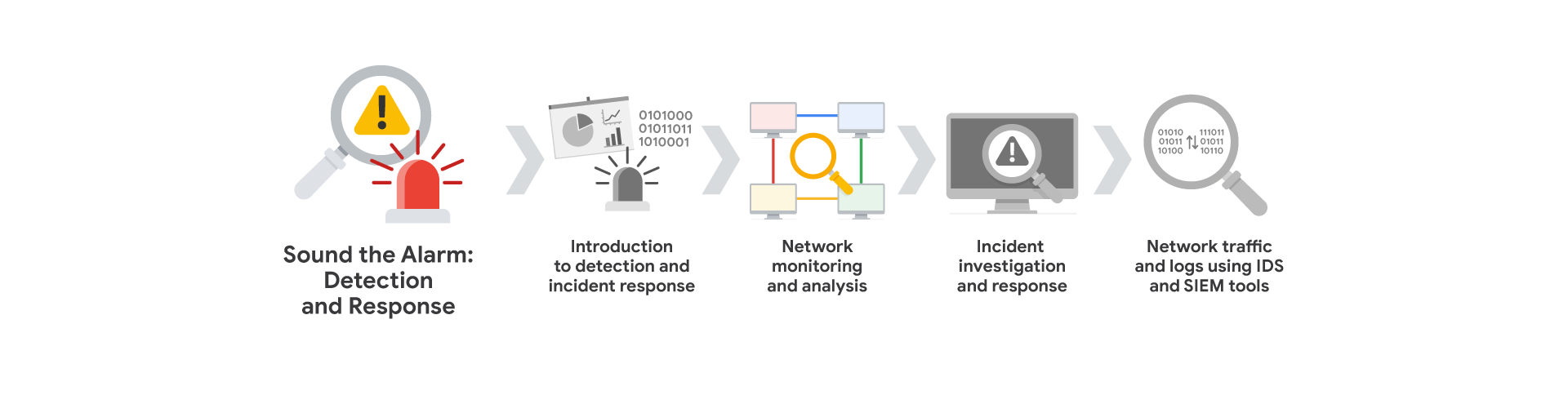


|  |
| --- |
| You will be introduced to detection and incident response, and the steps involved in the incident response process. You'll also explore how cybersecurity professionals verify and respond to malicious threats. |

Bạn sẽ được giới thiệu về phát hiện và ứng phó sự cố, cũng như các bước liên quan đến quy trình ứng phó sự cố. Bạn cũng sẽ tìm hiểu cách các chuyên gia an ninh mạng xác minh và ứng phó với các mối đe dọa độc hại.

|  |
| --- |
| **Module 2: Network monitoring and analysis** |

**Mô-đun 2: Giám sát và phân tích mạng**

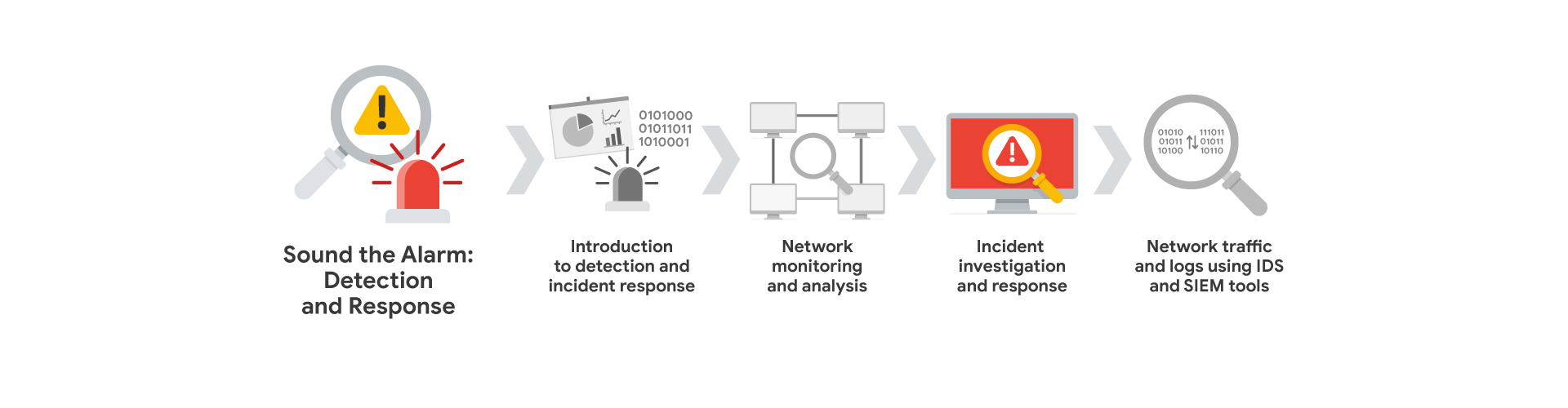


|  |
| --- |
| You will learn the importance of network monitoring, and how to understand network traffic. Then, you'll explore how to use network protocol analyzer tools, commonly referred to as packet sniffers. In particular, you'll sniff the network and analyze packets for malicious threats. You'll also craft filtering commands to analyze the contents of captured packets. |

Bạn sẽ học được tầm quan trọng của việc giám sát mạng và cách hiểu lưu lượng mạng. Sau đó, bạn sẽ khám phá cách sử dụng các công cụ phân tích giao thức mạng, thường được gọi là packet sniffer. Cụ thể, bạn sẽ sniff mạng và phân tích các gói tin để tìm ra các mối đe dọa độc hại. Bạn cũng sẽ tạo các lệnh lọc để phân tích nội dung của các gói tin đã thu thập được.

|  |
| --- |
| **Module 3: Incident investigation and response** |

**Mô-đun 3: Điều tra và ứng phó sự cố**

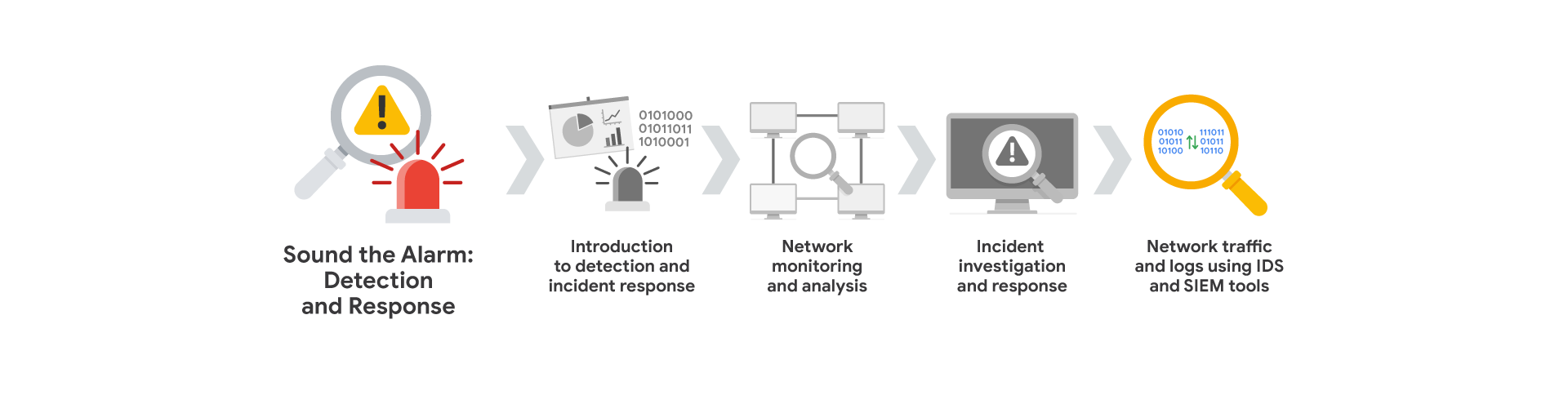


|  |
| --- |
| You will learn about the various processes and procedures in the stages of incident detection, investigation, analysis, and response. Then, you'll analyze the details of suspicious file hashes using investigative tools. You'll also learn about the importance of documentation, evidence collection, the triage process, and more. |

Bạn sẽ tìm hiểu về các quy trình và thủ tục khác nhau trong các giai đoạn phát hiện, điều tra, phân tích và phản hồi sự cố. Sau đó, bạn sẽ phân tích chi tiết các tệp băm đáng ngờ bằng các công cụ điều tra. Bạn cũng sẽ tìm hiểu về tầm quan trọng của tài liệu, thu thập bằng chứng, quy trình phân loại và nhiều nội dung khác.

|  |
| --- |
| **Module 4: Network traffic and logs using IDS and SIEM tools** |

**Mô-đun 4: Lưu lượng mạng và nhật ký sử dụng công cụ IDS và SIEM**



|  |
| --- |
| You will explore logs and their role in IDS and SIEM tools. You'll learn how these systems work to help cybersecurity teams monitor systems and detect malicious activity. You’ll also be introduced to some IDS and SIEM products, and practice using tools to perform queries. |

Bạn sẽ khám phá nhật ký và vai trò của chúng trong các công cụ IDS và SIEM. Bạn sẽ tìm hiểu cách các hệ thống này hoạt động để giúp các nhóm an ninh mạng giám sát hệ thống và phát hiện hoạt động độc hại. Bạn cũng sẽ được giới thiệu về một số sản phẩm IDS và SIEM và thực hành sử dụng các công cụ để thực hiện truy vấn.

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

**Những gì mong đợi**

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

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

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

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

**Mẹo để thành công**

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

* Bạn nên xem qua các mục trong mỗi bài học theo thứ tự xuất hiện vì thông tin và khái niệm mới sẽ dựa trên kiến ​​thức trước đó.
* Tham gia mọi cơ hội học tập để có được nhiều kiến ​​thức và kinh nghiệm nhất có thể.
* Nếu có điều gì khó hiểu, đừng ngần ngại phát lại video, xem lại bài đọc hoặc thực hiện lại hoạt động tự đánh giá.
* Sử dụng các tài nguyên bổ sung được tham chiếu trong khóa học này. Chúng được thiết kế để hỗ trợ việc học của bạn. Bạn có thể tìm thấy tất cả các tài nguyên này trong[Tài nguyên](https://www.coursera.org/learn/detection-and-response/resources/OQmsa)tab.
* Khi bạn gặp những liên kết hữu ích trong khóa học này, hãy đánh dấu trang để có thể tham khảo thông tin sau này để nghiên cứu hoặc xem lại.
* Hiểu và làm theo[Quy tắc ứng xử của Coursera](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?)để đảm bảo rằng cộng đồng học tập vẫn là nơi chào đón, thân thiện và hỗ trợ cho tất cả thành viên.

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

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

**Tài nguyên và mẹo 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. |

Với tư cách 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 biện pháp thực hành tốt nhất để bạn có trải nghiệm học tập tốt trên Coursera.

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

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

|  |
| --- |
| To receive your official Google Cybersecurity Certificate, you must:   * Pass all graded assignments in all 8 courses of the certificate program. Each graded assignment is part of a cumulative graded score for the course, and the passing grade for each course is 80%.   AND **one**of the following:   * Pay the [course certificate fee](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US), * Be approved for [Coursera Financial Aid](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US), **or** * Complete the certificate through an educational institution, employer, or agency that's sponsoring your participation. |

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

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

VÀ  **một** trong những điều sau đây:

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

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

**Thói quen lành mạnh để 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. * **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity. * **Chat (responsibly) with other learners:** If you have a question, chances are, you’re not alone. Use the [discussion forums](https://www.coursera.org/learn/detection-and-response/discussions) to ask for help from other learners taking this program. You can also visit Coursera’s [Global Online Community](https://coursera.community/). Other important things to know while learning with others can be found in the [Coursera Honor Code](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code) and [Code of Conduct](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct). * **Update your profile:** Consider [updating your profile](https://www.coursera.org/account/profile) on Coursera to include your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better. |

Sau đây là danh sách các biện pháp tốt nhất sẽ giúp bạn hoàn thành các khóa học trong chương trình đúng thời hạn:

* **Lên kế hoạch thời gian:** Đặt thời gian học tập thường xuyên và tuân thủ theo mỗi tuần có thể giúp bạn biến việc học thành một phần thói quen của mình. Sử dụng lịch hoặc thời gian biểu để lập 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 các bài đọc và hoàn thành các hoạt động.
* **Làm việc theo tốc độ của riêng bạn:** Mỗi người học khác nhau, vì vậy chương trình này được thiết kế để cho phép bạn làm việc theo tốc độ của riêng mình. Mặc dù thời hạn cá nhân của bạn bắt đầu khi bạn đăng ký, hãy thoải mái thực hiện chương trình theo tốc độ phù hợp nhất với bạn. Không có hình phạt nào cho các bài tập nộp trễ; để kiếm được chứng chỉ, tất cả những gì bạn phải làm là hoàn thành tất cả các bài tập. Bạn có thể gia hạn thời hạn của mình bất kỳ lúc nào bằng cách vào **Tổng quan** trong bảng điều hướng và chọn Chuyển **đổi phiên** . Nếu bạn đã bỏ lỡ các thời hạn trước đó, hãy chọn **Đặt lại thời hạn của tôi** thay thế.
* **Hãy tò mò:** Nếu bạn tìm thấy một ý tưởng khiến bạn hứng thú, hãy hành động! Đặt câu hỏi, tìm kiếm thêm thông tin chi tiết trực tuyến, khám phá các liên kết mà bạn quan tâm và ghi chú lại những khám phá của bạn. Các bước bạn thực hiện để hỗ trợ việc học của mình trong suốt quá trình sẽ nâng cao kiến ​​thức của bạn, tạo ra nhiều cơ hội hơn trong lĩnh vực tăng trưởng cao này và giúp bạn đủ điều kiện để xin việc.
* **Ghi chú:** Ghi chú sẽ giúp bạn nhớ thông tin quan trọng trong tương lai, đặc biệt là khi bạn chuẩn bị bước vào một lĩnh vực công việc mới. Ngoài ra, ghi chú là một cách hiệu quả để tạo kết nối giữa các chủ đề và hiểu rõ hơn về các chủ đề đó.
* **Xem lại các ví dụ:** Các ví dụ 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 các ví dụ để bạn xác thực công việc của mình hoặc kiểm tra lỗi. Mặc dù thường có nhiều cách để hoàn thành một bài tập, các ví dụ cung cấp hướng dẫn và cảm hứng về cách hoàn thành hoạt động.
* **Trò chuyện (có trách nhiệm) với những người học khác:** Nếu bạn có thắc mắc, rất có thể bạn không phải là người duy nhất. Sử dụng[diễn đàn thảo luận](https://www.coursera.org/learn/detection-and-response/discussions)để yêu cầu sự giúp đỡ từ những người học khác tham gia chương trình này. Bạn cũng có thể truy cập Coursera[Cộng đồng trực tuyến toàn cầu](https://coursera.community/). Những điều quan trọng khác cần biết khi học với người khác có thể được tìm thấy trong[Quy tắc danh dự của Coursera](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code)Và[Quy tắc ứng xử](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct).
* **Cập nhật hồ sơ của bạn:** Hãy cân nhắc[đang cập nhật hồ sơ của bạn](https://www.coursera.org/account/profile)trên Coursera để bao gồm ảnh, mục tiêu nghề nghiệp và nhiều thông tin khác. Khi những người học khác tìm thấy bạn trong diễn đàn thảo luận, họ có thể nhấp vào tên của bạn để truy cập hồ sơ của bạn và tìm hiểu thêm 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](https://support.microsoft.com/en-us/word): Microsoft Support page for Word * [Google Docs](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Help Center page for Google Docs * [Microsoft Excel: Help and learning](https://support.microsoft.com/en-us/excel): Microsoft Support page for Excel * [Google Sheets](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Help Center page for Google Sheets * [Microsoft PowerPoint: Help and learning](https://support.microsoft.com/en-us/powerpoint): Microsoft Support page for PowerPoint * [How to use Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Help Center page for Google Slides * [Common problems with labs](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Troubleshooting help for Qwiklabs activities |

Để hoàn thành một số hoạt động nhất định trong chương trình, bạn sẽ cần sử dụng tài liệu kỹ thuật số, bảng tính, bài thuyết trình 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](https://support.microsoft.com/en-us/word): Trang hỗ trợ của Microsoft dành cho Word
* [Tài liệu Google](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp cho Google Docs
* [Microsoft Excel: Trợ giúp và học tập](https://support.microsoft.com/en-us/excel): Trang hỗ trợ của Microsoft dành cho Excel
* [Trang tính Google](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp cho Google Trang tính
* [Microsoft PowerPoint: Trợ giúp và học tập](https://support.microsoft.com/en-us/powerpoint): Trang hỗ trợ của Microsoft dành cho PowerPoint
* [Cách sử dụng Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Trang Trung tâm trợ giúp cho Google Slides
* [Các vấn đề thường gặp với phòng thí nghiệm](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Trợ giúp khắc phục sự cố cho các hoạt động Qwiklabs

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

**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.   You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course’s [Resources](https://www.coursera.org/learn/detection-and-response/supplement/whU5f/course-6-glossary) section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.   * [Cybersecurity Certificate glossary](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?usp=sharing&resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ) |

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

* **Thuật ngữ mô-đun** : Vào cuối nội dung của mỗi mô-đun, bạn có thể xem lại thuật ngữ mô-đun đó. Thuật ngữ của mỗi mô-đun được xây dựng dựa trên các thuật ngữ từ các mô-đun trước đó trong khóa học đó. Thuật ngữ mô-đun không thể tải xuống; tuy nhiên, tất cả các thuật ngữ và định nghĩa đều có trong thuật ngữ khóa học và chứng chỉ, có thể tải xuống.
* **Thuật ngữ khóa học** : Vào cuối mỗi khóa học, bạn có thể truy cập và tải xuống thuật ngữ bao gồm tất cả các thuật ngữ trong khóa học đó.
* **Thuật ngữ chứng chỉ** : Thuật ngữ 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 các thuật ngữ chứng chỉ và lưu chúng trên máy tính của bạn. Bạn luôn có thể tìm thấy các thuật ngữ khóa học và chứng chỉ thông qua khóa học[Tài nguyên](https://www.coursera.org/learn/detection-and-response/supplement/whU5f/course-6-glossary)phần. Để truy cập vào **thuật ngữ Chứng chỉ an ninh mạng** , hãy nhấp vào liên kết bên dưới và chọn *Sử dụng mẫu* .

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

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

**Phản hồi khóa học**

|  |
| --- |
| Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.   * Click **thumbs-up** for materials that are helpful. * Click **thumbs-down** for materials that are not 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](https://learner.coursera.help/hc/en-us). |

Việc cung cấp phản hồi về video, bài đọc và các tài liệu khác rất dễ dàng. Khi mở tài nguyên trong trình duyệt, bạn có thể tìm thấy các biểu tượng ngón tay cái hướng lên và ngón tay cái hướng xuống.

* Nhấp vào **nút thích** để xem tài liệu hữu ích.
* Nhấp vào **nút không thích** đối với những tài liệu không hữu ích.

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

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

***1.4. Dave: Grow your cybersecurity career with mentors - Dave: Phát triển sự nghiệp an ninh mạng của bạn với những người cố vấn***

|  |
| --- |
| My name is Dave. I'm a Principal Security Strategist with Google Cloud. My job is to work directly with security practitioners to help them protect their organizations. What I love about my job is the variety. One day I might be troubleshooting a technical problem for a customer. The next day I might be coding up a solution to a certain problem. Every day is something new and I never get bored. I was a kid growing up in the Midwest. I went off to college to study engineering, I thought. But I realized that I wasn't really into engineering, but I loved computer science, which I didn't even know was an option. I ended up working as a help desk person early in college, but then I got a job as a system administrator. I found myself working at a startup in the payments industry. My job switched from being in general IT person to being a cybersecurity person. I spent seven years in that job and did everything from one man security shop to running a medium-sized security organization toward the end. Then I switched over to the other side of the table and started working for security vendors. That gave me the opportunity to see how literally hundreds of other organizations run their security programs, and that was really eye-opening. Cybersecurity is interesting because you can really bring your entire life experience to cybersecurity. What you're doing is trying to protect an organization, not necessarily like from an accident, but you're protecting an organization from a human being on the other side who's trying to do your organization harm. One thing that's becoming clear is that people from diverse backgrounds and diverse experiences typically bring a great deal of improvement to how we deal with that. I highly recommend getting involved with security organizations. It's a place to meet other people who can help you along in your career. I think people are surprised to learn just how much help is available in our industry. There are lots of folks who are more senior and more accomplished who are willing to be mentors. I think the best thing that you can do as someone who's looking for a mentor is to be assertive. Have a plan, have a few things in mind that you want to work on, and then reach out to someone who maybe works in that particular area of cybersecurity and ask them for help. I think you'll be surprised at just how helpful folks will be. |

Tên tôi là Dave.Tôi là Chuyên gia chiến lược bảo mật chính của Google Cloud.Công việc của tôi là làm việc trực tiếp vớicác chuyên gia an ninh giúp đỡhọ bảo vệ tổ chức của họ.Điều tôi thích ở công việc của mình là sự đa dạng.Một ngày nào đó tôi có thể khắc phục sự cốmột vấn đề kỹ thuật đối với khách hàng.Ngày hôm sau tôi có thể đang viết mãmột giải pháp cho một vấn đề nào đó.Mỗi ngày đều có điều mới mẻ và tôi không bao giờ cảm thấy buồn chán.Tôi là một đứa trẻ lớn lên ở vùng Trung Tây.Tôi nghĩ rằng mình đã đi học đại học để học ngành kỹ thuật.Nhưng tôi nhận ra rằng tôi không thực sự thích kỹ thuật,nhưng tôi yêu thích khoa học máy tính,mà tôi thậm chí còn không biết là có lựa chọn này.Cuối cùng tôi đã làm việc nhưmột người làm việc ở bộ phận trợ giúp vào đầu thời đại học,nhưng sau đó tôi đã có được công việc quản trị viên hệ thống.Tôi thấy mình đang làm việc tạimột công ty khởi nghiệp trong ngành thanh toán.Công việc của tôi đã chuyển từ nói chungTừ người làm CNTT trở thành người làm an ninh mạng.Tôi đã dành bảy năm cho công việc đó và đã làm mọi thứtừ một cửa hàng an ninh một người đàn ông đếnđiều hành một hệ thống an ninh vừatổ chức hướng tới mục tiêu cuối cùng.Sau đó tôi chuyển sang phía bên kia của bànvà bắt đầu làm việc cho các nhà cung cấp dịch vụ bảo mật.Điều đó đã cho tôi cơ hội đểxem cách thực sự hàng trămcủa các tổ chức khác chạy chương trình bảo mật của họ,và điều đó thực sự mở mang tầm mắt.An ninh mạng rất thú vị vì bạn thực sự có thểmang toàn bộ kinh nghiệm sống của bạn vào an ninh mạng.Những gì bạn đang làm là cố gắng bảo vệ một tổ chức,không nhất thiết giống như một tai nạn,nhưng bạn đang bảo vệ một tổ chức khỏi con ngườiđang ở phía bên kia là aicố gắng gây hại cho tổ chức của bạn.Một điều đang trở nên rõ rànglà những người có xuất thân đa dạng vànhững trải nghiệm đa dạng thường mang lạicải thiện đáng kể cách chúng ta giải quyết vấn đề đó.Tôi thực sự khuyên bạn nên lấycó liên quan đến các tổ chức an ninh.Đó là nơi để gặp gỡ những người kháccó thể giúp ích cho sự nghiệp của bạn.Tôi nghĩ mọi người ngạc nhiên khi biếtcó bao nhiêu sự trợ giúp có sẵn trong ngành của chúng tôi.Có rất nhiều người cao tuổi hơn vànhững người thành đạt hơn và sẵn sàng làm người cố vấn.Tôi nghĩ điều tốt nhất mà bạn có thể làm với tư cách là một ngườitìm kiếm một người cố vấn là phải quyết đoán.Có một kế hoạch, cómột vài điều trong đầu mà bạn muốn thực hiện,và sau đó liên hệ với một người nào đó có thể làm việc trongkhu vực cụ thể đóan ninh mạng và yêu cầu họ giúp đỡ.Tôi nghĩ bạn sẽ ngạc nhiênmọi người sẽ hữu ích đến mức nào.

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

**2. The incident response lifecycle – Vòng đời phản ứng sự cố**

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

|  |
| --- |
| Welcome. In my role as Principal Security Strategist, I've seen how the incident response operations that you'll learn about in this course are implemented in an organization. One of the things I find so exciting about detecting and responding to incidents is the challenge of using data to understand what an adversary has done in my organization's environment. No two investigations are ever the same, but there are patterns of behavior that you can learn to spot as you hone your analytic skills. |

Chào mừng. Với vai trò là Nhà chiến lược an ninh chính,Tôi đã thấy cách thức hoạt động ứng phó sự cố mà bạn sẽ tìm hiểu trong phần nàykhóa học được triển khai trong một tổ chức.Một trong những điều tôi thấy rất thú vị khi phát hiện vàứng phó với các sự cố là thách thức của việc sử dụng dữ liệu để hiểu những gìmột kẻ thù đã làm trong môi trường tổ chức của tôi.Không có hai cuộc điều tra nào giống hệt nhau, nhưng có những mô hình hành vimà bạn có thể học cách phát hiện khi bạn rèn luyện kỹ năng phân tích của mình.

|  |
| --- |
| Previously, you established a solid understanding of asset security, threats, and vulnerabilities. You explored the NIST Cyber Security Framework, or CSF, as a methodology for risk management. You learned about mitigating organizational risk through classifying and securing assets. And you also explored security and privacy controls to safeguard data. You used tools like MITRE and CVE to investigate common vulnerabilities and used techniques like threat modeling to develop an attacker's mindset. |

Trước đó, bạn đã thiết lập được sự hiểu biết vững chắc về an ninh tài sản,các mối đe dọa và lỗ hổng.Bạn đã khám phá Khung an ninh mạng NIST, hay CSF, như một phương pháp luận choquản lý rủi ro.Bạn đã học về việc giảm thiểu rủi ro tổ chức thông qua việc phân loạivà bảo đảm tài sản.Và bạn cũng đã khám phá các biện pháp kiểm soát bảo mật và quyền riêng tư để bảo vệ dữ liệu.Bạn đã sử dụng các công cụ như MITRE và CVE để điều tra các lỗ hổng phổ biến vàsử dụng các kỹ thuật như mô hình hóa mối đe dọa để phát triển tư duy của kẻ tấn công.

|  |
| --- |
| Next, we'll revisit the NIST CSF with a focus on the incident response lifecycle. You'll be given your own incident handler's journal, which you'll use throughout the rest of the course. You'll also be introduced to incident response teams, including the different team roles and how they organize to respond to incidents. And finally, you'll learn about the different types of documentation, detection, and management tools you'll use as a security professional working in incident response. Later on, you'll have an opportunity to use these tools. |

Tiếp theo, chúng ta sẽ xem lại NIST CSF và tập trung vào vòng đời ứng phó sự cố.Bạn sẽ được cấp nhật ký xử lý sự cố của riêng mình, nhật ký mà bạn sẽ sử dụng trong suốt quá trìnhphần còn lại của khóa học.Bạn cũng sẽ được giới thiệu với các nhóm ứng phó sự cố, bao gồmcác vai trò khác nhau của nhóm và cách họ tổ chức để ứng phó với các sự cố.Và cuối cùng, bạn sẽ tìm hiểu về các loại tài liệu khác nhau,phát hiện vàcác công cụ quản lý bạn sẽ sử dụng với tư cách là chuyên gia bảo mật làm việc trong lĩnh vực ứng phó sự cố.Sau này, bạn sẽ có cơ hội sử dụng những công cụ này.

|  |
| --- |
| Are you ready to begin your journey in detection and response? Let's begin! |

Bạn đã sẵn sàng bắt đầu hành trình phát hiện và ứng phó chưa?Chúng ta bắt đầu thôi!

***2.2. Introduction to the incident response lifecycle - Giới thiệu về vòng đời ứng phó sự cố***

|  |
| --- |
| Incident lifecycle frameworks provide a structure to support incident response operations. Frameworks help organizations develop a standardized approach to their incident response process, so that incidents are managed in an effective and consistent way. There are many different types of frameworks that organizations can adopt and modify according to their needs. |

Khung vòng đời sự cố cung cấp một cấu trúc để hỗ trợ phản hồi sự cốhoạt động.Các khuôn khổ giúp các tổ chức phát triển một cách tiếp cận chuẩn hóa đối với sự cố của họquá trình phản hồi, vì vậyđể các sự cố được quản lý một cách hiệu quả và nhất quán.Có nhiều loại khuôn khổ khác nhau mà các tổ chức có thể áp dụngvà sửa đổi theo nhu cầu của họ.

|  |
| --- |
| In this course, we'll focus on the NIST CSF. Then, we'll expand on the CSF and discuss the phases of the NIST incident response lifecycle. To recall, the five core functions of the NIST CSF are: identify, protect, detect, respond, and recover. This course will explore the last three steps of this framework: detect, respond, and recover. These last three steps are critical stages during incident response, and as an analyst, you'll detect and respond to incidents and implement actions for recovery. |

Trong khóa học này, chúng ta sẽ tập trung vào NIST CSF.Sau đó, chúng ta sẽ mở rộng CSF vàthảo luận về các giai đoạn của vòng đời ứng phó sự cố NIST.Để nhớ lại, năm chức năng cốt lõi của NIST CSF là: xác định,bảo vệ, phát hiện, ứng phó và phục hồi.Khóa học này sẽ khám phá ba bước cuối cùng của khuôn khổ này:phát hiện, phản hồi và phục hồi.Ba bước cuối cùng này là những giai đoạn quan trọng trong quá trình ứng phó sự cố vàvới tư cách là một nhà phân tích, bạn sẽ phát hiện và phản ứng với các sự cố vàthực hiện các hành động phục hồi.

|  |
| --- |
| The NIST incident response lifecycle is another NIST framework with additional substeps dedicated to incident response. It begins with preparation. Next, detection and analysis, and then containment, eradication and recovery, and finally post-incident activity. One thing to note is that the incident lifecycle isn't a linear process. It's a cycle, which means that steps can overlap as new discoveries are made. |

Vòng đời phản hồi sự cố của NIST là một khuôn khổ NIST khác với các bước phụ bổ sungdành riêng cho việc ứng phó sự cố.Nó bắt đầu bằng sự chuẩn bị. Tiếp theo, phát hiện và phân tích, vàsau đó là ngăn chặn, xóa bỏ và phục hồi, và cuối cùng là hoạt động sau sự cố.Một điều cần lưu ý là vòng đời của sự cố không phải là một quá trình tuyến tính.Đây là một chu trình, có nghĩa là các bước có thể chồng chéo lên nhau khi có những khám phá mới.

|  |
| --- |
| This lifecycle gives us a blueprint of how to effectively respond to incidents, but before we dive into incident detection and response, let's take some time to understand what an incident is. |

Vòng đời này cung cấp cho chúng ta bản thiết kế về cách ứng phó hiệu quả với các sự cố,nhưng trước khi chúng ta đi sâu vào việc phát hiện và ứng phó sự cố,hãy dành chút thời gian để hiểu sự cố là gì.

|  |
| --- |
| According to NIST, an incident is "an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Whoa, that's a lot to take in. Let's break it down. |

Theo NIST, một sự cố là "một sự việc thực sự hoặc sắp xảy ragây nguy hiểm, mà không có thẩm quyền hợp pháp, tính bảo mật, tính toàn vẹn hoặctính sẵn có của thông tin hoặc hệ thống thông tin;hoặc cấu thành hành vi vi phạm hoặc đe dọa vi phạm pháp luật ngay lập tức,chính sách bảo mật, quy trình bảo mật hoặc chính sách sử dụng được chấp nhận."Ồ, có quá nhiều thứ để tiếp thu.Chúng ta hãy phân tích nó nhé.

|  |
| --- |
| It's important to understand that all security incidents are events, but not all events are security incidents. What are events? An event is an observable occurrence on a network, system, or device. |

Điều quan trọng là phải hiểu rằng tất cả các sự cố bảo mật đều là sự kiện, nhưngkhông phải mọi sự kiện đều là sự cố an ninh.Sự kiện là gì?Sự kiện là hiện tượng có thể quan sát được trên mạng, hệ thống hoặc thiết bị.

|  |
| --- |
| Here's an example of an event. A user attempts to log into their email account, but they can't because they forgot their password. The user then requests a password reset and successfully changes their password. |

Đây là một ví dụ về một sự kiện. Người dùng cố gắng đăng nhập vào tài khoản email của họ,nhưng họ không thể vì họ quên mật khẩu.Sau đó, người dùng yêu cầu đặt lại mật khẩu và đã thay đổi mật khẩu thành công.

|  |
| --- |
| This is an observable event. Why? Because systems and applications log password reset requests and logs provide evidence that something happened. We know that someone successfully requested a password reset and that they did not violate security policies to access the account. |

Đây là một sự kiện có thể quan sát được.Tại sao?Bởi vì các hệ thống và ứng dụng ghi lại yêu cầu đặt lại mật khẩu vànhật ký cung cấp bằng chứng cho thấy có điều gì đó đã xảy ra.Chúng tôi biết rằng ai đó đã yêu cầu đặt lại mật khẩu thành công vàrằng họ không vi phạm chính sách bảo mật để truy cập vào tài khoản.

|  |
| --- |
| Now, imagine that instead of the rightful owner of the account, a malicious actor trying to gain access to the account, successfully initiated the password change request and changed the account password. This would be considered both an event and a security incident. It's an event because it's an observable occurrence. It's also a security incident because a malicious actor violated the security policy to unlawfully access an account that is not rightfully theirs. Remember, all security incidents are events, but not all events are security incidents. |

Bây giờ, hãy tưởng tượng rằng thay vì chủ sở hữu hợp pháp của tài khoản,một tác nhân độc hại đang cố gắng truy cập vào tài khoản,đã khởi tạo thành công yêu cầu thay đổi mật khẩu và đã thay đổi mật khẩu tài khoản.Điều này có thể được coi là cả một sự kiện và một sự cố an ninh.Đó là một sự kiện vì nó là hiện tượng có thể quan sát được.Đây cũng là một sự cố bảo mật vì một tác nhân độc hại đã vi phạm bảo mậtchính sách truy cập trái phép vào tài khoản không phải của mình.Hãy nhớ rằng, mọi sự cố bảo mật đều là sự kiện, nhưng không phải mọi sự kiện đều là sự cố bảo mật.

|  |
| --- |
| Just like detectives working a case carefully handle and document their evidence and findings, security analysts are required to do the same when they investigate a security incident. An incident investigation reveals critical information about the five W's of an incident: who triggered the incident, what happened, when the incident took place, where the incident took place, and why the incident occurred. |

Giống như các thám tử đang làm việc một vụ án xử lý cẩn thận vàghi lại bằng chứng và phát hiện của họ,các nhà phân tích an ninh được yêu cầu làm như vậy khi họ điều tra một vấn đề an ninhsự cố.Một cuộc điều tra sự cố tiết lộ thông tin quan trọng về năm chữ Wcủa một sự cố:người gây ra sự cố,chuyện gì đã xảy ra thế,khi sự việc xảy ra,nơi xảy ra sự cố và lý do xảy ra sự cố.

|  |
| --- |
| Keeping track of this information is essential not only during an incident investigation, but also during the closure of an investigation when it comes time to write the final report. As an analyst, you'll need a method to document and reference this information for easy access when you need it. |

Việc theo dõi thông tin này là điều cần thiết không chỉ trong trường hợp xảy ra sự cốcuộc điều tra, nhưng cũng trong quá trình kết thúc một cuộc điều trakhi đến lúc viết báo cáo cuối cùng. Là một nhà phân tích, bạn sẽ cần một phương phápđể ghi lại và tham khảo thông tin này để dễ dàng truy cập khi bạn cần.

|  |
| --- |
| A great way to do this is to use an incident handler's journal, which is a form of documentation used in incident response. Throughout this course, you'll be using your own incident handler's journal to take notes of any incident details. We'll discuss more on documentation in the upcoming lessons. |

Một cách tuyệt vời để thực hiện điều này là sử dụng nhật ký của người xử lý sự cố,là một hình thức ghi chép được sử dụng trong ứng phó sự cố.Trong suốt khóa học này, bạn sẽ sử dụng nhật ký xử lý sự cố của riêng mình để ghi chépghi chú về bất kỳ chi tiết sự cố nào.Chúng ta sẽ thảo luận thêm về tài liệu trong các bài học sắp tới.

***2.3. Explore: Apply the NIST lifecycle to a vishing scenario - Khám phá: Áp dụng vòng đời NIST vào kịch bản vishing***

|  |  |
| --- | --- |
| **Vishing attack: how to respond?** | |
| Infographic background image  **Preparation: the planning and training process**  The organization takes action to ensure it has the correct tools and resources in place:   * Set up uniform company email conventions * Create a collaborative, ethical environment where employees feel comfortable asking questions * Provide cybersecurity training on a quarterly basis | Infographic background image  **Detection and analysis: the detect and assess process**  Security professionals create processes to detect and assess incidents:   * Identify signs of an incident * Filter external emails to flag messages containing attachments such as voicemails * Have an incident response plan to reference |
| Infographic background image  **Containment, eradication, and recovery: the minimize and mitigate process**  Security professionals and stakeholders collaborate to minimize the impact of the incident and mitigate any operational disruption.   * Communicate with sender to confirm the origin of the voice message * Provide employees with an easy way to report and contain suspicious messages | Infographic background image  **Post-incident activity: the learning process**  New protocols, procedures, playbooks, etc. are implemented to help reduce any similar incidents in the future.   * Update the playbook to highlight additional red flags employees should be aware of * Review processes and workflows related to permissions and adjust oversight of those permissions |

|  |  |
| --- | --- |
| **Tấn công Vishing: ứng phó thế nào?** | |
| Infographic background image  **Chuẩn bị: quá trình lập kế hoạch và đào tạo**  Tổ chức thực hiện hành động để đảm bảo có sẵn các công cụ và nguồn lực phù hợp:   * Thiết lập quy ước email thống nhất của công ty * Tạo môi trường hợp tác, có đạo đức, nơi nhân viên cảm thấy thoải mái khi đặt câu hỏi * Cung cấp đào tạo về an ninh mạng hàng quý | Infographic background image  **Phát hiện và phân tích: quá trình phát hiện và đánh giá**  Các chuyên gia bảo mật tạo ra các quy trình để phát hiện và đánh giá sự cố:   * Xác định dấu hiệu của sự cố * Lọc các email bên ngoài để gắn cờ các thư có chứa tệp đính kèm như thư thoại * Có kế hoạch ứng phó sự cố để tham khảo |
| Infographic background image  **Ngăn chặn, diệt trừ và phục hồi: quá trình giảm thiểu và giảm nhẹ**  Các chuyên gia bảo mật và các bên liên quan hợp tác để giảm thiểu tác động của sự cố và giảm thiểu mọi gián đoạn hoạt động.   * Liên lạc với người gửi để xác nhận nguồn gốc của tin nhắn thoại * Cung cấp cho nhân viên một cách dễ dàng để báo cáo và chứa các tin nhắn đáng ngờ | Infographic background image  **Hoạt động sau sự cố: quá trình học tập**  Các giao thức, quy trình, cẩm nang mới, v.v. được triển khai để giúp giảm thiểu bất kỳ sự cố tương tự nào trong tương lai.   * Cập nhật cẩm nang để nêu bật những dấu hiệu cảnh báo bổ sung mà nhân viên nên biết * Xem lại các quy trình và quy trình công việc liên quan đến quyền và điều chỉnh việc giám sát các quyền đó |

***2.4. Portfolio Activity: Document an incident with an incident handler's journal - Hoạt động danh mục đầu tư: Ghi chép sự cố bằng nhật ký của người xử lý sự cố***

|  |
| --- |
| **Activity Overview**  In this activity, you will review the details of a security incident and document the incident using your incident handler's journal. Previously, you learned about the importance of documentation in the incident response process. You've also learned how an incident handler's journal is used to record information about security incidents as they are handled.  Throughout this course, you can apply your documentation skills using your incident handler's journal. With this journal, you can record information about the experiences you will have analyzing security incident scenarios through the course activities.  By the time you complete this course you will have multiple entries in your incident handler's journal that you can use as a helpful reference to recall concepts and tools. Later, you'll add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/detection-and-response/resources/H3ujO).  Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.  ***Note:*** *You can use your incident handler's journal as a personal space where you can keep track of your learning journey as you learn about incident detection and response concepts and interact with different cybersecurity tools. Feel free to include your thoughts, reflections, and any other important details or information.* |

**Tổng quan hoạt động**

Trong hoạt động này, bạn sẽ xem xét chi tiết về sự cố bảo mật và ghi lại sự cố bằng nhật ký của người xử lý sự cố. Trước đó, bạn đã tìm hiểu về tầm quan trọng của việc ghi chép trong quy trình ứng phó sự cố. Bạn cũng đã tìm hiểu cách nhật ký của người xử lý sự cố được sử dụng để ghi lại thông tin về sự cố bảo mật khi chúng được xử lý.

Trong suốt khóa học này, bạn có thể áp dụng các kỹ năng lập tài liệu của mình bằng cách sử dụng nhật ký xử lý sự cố. Với nhật ký này, bạn có thể ghi lại thông tin về những trải nghiệm bạn sẽ có khi phân tích các tình huống sự cố bảo mật thông qua các hoạt động của khóa học.

Khi bạn hoàn thành khóa học này, bạn sẽ có nhiều mục trong nhật ký xử lý sự cố mà bạn có thể sử dụng làm tài liệu tham khảo hữu ích để nhớ lại các khái niệm và công cụ. Sau đó, bạn sẽ thêm tài liệu này vào danh mục an ninh mạng của mình, mà bạn có thể chia sẻ với các nhà tuyển dụng hoặc người tuyển dụng tiềm năng. Để xem lại tầm quan trọng của việc xây dựng danh mục chuyên nghiệp và các tùy chọn để tạo danh mục của bạn, hãy đọc[Tạo danh mục đầu tư an ninh mạng](https://www.coursera.org/learn/detection-and-response/resources/H3ujO).

Hãy chắc chắn hoàn thành hoạt động này và trả lời các câu hỏi sau trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với bài làm của bạn.

***Lưu ý:*** *Bạn có thể sử dụng nhật ký xử lý sự cố của mình như một không gian cá nhân, nơi bạn có thể theo dõi hành trình học tập của mình khi tìm hiểu về các khái niệm phát hiện và ứng phó sự cố cũng như tương tác với các công cụ an ninh mạng khác nhau. Hãy thoải mái đưa vào suy nghĩ, phản hồi và bất kỳ chi tiết hoặc thông tin quan trọng nào khác.*

|  |
| --- |
| **Scenario**  Review the following scenario. Then complete the step-by-step instructions.  A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.  Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.  The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.  Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance. |

**Kịch bản**

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

Một phòng khám chăm sóc sức khỏe nhỏ của Hoa Kỳ chuyên cung cấp dịch vụ chăm sóc sức khỏe ban đầu đã gặp sự cố bảo mật vào sáng thứ Ba, khoảng 9:00 sáng. Một số nhân viên báo cáo rằng họ không thể sử dụng máy tính để truy cập các tệp như hồ sơ y tế. Hoạt động kinh doanh bị đóng cửa vì nhân viên không thể truy cập các tệp và phần mềm cần thiết để thực hiện công việc của họ.

Ngoài ra, nhân viên cũng báo cáo rằng một ghi chú đòi tiền chuộc đã được hiển thị trên máy tính của họ. Ghi chú đòi tiền chuộc nêu rằng tất cả các tệp của công ty đã được mã hóa bởi một nhóm tin tặc phi đạo đức có tổ chức, những kẻ được biết đến là nhắm vào các tổ chức trong ngành chăm sóc sức khỏe và vận tải. Để đổi lấy việc khôi phục quyền truy cập vào các tệp đã mã hóa, ghi chú đòi tiền chuộc yêu cầu một khoản tiền lớn để đổi lấy khóa giải mã.

Những kẻ tấn công đã có thể truy cập vào mạng của công ty bằng cách sử dụng email lừa đảo có mục tiêu, được gửi đến một số nhân viên của công ty. Email lừa đảo chứa tệp đính kèm độc hại cài đặt phần mềm độc hại vào máy tính của nhân viên sau khi tải xuống.

Sau khi những kẻ tấn công có được quyền truy cập, chúng triển khai phần mềm tống tiền, mã hóa các tệp quan trọng. Công ty không thể truy cập dữ liệu quan trọng của bệnh nhân, gây ra sự gián đoạn lớn trong hoạt động kinh doanh của họ. Công ty buộc phải tắt hệ thống máy tính và liên hệ với một số tổ chức để báo cáo sự cố và nhận hỗ trợ kỹ thuật.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước**

Làm theo hướng dẫn để hoàn thành từng bước của hoạt động. Sau đó, trả lời 5 câu hỏi ở cuối hoạt động trước khi chuyển sang mục khóa học tiếp theo để so sánh bài làm của bạn với bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the link and select *Use Template*.  Link to template: [Incident handler's journal](https://docs.google.com/document/d/1jGJhQKrNz7G62RaiIj7l-OTWBTKXVaerWSCRVS0xEQE/template/preview?resourcekey=0-JXYRihuX_a13YrV6ditJ3A) |

**Bước 1: Truy cập mẫu**

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

Liên kết đến mẫu:[Nhật ký của người xử lý sự cố](https://docs.google.com/document/d/1jGJhQKrNz7G62RaiIj7l-OTWBTKXVaerWSCRVS0xEQE/template/preview?resourcekey=0-JXYRihuX_a13YrV6ditJ3A)

|  |
| --- |
| **Step 2: Review the scenario**  Review the details of the scenario. Consider the following key details:   * A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. * The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. * An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key |

**Bước 2: Xem lại kịch bản**

Xem lại các chi tiết của kịch bản. Xem xét các chi tiết chính sau:

* Một phòng khám chăm sóc sức khỏe nhỏ ở Hoa Kỳ đã gặp sự cố an ninh vào lúc 9:00 sáng thứ Ba, gây gián đoạn nghiêm trọng đến hoạt động kinh doanh của họ.
* Nguyên nhân của sự cố bảo mật là một email lừa đảo có chứa tệp đính kèm độc hại. Sau khi tải xuống, ransomware đã được triển khai để mã hóa các tệp máy tính của tổ chức.
* Một nhóm tin tặc vô đạo đức có tổ chức đã để lại một yêu cầu đòi tiền chuộc nêu rằng các tập tin của công ty đã bị mã hóa và yêu cầu tiền để đổi lấy khóa giải mã

|  |
| --- |
| **Step 3: Record a journal entry**  Use the incident handler's journal to document your first journal entry about the given scenario. Ensure that you fill in all of the fields:   1. In the **Date** section, record the date of your journal entry. This should be the actual date that you record the entry, not a fictional date. 2. In the **Entry** section, provide a journal entry number. For example, if it is your first journal entry, enter 1. 3. In the **Description** section, provide a description about the entry. 4. In the **Tool(s) used** section, if any cybersecurity tools were used, list them here. 5. In the **The 5 W's** section, record the details about the given scenario.    1. Who caused the incident?    2. What happened?    3. When did the incident occur?    4. Where did the incident happen?    5. Why did the incident happen? 6. In the **Additional notes** row, record any thoughts or questions you have about the given scenario. |

**Bước 3: Ghi lại nhật ký**

Sử dụng nhật ký của người xử lý sự cố để ghi lại mục nhật ký đầu tiên của bạn về tình huống đã cho. Đảm bảo rằng bạn điền vào tất cả các trường:

1. Trong phần **Ngày** , hãy ghi lại ngày ghi nhật ký của bạn. Đây phải là ngày thực tế mà bạn ghi lại mục nhập, không phải là ngày hư cấu.
2. Trong phần **Mục nhập** , hãy cung cấp số mục nhập nhật ký. Ví dụ, nếu đây là mục nhập nhật ký đầu tiên của bạn, hãy nhập 1.
3. Trong phần **Mô tả** , hãy cung cấp mô tả về mục nhập.
4. Trong phần **Công cụ được sử dụng** , nếu có bất kỳ công cụ an ninh mạng nào được sử dụng, hãy liệt kê chúng ở đây.
5. Trong phần **5W** , hãy ghi lại thông tin chi tiết về tình huống đã cho.
   1. Ai là người gây ra vụ việc này?
   2. Chuyện gì đã xảy ra thế?
   3. Sự việc xảy ra khi nào?
   4. Sự việc xảy ra ở đâu?
   5. Tại sao sự việc lại xảy ra?
6. Trong hàng **Ghi chú bổ sung** , hãy ghi lại bất kỳ suy nghĩ hoặc câu hỏi nào bạn có về tình huống đã cho.

|  |
| --- |
| **Pro Tip: Save a copy of your work**  Finally, be sure to save a copy of your incident handler's journal so that you can quickly access it as you progress through the course. You can use it for your professional portfolio to demonstrate your knowledge and/or experience to potential employers. |

**Mẹo chuyên nghiệp: Lưu một bản sao tác phẩm của bạn**

Cuối cùng, hãy chắc chắn lưu một bản sao nhật ký xử lý sự cố của bạn để bạn có thể truy cập nhanh khi bạn tiến triển trong khóa học. Bạn có thể sử dụng nó cho danh mục đầu tư chuyên nghiệp của mình để chứng minh kiến ​​thức và/hoặc kinh nghiệm của bạn với các nhà tuyển dụng tiềm năng.

|  |
| --- |
| **What to Include in Your Response**  Be sure to include the following elements in your completed activity:   * The journal entry date and number * A description of the journal entry * 1-2 sentences addressing each of the 5 W's of the scenario:   + Who caused the incident?   + What happened?   + When did the incident occur?   + Where did the incident happen?   + Why did the incident happen? * 1-2 sentences on any additional thoughts or questions about the scenario. |

**Những gì cần đưa vào phản hồi của bạn**

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

* Ngày và số mục nhập nhật ký
* Mô tả về mục nhật ký
* 1-2 câu giải quyết từng câu hỏi trong 5 câu hỏi W của tình huống:
  + Ai là người gây ra vụ việc này?
  + Chuyện gì đã xảy ra thế?
  + Sự việc xảy ra khi nào?
  + Sự việc xảy ra ở đâu?
  + Tại sao sự việc lại xảy ra?
* 1-2 câu về bất kỳ suy nghĩ hoặc câu hỏi bổ sung nào về tình huống này.

|  |
| --- |
| **Step 4: Assess your activity**  The following is a self-assessment for your incident handler's journal. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your first entry in the incident handler's journal.  There are a total of 5 points possible for this activity and each statement is worth 1 point. The items correspond to each step you completed for the activity.  To complete the self-assessment, first open your incident handler's journal. Then respond yes or no to each statement.  When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this project is at least 80% (or 4/5 points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 4 points before continuing on to the next course item. |

**Bước 4: Đánh giá hoạt động của bạn**

Sau đây là bản tự đánh giá cho nhật ký xử lý sự cố của bạn. Bạn sẽ sử dụng các tuyên bố này để xem lại công việc của chính mình. Quá trình tự đánh giá là một phần quan trọng của trải nghiệm học tập vì nó cho phép bạn đánh giá *khách quan* mục nhập đầu tiên của mình trong nhật ký xử lý sự cố.

Tổng cộng có 5 điểm có thể đạt được cho hoạt động này và mỗi câu có giá trị 1 điểm. Các mục tương ứng với từng bước bạn đã hoàn thành cho hoạt động này.

Để hoàn tất việc tự đánh giá, trước tiên hãy mở nhật ký của người xử lý sự cố. Sau đó trả lời có hoặc không cho từng câu.

Khi bạn hoàn thành và nộp phản hồi, bạn sẽ nhận được điểm phần trăm. Điểm này sẽ giúp bạn xác nhận xem bạn đã hoàn thành các bước bắt buộc của hoạt động hay chưa. Điểm đậu được khuyến nghị cho dự án này là ít nhất 80% (hoặc 4/5 điểm). Nếu bạn muốn tăng điểm, bạn có thể sửa đổi dự án của mình và sau đó nộp lại phản hồi để phản ánh bất kỳ thay đổi nào bạn đã thực hiện. Cố gắng đạt được ít nhất 4 điểm trước khi tiếp tục đến mục khóa học tiếp theo.

***2.5. Portfolio Activity Exemplar: Document an incident with an incident handler's journal - Mẫu hoạt động danh mục đầu tư: Ghi lại sự cố bằng nhật ký của người xử lý sự cố***

|  |
| --- |
| **Portfolio Activity Exemplar: Document an incident with an incident handler's journal**  Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

**Mẫu hoạt động danh mục đầu tư: Ghi lại sự cố bằng nhật ký của người xử lý sự cố**

Sau đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ này đáp ứng được kỳ vọng của hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the link and select *Use Template*.  Link to exemplar: [Incident handler's journal entry exemplar](https://docs.google.com/document/d/1NdqPmIeVDjRMzVmOz_puj2Vw7YGZTyd_yrdcPqLTVYc/template/preview?usp=sharing) |

**Mẫu hoàn thành**

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

Liên kết đến ví dụ:[Mẫu mục nhật ký của người xử lý sự cố](https://docs.google.com/document/d/1NdqPmIeVDjRMzVmOz_puj2Vw7YGZTyd_yrdcPqLTVYc/template/preview?usp=sharing)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.  ***Note:*** *The exemplar represents one of many possible ways to complete this activity. Yours will likely differ in certain ways. What’s important is that your incident handler's journal records the details of the scenario. Knowing how to use an incident handler's journal to record notes and additional details during an incident investigation is important because it can be used as a reference for future incident response efforts.* |

**Đánh giá mẫu**

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

***Lưu ý:*** *Ví dụ này là một trong nhiều cách có thể để hoàn thành hoạt động này. Ví dụ của bạn có thể khác ở một số điểm. Điều quan trọng là nhật ký của người xử lý sự cố phải ghi lại chi tiết của tình huống. Biết cách sử dụng nhật ký của người xử lý sự cố để ghi lại ghi chú và các chi tiết bổ sung trong quá trình điều tra sự cố là điều quan trọng vì nó có thể được sử dụng làm tài liệu tham khảo cho các nỗ lực ứng phó sự cố trong tương lai.*

|  |
| --- |
| The exemplar contains one completed journal entry. The journal entry is dated, numbered, and provides a brief description of the scenario. Additionally, in the **The 5 W's section**, the journal entry addresses the following about the scenario:   * Who caused the incident? * What happened? * When did the incident occur? * Where did the incident happen? * Why did the incident happen?   Lastly, the journal entry includes additional questions about the scenario in the **Additional notes** section.  **Note**: The exemplar contains the first entry in the incident handler's journal. As you progress through the course, you'll complete the subsequent journal entries in your incident handler's journal template. |

Bản mẫu có một mục nhật ký đã hoàn thành. Mục nhật ký được ghi ngày, đánh số và cung cấp mô tả ngắn gọn về tình huống. Ngoài ra, trong **phần 5 W** , mục nhật ký đề cập đến những điều sau về tình huống:

* Ai là người gây ra vụ việc này?
* Chuyện gì đã xảy ra thế?
* Sự việc xảy ra khi nào?
* Sự việc xảy ra ở đâu?
* Tại sao sự việc lại xảy ra?

Cuối cùng, mục nhật ký bao gồm các câu hỏi bổ sung về tình huống trong phần **Ghi chú bổ sung** .

**Lưu ý** : Bản mẫu chứa mục nhập đầu tiên trong nhật ký của người xử lý sự cố. Khi bạn tiến triển trong khóa học, bạn sẽ hoàn thành các mục nhập nhật ký tiếp theo trong mẫu nhật ký của người xử lý sự cố.

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

**Những điểm chính**

|  |
| --- |
| This activity enabled you to practice applying your documentation skills to complete a journal entry about a ransomware scenario. Accurate and thorough documentation is a critical aspect in incident response because it helps to ensure that important information is not lost or overlooked, and it also allows you to capture aspects of an incident for future use. Continue practicing your documentation skills by creating additional journal entries as you complete the course activities. By the end of the course, you will add this document to your cybersecurity portfolio. |

Hoạt động này giúp bạn thực hành áp dụng các kỹ năng lập tài liệu của mình để hoàn thành mục nhật ký về một kịch bản ransomware. Tài liệu chính xác và đầy đủ là một khía cạnh quan trọng trong ứng phó sự cố vì nó giúp đảm bảo rằng thông tin quan trọng không bị mất hoặc bị bỏ sót, đồng thời cũng cho phép bạn nắm bắt các khía cạnh của sự cố để sử dụng trong tương lai. Tiếp tục thực hành các kỹ năng lập tài liệu của bạn bằng cách tạo các mục nhật ký bổ sung khi bạn hoàn thành các hoạt động của khóa học. Vào cuối khóa học, bạn sẽ thêm tài liệu này vào danh mục an ninh mạng của mình.

***2.6. Test your knowledge: The incident response lifecycle - Kiểm tra kiến thức của bạn: Vòng đời ứng phó sự cố***

**3. Incident response operations – Hoạt động ứng phó sự cố**

***3.1. Incident response teams - Đội ứng phó sự cố***

|  |
| --- |
| Hi again! In this section, we'll discuss how incident response teams manage incidents. |

Xin chào lần nữa!Trong phần này, chúng ta sẽ thảo luận về cách các nhóm ứng phó sự cố quản lý sự cố.

|  |
| --- |
| You may have been part of a team before. Whether it was a sports team, or a team in the workplace or at school, teams are most successful when everyone uses their diverse strengths to work towards a common goal. |

Bạn có thể đã từng là thành viên của một đội trước đây. Cho dù đó là một đội thể thao haymột nhóm ở nơi làm việc hoặc ở trường,các nhóm thành công nhất khi mọi người sử dụng những điểm mạnh khác nhau của mình để làm việchướng tới một mục tiêu chung.

|  |
| --- |
| Incident response teams aren't any different. A successful response to security incidents doesn't happen in isolation. It requires a team of both security and non-security professionals working together with defined roles. |

Các đội ứng phó sự cố cũng không có gì khác biệt.Phản ứng thành công đối với các sự cố an ninh không thể diễn ra một cách đơn lẻ.Nó đòi hỏi một đội ngũ cả về an ninh vànhững người không chuyên về an ninh làm việc cùng nhau với các vai trò được xác định.

|  |
| --- |
| Computer security incident response teams, or CSIRTs, are a specialized group of security professionals that are trained in incident management and response. The goal of CSIRTs are to effectively and efficiently manage incidents, provide services and resources for response and recovery, and prevent future incidents from occurring. |

Các nhóm ứng phó sự cố bảo mật máy tính, hay CSIRT, là một nhóm chuyên biệtchuyên gia an ninh được đào tạo về quản lý và ứng phó sự cố.Mục tiêu của CSIRT là quản lý các sự cố một cách hiệu quả và hiệu suất,cung cấp các dịch vụ và nguồn lực để ứng phó và phục hồi, vàngăn ngừa các sự cố tương tự xảy ra trong tương lai.

|  |
| --- |
| Security is a shared responsibility, which is why CSIRTs must work cross functionally with other departments to share relevant information. For example, if an incident resulted in the breach of sensitive data, like financial documents or PII, then the legal team must be consulted. Some regulatory compliance measures may require organizations to publicly disclose a security incident within a certain timeframe. This means that CSIRTs must collaborate with the organization's public relations team to coordinate efforts for public disclosure. |

An ninh là trách nhiệm chung, đó là lý do tại sao CSIRT phải hoạt động liên chức năngvới các phòng ban khác để chia sẻ thông tin có liên quan.Ví dụ, nếu một sự cố dẫn đến vi phạm dữ liệu nhạy cảm,như các tài liệu tài chính hoặc PII, thì phải tham khảo ý kiến ​​của nhóm pháp lý.Một số biện pháp tuân thủ quy định có thể yêu cầu các tổ chức phải công khaimột sự cố an ninh trong một khoảng thời gian nhất định.Điều này có nghĩa là CSIRT phải hợp tác với bộ phận quan hệ công chúng của tổ chứcnhóm phối hợp nỗ lực để công bố thông tin cho công chúng.

|  |
| --- |
| So how exactly does a CSIRT function? First, there's the security analyst. The analyst's job is to investigate security alerts to determine if an incident has occurred. If an incident has been detected, the analyst will determine the criticality rating of the incident. Some incidents can be easily remediated by the security analyst and don't require escalation. But if the incident is highly critical, it gets escalated to the technical lead, who provides technical leadership by guiding security incidents through their lifecycle. |

Vậy chính xác thì CSIRT hoạt động như thế nào?Đầu tiên là nhà phân tích bảo mật.Công việc của nhà phân tích là điều tra các cảnh báo bảo mật để xác định xem có sự cố nào khôngđã xảy ra.Nếu phát hiện ra sự cố,nhà phân tích sẽ xác định mức độ nghiêm trọng của sự cố.Một số sự cố có thể dễ dàng được khắc phục bởi nhà phân tích bảo mật vàkhông cần phải leo thang.Nhưng nếu sự cố đó cực kỳ nghiêm trọng,nó được chuyển đến người đứng đầu kỹ thuật, người cung cấp sự lãnh đạo kỹ thuật bằng cáchhướng dẫn các sự cố bảo mật trong suốt vòng đời của chúng.

|  |
| --- |
| During this time, the incident coordinator tracks and manages the activities of the CSIRT and other teams involved in the response effort. Their job is to ensure that incident response processes are followed and that teams are regularly updated on the incident status. Not all CSIRTs are the same. Depending on the organization, a CSIRT can also be referred to as an Incident Handling Team, or IHT, or Security Incident Response Team, SIRT. Depending on an organization's structure, some teams can also have a broader or specialized focus. For example, some teams may be solely dedicated to crisis management and others may be incorporated with a SOC. Roles can have different names too. For example, a technical lead can also be known as an Ops lead. |

Trong thời gian này, điều phối viên sự cố theo dõi và quản lý các hoạt động củaCSIRT và các nhóm khác tham gia vào nỗ lực ứng phó.Công việc của họ là đảm bảo các quy trình ứng phó sự cố được tuân thủ vàcác nhóm thường xuyên được cập nhật về tình hình sự cố.Không phải tất cả CSIRT đều giống nhau.Tùy thuộc vào tổ chức, CSIRT cũng có thể được gọi là Sự cốĐội xử lý, hay IHT, hoặc Đội ứng phó sự cố an ninh, SIRT.Tùy thuộc vào cấu trúc của tổ chức, một số nhóm cũng có thể có phạm vi rộng hơn hoặctập trung chuyên môn.Ví dụ, một số nhóm có thể chỉ chuyên quản lý khủng hoảng vànhững người khác có thể được kết hợp với SOC.Các vai trò cũng có thể có tên khác nhau. Ví dụ,Người đứng đầu bộ phận kỹ thuật cũng có thể được gọi là người đứng đầu bộ phận vận hành.

|  |
| --- |
| Regardless of the team's title or focus, they all share the same goal: incident management and response. |

Bất kể danh hiệu hay trọng tâm của đội là gì, tất cả đều có chung một mục tiêu:quản lý và ứng phó sự cố.

|  |
| --- |
| Now that you know a bit about incident response teams, we'll continue to learn about how incident response teams plan, organize, and respond to incidents. I'll meet you in the next video. |

Bây giờ bạn đã biết một chút về các nhóm ứng phó sự cố, chúng ta sẽ tiếp tục tìm hiểuvề cách các nhóm ứng phó sự cố lập kế hoạch, tổ chức và ứng phó với các sự cố.Tôi sẽ gặp lại các bạn trong video tiếp theo.

***3.2. Fatima: The importance of communication during incident response - Fatima: Tầm quan trọng của giao tiếp trong quá trình ứng phó sự cố***

|  |
| --- |
| My name is Fatima, and I'm a tech lead manager on Google's Detection and Response Team. If there is a hacker on the network, our job is to find them. Working in detection is really like an artist preparing for a show. We spend all this time developing all of these signatures to detect hackers, and then one day, it's time for the show. You get that same nervous energy and your question whether you're ready for the performance or not, but you really don't have a choice. The hackers are going to come and you have to be ready for them. I would say cybersecurity is very exciting. You never know when the next vulnerability is going to be released. You never know when the next incident is going to happen. A great example of an incident would be the Log4j vulnerability that happened in 2021. The entire company came together to investigate whether or not we were affected by this vulnerability. It was my team's job to make that determination. We ingest hundreds of millions of lines of logs per second. After we have these logs, it requires hunting and log diving through them, creating different signatures to match against these logs for signs of compromise. We were able to say all clear, we are not impacted by this and we're safe. Those are the moments. Those are the highlights. That's where everything comes together. Teamwork in an incident response scenario, is key. You cannot run an incident response without a really solid team, a team that works really well together, a team that really trust each other. The way to maintain clear and effective communication is by communicating a lot. During an incident it's a little bit counterintuitive, but the people who are the more senior engineers, these people become the operational leads. They are the people who are responsible for making sure that the communication is not breaking down within their function. So, we shift roles from being very technical to really focusing on the communication, aggregating the data, and surfacing the data to the right people who need to know about it. I definitely recommend cybersecurity as a career field because really the attackers, they're not going to let you get bored because they are very creative, so we have to be creative in the way that we go out looking for them. Being a person who likes to learn, knowing that there's always going to be a thing for me to learn and become good at, that's exciting and that keeps me motivated. |

Tên tôi là Fatima,và tôi là người quản lý kỹ thuật hàng đầu vềNhóm phát hiện và ứng phó của Google.Nếu có một hacker trên mạng,nhiệm vụ của chúng ta là tìm ra chúng.Làm việc trong phát hiện làthực sự giống như một nghệ sĩ đang chuẩn bị cho một buổi biểu diễn.Chúng tôi dành tất cả thời gian này để phát triển tất cảnhững chữ ký này để phát hiện tin tặc,và rồi một ngày nọ,đã đến lúc biểu diễn.Bạn có cùng năng lượng lo lắng đóvà câu hỏi của bạn liệu bạn cósẵn sàng cho buổi biểu diễn hay chưa,nhưng thực ra bạn không có lựa chọn nào cả.Những tin tặc sẽ đến vàbạn phải sẵn sàng cho chúng.Tôi cho rằng an ninh mạng rất thú vị.Bạn không bao giờ biết khi nàolỗ hổng tiếp theo sắp được phát hiện.Bạn không bao giờ biết khi nào sự cố tiếp theo sẽ xảy ra.Một ví dụ tuyệt vời về một sự cố sẽ làlỗ hổng Log4j xảy ra vào năm 2021.Toàn bộ công ty đã cùng nhau hợp tác đểđiều tra xem chúng ta có hay khôngbị ảnh hưởng bởi lỗ hổng này.Nhiệm vụ đưa ra quyết định đó là của nhóm tôi.Chúng tôi tiếp nhận hàng trăm triệu dòngcủa logarit mỗi giây.Sau khi chúng ta có những bản ghi này,nó đòi hỏi phải săn bắt và lặn qua chúng,tạo ra các chữ ký khác nhau đểphù hợp với những bản ghi nàyđể có dấu hiệu thỏa hiệp.Chúng tôi đã có thể nói rằng mọi việc đã ổn thỏa,chúng tôi không bị ảnh hưởng bởi điều này và chúng tôi an toàn.Đó là những khoảnh khắc. Đó là những điểm nổi bật.Đó chính là nơi mọi thứ kết hợp lại với nhau.Làm việc nhóm trong tình huống ứng phó sự cố là điều quan trọng.Bạn không thể chạy phản hồi sự cốnếu không có một đội thực sự vững mạnh,một đội làm việc thực sự tốt với nhau,một đội thực sự tin tưởng lẫn nhau.Cách duy trìgiao tiếp rõ ràng và hiệu quảlà bằng cách giao tiếp nhiều.Trong một sự cố, nó có vẻ hơi trái ngược với trực giác,nhưng những người là kỹ sư cao cấp hơn,những người này trở thành người dẫn đầu hoạt động.Họ là những người đangchịu trách nhiệm đảm bảo rằnggiao tiếp không phải làbị hỏng trong chức năng của chúng.Vì vậy, chúng ta chuyển đổi vai trò từ rấtkỹ thuật để thực sự tập trung vào giao tiếp,tổng hợp dữ liệu và đưa dữ liệu lên bề mặtđến đúng người cần biết về nó.Tôi chắc chắn đề xuất an ninh mạng nhưmột lĩnh vực nghề nghiệp vì thực sự những kẻ tấn công,họ sẽ không để bạn có đượcchán vì họ rất sáng tạo,vì vậy chúng ta phải sáng tạo trongcách chúng ta đi ra ngoài để tìm kiếm chúng.Là một người thích học hỏi,biết rằng sẽ luôn cómột điều tôi cần học và trở nên giỏi,điều đó thật thú vị và giúp tôi có động lực.

***3.3. Roles in response - Vai trò trong phản ứng***

|  |
| --- |
| **Roles in response** |

**Vai trò trong phản ứng**

|  |
| --- |
| So far, you've been introduced to the **National Institute of Standards and Technology (NIST) Incident Response Lifecycle**, which is a framework for incident response consisting of four phases:   * Preparation * Detection and Analysis * Containment, Eradication, and Recovery * Post-incident activity |

Cho đến nay, bạn đã được giới thiệu về **Vòng đời ứng phó sự cố của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST)** , đây là khuôn khổ ứng phó sự cố bao gồm bốn giai đoạn:

* Sự chuẩn bị
* Phát hiện và Phân tích
* Ngăn chặn, Diệt trừ và Phục hồi
* Hoạt động sau sự cố

|  |
| --- |
| As a security professional, you'll work on a team to monitor, detect, and respond to incidents. Previously, you learned about a **computer security incident response team (CSIRT)** and a **security operations center (SOC)**. This reading explains the different functions, roles, and responsibilities that make up CSIRTs and SOCs. |

Với tư cách là một chuyên gia bảo mật, bạn sẽ làm việc trong một nhóm để giám sát, phát hiện và ứng phó với các sự cố. Trước đó, bạn đã tìm hiểu về **nhóm ứng phó sự cố bảo mật máy tính (CSIRT)** và **trung tâm điều hành bảo mật (SOC)** . Bài đọc này giải thích các chức năng, vai trò và trách nhiệm khác nhau tạo nên CSIRT và SOC.

|  |
| --- |
| Understanding the composition of incident response teams will help you navigate an organization’s hierarchy, openly collaborate and communicate with others, and work cohesively to respond to incidents. You may even discover specific roles that you’re interested in pursuing as you begin your security career! |

Hiểu được thành phần của các nhóm ứng phó sự cố sẽ giúp bạn điều hướng hệ thống phân cấp của tổ chức, hợp tác và giao tiếp cởi mở với những người khác và làm việc gắn kết để ứng phó với các sự cố. Bạn thậm chí có thể khám phá ra những vai trò cụ thể mà bạn quan tâm khi bắt đầu sự nghiệp bảo mật của mình!

|  |
| --- |
| **Command, control, and communication** |

**Chỉ huy, kiểm soát và truyền thông**

|  |
| --- |
| A **computer security incident response team (CSIRT)** is a specialized group of security professionals that are trained in incident management and response. During incident response, teams can encounter a variety of different challenges. For incident response to be effective and efficient, there must be clear command**,** control, and communication of the situation to achieve the desired goal. |

Nhóm **ứng phó sự cố bảo mật máy tính (CSIRT)** là một nhóm chuyên gia bảo mật được đào tạo về quản lý và ứng phó sự cố. Trong quá trình ứng phó sự cố, các nhóm có thể gặp phải nhiều thách thức khác nhau. Để ứng phó sự cố có hiệu quả và hiệu suất, phải có chỉ huy **,** kiểm soát và truyền đạt rõ ràng về tình hình để đạt được mục tiêu mong muốn.

|  |
| --- |
| * **Command** refers to having the appropriate leadership and direction to oversee the response. * **Control** refers to the ability to manage technical aspects during incident response, like coordinating resources and assigning tasks. * **Communication** refers to the ability to keep stakeholders informed. |

* **Chỉ huy** có nghĩa là có sự lãnh đạo và chỉ đạo phù hợp để giám sát phản ứng.
* **Kiểm soát** đề cập đến khả năng quản lý các khía cạnh kỹ thuật trong quá trình ứng phó sự cố, như phối hợp nguồn lực và phân công nhiệm vụ.
* **Giao tiếp** đề cập đến khả năng cập nhật thông tin cho các bên liên quan.

|  |
| --- |
| Establishing a CSIRT organizational structure with clear and distinctive roles aids in achieving an effective and efficient response. |

Việc thiết lập một cơ cấu tổ chức CSIRT với các vai trò rõ ràng và khác biệt sẽ giúp đạt được phản ứng hiệu quả và hiệu suất cao.

|  |
| --- |
| **Roles in CSIRTs** |

**Vai trò trong CSIRT**

|  |
| --- |
| CSIRTs are organization dependent, so they can vary in their structure and operation. Structurally, they can exist as a separate, dedicated team or as a task force that meets when necessary. CSIRTs involve both nonsecurity and security professionals. Nonsecurity professionals are often consulted to offer their expertise on the incident. These professionals can be from external departments, such as human resources, public relations, management, IT, legal, and others. Security professionals involved in a CSIRT typically include three key security related roles:   1. **Security analyst** 2. **Technical lead** 3. **Incident coordinator** |

CSIRT phụ thuộc vào tổ chức, do đó chúng có thể khác nhau về cấu trúc và hoạt động. Về mặt cấu trúc, chúng có thể tồn tại như một nhóm chuyên trách riêng biệt hoặc như một lực lượng đặc nhiệm họp khi cần thiết. CSIRT bao gồm cả các chuyên gia an ninh và không chuyên về an ninh. Các chuyên gia an ninh thường được tham vấn để cung cấp chuyên môn của họ về sự cố. Những chuyên gia này có thể đến từ các phòng ban bên ngoài, chẳng hạn như nhân sự, quan hệ công chúng, quản lý, CNTT, pháp lý và các phòng ban khác. Các chuyên gia an ninh tham gia vào CSIRT thường bao gồm ba vai trò chính liên quan đến an ninh:

1. **Nhà phân tích an ninh**
2. **Trưởng nhóm kỹ thuật**
3. **Điều phối viên sự cố**

|  |
| --- |
| **Security analyst** |

**Nhà phân tích an ninh**

|  |
| --- |
| The job of the **security** **analyst** is to continuously monitor an environment for any security threats. This includes:   * Analyzing and triaging alerts * Performing root-cause investigations * Escalating or resolving alerts   If a critical threat is identified, then analysts escalate it to the appropriate team lead, such as the technical lead. |

Công việc của **nhà phân tích bảo mật** là liên tục giám sát môi trường để tìm ra bất kỳ mối đe dọa bảo mật nào. Bao gồm:

* Phân tích và phân loại cảnh báo
* Thực hiện điều tra nguyên nhân gốc rễ
* Tăng cấp hoặc giải quyết cảnh báo

Nếu xác định được mối đe dọa nghiêm trọng, các nhà phân tích sẽ báo cáo lên trưởng nhóm thích hợp, chẳng hạn như trưởng nhóm kỹ thuật.

|  |
| --- |
| **Technical lead** |

**Trưởng nhóm kỹ thuật**

|  |
| --- |
| The job of the technical lead is to manage all of the technical aspects of the incident response process, such as applying software patches or updates. They do this by first determining the root cause of the incident. Then, they create and implement the strategies for containing, eradicating, and recovering from the incident. Technical leads often collaborate with other teams to ensure their incident response priorities align with business priorities, such as reducing disruptions for customers or returning to normal operations. |

Công việc của trưởng nhóm kỹ thuật là quản lý tất cả các khía cạnh kỹ thuật của quy trình ứng phó sự cố, chẳng hạn như áp dụng các bản vá hoặc cập nhật phần mềm. Họ thực hiện việc này bằng cách đầu tiên xác định nguyên nhân gốc rễ của sự cố. Sau đó, họ tạo và triển khai các chiến lược để ngăn chặn, loại bỏ và phục hồi sau sự cố. Trưởng nhóm kỹ thuật thường hợp tác với các nhóm khác để đảm bảo các ưu tiên ứng phó sự cố của họ phù hợp với các ưu tiên kinh doanh, chẳng hạn như giảm sự gián đoạn cho khách hàng hoặc quay trở lại hoạt động bình thường.

|  |
| --- |
| **Incident coordinator** |

**Điều phối viên sự cố**

|  |
| --- |
| Responding to an incident also requires cross-collaboration with nonsecurity professionals. CSIRTs will often consult with and leverage the expertise of members from external departments. The job of the incident coordinator is to coordinate with the relevant departments during a security incident. By doing so, the lines of communication are open and clear, and all personnel are made aware of the incident status. Incident coordinators can also be found in other teams, like the SOC. |

Phản ứng với một sự cố cũng đòi hỏi sự hợp tác chéo với các chuyên gia không chuyên về an ninh. CSIRT thường sẽ tham khảo ý kiến ​​và tận dụng chuyên môn của các thành viên từ các phòng ban bên ngoài. Nhiệm vụ của điều phối viên sự cố là phối hợp với các phòng ban có liên quan trong suốt sự cố an ninh. Bằng cách đó, các đường dây liên lạc được mở và rõ ràng, và tất cả nhân viên đều được thông báo về tình trạng sự cố. Điều phối viên sự cố cũng có thể được tìm thấy trong các nhóm khác, như SOC.

|  |
| --- |
| **Other roles** |

**Các vai trò khác**

|  |
| --- |
| Depending on the organization, many other roles can be found in a CSIRT, including a dedicated communications lead, a legal lead, a planning lead, and more. |

Tùy thuộc vào tổ chức, CSIRT có thể đảm nhiệm nhiều vai trò khác nhau, bao gồm người phụ trách truyền thông chuyên trách, người phụ trách pháp lý, người phụ trách lập kế hoạch, v.v.

|  |
| --- |
| **Note**: Teams, roles, responsibilities, and organizational structures can differ for each company. For example, some different job titles for incident coordinator include incident commander and incident manager. |

**Lưu ý** : Các nhóm, vai trò, trách nhiệm và cơ cấu tổ chức có thể khác nhau đối với mỗi công ty. Ví dụ, một số chức danh công việc khác nhau cho điều phối viên sự cố bao gồm chỉ huy sự cố và quản lý sự cố.

|  |
| --- |
| **Security operations center** |

**Trung tâm điều hành an ninh**

|  |
| --- |
| A **security operations center (SOC)** is an organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks. Structurally, a SOC (usually pronounced "sock") often exists as its own separate unit or within a CSIRT. You may be familiar with the term *blue team*, which refers to the security professionals who are responsible for defending against all security threats and attacks at an organization. A SOC is involved in various types of blue team activities, such as network monitoring, analysis, and response to incidents. |

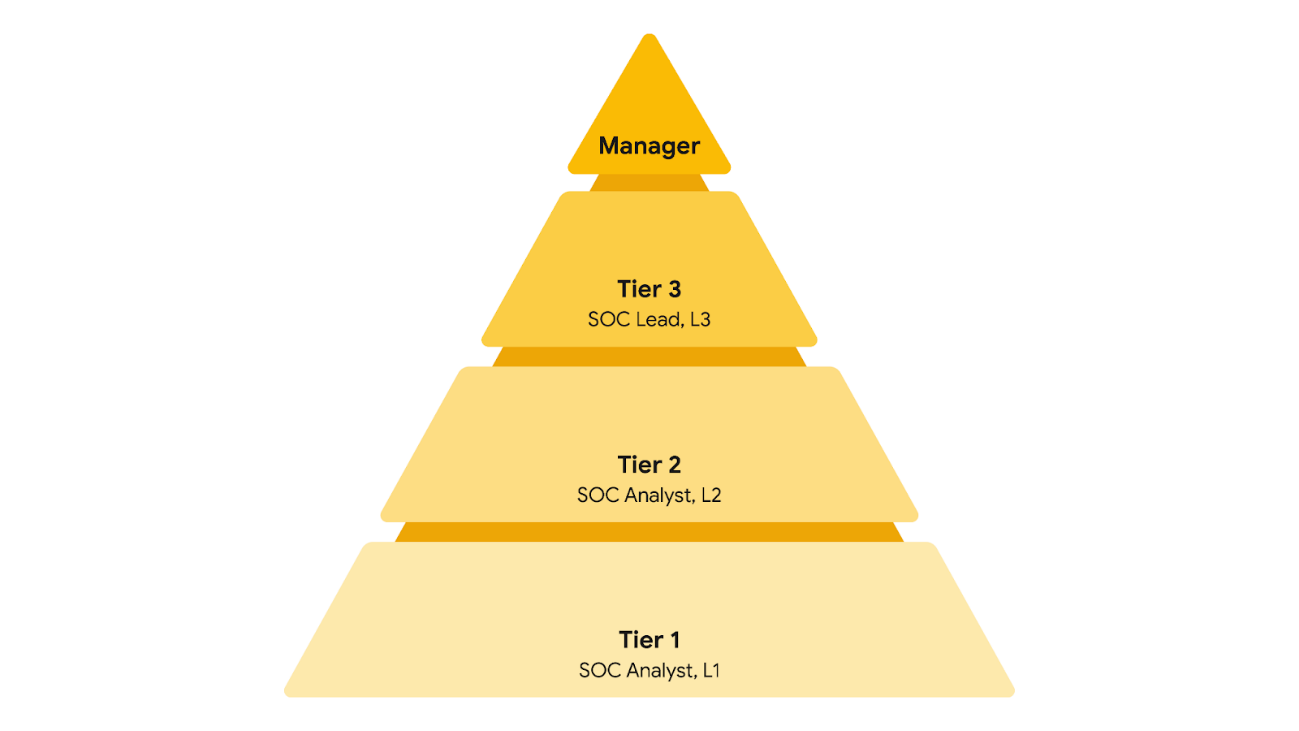
Trung **tâm hoạt động bảo mật (SOC)** là một đơn vị tổ chức chuyên giám sát mạng lưới, hệ thống và thiết bị để phát hiện các mối đe dọa hoặc tấn công bảo mật. Về mặt cấu trúc, SOC (thường được phát âm là "sock") thường tồn tại như một đơn vị riêng biệt hoặc trong một CSIRT. Bạn có thể quen thuộc với thuật ngữ *đội xanh* , dùng để chỉ các chuyên gia bảo mật chịu trách nhiệm phòng thủ chống lại mọi mối đe dọa và tấn công bảo mật tại một tổ chức. SOC tham gia vào nhiều loại hoạt động của đội xanh, chẳng hạn như giám sát mạng lưới, phân tích và ứng phó với các sự cố.

|  |
| --- |
| **SOC organization** |

**Tổ chức SOC**

|  |
| --- |
| A SOC is composed of SOC analysts, SOC leads, and SOC managers. Each role has its own respective responsibilities. SOC analysts are grouped into three different tiers. |

Một SOC bao gồm các nhà phân tích SOC, các trưởng nhóm SOC và các nhà quản lý SOC. Mỗi vai trò có trách nhiệm riêng. Các nhà phân tích SOC được nhóm thành ba cấp khác nhau.



|  |
| --- |
| **Tier 1 SOC analyst**  The first tier is composed of the least experienced SOC analysts who are known as level 1s (L1s). They are responsible for:   * Monitoring, reviewing, and prioritizing alerts based on criticality or severity * Creating and closing alerts using ticketing systems * Escalating alert tickets to Tier 2 or Tier 3 |

**Nhà phân tích SOC cấp 1**

Bậc đầu tiên bao gồm các nhà phân tích SOC ít kinh nghiệm nhất được gọi là cấp độ 1 (L1). Họ chịu trách nhiệm về:

* Theo dõi, xem xét và ưu tiên các cảnh báo dựa trên mức độ quan trọng hoặc nghiêm trọng
* Tạo và đóng cảnh báo bằng hệ thống vé
* Tăng mức cảnh báo lên Bậc 2 hoặc Bậc 3

|  |
| --- |
| **Tier 2 SOC analyst**  The second tier comprises the more experienced SOC analysts, or level 2s (L2s). They are responsible for:   * Receiving escalated tickets from L1 and conducting deeper investigations * Configuring and refining security tools * Reporting to the SOC Lead |

**Nhà phân tích SOC cấp 2**

Bậc thứ hai bao gồm các nhà phân tích SOC giàu kinh nghiệm hơn, hay cấp độ 2 (L2). Họ chịu trách nhiệm về:

* Nhận vé tăng cấp từ L1 và tiến hành điều tra sâu hơn
* Cấu hình và tinh chỉnh các công cụ bảo mật
* Báo cáo với Trưởng nhóm SOC

|  |
| --- |
| **Tier 3 SOC lead**  The third tier of a SOC is composed of the SOC leads, or level 3s (L3s). These highly experienced professionals are responsible for:   * Managing the operations of their team * Exploring methods of detection by performing advanced detection techniques, such as malware and forensics analysis * Reporting to the SOC manager |

**Người dẫn đầu SOC cấp 3**

Tầng thứ ba của SOC bao gồm các trưởng nhóm SOC hoặc cấp độ 3 (L3). Những chuyên gia giàu kinh nghiệm này chịu trách nhiệm về:

* Quản lý hoạt động của nhóm mình
* Khám phá các phương pháp phát hiện bằng cách thực hiện các kỹ thuật phát hiện tiên tiến, chẳng hạn như phân tích phần mềm độc hại và pháp y
* Báo cáo với người quản lý SOC

|  |
| --- |
| **SOC manager**  The SOC manager is at the top of the pyramid and is responsible for:   * Hiring, training, and evaluating the SOC team members * Creating performance metrics and managing the performance of the SOC team * Developing reports related to incidents, compliance, and auditing * Communicating findings to stakeholders such as executive management |

**Quản lý SOC**

Người quản lý SOC là người đứng đầu và chịu trách nhiệm về:

* Tuyển dụng, đào tạo và đánh giá các thành viên trong nhóm SOC
* Tạo số liệu đo lường hiệu suất và quản lý hiệu suất của nhóm SOC
* Phát triển các báo cáo liên quan đến sự cố, tuân thủ và kiểm toán
* Truyền đạt những phát hiện cho các bên liên quan như ban quản lý điều hành

|  |
| --- |
| **Other roles**  SOCs can also contain other specialized roles such as:   * **Forensic investigators**: Forensic investigators are commonly L2s and L3s who collect, preserve, and analyze digital evidence related to security incidents to determine what happened. * **Threat hunters**: Threat hunters are typically L3s who work to detect, analyze, and defend against new and advanced cybersecurity threats using threat intelligence.   **Note**: Just like CSIRTs, the organizational structure of a SOC can differ depending on the organization. |

**Các vai trò khác**

SOC cũng có thể chứa các vai trò chuyên biệt khác như:

* **Điều tra viên pháp y** : Điều tra viên pháp y thường là L2 và L3, những người thu thập, lưu giữ và phân tích bằng chứng kỹ thuật số liên quan đến các sự cố an ninh để xác định điều gì đã xảy ra.
* **Thợ săn mối đe dọa** : Thợ săn mối đe dọa thường là L3 làm việc để phát hiện, phân tích và phòng thủ chống lại các mối đe dọa an ninh mạng mới và tiên tiến bằng cách sử dụng thông tin tình báo về mối đe dọa.

**Lưu ý** : Giống như CSIRT, cơ cấu tổ chức của SOC có thể khác nhau tùy thuộc vào từng tổ chức.

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

**Những điểm chính**

|  |
| --- |
| As a security analyst, you will collaborate with your team members and people outside of your immediate team. Recognizing the organizational structure of an incident response team, such as a CSIRT or SOC, will help you understand how incidents move through their lifecycle and the responsibilities of different security roles throughout the process. Knowing the role that you and other professionals have during an incident response event will help you respond to challenging security situations by leveraging different perspectives and thinking of creative solutions. |

Với tư cách là một nhà phân tích bảo mật, bạn sẽ cộng tác với các thành viên trong nhóm và những người bên ngoài nhóm trực tiếp của bạn. Nhận biết cấu trúc tổ chức của nhóm ứng phó sự cố, chẳng hạn như CSIRT hoặc SOC, sẽ giúp bạn hiểu cách các sự cố di chuyển trong suốt vòng đời của chúng và trách nhiệm của các vai trò bảo mật khác nhau trong suốt quá trình. Biết được vai trò mà bạn và các chuyên gia khác có trong sự kiện ứng phó sự cố sẽ giúp bạn ứng phó với các tình huống bảo mật đầy thách thức bằng cách tận dụng các góc nhìn khác nhau và suy nghĩ về các giải pháp sáng tạo.

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

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| Here are some resources if you’d like to learn more about SOC organization or explore other incident response roles:   * [The security operations ecosystem](https://chronicle.security/blog/posts/soc-ecosystem-infographic/) * [Cyber career pathways tool](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool) * [Detection and Response](https://www.youtube.com/watch?v=QZ0cpBocl3c) at Google: Episode 2 of the [Hacking Google](https://www.youtube.com/playlist?list=PL590L5WQmH8dsxxz7ooJAgmijwOz0lh2H) series of videos |

Sau đây là một số tài nguyên nếu bạn muốn tìm hiểu thêm về tổ chức SOC hoặc khám phá các vai trò ứng phó sự cố khác:

* [Hệ sinh thái hoạt động an ninh](https://chronicle.security/blog/posts/soc-ecosystem-infographic/)
* [Công cụ định hướng nghề nghiệp an ninh mạng](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool)
* [Phát hiện và phản ứng](https://www.youtube.com/watch?v=QZ0cpBocl3c)tại Google: Tập 2 của[Hack Google](https://www.youtube.com/playlist?list=PL590L5WQmH8dsxxz7ooJAgmijwOz0lh2H)loạt video

***3.4. Incident response plans - Kế hoạch ứng phó sự cố***

|  |
| --- |
| So you've learned about incident response teams, the different types of roles, and their respective responsibilities. Now, let's talk about how teams respond to incidents using incident response plans. |

Vì vậy, bạn đã tìm hiểu về các nhóm ứng phó sự cố, các loại vai trò khác nhau vàtrách nhiệm của họ.Bây giờ, chúng ta hãy nói về cách các nhóm phản ứng với sự cố bằng cách sử dụng kế hoạch ứng phó sự cố.

|  |
| --- |
| When an incident occurs, incident response teams must be prepared to respond quickly, efficiently, and effectively. Whether it's a data breach, DDoS attack, or ransomware, incidents have the potential to cause significant damage to an organization. Like we previously mentioned, regulations may require organizations to report incidents within a certain timeframe. So it's crucial for organizations to have a formal incident response plan in place, so there's a prepared and consistent process to quickly respond to incidents once they occur. |

Khi sự cố xảy ra, các đội ứng phó sự cố phải chuẩn bị để phản ứng nhanh chóng,một cách hiệu quả và hiệu suất.Cho dù đó là vi phạm dữ liệu, tấn công DDoS hay phần mềm tống tiền,các sự cố có khả năng gây ra thiệt hại đáng kể cho một tổ chức.Như chúng tôi đã đề cập trước đó, các quy định có thể yêu cầu các tổ chức báo cáosự cố xảy ra trong một khoảng thời gian nhất định.Vì vậy, điều quan trọng đối với các tổ chức là phải có kế hoạch ứng phó sự cố chính thức,vì vậy có một sự chuẩn bị vàquy trình nhất quán để phản ứng nhanh với các sự cố khi chúng xảy ra.

|  |
| --- |
| You may remember learning that security plans consist of three basic elements: policies, standards, and procedures. An incident response plan is a document that outlines the procedures to take in each step of incident response. |

Bạn có thể nhớ rằng kế hoạch an ninh bao gồm ba yếu tố cơ bản:chính sách, tiêu chuẩn và thủ tục.Kế hoạch ứng phó sự cố là một tài liệu phác thảo các thủ tục cần thực hiệntừng bước ứng phó sự cố.

|  |
| --- |
| Response plans, just like response teams, are not all the same. Organizations tailor their plans to meet their unique requirements such as their mission, size, culture, industry, and structure. For example, smaller organizations may choose to include their incident response plan in their security plan, while others may choose to have them as separate documents. |

Các kế hoạch ứng phó, giống như các đội ứng phó, không phải tất cả đều giống nhau.Các tổ chức điều chỉnh kế hoạch của họ để đáp ứng các yêu cầu riêng của họchẳng hạn như sứ mệnh, quy mô, văn hóa, ngành công nghiệp và cơ cấu của họ.Ví dụ,các tổ chức nhỏ hơn có thể chọn đưa kế hoạch ứng phó sự cố của họ vàokế hoạch bảo mật của họ, trong khi những người khác có thể chọn lưu chúng dưới dạng các tài liệu riêng biệt.

|  |
| --- |
| Although not all incident plans are the same, there are common elements that they share. |

Mặc dù không phải tất cả các kế hoạch ứng phó sự cố đều giống nhau,có những yếu tố chung mà họ chia sẻ.

|  |
| --- |
| Incident plans have: Incident response procedures. These are step-by-step instructions on how to respond to incidents. System information. These are things like network diagrams, data flow diagrams, logging, and asset inventory information. And other documents like contact lists, forms, and templates. |

Kế hoạch ứng phó sự cố bao gồm: Quy trình ứng phó sự cố.Đây là hướng dẫn từng bước về cách ứng phó với sự cố.Thông tin hệ thống. Đây là những thứ như sơ đồ mạng,sơ đồ luồng dữ liệu, ghi nhật ký và thông tin kiểm kê tài sản.Và các tài liệu khác như danh sách liên lạc, biểu mẫu và mẫu.

|  |
| --- |
| Plans aren't perfect, and there's always room to adjust and improve as incidents occur. Incident processes and procedures must be regularly reviewed and tested. |

Kế hoạch không hoàn hảo và luôn có chỗ để điều chỉnh vàcải thiện khi sự cố xảy ra.Các quy trình và thủ tục xử lý sự cố phải được xem xét và kiểm tra thường xuyên.

|  |
| --- |
| This can be done through exercises like tabletops or simulations. These exercises ensure that all team members are familiar with the response plan. They also allow organizations to identify any missing gaps in a process to improve their incident response plan. Also, organizations may be required to complete specific types of exercises for regulatory reasons. |

Điều này có thể thực hiện được thông qua các bài tập như trên mặt bàn hoặc mô phỏng.Các bài tập này đảm bảo rằng tất cả các thành viên trong nhóm đều quen thuộcvới kế hoạch ứng phó.Chúng cũng cho phép các tổ chức xác định bất kỳ khoảng cách nào còn thiếu trong một quy trình để cải thiệnkế hoạch ứng phó sự cố của họ.Ngoài ra, các tổ chức có thể được yêu cầu hoàn thành các loại bài tập cụ thể cholý do pháp lý.

|  |
| --- |
| Coming up, we'll discuss the different types of tools used in incident response. |

Tiếp theo, chúng ta sẽ thảo luận về các loại công cụ khác nhau được sử dụng trong ứng phó sự cố.

***3.5. Test your knowledge: Incident response operations - Kiểm tra kiến thức của bạn: Hoạt động ứng phó sự cố***

**4. Incident response tools – Công cụ ứng phó sự cố**

***4.1. Incident response tools - Công cụ ứng phó sự cố***

|  |
| --- |
| As a security analyst, you'll play an important role in incident detection. After all, you're going to be at the front lines actively detecting threats. To do this, you'll not only rely on the security knowledge you've developed so far, but you'll also be using a variety of tools and technologies to support your investigations. |

Là một nhà phân tích an ninh,bạn sẽ đóng vai trò quan trọng trong việc phát hiện sự cố.Sau cùng, bạn sẽ ởtuyến đầu chủ động phát hiện các mối đe dọa.Để làm được điều này, bạn sẽ không chỉ dựa vàokiến thức bảo mật mà bạn đã phát triển cho đến nay,nhưng bạn cũng sẽ sử dụng nhiều công cụ khác nhau vàcông nghệ hỗ trợ cho cuộc điều tra của bạn.

|  |
| --- |
| A great carpenter doesn't just use a hammer to create a piece of furniture. They rely on a variety of tools in their toolbox to get the job done. They'll need to use a tape measure to measure dimensions, a saw to cut wood, and sandpaper to smooth the surface. |

Một thợ mộc giỏi không chỉ sử dụngmột cái búa để tạo ra một món đồ nội thất.Họ dựa vào nhiều công cụ khác nhau tronghộp công cụ của họ để hoàn thành công việc.Họ sẽ cần phải sử dụng thước dây để đo kích thước,một cái cưa để cắt gỗ,và giấy nhám để làm mịn bề mặt.

|  |
| --- |
| Likewise, as a security analyst, you won't be using a single tool to monitor, detect, and analyze events. You'll use detection and management tools to monitor system activity to identify events that require investigation. You'll use documentation tools to collect and compile evidence. And you'll also use different investigative tools for analyzing these events, like packet sniffers. New security technologies emerge, threats evolve, and attackers become stealthier to avoid detection. To become effective at detecting threats, you'll need to continuously expand your security toolbox. That's what makes the security field such an exciting one to be in. There's always something new to be learned. |

Tương tự như vậy, với tư cách là một nhà phân tích an ninh,bạn sẽ không sử dụng một công cụ duy nhất để giám sát,phát hiện và phân tích các sự kiện.Bạn sẽ sử dụng các công cụ phát hiện và quản lýđể theo dõi hoạt động của hệ thốngđể xác định những sự kiện cần điều tra.Bạn sẽ sử dụng các công cụ tài liệuđể thu thập và biên soạn bằng chứng.Và bạn cũng sẽ sử dụng các công cụ điều tra khác nhauđể phân tích các sự kiện này, giống như chương trình đánh hơi gói tin.Các công nghệ bảo mật mới xuất hiện, các mối đe dọa phát triển,và kẻ tấn công sẽ trở nên lén lút hơn để tránh bị phát hiện.Để có hiệu quả trong việc phát hiện các mối đe dọa,bạn sẽ cần phải liên tục mở rộng bộ công cụ bảo mật của mình.Đó là những gì làm cho lĩnh vực an ninhthật là thú vị khi tham gia.Luôn luôn có điều gì đó mới để học.

|  |
| --- |
| You might remember the incident handler's journal we shared with you from the previous section. You'll be using this journal as your own form of documentation as you work through the rest of this course. Consider this to be your first security tool to add to your toolbox. |

Bạn có thể nhớ nhật ký của người xử lý sự cốchúng tôi đã chia sẻ với bạn ở phần trước.Bạn sẽ sử dụng nhật ký này như một hình thức của riêng bạntài liệu khi bạn làm việctrong suốt phần còn lại của khóa học này.Hãy coi đây làcông cụ bảo mật đầu tiên bạn cần bổ sung vào hộp công cụ của mình.

***4.2. The value of documentation - Giá trị của tài liệu***

|  |
| --- |
| Hi there. Previously, you learned how an incident handler's journal is used for documenting the 5 W's of an incident: who, what, where, when, and why an incident occurred. In this section, we'll continue our discussion on documentation by exploring the different types of documentation, the importance of effective documentation, and we'll finish off with the discussion on documentation tools. |

Chào bạn.Trước đó, bạn đã học cách sử dụng nhật ký của người xử lý sự cố để ghi lại 5 chữ W củamột sự cố: ai, cái gì, ở đâu, khi nào và tại sao một sự cố xảy ra.Trong phần này, chúng ta sẽ tiếp tục thảo luận về tài liệu bằng cách khám phá cáccác loại tài liệu, tầm quan trọng của tài liệu hiệu quả, và chúng tôi sẽ kết thúcvới cuộc thảo luận về các công cụ ghi chép tài liệu.

|  |
| --- |
| Documentation is any form of recorded content that is used for a specific purpose. This can be audio, digital, or handwritten instructions, and even videos. There is no set industry standard for documentation, so many organizations set their own documentation practices. Regardless, documentation is meant to provide instruction and guidance on a specific topic. |

Tài liệu là bất kỳ hình thức nội dung được ghi lại nào được sử dụng chomột mục đích cụ thể.Có thể là hướng dẫn bằng âm thanh, kỹ thuật số, viết tay và thậm chí là video.Không có tiêu chuẩn công nghiệp nào được thiết lập cho tài liệu, vì vậynhiều tổ chức thiết lập các thông lệ ghi chép riêng của mình.Bất kể thế nào, tài liệu có mục đích cung cấp hướng dẫn và chỉ dẫnvề một chủ đề cụ thể.

|  |
| --- |
| There are also many types of documentation, and you may already be familiar with some of them from the previous lessons. These include playbooks, incident handler's journals, policies, plans, and final reports. Remember, there isn't an industry standard for documentation, which means that one organization's documentation practices may look completely different than another's. Often, organizations will tailor their documentation practices according to their needs and legal requirements. They may add, remove, or even merge documentation types. |

Ngoài ra còn có nhiều loại tài liệu,và có thể bạn đã quen thuộc với một số trong số chúng từ những bài học trước.Những điều này bao gồm sổ tay hướng dẫn, nhật ký xử lý sự cố, chính sách, kế hoạch,và báo cáo cuối cùng.Hãy nhớ rằng, không có một tiêu chuẩn công nghiệp nào cho tài liệu, điều đó có nghĩa là mộtThực hành lưu trữ tài liệu của một tổ chức có thể hoàn toàn khác so với tổ chức khác.Thông thường, các tổ chức sẽ điều chỉnh các hoạt động lập tài liệu của mình theo nhu cầu của họvà các yêu cầu pháp lý. Họ có thể thêm, xóa hoặc thậm chí hợp nhất các loại tài liệu.

|  |
| --- |
| Have you ever purchased a product, and didn't know how to use it, and consulted the product manual for instructions on how to do something like turn it on? Congrats, you've used documentation to solve an issue. |

Bạn đã bao giờ mua một sản phẩm, và không biết cách sử dụng nó, và được tư vấn chưa?hướng dẫn sử dụng sản phẩm để biết cách thực hiện một việc gì đó như bật sản phẩm lên?Xin chúc mừng, bạn đã sử dụng tài liệu để giải quyết vấn đề.

|  |
| --- |
| Previously, you've learned about how playbooks keep business operations safe, and in incident response, playbooks work similar to a product manual. As a refresher, a playbook is a manual that provides details about any operational action. You'll learn more about playbooks later. |

Trước đây, bạn đã tìm hiểu về cách các sổ tay hướng dẫn giữ cho hoạt động kinh doanh được an toàn,và trong ứng phó sự cố, sổ tay hướng dẫn hoạt động tương tự như hướng dẫn sử dụng sản phẩm.Để ôn lại,sổ tay hướng dẫn là một cuốn cẩm nang cung cấp thông tin chi tiết về bất kỳ hành động tác chiến nào.Bạn sẽ tìm hiểu thêm về sổ tay hướng dẫn sau.

|  |
| --- |
| Let's revisit that product manual example. Have you ever consulted a product manual for help and found yourself confused with the instructions and unable to get the help you needed? Whether it's had to do with unclear visuals and instructions or a confusing layout, you weren't able to use the documentation to solve your issue. This is an example of ineffective documentation. |

Chúng ta hãy xem lại ví dụ về hướng dẫn sử dụng sản phẩm đó.Bạn đã bao giờ tham khảo hướng dẫn sử dụng sản phẩm để được trợ giúp và thấy mình bối rối vớihướng dẫn nhưng không nhận được sự trợ giúp bạn cần?Cho dù nó có liên quan đến hình ảnh và hướng dẫn không rõ ràng hayBố cục khó hiểu, bạn không thể sử dụng tài liệu để giải quyết vấn đề của mình.Đây là một ví dụ về việc ghi chép tài liệu không hiệu quả.

|  |
| --- |
| Effective documentation reduces uncertainty and confusion. This is critical during a security incident when tensions are high and urgent response is required. As a security professional, you'll be using and creating documentation regularly. It's essential that the documentation you use and produce is clear, consistent, and accurate, so that you and your team can respond swiftly and decisively. |

Việc ghi chép hiệu quả sẽ làm giảm sự không chắc chắn và nhầm lẫn.Điều này rất quan trọng trong một sự cố an ninh khi căng thẳng lên cao vàcần phải có phản ứng khẩn cấp.Là một chuyên gia bảo mật, bạn sẽ sử dụng vàtạo tài liệu thường xuyên.Điều quan trọng là tài liệu bạn sử dụng và tạo ra phải rõ ràng, nhất quán,và chính xác, để bạn và nhóm của bạn có thể phản ứng nhanh chóng và quyết đoán.

|  |
| --- |
| Word processors are a common way to document. Some popular tools to use are Google Docs, OneNote, Evernote, and Notepad++. |

Trình xử lý văn bản là một cách phổ biến để lập tài liệu.Một số công cụ phổ biến để sử dụng là Google Docs, OneNote, Evernote và Notepad++.

|  |
| --- |
| Ticketing systems like Jira can also be used to document and track incidents. |

Các hệ thống ghi nhận sự cố như Jira cũng có thể được sử dụng để ghi lại và theo dõi các sự cố.

|  |
| --- |
| Lastly, Google Sheets, audio recorders, cameras, and handwritten notes are also tools you can use to document. |

Cuối cùng, Google Trang tính, máy ghi âm, máy ảnh vàghi chú viết tay cũng là công cụ bạn có thể sử dụng để ghi chép.

|  |
| --- |
| Our discussion on documentation has only just begun. Soon, you'll use your incident handler's journal to put your documentation skills to work. |

Cuộc thảo luận của chúng ta về tài liệu chỉ mới bắt đầu.Sớm thôi, bạn sẽ sử dụng nhật ký của người xử lý sự cố để ghi chép tài liệu của mìnhkỹ năng làm việc.

***4.3. Intrusion detection systems - Hệ thống phát hiện xâm nhập***

|  |
| --- |
| In this video, we'll introduce you to intrusion detection and intrusion prevention systems. |

Trong video này, chúng tôi sẽ giới thiệu cho bạnhệ thống phát hiện xâm nhập và ngăn chặn xâm nhập.

|  |
| --- |
| Imagine that you've just installed a home intrusion security system. You've installed intruder sensors for each entry and exit point in your home, including doors and windows. Those sensors work by sending out sound waves, and when an object touches a sound wave, the waves bounce back to your sensor and trigger an alert to your phone, notifying you that an intrusion was detected. |

Hãy tưởng tượng rằng bạn vừa cài đặthệ thống an ninh chống đột nhập nhà ở.Bạn đã cài đặt cảm biến đột nhập chomỗi lối vào và lối ra trong nhà bạn,bao gồm cửa ra vào và cửa sổ.Những cảm biến đó hoạt động bằng cách gửi rasóng âm, và khi một vật chạm vào sóng âm,những con sóng dội lạicảm biến của bạn và kích hoạt cảnh báo tới điện thoại của bạn,thông báo cho bạn biết rằng đã phát hiện có sự xâm nhập.

|  |
| --- |
| An intrusion detection system, or IDS, works in a very similar way to home intrusion sensors. An intrusion detection system is an application that monitors system and network activity, and produces alerts on possible intrusions. Like the home intrusion sensor, IDS collects and analyzes system information for abnormal activities. If something unusual is detected, the IDS sends out an alert to appropriate channels and personnel. |

Hệ thống phát hiện xâm nhập, hay IDS,hoạt động theo cách rất giống với cảm biến đột nhập gia đình.Hệ thống phát hiện xâm nhậplà một ứng dụng giám sáthoạt động của hệ thống và mạng, vàtạo cảnh báo về các cuộc xâm nhập có thể xảy ra.Giống như cảm biến xâm nhập nhà, IDS thu thập vàphân tích thông tin hệ thống để tìm ra các hoạt động bất thường.Nếu phát hiện có điều gì bất thường,IDS gửi ra một cảnh báođến các kênh và nhân sự thích hợp.

|  |
| --- |
| Now, imagine a jewelry storefront with a window sensor. When the sensor detects that the window's glass has been shattered, it triggers a steel roll-up door to automatically replace the shattered window and prevent unauthorized entry into the store. |

Bây giờ, hãy tưởng tượng một cửa hàng trang sức có cảm biến cửa sổ.Khi cảm biến phát hiện ra điều đókính cửa sổ đã bị vỡ,nó kích hoạt một cửa cuốn bằng thép để tự động thay thếcửa sổ vỡ và ngăn chặnxâm nhập trái phép vào cửa hàng.

|  |
| --- |
| This is what an intrusion prevention system does. Intrusion prevention systems, or IPS, have all the same capabilities as an IDS, but they can do more. They monitor system activity for intrusions and takes action to stop it. |

Đây chính là chức năng của hệ thống phòng chống xâm nhập.Hệ thống ngăn chặn xâm nhập, hay IPS,có tất cả các khả năng giống như một IDS,nhưng họ có thể làm được nhiều hơn thế.Họ theo dõi hoạt động của hệ thốngxâm nhập và có hành động ngăn chặn.

|  |
| --- |
| Many tools have the ability to perform the function of both IDS and IPS. Some popular tools are Snort, Zeek, Kismet, Sagan, and Suricata. We will be exploring Suricata in upcoming lessons. |

Nhiều công cụ có khả năng thực hiệnchức năng của cả IDS và IPS.Một số công cụ phổ biến là Snort,Zeek, Kismet, Sagan và Suricata.Chúng ta sẽ khám phá Suricata trong các bài học sắp tới.

|  |
| --- |
| You might be wondering, where do these alert notifications go? Well, coming up, we'll discuss how to manage alerts using security information and event management tools. |

Bạn có thể đang thắc mắc,những thông báo cảnh báo này sẽ được gửi đến đâu?Vâng, tiếp theo, chúng ta sẽ thảo luận về cách quản lý cảnh báosử dụng thông tin bảo mật và các công cụ quản lý sự kiện.

***4.4. Overview of detection tools - Tổng quan về các công cụ phát hiện***

|  |
| --- |
| **Overview of detection tools** |

**Tổng quan về các công cụ phát hiện**

|  |
| --- |
| Previously, you explored **intrusion detection system** (**IDS**) and **intrusion prevention system** (**IPS**) technologies. In this reading, you’ll compare and contrast these tools and learn about **endpoint detection and response** (**EDR**). As a security analyst, you'll likely work with these different tools, so it's important to understand their functions. |

Trước đó, bạn đã tìm hiểu về công nghệ **hệ thống phát hiện xâm nhập** ( **IDS** ) và **hệ thống ngăn chặn xâm nhập** ( **IPS ). Trong bài đọc này, bạn sẽ so sánh và đối chiếu các công cụ này và tìm hiểu về phát hiện và phản hồi điểm cuối** ( **EDR** ). Là một nhà phân tích bảo mật, bạn có thể sẽ làm việc với các công cụ khác nhau này, vì vậy, điều quan trọng là phải hiểu chức năng của chúng.

|  |
| --- |
| **Why you need detection tools** |

**Tại sao bạn cần công cụ phát hiện**

|  |
| --- |
| Detection tools work similarly to home security systems. Whereas home security systems monitor and protect homes against intrusion, cybersecurity detection tools help organizations protect their networks and systems against unwanted and unauthorized access. For organizations to protect their systems from security threats or attacks, they must be made aware when there is any indication of an intrusion. Detection tools make security professionals aware of the activity happening on a network or a system. The tools do this by continuously monitoring networks and systems for any suspicious activity. Once something unusual or suspicious is detected, the tool triggers an alert that notifies the security professional to investigate and stop the possible intrusion. |

Các công cụ phát hiện hoạt động tương tự như các hệ thống an ninh gia đình. Trong khi các hệ thống an ninh gia đình giám sát và bảo vệ ngôi nhà khỏi sự xâm nhập, các công cụ phát hiện an ninh mạng giúp các tổ chức bảo vệ mạng và hệ thống của họ khỏi sự truy cập không mong muốn và trái phép. Để các tổ chức bảo vệ hệ thống của mình khỏi các mối đe dọa hoặc tấn công an ninh, họ phải được thông báo khi có bất kỳ dấu hiệu nào của sự xâm nhập. Các công cụ phát hiện giúp các chuyên gia an ninh nhận biết được hoạt động đang diễn ra trên mạng hoặc hệ thống. Các công cụ thực hiện điều này bằng cách liên tục giám sát mạng và hệ thống để phát hiện bất kỳ hoạt động đáng ngờ nào. Khi phát hiện ra điều gì đó bất thường hoặc đáng ngờ, công cụ sẽ kích hoạt cảnh báo thông báo cho chuyên gia an ninh để điều tra và ngăn chặn sự xâm nhập có thể xảy ra.

|  |
| --- |
| **Detection tools** |

**Công cụ phát hiện**

|  |
| --- |
| As a security analyst, you'll likely encounter **IDS**, **IPS**, and **EDR** detection tools at some point, but it's important to understand the differences between them. Here is a comparison chart for quick reference: |

Là một nhà phân tích bảo mật, bạn có thể sẽ gặp phải các công cụ phát hiện **IDS** , **IPS** và **EDR** tại một số thời điểm, nhưng điều quan trọng là phải hiểu được sự khác biệt giữa chúng. Sau đây là biểu đồ so sánh để tham khảo nhanh:

|  |  |  |  |
| --- | --- | --- | --- |
| **Capability** | **IDS** | **IPS** | **EDR** |
| Detects malicious activity | ✓ | ✓ | ✓ |
| Prevents intrusions | N/A | ✓ | ✓ |
| Logs activity | ✓ | ✓ | ✓ |
| Generates alerts | ✓ | ✓ | ✓ |
| Performs behavioral analysis | N/A | N/A | ✓ |

|  |  |  |  |
| --- | --- | --- | --- |
| **Khả năng** | **IDS** | **IPS** | **EDR** |
| Phát hiện hoạt động độc hại | ✓ | ✓ | ✓ |
| Ngăn chặn sự xâm nhập | N/A | ✓ | ✓ |
| Nhật ký hoạt động | ✓ | ✓ | ✓ |
| Tạo cảnh báo | ✓ | ✓ | ✓ |
| Thực hiện phân tích hành vi | N/A | N/A | ✓ |

|  |
| --- |
| **Overview of IDS tools** |

**Tổng quan về các công cụ IDS**

|  |
| --- |
| An **intrusion detection system** (**IDS**) is an application that monitors system activity and alerts on possible intrusions. An IDS provides continuous monitoring of network events to help protect against security threats or attacks. The goal of an IDS is to detect potential malicious activity and generate an alert once such activity is detected. An IDS does *not* stop or prevent the activity. Instead, security professionals will investigate the alert and act to stop it, if necessary. |

Hệ **thống phát hiện xâm nhập** ( **IDS** ) là một ứng dụng giám sát hoạt động của hệ thống và cảnh báo về các cuộc xâm nhập có thể xảy ra. IDS cung cấp khả năng giám sát liên tục các sự kiện mạng để giúp bảo vệ chống lại các mối đe dọa hoặc tấn công bảo mật. Mục tiêu của IDS là phát hiện hoạt động độc hại tiềm ẩn và tạo cảnh báo khi phát hiện ra hoạt động đó. IDS không *dừng* hoặc ngăn chặn hoạt động. Thay vào đó, các chuyên gia bảo mật sẽ điều tra cảnh báo và hành động để ngăn chặn nếu cần thiết.

|  |
| --- |
| For example, an IDS can send out an alert when it identifies a suspicious user login, such as an unknown IP address logging into an application or a device at an unusual time. But, an IDS will not stop or prevent any further actions, like blocking the suspicious user login. |

Ví dụ, IDS có thể gửi cảnh báo khi xác định được người dùng đăng nhập đáng ngờ, chẳng hạn như địa chỉ IP không xác định đăng nhập vào ứng dụng hoặc thiết bị vào thời điểm bất thường. Nhưng IDS sẽ không dừng hoặc ngăn chặn bất kỳ hành động nào khác, chẳng hạn như chặn người dùng đăng nhập đáng ngờ.

|  |
| --- |
| Examples of IDS tools include Zeek, Suricata, Snort®, and Sagan. |

Ví dụ về các công cụ IDS bao gồm Zeek, Suricata, Snort® và Sagan.

|  |
| --- |
| **Detection categories**  As a security analyst, you will investigate alerts that an IDS generates. There are four types of detection categories you should be familiar with:   1. **A true positive** is an alert that correctly detects the presence of an attack. 2. **A true negative** is a state where there is no detection of malicious activity. This is when no malicious activity exists and no alert is triggered. 3. **A false positive** is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert. 4. **A false negative** is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to. |

**Các loại phát hiện**

Là một nhà phân tích bảo mật, bạn sẽ điều tra các cảnh báo mà IDS tạo ra. Có bốn loại danh mục phát hiện mà bạn nên biết:

1. **Kết quả dương tính thực sự** là cảnh báo phát hiện chính xác sự hiện diện của một cuộc tấn công.
2. **Tiêu cực thực sự** là trạng thái không phát hiện hoạt động độc hại. Đây là khi không có hoạt động độc hại nào tồn tại và không có cảnh báo nào được kích hoạt.
3. **Một cảnh báo dương tính giả** là một cảnh báo phát hiện không đúng sự hiện diện của mối đe dọa. Đây là khi một IDS xác định một hoạt động là độc hại, nhưng thực tế không phải vậy. Các cảnh báo dương tính giả gây bất tiện cho các nhóm bảo mật vì họ mất thời gian và nguồn lực để điều tra một cảnh báo bất hợp pháp.
4. **Kết quả âm tính giả** là trạng thái không phát hiện ra mối đe dọa. Đây là khi hoạt động độc hại xảy ra nhưng IDS không phát hiện ra. Kết quả âm tính giả rất nguy hiểm vì nhóm bảo mật không biết về các cuộc tấn công hợp pháp mà họ có thể dễ bị tấn công.

|  |
| --- |
| **Overview of IPS tools** |

**Tổng quan về các công cụ IPS**

|  |
| --- |
| An **intrusion prevention system** (**IPS**) is an application that monitors system activity for intrusive activity and takes action to stop the activity. An IPS works similarly to an IDS. But, IPS monitors system activity to detect and alert on intrusions, *and* it also takes action to *prevent* the activity and minimize its effects. For example, an IPS can send an alert and modify an access control list on a router to block specific traffic on a server. |

Hệ **thống ngăn chặn xâm nhập** ( **IPS** ) là một ứng dụng giám sát hoạt động của hệ thống để phát hiện hoạt động xâm nhập và thực hiện hành động để ngăn chặn hoạt động đó. IPS hoạt động tương tự như IDS. Nhưng IPS giám sát hoạt động của hệ thống để phát hiện và cảnh báo về các cuộc xâm nhập, *đồng thời* cũng thực hiện hành động để *ngăn chặn* hoạt động đó và giảm thiểu tác động của nó. Ví dụ, IPS có thể gửi cảnh báo và sửa đổi danh sách kiểm soát truy cập trên bộ định tuyến để chặn lưu lượng truy cập cụ thể trên máy chủ.

|  |
| --- |
| **Note:** Many IDS tools can also operate as an IPS. Tools like Suricata, Snort, and Sagan have both IDS and IPS capabilities. |

**Lưu ý:** Nhiều công cụ IDS cũng có thể hoạt động như IPS. Các công cụ như Suricata, Snort và Sagan có cả khả năng IDS và IPS.

|  |
| --- |
| **Overview of EDR tools** |

**Tổng quan về các công cụ EDR**

|  |
| --- |
| **Endpoint detection and response** (**EDR**) is an application that monitors an endpoint for malicious activity. EDR tools are installed on endpoints. Remember that an **endpoint** is any device connected on a network. Examples include end-user devices, like computers, phones, tablets, and more. |

**Endpoint detection and response** ( **EDR** ) là ứng dụng giám sát điểm cuối để tìm hoạt động độc hại. Các công cụ EDR được cài đặt trên điểm cuối. Hãy nhớ rằng **điểm cuối** là bất kỳ thiết bị nào được kết nối trên mạng. Ví dụ bao gồm các thiết bị của người dùng cuối, như máy tính, điện thoại, máy tính bảng, v.v.

|  |
| --- |
| EDR tools monitor, record, and analyze endpoint system activity to identify, alert, and respond to suspicious activity. Unlike IDS or IPS tools, EDRs collect endpoint activity data and perform *behavioral analysis* to identify threat patterns happening on an endpoint. Behavioral analysis uses the power of machine learning and artificial intelligence to analyze system behavior to identify malicious or unusual activity. EDR tools also use *automation* to stop attacks without the manual intervention of security professionals. For example, if an EDR detects an unusual process starting up on a user’s workstation that normally is not used, it can automatically block the process from running. |

Các công cụ EDR giám sát, ghi lại và phân tích hoạt động của hệ thống điểm cuối để xác định, cảnh báo và phản hồi hoạt động đáng ngờ. Không giống như các công cụ IDS hoặc IPS, EDR thu thập dữ liệu hoạt động của điểm cuối và thực hiện *phân tích hành vi* để xác định các kiểu đe dọa xảy ra trên điểm cuối. Phân tích hành vi sử dụng sức mạnh của máy học và trí tuệ nhân tạo để phân tích hành vi của hệ thống nhằm xác định hoạt động độc hại hoặc bất thường. Các công cụ EDR cũng sử dụng *tự động hóa* để ngăn chặn các cuộc tấn công mà không cần sự can thiệp thủ công của các chuyên gia bảo mật. Ví dụ: nếu EDR phát hiện ra một quy trình bất thường đang khởi động trên máy trạm của người dùng mà thông thường không được sử dụng, thì nó có thể tự động chặn quy trình đó chạy.

|  |
| --- |
| Tools like Open EDR®, Bitdefender™ Endpoint Detection and Response, and FortiEDR™ are examples of EDR tools. |

Các công cụ như Open EDR®, Bitdefender™ Endpoint Detection and Response và FortiEDR™ là những ví dụ về công cụ EDR.

|  |
| --- |
| **Note**: Security information and event management (SIEM) tools also have detection capabilities, which you'll explore later. |

**Lưu ý** : Các công cụ quản lý sự kiện và thông tin bảo mật (SIEM) cũng có khả năng phát hiện mà bạn sẽ khám phá sau.

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

**Những điểm chính**

|  |
| --- |
| Organizations deploy detection tools to gain awareness into the activity happening in their environments. IDS, IPS, and EDR are different types of detection tools. The value of detection tools is in their ability to detect, log, alert, and stop potential malicious activity. |

Các tổ chức triển khai các công cụ phát hiện để nâng cao nhận thức về hoạt động đang diễn ra trong môi trường của họ. IDS, IPS và EDR là các loại công cụ phát hiện khác nhau. Giá trị của các công cụ phát hiện nằm ở khả năng phát hiện, ghi nhật ký, cảnh báo và ngăn chặn hoạt động độc hại tiềm ẩn.

***4.5. Test your knowledge: Detection and documentation tools - Kiểm tra kiến thức của bạn: Công cụ phát hiện và ghi chép***

***4.6. Alert and event management with SIEM and SOAR tools - Quản lý cảnh báo và sự kiện bằng các công cụ SIEM và SOAR***

|  |
| --- |
| Our discussion on detection tools may have left you wondering where alerts are sent and how alerts are accessed by security analysts. This is where security information and event management, or SIEM, tools are used. |

Cuộc thảo luận của chúng tôi về các công cụ phát hiện có thể khiến bạn tự hỏi cảnh báo được gửi đến đâuvà cách các nhà phân tích bảo mật truy cập vào các cảnh báo.Đây là nơi sử dụng các công cụ quản lý sự kiện và thông tin bảo mật hay SIEM.

|  |
| --- |
| SIEM is a tool that collects and analyzes log data to monitor critical activities in an organization. SIEM provides security professionals with a high-level overview of what goes on in their networks. How exactly does it do this? |

SIEM là một công cụ thu thập vàphân tích dữ liệu nhật ký để theo dõi các hoạt động quan trọng trong một tổ chức.SIEM cung cấp cho các chuyên gia bảo mật cái nhìn tổng quan cấp cao về những gì diễn ra trongmạng lưới của họ.Chính xác thì nó làm được điều này như thế nào?

|  |
| --- |
| Let's use an example of a car. Cars have many different parts: tires, lights, and let's not forget all the internal machinery that's under the hood. There are many different components of a car, but how do you know if one of them has an issue? Aha, you guessed it! The dashboard warning lights. The dashboard notifies you about information related to the car's components, whether the tire pressure or battery voltage is low, you need to refuel, or a door hasn't been properly closed. A car's dashboard notifies you about the status of the car's components, so that you can take action to fix it. |

Chúng ta hãy lấy ví dụ về một chiếc ô tô.Xe ô tô có nhiều bộ phận khác nhau: lốp, đèn vàchúng ta đừng quên tất cả các máy móc bên trong nằm bên dưới mui xe.Có nhiều thành phần khác nhau của một chiếc ô tô,nhưng làm sao bạn biết được một trong số chúng có vấn đề?Aha, bạn đoán đúng rồi! Đèn cảnh báo trên bảng điều khiển.Bảng điều khiển thông báo cho bạn về thông tin liên quan đếncác bộ phận của xe, cho dù áp suất lốp hay điện áp ắc quy thấp,bạn cần tiếp nhiên liệu hoặc có cửa chưa được đóng đúng cách.Bảng điều khiển của ô tô thông báo cho bạn về tình trạng của các bộ phận trên ô tô, vì vậyđể bạn có thể hành động để khắc phục.

|  |
| --- |
| SIEM tools work in a similar way. Just like cars have many different components, a network can have thousands of different devices and systems, which make monitoring them quite the challenge. |

Các công cụ SIEM hoạt động theo cách tương tự.Giống như ô tô có nhiều thành phần khác nhau,một mạng có thể có hàng ngàn thiết bị khác nhau vàhệ thống, khiến cho việc giám sát chúng trở thành một thách thức khá lớn.

|  |
| --- |
| A car's dashboard gives the driver a clear picture of the status of their car, so they don't have to worry about inspecting each component themselves. |

Bảng điều khiển của ô tô cung cấp cho người lái xe hình ảnh rõ ràng về tình trạng của xe, vì vậyhọ không cần phải lo lắng về việc tự mình kiểm tra từng thành phần.

|  |
| --- |
| Similarly, a SIEM looks at data flows between all the different systems in the network and analyzes them to provide a real-time picture of any potential threats to the network. It does this by ingesting massive amounts of data and categorizes this data, so that it's easily accessible through a centralized platform similar to a car's dashboard. |

Tương tự như vậy, SIEM xem xét các luồng dữ liệu giữa tất cả các hệ thống khác nhau trongmạng lưới và phân tích chúng để cung cấp hình ảnh thời gian thực về bất kỳ mối đe dọa tiềm ẩn nàovào mạng.Nó thực hiện điều này bằng cách thu thập một lượng lớn dữ liệu và phân loại dữ liệu này, do đórằng nó có thể dễ dàng truy cập thông qua một nền tảng tập trung tương tự như ô tôbảng điều khiển.

|  |
| --- |
| Here's what the process looks like. First, SIEM tools collect and aggregate data. This data is typically in the form of logs, which are basically a record of all the events that happened on a given source. |

Quá trình này diễn ra như sau.Đầu tiên, các công cụ SIEM thu thập và tổng hợp dữ liệu.Dữ liệu này thường ở dạng nhật ký, về cơ bản là bản ghi chéptất cả các sự kiện xảy ra tại một nguồn nhất định.

|  |
| --- |
| Data can come from multiple sources such as IDS or IPS, databases, firewalls, applications, and more. After all this data gets collected, it gets aggregated. Aggregation simply means all this data from different data sources gets centralized in one place. |

Dữ liệu có thể đến từ nhiều nguồn như IDS hoặc IPS, cơ sở dữ liệu,tường lửa, ứng dụng và nhiều hơn nữa.Sau khi tất cả dữ liệu này được thu thập, chúng sẽ được tổng hợp lại.Tổng hợp đơn giản có nghĩa là tất cả dữ liệu này từ các nguồn dữ liệu khác nhau đượctập trung tại một nơi.

|  |
| --- |
| Depending on the number of data sources a SIEM collects from, a huge volume of raw unedited data can get collected. And not all data that's collected by a SIEM is relevant for security analysis purposes. |

Tùy thuộc vào số lượng nguồn dữ liệu mà SIEM thu thập,có thể thu thập được một khối lượng lớn dữ liệu thô chưa được chỉnh sửa.Và không phải tất cả dữ liệu được SIEM thu thập đều có liên quan đếnmục đích phân tích bảo mật.

|  |
| --- |
| Next, SIEM tools normalize data. Normalization takes the raw data that the SIEM has collected and cleans it up by removing non essential attributes so that only what's relevant is included. Data normalization also creates consistency in log records, which is helpful when you're searching for specific log information during incident investigation. |

Tiếp theo, các công cụ SIEM chuẩn hóa dữ liệu.Chuẩn hóa lấy dữ liệu thô mà SIEM đã thu thập và làm sạch nó bằng cáchloại bỏ các thuộc tính không cần thiết để chỉ giữ lại những gì có liên quan.Chuẩn hóa dữ liệu cũng tạo ra sự nhất quán trong các bản ghi nhật ký,điều này hữu ích khi bạn đang tìm kiếmthông tin nhật ký cụ thể trong quá trình điều tra sự cố.

|  |
| --- |
| Finally, the normalized data gets analyzed according to configured rules. SIEM analyzes the normalized data against a rule set to detect any possible security incidents, which then get categorized or reported as alerts for security analysts to review. |

Cuối cùng, dữ liệu đã chuẩn hóa sẽ được phân tích theo các quy tắc đã cấu hình.SIEM phân tích dữ liệu được chuẩn hóa theo một bộ quy tắc để phát hiện bất kỳ khả năng nàocác sự cố bảo mật, sau đó được phân loại hoặc báo cáo dưới dạng cảnh báocác nhà phân tích bảo mật để xem xét.

|  |
| --- |
| Now that you've explored the capabilities of SIEM tools, let's examine another security management tool. Security orchestration, automation, and response, or SOAR, is a collection of applications, tools, and workflows that uses automation to respond to security events. |

Bây giờ bạn đã khám phá được khả năng của các công cụ SIEM,hãy cùng xem xét một công cụ quản lý bảo mật khác.Điều phối an ninh, tự động hóa và phản hồi, hoặcSOAR là một tập hợp các ứng dụng, công cụ vàquy trình làm việc sử dụng tự động hóa để ứng phó với các sự kiện bảo mật.

|  |
| --- |
| While SIEM tools collect, analyze, and report on security events for security analysts to review, SOAR automates analysis and response to security events and incidents. SOAR can also be used to track and manage cases. Multiple incidents can form a case, and SOAR offers a way to view all of these incidents in one centralized place. |

Trong khi các công cụ SIEM thu thập, phân tích và báo cáo về các sự kiện bảo mật chocác nhà phân tích bảo mật để xem xét, SOAR tự động phân tích vàứng phó với các sự kiện và sự cố an ninh.SOAR cũng có thể được sử dụng để theo dõi và quản lý các trường hợp.Nhiều sự cố có thể hình thành một trường hợp, vàSOAR cung cấp giải pháp để xem tất cả các sự cố này tại một nơi tập trung.

|  |
| --- |
| Well, there you have it. You've learned how incident management tools like SIEM and SOAR make it easier for security analysts to see what's happening in a network and to respond to any threats efficiently. |

Vâng, bạn đã có nó rồi. Bạn đã biết cách các công cụ quản lý sự cố như SIEM và SOARgiúp các nhà phân tích bảo mật dễ dàng hơn trong việc xem những gì đang xảy ra trong mạng vàđể ứng phó hiệu quả với mọi mối đe dọa.

***4.7. Overview of SIEM technology - Tổng quan về công nghệ SIEM***

|  |
| --- |
| **Overview of SIEM technology** |

**Tổng quan về công nghệ SIEM**

|  |
| --- |
| Previously, you learned about the SIEM process. In this reading, you'll explore more about this process and why SIEM tools are an important part of incident detection and response. As a refresher, a **security information and event management** (**SIEM**) tool is an application that collects and analyzes log data to monitor critical activities in an organization. You might recall that SIEM tools help security analysts perform **log analysis** which is the process of examining logs to identify events of interest. |

Trước đây, bạn đã tìm hiểu về quy trình SIEM. Trong bài đọc này, bạn sẽ khám phá thêm về quy trình này và lý do tại sao các công cụ SIEM là một phần quan trọng của việc phát hiện và ứng phó sự cố. Để ôn lại, công cụ **quản lý sự kiện và thông tin bảo mật** ( **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. Bạn có thể nhớ lại rằng các công cụ SIEM giúp các nhà phân tích bảo mật thực hiện **phân tích nhật ký** , đây là quy trình kiểm tra nhật ký để xác định các sự kiện quan tâm.

|  |
| --- |
| **SIEM advantages** |

**Ưu điểm của SIEM**

|  |
| --- |
| SIEM tools collect and manage security-relevant data that can be used during investigations. This is important because SIEM tools provide awareness about the activity that occurs between devices on a network. The information SIEM tools provide can help security teams quickly investigate and respond to security incidents. SIEM tools have many advantages that can help security teams effectively respond to and manage incidents. Some of the advantages are:   * **Access to event data:** SIEM tools provide access to the event and activity data that happens on a network, including real-time activity. Networks can be connected to hundreds of different systems and devices. SIEM tools have the ability to ingest all of this data so that it can be accessed. * **Monitoring, detecting, and alerting:** SIEM tools continuously monitor systems and networks in real-time. They then analyze the collected data using detection rules to detect malicious activity. If an activity matches the rule, an alert is generated and sent out for security teams to assess. * **Log storage:** SIEM tools can act as a system for data retention, which can provide access to historical data. Data can be kept or deleted after a period depending on an organization's requirements. |

Các công cụ SIEM thu thập và quản lý dữ liệu liên quan đến bảo mật có thể được sử dụng trong quá trình điều tra. Điều này rất quan trọng vì các công cụ SIEM cung cấp nhận thức về hoạt động diễn ra giữa các thiết bị trên mạng. Thông tin mà các công cụ SIEM cung cấp có thể giúp các nhóm bảo mật nhanh chóng điều tra và ứng phó với các sự cố bảo mật. Các công cụ SIEM có nhiều ưu điểm có thể giúp các nhóm bảo mật ứng phó và quản lý sự cố hiệu quả. Một số ưu điểm là:

* **Truy cập dữ liệu sự kiện:** Các công cụ SIEM cung cấp quyền truy cập vào dữ liệu sự kiện và hoạt động diễn ra trên mạng, bao gồm hoạt động thời gian thực. Mạng có thể được kết nối với hàng trăm hệ thống và thiết bị khác nhau. Các công cụ SIEM có khả năng thu thập tất cả dữ liệu này để có thể truy cập.
* **Giám sát, phát hiện và cảnh báo:** Các công cụ SIEM liên tục giám sát hệ thống và mạng theo thời gian thực. Sau đó, chúng phân tích dữ liệu thu thập được bằng các quy tắc phát hiện để phát hiện hoạt động độc hại. Nếu một hoạt động khớp với quy tắc, một cảnh báo sẽ được tạo và gửi đi để các nhóm bảo mật đánh giá.
* **Lưu trữ nhật ký:** Các công cụ SIEM có thể hoạt động như một hệ thống lưu giữ dữ liệu, có thể cung cấp quyền truy cập vào dữ liệu lịch sử. Dữ liệu có thể được lưu giữ hoặc xóa sau một thời gian tùy thuộc vào yêu cầu của tổ chức.

|  |
| --- |
| **The SIEM process** |

**Quá trình SIEM**

|  |
| --- |
| The SIEM process consists of three critical steps:   1. **Collect and aggregate data** 2. **Normalize data** 3. **Analyze data** |

Quy trình SIEM bao gồm ba bước quan trọng:

1. **Thu thập và tổng hợp dữ liệu**
2. **Chuẩn hóa dữ liệu**
3. **Phân tích dữ liệu**

|  |
| --- |
| By understanding these steps, organizations can utilize the power of SIEM tools to gather, organize, and analyze security event data from different sources. Organizations can later use this information to improve their ability to identify and mitigate potential threats. |

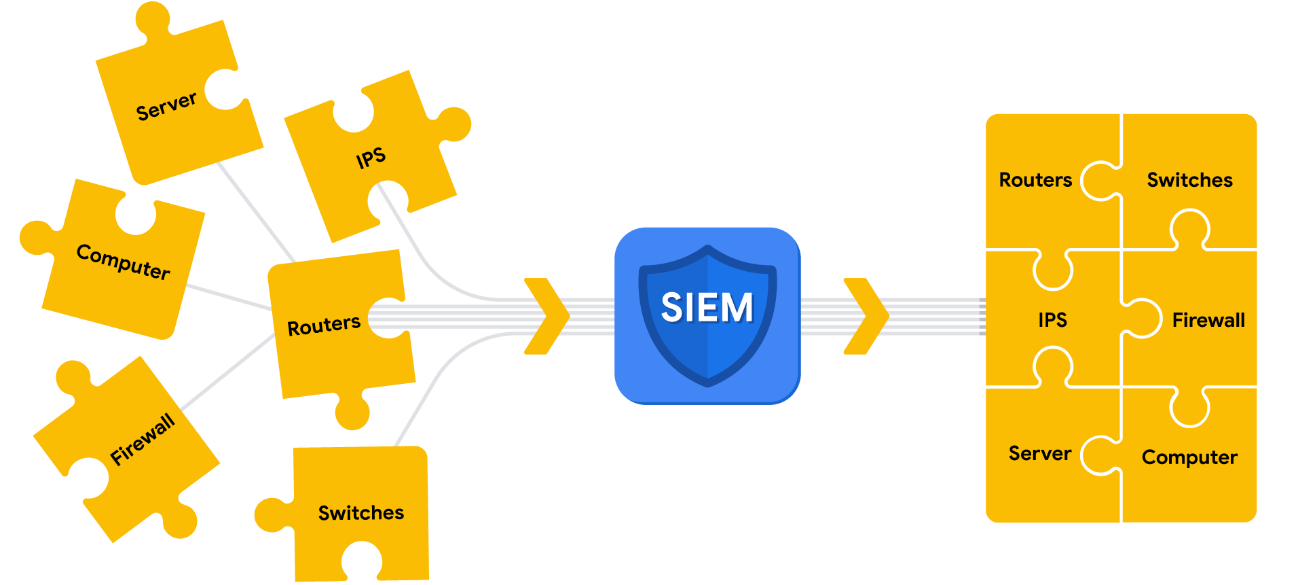
Bằng cách hiểu các bước này, các tổ chức có thể sử dụng sức mạnh của các công cụ SIEM để thu thập, sắp xếp và phân tích dữ liệu sự kiện bảo mật từ nhiều nguồn khác nhau. Các tổ chức sau đó có thể sử dụng thông tin này để cải thiện khả năng xác định và giảm thiểu các mối đe dọa tiềm ẩn.

|  |
| --- |
| **Collect and aggregate data** |

**Thu thập và tổng hợp dữ liệu**

|  |
| --- |
| SIEM tools require data for them to be effectively used. During the first step, the SIEM collects event data from various sources like firewalls, servers, routers, and more. This data, also known as logs, contains event details like timestamps, IP addresses, and more. **Logs** are a record of events that occur within an organization’s systems. After all of this log data is collected, it gets aggregated in one location. Aggregation refers to the process of consolidating log data into a centralized place. Through collection and aggregation, SIEM tools eliminate the need for manually reviewing and analyzing event data by accessing individual data sources. Instead, all event data is accessible in one location—the SIEM. |

Các công cụ SIEM cần dữ liệu để có thể sử dụng hiệu quả. Trong bước đầu tiên, SIEM thu thập dữ liệu sự kiện từ nhiều nguồn khác nhau như tường lửa, máy chủ, bộ định tuyến, v.v. Dữ liệu này, còn được gọi là nhật ký, chứa các chi tiết sự kiện như dấu thời gian, địa chỉ IP, v.v. **Nhật ký** là bản ghi các sự kiện xảy ra trong hệ thống của tổ chức. Sau khi tất cả dữ liệu nhật ký này được thu thập, chúng sẽ được tổng hợp tại một vị trí. Tổng hợp đề cập đến quá trình hợp nhất dữ liệu nhật ký vào một nơi tập trung. Thông qua việc thu thập và tổng hợp, các công cụ SIEM loại bỏ nhu cầu xem xét và phân tích dữ liệu sự kiện theo cách thủ công bằng cách truy cập các nguồn dữ liệu riêng lẻ. Thay vào đó, tất cả dữ liệu sự kiện đều có thể truy cập tại một vị trí—SIEM.



|  |
| --- |
| Parsing can occur during the first step of the SIEM process when data is collected and aggregated. *Parsing* maps data according to their fields and their corresponding values. For example, the following log example contains fields with values. At first, it might be difficult to interpret information from this log based on its format:  **April 3 11:01:21 server sshd[1088]: Failed password for user nuhara from 218.124.14.105 port 5023** |

Phân tích cú pháp có thể diễn ra trong bước đầu tiên của quy trình SIEM khi dữ liệu được thu thập và tổng hợp. *Phân tích* cú pháp ánh xạ dữ liệu theo các trường và giá trị tương ứng của chúng. Ví dụ, ví dụ nhật ký sau đây chứa các trường có giá trị. Lúc đầu, có thể khó diễn giải thông tin từ nhật ký này dựa trên định dạng của nó:

**April 3 11:01:21 server sshd[1088]: Failed password for user nuhara from 218.124.14.105 port 5023**

|  |
| --- |
| In a parsed format, the fields and values are extracted and paired making them easier to read and interpret:   * host = **server** * process = **sshd** * source\_user = **nuhara** * source ip = **218.124.14.105** * source port = **5023** |

Ở định dạng đã phân tích cú pháp, các trường và giá trị được trích xuất và ghép nối giúp chúng dễ đọc và diễn giải hơn:

* host = **server**
* process = **sshd**
* source\_user = **nuhara**
* source ip = **218.124.14.105**
* source port = **5023**

|  |
| --- |
| **Normalize data** |

**Chuẩn hóa dữ liệu**

|  |
| --- |
| SIEM tools collect data from many different sources. This data must be transformed into a single format so that it can be easily processed by the SIEM. However, each data source is different and data can be formatted in many different ways. For example, a firewall log can be formatted differently than a server log. |

Các công cụ SIEM thu thập dữ liệu từ nhiều nguồn khác nhau. Dữ liệu này phải được chuyển đổi thành một định dạng duy nhất để SIEM có thể dễ dàng xử lý. Tuy nhiên, mỗi nguồn dữ liệu là khác nhau và dữ liệu có thể được định dạng theo nhiều cách khác nhau. Ví dụ, nhật ký tường lửa có thể được định dạng khác với nhật ký máy chủ.



|  |
| --- |
| Collected event data should go through the process of normalization. *Normalization* converts data into a standard, structured format that is easily searchable. |

Dữ liệu sự kiện được thu thập phải trải qua quá trình chuẩn hóa. *Chuẩn hóa* chuyển đổi dữ liệu thành định dạng chuẩn, có cấu trúc, dễ tìm kiếm.

|  |
| --- |
| **Analyze data** |

**Phân tích dữ liệu**

|  |
| --- |
| After log data has been collected, aggregated, and normalized, the SIEM must do something useful with all of the data to enable security teams to investigate threats. During this final step in the process, SIEM tools analyze the data. Analysis can be done with some type of detection logic such as a set of rules and conditions. SIEM tools then apply these rules to the data, and if any of the log activity matches a rule, alerts are sent out to cybersecurity teams. |

Sau khi dữ liệu nhật ký đã được thu thập, tổng hợp và chuẩn hóa, SIEM phải thực hiện một số hành động hữu ích với tất cả dữ liệu để cho phép các nhóm bảo mật điều tra các mối đe dọa. Trong bước cuối cùng này của quy trình, các công cụ SIEM phân tích dữ liệu. Phân tích có thể được thực hiện với một số loại logic phát hiện như một tập hợp các quy tắc và điều kiện. Sau đó, các công cụ SIEM áp dụng các quy tắc này vào dữ liệu và nếu bất kỳ hoạt động nhật ký nào khớp với một quy tắc, các cảnh báo sẽ được gửi đến các nhóm an ninh mạng.

|  |
| --- |
| **Note**: A part of the analysis process includes correlation. *Correlation* involves the comparison of multiple log events to identify common patterns that indicate potential security threats. |

**Lưu ý** : Một phần của quá trình phân tích bao gồm tương quan. *Tương quan* liên quan đến việc so sánh nhiều sự kiện nhật ký để xác định các mẫu chung chỉ ra các mối đe dọa bảo mật tiềm ẩn.

|  |
| --- |
| **SIEM tools** |

**Công cụ SIEM**

|  |
| --- |
| There are many SIEM tools. The following are some SIEM tools commonly used in the cybersecurity industry:   * AlienVault® OSSIM™ * Chronicle * Elastic * Exabeam * IBM QRadar® Security Intelligence Platform * LogRhythm * Splunk |

Có nhiều công cụ SIEM. Sau đây là một số công cụ SIEM thường được sử dụng trong ngành an ninh mạng:

* AlienVault® OSSIM™
* Chronicle
* Elastic
* Exabeam
* IBM QRadar® Security Intelligence Platform
* LogRhythm
* Splunk

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

**Những điểm chính**

|  |
| --- |
| SIEM tools collect and organize enormous amounts of data to create meaningful insights for security teams. By understanding how SIEM tools work, what the process includes, and how organizations leverage them, you can contribute to efforts in detecting and responding to security incidents effectively. With this knowledge, you can assist in analyzing log data, identifying threats, and aiding incident response activities to help improve security posture and protect valuable assets from threats. |

Các công cụ SIEM thu thập và sắp xếp lượng dữ liệu khổng lồ để tạo ra những hiểu biết có ý nghĩa cho các nhóm bảo mật. Bằng cách hiểu cách thức hoạt động của các công cụ SIEM, quy trình bao gồm những gì và cách các tổ chức tận dụng chúng, bạn có thể đóng góp vào các nỗ lực phát hiện và ứng phó hiệu quả với các sự cố bảo mật. Với kiến ​​thức này, bạn có thể hỗ trợ phân tích dữ liệu nhật ký, xác định các mối đe dọa và hỗ trợ các hoạt động ứng phó sự cố để giúp cải thiện tình hình bảo mật và bảo vệ các tài sản có giá trị khỏi các mối đe dọa.

***4.8. Test your knowledge: Management tools - Kiểm tra kiến thức của bạn: Công cụ quản lý***

**5. Review: Introduction to detection and incident response – Đánh giá: Giới thiệu về phát hiện và ứng phó sự cố**

***5.1. Wrap-up - Tóm tắt***

|  |
| --- |
| Way to go! You made it through a new section, and you've learned a lot. |

Cố lên! Bạn đã vượt qua được rồimột phần mới và bạn đã học được rất nhiều điều.

|  |
| --- |
| As a refresher, we first covered the incident response lifecycle as a framework to support incident response processes. |

Để ôn lại, đầu tiên chúng ta đã đề cậpvòng đời phản ứng sự cố nhưmột khuôn khổ hỗ trợ các quy trình ứng phó sự cố.

|  |
| --- |
| You were also given your very own incident handler's journal for your incident investigations, which you'll continue to use throughout this course. |

Bạn cũng đã được trao tặng rất nhiềunhật ký của người xử lý sự cố riêngcho các cuộc điều tra sự cố của bạn,mà bạn sẽ tiếp tục sử dụng trong suốt khóa học này.

|  |
| --- |
| You explored how incident response teams operate together to respond to incidents using incident plans. |

Bạn đã khám phá cách các nhóm ứng phó sự cố hoạt độngcùng nhau ứng phó với các sự cố bằng cách sử dụng các kế hoạch ứng phó sự cố.

|  |
| --- |
| You also learned about the documentation, detection, and management tools used during incident response. |

Bạn cũng đã học về tài liệu, phát hiện,và các công cụ quản lý được sử dụng trong quá trình ứng phó sự cố.

|  |
| --- |
| Congrats on making it through the first part of your incident response journey. Coming up, we'll explore network monitoring. You'll also have the opportunity to apply your learning through the activities. I'll meet you in the next section. |

Xin chúc mừng vì đã vượt quaphần đầu tiên trong hành trình ứng phó sự cố của bạn.Tiếp theo, chúng ta sẽ khám phá về giám sát mạng.Bạn cũng sẽ có cơ hội đểáp dụng kiến ​​thức đã học thông qua các hoạt động.Tôi sẽ gặp lại bạn ở phần tiếp theo.

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

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

**Thuật ngữ trong mô-đun 1**

|  |
| --- |
| **Terms and definitions from Course 6, Module 1** |

**Các thuật ngữ và định nghĩa từ Khóa học 6, Mô-đun 1**

|  |
| --- |
| **Computer security incident response teams (CSIRT):** A specialized group of security professionals that are trained in incident management and response |

**Các nhóm ứng phó sự cố bảo mật máy tính (CSIRT):** Một nhóm chuyên gia bảo mật được đào tạo về quản lý và ứng phó sự cố

|  |
| --- |
| **Documentation:** Any form of recorded content that is used for a specific purpose |

**Tài liệu:** Bất kỳ hình thức nội dung được ghi lại nào được sử dụng cho một mục đích cụ thể

|  |
| --- |
| **Endpoint detection and response (EDR):** An application that monitors an endpoint for malicious activity |

**Phát hiện và phản hồi điểm cuối (EDR):** Một ứng dụng giám sát điểm cuối để tìm hoạt động độc hại

|  |
| --- |
| **Event:** An observable occurrence on a network, system, or device |

**Sự kiện:** Một hiện tượng có thể quan sát được trên mạng, hệ thống hoặc thiết bị

|  |
| --- |
| **False negative**: A state where the presence of a threat is not detected |

**Âm tính giả** : Trạng thái không phát hiện thấy sự hiện diện của mối đe dọa

|  |
| --- |
| **False positive:** An alert that incorrectly detects the presence of a threat |

**Dương tính giả:** Cảnh báo phát hiện sai sự hiện diện của mối đe dọa

|  |
| --- |
| **Incident:** An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies |

**Sự cố:** Một sự việc thực sự hoặc sắp xảy ra gây nguy hiểm, mà không có thẩm quyền hợp pháp, tính bảo mật, tính toàn vẹn hoặc tính khả dụng của thông tin hoặc hệ thống thông tin; hoặc cấu thành hành vi vi phạm hoặc đe dọa sắp xảy ra vi phạm pháp luật, chính sách bảo mật, quy trình bảo mật hoặc chính sách sử dụng được chấp nhận

|  |
| --- |
| **Incident handler’s journal:** A form of documentation used in incident response |

**Nhật ký xử lý sự cố:** Một hình thức tài liệu được sử dụng trong phản hồi sự cố

|  |
| --- |
| **Incident response plan:** A document that outlines the procedures to take in each step of incident response |

**Kế hoạch ứng phó sự cố:** Một tài liệu phác thảo các thủ tục cần thực hiện trong từng bước ứng phó sự cố

|  |
| --- |
| **Intrusion detection system (IDS):** An application that monitors system activity and alerts on possible intrusions |

**Hệ thống phát hiện xâm nhập (IDS):** Một ứng dụng giám sát hoạt động của hệ thống và cảnh báo về các cuộc xâm nhập có thể xảy ra

|  |
| --- |
| **Intrusion prevention system (IPS):** An application that monitors system activity for intrusive activity and takes action to stop the activity |

**Hệ thống ngăn chặn xâm nhập (IPS):** Một ứng dụng giám sát hoạt động của hệ thống để phát hiện hoạt động xâm nhập và thực hiện hành động để ngăn chặn hoạt động đó

|  |
| --- |
| **National Institute of Standards and Technology (NIST) Incident Response Lifecycle:** A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-incident activity |

**Vòng đời ứng phó sự cố của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST):** Một khuôn khổ ứng phó sự cố bao gồm bốn giai đoạn: Chuẩn bị; Phát hiện và Phân tích; Ngăn chặn, Diệt trừ và Phục hồi; và Hoạt động sau sự cố

|  |
| --- |
| **Playbook:** A manual that provides details about any operational action |

**Sổ tay hướng dẫn:** Một hướng dẫn cung cấp thông tin chi tiết về bất kỳ hành động tác chiến nào

|  |
| --- |
| **Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities in an organization |

**Quản lý thông tin và sự kiện 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 operations center (SOC):** An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks |

**Trung tâm điều hành bảo mật (SOC):** Một đơn vị tổ chức chuyên giám sát mạng, hệ thống và thiết bị để phát hiện các mối đe dọa hoặc tấn công bảo mật

|  |
| --- |
| **Security orchestration, automation, and response (SOAR):** A collection of applications, tools, and workflows that uses automation to respond to security events |

**Phối hợp, tự động hóa và phản hồi bảo mật (SOAR):** Một 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

|  |
| --- |
| **True negative:** A state where there is no detection of malicious activity |

**Âm tính thực sự:** Trạng thái không phát hiện hoạt động độc hại

|  |
| --- |
| **True positive** An alert that correctly detects the presence of an attack |

**Đúng là dương tính** Một cảnh báo phát hiện chính xác sự hiện diện của một cuộc tấn công

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

**Module 2: Network monitoring and analysis - Giám sát và phân tích mạng**

|  |
| --- |
| You will explore network analysis tools, commonly referred to as packet sniffers. In particular, you'll sniff the network and analyze packets for malicious threats. You'll also craft filtering commands to analyze the contents of captured packets. |

Bạn sẽ khám phá các công cụ phân tích mạng, thường được gọi là packet sniffer. Cụ thể, bạn sẽ sniff mạng và phân tích các gói tin để tìm ra các mối đe dọa độc hại. Bạn cũng sẽ tạo các lệnh lọc để phân tích nội dung của các gói tin đã thu thập được.

|  |
| --- |
| **Learning Objectives**   * Describe how network traffic analysis can help to detect, prevent, and respond to security incidents. * Use packet sniffing tools to capture and view network communications. * Analyze packets to interpret network communications. |

**Mục tiêu học tập**

* Mô tả cách phân tích lưu lượng mạng có thể giúp phát hiện, ngăn ngừa và ứng phó với các sự cố bảo mật.
* Sử dụng công cụ theo dõi gói tin để nắm bắt và xem thông tin liên lạc mạng.
* Phân tích các gói tin để giải thích thông tin liên lạc mạng.

**1. Understand network traffic – Hiểu lưu lượng mạng**

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

|  |
| --- |
| Welcome back! I'm so glad you're joining us. Previously, you were introduced to incident detection and response. You may also remember learning about networking from a previous course. |

Chào mừng bạn trở lại! Tôi rất vui vì bạn đã tham gia cùng chúng tôi.Trước đó, bạn đã được giới thiệu vớiphát hiện và ứng phó sự cố.Bạn cũng có thể nhớ lại việc học vềkết nối mạng từ khóa học trước.

|  |
| --- |
| To recap, you learned about how devices talk to each other using network protocols and the different types of network attacks. You also examined some network security best practices. |

Để tóm tắt lại, bạn đã học vềcách các thiết bị giao tiếp với nhausử dụng các giao thức mạng vàcác loại tấn công mạng khác nhau.Bạn cũng đã xem xét một số biện pháp bảo mật mạng tốt nhất.

|  |
| --- |
| Here, we'll expand on networking and shift our focus to network analysis. First, you'll examine network communications by exploring network traffic flows. Next, you'll learn about viewing and capturing network traffic using packet sniffers. Then, you'll be introduced to packet analysis, where you'll examine packet fields and decode communication between devices and networks. |

Ở đây, chúng tôi sẽ mở rộng về mạng lưới vàchuyển trọng tâm sang phân tích mạng.Đầu tiên, bạn sẽ kiểm tramạng lưới truyền thông bằngkhám phá luồng lưu lượng mạng.Tiếp theo, bạn sẽ học về cách xem vàthu thập lưu lượng mạng bằng cách sử dụng chương trình đánh hơi gói tin.Sau đó, bạn sẽ được giới thiệu về phân tích gói tin,nơi bạn sẽ kiểm tra các trường gói tin và giải mãgiao tiếp giữa các thiết bị và mạng.

|  |
| --- |
| As a security professional, you'll be tasked with monitoring networks and system infrastructure to detect malicious activities. And this section will provide you with the opportunity to develop your network and packet analysis skills. Are you ready to begin? Let's get started! |

Là một chuyên gia an ninh,bạn sẽ được giao nhiệm vụ giám sát mạng lưới vàcơ sở hạ tầng hệ thống để phát hiện các hoạt động độc hại.Và phần này sẽ cung cấp cho bạn cơ hội đểphát triển kỹ năng phân tích mạng và gói tin của bạn.Bạn đã sẵn sàng để bắt đầu chưa? Chúng ta hãy bắt đầu nhé!

***1.2. Casey: Apply soft skills in cybersecurity - Casey: Áp dụng các kỹ năng mềm trong an ninh mạng***

|  |
| --- |
| Hi, my name is Casey and I'm part of the Google Cloud Enterprise Security sales team. First of all, the biggest piece of advice I can give is: do it. I want you to be here. We need all the people. It's a non-stop, ever-changing world in cybersecurity, which is why it's such a fun place to be. We need more diversity in security. We need everybody participating. We need people with diversity of thought, diversity of backgrounds, diversity of perspectives. I think some of the most important soft skills in cybersecurity are, number 1, being able to clearly summarize what you're trying to say, massively important. One of the other soft skills that I think could even be more important than clear communication is working with an open mindset. The threat landscape is continuously changing. The threat actors, the bad actors, they never sleep, and so neither can we. One of the things that makes cybersecurity so fun, in my opinion, is because it changes constantly. And if we have a fixed mindset going in, and what I mean by a fixed mindset is, I think I know the answer to this, I think I understand exactly what's going on, we are absolutely going to miss the boat. We need to be able to always stay curious. And from a cybersecurity point of view, it's very important to leave no stone unturned. One of the best things about soft skills is that we all have them and we're already using them every single day. So every one of you that's watching this already has a head start in cybersecurity. |

Xin chào, tôi tên là Casey và tôi là một phần củanhóm bán hàng Google Cloud Enterprise Security.Trước hết, phần lớn nhấtlời khuyên tôi có thể đưa ra là: hãy làm đi.Tôi muốn bạn ở đây.Chúng tôi cần tất cả mọi người.Đó là một sự không ngừng nghỉ,thế giới an ninh mạng luôn thay đổi,đó là lý do tại sao đây lại là nơi thú vị đến vậy.Chúng ta cần sự đa dạng hơn về an ninh.Chúng tôi cần sự tham gia của mọi người.Chúng ta cần những người có tư tưởng đa dạng,sự đa dạng về xuất thân, sự đa dạng về quan điểm.Tôi nghĩ một số kỹ năng mềm quan trọng nhất trongan ninh mạng là số 1,có thể rõ ràngtóm tắt những gì bạn đang cố gắng nói, điều này cực kỳ quan trọng.Một trong những kỹ năng mềm khác mà tôinghĩ thậm chí có thể nhiều hơnquan trọng hơn giao tiếp rõ ràngđang làm việc với tư duy cởi mở.Bối cảnh mối đe dọa liên tục thay đổi.Những kẻ đe dọa, những kẻ xấu,họ không bao giờ ngủ và chúng ta cũng vậy.Một trong những điều làm cho an ninh mạng trở nên thú vị,Theo tôi, là vì nó thay đổi liên tục.Và nếu chúng ta có một tư duy cố định,và ý tôi muốn nói đến tư duy cố định là,Tôi nghĩ tôi biết câu trả lời cho câu hỏi này,Tôi nghĩ tôi hiểu chính xác những gì đang diễn ra,chúng ta chắc chắn sẽ bỏ lỡ cơ hội này.Chúng ta cần phải luôn duy trì sự tò mò.Và từ góc độ an ninh mạng,điều rất quan trọng là phải tìm ra mọi manh mối.Một trong những điều tốt nhất vềkỹ năng mềm là tất cả chúng ta đều cóvà chúng ta đã sử dụng chúng hàng ngày.Vì vậy, tất cả mọi người đang xemđiều này đã có bước khởi đầu thuận lợi trong an ninh mạng.

***1.3. The importance of network traffic flows - Tầm quan trọng của luồng lưu lượng mạng***

|  |
| --- |
| In many organizations, network communication travels over multiple networks in different countries and across different devices. Data can get unintentionally sent and stored in insecure places, like personal email inboxes or cloud storage platforms. Users trust that their data is safely and securely sent and stored. And it's the job of security professionals like you to help protect these communications in transit and at rest. |

Trong nhiều tổ chức, truyền thông mạng được truyền qua nhiềumạng lưới ở nhiều quốc gia khác nhau và trên nhiều thiết bị khác nhau.Dữ liệu có thể được gửi và lưu trữ một cách vô tình ở những nơi không an toàn,như hộp thư email cá nhân hoặc nền tảng lưu trữ đám mây.Người dùng tin tưởng rằng dữ liệu của họ được gửi và lưu trữ một cách an toàn và bảo mật.Và đó là công việc của các chuyên gia an ninh như bạn để giúp bảo vệ những thứ nàythông tin liên lạc khi đang di chuyển và khi dừng.

|  |
| --- |
| Previously, you may recall learning how to identify and secure critical assets through security controls like data classification and encryption. Coming up, we'll expand on this topic and examine how network traffic analysis can be used to monitor network activity and identify potential malicious activity. |

Trước đây, bạn có thể nhớ lại cách học cách xác định và bảo mật tài sản quan trọngthông qua các biện pháp kiểm soát bảo mật như phân loại và mã hóa dữ liệu.Tiếp theo, chúng tôi sẽ mở rộng chủ đề này và xem xét cách phân tích lưu lượng mạng có thểđược sử dụng để giám sát hoạt động mạng và xác định hoạt động độc hại tiềm ẩn.

|  |
| --- |
| So what is network traffic? Network traffic is the amount of data that moves across a network. While network data is the data that's transmitted between devices on a network. |

Vậy lưu lượng mạng là gì?Lưu lượng mạng là lượng dữ liệu di chuyển qua mạng.Trong khi dữ liệu mạng là dữ liệu được truyền giữa các thiết bị trên mạng.

|  |
| --- |
| Depending on the size of a network, there can be a huge volume of network traffic at any given moment. For example, in a large, multinational organization, there may be thousands of employees sending and receiving emails at any given time. That's a lot of network traffic. With such large volumes of traffic being produced, how do you know what's normal behavior, or what's unusual and requires investigation as a potential security incident? |

Tùy thuộc vào kích thước của mạng,có thể có một lượng lớn lưu lượng mạng tại bất kỳ thời điểm nào.Ví dụ, trong một tổ chức đa quốc gia lớn, có thể cócó hàng ngàn nhân viên gửi và nhận email tại bất kỳ thời điểm nào.Đó là lưu lượng mạng rất lớn.Với khối lượng giao thông lớn như vậy được tạo ra,làm sao bạn biết được hành vi nào là bình thường, hay hành vi nào là bất thường vàcần phải điều tra như một sự cố an ninh tiềm ẩn?

|  |
| --- |
| Imagine being stuck in unexpected traffic during your regular drive to work. And, as you move along, you realize something unusual caused the traffic, like a minor vehicle collision which slowed down the expected flow. On the road, we have certain expectations about traffic flows based on our commuting experience. Peak traffic patterns like morning and evening rush are normal and expected, while abnormal traffic during off-peak times reveals that something unexpected has happened, like a vehicle collision. |

Hãy tưởng tượng bạn đang bị kẹt xe bất ngờ khi đang lái xe đi làm.Và khi bạn di chuyển, bạn nhận ra có điều gì đó bất thường gây ra tình trạng tắc đường,giống như một vụ va chạm xe nhỏ làm chậm dòng chảy dự kiến.Trên đường,chúng ta có những kỳ vọng nhất định về lưu lượng giao thông dựa trên kinh nghiệm đi lại của mình.Các mô hình giao thông cao điểm như giờ cao điểm buổi sáng và buổi tối là bình thường và được mong đợi,trong khi lưu lượng giao thông bất thường trong thời gian ngoài giờ cao điểm cho thấy điều gì đóđã xảy ra sự cố bất ngờ, như va chạm xe cộ.

|  |
| --- |
| Network traffic works in the same way. By understanding how data should be flowing across the network, you can develop an understanding of expected network traffic flow. By knowing what's normal, you can easily spot what's abnormal. We can detect traffic abnormalities through observation to spot indicators of compromise, also known as IoC, which are observable evidence that suggests signs of a potential security incident. |

Lưu lượng mạng cũng hoạt động theo cách tương tự.Bằng cách hiểu cách dữ liệu nên được truyền qua mạng,bạn có thể hiểu được lưu lượng mạng dự kiến.Bằng cách biết được điều gì là bình thường, bạn có thể dễ dàng phát hiện ra điều gì là bất thường.Chúng ta có thể phát hiện ra những bất thường về giao thông thông qua việc quan sát để phát hiện các chỉ sốcủa sự thỏa hiệp, còn được gọi là IoC, là bằng chứng có thể quan sát được rằnggợi ý dấu hiệu của một sự cố an ninh tiềm ẩn.

|  |
| --- |
| Take, for instance, data exfiltration, which is the unauthorized transmission of data from a system. Attackers use data exfiltration to steal or leak data such as user names, passwords, or intellectual property. By observing network traffic, we can determine if there's any indicators of compromise, such as large volumes of outbound traffic leaving a host. This is a sign of possible data exfiltration which can be further investigated. |

Lấy ví dụ, việc rò rỉ dữ liệu,là hành vi truyền dữ liệu trái phép từ một hệ thống.Kẻ tấn công sử dụng việc rò rỉ dữ liệu để đánh cắp hoặc rò rỉ dữ liệu như tên người dùng,mật khẩu hoặc sở hữu trí tuệ.Bằng cách quan sát lưu lượng mạng, chúng ta có thể xác định xem có bất kỳ chỉ số nào vềsự thỏa hiệp, chẳng hạn như khối lượng lớn lưu lượng truy cập đi ra khỏi máy chủ.Đây là dấu hiệu của việc rò rỉ dữ liệu có thể xảy rađược điều tra thêm.

|  |
| --- |
| Understanding and monitoring network traffic for inconsistencies is an important aspect of a security professional's job. Coming up, we'll explore what a data exfiltration attack looks like in real-time. Meet you there. |

Hiểu và giám sát lưu lượng mạng chosự không nhất quán là một khía cạnh quan trọng trong công việc của một chuyên gia an ninh.Sắp tới,chúng ta sẽ khám phá xem một cuộc tấn công đánh cắp dữ liệu diễn ra như thế nào trong thời gian thực.Gặp bạn ở đó nhé.

***1.4. Maintain awareness with network monitoring - Duy trì nhận thức với giám sát mạng***

|  |
| --- |
| **Maintain awareness with network monitoring** |

**Duy trì nhận thức với giám sát mạng**

|  |
| --- |
| Network communication can be noisy! Events like sending an email, streaming a video, or visiting a website all produce network communications in the form of network traffic and network data. As a reminder, **network traffic** is the amount of data that moves across a network. It can also include the type of data that is transferred, such as HTTP. **Network** **data** is the data that's transmitted between devices on a network. |

Giao tiếp mạng có thể bị nhiễu! Các sự kiện như gửi email, phát trực tuyến video hoặc truy cập trang web đều tạo ra giao tiếp mạng dưới dạng lưu lượng mạng và dữ liệu mạng. Xin nhắc lại, **lưu lượng mạng** là lượng dữ liệu di chuyển qua mạng. Nó cũng có thể bao gồm loại dữ liệu được truyền, chẳng hạn như HTTP. **Dữ liệu mạng** là dữ liệu được truyền giữa các thiết bị trên mạng.

|  |
| --- |
| Network monitoring is essential in maintaining situational awareness of any activity on a network. By collecting and analyzing network traffic, organizations can detect suspicious network activity. But before networks can be monitored, you must know exactly what to monitor. In this reading, you'll learn more about the importance of network monitoring, ways to monitor your network, and network monitoring tools. |

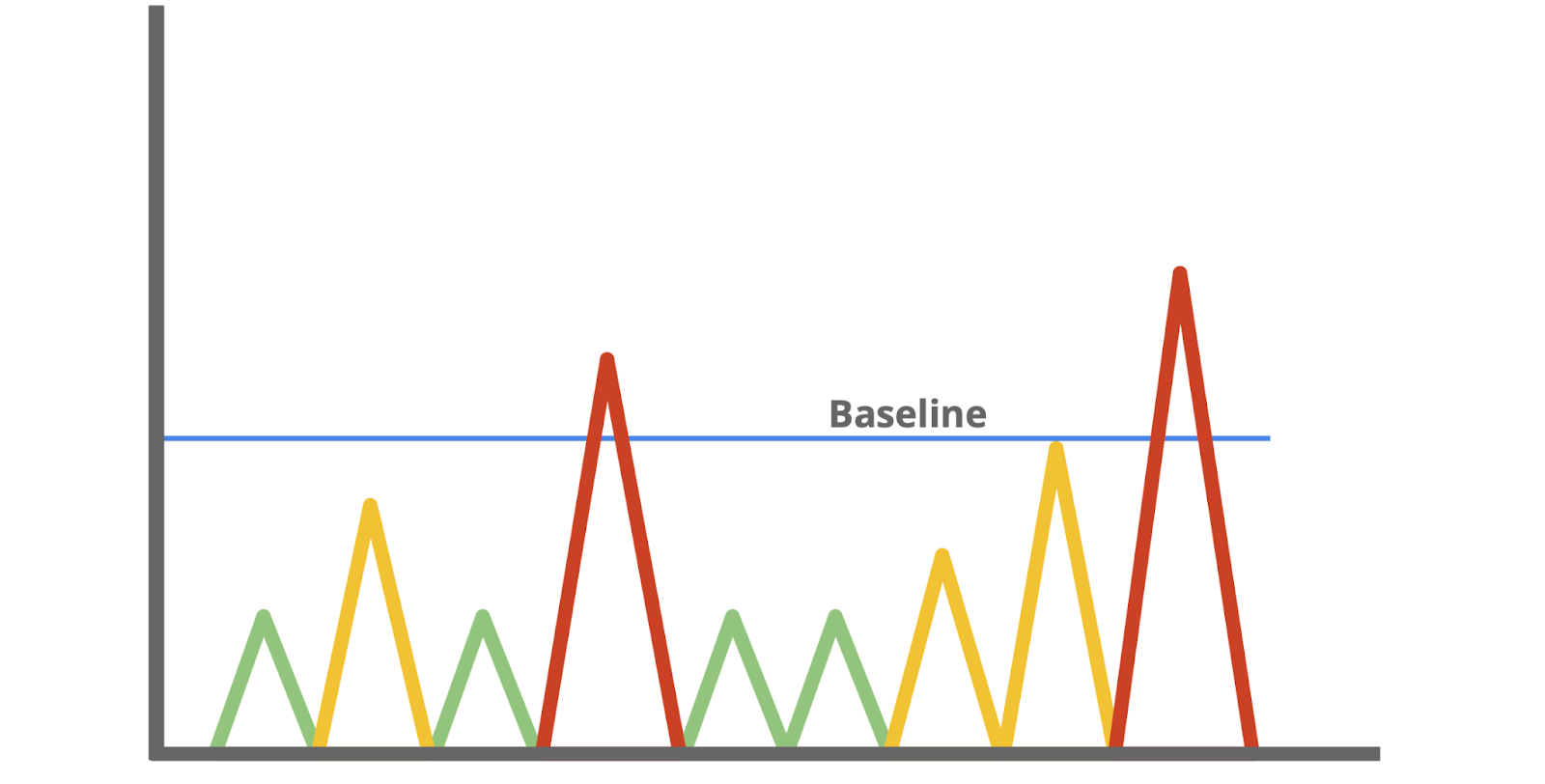
Giám sát mạng là điều cần thiết để duy trì nhận thức tình huống về bất kỳ hoạt động nào trên mạng. Bằng cách thu thập và phân tích lưu lượng mạng, các tổ chức có thể phát hiện hoạt động mạng đáng ngờ. Nhưng trước khi có thể giám sát mạng, bạn phải biết chính xác những gì cần giám sát. Trong bài đọc này, bạn sẽ tìm hiểu thêm về tầm quan trọng của giám sát mạng, cách giám sát mạng và các công cụ giám sát mạng.

|  |
| --- |
| **Know your network** |

**Biết mạng lưới của bạn**

|  |
| --- |
| As you’ve learned, networks connect devices, and devices then communicate and exchange data using network protocols. Network communications provide information about connections such as source and destination IP addresses, amount of data transferred, date and time, and more. This information can be valuable for security professionals when developing a **baseline** of normal or expected behavior. |

Như bạn đã biết, mạng kết nối các thiết bị và sau đó các thiết bị giao tiếp và trao đổi dữ liệu bằng giao thức mạng. Giao tiếp mạng cung cấp thông tin về các kết nối như địa chỉ IP nguồn và đích, lượng dữ liệu được truyền, ngày giờ, v.v. Thông tin này có thể có giá trị đối với các chuyên gia bảo mật khi xây dựng **đường cơ sở** về hành vi bình thường hoặc dự kiến.



|  |
| --- |
| A baseline is a reference point that’s used for comparison. You've probably encountered or used baselines at some point. For example, a grocery amount for a personal budget is an example of a baseline that can be used to help identify any patterns or changes in spending habits. In security, baselines help establish a standard of expected or normal behavior for systems, devices, and networks. Essentially, by knowing the baseline of *normal* network behavior, you'll be better able to identify *abnormal* network behavior. |

Đường cơ sở là điểm tham chiếu được sử dụng để so sánh. Có thể bạn đã từng gặp hoặc sử dụng đường cơ sở tại một thời điểm nào đó. Ví dụ, số tiền mua sắm tạp hóa cho ngân sách cá nhân là một ví dụ về đường cơ sở có thể được sử dụng để giúp xác định bất kỳ mô hình hoặc thay đổi nào trong thói quen chi tiêu. Trong bảo mật, đường cơ sở giúp thiết lập tiêu chuẩn về hành vi bình thường hoặc mong đợi cho các hệ thống, thiết bị và mạng. Về cơ bản, bằng cách biết đường cơ sở của hành vi mạng *bình thường* , bạn sẽ có thể xác định hành vi mạng *bất thường* tốt hơn .

|  |
| --- |
| **Monitor your network** |

**Giám sát mạng của bạn**

|  |
| --- |
| Once you’ve determined a baseline, you can monitor a network to identify any deviations from that baseline. Monitoring involves examining network components to detect unusual activities, such as large and unusual data transfers. Here are examples of network components that can be monitored to detect malicious activity: |

Sau khi xác định được đường cơ sở, bạn có thể giám sát mạng để xác định bất kỳ sự sai lệch nào so với đường cơ sở đó. Giám sát bao gồm việc kiểm tra các thành phần mạng để phát hiện các hoạt động bất thường, chẳng hạn như các lần truyền dữ liệu lớn và bất thường. Sau đây là các ví dụ về các thành phần mạng có thể được giám sát để phát hiện hoạt động độc hại:

|  |
| --- |
| **Flow analysis** |

**Phân tích dòng chảy**

|  |
| --- |
| Flow refers to the movement of network communications and includes information related to packets, protocols, and ports. Packets can travel to ports, which receive and transmit communications. Ports are often, but not always, associated with network protocols. For example, port 443 is commonly used by HTTPS which is a protocol that provides website traffic encryption. |

Flow đề cập đến sự di chuyển của các thông tin liên lạc mạng và bao gồm thông tin liên quan đến các gói tin, giao thức và cổng. Các gói tin có thể di chuyển đến các cổng, nơi nhận và truyền thông tin liên lạc. Các cổng thường, nhưng không phải lúc nào cũng, được liên kết với các giao thức mạng. Ví dụ, cổng 443 thường được sử dụng bởi HTTPS, đây là giao thức cung cấp mã hóa lưu lượng truy cập trang web.

|  |
| --- |
| However, malicious actors can use protocols and ports that are not commonly associated to maintain communications between the compromised system and their own machine. These communications are what’s known as **command and control (C2)**,which are the techniques used by malicious actors to maintain communications with compromised systems. |

Tuy nhiên, những kẻ tấn công có thể sử dụng các giao thức và cổng không thường được liên kết để duy trì liên lạc giữa hệ thống bị xâm phạm và máy của chúng. Những liên lạc này được gọi là **lệnh và điều khiển (C2)** , tức là các kỹ thuật mà những kẻ tấn công có hại sử dụng để duy trì liên lạc với các hệ thống bị xâm phạm.

|  |
| --- |
| For example, malicious actors can use HTTPS protocol over port 8088 as opposed to its commonly associated port 443 to communicate with compromised systems. Organizations must know which ports should be open and approved for connections, and watch out for any mismatches between ports and their associated protocols. |

Ví dụ, các tác nhân độc hại có thể sử dụng giao thức HTTPS qua cổng 8088 thay vì cổng 443 thường được liên kết để giao tiếp với các hệ thống bị xâm phạm. Các tổ chức phải biết cổng nào nên được mở và chấp thuận để kết nối, đồng thời cảnh giác với bất kỳ sự không khớp nào giữa các cổng và các giao thức liên quan của chúng.

|  |
| --- |
| **Packet payload information** |

**Thông tin tải trọng gói tin**

|  |
| --- |
| Network packets contain components related to the transmission of the packet. This includes details like source and destination IP address, and the packet payload information, which is the actual data that’s transmitted. Often, this data is encrypted and requires decryption for it to be readable. Organizations can monitor the payload information of packets to uncover unusual activity, such as sensitive data transmitting outside of the network, which could indicate a possible data exfiltration attack. |

Các gói mạng chứa các thành phần liên quan đến việc truyền gói. Bao gồm các chi tiết như địa chỉ IP nguồn và đích, và thông tin tải trọng gói, là dữ liệu thực tế được truyền. Thông thường, dữ liệu này được mã hóa và cần giải mã để có thể đọc được. Các tổ chức có thể theo dõi thông tin tải trọng của các gói để phát hiện hoạt động bất thường, chẳng hạn như dữ liệu nhạy cảm được truyền ra bên ngoài mạng, có thể chỉ ra một cuộc tấn công rò rỉ dữ liệu có thể xảy ra.

|  |
| --- |
| **Temporal patterns** |

**Mẫu thời gian**

|  |
| --- |
| Network packets contain information relating to time. This information is useful in understanding time patterns. For example, a company operating in North America experiences bulk traffic flows between 9 a.m. to 5 p.m., which is the baseline of normal network activity. If large volumes of traffic are suddenly outside of the normal hours of network activity, then this is considered *off baseline* and should be investigated. |

Các gói mạng chứa thông tin liên quan đến thời gian. Thông tin này hữu ích trong việc hiểu các mẫu thời gian. Ví dụ, một công ty hoạt động ở Bắc Mỹ có lưu lượng truy cập lớn từ 9 giờ sáng đến 5 giờ chiều, đây là thời gian cơ sở của hoạt động mạng bình thường. Nếu lưu lượng truy cập lớn đột nhiên nằm ngoài giờ hoạt động mạng bình thường, thì điều này được coi là *ngoài thời gian cơ sở* và cần được điều tra.

|  |
| --- |
| Through network monitoring, organizations can promptly detect network intrusions and work to prevent them from happening by securing network components. |

Thông qua giám sát mạng, các tổ chức có thể phát hiện kịp thời các cuộc xâm nhập mạng và ngăn chặn chúng xảy ra bằng cách bảo mật các thành phần mạng.

|  |
| --- |
| **Protect your network** |

**Bảo vệ mạng của bạn**

|  |
| --- |
| In this program, you’ve learned about **security operations centers** (**SOC**) and their role in monitoring systems against security threats and attacks. Organizations may deploy a **network operations center** (**NOC**), which is an organizational unit that monitors the performance of a network and responds to any network disruption, such as a network outage. While a SOC is focused on maintaining the security of an organization through detection and response, a NOC is responsible for maintaining network performance, availability, and uptime. |

Trong chương trình này, bạn đã tìm hiểu về **các trung tâm hoạt động bảo mật** ( **SOC** ) và vai trò của chúng trong việc giám sát các hệ thống chống lại các mối đe dọa và tấn công bảo mật. Các tổ chức có thể triển khai một **trung tâm hoạt động mạng** ( **NOC** ), đây là một đơn vị tổ chức giám sát hiệu suất của mạng và phản hồi bất kỳ sự gián đoạn mạng nào, chẳng hạn như sự cố mất mạng. Trong khi SOC tập trung vào việc duy trì tính bảo mật của một tổ chức thông qua phát hiện và phản hồi, NOC chịu trách nhiệm duy trì hiệu suất, tính khả dụng và thời gian hoạt động của mạng.



|  |
| --- |
| Security analysts monitor networks to identify any signs of potential security incidents known as **indicators of compromise** (**IoC**) and  protect networks from threats or attacks. To do this, they must understand the environment that network communications travel through so that they can identify deviations in network traffic. |

Các nhà phân tích bảo mật giám sát mạng để xác định bất kỳ dấu hiệu nào của các sự cố bảo mật tiềm ẩn được gọi là **chỉ số xâm phạm** ( **IoC** ) và bảo vệ mạng khỏi các mối đe dọa hoặc tấn công. Để làm được điều này, họ phải hiểu môi trường mà các thông tin liên lạc mạng đi qua để có thể xác định các sai lệch trong lưu lượng mạng.

|  |
| --- |
| **Network monitoring tools** |

**Công cụ giám sát mạng**

|  |
| --- |
| Network monitoring can be automated or performed manually. Some common network monitoring tools can include:   * **Intrusion detection systems** (**IDS**) monitor system activity and alert on possible intrusions. An IDS will detect and alert on the deviations you’ve configured it to detect. Most commonly, IDS tools will monitor the content of packet payload to detect patterns associated with threats such as malware or phishing attempts. * **Network protocol analyzers**, also known as packet sniffers, are tools designed to capture and analyze data traffic within a network. They can be used to analyze network communications manually in detail. Examples include tools such as tcpdump and Wireshark, which can be used by security professionals to record network communications through packet captures. Packet captures can then be investigated to identify potentially malicious activity. |

Giám sát mạng có thể được tự động hóa hoặc thực hiện thủ công. Một số công cụ giám sát mạng phổ biến có thể bao gồm:

* **Hệ thống phát hiện xâm nhập** ( **IDS** ) giám sát hoạt động của hệ thống và cảnh báo về các cuộc xâm nhập có thể xảy ra. IDS sẽ phát hiện và cảnh báo về các sai lệch mà bạn đã cấu hình để phát hiện. Thông thường nhất, các công cụ IDS sẽ giám sát nội dung của tải trọng gói tin để phát hiện các mẫu liên quan đến các mối đe dọa như phần mềm độc hại hoặc các nỗ lực lừa đảo.
* **Network protocol analyzer** , còn được gọi là packet sniffer, là các công cụ được thiết kế để thu thập và phân tích lưu lượng dữ liệu trong mạng. Chúng có thể được sử dụng để phân tích thủ công các giao tiếp mạng một cách chi tiết. Ví dụ bao gồm các công cụ như tcpdump và Wireshark, có thể được các chuyên gia bảo mật sử dụng để ghi lại các giao tiếp mạng thông qua việc thu thập các gói tin. Sau đó, việc thu thập các gói tin có thể được điều tra để xác định hoạt động có khả năng gây hại.

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

**Những điểm chính**

|  |
| --- |
| Monitoring and protecting networks from intrusions and attacks are key responsibilities of security professionals. You can’t protect what you don’t know. As a security analyst, you’ll need to know the components of a network and the communications that happen on it, so you can better protect it. Baselines provide a way to understand network traffic by uncovering common patterns which help in identifying any deviations from the expected traffic patterns. Tools like intrusion detection systems and network protocol analyzers support efforts in monitoring network activities. |

Giám sát và bảo vệ mạng khỏi các cuộc xâm nhập và tấn công là trách nhiệm chính của các chuyên gia bảo mật. Bạn không thể bảo vệ những gì bạn không biết. Là một nhà phân tích bảo mật, bạn sẽ cần biết các thành phần của mạng và các thông tin liên lạc diễn ra trên đó, để bạn có thể bảo vệ mạng tốt hơn. Đường cơ sở cung cấp một cách để hiểu lưu lượng mạng bằng cách khám phá các mẫu chung giúp xác định bất kỳ sự sai lệch nào so với các mẫu lưu lượng dự kiến. Các công cụ như hệ thống phát hiện xâm nhập và trình phân tích giao thức mạng hỗ trợ các nỗ lực giám sát các hoạt động của mạng.

|  |
| --- |
| **Resources** |

**Tài nguyên**

|  |
| --- |
| * If you would like to learn more about network components organizations can monitor, check out [network traffic - MITRE ATT&CK®](https://attack.mitre.org/datasources/DS0029/) * Attackers can leverage different techniques to exfiltrate data, should you like to learn more, check out [data exfiltration techniques - MITRE ATT&CK®](https://attack.mitre.org/tactics/TA0010/) |

* Nếu bạn muốn tìm hiểu thêm về các thành phần mạng mà tổ chức có thể giám sát, hãy xem[lưu lượng mạng - MITER ATT&CK®](https://attack.mitre.org/datasources/DS0029/)
* Kẻ tấn công có thể sử dụng các kỹ thuật khác nhau để đánh cắp dữ liệu, nếu bạn muốn tìm hiểu thêm, hãy xem[kỹ thuật lọc dữ liệu - MITER ATT&CK®](https://attack.mitre.org/tactics/TA0010/)

***1.5. Data exfiltration attacks - Các cuộc tấn công đánh cắp dữ liệu***

|  |
| --- |
| Monitoring network traffic helps security professionals detect, prevent, and respond to attacks. In my experience as a security professional, monitoring for deviations from typical network traffic patterns has yielded big results. Even if information is encrypted, monitoring network traffic is still important for security purposes. |

Giám sát lưu lượng mạnggiúp các chuyên gia an ninh phát hiện,ngăn chặn và ứng phó với các cuộc tấn công.Theo kinh nghiệm của tôi với tư cách là một chuyên gia an ninh,giám sát các sai lệch từcác mô hình lưu lượng mạng điển hình đã mang lại kết quả lớn.Ngay cả khi thông tin được mã hóa,giám sát lưu lượng mạng vẫn cònquan trọng cho mục đích an ninh.

|  |
| --- |
| Let's discuss how the detection and response process might work in a data exfiltration attack. First, we'll outline the attacker's perspective. |

Hãy thảo luận về cách phát hiện và phản ứngquá trình này có thể hoạt động trong một cuộc tấn công đánh cắp dữ liệu.Đầu tiên, chúng ta sẽ phác thảo quan điểm của kẻ tấn công.

|  |
| --- |
| Before attackers can perform data exfiltration, they'll need to gain initial access into a network and computer system. This can be done through a social engineering attack like phishing, which tricks people into disclosing sensitive data. Attackers can send phishing emails with attachments or links that trick their target into entering their credentials. Now, an attacker has successfully gained access to their device. |

Trước khi kẻ tấn công có thể thực hiện việc đánh cắp dữ liệu,họ sẽ cần phải có được quyền truy cập ban đầuvào mạng lưới và hệ thống máy tính.Điều này có thể được thực hiện thông qua một mạng xã hộitấn công kỹ thuật như lừa đảo,lừa mọi người tiết lộ dữ liệu nhạy cảm.Kẻ tấn công có thể gửi email lừa đảo có tệp đính kèm hoặcliên kết đánh lừa mục tiêu của họvào việc nhập thông tin đăng nhập của họ.Bây giờ, kẻ tấn công đãđã truy cập thành công vào thiết bị của họ.

|  |
| --- |
| After gaining their initial position into the system, an attacker won't stop there. The goal for attackers is to maintain access in the environment and avoid being detected for as long as possible. To do this, they'll perform a tactic known as lateral movement, or pivoting. This is when they'll spend time exploring the network with the goal of expanding and maintaining their access to other systems on the network. |

Sau khi đạt được vị trí ban đầu của họ vàohệ thống, kẻ tấn công sẽ không dừng lại ở đó.Mục tiêu của kẻ tấn công là duy trì quyền truy cập trongmôi trường và tránh bịđược phát hiện trong thời gian dài nhất có thể.Để làm được điều này, họ sẽ thực hiệnmột chiến thuật được gọi là di chuyển ngang hoặc xoay trục.Đây là lúc họ sẽ dành thời giankhám phá mạng lưới với mục tiêumở rộng và duy trì quyền truy cập của họđến các hệ thống khác trên mạng.

|  |
| --- |
| As an attacker pivots in the network, they'll scope out the environment to identify valuable assets, such as sensitive data like proprietary code, personally identifiable information like names and addresses, or financial records. They'll do this by searching locations such as network file shares, intranet sites, code repositories, and more. |

Khi kẻ tấn công xoay vòng trong mạng,họ sẽ thăm dò môi trườngđể xác định tài sản có giá trị,chẳng hạn như dữ liệu nhạy cảm như mã độc quyền,thông tin nhận dạng cá nhân nhưtên và địa chỉ hoặc hồ sơ tài chính.Họ sẽ làm điều này bằng cách tìm kiếmcác vị trí như chia sẻ tệp mạng,các trang mạng nội bộ, kho lưu trữ mã và nhiều hơn nữa.

|  |
| --- |
| After the attacker identifies the assets of value, they'll need to collect, package, and prepare the data for exfiltration outside of the organization's network and into the attacker's hands. One way they may do this is by reducing the data size. This helps attackers hide the stolen data and bypass security controls. |

Sau khi kẻ tấn công xác định được tài sản có giá trị,họ sẽ cần phải thu thập, đóng gói,và chuẩn bị dữ liệu để lọc ra bên ngoàimạng lưới của tổ chức và vào tay kẻ tấn công.Một cách họ có thể thực hiện điều này là bằng cách giảm kích thước dữ liệu.Điều này giúp kẻ tấn công ẩn náudữ liệu bị đánh cắp và vượt qua các biện pháp kiểm soát an ninh.

|  |
| --- |
| Finally, the attacker will exfiltrate the data to their destination of choice. There are many ways to do this. For example, attackers can email the stolen data to themselves using the compromised email account. |

Cuối cùng, kẻ tấn công sẽ trích xuấtdữ liệu đến đích mà họ lựa chọn.Có nhiều cách để làm điều này. Ví dụ,kẻ tấn công có thể gửi dữ liệu bị đánh cắp qua email đếnsử dụng tài khoản email bị xâm phạm.

|  |
| --- |
| Now that you've tapped into the attacker's perspective, let's explore how organizations can defend against this type of attack. |

Bây giờ bạn đã khai thác được quan điểm của kẻ tấn công,hãy cùng khám phá cách các tổ chứccó thể phòng thủ chống lại kiểu tấn công này.

|  |
| --- |
| First, security teams must prevent attacker access. There are many methods you can use to protect your network from phishing attempts. For example, requiring users to use multi-factor authentication. |

Đầu tiên, nhóm bảo mật phải ngăn chặn kẻ tấn công truy cập.Có nhiều phương pháp bạn có thể sử dụng đểbảo vệ mạng của bạn khỏi các nỗ lực lừa đảo.Ví dụ, yêu cầu người dùngsử dụng xác thực đa yếu tố.

|  |
| --- |
| Attackers that gain access to a network can remain unnoticed for a while. It's important that security teams monitor network activity to identify any suspicious activity that can indicate a compromise. For example, multiple user logins coming from IP addresses outside of the network should be investigated. |

Những kẻ tấn công có thể truy cập vào mạngcó thể không được chú ý trong một thời gian.Điều quan trọng là các đội an ninhgiám sát hoạt động mạng đểxác định bất kỳ hoạt động đáng ngờ nàođiều đó có thể chỉ ra một sự thỏa hiệp.Ví dụ, nhiều người dùng đăng nhập đến từĐịa chỉ IP bên ngoàimạng lưới cần được điều tra.

|  |
| --- |
| Earlier, you examined how to identify, classify, and protect assets using asset inventories and security controls. As part of an organization's security policy, all assets should be cataloged in an asset inventory. The appropriate security controls should also be applied to protect these assets from unauthorized access. |

Trước đó, bạn đã xem xét cách xác định, phân loại,và bảo vệ tài sản bằng cách sử dụngkiểm kê tài sản và kiểm soát an ninh.Là một phần của chính sách bảo mật của tổ chức,tất cả tài sản phải được lập danh mục trong bản kiểm kê tài sản.Các biện pháp kiểm soát an ninh thích hợp cũng nên được áp dụngđể bảo vệ những tài sản này khỏi sự truy cập trái phép.

|  |
| --- |
| Lastly, if a data exfiltration attack is successful, security teams must detect and stop the exfiltration. To detect the attack, indicators of unusual data collection can be identified through network monitoring. These include: large internal file transfers, large external uploads, and unexpected file writes. |

Cuối cùng, nếu một cuộc tấn công đánh cắp dữ liệu thành công,đội an ninh phải phát hiện và ngăn chặn việc rò rỉ.Để phát hiện cuộc tấn công,các chỉ số thu thập dữ liệu bất thường có thểđược xác định thông qua giám sát mạng.Bao gồm: chuyển tập tin nội bộ lớn,tải lên bên ngoài lớn,và ghi tệp tin bất ngờ.

|  |
| --- |
| SIEM tools can detect an alert on these activities. Once an alert has been sent out, security teams investigate and stop the attack from continuing. There are many ways to stop an attack like this. For instance, once the unusual activity is identified, you can block the IP addresses associated with the attacker using firewall rules. |

Các công cụ SIEM có thể phát hiện cảnh báo về những hoạt động này.Sau khi cảnh báo đã được gửi đi,đội an ninh điều tra vàngăn chặn cuộc tấn công tiếp tục.Có nhiều cách để ngăn chặn một cuộc tấn công như thế này.Ví dụ, một khi hoạt động bất thường được xác định,bạn có thể chặn các địa chỉ IPcó liên quan đến kẻ tấn công sử dụng các quy tắc tường lửa.

|  |
| --- |
| Data exfiltration attacks are just one of many attacks that can be detected through network monitoring. Coming up, you'll learn how to monitor and analyze network communications using packet sniffers. |

Các cuộc tấn công đánh cắp dữ liệu chỉ là một trong nhữngnhiều cuộc tấn công có thể đượcđược phát hiện thông qua giám sát mạng.Tiếp theo, bạn sẽ học cách theo dõi vàphân tích truyền thông mạng bằng cách sử dụng chương trình đánh hơi gói tin.

***1.6. Test your knowledge: Understand network traffic - Kiểm tra kiến thức của bạn: Hiểu về lưu lượng mạng***

**2. Capture and view network traffic – Chụp và xem lưu lượng mạng**

***2.1. Packets and packet captures - Các gói tin và việc bắt gói tin***

|  |
| --- |
| Whether it's an employee sending an email or a malicious actor attempting to exfiltrate confidential data, actions that are performed on a network can be identified through examining network traffic flows. |

Cho dù đó là một nhân viên gửi email haymột kẻ xấu đang cố gắngđể đánh cắp dữ liệu bí mật,các hành động được thực hiện trên mạng có thể làđược xác định thông qua việc kiểm tra luồng lưu lượng mạng.

|  |
| --- |
| Understanding these network communications provides valuable insight into the activities happening in a network. This way, you can better understand what's going on in an environment and defend against potential threats. With this in mind, let's examine how to record network traffic through packet captures. |

Hiểu được những giao tiếp mạng này cung cấpcái nhìn sâu sắc có giá trị vào các hoạt độngxảy ra trong mạng lưới.Bằng cách này, bạn có thể hiểu rõ hơn những gì đang diễn ra trongmôi trường và bảo vệ chống lại các mối đe dọa tiềm tàng.Với điều này trong tâm trí, chúng ta hãy xem xét làm thế nào đểghi lại lưu lượng mạng thông qua việc bắt gói tin.

|  |
| --- |
| Previously in the program, you learned that when data is sent, it's divided into packets. Just like an addressed envelope in the mail, packets contain delivery information which is used to route it to its destination. |

Trước đó trong chương trình,bạn đã học được rằng khi dữ liệu được gửi đi,Nó được chia thành các gói.Giống như một phong bì có ghi địa chỉ trong thư,các gói chứa thông tin phân phốiđược sử dụng để định tuyến đến đích.

|  |
| --- |
| This information includes a sender and receiver's IP address, the type of packet that's being sent, and more. Packets can provide lots of information about the communications happening between devices over a network. |

Thông tin này bao gồm người gửivà địa chỉ IP của người nhận,loại gói tin đang được gửi và nhiều thông tin khác.Các gói tin có thể cung cấp nhiều thông tin vềcác giao tiếp diễn ra giữathiết bị qua mạng.

|  |
| --- |
| You may also recall that a packet has multiple components. There's the header, which includes information like the type of network protocol and port being used. Imagine this as being the name and mailing address located on an envelope. |

Bạn cũng có thể nhớ lại rằngmột gói tin có nhiều thành phần.Có tiêu đề, bao gồm thông tin nhưloại giao thức mạng và cổng đang được sử dụng.Hãy tưởng tượng đây là tên vàđịa chỉ gửi thư ghi trên phong bì.

|  |
| --- |
| Network protocols are a set of rules that determine the transmission of data between devices on a network. Ports are non-physical locations on a computer that organize data transmission between devices on a network. |

Giao thức mạng là một tập hợp các quy tắc xác địnhviệc truyền dữ liệu giữa các thiết bị trên mạng.Cổng là vị trí không vật lý trên máy tínhtổ chức truyền dữ liệugiữa các thiết bị trên mạng.

|  |
| --- |
| The header also contains the packet's source and destination IP address. We'll explore more information contained in the header in a later section. |

Tiêu đề cũng chứađịa chỉ IP nguồn và đích của gói tin.Chúng tôi sẽ khám phá thêm thông tincó trong tiêu đề ở phần sau.

|  |
| --- |
| Next, there's the payload, which contains the actual data that's being delivered. This is like the content of a letter inside of an envelope. And there's the footer, which signifies the end of the packet. |

Tiếp theo, có tải trọng,chứa dữ liệu thực tế đang được phân phối.Điều này giống như nội dung củamột lá thư bên trong phong bì.Và có phần chân trang,báo hiệu sự kết thúc của gói tin.

|  |
| --- |
| So how exactly can you observe a network packet? Just like scents are invisible but can be smelled, packets are invisible but can be captured using tools called packet sniffers. |

Vậy chính xác thì bạn có thể quan sát một gói tin mạng như thế nào?Giống như mùi hương vô hình nhưng có thể ngửi thấy,các gói tin là vô hình nhưng có thểđược thu thập bằng các công cụ gọi là packet sniffer.

|  |
| --- |
| You may remember packet sniffers from a previous section. A network protocol analyzer, or packet sniffer, is a tool designed to capture and analyze data traffic within a network. As a security analyst, you'll use packet sniffers to inspect packets for indicators of compromise. |

Bạn có thể nhớ về chương trình đánh hơi gói tin ở phần trước.Một trình phân tích giao thức mạng hoặc trình đánh hơi gói tin,là một công cụ được thiết kế để nắm bắt vàphân tích lưu lượng dữ liệu trong mạng.Là một nhà phân tích an ninh,bạn sẽ sử dụng các gói sniffer để kiểm tracác gói dữ liệu về chỉ số xâm phạm.

|  |
| --- |
| Through packet sniffing, we can grab a detailed snapshot of packets that travel over a network in the form of a packet capture. A packet capture, or P-cap, is a file containing data packets intercepted from an interface or network. It's sort of like intercepting an envelope in the mail. |

Thông qua việc đánh hơi gói tin, chúng ta có thể chụp ảnh nhanh chi tiếtcác gói tin di chuyển quamột mạng lưới dưới dạng bắt gói tin.Một gói tin bắt giữ, hoặc P-cap, là một tập tinchứa các gói dữ liệu bị chặntừ một giao diện hoặc mạng.Giống như việc chặn một chiếc phong bì trong thư vậy.

|  |
| --- |
| Packet captures are incredibly useful during incident investigation. By having access to the communications happening between devices over a network, you can observe network interactions and start to build a storyline to determine what exactly happened. |

Việc bắt gói tin cực kỳ hữu íchtrong quá trình điều tra sự cố.Bằng cách tiếp cận các thông tin liên lạcxảy ra giữa các thiết bị qua mạng,bạn có thể quan sát các tương tác mạng và bắt đầu xây dựngmột cốt truyện để xác định chính xác điều gì đã xảy ra.

|  |
| --- |
| Coming up, we'll discuss the importance of packet analysis. Meet you there. |

Tiếp theo, chúng ta sẽ thảo luận về tầm quan trọngcủa phân tích gói tin. Gặp bạn ở đó.

***2.2. Learn more about packet captures - Tìm hiểu thêm về việc bắt gói tin***

|  |
| --- |
| **Learn more about packet captures** |

**Tìm hiểu thêm về việc bắt gói tin**

|  |
| --- |
| The role of security analysts involves monitoring and analyzing network traffic flows. One way to do this is by generating packet captures and then analyzing the captured traffic to identify unusual activity on a network. |

Vai trò của các nhà phân tích bảo mật liên quan đến việc giám sát và phân tích luồng lưu lượng mạng. Một cách để thực hiện điều này là tạo các gói tin bắt được và sau đó phân tích lưu lượng đã bắt được để xác định hoạt động bất thường trên mạng.

|  |
| --- |
| Previously, you explored the fundamentals of networks. Throughout this section, you’ll refer to your foundation in networking to better understand network traffic flows. In this reading, you'll learn about the three main aspects of network analysis: packets, network protocol analyzers, and packet captures. |

Trước đó, bạn đã khám phá những điều cơ bản về mạng. Trong suốt phần này, bạn sẽ tham khảo nền tảng về mạng của mình để hiểu rõ hơn về luồng lưu lượng mạng. Trong phần đọc này, bạn sẽ tìm hiểu về ba khía cạnh chính của phân tích mạng: gói tin, trình phân tích giao thức mạng và bắt gói tin.

|  |
| --- |
| **Packets** |

**Gói tin**

|  |
| --- |
| Previously in the program, you learned that a **data packet** is a basic unit of information that travels from one device to another within a network. Detecting network intrusions begins at the packet level. That's because packets form the basis of information exchange over a network. Each time you perform an activity on the internet—like visiting a website—packets are sent and received between your computer and the website’s server. These packets are what help transmit information through a network. For example, when uploading an image to a website, the data gets broken up into multiple packets, which then get routed to the intended destination and reassembled upon delivery. |

Trước đó trong chương trình, bạn đã học rằng một **gói dữ liệu** là một đơn vị thông tin cơ bản di chuyển từ thiết bị này sang thiết bị khác trong mạng. Phát hiện xâm nhập mạng bắt đầu ở cấp độ gói. Đó là vì các gói tạo thành cơ sở trao đổi thông tin qua mạng. Mỗi lần bạn thực hiện một hoạt động trên internet—như truy cập trang web—các gói được gửi và nhận giữa máy tính của bạn và máy chủ của trang web. Các gói này là những gì giúp truyền thông tin qua mạng. Ví dụ, khi tải hình ảnh lên trang web, dữ liệu sẽ được chia thành nhiều gói, sau đó được định tuyến đến đích dự định và lắp ráp lại khi giao hàng.

|  |
| --- |
| In cybersecurity, packets provide valuable information that helps add context to events during investigations. Understanding the transfer of information through packets will not only help you develop insight on network activity, it will also help you identify abnormalities and better defend networks from attacks. |

Trong an ninh mạng, các gói tin cung cấp thông tin có giá trị giúp bổ sung ngữ cảnh cho các sự kiện trong quá trình điều tra. Hiểu được cách truyền thông tin qua các gói tin không chỉ giúp bạn hiểu sâu hơn về hoạt động mạng mà còn giúp bạn xác định các bất thường và bảo vệ mạng tốt hơn khỏi các cuộc tấn công.

|  |
| --- |
| Packets contain three components: the header, the payload, and the footer. Here’s a description of each of these components. |

Các gói tin chứa ba thành phần: tiêu đề, tải trọng và chân trang. Sau đây là mô tả về từng thành phần này.

|  |
| --- |
| **Header** |

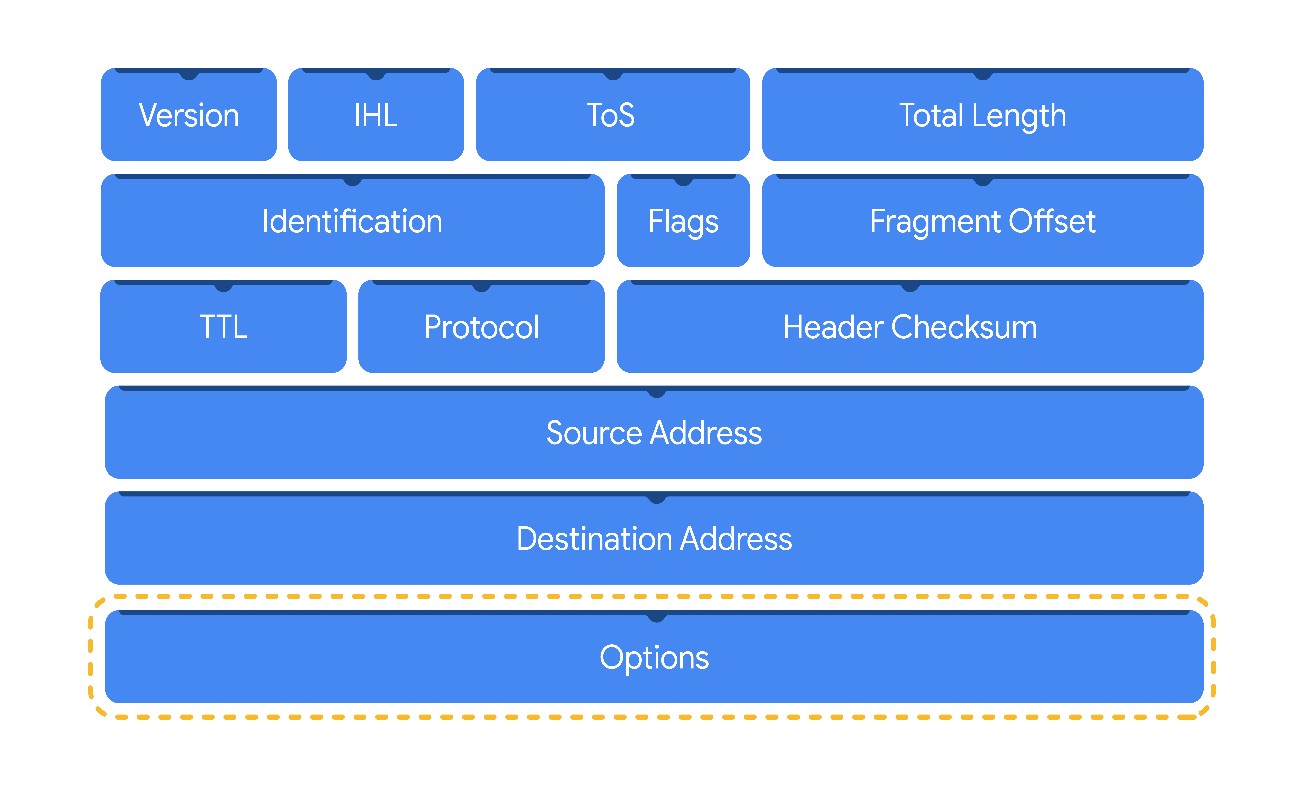
**Tiêu đề**

|  |
| --- |
| Packets begin with the most essential component: theheader. Packets can have several headers depending on the protocols used such as an Ethernet header, an IP header, a TCP header, and more. Headers provide information that’s used to route packets to their destination. This includes information about the source and destination IP addresses, packet length, protocol, packet identification numbers, and more. |

Các gói tin bắt đầu bằng thành phần thiết yếu nhất: tiêu đề. Các gói tin có thể có nhiều tiêu đề tùy thuộc vào giao thức được sử dụng như tiêu đề Ethernet, tiêu đề IP, tiêu đề TCP, v.v. Tiêu đề cung cấp thông tin được sử dụng để định tuyến các gói tin đến đích của chúng. Thông tin này bao gồm thông tin về địa chỉ IP nguồn và đích, độ dài gói tin, giao thức, số nhận dạng gói tin, v.v.

|  |
| --- |
| Here is an IPv4 header with the information it provides: |

Dưới đây là tiêu đề IPv4 có chứa thông tin mà nó cung cấp:



|  |
| --- |
| **Payload** |

**Tải trọng**

|  |
| --- |
| Thepayload component directly follows the header and contains the actual data being delivered. Think back to the example of uploading an image to a website; the payload of this packet would be the image itself. |

Thành phần tải trọng theo sau trực tiếp tiêu đề và chứa dữ liệu thực tế được phân phối. Hãy nghĩ lại ví dụ về việc tải hình ảnh lên trang web; tải trọng của gói tin này sẽ là chính hình ảnh đó.

|  |
| --- |
| **Footer** |

**Chân trang**

|  |
| --- |
| The footer, also known as the trailer, is located at the end of a packet. The Ethernet protocol uses footers to provide error-checking information to determine if data has been corrupted. In addition, Ethernet network packets that are analyzed might not display footer information due to network configurations.  **Note:** Most protocols, such as the Internet Protocol (IP), *do not* use footers. |

Footer, còn được gọi là trailer, nằm ở cuối gói tin. Giao thức Ethernet sử dụng footer để cung cấp thông tin kiểm tra lỗi nhằm xác định xem dữ liệu có bị hỏng không. Ngoài ra, các gói tin mạng Ethernet được phân tích có thể không hiển thị thông tin footer do cấu hình mạng.

**Lưu ý:** Hầu hết các giao thức, chẳng hạn như Giao thức Internet (IP), *không* sử dụng chân trang.

|  |
| --- |
| **Network protocol analyzers** |

**Máy phân tích giao thức mạng**

|  |
| --- |
| **Network protocol analyzers** **(packet sniffers)** are tools designed to capture and analyze data traffic within a network. Examples of network protocol analyzers include tcpdump, Wireshark, and TShark. |

**Trình phân tích giao thức mạng (packet sniffer)** là các công cụ được thiết kế để thu thập và phân tích lưu lượng dữ liệu trong mạng. Ví dụ về trình phân tích giao thức mạng bao gồm tcpdump, Wireshark và TShark.

|  |
| --- |
| Beyond their use in security as an investigative tool used to monitor networks and identify suspicious activity, network protocol analyzers can be used to collect network statistics, such as bandwidth or speed, and troubleshoot network performance issues, like slowdowns. |

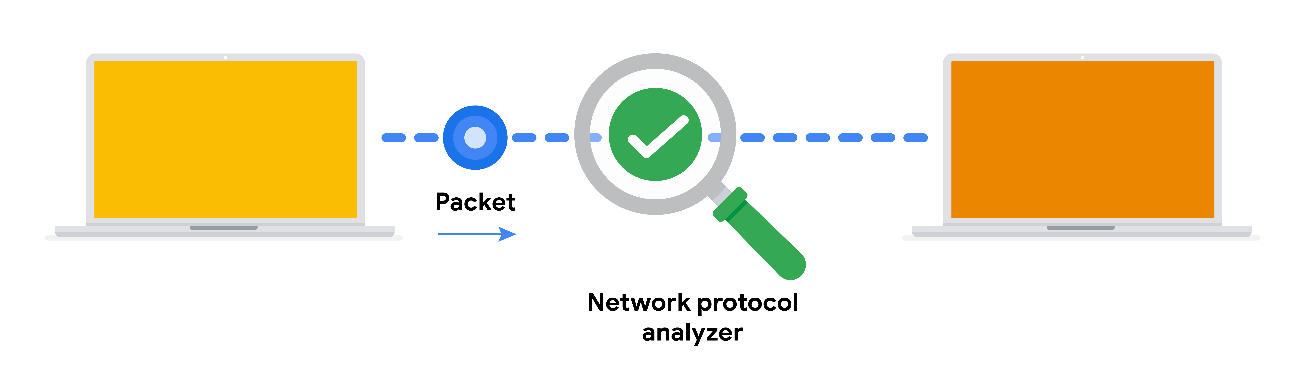
Ngoài việc sử dụng trong bảo mật như một công cụ điều tra để giám sát mạng và xác định hoạt động đáng ngờ, các trình phân tích giao thức mạng có thể được sử dụng để thu thập số liệu thống kê mạng, chẳng hạn như băng thông hoặc tốc độ, và khắc phục sự cố về hiệu suất mạng, như chậm lại.

|  |
| --- |
| Network protocol analyzers can also be used for malicious purposes. For example, malicious actors can use network protocol analyzers to capture packets containing sensitive data, such as account login information. |

Trình phân tích giao thức mạng cũng có thể được sử dụng cho mục đích xấu. Ví dụ, kẻ xấu có thể sử dụng trình phân tích giao thức mạng để bắt các gói tin chứa dữ liệu nhạy cảm, chẳng hạn như thông tin đăng nhập tài khoản.

|  |
| --- |
| Here’s a network diagram illustrating how packets get transmitted from a sender to the receiver. A network protocol analyzer is placed in the middle of the communications to capture the data packets that travel over the wire. |

Sau đây là sơ đồ mạng minh họa cách các gói tin được truyền từ người gửi đến người nhận. Một bộ phân tích giao thức mạng được đặt ở giữa quá trình truyền thông để thu thập các gói dữ liệu truyền qua dây.



|  |
| --- |
| **How network protocol analyzers work** |

**Cách thức hoạt động của máy phân tích giao thức mạng**

|  |
| --- |
| Network protocol analyzers use both software and hardware capabilities to capture network traffic and display it for security analysts to examine and analyze. Here’s how:   1. First, packets must be collected from the network via the **Network Interface Card (NIC)**, which is hardware that connects computers to a network, like a router. NICs receive and transmit network traffic, but by default they only listen to network traffic that’s addressed to them. To capture all network traffic that is sent over the network, a NIC must be switched to a mode that has access to all visible network data packets. In wireless interfaces this is often referred to as monitoring mode, and in other systems it may be called promiscuous mode. This mode enables the NIC to have access to all visible network data packets, but it won’t help analysts access all packets across a network. A network protocol analyzer must be positioned in an appropriate network segment to access all traffic between different hosts. 2. The network protocol analyzer collects the network traffic in raw binary format. Binary format consists of 0s and 1s and is not as easy for humans to interpret. The network protocol analyzer takes the binary and converts it so that it’s displayed in a human-readable format, so analysts can easily read and understand the information. |

Các trình phân tích giao thức mạng sử dụng cả khả năng phần mềm và phần cứng để nắm bắt lưu lượng mạng và hiển thị để các nhà phân tích bảo mật kiểm tra và phân tích. Sau đây là cách thực hiện:

1. Đầu tiên, các gói tin phải được thu thập từ mạng thông qua **Thẻ giao diện mạng (NIC)** , là phần cứng kết nối máy tính với mạng, như bộ định tuyến. NIC nhận và truyền lưu lượng mạng, nhưng theo mặc định, chúng chỉ lắng nghe lưu lượng mạng được gửi đến chúng. Để nắm bắt tất cả lưu lượng mạng được gửi qua mạng, NIC phải được chuyển sang chế độ có thể truy cập vào tất cả các gói dữ liệu mạng có thể nhìn thấy. Trong các giao diện không dây, chế độ này thường được gọi là chế độ giám sát và trong các hệ thống khác, chế độ này có thể được gọi là chế độ hỗn tạp. Chế độ này cho phép NIC có thể truy cập vào tất cả các gói dữ liệu mạng có thể nhìn thấy, nhưng nó sẽ không giúp các nhà phân tích truy cập vào tất cả các gói tin trên toàn mạng. Một trình phân tích giao thức mạng phải được định vị trong một phân đoạn mạng thích hợp để truy cập vào tất cả lưu lượng giữa các máy chủ khác nhau.
2. Bộ phân tích giao thức mạng thu thập lưu lượng mạng ở định dạng nhị phân thô. Định dạng nhị phân bao gồm 0 và 1 và không dễ để con người diễn giải. Bộ phân tích giao thức mạng lấy nhị phân và chuyển đổi để hiển thị ở định dạng mà con người có thể đọc được, do đó các nhà phân tích có thể dễ dàng đọc và hiểu thông tin.

|  |
| --- |
| **Capturing packets** |

**Chụp các gói tin**

|  |
| --- |
| **Packet sniffing** is the practice of capturing and inspecting data packets across a network. A **packet capture (p-cap)** is a file containing data packets intercepted from an interface or network. Packet captures can be viewed and further analyzed using network protocol analyzers. For example, you can filter packet captures to only display information that's most relevant to your investigation, such as packets sent from a specific IP address. |

**Packet sniffing** là hoạt động thu thập và kiểm tra các gói dữ liệu trên mạng. **Packet capture (p-cap)** là một tệp chứa các gói dữ liệu bị chặn từ một giao diện hoặc mạng. Packet capture có thể được xem và phân tích thêm bằng các trình phân tích giao thức mạng. Ví dụ: bạn có thể lọc các packet capture để chỉ hiển thị thông tin có liên quan nhất đến cuộc điều tra của mình, chẳng hạn như các gói được gửi từ một địa chỉ IP cụ thể.

|  |
| --- |
| **Note**: Using network protocol analyzers to intercept and examine private network communications without permission is considered illegal in many places. |

**Lưu ý** : Việc sử dụng trình phân tích giao thức mạng để chặn và kiểm tra các liên lạc mạng riêng tư mà không được phép bị coi là bất hợp pháp ở nhiều nơi.

|  |
| --- |
| P-cap files can come in many formats depending on the packet capture library that’s used. Each format has different uses and network tools may use or support specific packet capture file formats by default. You should be familiar with the following libraries and formats:   1. **Libpcap** is a packet capture library designed to be used by Unix-like systems, like Linux and MacOS®. Tools like tcpdump use Libpcap as the default packet capture file format. 2. **WinPcap** is an open-source packet capture library designed for devices running Windows operating systems. It’s considered an older file format and isn’t predominantly used. 3. **Npcap** is a librarydesigned by the port scanning tool Nmap that is commonly used in Windows operating systems. 4. **PCAPng** is a modern file format that can simultaneously capture packets and store data. Its ability to do both explains the “ng,” which stands for “next generation.” |

Tệp P-cap có thể có nhiều định dạng tùy thuộc vào thư viện chụp gói tin được sử dụng. Mỗi định dạng có cách sử dụng khác nhau và các công cụ mạng có thể sử dụng hoặc hỗ trợ các định dạng tệp chụp gói tin cụ thể theo mặc định. Bạn nên quen thuộc với các thư viện và định dạng sau:

1. **Libpcap** là một thư viện bắt gói tin được thiết kế để sử dụng trong các hệ thống giống Unix, như Linux và MacOS®. Các công cụ như tcpdump sử dụng Libpcap làm định dạng tệp bắt gói tin mặc định.
2. **WinPcap** là một thư viện chụp gói tin mã nguồn mở được thiết kế cho các thiết bị chạy hệ điều hành Windows. Nó được coi là một định dạng tệp cũ hơn và không được sử dụng rộng rãi.
3. **Npcap** là một thư viện được thiết kế bởi công cụ quét cổng Nmap thường được sử dụng trong hệ điều hành Windows.
4. **PCAPng** là một định dạng tệp hiện đại có thể đồng thời thu thập các gói tin và lưu trữ dữ liệu. Khả năng thực hiện cả hai chức năng này giải thích cho "ng", viết tắt của "next generation".

|  |
| --- |
| **Pro tip:** Analyzing your home network can be a good way to practice using these tools. |

**Mẹo chuyên nghiệp:** Phân tích mạng gia đình có thể là một cách tốt để thực hành sử dụng các công cụ này.

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

**Những điểm chính**

|  |
| --- |
| Network protocol analyzers are helpful investigative tools that provide you with insight into the activity happening on a network. As an analyst, you'll use network protocol analyzer tools to view and analyze packet capture files to better understand network communications and defend against intrusions. |

Trình phân tích giao thức mạng là công cụ điều tra hữu ích cung cấp cho bạn thông tin chi tiết về hoạt động đang diễn ra trên mạng. Là một nhà phân tích, bạn sẽ sử dụng các công cụ phân tích giao thức mạng để xem và phân tích các tệp bắt gói tin để hiểu rõ hơn về giao tiếp mạng và bảo vệ chống lại sự xâm nhập.

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

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| This Infosec article describes the risks of [packet crafting](https://resources.infosecinstitute.com/topic/packet-crafting-a-serious-crime/), a technique used to test a network’s structure. |

Bài viết Infosec này mô tả những rủi ro của[chế tạo gói](https://resources.infosecinstitute.com/topic/packet-crafting-a-serious-crime/), một kỹ thuật được sử dụng để kiểm tra cấu trúc của mạng.

***2.3. Interpret network communications with packets - Giải thích các giao tiếp mạng bằng các gói tin***

|  |
| --- |
| If a packet capture is like intercepting an envelope in the mail, then packet analysis is like reading the letter inside of the envelope. Let's discuss how analyzing packets can help us interpret and understand network communications. |

Nếu việc bắt gói tin giống như việc chặn một phong bì trong thư,khi đó việc phân tích gói tin giống như việc đọc lá thư bên trong phong bì.Hãy thảo luận về cách phân tích các gói tin có thể giúp chúng ta giải thích vàhiểu về truyền thông mạng.

|  |
| --- |
| As you may know, networks are noisy. There's an enormous volume of communications happening between devices at any given time. And because of this, packet captures can contain large amounts of network communications, making analysis challenging and time-consuming. |

Như bạn có thể biết, mạng rất nhiễu.Có một khối lượng lớn thông tin liên lạc diễn ra giữa các thiết bịtại bất kỳ thời điểm nào.Và vì lý do này, việc bắt gói tin có thể chứa một lượng lớn thông tin mạnggiao tiếp, khiến việc phân tích trở nên khó khăn và tốn thời gian.

|  |
| --- |
| As a security professional, you'll be working against the clock to protect networks and computer systems from potential attacks. You may analyze network evidence in the form of packet captures to identify indicators of compromise. Having the ability to filter network traffic using packet sniffers to gather relevant information is an essential skill to have. For example, let's say that you were tasked with analyzing a packet capture to find any indication of data exfiltration. How would you go about this? |

Là một chuyên gia an ninh, bạn sẽ phải làm việc hết sức mình để bảo vệmạng lưới và hệ thống máy tính khỏi các cuộc tấn công tiềm ẩn.Bạn có thể phân tích bằng chứng mạng dưới dạng chụp gói tin để xác địnhdấu hiệu của sự thỏa hiệp.Có khả năng lọc lưu lượng mạng bằng cách sử dụng các trình đánh hơi gói tin để thu thậpthông tin có liên quan là một kỹ năng thiết yếu cần có.Ví dụ, giả sử bạn được giao nhiệm vụ phân tích một gói tin bắt đượcđể tìm bất kỳ dấu hiệu nào cho thấy dữ liệu bị rò rỉ.Bạn sẽ thực hiện việc này thế nào?

|  |
| --- |
| Using a network analyzer tool, you can filter the packet capture to sort packets. This can help you quickly identify an event associated with data exfiltration, like large amounts of data leaving a database. There are many other filters you can apply to packet captures to find the information you need to support an investigation efficiently. |

Bằng cách sử dụng công cụ phân tích mạng, bạn có thể lọc gói tin để sắp xếp các gói tin.Điều này có thể giúp bạn nhanh chóng xác định sự kiện liên quan đến việc rò rỉ dữ liệu,giống như lượng lớn dữ liệu rời khỏi cơ sở dữ liệu.Có nhiều bộ lọc khác mà bạn có thể áp dụng để chụp gói tin để tìm thông tinbạn cần hỗ trợ cuộc điều tra một cách hiệu quả.

|  |
| --- |
| Examples of network analyzer tools include tcpdump and Wireshark. tcpdump is accessed through a command line while Wireshark has a graphical user interface, or GUI. Both tools are useful for security analysts, and soon you'll have the opportunity to explore both. |

Ví dụ về công cụ phân tích mạng bao gồm tcpdump và Wireshark.tcpdump được truy cập thông qua dòng lệnh trong khi Wireshark có giao diện người dùng đồ họagiao diện hoặc GUI.Cả hai công cụ đều hữu ích cho các nhà phân tích bảo mật vàbạn sẽ sớm có cơ hội khám phá cả hai.

|  |
| --- |
| Before we begin using these tools, let's explore packet fields in detail, specifically, IP headers. Meet you there. |

Trước khi bắt đầu sử dụng các công cụ này, chúng ta hãy cùng khám phá chi tiết các trường gói tin,cụ thể là tiêu đề IP.Gặp bạn ở đó nhé.

***2.4. Reexamine the fields of a packet header - Kiểm tra lại các trường của tiêu đề gói tin***

|  |
| --- |
| While there are many different tools available to use, it's important as a security analyst that you learn how to read and analyze packets manually. To do so, let's examine an important packet component: IP headers. |

Mặc dù có nhiều công cụ khác nhau có thể sử dụng,điều quan trọng là với tư cách là một nhà phân tích bảo mật, bạn phải họccách đọc và phân tích các gói tin theo cách thủ công.Để làm như vậy, chúng ta hãy xem xétmột thành phần gói tin quan trọng: tiêu đề IP.

|  |
| --- |
| Previously, you learned about the four layers of the TCP/IP model. Remember, the TCP/IP model is a framework that is used to visualize how data is organized and transmitted across a network. |

Trước đó, bạn đã học vềbốn lớp của mô hình TCP/IP.Hãy nhớ rằng, mô hình TCP/IP là một khuôn khổ được sử dụng đểhình dung dữ liệu như thế nàođược tổ chức và truyền qua mạng.

|  |
| --- |
| The internet layer accepts and delivers packets for the network. It's also the layer where the Internet Protocol operates as the foundation for all communications on the internet. It's responsible for making sure packets reach their destinations. |

Lớp internet chấp nhận vàcung cấp các gói tin cho mạng.Đây cũng là lớp mà Giao thức Internet hoạt độnglà nền tảng cho mọi hoạt động truyền thông trên Internet.Nó có trách nhiệm tạo rachắc chắn các gói tin sẽ đến được đích.

|  |
| --- |
| The Internet Protocol operates like a mail courier delivering an envelope. Instead of using the delivery information found on the envelope, the Internet Protocol uses the information found in a packet header, like IP addresses. It then determines the best available route for packets to take, so that data can be sent and received between hosts. |

Giao thức Internet hoạt động như thế nàomột người đưa thư đang chuyển phong bì.Thay vì sử dụng thông tin giao hàngtìm thấy trên phong bì,Giao thức Internet sử dụng thông tinđược tìm thấy trong tiêu đề gói tin, như địa chỉ IP.Sau đó nó xác định tuyến đường tốt nhất có sẵnđể các gói tin được lấy,để dữ liệu có thể được gửi và nhận giữa các máy chủ.

|  |
| --- |
| As you may already know, IP packets contain headers. Headers contain the data fields essential to the transfer of data to its intended destination. Different protocols use different headers. |

Như bạn có thể đã biết,Các gói tin IP chứa tiêu đề.Tiêu đề chứa các trường dữ liệu cần thiết đểviệc chuyển dữ liệu đến đích dự kiến.Các giao thức khác nhau sử dụng các tiêu đề khác nhau.

|  |
| --- |
| There are two different versions of the Internet Protocol: IPv4, which is considered to be the foundation of internet communications, and IPv6, which is the most recent version of the Internet Protocol. Remember, different protocols use different headers. So IPv4 and IPv6 headers differ, but they contain similar fields with different names. IPv4 is still the most widely used, so we'll focus on examining the fields of an IPv4 header. |

Có hai phiên bản khác nhau củaGiao thức Internet: IPv4,được coi lànền tảng của truyền thông internet,và IPv6, đó làphiên bản mới nhất của Giao thức Internet.Hãy nhớ rằng các giao thức khác nhau sử dụng các tiêu đề khác nhau.Vì vậy, tiêu đề IPv4 và IPv6 khác nhau,nhưng chúng chứa các trường tương tự với tên gọi khác nhau.IPv4 vẫn là giao thức được sử dụng rộng rãi nhất,vì vậy chúng ta sẽ tập trung vào việc kiểm tra các trường của tiêu đề IPv4.

|  |
| --- |
| Let's start with the Version field, which specifies which version of IP is being used, either IPv4 or IPv6. Referring back to our mail analogy, the Version field is like the different classes of mail, like priority, express, or regular. |

Chúng ta hãy bắt đầu với trường Phiên bản,chỉ rõ phiên bản IP nào đang được sử dụng,hoặc IPv4 hoặc IPv6.Quay trở lại phép so sánh thư từ của chúng ta,trường Phiên bản giống như các lớp thư khác nhau,như ưu tiên, nhanh hoặc thông thường.

|  |
| --- |
| Next, IHL stands for Internet Header Length. This field specifies the length of the IP header plus any options. |

Tiếp theo, IHL là viết tắt của Internet Header Length.Trường này chỉ định độ dài củatiêu đề IP cùng với bất kỳ tùy chọn nào.

|  |
| --- |
| The next field, ToS stands for Type of Service. This field tells us if certain packets should be treated with different care. For example, think of ToS like a fragile sticker on a mailed package. |

Trường tiếp theo, ToS là viết tắt của Type of Service (Loại dịch vụ).Trường này cho chúng ta biết nếumột số gói hàng cần được xử lý cẩn thận khác nhau.Ví dụ, hãy nghĩ về ToS nhưnhãn dán dễ vỡ trên gói hàng được gửi qua đường bưu điện.

|  |
| --- |
| Next is the Total Length field, which identifies the length of the entire packet, including the headers and the data. This can be compared to the dimensions and weight of an envelope. |

Tiếp theo là trường Tổng chiều dài,xác định độ dài của toàn bộ gói tin,bao gồm tiêu đề và dữ liệu.Điều này có thể được so sánh với các kích thướcvà trọng lượng của phong bì.

|  |
| --- |
| The next three fields, Identification, Flags, and Fragment Offset, deal with information related to fragmentation. Fragmentation is when an IP packet gets broken up into chunks, which then get transmitted over the wire and reassembled when they arrive at their destination. These three fields specify if fragmentation has been used and how to reassemble the broken packets in the correct order. This is similar to how mail can travel through multiple routes like mailboxes, processing facilities, airplanes, and mail trucks before it reaches its destination. |

Ba trường tiếp theo,Nhận dạng, Cờ,và Bù trừ đoạn,xử lý thông tin liên quan đến phân mảnh.Phân mảnh là khi một gói IPbị vỡ thành từng mảnh,sau đó được truyền qua dây vàđược lắp ráp lại khi chúng đến đích.Ba trường này chỉ định xem sự phân mảnh đã được thực hiện hay chưađã sử dụng và cách lắp ráp lạicác gói tin bị hỏng theo đúng thứ tự.Điều này tương tự như cách thư có thể di chuyểnthông qua nhiều tuyến đường như hộp thư,cơ sở chế biến, máy bay vàxe chở thư trước khi đến đích.

|  |
| --- |
| The TTL field stands for Time to Live. Like its name suggests, this field determines how long a packet can live before it gets dropped. Without this field, packets could loop through routers endlessly. TTL is similar to how tracking information provides details about an envelope's expected delivery date. |

Trường TTL là viết tắt của Time to Live (Thời gian sống).Như tên gọi của nó gợi ý,trường này xác định thời gianmột gói tin có thể tồn tại trước khi bị loại bỏ.Nếu không có trường này, các gói tin có thểlặp qua các bộ định tuyến vô tận.TTL tương tự như cách theo dõi thông tincung cấp thông tin chi tiết vềngày dự kiến ​​giao phong bì.

|  |
| --- |
| The Protocol field specifies the protocol used by providing a value which corresponds to a protocol. For example, TCP is represented by 6. This is similar to including the number of a house in a postal address. |

Trường Giao thức chỉ định giao thức được sử dụng bởicung cấp giá trị tương ứng với một giao thức.Ví dụ, TCP được biểu thị bằng 6.Điều này tương tự như việc bao gồm sốcủa một ngôi nhà trong địa chỉ bưu chính.

|  |
| --- |
| The Header Checksum stores a value called a checksum, which is used to determine if any errors have occurred in the header. |

Tổng kiểm tra tiêu đề lưu trữ một giá trị được gọi là tổng kiểm tra,được sử dụng để xác định xemcó bất kỳ lỗi nào xảy ra ở phần tiêu đề.

|  |
| --- |
| The Source Address specifies the source IP address and the Destination Address specifies the destination IP address. This is just like the sender and receiver's contact information found on an envelope. |

Địa chỉ nguồn chỉ định địa chỉ IP nguồn vàĐịa chỉ đích chỉ địnhđịa chỉ IP đích.Điều này giống như người gửi vàthông tin liên lạc của người nhận được tìm thấy trên phong bì.

|  |
| --- |
| The Options field is not required and is commonly used for network troubleshooting rather than common traffic. If it's used, the header length increases. It's like purchasing postal insurance for an envelope. |

Trường Tùy chọn không bắt buộc và thường làđược sử dụng để khắc phục sự cố mạngthay vì giao thông thông thường.Nếu sử dụng, độ dài tiêu đề sẽ tăng lên.Giống như việc mua bảo hiểm bưu chính cho một chiếc phong bì vậy.

|  |
| --- |
| Finally, at the end of the packet header is where the packet's data resides, like the text in an email message. |

Cuối cùng, ở phần cuối của tiêu đề gói tinlà nơi dữ liệu của gói tin được lưu trữ,giống như văn bản trong tin nhắn email.

|  |
| --- |
| Who knew that the packets of data we send across networks contain so much information? Coming up soon, you'll have the opportunity to examine these packet fields in detail. |

Ai biết rằng các gói dữ liệu chúng ta gửitrên mạng có chứa nhiều thông tin như vậy?Sắp tới, bạn sẽ có cơ hộikiểm tra chi tiết các trường gói tin này.

***2.5. Investigate packet details - Điều tra chi tiết gói tin***

|  |
| --- |
| **Investigate packet details** |

|  |
| --- |
| So far, you've learned about how network protocol analyzers (packet sniffers) intercept network communications. You've also learned how you can analyze packet captures (p-caps) to gain insight into the activity happening on a network. As a security analyst, you'll use your packet analysis skills to inspect network packets and identify suspicious activity during investigations. |

|  |
| --- |
| In this reading, you'll re-examine IPv4 and IPv6 headers. Then, you'll explore how you can use Wireshark to investigate the details of packet capture files. |

|  |
| --- |
| **Internet Protocol (IP)** |

|  |
| --- |
| Packets form the foundation of data exchange over a network, which means that detection begins at the packet level. The **Internet Protocol (IP)** includes a set of standards used for routing and addressing data packets as they travel between devices on a network. IP operates as the foundation for all communications over the internet. |

|  |
| --- |
| IP ensures that packets reach their destinations. There are two versions of IP that you will find in use today: IPv4 and IPv6. Both versions use different headers to structure packet information. |

|  |
| --- |
| **IPv4** |

|  |
| --- |
| IPv4 is the most commonly used version of IP. There are thirteen fields in the header:   * **Version**: This field indicates the IP version. For an IPv4 header, IPv4 is used. * **Internet Header Length (IHL)**: This field specifies the length of the IPv4 header including any Options. * **Type of Service (ToS)**: This field provides information about packet priority for delivery. * **Total Length**: This field specifies the total length of the entire IP packet including the header and the data. * **Identification**: Packets that are too large to send are fragmented into smaller pieces. This field specifies a unique identifier for fragments of an original IP packet so that they can be reassembled once they reach their destination. * **Flags**: This field provides information about packet fragmentation including whether the original packet has been fragmented and if there are more fragments in transit. * **Fragment Offset**: This field is used to identify the correct sequence of fragments. * **Time to Live (TTL)**: This field limits how long a packet can be circulated in a network, preventing packets from being forwarded by routers indefinitely. * **Protocol**: This field specifies the protocol used for the data portion of the packet. * **Header Checksum**: This field specifies a checksum value which is used for error-checking the header. * **Source Address**: This field specifies the source address of the sender. * **Destination Address**: This field specifies the destination address of the receiver. * **Options**: This field is optional and can be used to apply security options to a packet. |

|  |
| --- |
| **IPv6** |

|  |
| --- |
| IPv6 adoption has been increasing because of its large address space. There are eight fields in the header:   * **Version**: This field indicates the IP version. For an IPv6 header, IPv6 is used. * **Traffic Class**: This field is similar to the IPv4 Type of Service field. The Traffic Class field provides information about the packet's priority or class to help with packet delivery. * **Flow Label**: This field identifies the packets of a flow. A flow is the sequence of packets sent from a specific source. * **Payload Length**: This field specifies the length of the data portion of the packet. * **Next Header**: This field indicates the type of header that follows the IPv6 header such as TCP. * **Hop Limit**: This field is similar to the IPv4 Time to Live field. The Hop Limit limits how long a packet can travel in a network before being discarded. * **Source Address**: This field specifies the source address of the sender. * **Destination Address**: This field specifies the destination address of the receiver. |

|  |
| --- |
| Header fields contain valuable information for investigations and tools like Wireshark help to display these fields in a human-readable format. |

|  |
| --- |
| **Wireshark** |

|  |
| --- |
| **Wireshark** is an open-source network protocol analyzer. It uses a graphical user interface (GUI), which makes it easier to visualize network communications for packet analysis purposes. Wireshark has many features to explore that are beyond the scope of this course. You'll focus on how to use basic filtering to isolate network packets so that you can find what you need. |

|  |
| --- |
| **Display filters** |

|  |
| --- |
| Wireshark's display filters let you apply filters to packet capture files. This is helpful when you are inspecting packet captures with large volumes of information. Display filters will help you find specific information that's most relevant to your investigation. You can filter packets based on information such as protocols, IP addresses, ports, and virtually any other property found in a packet. Here, you'll focus on display filtering syntax and filtering for protocols, IP addresses, and ports. |

|  |
| --- |
| **Comparison operators** |

|  |
| --- |
| You can use different comparison operators to locate specific header fields and values. Comparison operators can be expressed using either abbreviations or symbols. For example, this filter using the **==** equal symbol in this filter **ip.src == 8.8.8.8** is identical to using the **eq** abbreviation in this filter **ip.src eq 8.8.8.8**. |

|  |
| --- |
| This table summarizes the different types of comparison operators you can use for display filtering. |

|  |  |  |
| --- | --- | --- |
| **Operator type** | **Symbol** | **Abbreviation** |
| Equal | **==** | eq |
| Not equal | **!=** | ne |
| Greater than | **>** | gt |
| Less than | **<** | lt |
| Greater than or equal to | **>=** | ge |
| Less than or equal to | **<=** | le |

|  |
| --- |
| **Pro tip:** You can combine comparison operators with Boolean logical operators like **and** and **or** to create complex display filters. Parentheses can also be used to group expressions and to prioritize search terms. |

|  |
| --- |
| **Contains operator** |

|  |
| --- |
| The **contains** operator is used to filter packets that contain an exact match of a string of text. Here is an example of a filter that displays all HTTP streams that match the keyword **"moved"**. |

|  |
| --- |
| **Matches operator** |

|  |
| --- |
| The **matches** operator is used to filter packets based on the regular expression (regex) that's specified. Regular expression is a sequence of characters that forms a pattern. You'll explore more about regular expressions later in this program. |

|  |
| --- |
| **Filter toolbar** |

|  |
| --- |
| You can apply filters to a packet capture using Wireshark's filter toolbar. In this example, **dns** is the applied filter, which means Wireshark will only display packets containing the DNS protocol. |

|  |
| --- |
| **Pro tip**: Wireshark uses different colors to represent protocols. You can customize colors and create your own filters. |

|  |
| --- |
| **Filter for protocols** |

|  |
| --- |
| Protocol filtering is one of the simplest ways you can use display filters. You can simply enter the name of the protocol to filter. For example, to filter for DNS packets simply type **dns** in the filter toolbar. Here is a list of some protocols you can filter for:   * dns * http * ftp * ssh * arp * telnet * icmp |

|  |
| --- |
| **Filter for an IP address** |

|  |
| --- |
| You can use display filters to locate packets with a specific IP address. |

|  |
| --- |
| For example, if you would like to filter packets that contain a specific IP address use **ip.addr**, followed by a space, the equal **==** comparison operator, and the IP address. Here is an example of a display filter that filters for the IP address **172.21.224.2**:  **ip.addr == 172.21.224.2** |

|  |
| --- |
| To filter for packets originating from a specific source IP address, you can use the **ip.src** filter. Here is an example that looks for the **10.10.10.10** source IP address:  **ip.src == 10.10.10.10** |

|  |
| --- |
| To filter for packets delivered to a specific destination IP address, you can use the **ip.dst** filter. Here is an example that searches for the **4.4.4.4** destination IP address:  **ip.dst == 4.4.4.4** |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

***2.6. Resources for completing labs - Tài nguyên để hoàn thành phòng thí nghiệm***

***2.7. Lab tips and troubleshooting steps - Mẹo phòng thí nghiệm và các bước khắc phục sự cố***

***2.8. Activity: Analyze your first packet - Hoạt động: Phân tích gói tin đầu tiên của bạn***

***2.9. Optional Exemplar: Analyze your first packet - Mẫu tùy chọn: Phân tích gói đầu tiên của bạn***

***2.10. Test your knowledge: Capture and view network traffic - Kiểm tra kiến ​​thức của bạn: Ghi lại và xem lưu lượng mạng***

**3. Packet inspection – Kiểm tra gói**

***3.1. Packet captures with tcpdump - Bắt gói tin bằng tcpdump***

***3.2. Overview of tcpdump - Tổng quan về tcpdump***

***3.3. Activity: Capture your first packet - Hoạt động: Chụp gói tin đầu tiên của bạn***

***3.4. Optional Exemplar: Capture your first packet - Mẫu tùy chọn: Chụp gói tin đầu tiên của bạn***

***3.5. Test your knowledge: Packet inspection - Kiểm tra kiến thức của bạn: Kiểm tra gói tin***

***3.6. Activity: Research network protocol analyzers - Hoạt động: Nghiên cứu các trình phân tích giao thức mạng***

***3.7. Activity Exemplar: Research network protocol analyzers - Hoạt động mẫu: Nghiên cứu các trình phân tích giao thức mạng***

**4. Review: Network monitoring and analysis - Đánh giá: Giám sát và phân tích mạng**

***4.1. Wrap-up - Tóm tắt***

***4.2. Glossary terms from module 2 - Thuật ngữ trong mô-đun 2***

***4.3. Module 2 challenge - Thử thách Module 2***