

Khóa học 1 — Nền tảng về An ninh mạng

Trong khóa học này, học viên sẽ bước đầu làm quen với thế giới an ninh mạng thông qua chương trình học tương tác do Google phát triển. Học viên sẽ xác định được những sự kiện quan trọng dẫn đến sự hình thành ngành an ninh mạng, giải thích tầm quan trọng của an ninh mạng đối với hoạt động kinh doanh ngày nay, cũng như tìm hiểu những trách nhiệm và kỹ năng cần có trong công việc của một chuyên gia phân tích an ninh mạng mới vào nghề.

Đến hết khóa học này, học viên sẽ:

- Xác định được tác động của các vụ tấn công bảo mật lên hoạt động kinh doanh.
- Hiểu được những trách nhiệm và kỹ năng cần có trong công việc của một chuyên gia phân tích an ninh mạng mới vào nghề.
- Nhận biết được các vụ tấn công vào tổ chức trong quá khứ cũng như hiện tại đã dẫn đến sự hình thành và phát triển ngành an ninh mạng như thế nào.
- Tìm hiểu 8 lĩnh vực bảo mật theo CISSP.
- Xác định lĩnh vực, khuôn khổ và biện pháp kiểm soát bảo mật.
- Giải thích khái niệm đạo đức an ninh.
- Nhận biết các công cụ thường dùng của chuyên gia phân tích an ninh mạng.

Hoạt động đưa vào hồ sơ: Trong khóa học 1, học viên cần viết một tuyên ngôn cá nhân để đưa vào hồ sơ.

KỸ NĂNG THU ĐƯỢC:

- ❑ Giới thiệu về các khái niệm trong an ninh mạng
- ❑ Các vụ tấn công trước đây như vi-rút Brain hay sâu Morris
- ❑ Đạo đức trong an ninh mạng
- ❑ Kỹ năng công sở như giao tiếp và cộng tác

CHỦ ĐỀ:

- ★ Làm quen với thế giới an ninh mạng
- ★ Sự phát triển của ngành an ninh mạng
- ★ Bảo vệ khỏi mối đe dọa, rủi ro và lỗ hổng
- ★ Công cụ an ninh mạng và ngôn ngữ lập trình

SỐ LIỆU VỀ NỘI DUNG:

| | | |
|---|----|---------------------|
|  | 29 | Video |
|  | 21 | Bài đọc |
|  | 12 | Bài kiểm tra |
|  | 10 | Hoạt động thực hành |

Course 1: Foundations of Cybersecurity

Khóa 1: Nền tảng của An ninh mạng

Contents

| | |
|---|----|
| Module 1: Welcome to the exciting world of cybersecurity – Chào mừng đến với thế giới thú vị của an ninh mạng | 5 |
| 1. Get started with the certificate program – Bắt đầu với chương trình chứng chỉ | 5 |
| 1.1. Welcome to the Google Cybersecurity Certificate – Chào mừng đến với Chứng chỉ an ninh mạng của Google | 5 |
| 1.2. Google Cybersecurity Certificate overview – Tổng quan về Chứng chỉ an ninh mạng của Google | 12 |
| 1.3. Course 1 overview – Tổng quan về khóa 1 | 15 |
| 1.4. Your Google Cybersecurity Certificate roadmap – Lộ trình Chứng chỉ An ninh mạng của Google của bạn | 22 |
| 1.5. Welcome to week 1 – Chào mừng đến với tuần 1 | 33 |
| 1.6. Commit to completing the program – Cam kết hoàn thành chương trình ... | 34 |
| 1.7. Helpful resources and tips – Tài nguyên và lời khuyên hữu ích | 34 |
| 1.8. Participate in program surveys – Tham gia khảo sát chương trình | 40 |
| 1.9. Google Cybersecurity Certificate participant entry survey – Bản khảo sát dành cho người tham gia Chứng chỉ An ninh mạng của Google | 42 |
| 1.10. Connect with your classmates – Kết nối với bạn cùng lớp của bạn | 42 |
| 2. Introduction to cybersecurity – Giới thiệu về an ninh mạng | 43 |
| 2.1. Introduction to cybersecurity – Giới thiệu về an ninh mạng | 43 |
| 2.2. Toni: My path to cybersecurity – Toni: Con đường đến với an ninh mạng của tôi | 45 |
| 2.3. Responsibilities of an entry-level cybersecurity analyst – Trách nhiệm của một nhà phân tích an ninh mạng cấp độ đầu vào | 47 |
| 2.4. Nikki: A day in the life of a security engineer – Nikki: Một ngày trong cuộc đời của kỹ sư an ninh | 49 |
| 2.5. Common cybersecurity terminology – Thuật ngữ an ninh mạng phổ biến .. | 51 |
| 2.6. Test your knowledge: Introduction to cybersecurity – Kiểm tra kiến thức của bạn: Giới thiệu về an ninh mạng | 53 |
| 3. Core skills for cybersecurity professionals – Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng | 53 |
| 3.1. Core skills for cybersecurity professionals | 54 |
| 3.2. Veronica: My path to working in cybersecurity | 56 |
| 3.3. Transferable and technical cybersecurity skills | 57 |
| 3.4. The importance of cybersecurity | 61 |
| 3.5. Explore: Keep organizations secure | 63 |

Course 1: Foundations of Cybersecurity

Khóa 1: Nền tảng của An ninh mạng

| | |
|--|------------|
| 3.6. The value of cybersecurity | 65 |
| 3.7. Test your knowledge: Core skills for cybersecurity professionals | 66 |
| 4. Review: Welcome to the exciting world of cybersecurity – Đánh giá: Chào mừng đến với thế giới đầy thú vị của An ninh mạng..... | 66 |
| 4.1. Wrap-up..... | 66 |
| 4.2. Glossary terms from module 1..... | 66 |
| 4.3. Module 1 challenge | 68 |
| Module 2: The evolution of cybersecurity – Sự phát triển của an ninh mạng..... | 69 |
| 1. The history of cybersecurity – Lịch sử an ninh mạng..... | 69 |
| 1.1 Welcome to module 2 – Chào mừng đến với module 2 | 69 |
| 1.2. Past cybersecurity attacks – Các cuộc tấn công an ninh mạng trong quá khứ | 70 |
| 1.3. Attacks in the digital age – Tấn công trong thời đại kỹ thuật số | 72 |
| 1.4. Common attacks and their effectiveness – Các cuộc tấn công phổ biến và hiệu quả của chúng | 75 |
| 1.5. Identify: Methods of attack – Xác định: Phương thức tấn công | 80 |
| 1.6. Sean: Keep your cool during a data breach – Sean: Hãy bình tĩnh khi có sự cố vi phạm dữ liệu | 85 |
| 1.7. Test your knowledge: The history of cybersecurity – Kiểm tra kiến thức của bạn: Lịch sử an ninh mạng | 86 |
| 2. The eight CISSP security domains – Tám miền bảo mật CISSP | 86 |
| 2.1. Introduction to the eight CISSP security domains, Part 1 – Giới thiệu về tám miền bảo mật CISSP, Phần 1 | 86 |
| 2.2. Introduction to the eight CISSP security domains, Part 2 – Giới thiệu về tám miền bảo mật CISSP, Phần 2 | 89 |
| 2.3. Determine the type of attack – Xác định kiểu tấn công..... | 91 |
| 2.4. Understand attackers – Hiểu kẻ tấn công..... | 95 |
| 2.5. Test your knowledge: The eight CISSP security domains – Kiểm tra kiến thức của bạn: Tám miền bảo mật CISSP | 99 |
| 3. Review: The evolution of cybersecurity – Đánh giá: Sự phát triển của an ninh mạng..... | 99 |
| 3.1. Wrap-up – Gợi lại..... | 99 |
| 3.2. Glossary terms from module 2 – Thuật ngữ trong học phần 2..... | 100 |
| 3.3. Module 2 challenge – Thử thách module 2 | 102 |
| Module 3: Protect against threats, risks, and vulnerabilities – Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng..... | 103 |
| 1. Frameworks and controls – Frameworks và kiểm soát | 103 |

Course 1: Foundations of Cybersecurity

Khóa 1: Nền tảng của An ninh mạng

| | |
|--|-----|
| <i>1.1. Welcome to module 3 – Chào mừng đến với module 3</i> | 103 |
| <i>1.2. Introduction to security frameworks and controls – Giới thiệu về khung bảo mật và kiểm soát</i> | 105 |
| <i>1.3. Secure design – Thiết kế an toàn</i> | 108 |
| <i>1.4. Controls, frameworks, and compliance – Kiểm soát, khuôn khổ và tuân thủ</i> | 111 |
| <i>1.5. Heather: Protect sensitive data and information – Heather: Bảo vệ dữ liệu và thông tin nhạy cảm</i> | 118 |
| <i>1.6. Test your knowledge: Frameworks and controls – Kiểm tra kiến thức của bạn: Khung và điều khiển</i> | 119 |
| 2. Ethics in cybersecurity – Đạo đức trong an ninh mạng | 119 |
| <i>2.1. Ethics in cybersecurity – Đạo đức trong an ninh mạng</i> | 120 |
| <i>2.2. Ethical concepts that guide cybersecurity decisions – Các khái niệm đạo đức hướng dẫn các quyết định về an ninh mạng</i> | 123 |
| <i>2.3. Practice: Ethics for cybersecurity professionals – Thực hành: Đạo đức dành cho chuyên gia an ninh mạng</i> | 127 |
| <i>2.4. Holly: The importance of ethics as a cybersecurity professional – Holly: Tầm quan trọng của đạo đức với tư cách là một chuyên gia an ninh mạng</i> | 130 |
| <i>2.5. Use ethics to make decisions – Sử dụng đạo đức để đưa ra quyết định</i> | 131 |
| <i>2.6. Test your knowledge: Ethics in cybersecurity – Kiểm tra kiến thức của bạn: Đạo đức trong an ninh mạng</i> | 132 |
| 3. Review: Protect against threats, risks, and vulnerabilities – Đánh giá: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng | 132 |
| <i>3.1. Wrap-up – Gợi lại</i> | 132 |
| <i>3.2. Glossary terms from module 3 – Thuật ngữ trong học phần 3</i> | 133 |
| <i>3.3. Module 3 challenge – Thử thách module 3</i> | 135 |
| Module 4: Cybersecurity tools and programming languages – Các công cụ an ninh mạng và ngôn ngữ lập trình | 136 |
| 1. Important cybersecurity tools – Các công cụ an ninh mạng quan trọng | 136 |
| <i>1.1. Welcome to module 4 – Chào mừng đến với module 4</i> | 136 |
| <i>1.2. Common cybersecurity tools – Các công cụ an ninh mạng phổ biến</i> | 138 |
| <i>1.3. Tools for protecting business operations – Công cụ bảo vệ hoạt động kinh doanh</i> | 141 |
| <i>1.4. Explore: Tools and their purposes – Khám phá: Công cụ và mục đích của chúng</i> | 146 |
| <i>1.5. Test your knowledge: Important cybersecurity tools – Kiểm tra kiến thức của bạn: Các công cụ an ninh mạng quan trọng</i> | 147 |

Course 1: Foundations of Cybersecurity

Khóa 1: Nền tảng của An ninh mạng

| | |
|---|------------|
| 2. Core cybersecurity knowledge and skills – Kiến thức và kỹ năng an ninh mạng cốt lõi..... | 147 |
| 2.1. <i>Introduction to Linux, SQL, and Python – Giới thiệu về Linux, SQL và Python.....</i> | <i>147</i> |
| 2.2. <i>Use tools to protect business operations – Sử dụng công cụ để bảo vệ hoạt động kinh doanh</i> | <i>149</i> |
| 2.3. <i>Test your knowledge: Core cybersecurity knowledge and skills – Kiểm tra kiến thức của bạn: Kiến thức và kỹ năng cốt lõi về an ninh mạng</i> | <i>153</i> |
| 2.4. <i>Create a cybersecurity portfolio – Tạo danh mục đầu tư an ninh mạng ...</i> | <i>153</i> |
| 2.5. <i>Portfolio Activity: Draft a professional statement – Hoạt động danh mục đầu tư: Soạn thảo một tuyên bố chuyên nghiệp</i> | <i>158</i> |
| 2.6. <i>Portfolio Activity Exemplar: Draft a professional statement – Ví dụ về hoạt động danh mục đầu tư: Dự thảo một tuyên bố chuyên nghiệp</i> | <i>159</i> |
| 3. Review: Cybersecurity tools and programming languages – Đánh giá: Các công cụ an ninh mạng và ngôn ngữ lập trình..... | 159 |
| 3.1. <i>Wrap-up – Gói lại.....</i> | <i>159</i> |
| 3.2. <i>Glossary terms from module 4 – Thuật ngữ trong phần 4.....</i> | <i>159</i> |
| 3.3. <i>Module 4 challenge – Thử thách module 4</i> | <i>161</i> |
| 4. Congratulations on completing Course 1! – Chúc mừng bạn đã hoàn thành Khóa 1!..... | 161 |
| 4.1. <i>Course wrap-up – Tóm tắt khóa học</i> | <i>161</i> |
| 4.2. <i>Course 1 glossary – Thuật ngữ khóa 1</i> | <i>162</i> |
| 4.3. <i>Your Course 1 learning journey – Hành trình học tập khóa 1 của bạn</i> | <i>162</i> |
| 4.4. <i>Get started on the next course – Bắt đầu khóa học tiếp theo</i> | <i>163</i> |

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Module 1: Welcome to the exciting world of cybersecurity – Chào mừng đến với thế giới thú vị của an ninh mạng

Begin your journey into cybersecurity! You'll explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals.

Bắt đầu hành trình của bạn vào an ninh mạng! Bạn sẽ khám phá lĩnh vực an ninh mạng và tìm hiểu về trách nhiệm công việc của các chuyên gia an ninh mạng.

Learning Objectives

- Explain how this certificate program will help prepare learners for a career in security
- Define the field of security
- Explore the job responsibilities of an entry-level security analyst
- Recognize core skills and knowledge needed to become a security analyst
- Describe how security analysts protect networks and information

Mục tiêu học tập

- Giải thích chương trình chứng chỉ này sẽ giúp người học chuẩn bị như thế nào cho sự nghiệp trong lĩnh vực an ninh
- Xác định lĩnh vực bảo mật
- Khám phá trách nhiệm công việc của một nhà phân tích bảo mật cấp đầu vào
- Nhận biết các kỹ năng và kiến thức cốt lõi cần thiết để trở thành nhà phân tích bảo mật
- Mô tả cách các nhà phân tích bảo mật bảo vệ mạng và thông tin

1. Get started with the certificate program – Bắt đầu với chương trình chứng chỉ

1.1. Welcome to the Google Cybersecurity Certificate – Chào mừng đến với Chứng chỉ an ninh mạng của Google

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Hello and welcome to the Google Career Certificate focused on cybersecurity. I'm so excited that you're here! My name is Toni, and I am a Security Engineering Manager at Google. I'll be your instructor for the first course of this certificate program. By starting this course, you've already taken a big step towards building new skills that will help you in your career.

Xin chào và chào mừng bạn đến với Chứng chỉ nghề nghiệp của Google (Google Career Certificate) tập trung vào an ninh mạng (cybersecurity). Tôi rất vui vì bạn ở đây! Tên tôi là Toni và tôi là Giám đốc kỹ thuật bảo mật tại Google. Tôi sẽ là người hướng dẫn bạn khóa học đầu tiên của chương trình chứng chỉ này. Khi bắt đầu khóa học này, bạn đã tiến được một bước lớn trong việc xây dựng các kỹ năng mới sẽ giúp ích cho bạn trong sự nghiệp của mình.

Cybersecurity may seem daunting at first, but you'd be surprised by the different backgrounds many of us have. I worked as an intelligence analyst before I got my first job in the security industry, and I'm excited to be your instructor as you begin your journey into security.

Ban đầu, an ninh mạng có vẻ khó khăn, nhưng bạn sẽ ngạc nhiên bởi nền tảng kiến thức khác nhau mà nhiều người trong chúng ta có. Tôi đã làm việc với tư cách là nhà phân tích tình báo trước khi có công việc đầu tiên trong ngành bảo mật và tôi rất vui được trở thành người hướng dẫn cho bạn khi bạn bắt đầu hành trình vào lĩnh vực bảo mật.

The demand for security professionals is growing at an incredible rate. By 2030, the U.S. Bureau of Labor Statistics expects security roles to grow by more than 30%, which is higher than the average growth rate for other occupations.

Nhu cầu về các chuyên gia bảo mật đang tăng với tốc độ đáng kinh ngạc. Đến năm 2030, Cục Thống kê Lao động Hoa Kỳ kỳ vọng vai trò an ninh sẽ tăng hơn 30%, cao hơn tốc độ tăng trưởng trung bình của các ngành nghề khác.

Global access to the internet is expanding. Every day, more people and organizations are adopting new digital technologies. Having a diverse community of security professionals with unique backgrounds, perspectives, and experiences is essential for protecting and serving different markets.

Truy cập toàn cầu vào internet đang mở rộng. Mỗi ngày, ngày càng có nhiều người và tổ chức áp dụng các công nghệ kỹ thuật số mới. Việc có một cộng đồng đa dạng gồm các chuyên gia bảo mật có nền tảng, quan điểm và kinh nghiệm độc đáo là điều cần thiết để bảo vệ và phục vụ các thị trường khác nhau.

Working in security has allowed me to work with people from all around the world. Working with people who have diverse backgrounds ensures that our teams get to ask lots of questions and come up with more creative solutions.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Làm việc trong lĩnh vực bảo mật đã cho phép tôi làm việc với mọi người từ khắp nơi trên thế giới. Làm việc với những người có nền tảng đa dạng đảm bảo rằng nhóm của chúng tôi có thể đặt nhiều câu hỏi và đưa ra nhiều giải pháp sáng tạo hơn.

The main objective in security is to protect organizations and people. This line of work allows you to support and interact with people across the globe.

Mục tiêu chính của bảo mật là bảo vệ các tổ chức và con người. Công việc này cho phép bạn hỗ trợ và tương tác với mọi người trên toàn cầu.

There are many openings for entry-level security analysts, and employers are struggling to find enough candidates with the right expertise. This program is designed to give you the knowledge and skills you need to start or advance in the security profession. No matter your current skill level, by the time you finish this certificate program, you'll be prepared to find a security-related job or expand your career in security.

Có rất nhiều cơ hội dành cho các nhà phân tích bảo mật cấp độ đầu vào và các nhà tuyển dụng đang gặp khó khăn trong việc tìm đủ ứng viên có chuyên môn phù hợp. Chương trình này được thiết kế để cung cấp cho bạn kiến thức và kỹ năng cần thiết để bắt đầu hoặc thăng tiến trong nghề bảo mật. Bất kể trình độ kỹ năng hiện tại của bạn là gì, khi bạn hoàn thành chương trình chứng chỉ này, bạn sẽ sẵn sàng tìm một công việc liên quan đến bảo mật hoặc mở rộng sự nghiệp của mình trong lĩnh vực bảo mật.

You may be wondering, what do security professionals actually do? Have you ever had to update your password online to include a number or a special symbol? If so, then you're already familiar with basic security measures, like password management. And if you've ever received a notification from a service provider about stolen data or a software hack, then you have first-hand experience with the impact of a security breach. If you've ever asked yourself how organizations safeguard data, then you already have two important traits that are necessary to thrive in this industry: curiosity and excitement.

Có thể bạn đang thắc mắc, các chuyên gia bảo mật thực sự làm gì? Bạn đã bao giờ phải cập nhật mật khẩu trực tuyến của mình để bao gồm một số hoặc một ký hiệu đặc biệt chưa? Nếu vậy thì bạn đã quen với các biện pháp bảo mật cơ bản, như quản lý mật khẩu. Và nếu bạn đã từng nhận được thông báo từ nhà cung cấp dịch vụ về dữ liệu bị đánh cắp hoặc bị hack phần mềm thì bạn đã có trải nghiệm trực tiếp về tác động của vi phạm bảo mật. Nếu bạn từng tự hỏi các tổ chức bảo vệ dữ liệu như thế nào thì bạn đã có sẵn hai đặc điểm quan trọng cần thiết để phát triển trong ngành này: tính tò mò và sự hào hứng.

Security analysts help minimize risks to organizations and people. Analysts work to proactively guard against incidents while continuously monitoring systems and networks. And, if an incident does occur, they investigate and report their findings. They are always asking questions and looking for solutions.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Các nhà phân tích bảo mật giúp giảm thiểu rủi ro cho tổ chức và con người. Các nhà phân tích làm việc để chủ động đề phòng sự cố trong khi liên tục giám sát các hệ thống và mạng. Và nếu một sự cố xảy ra, họ sẽ điều tra và báo cáo những phát hiện của mình. Họ luôn đặt câu hỏi và tìm kiếm giải pháp.

One of the best things about the security industry is the many paths and career options it exposes you to. Each option involves a unique set of skills and responsibilities. No matter what your background is, you'll probably find that you already have some relevant experience. If you enjoy collaborating with and helping others, solving puzzles, and are motivated by challenges, then this is the career for you.

Một trong những điều tốt nhất về ngành bảo mật là có nhiều con đường và lựa chọn nghề nghiệp mà nó mang lại cho bạn. Mỗi lựa chọn liên quan đến một bộ kỹ năng và trách nhiệm riêng. Cho dù nền tảng của bạn là gì, có thể bạn sẽ thấy rằng mình đã có một số kinh nghiệm liên quan. Nếu bạn thích hợp tác và giúp đỡ người khác, giải các câu đố và được thúc đẩy bởi các thử thách thì đây là nghề nghiệp dành cho bạn.

For example, my background as an intelligence analyst had nothing to do with cybersecurity. However, having strong critical thinking skills and communication skills provided a solid foundation for my success when I decided to pursue a career in security.

Ví dụ, nền tảng của tôi là một nhà phân tích tình báo không liên quan gì đến an ninh mạng. Tuy nhiên, việc có kỹ năng tư duy phản biện mạnh mẽ và kỹ năng giao tiếp đã tạo nền tảng vững chắc cho thành công của tôi khi tôi quyết định theo đuổi nghề bảo vệ.

If you're not sure what direction you want to take in the security industry, that's okay. This program will give you an overview of many different types of available jobs. It will also let you explore certain specialized skill sets to help you figure out where you want to take your career.

Nếu bạn không chắc chắn mình muốn đi theo hướng nào trong ngành bảo mật thì cũng không sao. Chương trình này sẽ cung cấp cho bạn cái nhìn tổng quan về nhiều loại công việc hiện có khác nhau. Nó cũng sẽ cho phép bạn khám phá một số bộ kỹ năng chuyên biệt nhất định để giúp bạn tìm ra nơi bạn muốn theo đuổi sự nghiệp của mình.

The Google Career Certificates are designed by industry professionals with decades of experience here at Google. You'll have a different expert from Google guide you through each course in the certificate. We'll share our knowledge in videos, provide practice opportunities with hands-on activities, and take you through real scenarios that you might encounter on the job.

Chúng chỉ nghề nghiệp của Google được thiết kế bởi các chuyên gia trong ngành với hàng chục năm kinh nghiệm tại Google. Bạn sẽ được một chuyên gia khác của Google hướng dẫn bạn qua từng khóa học trong chứng chỉ. Chúng tôi sẽ

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

chia sẻ kiến thức của mình qua video, cung cấp cơ hội thực hành bằng các hoạt động thực hành và đưa bạn qua các tình huống thực tế mà bạn có thể gặp phải trong công việc.

Throughout this program, you'll gain hands-on practice with detecting and responding to attacks, monitoring and protecting networks, investigating incidents, and writing code to automate tasks.

Trong suốt chương trình này, bạn sẽ được thực hành thực hành cách phát hiện và ứng phó với các cuộc tấn công, giám sát và bảo vệ mạng, điều tra sự cố và viết mã để tự động hóa các tác vụ.

The program is made up of several courses that are designed to help you land an entry-level job. You'll learn about topics like: core security concepts; security domains; network security; computing basics, including Linux and SQL; along with understanding assets, threats, and vulnerabilities. Our goal is to help you reach your goal of joining the security industry.

Chương trình này bao gồm một số khóa học được thiết kế để giúp bạn có được một công việc ở trình độ đầu vào. Bạn sẽ tìm hiểu về các chủ đề như: khái niệm bảo mật cốt lõi; miền bảo mật; an ninh mạng; kiến thức cơ bản về điện toán, bao gồm Linux và SQL; cùng với sự hiểu biết về tài sản, mối đe dọa và lỗ hổng. Mục tiêu của chúng tôi là giúp bạn đạt được mục tiêu gia nhập ngành bảo mật.

You'll learn about incident detection and response, as well as how to use programming languages, like Python, to accomplish common security tasks. You'll also gain valuable job search strategies that will benefit you as you begin to find and apply for jobs in the security profession.

Bạn sẽ tìm hiểu về cách phát hiện và ứng phó sự cố cũng như cách sử dụng các ngôn ngữ lập trình như Python để hoàn thành các tác vụ bảo mật thông thường. Bạn cũng sẽ đạt được các chiến lược tìm kiếm việc làm có giá trị sẽ mang lại lợi ích cho bạn khi bạn bắt đầu tìm và nộp đơn xin việc trong ngành bảo mật.

Completing this Google Career Certificate will help you develop skills and learn how to use tools to prepare you for a job in a fast-growing, high-demand field.

Việc hoàn thành Chứng chỉ nghề nghiệp của Google này sẽ giúp bạn phát triển các kỹ năng và học cách sử dụng các công cụ để chuẩn bị cho bạn làm việc trong lĩnh vực có nhu cầu cao, đang phát triển nhanh.

The certificate is designed to prepare you for a job in 3-6 months if you work on the certificate part-time. Once you graduate, you can connect with over 200 employers who are interested in hiring Google Career Certificate graduates, like you. Whether you're looking to switch jobs, start a new career, or level up your skills, this Google Career Certificate can open doors to new job opportunities.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Chúng tôi đã được thiết kế để giúp bạn chuẩn bị cho công việc sau 3-6 tháng nếu bạn làm việc bán thời gian với chúng tôi. Sau khi tốt nghiệp, bạn có thể kết nối với hơn 200 nhà tuyển dụng quan tâm đến việc tuyển dụng những sinh viên tốt nghiệp có Chứng chỉ nghề nghiệp của Google, giống như bạn. Cho dù bạn đang muốn chuyển đổi công việc, bắt đầu một sự nghiệp mới hay nâng cao kỹ năng của mình, Chứng chỉ nghề nghiệp của Google này có thể mở ra những cơ hội việc làm mới.

You don't need prior experience or knowledge in the security field because this certificate program will begin with the basics. I'll be by your side throughout this first course, making sure that you're learning the foundational knowledge needed to succeed in the field. This program is also flexible. You can complete all of the courses in this certificate on your own terms and at your own pace, online.

Bạn không cần có kinh nghiệm hoặc kiến thức trước đó trong lĩnh vực bảo mật vì chương trình chứng chỉ này sẽ bắt đầu với những điều cơ bản. Tôi sẽ đồng hành cùng bạn trong suốt khóa học đầu tiên này, đảm bảo rằng bạn đang học những kiến thức nền tảng cần thiết để thành công trong lĩnh vực này. Chương trình này cũng linh hoạt. Bạn có thể hoàn thành trực tuyến tất cả các khóa học trong chứng chỉ này theo điều kiện và tốc độ của riêng bạn.

We've gathered some amazing instructors to support you on your journey, and they'd like to introduce themselves now:

Chúng tôi đã tập hợp một số người hướng dẫn tuyệt vời để hỗ trợ bạn trên hành trình của mình và bây giờ họ xin giới thiệu về họ:

Hi! My name is Ashley, and I'm a Customer Engineering Enablement Lead for Security Operations Sales at Google. I'll take you through security domains, frameworks and controls, as well as common security threats, risks, and vulnerabilities. You'll also be introduced to common tools used by security analysts. I can't wait to get started!

CHÀO! Tên tôi là Ashley và tôi là Trưởng nhóm hỗ trợ kỹ thuật khách hàng cho hoạt động bán hàng hoạt động bảo mật tại Google. Tôi sẽ hướng dẫn bạn về các miền, khuôn khổ và biện pháp kiểm soát bảo mật cũng như các mối đe dọa, rủi ro và lỗ hổng bảo mật phổ biến. Bạn cũng sẽ được giới thiệu các công cụ phổ biến được các nhà phân tích bảo mật sử dụng. Tôi nóng lòng muốn bắt đầu!

Hi there! My name is Chris, and I'm the Chief Information Security Officer for Google Fiber. I'm excited to talk to you about the structure of a network, network protocols, common network attacks, and how to secure a network.

Chào bạn! Tên tôi là Chris và tôi là Giám đốc An ninh Thông tin của Google Fiber. Tôi rất vui được nói chuyện với bạn về cấu trúc của mạng, các giao thức mạng, các cuộc tấn công mạng phổ biến và cách bảo mật mạng.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Hi there! My name is Kim, and I'm a Technical Program Manager at Google. I will guide you through foundational computing skills that support the work of a security analyst. We'll also learn about operating systems, the Linux command line, and SQL.

Chào bạn! Tên tôi là Kim và tôi là Giám đốc chương trình kỹ thuật tại Google. Tôi sẽ hướng dẫn bạn các kỹ năng tính toán cơ bản hỗ trợ công việc của một nhà phân tích bảo mật. Chúng ta cũng sẽ tìm hiểu về hệ điều hành, dòng lệnh Linux và SQL.

Hi! My name is Da'Queshia, and I'm a Security Engineer at Google. Together we'll explore protecting organizational assets through a variety of security controls and develop a deeper understanding of risks and vulnerabilities.

CHÀO! Tên tôi là Da'Queshia và tôi là Kỹ sư bảo mật tại Google. Cùng nhau, chúng ta sẽ khám phá việc bảo vệ tài sản của tổ chức thông qua nhiều biện pháp kiểm soát bảo mật khác nhau và phát triển sự hiểu biết sâu sắc hơn về các rủi ro và lỗ hổng bảo mật.

Hi! My name is Dave, and I'm a Principal Security Strategist at Google. In our time together, we'll learn about detecting and responding to security incidents. You'll also have the chance to monitor and analyze network activity using powerful security tools.

CHÀO! Tên tôi là Dave và tôi là Nhà chiến lược bảo mật chính tại Google. Trong thời gian cùng nhau, chúng ta sẽ tìm hiểu về cách phát hiện và ứng phó với các sự cố bảo mật. Bạn cũng sẽ có cơ hội giám sát và phân tích hoạt động mạng bằng các công cụ bảo mật mạnh mẽ.

Hello! I'm Angel, and I'm a Security Engineer at Google. We'll explore foundational Python programming concepts to help you automate common security tasks.

Xin chào! Tôi là Angel và tôi là Kỹ sư bảo mật tại Google. Chúng ta sẽ khám phá các khái niệm lập trình Python cơ bản để giúp bạn tự động hóa các tác vụ bảo mật phổ biến.

Hello! I'm Dion. I'm a Program Manager at Google. I'm your instructor for the first portion of the final course of the program. There, we'll discuss how to escalate incidents and communicate with stakeholders.

Xin chào! Tôi là Dion. Tôi là Người quản lý chương trình tại Google. Tôi là người hướng dẫn bạn phần đầu tiên của khóa học cuối cùng của chương trình. Ở đó, chúng ta sẽ thảo luận cách báo cáo sự cố và liên lạc với các bên liên quan.

And my name is Emily. I'm a Program Manager at Google. I'll guide you through the final portion of the program and share ways that you can engage with the security community and prepare for your upcoming job search.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Và tên tôi là Emily. Tôi là Người quản lý chương trình tại Google. Tôi sẽ hướng dẫn bạn qua phần cuối cùng của chương trình và chia sẻ những cách mà bạn có thể tương tác với cộng đồng bảo mật và chuẩn bị cho quá trình tìm kiếm việc làm sắp tới của mình.

And, as you already know, I'll guide you through the first course of this program. This is such a great time to grow your career in the field of security. Sound exciting? Let's get started!

Và như bạn đã biết, tôi sẽ hướng dẫn bạn khóa học đầu tiên của chương trình này. Đây là thời điểm tuyệt vời để phát triển sự nghiệp của bạn trong lĩnh vực an ninh. Nghe có vẻ thú vị? Bắt đầu nào!

1.2. Google Cybersecurity Certificate overview – Tổng quan về Chứng chỉ an ninh mạng của Google

Hello, and welcome to the Google Cybersecurity Certificate! In this program, you will explore the growing field of cybersecurity, learn how cybersecurity is crucial to organizations and the people they serve, and develop relevant skills for a future career in the field. By completing the eight courses in this certificate program, you'll prepare for entry level jobs in cybersecurity, such as cybersecurity analyst, security analyst, and security operations center (SOC) analyst. No prior experience in cybersecurity is required to complete this program.

Xin chào và chào mừng bạn đến với Chứng chỉ an ninh mạng của Google! Trong chương trình này, bạn sẽ khám phá lĩnh vực an ninh mạng đang phát triển, tìm hiểu tầm quan trọng của an ninh mạng đối với các tổ chức và những người mà họ phục vụ, đồng thời phát triển các kỹ năng liên quan cho sự nghiệp tương lai trong lĩnh vực này. Bằng cách hoàn thành tám khóa học trong chương trình chứng chỉ này, bạn sẽ chuẩn bị để vào học

các công việc cấp cao trong lĩnh vực an ninh mạng, chẳng hạn như nhà phân tích an ninh mạng, nhà phân tích bảo mật và nhà phân tích trung tâm điều hành bảo mật (SOC). Không cần có kinh nghiệm trước đó về an ninh mạng để hoàn thành chương trình này.

Enter a growing field

Why are skills in cybersecurity in such high demand? The world is undergoing a digital transformation. Every day, global access to the internet is expanding, introducing more devices, more applications, and an even larger amount of data to the World Wide Web. As a result, threats, risks, and vulnerabilities are expanding and causing a significant amount of harm to organizations and people. Cybersecurity professionals are in high demand to help keep organizations, people, and data safe.

Throughout the program, you will have multiple opportunities to develop your cybersecurity knowledge and skills. You will explore concepts and scenarios to learn what an entry-level cybersecurity analyst must know and be able to do to thrive in the cybersecurity profession.

Nhập một lĩnh vực đang phát triển

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Tại sao kỹ năng về an ninh mạng lại có nhu cầu cao như vậy? Thế giới đang trải qua quá trình chuyển đổi kỹ thuật số. Mỗi ngày, khả năng truy cập Internet toàn cầu đang mở rộng, giới thiệu nhiều thiết bị hơn, nhiều ứng dụng hơn và lượng dữ liệu thậm chí còn lớn hơn cho World Wide Web. Do đó, các mối đe dọa, rủi ro và lỗ hổng ngày càng mở rộng và gây ra thiệt hại đáng kể cho các tổ chức và con người. Các chuyên gia an ninh mạng đang có nhu cầu cao để giúp giữ an toàn cho các tổ chức, con người và dữ liệu.

Trong suốt chương trình, bạn sẽ có nhiều cơ hội để phát triển kiến thức và kỹ năng về an ninh mạng của mình. Bạn sẽ khám phá các khái niệm và kịch bản để tìm hiểu những điều mà một nhà phân tích an ninh mạng cấp độ đầu vào phải biết và có thể làm để phát triển mạnh trong nghề an ninh mạng.

Google Cybersecurity Certificate courses

The Google Cybersecurity Certificate has eight courses that focus and build upon core concepts and skills related to the daily work of cybersecurity professionals, including foundational cybersecurity models and frameworks that are used to mitigate risk; protecting networks and data; using programming to automate tasks; identifying and responding to security incidents; and communicating and collaborating with stakeholders. Additionally, you will apply what you've learned in each course by completing portfolio projects that can be used to showcase your understanding of essential cybersecurity concepts to potential employers. The courses of the program are as follows:

Các khóa học Chứng chỉ An ninh mạng của Google

Chứng chỉ An ninh mạng của Google có tám khóa học tập trung và xây dựng dựa trên các khái niệm và kỹ năng cốt lõi liên quan đến công việc hàng ngày của các chuyên gia an ninh mạng, bao gồm các mô hình và khuôn khổ an ninh mạng cơ bản được dùng để giảm thiểu rủi ro; bảo vệ mạng và dữ liệu; sử dụng lập trình để tự động hóa các nhiệm vụ; xác định và ứng phó với các sự cố an ninh; và giao tiếp và cộng tác với các bên liên quan. Ngoài ra, bạn sẽ áp dụng những gì đã học trong mỗi khóa học bằng cách hoàn thành các dự án danh mục đầu tư có thể được sử dụng để thể hiện sự hiểu biết của bạn về các khái niệm an ninh mạng thiết yếu với các nhà tuyển dụng tiềm năng. Các khóa học của chương trình như sau:

1. [Foundations of Cybersecurity](#).(current course)
2. [Play It Safe: Manage Security Risks](#)
3. [Connect and Protect: Networks and Network Security](#)
4. [Tools of the Trade: Linux and SQL](#)
5. [Assets, Threats, and Vulnerabilities](#)
6. [Sound the Alarm: Detection and Response](#)
7. [Automate Cybersecurity Tasks with Python](#)

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

8. [Put It to Work: Prepare for Cybersecurity Jobs](#)



Benefits for job seekers

After completing all eight courses, Google Cybersecurity Certificate graduates have access to job search resources, courtesy of Google. You'll have the opportunity to:

- Build your resume, participate in mock interviews, and receive job search tips through Big Interview, a job-training platform that's free for program graduates.
- Improve your interview technique with Interview Warmup, a tool built by Google with certificate graduates in mind. Access cybersecurity-specific practice questions, transcripts of your responses, and automatic insights that help you grow your skills and confidence.
- Access thousands of job postings and free one-on-one career coaching with Career Circle. (You must be eligible to work in the U.S. to join.)
- Claim your Google Cybersecurity Certificate badge, and share your achievement on LinkedIn® professional networking services to stand out among other candidates to potential employers.
- Prepare for the CompTIA Security+ exam, the industry-leading certification for cybersecurity roles. You'll earn a dual credential when you complete both the Google Cybersecurity Certificate and the CompTIA Security+ exam.

Congratulations on taking this first step to build your skills for a career in cybersecurity. Enjoy the journey!

Lợi ích cho người tìm việc

Sau khi hoàn thành tất cả tám khóa học, sinh viên tốt nghiệp Chứng chỉ An ninh mạng của Google có quyền truy cập vào các tài nguyên tìm kiếm việc làm do Google cung cấp. Bạn sẽ có cơ hội:

- Xây dựng sơ yếu lý lịch của bạn, tham gia các cuộc phỏng vấn thử và nhận các mẹo tìm việc làm thông qua Big Interview, một nền tảng đào tạo việc làm miễn phí cho sinh viên tốt nghiệp chương trình.
- Cải thiện kỹ thuật phỏng vấn của bạn với Phỏng vấn khởi động, một công cụ do Google xây dựng dành cho những sinh viên tốt nghiệp có chứng chỉ. Truy cập các câu hỏi thực hành dành riêng cho an ninh mạng, bản ghi câu trả lời của bạn và thông tin chi tiết tự động giúp bạn phát triển kỹ năng và sự tự tin của mình.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

- Truy cập hàng nghìn tin tuyển dụng và huấn luyện nghề nghiệp trực tiếp miễn phí với Vòng tròn nghề nghiệp. (Bạn phải đủ điều kiện làm việc tại Hoa Kỳ để tham gia.)
- Yêu cầu huy hiệu Chứng chỉ an ninh mạng của Google và chia sẻ thành tích của bạn trên các dịch vụ mạng chuyên nghiệp LinkedIn® để nổi bật giữa các ứng viên khác với các nhà tuyển dụng tiềm năng.
- Chuẩn bị cho kỳ thi CompTIA Security+, chứng chỉ hàng đầu trong ngành về vai trò an ninh mạng. Bạn sẽ nhận được chứng chỉ kép khi hoàn thành cả Chứng chỉ an ninh mạng của Google và bài kiểm tra CompTIA Security+.

Chúc mừng bạn đã thực hiện bước đầu tiên này để xây dựng kỹ năng cho sự nghiệp trong lĩnh vực an ninh mạng. Tận hưởng cuộc hành trình!

1.3. Course 1 overview – Tổng quan về khóa 1



to Course 1

Hello and welcome to **Foundations of Cybersecurity** the first course in the Google Cybersecurity Certificate. You've begun an exciting journey!

In this course you will learn the primary job responsibilities and core skills of those who work in the field of cybersecurity. You will explore the eight Certified Information Systems Security Professional (CISSP) security domains various security frameworks and controls as well as a foundational security model called the confidentiality integrity and availability (CIA) triad. You will also be introduced to some common tools used by security analysts that help protect organizations and people alike.

Xin chào và chào mừng bạn đến với Khóa học cơ bản về an ninh mạng, khóa học đầu tiên trong Chứng chỉ an ninh mạng của Google. Bạn đã bắt đầu một cuộc hành trình thú vị!

Trong khóa học này, bạn sẽ tìm hiểu các trách nhiệm công việc chính và kỹ năng cốt lõi của những người làm việc trong lĩnh vực an ninh mạng. Bạn sẽ khám phá tám miền bảo mật của Chuyên gia Bảo mật Hệ thống Thông tin được Chứng nhận (CISSP), các khuôn khổ và biện pháp kiểm soát bảo mật khác nhau cũng như mô hình bảo mật nền tảng được gọi là bộ ba tính toàn vẹn và sẵn sàng bảo mật (CIA). Bạn cũng sẽ được giới thiệu một số công cụ phổ biến được các nhà phân tích bảo mật sử dụng để giúp bảo vệ các tổ chức cũng như con người.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. Foundations of Cybersecurity is the first course.

Tiến độ chương trình chứng chỉ

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. Nền tảng của An ninh mạng là khóa học đầu tiên.



1. [Foundations of Cybersecurity](#) - Gain an understanding of network-level vulnerabilities and how to secure networks.
2. [Play It Safe: Manage Security Risks](#) - Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
3. [Connect and Protect: Networks and Network Security](#) - Gain an understanding of network-level vulnerabilities and how to secure networks.
4. [Tools of the Trade: Linux and SQL](#) - Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
5. [Assets, Threats, and Vulnerabilities](#) - Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
6. [Sound the Alarm: Detection and Response](#) - Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. [Automate Cybersecurity Tasks with Python](#) - Explore the Python programming language and write code to automate cybersecurity tasks.
8. [Put It to Work: Prepare for Cybersecurity Jobs](#) - Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

1. [Foundations of Cybersecurity](#) - Hiểu biết về các lỗ hổng ở cấp độ mạng và cách bảo mật mạng.
2. [Play It Safe: Manage Security Risks](#) - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
3. [Connect and Protect: Networks and Network Security](#) - Hiểu biết về các lỗ hổng cấp độ mạng và cách bảo mật mạng.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

4. [Tools of the Trade: Linux and SQL](#) - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
5. [Assets, Threats, and Vulnerabilities](#) - Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.
6. [Sound the Alarm: Detection and Response](#) - Hiểu rõ vòng đời ứng phó sự cố và thực hành sử dụng các công cụ phát hiện và ứng phó sự cố an ninh mạng.
7. [Automate Cybersecurity Tasks with Python](#) - Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. [Put It to Work: Prepare for Cybersecurity Jobs](#) - Tìm hiểu về phân loại sự cố, trình báo và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

Course 1 content

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

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

Nội dung khóa 1

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

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

Module 1: Welcome to the exciting world of cybersecurity

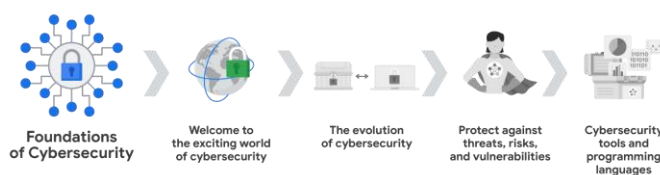
Begin your journey into cybersecurity! You'll explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals.

Mô-đun 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Bắt đầu hành trình của bạn vào an ninh mạng! Bạn sẽ khám phá lĩnh vực an ninh mạng và tìm hiểu về trách nhiệm công việc của các chuyên gia an ninh mạng.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

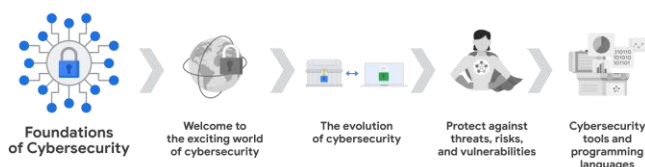


Module 2: The evolution of cybersecurity

You will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. You will also understand how past and present cyber attacks have influenced the development of the security field. In addition, you'll get an overview of the eight security domains.

Mô-đun 2: Sự phát triển của an ninh mạng

Bạn sẽ khám phá các mối đe dọa an ninh mạng đã xuất hiện và phát triển như thế nào cùng với việc sử dụng máy tính. Bạn cũng sẽ hiểu các cuộc tấn công mạng trong quá khứ và hiện tại đã ảnh hưởng như thế nào đến sự phát triển của lĩnh vực bảo mật. Ngoài ra, bạn sẽ có được cái nhìn tổng quan về tám lĩnh vực bảo mật.



Module 3: Protect against threats, risks, and vulnerabilities

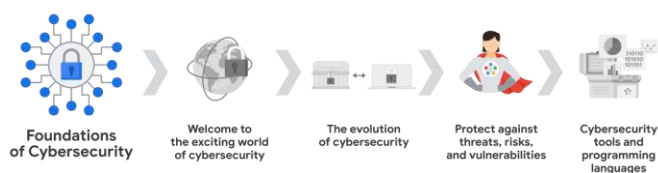
You will learn about security frameworks and controls, which are used to mitigate organizational risk. You'll cover principles of the CIA triad and various National Institute of Standards and Technology (NIST) frameworks. In addition, you'll explore security ethics.

Mô-đun 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Bạn sẽ tìm hiểu về các khuôn khổ và biện pháp kiểm soát bảo mật được sử dụng để giảm thiểu rủi ro cho tổ chức. Bạn sẽ đề cập đến các nguyên tắc của bộ ba CIA và các khuôn khổ khác nhau của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Ngoài ra, bạn sẽ khám phá đạo đức bảo mật.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

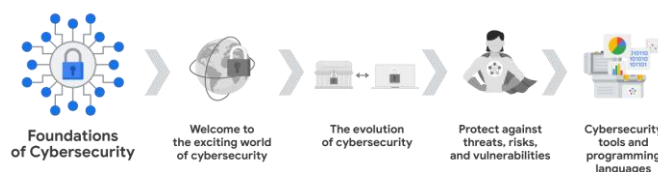


Module 4: Cybersecurity tools and programming languages

You'll discover common tools used by cybersecurity analysts to identify and eliminate risk. You'll learn about security information and event management (SIEM) tools, network protocol analyzers, and programming languages such as Python and SQL.

Mô-đun 4: Công cụ an ninh mạng và ngôn ngữ lập trình

Bạn sẽ khám phá các công cụ phổ biến được các nhà phân tích an ninh mạng sử dụng để xác định và loại bỏ rủi ro. Bạn sẽ tìm hiểu về các công cụ quản lý sự kiện và thông tin bảo mật (SIEM), bộ phân tích giao thức mạng và các ngôn ngữ lập trình như Python và SQL.



Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

What to expect

Each course offers many types of learning opportunities:

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

Những gì mong đợi

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

- **Các video** do người hướng dẫn của Google dẫn dắt dạy các khái niệm mới, giới thiệu cách sử dụng các công cụ có liên quan, cung cấp hỗ trợ nghề nghiệp và cung cấp những câu chuyện cá nhân đầy cảm hứng.
- **Bài đọc** được xây dựng dựa trên các chủ đề được thảo luận trong video, giới thiệu các khái niệm liên quan, chia sẻ các tài nguyên hữu ích và mô tả các nghiên cứu điển hình.
- **Lời nhắc thảo luận** khám phá các chủ đề khóa học để hiểu rõ hơn và cho phép bạn trò chuyện cũng như trao đổi ý tưởng với những người học khác trong diễn đàn thảo luận.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

- **Các hoạt động tự đánh giá và phòng thí nghiệm** giúp bạn thực hành thực hành trong việc áp dụng các kỹ năng bạn đang học và cho phép bạn đánh giá bài làm của chính mình bằng cách so sánh nó với một ví dụ hoàn chỉnh.
- **Các plug-in tương tác** khuyến khích bạn thực hành các nhiệm vụ cụ thể và giúp bạn tích hợp kiến thức bạn đã thu được trong khóa học.
- **Các câu đố trong video** giúp bạn kiểm tra mức độ hiểu của mình khi bạn xem qua từng video.
- **Các câu hỏi thực hành** cho phép bạn kiểm tra sự hiểu biết của mình về các khái niệm chính và cung cấp những phản hồi có giá trị.
- **Các câu hỏi được chấm điểm** thể hiện sự hiểu biết của bạn về các khái niệm chính của khóa học. Bạn phải đạt 80% điểm trở lên trong mỗi bài kiểm tra được xếp loại để nhận được chứng chỉ và bạn có thể làm bài kiểm tra được xếp loại nhiều lần để đạt được điểm đậu.

Tips for success

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

Lời khuyên để thành công

- Chúng tôi đặc biệt khuyên bạn nên xem qua các mục trong mỗi bài học theo thứ tự xuất hiện vì thông tin và khái niệm mới được xây dựng dựa trên kiến thức trước đó.
- Tham gia vào mọi cơ hội học tập để có được càng nhiều kiến thức và kinh nghiệm càng tốt

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

- Nếu có điều gì đó khó hiểu, đừng ngần ngại phát lại video, xem lại bài đọc hoặc lặp lại hoạt động tự xem xét.
- Sử dụng các tài nguyên bổ sung được tham khảo 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 tab Tài nguyên.
- Khi bạn gặp những liên kết hữu ích trong khóa học này, hãy đánh dấu chúng để bạn có thể tham khảo thông tin sau này để nghiên cứu hoặc ôn tập.
- Hiểu và tuân theo Quy tắc ứng xử của Coursera để đảm bảo rằng cộng đồng học tập vẫn là nơi thân thiện, thân thiện và hỗ trợ cho tất cả các thành viên.

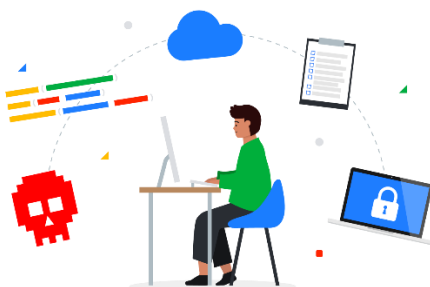
1.4. Your Google Cybersecurity Certificate roadmap – Lộ trình Chứng chỉ An ninh mạng của Google của bạn

Your Google Cybersecurity Certificate roadmap

Use this guide to review the topics covered, tools used, and skills you will gain in each course.

Lộ trình Chứng chỉ An ninh mạng của Google của bạn

Sử dụng hướng dẫn này để xem lại các chủ đề được đề cập, các công cụ được sử dụng và kỹ năng bạn sẽ đạt được trong mỗi khóa học.



Which course?

For details on topics covered, tools used, and skills you will gain, select the course you'd like to learn more about.

Khóa học nào?

Để biết thông tin chi tiết về các chủ đề được đề cập, các công cụ được sử dụng và kỹ năng bạn sẽ đạt được, hãy chọn khóa học bạn muốn tìm hiểu thêm.

What tools, solutions, or platforms are included in the curriculum?

The curriculum includes SIEM tools, playbooks, network and cloud security, network protocol analyzers, and programming languages.

Do I need to take the courses in a certain order?

We highly recommend completing the courses in the order presented. The content in each course builds on information from previous lessons.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Do I need to have a background in cybersecurity?

This certificate program is for learners with little to no experience in the cybersecurity field.

How will I develop a professional cybersecurity portfolio?

Throughout the program, you will have multiple opportunities to apply what you learn in order to create a compelling, relevant portfolio to share during your job search.

Những công cụ, giải pháp hoặc nền tảng nào được đưa vào chương trình giảng dạy?

Chương trình giảng dạy bao gồm các công cụ SIEM, sách hướng dẫn, bảo mật mạng và đám mây, máy phân tích giao thức mạng và ngôn ngữ lập trình.

Tôi có cần tham gia các khóa học theo một thứ tự nhất định không?

Chúng tôi thực sự khuyên bạn nên hoàn thành các khóa học theo thứ tự được trình bày. Nội dung trong mỗi khóa học được xây dựng dựa trên thông tin từ các bài học trước.

Tôi có cần phải có kiến thức nền tảng về an ninh mạng không?

Chương trình chứng chỉ này dành cho người học có ít hoặc không có kinh nghiệm trong lĩnh vực an ninh mạng.

Làm cách nào tôi có thể phát triển danh mục đầu tư an ninh mạng chuyên nghiệp?

Trong suốt chương trình, bạn sẽ có nhiều cơ hội áp dụng những gì mình học được để tạo ra một danh mục đầu tư hấp dẫn, phù hợp để chia sẻ trong quá trình tìm kiếm việc làm của mình.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

1. Foundations of Cybersecurity



In this course, you will:

- Define the field of security
- Recognize core skills and knowledge needed to become a security analyst
- Identify how security attacks impact business operations
- Identify eight security domains
- Define security frameworks and controls

Skill sets:

- Communicating effectively
- Collaborating with others
- Identifying threats, risks, and vulnerabilities
- Problem-solving

Trong khóa học này, bạn sẽ:

- Xác định lĩnh vực bảo mật
- Nhận biết các kỹ năng và kiến thức cốt lõi cần thiết để trở thành nhà phân tích bảo mật
- Xác định các cuộc tấn công bảo mật ảnh hưởng đến hoạt động kinh doanh như thế nào
- Xác định tám miền bảo mật
- Xác định các khuôn khổ và biện pháp kiểm soát bảo mật

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Bộ kỹ năng:

- Giao tiếp hiệu quả
- Cộng tác với người khác
- Xác định các mối đe dọa, rủi ro và lỗ hổng
- Giải quyết vấn đề

2. *Play It Safe: Manage Security Risks*



In this course, you will:

- Recognize and explain the focus of eight security domains
- Identify the steps of risk management
- Describe the CIA triad
- Identify security principles
- Define and describe the purpose of a playbook
- Explain how entry-level security analysts use SIEM dashboards

Skill sets:

- Applying the CIA triad to workplace situations
- Analyzing log data
- Identifying the phases of an incident response playbook

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Trong khóa học này, bạn sẽ:

- Nhận biết và giải thích trọng tâm của tám lĩnh vực bảo mật
- Xác định các bước quản lý rủi ro
- Mô tả bộ ba CIA
- Xác định các nguyên tắc bảo mật
- Xác định và mô tả mục đích của playbook
- Giải thích cách các nhà phân tích bảo mật cấp cơ bản sử dụng bảng thông tin SIEM

Bộ kỹ năng:

- Áp dụng bộ ba CIA vào các tình huống tại nơi làm việc
- Phân tích dữ liệu nhật ký
- Xác định các giai đoạn của cảm nang ứng phó sự cố

3. *Connect and Protect: Networks and Network Security*



In this course, you will:

- Define types of networks
- Explain how data is sent and received over a network
- Recognize common network protocols
- Compare and contrast local networks to cloud computing
- Explain how to secure a network against intrusion tactics

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Skill sets:

- Configuring a firewall
- Recognizing components of computer networks and cloud computing
- Analyzing threats
- Implementing security hardening

Trong khóa học này, bạn sẽ:

- Xác định các loại mạng
- Giải thích cách gửi và nhận dữ liệu qua mạng
- Nhận biết các giao thức mạng phổ biến
- So sánh và đối chiếu mạng cục bộ với điện toán đám mây
- Giải thích cách bảo mật mạng khỏi các chiến thuật xâm nhập

Bộ kỹ năng:

- Cấu hình tường lửa
- Nhận biết các thành phần của mạng máy tính và điện toán đám mây
- Phân tích các mối đe dọa
- Thực hiện tăng cường an ninh

4. Tools of the Trade: Linux and SQL



Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

In this course, you will:

- Describe the main functions of an operating system
- Explain the relationship between operating systems, applications, and hardware
- Compare a graphical user interface to a command line interface
- Navigate the file system using Linux commands via the Bash shell
- Use SQL to retrieve information from a database

Skill sets:

- Interacting with both a graphical user interface (GUI) and command line interface (CLI)
- Querying a database with SQL
- Filtering on a particular word with the Linux command line
- Authenticating and authorizing users with the Linux command line

Trong khóa học này, bạn sẽ:

- Nêu chức năng chính của hệ điều hành
- Giải thích mối quan hệ giữa hệ điều hành, ứng dụng và phần cứng
- So sánh giao diện người dùng đồ họa với giao diện dòng lệnh
- Điều hướng hệ thống tệp bằng lệnh Linux thông qua shell Bash
- Sử dụng SQL để lấy thông tin từ cơ sở dữ liệu

Bộ kỹ năng:

- Tương tác với cả giao diện người dùng đồ họa (GUI) và giao diện dòng lệnh (CLI)
- Truy vấn cơ sở dữ liệu bằng SQL
- Lọc một từ cụ thể bằng dòng lệnh Linux
- Xác thực và ủy quyền người dùng bằng dòng lệnh Linux

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

5. Assets, Threats, and Vulnerabilities



In this course, you will:

- Explain security's role in mitigating organizational risk
- Describe the defense in depth strategy
- Explain how vulnerability assessments are used to assess potential risk
- Develop an attacker mindset to recognize threats
- Discuss the role encryption and hashing play in securing assets
- Identify forms of social engineering, malware, and web-based exploits

Skill sets:

- Classifying assets
- Decrypting a message
- Searching the CVE database for vulnerable applications
- Analyzing attack surfaces
- Applying the PASTA threat modeling framework

Trong khóa học này, bạn sẽ:

- Giải thích vai trò của bảo mật trong việc giảm thiểu rủi ro tổ chức
- Mô tả chiến lược phòng thủ theo chiều sâu
- Giải thích cách sử dụng đánh giá lỗ hổng để đánh giá rủi ro tiềm ẩn
- Phát triển tư duy của kẻ tấn công để nhận ra các mối đe dọa
- Thảo luận về vai trò của mã hóa và băm trong việc bảo mật tài sản
- Xác định các hình thức tấn công kỹ thuật xã hội, phần mềm độc hại và khai thác dựa trên web

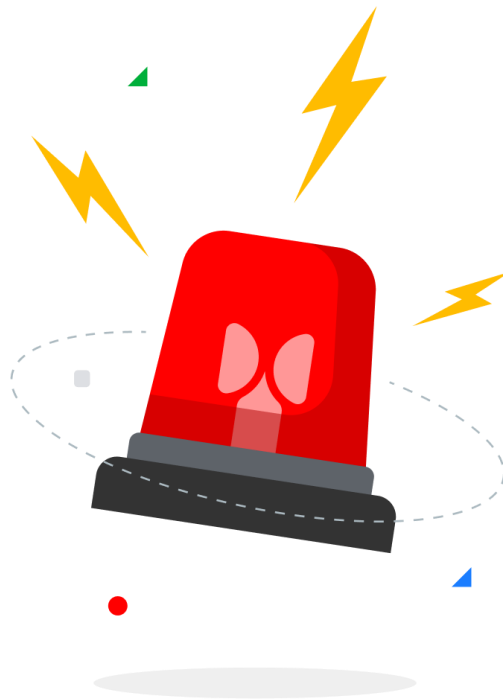
Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Bộ kỹ năng:

- Phân loại tài sản
- Giải mã tin nhắn
- Tìm kiếm cơ sở dữ liệu CVE để tìm các ứng dụng dễ bị tấn công
- Phân tích bề mặt tấn công
- Áp dụng khung mô hình hóa mối đe dọa PASTA

6. Sound the Alarm: Detection and Response



In this course, you will:

- Explain the lifecycle of an incident
- Use packet sniffing tools to capture and view network communications
- Perform artifact investigations to analyze and verify security incidents
- Identify the steps to contain, eradicate, and recover from an incident
- Interpret the basic syntax and components of signatures and logs in IDS and NIDS tools

Skill sets:

- Capturing, viewing, and analyzing a packet
- Investigating a suspicious hash file
- Following a playbook
- Examining alerts, logs, and rules
- Performing queries with SIEM tools

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

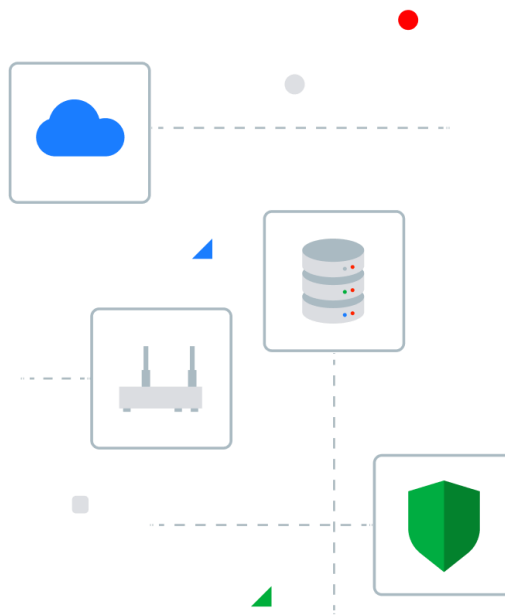
Trong khóa học này, bạn sẽ:

- Giải thích vòng đời của một sự cố
- Sử dụng các công cụ đánh hơi gói để nắm bắt và xem thông tin liên lạc trên mạng
- Thực hiện điều tra giả tạo để phân tích và xác minh các sự cố bảo mật
- Xác định các bước để ngăn chặn, loại bỏ và phục hồi sau sự cố
- Giải thích cú pháp cơ bản và các thành phần của chữ ký và nhật ký trong công cụ IDS và NIDS

Bộ kỹ năng:

- Chụp, xem và phân tích gói tin
- Điều tra một tệp băm đáng ngờ
- Theo dõi một vở kịch
- Kiểm tra cảnh báo, nhật ký và quy tắc
- Thực hiện truy vấn bằng công cụ SIEM

7. [Automate Cybersecurity Tasks with Python](#)



In this course, you will:

- Explain how the Python programming language is used in security
- Write a simple algorithm
- Use regular expressions in Python to extract information from text
- Use Python to automate tasks performed by security professionals
- Use Python to parse a file

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Skill sets:

- Working with strings and their index values
- Applying regular expressions (regex)
- Importing and parsing a file
- Debugging code

Trong khóa học này, bạn sẽ:

- Giải thích cách sử dụng ngôn ngữ lập trình Python trong bảo mật
- Viết một thuật toán đơn giản
- Sử dụng biểu thức chính quy trong Python để trích xuất thông tin từ văn bản
- Sử dụng Python để tự động hóa các tác vụ được thực hiện bởi các chuyên gia bảo mật
- Sử dụng Python để phân tích một tệp

Bộ kỹ năng:

- Làm việc với các chuỗi và giá trị chỉ mục của chúng
- Áp dụng biểu thức chính quy (regex)
- Nhập và phân tích tệp
- Mã gỡ lỗi

8. [Put It to Work: Prepare for Cybersecurity Jobs](#)



Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

In this course, you will:

- Define stakeholders and describe their security roles
- Communicate sensitive information with care and confidentiality
- Identify reliable sources within the security community
- Determine opportunities to become engaged with the security community
- Determine ways to establish and advance a career in security, by engaging with the security community
- Find, apply for, and prepare for job interviews

Skill sets:

- Creating a dashboard
- Creating or updating a resume
- Using the STAR method for interview questions
- Drafting an elevator pitch

Trong khóa học này, bạn sẽ:

- Xác định các bên liên quan và mô tả vai trò bảo mật của họ
- Truyền đạt thông tin nhạy cảm một cách cẩn thận và bảo mật
- Xác định các nguồn đáng tin cậy trong cộng đồng bảo mật
- Xác định cơ hội tham gia với cộng đồng bảo mật
- Xác định các cách để thiết lập và phát triển sự nghiệp trong lĩnh vực bảo mật bằng cách tham gia vào cộng đồng bảo mật
- Tìm, nộp đơn và chuẩn bị cho các cuộc phỏng vấn việc làm

Bộ kỹ năng:

- Tạo bảng điều khiển
- Tạo hoặc cập nhật sơ yếu lý lịch
- Sử dụng phương pháp STAR cho các câu hỏi phỏng vấn
- Soạn thảo một quảng cáo chiêu hàng

1.5. Welcome to week 1 – Chào mừng đến với tuần 1

Hi again! Now that you have some idea of what to expect from the program as a whole, let's discuss more about what you'll learn in this course.

Chào bạn lần nữa nhé! Bây giờ bạn đã có một số ý tưởng về những gì mong đợi từ toàn bộ chương trình, hãy thảo luận thêm về những gì bạn sẽ học trong khóa học này.

This course will introduce you to the world of security and how it's used to protect business operations, users, and devices, so you can contribute to the creation of a safer internet for all.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Khóa học này sẽ giới thiệu cho bạn về thế giới bảo mật và cách nó được sử dụng để bảo vệ hoạt động kinh doanh, người dùng và thiết bị, để bạn có thể góp phần tạo ra một mạng Internet an toàn hơn cho tất cả mọi người.

In this section, we'll cover foundational security concepts. First, we'll define security. Then, we'll explore common job responsibilities of security analysts. Building on that, we'll cover core skills a security analyst may have. Finally, we'll discuss the value of security for protecting organizations and people.

Trong phần này, chúng tôi sẽ đề cập đến các khái niệm bảo mật cơ bản. Đầu tiên, chúng ta sẽ định nghĩa bảo mật. Sau đó, chúng ta sẽ khám phá trách nhiệm công việc chung của các nhà phân tích bảo mật. Dựa trên đó, chúng tôi sẽ đề cập đến các kỹ năng cốt lõi mà một nhà phân tích bảo mật có thể có. Cuối cùng, chúng ta sẽ thảo luận về giá trị của bảo mật trong việc bảo vệ các tổ chức và con người.

Later on, we'll cover eight security domains. Then, we'll cover common security frameworks and controls. Finally, we'll wrap up the course by discussing common tools and programming languages that entry-level security analysts may use.

Sau này, chúng tôi sẽ đề cập đến tám lĩnh vực bảo mật. Sau đó, chúng tôi sẽ đề cập đến các khuôn khổ và biện pháp kiểm soát bảo mật phổ biến. Cuối cùng, chúng ta sẽ kết thúc khóa học bằng cách thảo luận về các công cụ và ngôn ngữ lập trình phổ biến mà các nhà phân tích bảo mật cấp cơ bản có thể sử dụng.

Coming up, we'll go over some resources that will allow you to get the most out of this program. I'm really excited for you to start this journey--let's begin!

Sắp tới, chúng ta sẽ đi qua một số tài nguyên cho phép bạn tận dụng tối đa chương trình này. Tôi thực sự vui mừng khi bạn bắt đầu cuộc hành trình này--hãy bắt đầu!

1.6. Commit to completing the program – Cam kết hoàn thành chương trình

1.7. Helpful resources and tips – Tài nguyên và lời khuyên hữu ích

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

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

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Course completion to obtain a certificate

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

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

Hoàn thành khóa học để được cấp chứng chỉ

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

- [Trả phí chứng chỉ khóa học](#) hoặc [nộp đơn và được chấp thuận nhận học bổng Coursera](#).
- Vượt qua tất cả các câu hỏi được chấm điểm trong 8 khóa học với số điểm ít nhất là 80%. Mỗi bài kiểm tra được chấm điểm trong một khóa học là một phần của điểm tích lũy cho khóa học đó.

Healthy habits for course completion

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

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

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.
- **Build your career identity:** Your career identity is the unique value you bring to the workforce. [Watch this video](#) to learn about the key components of career identity and write your own career identity statement. Discovering and defining your own career identity makes you better equipped to choose a career path that aligns with your strengths, values, and goals and is more effective in your chosen profession.
- **Connect with other learners:** If you have a question, chances are, you're not alone. Reach out in the discussion forum to ask for help from other learners in this program. You can also visit Coursera's private Google Cybersecurity Community to expand your network, discuss career journeys, and share experiences. Check out the quick start guide.
- **Update your profile:** Consider updating your profile on Coursera with 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.

Thói quen lành mạnh khi hoàn thành khóa học

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

- **Lập kế hoạch thời gian của bạn:** Đặt thời gian học tập thường xuyên và tuân theo chúng mỗi tuần có thể giúp bạn biến việc học trở thành một phần thói quen của mình. Sử dụng lịch hoặc thời gian biểu để tạo lịch trình và liệt kê những việc bạn dự định làm mỗi ngày để đặt ra các mục tiêu có thể đạt được. Tìm một không gian cho phép bạn tập trung khi xem video, xem lại bài đọc và hoàn thành các hoạt động.
- **Làm việc theo tốc độ của riêng bạn:** Mọi người học theo cách khác nhau, vì vậy chương trình này được thiết kế để giúp bạn làm việc theo tốc độ của riêng mình. Mặc dù thời hạn được cá nhân hóa của bạn bắt đầu khi bạn đăng ký, nhưng hãy thoải mái chuyển qua chương trình với tốc độ phù hợp nhất với bạn. Không có hình phạt cho bài tập muộn; để có được chứng chỉ, tất cả những gì bạn phải làm là hoàn thành tất cả công việc. Bạn có thể gia hạn thời hạn của mình bất kỳ lúc nào bằng cách đi tới **Tổng quan** trong bảng điều hướng và chọn **Chuyển đổi phiên**. Nếu bạn đã bỏ lỡ thời hạn trước đó, hãy chọn **Đặt lại thời hạn của tôi**.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

- **Hãy tò mò:** Nếu bạn tìm thấy một ý tưởng khiến bạn hứng thú, hãy hành động theo nó! Đặt câu hỏi, tìm kiếm thêm chi tiết trực tuyến, khám phá các liên kết mà bạn quan tâm và ghi chú những khám phá của bạn. Các bước bạn thực hiện để hỗ trợ quá trình học tập của mình sẽ nâng cao kiến thức của bạn, tạo ra nhiều cơ hội hơn trong lĩnh vực có tốc độ tăng trưởng cao này và giúp bạn đủ điều kiện tìm việc làm.\
- **Ghi chú:** Ghi chú sẽ giúp bạn ghi nhớ những thông tin quan trọng trong tương lai, đặc biệt khi bạn đang chuẩn bị bước vào một lĩnh vực công việc mới. Ngoài ra, ghi chép là một cách hiệu quả để tạo sự kết nối giữa các chủ đề và hiểu rõ hơn về các chủ đề đó.
- **Xem lại các mẫu:** Các mẫu là các bài tập đã hoàn thành đáp ứng đầy đủ các tiêu chí của hoạt động. Nhiều hoạt động trong chương trình này có mẫu để bạn xác thực công việc của mình hoặc kiểm tra lỗi. Mặc dù thường có nhiều cách để hoàn thành nhiệm vụ nhưng các ví dụ mẫu sẽ đưa ra hướng dẫn và nguồn cảm hứng về cách hoàn thành hoạt động.
- **Xây dựng bản sắc nghề nghiệp của bạn:** Bản sắc nghề nghiệp của bạn là giá trị duy nhất mà bạn mang lại cho lực lượng lao động. [Xem video này](#) để tìm hiểu về các thành phần chính của bản sắc nghề nghiệp và viết tuyên bố về bản sắc nghề nghiệp của riêng bạn. Việc khám phá và xác định bản sắc nghề nghiệp của riêng bạn giúp bạn được trang bị tốt hơn để chọn con đường sự nghiệp phù hợp với thế mạnh, giá trị và mục tiêu của mình và hiệu quả hơn trong nghề nghiệp bạn đã chọn.
- **Kết nối với những người học khác:** Nếu bạn có câu hỏi, rất có thể bạn không đơn độc. Hãy liên hệ trong diễn đàn thảo luận để yêu cầu sự giúp đỡ từ những người học khác trong chương trình này. Bạn cũng có thể truy cập trang riêng của Coursera [Cộng đồng an ninh mạng của Google](#) để mở rộng mạng lưới của bạn, thảo luận về hành trình sự nghiệp và chia sẻ kinh nghiệm. [Kiểm tra hướng dẫn nhanh](#).
- **Cập nhật hồ sơ của bạn:** Hãy xem xét [cập nhật hồ sơ](#) của bạn trên Coursera với ảnh của bạn, mục tiêu nghề nghiệp, v.v. Khi những người học khác tìm thấy bạn trong các diễn đàn thảo luận, họ có thể nhấp vào tên của bạn để truy cập hồ sơ của bạn và hiểu rõ hơn về bạn.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Documents, spreadsheets, presentations, and labs for course activities

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

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

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

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

- [Microsoft Word: Help and learning](#): Trang hỗ trợ của Microsoft dành cho Word
- [Google Docs](#): Trang Trung tâm trợ giúp dành cho Google Documents
- [Microsoft Excel: Help and learning](#): Trang hỗ trợ của Microsoft dành cho Excel
- [Google Sheets](#): Trang Trung tâm trợ giúp dành cho Google Trang tính
- [Microsoft PowerPoint: Help and learning](#): Trang hỗ trợ của Microsoft dành cho PowerPoint
- [How to use Google Slides](#): Trang Trung tâm trợ giúp dành cho Google Trình trình bày
- [Common problems with labs](#): Trợ giúp khắc phục sự cố cho các hoạt động Qwiklabs

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Module, course, and certificate glossaries

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.
- **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.
- **Course glossaries:** At the end of each course, you can access and download a glossary that covers all of the terms in that course.

You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course's [Resources](#) section. To access the **Cybersecurity Certificate glossary**, click the link below and select Use Template.

- [Cybersecurity Certificate glossary](#)

OR

- If you don't have a Google account, you can download the glossary directly from the attachment below.

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

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

- **Bảng chú giải thuật ngữ của mô-đun:** Ở cuối nội dung của mỗi mô-đun, bạn có thể xem lại bảng chú giải thuật ngữ của mô-đun đó. Bảng thuật ngữ của mỗi mô-đun được xây dựng dựa trên các thuật ngữ từ các mô-đun trước đó trong khóa học đó. Bảng thuật ngữ mô-đun không thể tải xuống được; tuy nhiên, tất cả các thuật ngữ và định nghĩa đều có trong bảng thuật ngữ khóa học và chứng chỉ, có thể tải xuống được.
- **Bảng chú giải thuật ngữ chứng chỉ:** Bảng chú giải thuật ngữ chứng chỉ bao gồm tất cả các thuật ngữ trong toàn bộ chương trình chứng chỉ và là

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

nguồn tài nguyên hữu ích mà bạn có thể tham khảo trong suốt chương trình hoặc bất kỳ lúc nào trong tương lai.

- **Bảng thuật ngữ khóa học:** Vào cuối mỗi khóa học, bạn có thể truy cập và tải xuống bảng chú giải thuật ngữ bao gồm tất cả các thuật ngữ trong khóa học đó.

Bạn có thể truy cập và tải xuống bảng chú giải chứng chỉ và lưu chúng trên máy tính của mình. Bạn luôn có thể tìm thấy bảng thuật ngữ khóa học và chứng chỉ thông qua phần [Tài nguyên](#) của khóa học. Để truy cập bảng chú giải Chứng chỉ An ninh mạng, hãy nhấp vào liên kết bên dưới và chọn Sử dụng Mẫu.

- [Thuật ngữ chứng chỉ an ninh mạng](#)

HOẶC

- Nếu chưa có tài khoản Google, bạn có thể tải xuống bảng thuật ngữ trực tiếp từ tệp đính kèm bên dưới.

Course feedback

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

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

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

For technical help, visit the [Learner Help Center](#).

Phản hồi khóa học

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

- Hãy bấm nút thích để xem những tài liệu bạn thấy hữu ích.
- Hãy bấm nút không thích đối với những tài liệu mà bạn thấy không hữu ích.

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

Để được trợ giúp kỹ thuật, hãy truy cập [Trung tâm trợ giúp người học](#).

1.8. Participate in program surveys – Tham gia khảo sát chương trình

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Participate in program surveys

During this certificate program, you will be asked to complete a few short surveys. These are part of a research study being conducted to understand how effectively the certificate meets your career training needs. Keep reading for a summary of what each survey will cover.

Your survey participation is optional but extremely helpful in making this program as effective as possible. All data is kept confidential and is aggregated for review in accordance with [Coursera's privacy policy](#). Your name is separated from your data when it is stored.

There are no right or wrong answers. Your responses or personal data:

- Won't affect your program experience, scores, or ability to receive a certificate or job offer
- Won't be shared outside of our research team unless you give permission to share your contact information with hiring partners

Thanks for your consideration and time!

Tham gia khảo sát chương trình

Trong chương trình chứng chỉ này, bạn sẽ được yêu cầu hoàn thành một số khảo sát ngắn. Đây là một phần của nghiên cứu đang được thực hiện để hiểu mức độ hiệu quả của chứng chỉ đáp ứng nhu cầu đào tạo nghề nghiệp của bạn. Hãy tiếp tục đọc để biết bản tóm tắt về những nội dung mà mỗi cuộc khảo sát sẽ đề cập.

Việc tham gia khảo sát của bạn là tùy chọn nhưng cực kỳ hữu ích trong việc làm cho chương trình này hiệu quả nhất có thể. Tất cả dữ liệu được giữ bí mật và được tổng hợp để xem xét theo [chính sách quyền riêng tư của Coursera](#). Tên của bạn được tách khỏi dữ liệu của bạn khi nó được lưu trữ.

Không có câu trả lời đúng hay sai. Phản hồi hoặc dữ liệu cá nhân của bạn:

- Sẽ không ảnh hưởng đến trải nghiệm chương trình, điểm số hoặc khả năng nhận được chứng chỉ hoặc lời mời làm việc của bạn
- Sẽ không được chia sẻ ra bên ngoài nhóm nghiên cứu của chúng tôi trừ khi bạn cho phép chia sẻ thông tin liên hệ của mình với các đối tác tuyển dụng

Cảm ơn sự quan tâm và thời gian của bạn!

Entry survey

First, you will have an opportunity to answer a brief survey to help researchers understand why you enrolled in this certificate program. If you don't fill out the survey now, you will receive an invitation to fill it out after completing your first video or activity.

The survey asks about your experiences leading up to this program and the goals you hope to achieve. This is critical information to ensure your needs as a learner are met and that this program will continue to be offered in the future.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Khảo sát đầu vào

Đầu tiên, bạn sẽ có cơ hội trả lời một cuộc khảo sát ngắn gọn để giúp các nhà nghiên cứu hiểu lý do tại sao bạn đăng ký tham gia chương trình chứng chỉ này. Nếu không điền vào bản khảo sát ngay bây giờ, bạn sẽ nhận được lời mời điền vào bản khảo sát sau khi hoàn thành video hoặc hoạt động đầu tiên của mình.

Cuộc khảo sát hỏi về trải nghiệm của bạn khi tham gia chương trình này và những mục tiêu bạn hy vọng đạt được. Đây là thông tin quan trọng để đảm bảo đáp ứng nhu cầu của bạn với tư cách là người học và chương trình này sẽ tiếp tục được cung cấp trong tương lai.

Individual course feedback

After you complete the last graded assignment within an individual course, you might be asked to complete a survey. This survey will revisit questions from the previous survey and ask what you have learned up to that point in the program. Again, filling out this information is voluntary but extremely beneficial to the program and future learners.

Phản hồi khóa học cá nhân

Sau khi bạn hoàn thành bài tập được chấm điểm cuối cùng trong một khóa học riêng lẻ, bạn có thể được yêu cầu hoàn thành một bản khảo sát. Cuộc khảo sát này sẽ xem lại các câu hỏi từ cuộc khảo sát trước đó và hỏi bạn đã học được gì cho đến thời điểm đó trong chương trình. Xin nhắc lại, việc điền thông tin này là tự nguyện nhưng cực kỳ có lợi cho chương trình và người học sau này.

Certificate completion survey

After you complete the last graded assignment in the final (eighth) course of the certificate program, you will be asked to complete a survey that revisits some earlier questions and asks what you have learned throughout the duration of the program. This survey also asks whether you would like to share your contact information with prospective employers. Filling out the survey and sharing your contact information with prospective employers is completely optional and will not affect your course experience, scores, or ability to receive a certificate or job offer in any way.

Khảo sát hoàn thành chứng chỉ

Sau khi bạn hoàn thành bài tập được chấm điểm cuối cùng trong khóa học cuối cùng (thứ tám) của chương trình chứng chỉ, bạn sẽ được yêu cầu hoàn thành một bản khảo sát để xem lại một số câu hỏi trước đó và hỏi bạn đã học được gì trong suốt thời gian của chương trình. Cuộc khảo sát này cũng hỏi xem bạn có muốn chia sẻ thông tin liên hệ của mình với các nhà tuyển dụng tiềm năng hay không. Việc điền vào bản khảo sát và chia sẻ thông tin liên hệ của bạn với các nhà tuyển dụng tiềm năng là hoàn toàn tùy chọn và sẽ không ảnh hưởng đến kinh nghiệm, điểm số hoặc khả năng nhận chứng chỉ hoặc lời mời làm việc của bạn dưới bất kỳ hình thức nào.

1.9. Google Cybersecurity Certificate participant entry survey – Bản khảo sát dành cho người tham gia Chứng chỉ An ninh mạng của Google

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

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

2. Introduction to cybersecurity – Giới thiệu về an ninh mạng

2.1. Introduction to cybersecurity – Giới thiệu về an ninh mạng

Imagine that you're preparing for a storm. You've received notification that a storm is coming. You prepare by gathering the tools and materials you'll need to stay safe. You make sure your windows and doors are secure. You assemble a first aid kit, tools, food and water. You're prepared. The storm hits and there are powerful winds and heavy rain. The storm is using its force to try and breach your home. You notice some water leaks and begin patching them quickly in order to minimize any risk or potential damage.

Hãy tưởng tượng rằng bạn đang chuẩn bị cho một cơn bão. Bạn đã nhận được thông báo rằng một cơn bão đang đến. Bạn chuẩn bị bằng cách thu thập các công cụ và vật liệu cần thiết để giữ an toàn. Bạn đảm bảo cửa sổ và cửa ra vào của bạn được an toàn. Bạn tập hợp một bộ sơ cứu, dụng cụ, thực phẩm và nước uống. Bạn đã chuẩn bị sẵn sàng. Bão ập đến kèm theo gió mạnh và mưa lớn. Cơn bão đang sử dụng sức mạnh của nó để cố gắng xâm nhập vào nhà của bạn. Bạn nhận thấy một số rò rỉ nước và bắt đầu vá chúng nhanh chóng để giảm thiểu mọi rủi ro hoặc thiệt hại tiềm ẩn.

Handling a security incident is no different. Organizations must prepare for the storm by ensuring they have the tools to mitigate and quickly respond to outside threats. The objective is to minimize risk and potential damage.

Xử lý một sự cố an ninh cũng không khác. Các tổ chức phải chuẩn bị cho cơn bão bằng cách đảm bảo họ có các công cụ để giảm thiểu và ứng phó nhanh chóng với các mối đe dọa bên ngoài. Mục tiêu là giảm thiểu rủi ro và thiệt hại có thể xảy ra.

As a security analyst, you'll work to protect your organization and the people it serves from a variety of risks and outside threats. And if a threat does get through, you and your team will provide a solution to remedy the situation.

Với tư cách là nhà phân tích bảo mật, bạn sẽ làm việc để bảo vệ tổ chức của mình và những người mà tổ chức đó phục vụ khỏi nhiều rủi ro và mối đe dọa từ bên ngoài. Và nếu mối đe dọa vượt qua được, bạn và nhóm của bạn sẽ đưa ra giải pháp để khắc phục tình hình.

To help you better understand what this means, we'll define security and discuss the roles of security professionals in organizations.

Để giúp bạn hiểu rõ hơn ý nghĩa của điều này, chúng tôi sẽ xác định bảo mật và thảo luận về vai trò của các chuyên gia bảo mật trong tổ chức.

Let's start with some definitions: Cybersecurity, or security, is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

Hãy bắt đầu với một số định nghĩa: An ninh mạng hay bảo mật là hoạt động đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác trái phép.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

For example, requiring complex passwords to access sites and services improves confidentiality by making it much more difficult for a threat actor to compromise them. A threat actor is any person or group who presents a security risk.

Ví dụ: yêu cầu mật khẩu phức tạp để truy cập các trang web và dịch vụ sẽ cải thiện tính bảo mật bằng cách khiến tác nhân đe dọa khó xâm phạm chúng hơn nhiều. Tác nhân đe dọa là bất kỳ cá nhân hoặc nhóm nào có nguy cơ bảo mật.

Now that you know the definition of security, let's discuss what security teams do for an organization.

Bây giờ bạn đã biết định nghĩa về bảo mật, hãy cùng thảo luận xem nhóm bảo mật sẽ làm gì cho một tổ chức.

Security protects against external and internal threats. An external threat is someone outside of the organization trying to gain access to private information, networks or devices.

An ninh bảo vệ chống lại các mối đe dọa bên ngoài và bên trong. Mối đe dọa bên ngoài là ai đó bên ngoài tổ chức đang cố gắng truy cập vào thông tin, mạng hoặc thiết bị riêng tư.

An internal threat comes from current or former employees, external vendors, or trusted partners. Often these internal threats are accidental, such as an employee clicking on a compromised link in an email. Other times, the internal actor intentionally engages in activities such as unauthorized data access or abusing systems for personal use.

Mối đe dọa nội bộ đến từ nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy. Thông thường, những mối đe dọa nội bộ này là vô tình, chẳng hạn như nhân viên nhấp vào liên kết bị xâm phạm trong email. Trong những trường hợp khác, tác nhân nội bộ cố tình tham gia vào các hoạt động như truy cập dữ liệu trái phép hoặc lạm dụng hệ thống để sử dụng cho mục đích cá nhân.

Experienced security professionals will help organizations mitigate or reduce the impact of threats like these.

Các chuyên gia bảo mật có kinh nghiệm sẽ giúp các tổ chức giảm thiểu hoặc giảm thiểu tác động của các mối đe dọa như thế này.

Security teams also ensure an organization meets regulatory compliance, or laws and guidelines, that require the implementation of specific security standards.

Các nhóm bảo mật cũng đảm bảo tổ chức đáp ứng việc tuân thủ quy định hoặc luật pháp và hướng dẫn yêu cầu triển khai các tiêu chuẩn bảo mật cụ thể.

Ensuring that organizations are in compliance may allow them to avoid fines and audits, while also upholding their ethical obligation to protect users.

Việc đảm bảo rằng các tổ chức tuân thủ có thể cho phép họ tránh bị phạt tiền và kiểm tra, đồng thời duy trì nghĩa vụ đạo đức của mình để bảo vệ người dùng.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Security teams also maintain and improve business productivity. By establishing a plan for business continuity, security teams allow people to do their jobs, even in the case of something like a data breach.

Điều chắc chắn rằng các tổ chức cộng thủ có thể cho phép họ tránh bị phạt tiền và kiểm tra, đồng thời duy trì nghĩa vụ đạo đức của mình để bảo vệ người sử dụng.

Being security conscious can also reduce expenses associated with risks, such as recovering from data loss or operational downtime, and potentially avoiding fines. The last benefit of security that we'll discuss is maintaining brand trust. If services or customer data are compromised, this can lower trust in the organization, damage the brand, and hurt the business in the long term. Loss of customer trust may also lead to less revenue for the business.

Ý thức về bảo mật cũng có thể giảm chi phí liên quan đến rủi ro, chẳng hạn như khôi phục sau khi mất dữ liệu hoặc thời gian ngừng hoạt động và có khả năng tránh bị phạt. Lợi ích cuối cùng của bảo mật mà chúng ta sẽ thảo luận là duy trì niềm tin vào thương hiệu. Nếu dịch vụ hoặc dữ liệu khách hàng bị xâm phạm, điều này có thể làm giảm niềm tin vào tổ chức, làm tổn hại đến thương hiệu và gây tổn hại cho doanh nghiệp về lâu dài. Mất niềm tin của khách hàng cũng có thể dẫn đến doanh thu ít hơn cho doanh nghiệp.

Now, let's go over some common security-based roles. After completing this certificate program, here are some job titles you may want to search for: Security analyst or specialist, Cybersecurity analyst or specialist, Security operation center or SOC analyst, Information security analyst.

Bây giờ, chúng ta hãy đi qua một số vai trò dựa trên bảo mật phổ biến. Sau khi hoàn thành chương trình chứng chỉ này, dưới đây là một số chức danh công việc bạn có thể muốn tìm kiếm: Nhà phân tích hoặc chuyên gia bảo mật, nhà phân tích hoặc chuyên gia An ninh mạng, Trung tâm điều hành bảo mật hoặc nhà phân tích SOC, nhà phân tích bảo mật thông tin.

You'll also learn more about the responsibilities associated with some of these job titles later in the program.

Bạn cũng sẽ tìm hiểu thêm về trách nhiệm liên quan đến một số chức danh công việc này ở phần sau của chương trình.

As you may now realize, the field of security includes many topics and concepts and every activity you complete in this program moves you one step closer to a new job. Let's keep learning together.

Như bây giờ bạn có thể nhận ra, lĩnh vực bảo mật bao gồm nhiều chủ đề và khái niệm và mọi hoạt động bạn hoàn thành trong chương trình này sẽ đưa bạn đến gần hơn một bước với công việc mới. Hãy cùng nhau tiếp tục học tập nhé.

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

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Hi, I'm Toni, I'm a Security Engineering Manager. Our teams protect Google and its users from serious threats. Usually government-backed attackers, coordinated influence operations and serious cybercrime threat actors. I grew up as an army brat. My dad was in the military and we moved around a lot. I've always had an interest in security sort of generally. I got really hooked on international relations when I was in high school. I did a lot of Model United Nations. And that really sort of brought these two things together for me, the way that security works in the world. I come from a big family. I knew I was going to need financial assistance to go to college. And the Department of Defense provides a lot of educational opportunities that are tied to service. So this was a natural fit for me. I knew I was interested in this area and this was going to provide a career path into something I was passionate about. I started as an intelligence analyst, but not focused on cybersecurity. I worked counterinsurgency for a number of years and geopolitical intelligence issues. Eventually, as I looked and saw that the way that cybersecurity was starting to have an impact both in our daily lives and in that world of international relations, I got more and more drawn to it. Transitioning into cybersecurity was a huge shift for me. I came in without a solid technical background, had to learn a lot of that on the job and through self-paced learning in different types of courses, I needed to learn programming languages like Python and SQL, two of the things that we cover in this certificate, I needed to learn a whole new language about the vocabulary of threats and the different components and how those manifest technically. One of the things that I had to figure out very early in this journey is what kind of learner I was. I work best with a structured learning style. So turning to a lot of these online courses and resources that took this material and structured it sort of from first principles through application resonated very well for me. A lot of this was also learned on the job by co-workers who were willing to share and invest time in helping me understand this. I asked a lot of questions and I still do. Most of cybersecurity work is going to be learned on the job in the specific environment that you're protecting. So you have to work well with your teammates in order to be able to build that knowledge base. My advice would be to stay curious and keep learning, especially focusing on your technical skills and growing those throughout your career. It's really easy to get imposter syndrome in cybersecurity because it's so broad and mastery of all these different areas is a lifetime's work. And sometimes that imposter syndrome can shut us down and make it feel like, why bother trying to keep growing. I'm never going to be able to master this instead of motivating us. So keep learning, push through that fear. The efforts always going to be rewarded.

Xin chào, tôi là Toni, tôi là Giám đốc Kỹ thuật Bảo mật. Nhóm của chúng tôi bảo vệ Google và người dùng của Google khỏi các mối đe dọa nghiêm trọng. Thường là những kẻ tấn công được chính phủ hậu thuẫn, các hoạt động gây ảnh hưởng phối hợp và các tác nhân đe dọa tội phạm mạng nghiêm trọng. Tôi lớn lên như một cậu nhóc quân đội. Bố tôi làm trong quân đội và chúng tôi di chuyển rất nhiều nơi. Nói chung, tôi luôn quan tâm đến vấn đề bảo mật. Tôi thực sự say mê quan hệ quốc tế khi còn học trung học. Tôi đã làm rất nhiều Mô hình Liên Hợp Quốc. Và điều đó thực sự đã mang hai thứ này lại với nhau đối với tôi, cách thức hoạt động của bảo mật trên thế giới. Tôi đến từ một gia đình lớn. Tôi biết tôi sẽ cần hỗ trợ tài chính để đi học đại học. Và Bộ Quốc phòng cung cấp rất nhiều cơ hội giáo dục gắn liền với việc phục vụ. Vì vậy, đây là một sự phù hợp tự nhiên đối với tôi. Tôi biết tôi quan tâm đến lĩnh vực này và điều này sẽ

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

mang lại con đường sự nghiệp cho lĩnh vực mà tôi đam mê. Tôi bắt đầu làm nhà phân tích tình báo, nhưng không tập trung vào an ninh mạng. Tôi đã làm việc trong lĩnh vực chống nổi dậy trong nhiều năm và nghiên cứu các vấn đề tình báo địa chính trị. Cuối cùng, khi tôi xem xét và nhận thấy rằng an ninh mạng bắt đầu có tác động đến cả cuộc sống hàng ngày của chúng ta và trong thế giới quan hệ quốc tế, tôi ngày càng bị cuốn hút vào nó. Chuyển sang lĩnh vực an ninh mạng là một sự thay đổi lớn đối với tôi. Tôi đến đây mà không có nền tảng kỹ thuật vững chắc, phải học rất nhiều thứ trong công việc và thông qua việc tự học theo các loại khóa học khác nhau, tôi cần học các ngôn ngữ lập trình như Python và SQL, hai trong số những thứ chúng tôi đề cập trong Chứng chỉ này, tôi cần học một ngôn ngữ hoàn toàn mới về từ vựng của các mối đe dọa và các thành phần khác nhau cũng như cách chúng biểu hiện về mặt kỹ thuật. Một trong những điều mà tôi phải nhận ra từ rất sớm trong cuộc hành trình này là tôi là loại người học tập như thế nào. Tôi làm việc hiệu quả nhất với phong cách học tập có cấu trúc. Vì vậy, việc chuyển sang sử dụng nhiều khóa học và tài nguyên trực tuyến sử dụng tài liệu này và cấu trúc nó từ những nguyên tắc đầu tiên cho đến ứng dụng đã tạo được tiếng vang rất lớn đối với tôi. Rất nhiều điều trong số này cũng đã được học hỏi trong công việc bởi những đồng nghiệp sẵn sàng chia sẻ và đầu tư thời gian để giúp tôi hiểu điều này. Tôi đã hỏi rất nhiều câu hỏi và tôi vẫn làm. Hầu hết công việc an ninh mạng sẽ được học trong công việc trong môi trường cụ thể mà bạn đang bảo vệ. Vì vậy, bạn phải phối hợp tốt với đồng đội của mình thì mới có thể xây dựng được nền tảng kiến thức đó. Lời khuyên của tôi là hãy luôn tò mò và không ngừng học hỏi, đặc biệt là tập trung vào các kỹ năng kỹ thuật của bạn và phát triển chúng trong suốt sự nghiệp của bạn. Thực sự rất dễ mắc phải hội chứng kẻ mạo danh trong lĩnh vực an ninh mạng vì nó quá rộng và việc thành thạo tất cả các lĩnh vực khác nhau này là công việc cả đời. Và đôi khi hội chứng kẻ mạo danh đó có thể khiến chúng ta im lặng và khiến chúng ta cảm thấy như thế, tại sao phải cố gắng tiếp tục phát triển. Tôi sẽ không bao giờ có thể làm chủ được điều này thay vì động viên chúng tôi. Vì vậy, hãy tiếp tục học hỏi, vượt qua nỗi sợ hãi đó. Những nỗ lực luôn được đền đáp xứng đáng.

2.3. Responsibilities of an entry-level cybersecurity analyst – Trách nhiệm của một nhà phân tích an ninh mạng cấp độ đầu vào

Technology is rapidly changing and so are the tactics and techniques that attackers use. As digital infrastructure evolves, security professionals are expected to continually grow their skills in order to protect and secure sensitive information. In this video, we'll discuss some job responsibilities of an entry-level security analyst.

Công nghệ đang thay đổi nhanh chóng và các chiến thuật cũng như kỹ thuật mà kẻ tấn công sử dụng cũng vậy. Khi cơ sở hạ tầng kỹ thuật số phát triển, các chuyên gia bảo mật dự kiến sẽ liên tục phát triển kỹ năng của mình để bảo vệ và bảo mật thông tin nhạy cảm. Trong video này, chúng ta sẽ thảo luận về một số trách nhiệm công việc của một nhà phân tích bảo mật cấp mới vào nghề.

So, what do security analysts do? Security analysts are responsible for monitoring and protecting information and systems.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Vậy, các nhà phân tích chứng khoán làm gì? Các nhà phân tích bảo mật chịu trách nhiệm giám sát và bảo vệ thông tin và hệ thống.

Now, we'll discuss three primary responsibilities of a security analyst, starting with protecting computer and network systems. Protecting computer and network systems requires an analyst to monitor an organization's internal network. If a threat is detected, then an analyst is generally the first to respond. Analysts also often take part in exercises to search for weaknesses in an organization's own systems.

Bây giờ, chúng ta sẽ thảo luận ba trách nhiệm chính của một nhà phân tích bảo mật, bắt đầu bằng việc bảo vệ hệ thống mạng và máy tính. Bảo vệ hệ thống máy tính và mạng đòi hỏi nhà phân tích phải giám sát mạng nội bộ của tổ chức. Nếu một mối đe dọa được phát hiện thì nhà phân tích thường là người đầu tiên phản ứng. Các nhà phân tích cũng thường tham gia vào các hoạt động tìm kiếm điểm yếu trong hệ thống của tổ chức.

For example, a security analyst may contribute to penetration testing or ethical hacking. The goal is to penetrate or hack their own organization's internal network to identify vulnerabilities and suggest ways to strengthen their security measures.

Ví dụ: một nhà phân tích bảo mật có thể đóng góp vào việc kiểm tra thâm nhập hoặc hack có đạo đức. Mục tiêu là xâm nhập hoặc hack mạng nội bộ của tổ chức họ để xác định các lỗ hổng và đề xuất cách tăng cường các biện pháp bảo mật của họ.

Think of it like this. After you lock your car, you check the door handles to make sure no one can access any valuables you keep inside.

Hãy nghĩ về nó như thế này. Sau khi khóa xe, bạn kiểm tra tay nắm cửa để đảm bảo không ai có thể lấy được bất kỳ vật có giá trị nào bạn để bên trong.

Security analysts also proactively work to prevent threats from happening in the first place. One way they do this is by working with information technology, or IT, teams to install prevention software for the purposes of identifying risks and vulnerabilities.

Các nhà phân tích bảo mật cũng chủ động làm việc để ngăn chặn các mối đe dọa xảy ra ngay từ đầu. Một cách để họ thực hiện điều này là làm việc với các nhóm công nghệ thông tin hoặc CNTT để cài đặt phần mềm phòng ngừa nhằm mục đích xác định rủi ro và lỗ hổng.

Analysts may also be involved in software and hardware development. They'll often work with development teams to support product security by setting up appropriate processes and systems to meet the organization's data protection needs.

Các nhà phân tích cũng có thể tham gia phát triển phần mềm và phần cứng. Họ thường làm việc với các nhóm phát triển để hỗ trợ bảo mật sản phẩm bằng cách thiết lập các quy trình và hệ thống phù hợp nhằm đáp ứng nhu cầu bảo vệ dữ liệu của tổ chức.

The last task we'll discuss is conducting periodic security audits. A security audit is a review of an organization's security records, activities, and other related documents. For example, an analyst may examine in-house security issues, such as making sure that confidential information, like individual computer passwords, isn't available to all employees.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Nhiệm vụ cuối cùng chúng ta sẽ thảo luận là tiến hành kiểm tra bảo mật định kỳ. Kiểm toán bảo mật là việc xem xét hồ sơ, hoạt động bảo mật và các tài liệu liên quan khác của tổ chức. Ví dụ: một nhà phân tích có thể kiểm tra các vấn đề bảo mật nội bộ, chẳng hạn như đảm bảo rằng thông tin bí mật, như mật khẩu máy tính cá nhân, không được cung cấp cho tất cả nhân viên.

Phew, that was a lot to cover! But hopefully you have a general idea of what entry-level security analysts do on a day-to-day basis.

Phù, có quá nhiều thứ cần phải giải quyết! Nhưng hy vọng bạn có ý tưởng chung về công việc hàng ngày của các nhà phân tích bảo mật cấp thấp.

Security analysts are an important part of any organization. Their daily tasks protect small businesses, large companies, nonprofit organizations, and government agencies. They also help to ensure that the people served by those organizations remain safe.

Các nhà phân tích bảo mật là một phần quan trọng của bất kỳ tổ chức nào. Nhiệm vụ hàng ngày của họ là bảo vệ các doanh nghiệp nhỏ, công ty lớn, tổ chức phi lợi nhuận và cơ quan chính phủ. Chúng cũng giúp đảm bảo rằng những người được các tổ chức đó phục vụ vẫn được an toàn.

2.4. Nikki: A day in the life of a security engineer – Nikki: Một ngày trong cuộc đời của kỹ sư an ninh

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

[MUSIC] My name is Nikki and I'm a security engineer at Google. I am part of the insider threat detection team at Google, so my role is more focused on catching insider threats or insider suspicious activity within the company. My first experience with cybersecurity was when I was interning at the aquarium. I learned a lot of network security there, they had a lot of phishing attempts, of course, you know, at the aquarium. My manager was really focused on making sure that our networks were secure and I learned a lot from him and that really sparked my interest in cybersecurity. The main reason I chose to pursue a career in cybersecurity is just how flexible the career path is. Once you're in security, there's so many different fields you can dive into. Whether it's through the blue team, protecting the user or the red team, which is just, you know, poking holes in other people's defenses and letting them know where they're going wrong. A day in the life as a entry-level security professional? Um, it can change day to day, but there's two basic parts to it. There's the operation side, which is responding to detections and doing investigations. And then there's the project side where you're working with other teams to build new detections or improve the current detections. The difference between this entry-level cybersecurity analyst and an entry-level cybersecurity engineer is pretty much that the analyst is more focused on operations and the engineer, while they can do operations, they also build the, the detections and they do more project focused work. My favorite task is probably the operations side doing investigations because we can sometimes get something like this actor did such and such on this day. And we're supposed to then dive into what they've been doing, what they've been working on to figure out if there's any suspicious activity or if it was just a false positive. One of the biggest ways I've made an impact as an entry-level cybersecurity professional is actually working on the playbooks that, um, our team uses. A playbook is a list of how to go through a certain detection, and what the analyst needs to look at in order to investigate those incidents. I was really proud of those, those playbooks that I've made so far because a lot of my teammates have even said how helpful they've been to them. If you love solving problems, if you love protecting user data, being at the front lines of a lot of headlines, then this is definitely the role for you.

[NHẠC] Tên tôi là Nikki và tôi là kỹ sư bảo mật tại Google. Tôi là thành viên của nhóm phát hiện mối đe dọa nội bộ tại Google, vì vậy vai trò của tôi tập trung hơn vào việc phát hiện các mối đe dọa nội bộ hoặc hoạt động đáng ngờ từ nội bộ trong công ty. Trải nghiệm đầu tiên của tôi về an ninh mạng là khi tôi đang thực tập tại thủy cung. Tôi đã học được rất nhiều điều về an ninh mạng ở đó, họ đã thực hiện rất nhiều nỗ lực lừa đảo, bạn biết đấy, ở thủy cung. Người quản lý của tôi thực sự tập trung vào việc đảm bảo mạng của chúng tôi được an toàn và tôi đã học được rất nhiều điều từ anh ấy và điều đó thực sự khơi dậy sự quan tâm của tôi đối với an ninh mạng. Lý do chính khiến tôi chọn theo đuổi nghề an ninh mạng là vì con đường sự nghiệp linh hoạt đến mức nào. Khi bạn đã ở trạng thái bảo mật, có rất nhiều lĩnh vực khác nhau mà bạn có thể tham gia. Cho dù đó là thông qua đội xanh, bảo vệ người dùng hay đội đỏ, bạn biết đấy, điều đó chỉ là chọc thủng hàng phòng ngự của người khác và cho họ biết họ đã sai ở đâu. Một ngày trong cuộc đời của một chuyên gia bảo mật cấp đầu vào? Ừm, nó có thể thay đổi hàng ngày, nhưng nó có hai phần cơ bản. Có phía hoạt động, đang ứng phó với các phát hiện và thực hiện điều tra. Và sau đó là phía dự án nơi bạn đang làm việc với các nhóm khác để xây dựng các phát hiện mới hoặc cải thiện các phát hiện hiện tại. Sự khác biệt giữa nhà phân tích an ninh mạng cấp độ đầu vào này và kỹ sư an ninh mạng cấp độ đầu vào

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

khá nhiều là nhà phân tích tập trung hơn vào hoạt động và kỹ sư, trong khi họ có thể thực hiện các hoạt động, họ cũng xây dựng, phát hiện và họ tập trung vào dự án hơn công việc. Nhiệm vụ yêu thích của tôi có lẽ là bên điều hành thực hiện các cuộc điều tra vì đôi khi chúng tôi có thể nhận được điều gì đó giống như diễn viên này đã làm như vậy vào ngày này. Và sau đó chúng ta phải đi sâu vào những gì họ đang làm, những gì họ đang tiến hành để tìm hiểu xem có bất kỳ hoạt động đáng ngờ nào hay đó chỉ là một kết quả dương tính giả. Một trong những cách lớn nhất mà tôi đã tạo ra tác động với tư cách là một chuyên gia an ninh mạng cấp độ đầu vào là thực sự làm việc trên các cảm nang mà nhóm chúng tôi sử dụng. Cảm nang là danh sách cách thực hiện một phát hiện nhất định và những gì nhà phân tích cần xem xét để điều tra những sự cố đó. Tôi thực sự tự hào về những cuốn sách đó, những cuốn sách mà tôi đã làm cho đến nay bởi vì nhiều đồng đội của tôi thậm chí còn nói rằng chúng đã giúp ích cho họ như thế nào. Nếu bạn thích giải quyết vấn đề, nếu bạn thích bảo vệ dữ liệu người dùng, đứng đầu trên nhiều tiêu đề, thì đây chắc chắn là vai trò dành cho bạn.

2.5. Common cybersecurity terminology – Thuật ngữ an ninh mạng phổ biến

As you've learned, **cybersecurity** (also known as security) is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. In this reading, you'll be introduced to some key terms used in the cybersecurity profession. Then, you'll be provided with a resource that's useful for staying informed about changes to cybersecurity terminology.

Như bạn đã biết, an ninh mạng (còn được gọi là bảo mật) là biện pháp đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác trái phép. Trong bài đọc này, bạn sẽ được giới thiệu một số thuật ngữ chính được sử dụng trong ngành an ninh mạng. Sau đó, bạn sẽ được cung cấp một nguồn tài nguyên hữu ích để luôn cập nhật thông tin về những thay đổi đối với thuật ngữ an ninh mạng.

Key cybersecurity terms and concepts

There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts.

Các thuật ngữ và khái niệm an ninh mạng chính

Có nhiều thuật ngữ và khái niệm quan trọng mà các chuyên gia bảo mật cần biết. Làm quen với chúng có thể giúp bạn xác định rõ hơn các mối đe dọa có thể gây hại cho tổ chức cũng như mọi người. Một nhà phân tích bảo mật hoặc nhà phân tích an ninh mạng tập trung vào việc giám sát các mạng để phát hiện các vi phạm. Họ cũng giúp phát triển các chiến lược để bảo mật tổ chức và nghiên cứu các xu hướng bảo mật công nghệ thông tin (IT) để luôn cảnh giác và được thông báo về các mối đe dọa tiềm ẩn. Ngoài ra,

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

một nhà phân tích làm việc để ngăn ngừa sự cố. Để các nhà phân tích thực hiện hiệu quả các loại nhiệm vụ này, họ cần phát triển kiến thức về các khái niệm chính sau.

Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

Tuân thủ là quá trình tuân thủ các tiêu chuẩn nội bộ và quy định bên ngoài, đồng thời cho phép các tổ chức tránh bị phạt và vi phạm an ninh.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

Khung bảo mật là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư.

Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.

Kiểm soát bảo mật là các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể. Chúng được sử dụng cùng với các khung bảo mật để thiết lập một thể trận bảo mật mạnh mẽ.

Security posture is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

Tình trạng bảo mật là khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi. Một trạng thái bảo mật mạnh mẽ dẫn đến rủi ro thấp hơn cho tổ chức.

A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.

Tác nhân đe dọa hoặc kẻ tấn công độc hại là bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật. Rủi ro này có thể liên quan đến máy tính, ứng dụng, mạng và dữ liệu.

An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access.

Mối đe dọa nội bộ có thể là nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy gây ra rủi ro bảo mật. Đôi khi, một mối đe dọa nội bộ là vô tình. Ví dụ: một nhân viên vô tình nhấp vào liên kết email độc hại sẽ bị coi là mối đe dọa vô tình. Đôi khi, tác nhân đe dọa nội bộ cố tình tham gia vào các hoạt động rủi ro, chẳng hạn như truy cập dữ liệu trái phép.

Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization's network.

An ninh mạng là hoạt động giữ an toàn cho cơ sở hạ tầng mạng của một tổ chức khỏi bị truy cập trái phép. Điều này bao gồm dữ liệu, dịch vụ, hệ thống và thiết bị được lưu trữ trong mạng của tổ chức.

Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

Bảo mật đám mây là quá trình đảm bảo rằng các tài sản được lưu trữ trên đám mây được định cấu hình đúng cách hoặc được thiết lập chính xác và quyền truy cập vào các tài sản đó được giới hạn ở những người dùng được ủy quyền. Đám mây là một mạng được tạo thành từ một tập hợp các máy chủ hoặc máy tính lưu trữ tài nguyên và dữ liệu ở các vị trí vật lý từ xa được gọi là trung tâm dữ liệu có thể được truy cập qua internet. Bảo mật đám mây là một lĩnh vực an ninh mạng đang phát triển, đặc biệt tập trung vào việc bảo vệ dữ liệu, ứng dụng và cơ sở hạ tầng trên đám mây.

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:

- Automation of repetitive tasks (e.g., searching a list of malicious domains)
- Reviewing web traffic
- Alerting suspicious activity

Lập trình là một quá trình có thể được sử dụng để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ. Những nhiệm vụ này có thể bao gồm:

- Tự động hóa các tác vụ lặp đi lặp lại (ví dụ: tìm kiếm danh sách các miền độc hại)
- Xem xét lưu lượng truy cập web
- Cảnh báo hoạt động đáng ngờ

Key takeaways

Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks, and vulnerabilities. To explore a variety of cybersecurity terms, visit the [National Institute of Standards and Technology glossary](#). Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages.

Bài học chính

Hiểu các thuật ngữ và khái niệm kỹ thuật chính được sử dụng trong lĩnh vực bảo mật sẽ giúp bạn chuẩn bị cho vai trò là nhà phân tích bảo mật. Biết các thuật ngữ này có thể giúp bạn xác định các mối đe dọa, rủi ro và lỗ hổng phổ biến. Để khám phá nhiều thuật ngữ an ninh mạng, hãy truy cập bảng thuật ngữ của Viện Tiêu chuẩn và Công nghệ Quốc gia. Hoặc sử dụng trình duyệt của bạn để tìm kiếm các thuật ngữ an ninh mạng đáng tin cậy, chất lượng cao từ các viện nghiên cứu hoặc cơ quan chính phủ. Bảng thuật ngữ có sẵn bằng nhiều ngôn ngữ.

2.6. Test your knowledge: Introduction to cybersecurity – Kiểm tra kiến thức của bạn: Giới thiệu về an ninh mạng

3. Core skills for cybersecurity professionals – Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

3.1. Core skills for cybersecurity professionals

Core skills for cybersecurity professionals

For any job, you need certain skills to be successful, and many of these core skills are transferable from one role to the next. No matter what job you currently have, you likely have many core skills already. Having a diverse background enhances your core skills, which means your personal experiences and perspectives are especially valuable.

Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng

Đối với bất kỳ công việc nào, bạn đều cần những kỹ năng nhất định để thành công và nhiều kỹ năng cốt lõi này có thể chuyển từ vai trò này sang vai trò tiếp theo. Cho dù hiện tại bạn đang làm công việc gì, bạn đều có thể đã có sẵn nhiều kỹ năng cốt lõi. Có nền tảng đa dạng sẽ nâng cao các kỹ năng cốt lõi của bạn, điều đó có nghĩa là kinh nghiệm và quan điểm cá nhân của bạn đặc biệt có giá trị.

In this video, we'll discuss both transferable and technical skills that are particularly useful for a security analyst.

Trong video này, chúng ta sẽ thảo luận về cả kỹ năng chuyển giao và kỹ năng kỹ thuật đặc biệt hữu ích đối với nhà phân tích bảo mật.

Transferable skills are skills from other areas that can apply to different careers.

Kỹ năng chuyển đổi là những kỹ năng từ các lĩnh vực khác có thể áp dụng cho các ngành nghề khác nhau.

Technical skills may apply to several professions as well. However, at times they may require knowledge of specific tools, procedures, and policies.

Kỹ năng kỹ thuật cũng có thể áp dụng cho một số ngành nghề. Tuy nhiên, đôi khi họ có thể yêu cầu kiến thức về các công cụ, thủ tục và chính sách cụ thể.

Let's discuss some core transferable skills you may already have that will benefit you in a career as a security analyst. Communication is a transferable skill for a security analyst. They will often need to describe certain threats, risks, or vulnerabilities to people who may not have a technical background.

Hãy thảo luận về một số kỹ năng cốt lõi có thể chuyển giao mà bạn có thể đã có, điều này sẽ mang lại lợi ích cho bạn trong sự nghiệp phân tích chứng khoán. Giao tiếp là một kỹ năng có thể chuyển giao đối với một nhà phân tích bảo mật. Họ thường sẽ cần mô tả các mối đe dọa, rủi ro hoặc lỗ hổng nhất định cho những người có thể không có nền tảng kỹ thuật.

For example, security analysts may be tasked with interpreting and communicating policies and procedures to other employees. Or analysts may be asked to report findings to their supervisors, so the appropriate actions can be taken to secure the organization.

Ví dụ, các nhà phân tích bảo mật có thể được giao nhiệm vụ giải thích và truyền đạt các chính sách và thủ tục cho các nhân viên khác. Hoặc các nhà phân tích có thể được yêu cầu báo cáo những phát hiện cho người giám sát của họ để có thể thực hiện các hành động thích hợp nhằm bảo đảm an toàn cho tổ chức.

Another transferable skill is collaboration. Security analysts often work in teams with engineers, digital forensic investigators, and program managers. For example, if you

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

are working to roll out a new security feature, you will likely have a project manager, an engineer, and an ethical hacker on your team. Security analysts also need to be able to analyze complex scenarios that they may encounter. For example, a security analyst may need to make recommendations about how different tools can support efficiency and safeguard an organization's internal network.

Một kỹ năng có thể chuyển giao khác là sự hợp tác. Các nhà phân tích bảo mật thường làm việc theo nhóm với các kỹ sư, nhà điều tra pháp y kỹ thuật số và người quản lý chương trình. Ví dụ: nếu bạn đang nỗ lực triển khai một tính năng bảo mật mới, bạn có thể sẽ có người quản lý dự án, kỹ sư và một hacker đạo đức trong nhóm của mình. Các nhà phân tích bảo mật cũng cần có khả năng phân tích các tình huống phức tạp mà họ có thể gặp phải. Ví dụ: nhà phân tích bảo mật có thể cần đưa ra khuyến nghị về cách các công cụ khác nhau có thể hỗ trợ hiệu quả và bảo vệ mạng nội bộ của tổ chức.

The last transferable skill that we'll discuss is problem-solving. Identifying a security problem and then diagnosing it and providing solutions is a necessary skill to keep business operations safe. Understanding threat actors and identifying trends can provide insight on how to handle future threats.

Kỹ năng chuyển giao cuối cùng mà chúng ta sẽ thảo luận là giải quyết vấn đề. Xác định một vấn đề bảo mật, sau đó chẩn đoán nó và đưa ra giải pháp là một kỹ năng cần thiết để giữ cho hoạt động kinh doanh được an toàn. Hiểu các tác nhân đe dọa và xác định xu hướng có thể cung cấp cái nhìn sâu sắc về cách xử lý các mối đe dọa trong tương lai.

Okay, now that we've covered some important transferable skills, let's discuss some technical skills that security analysts need to develop. A basic understanding of programming languages is an important skill to develop because security analysts can use programming to automate tasks and identify error messages.

Được rồi, bây giờ chúng ta đã đề cập đến một số kỹ năng chuyển giao quan trọng, hãy thảo luận về một số kỹ năng kỹ thuật mà các nhà phân tích bảo mật cần phát triển. Hiểu biết cơ bản về ngôn ngữ lập trình là một kỹ năng quan trọng cần phát triển vì các nhà phân tích bảo mật có thể sử dụng lập trình để tự động hóa các tác vụ và xác định các thông báo lỗi.

Like learning any other language, learning a programming language may seem challenging at first. However, this certificate program assumes no prior programming experience, so we'll start at the very beginning and provide several opportunities for hands-on practice with languages like Python and SQL.

Giống như học bất kỳ ngôn ngữ nào khác, việc học một ngôn ngữ lập trình lúc đầu có vẻ khó khăn. Tuy nhiên, chương trình chứng chỉ này yêu cầu bạn không có kinh nghiệm lập trình trước đó, vì vậy chúng tôi sẽ bắt đầu ngay từ đầu và cung cấp một số cơ hội thực hành thực hành với các ngôn ngữ như Python và SQL.

Another important technical skill is knowing how to use security information and event management, or SIEM, tools. Security professionals use SIEM tools to identify and analyze security threats, risks, and vulnerabilities. For example, a SIEM tool may alert you that an unknown user has accessed the system. In the event of an unknown user accessing the system, you may use computer forensics to investigate the incident.

Một kỹ năng kỹ thuật quan trọng khác là biết cách sử dụng các công cụ quản lý sự kiện và thông tin bảo mật hoặc SIEM. Các chuyên gia bảo mật sử dụng các công cụ SIEM để xác định và phân tích các mối đe dọa, rủi ro và lỗ hổng bảo mật. Ví dụ: công cụ SIEM có thể cảnh báo bạn rằng một người dùng không xác định đã truy cập hệ thống. Trong

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

trường hợp người dùng không xác định truy cập vào hệ thống, bạn có thể sử dụng pháp y máy tính để điều tra vụ việc.

Now, let's discuss computer forensics. Similar to an investigator and a forensic scientist working in the criminal justice system, digital forensic investigators will attempt to identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices.

Bây giờ chúng ta hãy thảo luận về pháp y máy tính. Tương tự như điều tra viên và nhà khoa học pháp y làm việc trong hệ thống tư pháp hình sự, điều tra viên pháp y kỹ thuật số sẽ cố gắng xác định, phân tích và lưu giữ bằng chứng tội phạm trong mạng, máy tính và thiết bị điện tử.

Keep in mind that you may already have some of the core skills we've discussed. And if you don't have the technical skills, that's okay! This program is designed to support you in learning those skills.

Hãy nhớ rằng bạn có thể đã có một số kỹ năng cốt lõi mà chúng ta đã thảo luận. Và nếu bạn không có kỹ năng kỹ thuật thì cũng không sao! Chương trình này được thiết kế để hỗ trợ bạn học những kỹ năng đó.

For example, over the past seven years working in cybersecurity, I've learned that security analysts need to have intellectual curiosity and the motivation to keep learning in order to succeed. Personally, I dedicate time on a regular basis towards learning more Python and SQL skills in order to meet the demands of the projects I'm working on. You'll get to learn about Python and SQL later in this program.

Ví dụ, trong bảy năm làm việc trong lĩnh vực an ninh mạng, tôi đã học được rằng các nhà phân tích bảo mật cần phải có trí tò mò trí tuệ và động lực không ngừng học hỏi để thành công. Cá nhân tôi thường xuyên dành thời gian để học thêm các kỹ năng Python và SQL nhằm đáp ứng nhu cầu của các dự án mà tôi đang thực hiện. Bạn sẽ tìm hiểu về Python và SQL sau trong chương trình này.

As you continue this journey, you'll build the knowledge and skills you need to enter the security field.

Khi tiếp tục hành trình này, bạn sẽ xây dựng kiến thức và kỹ năng cần thiết để tham gia vào lĩnh vực bảo mật.

3.2. Veronica: My path to working in cybersecurity

Veronica: My path to working in cybersecurity

Hi, I'm Veronica and I'm a security engineer at Google. My journey into cybersecurity has changed my life for the better in so many ways. The most important part is fulfilling work. I get to do something that I absolutely love and that I'm super interested in, and I feel very lucky that this is what I get to do for work. Before I entered my current field, I had no idea what cybersecurity was. My knowledge of cybersecurity was using secure passwords, and that was about it. So if you asked me, you know, would I be in cybersecurity five years ago? I would've said, what is that? Someone without a technical background can 100% be successful in cybersecurity. My path to my current role in cybersecurity started as an IT resident here at Google staff in Techstop. I learned a lot of analytical thinking skills, working on a help desk, troubleshooting, debugging. I didn't realize I had transferable skills until I got into my role in cybersecurity. And from there, I took it upon myself to bug a bunch of security

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

engineers, interviewed a lot of them. I didn't get here alone. It took a village of mentors to get me here, so don't be afraid to ask for help. I don't think someone needs a college degree to go into cybersecurity. Some of the brightest minds that I get to work with don't have a college degree, so I think that's one of the best parts about the industry. Looking back at my career, I wish I would have known that I don't have to check all the boxes, that I don't have to be an expert in the area to shoot my shot, and I also wish I would've known that perfectionism can get in the way of what you want to achieve.

Veronica: Con đường làm việc trong lĩnh vực an ninh mạng của tôi

Xin chào, tôi là Veronica và tôi là kỹ sư bảo mật tại Google. Hành trình của tôi vào lĩnh vực an ninh mạng đã thay đổi cuộc sống của tôi tốt hơn theo nhiều cách. Phần quan trọng nhất là hoàn thành công việc. Tôi được làm điều gì đó mà tôi thực sự yêu thích và cực kỳ hứng thú, đồng thời tôi cảm thấy rất may mắn vì đây là điều tôi được làm trong công việc. Trước khi bước vào lĩnh vực hiện tại, tôi không biết an ninh mạng là gì. Kiến thức của tôi về an ninh mạng là sử dụng mật khẩu an toàn và chỉ có vậy thôi. Vì vậy, nếu bạn hỏi tôi, bạn biết đấy, liệu tôi có tham gia lĩnh vực an ninh mạng 5 năm trước không? Tôi sẽ nói, đó là gì? Người không có nền tảng kỹ thuật có thể thành công 100% trong lĩnh vực an ninh mạng. Con đường dẫn đến vai trò hiện tại của tôi trong lĩnh vực an ninh mạng bắt đầu với tư cách là nhân viên CNTT tại nhân viên Google ở Techstop. Tôi đã học được rất nhiều kỹ năng tư duy phân tích, làm việc trên bàn trợ giúp, xử lý sự cố, gỡ lỗi. Tôi đã không nhận ra mình có những kỹ năng có thể chuyển giao cho đến khi đảm nhận vai trò của mình trong lĩnh vực an ninh mạng. Và từ đó, tôi tự mình theo dõi một loạt kỹ sư bảo mật, phỏng vấn rất nhiều người trong số họ. Tôi không đến đây một mình. Phải mất cả làng cô vẫn mới đưa được tôi đến đây, vì vậy đừng ngại yêu cầu giúp đỡ. Tôi không nghĩ ai đó cần có bằng đại học để theo học ngành an ninh mạng. Một số bộ óc thông minh nhất mà tôi được làm việc cùng không có bằng đại học, vì vậy tôi nghĩ đó là một trong những điểm hay nhất của ngành. Nhìn lại sự nghiệp của mình, tôi ước mình biết rằng tôi không cần phải đánh dấu vào tất cả các ô, rằng tôi không cần phải là chuyên gia trong lĩnh vực này mới có thể bắt đầu, và tôi cũng ước mình đã làm được điều đó. biết rằng chủ nghĩa hoàn hảo có thể cản trở những gì bạn muốn đạt được.

3.3. Transferable and technical cybersecurity skills

Transferable and technical cybersecurity skills

Previously, you learned that cybersecurity analysts need to develop certain core skills to be successful at work. **Transferable skills** are skills from other areas of study or practice that can apply to different careers. **Technical skills** may apply to several professions, as well; however, they typically require knowledge of specific tools, procedures, and policies. In this reading, you'll explore both transferable skills and technical skills further.

Kỹ năng an ninh mạng có thể chuyển giao và kỹ thuật

Trước đây, bạn đã biết rằng các nhà phân tích an ninh mạng cần phát triển một số kỹ năng cốt lõi nhất định để thành công trong công việc. **Kỹ năng chuyển đổi** là những kỹ năng từ các lĩnh vực học tập hoặc thực hành khác có thể áp dụng cho các ngành nghề khác nhau. **Kỹ năng kỹ thuật** cũng có thể áp dụng cho một số ngành nghề; tuy nhiên,

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

họ thường yêu cầu kiến thức về các công cụ, thủ tục và chính sách cụ thể. Trong bài đọc này, bạn sẽ khám phá thêm cả kỹ năng chuyển giao và kỹ năng kỹ thuật.

Transferable skills

You have probably developed many transferable skills through life experiences; some of those skills will help you thrive as a cybersecurity professional. These include:

- **Communication:** As a cybersecurity analyst, you will need to communicate and collaborate with others. Understanding others' questions or concerns and communicating information clearly to individuals with technical and non-technical knowledge will help you mitigate security issues quickly.
- **Problem-solving:** One of your main tasks as a cybersecurity analyst will be to proactively identify and solve problems. You can do this by recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You'll likely need to compromise.
- **Time management:** Having a heightened sense of urgency and prioritizing tasks appropriately is essential in the cybersecurity field. So, effective time management will help you minimize potential damage and risk to critical assets and data. Additionally, it will be important to prioritize tasks and stay focused on the most urgent issue.
- **Growth mindset:** This is an evolving industry, so an important transferable skill is a willingness to learn. Technology moves fast, and that's a great thing! It doesn't mean you will need to learn it all, but it does mean that you'll need to continue to learn throughout your career. Fortunately, you will be able to apply much of what you learn in this program to your ongoing professional development.
- **Diverse perspectives:** The only way to go far is together. By having respect for each other and encouraging diverse perspectives and mutual respect, you'll undoubtedly find multiple and better solutions to security problems.

Kỹ năng chuyển nhượng

Bạn có thể đã phát triển nhiều kỹ năng có thể chuyển đổi thông qua kinh nghiệm sống; một số kỹ năng đó sẽ giúp bạn phát triển thành chuyên gia an ninh mạng. Bao gồm các:

- **Giao tiếp:** Là một nhà phân tích an ninh mạng, bạn sẽ cần giao tiếp và cộng tác với những người khác. Hiểu được câu hỏi hoặc mối quan tâm của người khác và truyền đạt thông tin rõ ràng đến những cá nhân có kiến thức về kỹ thuật và phi kỹ thuật sẽ giúp bạn giảm thiểu các vấn đề bảo mật một cách nhanh chóng.
- **Giải quyết vấn đề:** Một trong những nhiệm vụ chính của bạn với tư cách là nhà phân tích an ninh mạng là chủ động xác định và giải quyết vấn đề. Bạn có thể làm điều này bằng cách nhận ra các kiểu tấn công, sau đó xác định giải pháp hiệu quả nhất để giảm thiểu rủi ro. Đừng ngại chấp nhận rủi ro và thử những

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

điều mới. Ngoài ra, hãy hiểu rằng rất hiếm khi tìm được giải pháp hoàn hảo cho một vấn đề. Bạn có thể sẽ cần phải thỏa hiệp.

- **Quản lý thời gian:** Nâng cao ý thức cấp bách và sắp xếp thứ tự ưu tiên các nhiệm vụ một cách hợp lý là điều cần thiết trong lĩnh vực an ninh mạng. Vì vậy, quản lý thời gian hiệu quả sẽ giúp bạn giảm thiểu thiệt hại và rủi ro tiềm ẩn đối với các tài sản và dữ liệu quan trọng. Ngoài ra, điều quan trọng là phải ưu tiên các nhiệm vụ và tập trung vào vấn đề cấp bách nhất.
- **Tư duy phát triển:** Đây là một ngành đang phát triển, vì vậy một kỹ năng quan trọng có thể chuyển giao là sẵn sàng học hỏi. Công nghệ phát triển rất nhanh và đó là một điều tuyệt vời! Điều đó không có nghĩa là bạn sẽ cần phải học tất cả, nhưng điều đó có nghĩa là bạn sẽ cần phải tiếp tục học hỏi trong suốt sự nghiệp của mình. May mắn thay, bạn sẽ có thể áp dụng phần lớn những gì học được trong chương trình này vào quá trình phát triển nghề nghiệp đang diễn ra của mình.
- **Quan điểm đa dạng:** Con đường duy nhất để đi xa là cùng nhau. Bằng cách tôn trọng lẫn nhau và khuyến khích những quan điểm đa dạng cũng như tôn trọng lẫn nhau, chắc chắn bạn sẽ tìm thấy nhiều giải pháp tốt hơn và đa dạng hơn cho các vấn đề bảo mật.

Technical skills

There are many technical skills that will help you be successful in the cybersecurity field. You'll learn and practice these skills as you progress through the certificate program. Some of the tools and concepts you'll need to use and be able to understand include:

- **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.
- **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts' ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.
- **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It's important to become familiar with IDSs because they're a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
- **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.

- **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization's outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

Kĩ năng công nghệ

Có nhiều kỹ năng kỹ thuật sẽ giúp bạn thành công trong lĩnh vực an ninh mạng. Bạn sẽ học và thực hành những kỹ năng này khi bạn tiến bộ thông qua chương trình chứng chỉ. Một số công cụ và khái niệm bạn sẽ cần sử dụng và có thể hiểu được bao gồm:

- **Ngôn ngữ lập trình:** Bằng cách hiểu cách sử dụng ngôn ngữ lập trình, các nhà phân tích an ninh mạng có thể tự động hóa các tác vụ vốn rất tốn thời gian. Ví dụ về các tác vụ mà lập trình có thể được sử dụng bao gồm tìm kiếm dữ liệu để xác định các mối đe dọa tiềm ẩn hoặc tổ chức và phân tích thông tin để xác định các mẫu liên quan đến vấn đề bảo mật.
- **Công cụ quản lý sự kiện và thông tin bảo mật (SIEM):** Công cụ SIEM thu thập và phân tích dữ liệu nhật ký hoặc bản ghi các sự kiện như hành vi đăng nhập bất thường và hỗ trợ khả năng giám sát các hoạt động quan trọng trong tổ chức của nhà phân tích. Điều này giúp các chuyên gia an ninh mạng xác định và phân tích các mối đe dọa, rủi ro và lỗ hổng bảo mật tiềm ẩn hiệu quả hơn.
- **Hệ thống phát hiện xâm nhập (IDS):** Các nhà phân tích an ninh mạng sử dụng IDS để giám sát hoạt động của hệ thống và cảnh báo về các hành vi xâm nhập có thể xảy ra. Điều quan trọng là phải làm quen với IDS vì chúng là công cụ chính mà mọi tổ chức sử dụng để bảo vệ tài sản và dữ liệu. Ví dụ: bạn có thể sử dụng IDS để giám sát mạng nhằm phát hiện các dấu hiệu hoạt động độc hại, như truy cập trái phép vào mạng.
- **Kiến thức về bối cảnh mối đe dọa:** Nhận thức được các xu hướng hiện tại liên quan đến tác nhân đe dọa, phần mềm độc hại hoặc phương pháp đe dọa là rất quan trọng. Kiến thức này cho phép các nhóm bảo mật xây dựng hệ thống phòng thủ mạnh mẽ hơn trước các chiến thuật và kỹ thuật của tác nhân đe dọa. Bằng cách cập nhật các xu hướng và kiểu tấn công, các chuyên gia bảo mật có thể nhận biết tốt hơn khi các loại mối đe dọa mới xuất hiện, chẳng hạn như biến thể ransomware mới.
- **Ứng phó sự cố:** Các nhà phân tích an ninh mạng cần có khả năng tuân theo các chính sách và quy trình đã được thiết lập để ứng phó với sự cố một cách thích hợp. Ví dụ: nhà phân tích bảo mật có thể nhận được cảnh báo về một cuộc tấn công phần mềm độc hại có thể xảy ra, sau đó làm theo các quy trình được nêu ra của tổ chức để bắt đầu quá trình ứng phó sự cố. Điều này có thể liên quan đến

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

việc tiến hành một cuộc điều tra để xác định vấn đề gốc rễ và thiết lập các cách để khắc phục nó.

CompTIA Security+

In addition to gaining skills that will help you succeed as a cybersecurity professional, the Google Cybersecurity Certificate helps prepare you for the [CompTIA Security+ exam](#), the industry leading certification for cybersecurity roles. You'll earn a dual credential when you complete both, which can be shared with potential employers. After completing all eight courses in the Google Cybersecurity Certificate, you will unlock a 30% discount for the CompTIA Security+ exam and additional practice materials.

Bảo mật CompTIA+

Ngoài việc đạt được các kỹ năng giúp bạn thành công với tư cách là chuyên gia an ninh mạng, Chứng chỉ an ninh mạng của Google còn giúp bạn chuẩn bị cho [Kỳ thi CompTIA Security+](#), chứng nhận hàng đầu trong ngành về vai trò an ninh mạng. Bạn sẽ nhận được chứng chỉ kép khi hoàn thành cả hai, chứng chỉ này có thể được chia sẻ với các nhà tuyển dụng tiềm năng. Sau khi hoàn thành tất cả tám khóa học trong Chứng chỉ an ninh mạng của Google, bạn sẽ được giảm giá 30% cho kỳ thi CompTIA Security+ và các tài liệu thực hành bổ sung.

Key takeaways

Understanding the benefits of core transferable and technical skills can help prepare you to successfully enter the cybersecurity workforce. Throughout this program, you'll have multiple opportunities to develop these and other key cybersecurity analyst skills.

Bài học chính

Hiểu được lợi ích của các kỹ năng kỹ thuật và chuyển giao cốt lõi có thể giúp bạn chuẩn bị gia nhập thành công lực lượng lao động an ninh mạng. Trong suốt chương trình này, bạn sẽ có nhiều cơ hội để phát triển những kỹ năng này và các kỹ năng phân tích an ninh mạng quan trọng khác.

3.4. The importance of cybersecurity

As we've discussed security professionals protect many physical and digital assets. These skills are desired by organizations and government entities because risk needs to be managed. Let's continue to discuss why security matters.

Như chúng ta đã thảo luận, các chuyên gia bảo mật bảo vệ nhiều tài sản vật lý và kỹ thuật số. Những kỹ năng này được các tổ chức mong muốn và các cơ quan chính phủ vì rủi ro cần phải được quản lý. Hãy tiếp tục thảo luận tại sao vấn đề bảo mật lại quan trọng.

Security is essential for ensuring an organization's business continuity and ethical standing. There are both legal implications and moral considerations to maintaining an organization's security. A data breach for example affects everyone that is associated with the organization. This is because data losses or leaks can affect an

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

organization's reputation as well as the lives and reputations of their users clients and customers. By maintaining strong security measures organizations can increase user trust. This may lead to financial growth and ongoing business referrals.

Bảo mật là điều cần thiết để đảm bảo tính liên tục trong kinh doanh của tổ chức và hỗ trợ đúng đạo đức. Có cả ý nghĩa pháp lý và cân nhắc về mặt đạo đức để duy trì an ninh của một tổ chức. Ví dụ, một vi phạm dữ liệu ảnh hưởng đến tất cả những người có liên quan đến tổ chức. Điều này là do việc mất hoặc rò rỉ dữ liệu có thể ảnh hưởng đến danh tiếng của tổ chức cũng như tính mạng và danh tiếng của người sử dụng, khách hàng và khách hàng của họ. Bằng cách duy trì các biện pháp bảo mật mạnh mẽ, các tổ chức có thể tăng cường sự tin tưởng của người dùng. Điều này có thể dẫn đến tăng trưởng tài chính và giới thiệu kinh doanh liên tục.

As previously mentioned organizations are not the only ones that suffer during a data breach. Maintaining and securing user customer and vendor data is an important part of preventing incidents that may expose people's personally identifiable information.

Như đã nói ở trên, các tổ chức không phải là những người duy nhất phải chịu thiệt hại khi vi phạm dữ liệu. Duy trì và bảo mật người dùng, khách hàng và Dữ liệu nhà cung cấp là một phần quan trọng trong việc ngăn chặn các sự cố có thể xảy ra. Tiết lộ thông tin nhận dạng cá nhân của mọi người.

Personally identifiable information known as PII is any information used to infer an individual's identity. PII includes someone's full name date of birth physical address phone number email address internet protocol or IP address and similar information.

Thông tin nhận dạng cá nhân, được gọi là PII, là bất kỳ thông tin được sử dụng để suy ra danh tính của một cá nhân. PII bao gồm tên đầy đủ của ai đó, ngày sinh, địa chỉ vật lý, số điện thoại, địa chỉ email, giao thức internet hoặc địa chỉ IP và thông tin tương tự.

Sensitive personally identifiable information known as SPII is a specific type of PII that falls under stricter handling guidelines and may include social security numbers medical or financial information and biometric data such as facial recognition. If SPII is stolen this has the potential to be significantly more damaging to an individual than if PII is stolen.

Thông tin nhận dạng cá nhân nhạy cảm, đã biết dưới dạng SPII, là một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn và có thể bao gồm số an sinh xã hội, y tế hoặc thông tin tài chính và dữ liệu sinh trắc học, chẳng hạn như nhận dạng khuôn mặt. Nếu SPII bị đánh cắp, điều này có khả năng gây thiệt hại đáng kể, gây tổn hại cho một cá nhân nhiều hơn nếu PII bị đánh cắp.

PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised leaked or stolen identity theft is the primary concern.

Dữ liệu PII và SPII là tài sản chính mà kẻ đe dọa sẽ tìm kiếm nếu một tổ chức gặp phải vi phạm. Khi thông tin nhận dạng của một người bị xâm phạm, rò rỉ, hoặc bị đánh cắp, trộm cắp danh tính là mối quan tâm hàng đầu.

Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain.

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Trộm cắp danh tính là hành vi đánh cắp thông tin cá nhân để thực hiện hành vi lừa đảo trong khi mạo danh nạn nhân. Và mục tiêu chính của hành vi trộm cắp danh tính là thu lợi tài chính.

We've explored several reasons why security matters. Employers need security analysts like you to fill the current and future demand to protect data products and people while ensuring confidentiality integrity and safe access to information. This is why the U.S. Bureau of Labor Statistics expects the demand for security professionals to grow by more than 30% by the year 2030.

Chúng tôi đã khám phá một số lý do tại sao vấn đề bảo mật lại quan trọng. Nhà tuyển dụng cần các nhà phân tích bảo mật như bạn để hoàn thành công việc hiện tại và nhu cầu trong tương lai để bảo vệ dữ liệu, sản phẩm và con người đồng thời đảm bảo tính bảo mật, tính toàn vẹn và truy cập thông tin một cách an toàn. Đây là lý do tại sao Cục Thống kê Lao động Hoa Kỳ dự kiến nhu cầu về số lượng chuyên gia bảo mật sẽ tăng hơn 30% vào năm 2030.

So keep learning and eventually you'll be able to do your part to create a safer and more secure environment for organizations and people alike!

Vì vậy, hãy tiếp tục học hỏi và cuối cùng bạn sẽ có thể góp phần tạo ra một môi trường an toàn hơn và môi trường an toàn hơn cho các tổ chức và mọi người!

3.5. Explore: Keep organizations secure

Learn to keep organizations secure

Học cách giữ tổ chức chắc chắn

Analytical thinking



Analytical thinking

Security analysts often use **analytical thinking**, which means to think carefully and thoroughly. Analysts use this skill when **monitoring and securing computer and network systems**, responding to potential threats, defining system privileges, and determining ways to mitigate risk.

Collaboration



Collaboration

Collaboration means working with stakeholders and other team members. Security analysts often use this skill when **responding to an active threat**. They'll work with others when blocking unauthorized access and ensuring any compromised systems are restored.


| | |
|---------------------|---------------|
| Analytical thinking | Collaboration |
| Tư duy phân tích | Sự hợp tác |

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng


| | |
|--|--|
| <p>Các nhà phân tích chứng khoán thường sử dụng tư duy phân tích, nghĩa là suy nghĩ cẩn thận và kỹ lưỡng. Các nhà phân tích sử dụng kỹ năng này khi giám sát và bảo mật hệ thống máy tính và mạng, ứng phó với các mối đe dọa tiềm ẩn, xác định đặc quyền hệ thống và xác định cách giảm thiểu rủi ro.</p> | <p>Hợp tác có nghĩa là làm việc với các bên liên quan và các thành viên khác trong nhóm. Các nhà phân tích bảo mật thường sử dụng kỹ năng này khi ứng phó với một mối đe dọa đang diễn ra. Họ sẽ làm việc với những người khác khi chặn truy cập trái phép và đảm bảo mọi hệ thống bị xâm nhập đều được khôi phục.</p> |
|--|--|

Malware prevention



Malware prevention
When a specific threat or vulnerability is identified, an analyst might **install prevention software**, which is software that works to proactively prevent a threat from occurring. Because malware is designed to harm devices or networks, **malware prevention** is essential.

Communication




Communication
As an analyst prevents and encounters threats, risks, or vulnerabilities, they document and **report findings**. A report might detail attempts to secure systems, test weak points, or offer solutions for system improvement. When reporting findings, strong **communication** skills are important.

| Malware prevention | Communication |
|--|---|
| <p>Phòng chống phần mềm độc hại Khi xác định được một mối đe dọa hoặc lỗ hổng cụ thể, nhà phân tích có thể cài đặt phần mềm phòng ngừa, đây là phần mềm hoạt động để chủ động ngăn chặn mối đe dọa xảy ra. Vì phần mềm độc hại được thiết kế để gây hại cho thiết bị hoặc mạng nên việc ngăn chặn phần mềm độc hại là điều cần thiết.</p> | <p>Giao tiếp Khi một nhà phân tích ngăn chặn và gặp phải các mối đe dọa, rủi ro hoặc lỗ hổng, họ sẽ ghi lại và báo cáo các phát hiện. Một báo cáo có thể trình bày chi tiết các nỗ lực nhằm bảo mật hệ thống, kiểm tra các điểm yếu hoặc đưa ra giải pháp cải tiến hệ thống. Khi báo cáo các phát hiện, kỹ năng giao tiếp tốt là rất quan trọng.</p> |


Module 1: Welcome to the exciting world of cybersecurity
Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Understanding programming languages



Understanding programming languages
Analysts may sometimes work with software development teams to analyze and support security, install software, and set up appropriate processes. When involved with **software development** projects, it can be helpful for an analyst to **understand programming languages**.

Using SIEM tools



Using SIEM tools
When security analysts need to review vulnerabilities, they conduct a **periodic security audit**. This is a review of an organization's records, activities, and related documents. During audits, **Security Information and Event Management (SIEM) tools** help analysts better understand security threats, risks, and vulnerabilities.

| Understanding programming languages | Using SIEM tools |
|---|---|
| <p>Hiểu ngôn ngữ lập trình</p> <p>Các nhà phân tích đôi khi có thể làm việc với các nhóm phát triển phần mềm để phân tích và hỗ trợ bảo mật, cài đặt phần mềm và thiết lập các quy trình thích hợp. Khi tham gia vào các dự án phát triển phần mềm, việc hiểu ngôn ngữ lập trình có thể hữu ích cho nhà phân tích.</p> | <p>Sử dụng công cụ SIEM</p> <p>Khi các nhà phân tích bảo mật cần xem xét các lỗ hổng, họ sẽ tiến hành kiểm tra bảo mật định kỳ. Đây là việc xem xét hồ sơ, hoạt động và các tài liệu liên quan của tổ chức. Trong quá trình kiểm tra, các công cụ Quản lý sự kiện và thông tin bảo mật (SIEM) giúp các nhà phân tích hiểu rõ hơn về các mối đe dọa, rủi ro và lỗ hổng bảo mật.</p> |

3.6. The value of cybersecurity

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

3.7. Test your knowledge: Core skills for cybersecurity professionals

4. Review: Welcome to the exciting world of cybersecurity – Đánh giá: Chào mừng đến với thế giới đầy thú vị của An ninh mạng

4.1. Wrap-up

Wrap-up

Congratulations on completing the first section of this course! Let's quickly review what we've covered so far, before moving on.

We defined security and introduced the benefits of implementing security in an organization. Then, we discussed different job responsibilities, such as managing threats and installing prevention software. We also introduced some important core skills, like collaboration and computer forensics. We finished by discussing the value of security and how it supports critical business functions.

I hope you've gained a greater understanding of security. If you feel like you need a refresher before moving on, you can always go back and review any content you're unsure about.

By learning the basics, you are laying the foundation for the rest of your security career.

Coming up, we'll explore some well-known attacks that shaped the security industry. I'm excited to continue this journey with you!

Gợi lại

Chúc mừng bạn đã hoàn thành phần đầu tiên của khóa học này! Hãy nhanh chóng xem lại những gì chúng ta có được đề cập cho đến nay, trước khi tiếp tục.

Chúng tôi đã xác định bảo mật và giới thiệu lợi ích của việc thực hiện bảo mật trong một tổ chức. Sau đó, chúng tôi thảo luận về các trách nhiệm công việc khác nhau, chẳng hạn như quản lý các mối đe dọa và cài đặt phần mềm phòng ngừa. Chúng tôi cũng giới thiệu một số kỹ năng cốt lõi quan trọng, như sự hợp tác và điều tra máy tính. Chúng ta kết thúc bằng việc thảo luận về giá trị của sự an toàn và cách nó hỗ trợ các chức năng kinh doanh quan trọng.

Tôi hy vọng bạn đã hiểu rõ hơn về bảo mật. Nếu bạn cảm thấy cần ôn lại trước khi tiếp tục, bạn luôn có thể quay lại và xem lại bất kỳ nội dung nào bạn không chắc chắn.

Bằng cách học những điều cơ bản, bạn đang đặt nền móng cho phần còn lại của sự nghiệp bảo mật của bạn.

Sắp tới chúng ta sẽ khám phá một số cuộc tấn công nổi tiếng đã định hình ngành công nghiệp bảo mật. Tôi rất vui được tiếp tục cuộc hành trình này với bạn!

4.2. Glossary terms from module 1

Glossary terms from module 1

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Terms and definitions from Course 1, Module 1

Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

Cloud security: The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

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

Network security: The practice of keeping an organization's network infrastructure secure from unauthorized access

Personally identifiable information (PII): Any information used to infer an individual's identity

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

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Technical skills: Skills that require knowledge of specific tools, procedures, and policies

Threat: Any circumstance or event that can negatively impact assets

Threat actor: Any person or group who presents a security risk

Transferable skills: Skills from other areas that can apply to different careers

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

An ninh mạng (hoặc bảo mật): Thực tiễn đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác tội phạm

Bảo mật đám mây: Quá trình đảm bảo rằng các tài sản được lưu trữ trên đám mây được cấu hình đúng cách và quyền truy cập vào các tài sản đó được giới hạn ở những người dùng được ủy quyền

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

An ninh mạng: Thực tiễn giữ an toàn cho cơ sở hạ tầng mạng của tổ chức khỏi bị truy cập trái phép

Module 1: Welcome to the exciting world of cybersecurity

Phần 1: Chào mừng đến với thế giới thú vị của an ninh mạng

Thông tin nhận dạng cá nhân (PII): Bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân

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

Thông tin nhận dạng cá nhân nhạy cảm (SPII): Một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn

Kỹ năng kỹ thuật: Kỹ năng đòi hỏi kiến thức về các công cụ, thủ tục và chính sách cụ thể

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

Tác nhân đe dọa: Bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật

Kỹ năng có thể chuyển giao: Kỹ năng từ các lĩnh vực khác có thể áp dụng cho các ngành nghề khác nhau

4.3. Module 1 challenge

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Module 2: The evolution of cybersecurity – Sự phát triển của an ninh mạng

You will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. You will also understand how past and present cyber attacks have influenced the development of the security field. In addition, you'll get an overview of the eight security domains.

Bạn sẽ khám phá các mối đe dọa an ninh mạng đã xuất hiện và phát triển như thế nào cùng với việc sử dụng máy tính. Bạn cũng sẽ hiểu các cuộc tấn công mạng trong quá khứ và hiện tại đã ảnh hưởng như thế nào đến sự phát triển của lĩnh vực bảo mật. Ngoài ra, bạn sẽ có được cái nhìn tổng quan về tám lĩnh vực bảo mật.

Learning Objectives

- Identify the most common types of attacks, past and present
- Identify how security attacks impact business operations
- Recognize how past and present attacks on business operations have led to the development of the security field
- Identify the CISSP eight security domains

Mục tiêu học tập

- Xác định các loại tấn công phổ biến nhất, trong quá khứ và hiện tại
- Xác định các cuộc tấn công bảo mật ảnh hưởng đến hoạt động kinh doanh như thế nào
- Nhận biết các cuộc tấn công trong quá khứ và hiện tại vào hoạt động kinh doanh đã dẫn đến sự phát triển của lĩnh vực bảo mật như thế nào
- Xác định tám miền bảo mật CISSP

1. The history of cybersecurity – Lịch sử an ninh mạng

1.1 Welcome to module 2 – Chào mừng đến với module 2

Welcome back! When it comes to security, there is so much to learn, and I'm thrilled to be part of your career journey.

Chào mừng trở lại! Khi nói đến vấn đề bảo mật, có rất nhiều điều để học, và tôi vui mừng được trở thành một phần trong hành trình sự nghiệp của bạn.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

This is such an exciting time to be learning about security! When I learned about international hacks that impacted both private companies and government organizations, I was inspired to want to work in security because I realized how dynamic and important this field is.

Đây quả là khoảng thời gian thú vị đang tìm hiểu về bảo mật! Khi tôi biết về các vụ hack quốc tế ảnh hưởng đến cả các công ty tư nhân và các tổ chức chính phủ, Tôi được truyền cảm hứng muốn làm việc trong lĩnh vực an ninh bởi vì tôi nhận ra lĩnh vực này năng động và quan trọng như thế nào.

One reason there are so many jobs in the security field today, is because of attacks that happened in the 1980s and 1990s. Decades later, security professionals are still actively working to protect organizations and people from variations of these early computer attacks.

Một lý do có ngày nay có rất nhiều việc làm trong lĩnh vực an ninh, là do các cuộc tấn công xảy ra vào những năm 1980 và 1990. Nhiều thập kỷ sau, các chuyên gia an ninh vẫn đang tích cực làm việc để bảo vệ tổ chức và người dân từ các biến thể của những cuộc tấn công máy tính đầu tiên này.

In this section of the course, we'll discuss viruses and malware, and introduce the concept of social engineering. Then, we'll discuss how the digital age ushered in a new era of threat actors. Knowing the evolution of each attack is key to protecting against future attacks. Lastly, we'll provide an overview of eight security domains.

Trong phần này của khóa học, chúng ta sẽ thảo luận về virus và phần mềm độc hại và giới thiệu khái niệm về kỹ thuật xã hội. Sau đó, chúng ta sẽ thảo luận về cách thời đại kỹ thuật số đã mở ra một kỷ nguyên mới của các tác nhân đe dọa. Biết diễn biến của mỗi đòn tấn công là chìa khóa để bảo vệ chống lại các cuộc tấn công trong tương lai. Cuối cùng, chúng tôi sẽ cung cấp tổng quan về tám lĩnh vực bảo mật.

Next up, we'll travel back in time, to explore some of the viruses, data breaches, and malware attacks that have helped shape the industry as we know it today.

Tiếp theo, chúng ta sẽ du hành ngược thời gian, để khám phá một số loại virus, vi phạm dữ liệu và tấn công phần mềm độc hại đã giúp định hình ngành công nghiệp như chúng ta biết ngày nay.

1.2. Past cybersecurity attacks – Các cuộc tấn công an ninh mạng trong quá khứ

Past cybersecurity attacks

The security industry is constantly evolving, but many present-day attacks are not entirely new. Attackers often alter or enhance previous methods. Understanding past attacks can provide direction for how to handle or investigate incidents in your job as a security analyst. First, let's go over a couple of key terms that will support your understanding of the attacks we'll discuss. A computer virus is malicious code written to interfere with computer operations and cause damage to data and software. The virus attaches itself to programs or documents on a computer, then spreads and infects one or more computers in a network. Today, viruses are more commonly referred to as malware, which is software designed to harm devices or networks. Two examples of early malware attacks that we'll cover are the Brain virus and the Morris worm.

Ngành an ninh không ngừng phát triển nhưng nhiều cuộc tấn công ngày nay không hoàn toàn mới. Những kẻ tấn công thường thay đổi hoặc nâng cao các phương pháp trước

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

đó. Hiểu các cuộc tấn công trong quá khứ có thể đưa ra hướng xử lý hoặc điều tra các sự cố trong công việc của bạn là một nhà phân tích bảo mật. Đầu tiên, chúng ta hãy đi qua một số thuật ngữ chính. Điều đó sẽ hỗ trợ sự hiểu biết của bạn về các cuộc tấn công mà chúng ta sẽ thảo luận. Virus máy tính là mã độc được viết để can thiệp vào hoạt động của máy tính và nguyên nhân như hỏng dữ liệu và phần mềm. Virus tự bám vào chương trình hoặc tài liệu trên máy tính, sau đó lây lan và lây nhiễm một hoặc nhiều máy tính trong mạng. Ngày nay, virus thường được gọi là phần mềm độc hại, là phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng. Hai ví dụ về các cuộc tấn công phần mềm độc hại ban đầu mà chúng tôi sẽ bao gồm virus Brain và sâu Morris.

They were created by malware developers to accomplish specific tasks. However, the developers underestimated the impact their malware would have and the amount of infected computers there would be. Let's take a closer look at these attacks and discuss how they helped shape security as we know it today. In 1986, the Alvi brothers created the Brain virus, although the intention of the virus was to track illegal copies of medical software and prevent pirated licenses, what the virus actually did was unexpected. Once a person used a pirated copy of the software, the virus-infected that computer. Then, any disk that was inserted into the computer was also infected. The virus spread to a new computer every time someone used one of the infected disks. Undetected, the virus spread globally within a couple of months. Although the intention was not to destroy data or hardware, the virus slowed down productivity and significantly impacted business operations.

Chúng được tạo ra bởi các nhà phát triển phần mềm độc hại để hoàn thành các nhiệm vụ cụ thể. Tuy nhiên, các nhà phát triển đã đánh giá thấp tác động phần mềm độc hại của họ sẽ có và số lượng số máy tính bị nhiễm sẽ có. Chúng ta hãy xem xét kỹ hơn các cuộc tấn công này và thảo luận về cách họ đã giúp hình thành an ninh như chúng ta biết ngày nay. Năm 1986, anh em nhà Alvi đã tạo ra virus Brain, mặc dù mục đích của virus là theo dõi sao chép bất hợp pháp phần mềm y tế và ngăn chặn giấy phép vi phạm bản quyền, những gì virus thực sự đã làm thật bất ngờ. Khi một người sử dụng bản sao lậu của phần mềm, bị nhiễm virus máy tính đó. Sau đó, bất kỳ đĩa nào được đưa vào máy tính cũng bị nhiễm virus. Virus lây lan sang máy tính mới mỗi khi ai đó sử dụng một trong các đĩa bị nhiễm. Virus không bị phát hiện lan rộng trên toàn cầu trong vòng một vài tháng. Mặc dù mục đích không phải là phá hủy dữ liệu hoặc phần cứng, virus làm chậm năng suất và đã ảnh hưởng đáng kể đến hoạt động kinh doanh.

The Brain virus fundamentally altered the computing industry, emphasizing the need for a plan to maintain security and productivity. As a security analyst, you will follow and maintain strategies put in place to ensure your organization has a plan to keep their data and people safe. Another influential computer attack was the Morris worm.

Về cơ bản virus não đã thay đổi ngành công nghiệp máy tính, nhấn mạnh sự cần thiết của một kế hoạch duy trì an ninh và năng suất. Là một nhà phân tích chứng khoán, bạn sẽ theo dõi và duy trì chiến lược được đưa ra để đảm bảo tổ chức của bạn có một kế hoạch để giữ an toàn cho dữ liệu của họ và mọi người. Một cuộc tấn công máy tính có ảnh hưởng khác là sâu Morris.

In 1988, Robert Morris developed a program to assess the size of the internet. The program crawled the web and installed itself onto other computers to tally the number of computers that were connected to the internet. Sounds simple, right? The program, however, failed to keep track of the computers it had already compromised and

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

continued to re-install itself until the computers ran out of memory and crashed. About 6,000 computers were affected, representing 10% of the internet at the time. This attack cost millions of dollars in damages due to business disruptions and the efforts required to remove the worm. After the Morris worm, Computer Emergency Response Teams, known as CERTs®, were established to respond to computer security incidents. CERTs still exist today, but their place in the security industry has expanded to include more responsibilities. Later in this program, you'll learn more about the core functions of these security teams and gain hands-on practice with detection and response tools. Early attacks played a key role in shaping the current security industry. And coming up, we'll discuss how attacks evolved in the digital age.

Năm 1988, Robert Morris đã phát triển một chương trình để đánh giá kích thước của internet. Chương trình đã thu thập thông tin trên web và tự cài đặt vào các máy tính khác để kiểm đếm số lượng của các máy tính đã được kết nối với Internet. Nghe có vẻ đơn giản phải không? Tuy nhiên, chương trình đã thất bại theo dõi các máy tính nó có đã bị xâm phạm và tiếp tục cài đặt lại cho đến khi máy tính hết bộ nhớ và bị hỏng. Khoảng 6.000 máy tính bị ảnh hưởng chiếm 10% Internet vào thời điểm đó. Cuộc tấn công này gây thiệt hại hàng triệu đô la do sự gián đoạn kinh doanh và những nỗ lực cần thiết để loại bỏ sâu. Sau sâu Morris, Đội ứng phó khẩn cấp máy tính, được gọi là CERTs®, được thành lập để ứng phó với các sự cố an ninh máy tính. CERT vẫn tồn tại cho đến ngày nay, nhưng vị trí của họ trong ngành an ninh có được mở rộng để bao gồm nhiều trách nhiệm hơn. Sau đó trong chương trình này, bạn sẽ tìm hiểu thêm về chức năng cốt lõi của các đội bảo mật này và được thực hành thực tế với các công cụ phát hiện và phản hồi. Các cuộc tấn công sớm đóng một vai trò quan trọng trong việc định hình ngành công nghiệp an ninh hiện nay. Và sắp tới, chúng ta sẽ thảo luận về cách các cuộc tấn công phát triển trong thời đại kỹ thuật số.

1.3. Attacks in the digital age – Tấn công trong thời đại kỹ thuật số

Attacks in the digital age

With the expansion of reliable high-speed internet, the number of computers connected to the internet increased dramatically. Because malware could spread through the internet, threat actors no longer needed to use physical disks to spread viruses.

Với việc mở rộng mạng Internet tốc độ cao đáng tin cậy, số lượng máy tính kết nối internet tăng lên đáng kể. Vì phần mềm độc hại có thể lây lan qua internet, Các tác nhân đe dọa không còn cần thiết phải sử dụng đĩa vật lý để phát tán vi-rút.

To better understand attacks in the digital age, we'll discuss two notable attacks that relied on the internet: the LoveLetter attack and the Equifax breach.

Để hiểu rõ hơn về các cuộc tấn công trong thời đại kỹ thuật số, chúng ta sẽ thảo luận về hai cuộc tấn công đáng chú ý dựa trên internet: cuộc tấn công LoveLetter và vi phạm Equifax.

In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled,

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

"Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over \$10 billion dollars in damages. The LoveLetter attack is the first example of social engineering.

Vào năm 2000, Onel De Guzman đã tạo ra Thư tình phần mềm độc hại để đánh cắp thông tin đăng nhập internet. Cuộc tấn công này lan truyền nhanh chóng và lợi dụng những người chưa phát triển một sự nghi ngờ lành mạnh đối với các email không được yêu cầu. Người dùng đã nhận được một email có dòng tiêu đề "I Love You". Mỗi email đều chứa một tệp đính kèm có nhãn "Thư tình dành cho em". Khi tệp đính kèm được mở, phần mềm độc hại sẽ quét sổ địa chỉ của người dùng. Sau đó, nó tự động gửi đến từng người trong danh sách và đã cài đặt một chương trình để thu thập thông tin người dùng và mật khẩu. Người nhận sẽ nghĩ rằng họ đang nhận được email từ một người bạn, nhưng nó thực sự là phần mềm độc hại. Bức thư tình cuối cùng đã lây nhiễm sang 45 triệu máy tính trên toàn cầu và được cho là đã gây ra thiệt hại hơn 10 tỷ USD. Cuộc tấn công LoveLetter là ví dụ đầu tiên của kỹ thuật xã hội.

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

Kỹ thuật xã hội là một kỹ thuật thao túng khai thác lỗi của con người để có được thông tin cá nhân, quyền truy cập hoặc vật có giá trị.

After the LoveLetter, attackers understood the power of social engineering. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Many people are now prioritizing convenience over privacy. The trade-off of this evolving shift is that these tools may lead to increased vulnerability, if people do not use them appropriately.

Sau bức thư tình, Những kẻ tấn công hiểu được sức mạnh của kỹ thuật xã hội. Số lượng các cuộc tấn công kỹ thuật xã hội đang gia tăng với mỗi ứng dụng truyền thông xã hội cho phép công chúng truy cập vào dữ liệu của mọi người. Nhiều người hiện đang ưu tiên sự thuận tiện hơn quyền riêng tư. Sự đánh đổi của sự thay đổi đang phát triển này là những công cụ này có thể dẫn đến tính dễ bị tổn thương tăng lên nếu người dân không sử dụng chúng một cách hợp lý.

As a security professional, your role is to identify and manage inappropriate use of technology that may place your organization and all the people associated with it at risk. One way to safeguard your organization is to conduct regular internal trainings, which you as a future security analyst may be asked to lead or participate in.

Là một chuyên gia bảo mật, vai trò của bạn là xác định và quản lý việc sử dụng công nghệ không phù hợp có thể khiến tổ chức của bạn và tất cả những người liên quan đến nó đều gặp rủi ro. Một cách để bảo vệ tổ chức của bạn là tiến hành đào tạo nội bộ thường xuyên, mà bạn với tư cách là nhà phân tích bảo mật trong tương lai có thể được yêu cầu lãnh đạo hoặc tham gia.

Today, it's common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive. Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Ngày nay, điều đó là phổ biến đối với nhân viên được đào tạo về cách xác định các cuộc tấn công lừa đảo qua mạng xã hội. Cụ thể là lừa đảo qua email họ nhận được. Lừa đảo trực tuyến là việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.

Now, let's discuss the Equifax breach. In 2017, attackers successfully infiltrated the credit reporting agency, Equifax. This resulted in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans.

Bây giờ, hãy thảo luận về vụ vi phạm Equifax. Năm 2017, Những kẻ tấn công đã xâm nhập thành công vào cơ quan báo cáo tín dụng Equifax. Điều này dẫn đến một trong những vụ vi phạm dữ liệu nhạy cảm lớn nhất được biết đến. Hơn 143 triệu hồ sơ khách hàng đã bị đánh cắp vi phạm đã ảnh hưởng đến khoảng 40% tổng số người Mỹ.

The records included personally identifiable information including social security numbers, birth dates, driver's license numbers, home addresses, and credit card numbers. From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. The company failed to take the actions needed to fix multiple known vulnerabilities in the months leading up to the data breach.

Các hồ sơ bao gồm thông tin nhận dạng cá nhân bao gồm số an sinh xã hội, ngày sinh, số giấy phép lái xe, địa chỉ nhà và số thẻ tín dụng. Từ quan điểm bảo mật, vi phạm xảy ra do nhiều lỗi từ phía Equifax. Những kẻ tấn công không chỉ lợi dụng một lỗ hổng, Có một vài. Công ty đã không thực hiện các hành động cần thiết để khắc phục nhiều lỗi đã biết lỗ hổng trong những tháng dẫn đến vi phạm dữ liệu.

In the end, Equifax settled with the U.S. government and paid over \$575 million dollars to resolve customer complaints and cover required fines.

Cuối cùng, Equifax đã giải quyết với chính phủ Hoa Kỳ và đã trả hơn 575 triệu đô la để giải quyết khiếu nại của khách hàng và trang trải các khoản tiền phạt bắt buộc.

While there have been other data breaches before and after the Equifax breach, the large settlement with the U.S. government alerted companies to the financial impact of a breach and the need to implement preventative measures.

Mặc dù đã có những vụ vi phạm dữ liệu khác trước và sau vụ vi phạm Equifax, thỏa thuận lớn với chính phủ Hoa Kỳ đã cảnh báo các công ty tác động tài chính của hành vi vi phạm và sự cần thiết phải thực hiện các biện pháp phòng ngừa.

These are just a couple of well-known incidents that have shaped the security industry. Knowing about them will help you in your security career. Understanding different types of malware and social engineering attacks will allow you to communicate about security risks during future job interviews.

Đây chỉ là một vài sự cố nổi tiếng đã định hình ngành an ninh. Biết về họ sẽ giúp ích cho sự nghiệp bảo mật của bạn. Việc hiểu rõ các loại phần mềm độc hại và tấn công kỹ thuật xã hội khác nhau sẽ cho phép bạn trao đổi về các rủi ro bảo mật trong các cuộc phỏng vấn việc làm trong tương lai.

As a future security professional constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job. By noticing similar trends patterns

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

and methodologies

you may be able to identify a potential breach and limit future damage.

Là một chuyên gia bảo mật tương lai, không ngừng thích nghi và đào tạo bản thân về chiến thuật và kỹ thuật của các tác nhân đe dọa sẽ là một phần công việc của bạn. Bằng cách nhận thấy các xu hướng, mô hình và phương pháp tương tự, bạn có thể xác định được hành vi vi phạm tiềm ẩn và hạn chế thiệt hại trong tương lai.

Finally

understanding how security affects people's lives is a good reminder of why the work you will do is so important!

Cuối cùng, hiểu được an ninh ảnh hưởng như thế nào đến cuộc sống của con người là một lời nhắc nhở hữu ích về lý do tại sao công việc bạn sẽ làm lại quan trọng đến vậy!

1.4. Common attacks and their effectiveness – Các cuộc tấn công phổ biến và hiệu quả của chúng

Common attacks and their effectiveness

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, and the evolving tactics and techniques threat actors use, will help you better protect organizations and people.

Các cuộc tấn công phổ biến và hiệu quả của chúng

Trước đây, bạn đã tìm hiểu về các cuộc tấn công trong quá khứ và hiện tại đã giúp định hình ngành an ninh mạng. Chúng bao gồm cuộc tấn công LoveLetter, còn được gọi là virus ILOVEYOU và sâu Morris. Một kết quả là việc thành lập các nhóm ứng phó, hiện nay thường được gọi là các nhóm ứng phó sự cố bảo mật máy tính (CSIRT). Trong bài đọc này, bạn sẽ tìm hiểu thêm về các phương pháp tấn công phổ biến. Làm quen với các phương thức tấn công khác nhau cũng như các chiến thuật và kỹ thuật ngày càng phát triển mà các tác nhân đe dọa sử dụng sẽ giúp bạn bảo vệ tổ chức và con người tốt hơn.

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

- **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
- **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
- **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
- **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Lừa đảo

Lừa đảo trực tuyến là việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.

Một số loại tấn công lừa đảo phổ biến nhất hiện nay bao gồm:

- **Thỏa hiệp email doanh nghiệp (BEC):** Kẻ đe dọa gửi một email có vẻ như đến từ một nguồn đã biết để đưa ra yêu cầu thông tin có vẻ hợp pháp nhằm đạt được lợi thế tài chính.
- **Lừa đảo trực tuyến:** Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể. Email dường như có nguồn gốc từ một nguồn đáng tin cậy.
- **Whaling:** Một hình thức lừa đảo giáo. Các tác nhân đe dọa nhắm vào các giám đốc điều hành của công ty để có quyền truy cập vào dữ liệu nhạy cảm.
- **Vishing:** Việc khai thác giao tiếp bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết.
- **Smishing:** Việc sử dụng tin nhắn văn bản để lừa người dùng nhằm lấy được thông tin nhạy cảm hoặc mạo danh một nguồn đã biết.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

- **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware:** Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Phần mềm độc hại là phần mềm được thiết kế nhằm gây hại cho thiết bị hoặc mạng. Có nhiều loại phần mềm độc hại. Mục đích chính của phần mềm độc hại là lấy tiền hoặc trong một số trường hợp là lợi thế thông minh có thể được sử dụng để chống lại một cá nhân, tổ chức hoặc lãnh thổ.

Một số loại tấn công phần mềm độc hại phổ biến nhất hiện nay bao gồm:

- **Virus:** Mã độc được viết nhằm can thiệp vào hoạt động của máy tính và gây hư hỏng dữ liệu, phần mềm. Vi-rút cần được tạo ra bởi người dùng (tức là tác nhân đe dọa), người này truyền vi-rút thông qua tệp đính kèm hoặc tệp tải xuống độc hại. Khi ai đó mở tệp đính kèm hoặc tệp tải xuống độc hại, vi-rút sẽ ẩn mình trong các tệp khác trong hệ thống hiện đã bị nhiễm. Khi các tệp bị nhiễm được mở, nó cho phép vi-rút chèn mã riêng của nó để làm hỏng và/hoặc phá hủy dữ liệu trong hệ thống.
- **Worms:** Phần mềm độc hại có thể tự nhân bản và lây lan trên các hệ thống. Ngược lại với virus, người dùng không cần phải tải sâu xuống. Thay vào đó, nó tự sao chép và lây lan từ máy tính đã bị nhiễm sang các thiết bị khác trên cùng mạng.
- **Phần mềm tống tiền:** Một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập.
- **Phần mềm gián điệp:** Phần mềm độc hại được sử dụng để thu thập và bán thông tin mà không có sự đồng ý. Phần mềm gián điệp có thể được sử dụng để truy cập các thiết bị. Điều này cho phép các tác nhân đe dọa thu thập dữ liệu cá nhân, chẳng hạn như email riêng tư, văn bản, bản ghi âm giọng nói và hình ảnh cũng như vị trí.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

- **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.
- **USB baiting:** A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
- **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Reasons why social engineering attacks are effective include:

- **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- **Scarcity:** A tactic used to imply that goods or services are in limited supply.
- **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.
- **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.
- **Urgency:** A threat actor persuades others to respond quickly and without questioning.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Kỹ thuật xã hội là một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc vật có giá trị. Lỗi của con người thường là kết quả của việc tin tưởng ai đó mà không thắc mắc. Nhiệm vụ của kẻ đe dọa, hoạt động như một kẻ lừa đảo xã hội, là tạo ra một môi trường tin tưởng sai lầm và dối trá để lợi dụng càng nhiều người càng tốt.

Một số loại tấn công kỹ thuật xã hội phổ biến nhất hiện nay bao gồm:

- **Lừa đảo trên mạng xã hội:** Kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của chúng từ các trang mạng xã hội. Sau đó, họ bắt đầu một cuộc tấn công.
- **Tấn công Watering Hole:** Kẻ đe dọa tấn công một trang web thường xuyên được một nhóm người dùng cụ thể truy cập.
- **Bẫy USB:** Kẻ đe dọa có chiến lược để lại thẻ USB chứa phần mềm độc hại để nhân viên tìm và cài đặt, nhằm vô tình lây nhiễm vào mạng.
- **Kỹ thuật xã hội vật lý:** Kẻ đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế.

Nguyên tắc kỹ thuật xã hội

Kỹ thuật xã hội cực kỳ hiệu quả. Điều này là do mọi người thường tin tưởng và có điều kiện để tôn trọng quyền lực. Số lượng các cuộc tấn công kỹ thuật xã hội đang gia tăng với mỗi ứng dụng truyền thông xã hội mới cho phép truy cập công khai vào dữ liệu của mọi người. Mặc dù việc chia sẻ dữ liệu cá nhân—chẳng hạn như vị trí hoặc ảnh của bạn—có thể thuận tiện nhưng cũng có rủi ro.

Lý do tại sao các cuộc tấn công kỹ thuật xã hội có hiệu quả bao gồm:

- **Quyền hạn:** Các tác nhân đe dọa mạo danh những cá nhân có quyền lực. Điều này là do mọi người nói chung đã có thói quen tôn trọng và tuân theo những người có thẩm quyền.
- **Đe dọa:** Những kẻ đe dọa sử dụng chiến thuật bắt nạt. Điều này bao gồm việc thuyết phục và đe dọa nạn nhân làm theo những gì họ được yêu cầu.
- **Sự đồng thuận/Bằng chứng xã hội:** Bởi vì mọi người đôi khi làm những việc mà họ tin rằng nhiều người khác đang làm, nên những kẻ đe dọa lợi dụng lòng tin của người khác để giả vờ rằng họ hợp pháp. Ví dụ: kẻ đe dọa có thể cố gắng giành quyền truy cập vào dữ liệu riêng tư bằng cách nói với nhân viên rằng những người khác trong công ty đã cấp cho họ quyền truy cập vào dữ liệu đó trước đây.
- **Sự khan hiếm:** Một chiến thuật được sử dụng để ám chỉ rằng hàng hóa hoặc dịch vụ có nguồn cung hạn chế.
- **Tính quen thuộc:** Các tác nhân đe dọa thiết lập kết nối cảm xúc giả tạo với người dùng và có thể bị lợi dụng.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- **Sự tin cậy:** Các tác nhân đe dọa thiết lập mối quan hệ tình cảm với người dùng và mối quan hệ này có thể bị lợi dụng *theo thời gian*. Họ sử dụng mối quan hệ này để phát triển lòng tin và thu thập thông tin cá nhân.
- **Khẩn cấp:** Kẻ đe dọa thuyết phục người khác phản ứng nhanh chóng và không đặt câu hỏi.

Key takeaways


In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it's so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks.

Bài học chính

Trong bài đọc này, bạn đã tìm hiểu về một số cuộc tấn công phổ biến và tác động của chúng. Bạn cũng đã tìm hiểu về kỹ thuật xã hội và lý do tại sao nó lại thành công như vậy. Mặc dù đây chỉ là phần giới thiệu ngắn gọn về các loại tấn công nhưng bạn sẽ có nhiều cơ hội trong suốt chương trình để phát triển hơn nữa sự hiểu biết của mình về cách xác định và phòng vệ trước các cuộc tấn công an ninh mạng.

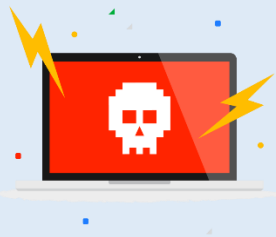


1.5. Identify: Methods of attack – Xác định: Phương thức tấn công

| | | |
|-----------------------------|------------------------------------|------------------------------|
| Malware | Virus | Worm |
| Ransomware | Spyware | Phishing |
| Spear phishing | Whaling | BEC |
| Vishing | Social engineering | Social media phishing |
| Watering hole attack | Physical social engineering | USB baiting |

| | |
|---------------------------------------|---|
| Malware – Phần mềm độc hại | <p>A software designed to harm devices or networks – Một phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng</p>  |
| Term: Virus – Thuật ngữ: Virus | <p>A malware program that modifies other computer programs by inserting its own code to damage and/or destroy data – Một chương trình phần mềm độc hại sửa đổi các</p> |


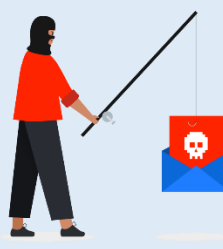

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

| | |
|--|--|
| | <p>chương trình máy tính khác bằng cách chèn mã của chính nó để làm hỏng và/hoặc phá hủy dữ liệu Example of: Malware</p>  |
| <p>Term: Worm – Thuật ngữ: Sâu</p> | <p>Malware that self-replicates, spreading across the network and infecting computers – Phần mềm độc hại tự nhân bản, lây lan trên mạng và lây nhiễm vào máy tính Example of: Malware</p>  |
| <p>Term: Ransomware – Thuật ngữ: Phần mềm tống tiền</p> | <p>A malicious attack during which threat actors encrypt an organization's data and demand payment to restore access – Một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập Example of: Malware</p>  |
| <p>Term: Spyware – Thuật ngữ: Phần mềm gián điệp</p> | <p>Malicious software installed on a user's computer without their permission, which is used to spy on and steal user data – Phần mềm độc hại được cài đặt trên máy tính của người dùng mà không có sự cho phép của</p> |

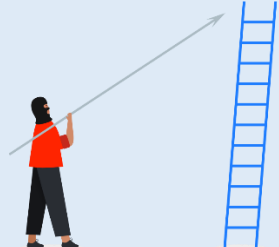

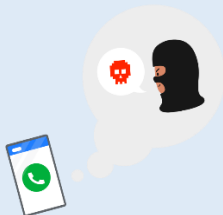
Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

| | |
|--|--|
| | <p>họ, được sử dụng để theo dõi và đánh cắp dữ liệu của người dùng</p> <p>Example of: Malware</p>  |
| <p>Term: Phishing – Thuật ngữ: Lừa đảo</p> | <p>The use of digital communications to trick people into revealing sensitive data or deploying malicious software – Việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại</p>  |
| <p>Term: Spear phishing – Thuật ngữ: Lừa đảo trực tuyến</p> | <p>A malicious email attack targeting a specific user or group of users that appears to originate from a trusted source – Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể có vẻ như đến từ một nguồn đáng tin cậy</p> <p>Example of: Phishing</p>  |
| <p>Term: Whaling – Thuật ngữ: Whaling</p> | <p>A form of spear phishing during which threat actors target executives in order to gain access to sensitive data – Một hình thức lừa đảo trực tuyến trong đó các tác</p> |


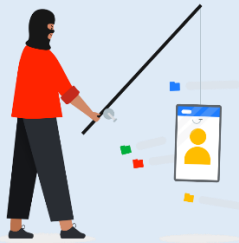

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

| | |
|---|---|
| | <p>nhân đe dọa nhắm mục tiêu vào các giám đốc điều hành để có quyền truy cập vào dữ liệu nhạy cảm</p> <p>Example of: Phishing</p>  |
| <p>Term: Business email compromise (BEC) – Thuật ngữ: Thỏa hiệp email doanh nghiệp (BEC)</p> | <p>An attack in which a threat actor impersonates a known source to obtain a financial advantage – Một cuộc tấn công trong đó kẻ đe dọa mạo danh một nguồn đã biết để đạt được lợi thế tài chính</p> <p>Example of: Phishing</p>  |
| <p>Term: Vishing – Thuật ngữ: Vishing</p> | <p>The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source – Việc khai thác liên lạc bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết</p> <p>Example of: Phishing</p>  |
| <p>Term: Social engineering – Thuật ngữ: Kỹ thuật xã hội</p> | <p>A manipulation technique that exploits human error to gain unauthorized access to</p> |

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

| | |
|---|---|
| | <p>sensitive, private, and/or valuable data – Một kỹ thuật thao túng khai thác lỗi của con người để có được quyền truy cập trái phép vào dữ liệu nhạy cảm, riêng tư và/hoặc có giá trị</p>  |
| <p>Term: Social media phishing – Thuật ngữ: Lừa đảo trên mạng xã hội</p> | <p>An attack in which a threat actor collects detailed information about their target on social media sites before initiating an attack – Một cuộc tấn công trong đó kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của chúng trên các trang truyền thông xã hội trước khi bắt đầu một cuộc tấn công</p> <p>Example of: Social engineering</p>  |
| <p>Term: Watering hole attack – Thuật ngữ: Watering hole attack</p> | <p>An attack in which a threat actor compromises a website frequently visited by a specific group of users – Một cuộc tấn công trong đó kẻ đe dọa xâm phạm một trang web thường xuyên được một nhóm người dùng cụ thể truy cập</p> <p>Example of: Social engineering</p>  |

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

| | |
|---|--|
| <p>Term: Physical social engineering – Thuật ngữ: Kỹ thuật xã hội vật lý</p> | <p>An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location – Một cuộc tấn công trong đó kẻ đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế</p> <p>Example of: Social engineering</p>  |
| <p>Term: USB baiting – Thuật ngữ: mồi USB</p> | <p>An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and unknowingly infect a network – Một cuộc tấn công trong đó kẻ đe dọa có chiến lược để lại một thanh USB chứa phần mềm độc hại để nhân viên tìm thấy và vô tình lây nhiễm vào mạng</p> <p>Example of: Social engineering</p>  |

1.6. Sean: Keep your cool during a data breach – Sean: Hãy bình tĩnh khi có sự cố vi phạm dữ liệu

Sean: Keep your cool during a data breach

Hi, my name is Sean. I'm a Technical Program Manager in Google workspace. I am a 30 year security veteran within the security space across six different industries. During your first data breach, the most important thing that you can do is keep your cool. Everyone around is going to be freaking out. If you are on the security team and you are managing the incident, you have to legitimately be the cool guy in the room. Be that person that has the pause in the conversation. Somebody might be like, do you know what's going on? I absolutely do. I think the biggest breach I've ever had

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

was a phone call. An engineer for another financial, bought a server off eBay. That server fired it up hadn't been wiped. Twenty million credit card records were on it. That triggered a whole review of we had not been controlling for how do third parties because we were now outsourcing data centers. How do third parties wipe the servers that we no longer use? The first thing you're going to do is to contain the breach. If you are still hemorrhaging data, you go through your progressions to stop hemorrhaging data. So if that means shutting down a server, shutting down a data center, shutting down comms, whatever, stopping the data loss is that is your number one priority. Your job as an incident manager or as somebody working a breach is to stop the breach and then investigate the breach. So executing your incident management by plan is the most important thing that an entry level person can keep in mind.

Xin chào, tên tôi là Sean. Tôi là Người quản lý chương trình kỹ thuật trong không gian làm việc của Google. Tôi là một cựu chiến binh an ninh 30 năm trong không gian an ninh trên sáu ngành công nghiệp khác nhau. Trong lần vi phạm dữ liệu đầu tiên của bạn, điều quan trọng nhất mà bạn có thể làm là giữ bình tĩnh của bạn. Mọi người xung quanh sẽ phát hoảng. Nếu bạn đang ở trên đội an ninh và bạn đang quản lý vụ việc, bạn phải là một chàng trai tuyệt vời trong phòng một cách hợp pháp. Hãy là người tạm dừng cuộc trò chuyện. Ai đó có thể sẽ như thế này, bạn có biết chuyện gì đang xảy ra không? Tôi hoàn toàn làm được. Tôi nghĩ vi phạm lớn nhất tôi từng có đã có một cuộc điện thoại. Một kỹ sư tài chính khác, đã mua một máy chủ từ eBay. Máy chủ đó kích hoạt nó vẫn chưa bị xóa. Hai mươi triệu hồ sơ thẻ tín dụng có trong đó. Điều đó đã kích hoạt một cuộc đánh giá toàn bộ trong số chúng tôi đã không kiểm soát đối với bên thứ ba thì sao vì chúng tôi hiện đang thuê ngoài các trung tâm dữ liệu. Làm thế nào để bên thứ ba xóa sạch các máy chủ mà chúng tôi không còn sử dụng nữa? Điều đầu tiên bạn sẽ làm là để ngăn chặn sự vi phạm. Nếu bạn vẫn đang xuất huyết dữ liệu, bạn trải qua quá trình tiến triển của mình để ngừng xuất huyết dữ liệu. Vậy nếu điều đó có nghĩa là tắt máy chủ, đóng cửa trung tâm dữ liệu, tắt liên lạc, sao cũng được, ngăn chặn việc mất dữ liệu là đó là ưu tiên số một của bạn. Công việc của bạn với tư cách là người quản lý sự cố hoặc là người đang làm việc vi phạm là phải dừng lại vi phạm và sau đó điều tra vi phạm. Vì vậy, việc thực hiện quản lý sự cố theo kế hoạch là điều quan trọng nhất đó một người ở trình độ đầu vào có thể ghi nhớ.

1.7. Test your knowledge: The history of cybersecurity – Kiểm tra kiến thức của bạn: Lịch sử an ninh mạng

2. The eight CISSP security domains – Tám miền bảo mật CISSP

2.1. Introduction to the eight CISSP security domains, Part 1 – Giới thiệu về tám miền bảo mật CISSP, Phần 1

Introduction to the eight CISSP security domains, Part 1

As the tactics of threat actors evolve, so do the roles of security professionals. Having a solid understanding of core security concepts will support your growth in this field. One way to better understand these core concepts is by organizing them into categories, called security domains.

Giới thiệu về tám miền bảo mật CISSP, Phần 1

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Khi chiến thuật của các tác nhân đe dọa phát triển thì vai trò của các chuyên gia bảo mật cũng thay đổi. Có sự hiểu biết vững chắc về các khái niệm bảo mật cốt lõi sẽ hỗ trợ sự phát triển của bạn trong lĩnh vực này. Một cách dễ hiểu rõ hơn những khái niệm cốt lõi này là tổ chức chúng thành các danh mục, được gọi là miền bảo mật.

As of 2022, CISSP has defined eight domains to organize the work of security professionals. It's important to understand that these domains are related and that gaps in one domain can result in negative consequences to an entire organization.

Tính đến năm 2022, CISSP đã xác định tám miền tổ chức công việc của các chuyên gia an ninh. Điều quan trọng là phải hiểu rằng các lĩnh vực này có liên quan với nhau và những khoảng trống trong một miền có thể dẫn đến hậu quả tiêu cực cho toàn bộ tổ chức.

It's also important to understand the domains because it may help you better understand your career goals and your role within an organization. As you learn more about the elements of each domain, the work involved in one may appeal to you more than the others. This domain may become a career path for you to explore further.

Điều quan trọng là phải hiểu tên miền vì nó có thể giúp ích bạn hiểu rõ hơn về mục tiêu nghề nghiệp và vai trò của mình trong tổ chức. Khi bạn tìm hiểu thêm về các thành phần của từng miền, công việc liên quan đến một công việc có thể hấp dẫn bạn hơn những công việc khác. Tên miền này có thể trở thành con đường sự nghiệp để bạn khám phá thêm.

CISSP defines eight domains in total, and we'll discuss all eight between this video and the next. In this video, we're going to cover the first four: security and risk management, asset security, security architecture and engineering, and communication and network security.

CISSP xác định tổng cộng tám miền và chúng ta sẽ thảo luận về tất cả tám điều trong video này và video tiếp theo. Trong video này, chúng ta sẽ đề cập đến bốn điều đầu tiên: an ninh và quản lý rủi ro, bảo mật tài sản, kiến trúc và kỹ thuật an ninh, an ninh mạng và truyền thông.

Let's start with the first domain, security and risk management. Security and risk management focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. For example, security analysts may need to update company policies related to private health information if a change is made to a federal compliance regulation such as the Health Insurance Portability and Accountability Act, also known as HIPAA.

Hãy bắt đầu với lĩnh vực đầu tiên, bảo mật và quản lý rủi ro. Quản lý rủi ro và bảo mật tập trung vào việc xác định các mục tiêu và mục đích bảo mật, giảm thiểu rủi ro, tuân thủ, kinh doanh liên tục và pháp luật. Ví dụ: nhà phân tích bảo mật có thể cần cập nhật chính sách của công ty liên quan đến thông tin sức khỏe cá nhân nếu một thay đổi được thực hiện đối với quy định tuân thủ của liên bang như Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế, còn được gọi là HIPAA.

The second domain is asset security. This domain focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. When working with this domain, security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Lĩnh vực thứ hai là bảo mật tài sản. Miền này tập trung vào việc bảo mật tài sản vật lý và kỹ thuật số. Nó cũng liên quan đến việc lưu trữ, bảo trì, duy trì và sự phá hủy dữ liệu. Khi làm việc với miền này, các nhà phân tích bảo mật có thể được giao nhiệm vụ đảm bảo rằng thiết bị cũ được xử lý đúng cách và bị phá hủy, bao gồm bất kỳ loại thông tin bí mật nào.

The third domain is security architecture and engineering. This domain focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. As a security analyst, you may be tasked with configuring a firewall. A firewall is a device used to monitor and filter incoming and outgoing computer network traffic. Setting up a firewall correctly helps prevent attacks that could affect productivity.

Lĩnh vực thứ ba là kiến trúc và kỹ thuật bảo mật. Miền này tập trung vào việc tối ưu hóa bảo mật dữ liệu bằng cách đảm bảo các công cụ hiệu quả, các hệ thống và quy trình đang được thực hiện. Là một nhà phân tích bảo mật, bạn có thể được giao nhiệm vụ cấu hình tường lửa. Tường lửa là một thiết bị được sử dụng để giám sát và lọc các thông tin đến và lưu lượng mạng máy tính đi. Thiết lập tường lửa đúng cách giúp ngăn chặn các cuộc tấn công có thể ảnh hưởng đến năng suất.

The fourth security domain is communication and network security. This domain focuses on managing and securing physical networks and wireless communications. As a security analyst, you may be asked to analyze user behavior within your organization.

Lĩnh vực bảo mật thứ tư là an ninh mạng và truyền thông. Miền này tập trung vào việc quản lý và bảo mật mạng vật lý và giao tiếp không dây. Là một nhà phân tích chứng khoán, bạn có thể được yêu cầu phân tích hành vi của người dùng trong tổ chức của mình.

Imagine discovering that users are connecting to unsecured wireless hotspots. This could leave the organization and its employees vulnerable to attacks. To ensure communications are secure, you would create a network policy to prevent and mitigate exposure.

Hãy tưởng tượng phát hiện ra rằng người dùng đang kết nối với các điểm truy cập không dây không an toàn. Điều này có thể khiến tổ chức và nhân viên của tổ chức dễ bị tấn công. Để đảm bảo thông tin liên lạc được an toàn, bạn sẽ tạo một chính sách mạng để ngăn ngừa và giảm thiểu phơi nhiễm.

Maintaining an organization's security is a team effort, and there are many moving parts. As an entry-level analyst, you will continue to develop your skills by learning how to mitigate risks to keep people and data safe.

Duy trì an ninh của một tổ chức là nỗ lực của nhóm và có nhiều bộ phận chuyển động. Là một nhà phân tích cấp đầu vào, bạn sẽ tiếp tục phát triển kỹ năng của mình bằng cách học cách giảm thiểu rủi ro để giữ an toàn cho con người và dữ liệu.

You don't need to be an expert in all domains. But, having a basic understanding of them will aid you in your journey as a security professional.

Bạn không cần phải là chuyên gia trong mọi lĩnh vực. Tuy nhiên, có sự hiểu biết cơ bản trong số họ sẽ hỗ trợ bạn trong hành trình trở thành một chuyên gia bảo mật.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

You're doing great! We have just introduced the first four security domains, and in the next video, we'll discuss four more! See you soon!

Bạn đang làm rất tốt! Chúng tôi vừa giới thiệu bốn biện pháp bảo mật đầu tiên tên miền và trong video tiếp theo, chúng ta sẽ thảo luận thêm về bốn tên miền nữa! Hẹn sớm gặp lại!

2.2. Introduction to the eight CISSP security domains, Part 2 – Giới thiệu về tám miền bảo mật CISSP, Phần 2

Introduction to the eight CISSP security domains, Part 2

Welcome back. In the last video, we introduced you to the first four security domains. In this video, we'll introduce you to the next four security domains: identity and access management, security assessment and testing, security operations, and software development security.

Giới thiệu về tám miền bảo mật CISSP, Phần 2

Chào mừng trở lại. Trong video cuối cùng, chúng tôi đã giới thiệu cho bạn bốn miền bảo mật đầu tiên. Trong video này chúng tôi sẽ giới thiệu bạn đến bốn miền bảo mật tiếp theo: quản lý danh tính và quyền truy cập, đánh giá và kiểm tra an ninh, hoạt động bảo mật và bảo mật phát triển phần mềm.

Familiarizing yourself with these domains will allow you to navigate the complex world of security. The domains outline and organize how a team of security professionals work together. Depending on the organization, analyst roles may sit at the intersection of multiple domains or focus on one specific domain. Knowing where a particular role fits within the security landscape will help you prepare for job interviews and work as part of a full security team.

Làm quen với những miền này sẽ cho phép bạn điều hướng thế giới bảo mật phức tạp. Các miền phác thảo và tổ chức cách một nhóm chuyên gia bảo mật làm việc cùng nhau. Tùy theo tổ chức, vai trò của nhà phân tích có thể nằm ở giao điểm của nhiều tên miền hoặc tập trung vào một tên miền cụ thể. Biết vai trò cụ thể ở đâu phù hợp với bối cảnh an ninh sẽ giúp bạn chuẩn bị cho cuộc phỏng vấn xin việc và làm việc như một phần của đội bảo mật đầy đủ.

Let's move into the fifth domain: identity and access management. Identity and access management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications. Validating the identities of employees and documenting access roles are essential to maintaining the organization's physical and digital security. For example, as a security analyst, you may be tasked with setting up employees' keycard access to buildings.

Hãy chuyển sang miền thứ năm: quản lý danh tính và quyền truy cập. Quản lý danh tính và quyền truy cập tập trung vào việc giữ an toàn cho dữ liệu, bằng cách đảm bảo người dùng tuân theo các chính sách đã thiết lập để kiểm soát và quản lý tài sản vật chất, như không gian văn phòng, và các tài sản logic, chẳng hạn như mạng và ứng dụng. Xác thực danh tính của nhân viên và ghi lại vai trò truy cập là cần thiết để duy trì an ninh vật lý và kỹ thuật số của tổ chức. Ví dụ, với tư cách là một nhà phân tích chứng khoán, bạn có thể được giao nhiệm vụ thiết lập thẻ khóa của nhân viên vào các tòa nhà.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

The sixth domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access. For example, access to payroll information is often limited to certain employees, so analysts may be asked to regularly audit permissions to ensure that no unauthorized person can view employee salaries.

Lĩnh vực thứ sáu là đánh giá và kiểm tra bảo mật. Miền này tập trung vào tiến hành kiểm tra kiểm soát an ninh, thu thập, phân tích dữ liệu và tiến hành kiểm tra an ninh để giám sát rủi ro, mối đe dọa và điểm yếu. Các nhà phân tích chứng khoán có thể tiến hành kiểm tra thường xuyên các quyền của người dùng, để đảm bảo rằng người dùng có cấp độ truy cập chính xác. Ví dụ, truy cập vào Thông tin về bảng lương thường xuyên giới hạn ở một số nhân viên nhất định, vì vậy các nhà phân tích có thể được yêu cầu thường xuyên kiểm tra quyền để đảm bảo rằng không có người trái phép có thể xem lương nhân viên.

The seventh domain is security operations. This domain focuses on conducting investigations and implementing preventative measures. Imagine that you, as a security analyst, receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat.

Lĩnh vực thứ bảy là hoạt động an ninh. Miền này tập trung vào việc tiến hành điều tra và thực hiện các biện pháp ngăn chặn. Hãy tưởng tượng rằng bạn, với tư cách là một nhà phân tích chứng khoán, nhận được cảnh báo rằng một thiết bị không xác định đã được kết nối với mạng nội bộ của bạn. Bạn sẽ cần phải tuân theo các chính sách của tổ chức và các thủ tục để nhanh chóng ngăn chặn mối đe dọa tiềm tàng.

The final, eighth domain is software development security. This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services. A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle. If, for example, one of your partner teams is creating a new mobile app, then you may be asked to advise on the password policies or ensure that any user data is properly secured and managed.

Lĩnh vực cuối cùng thứ tám là bảo mật phát triển phần mềm. Miền này tập trung vào việc sử dụng các phương pháp mã hóa an toàn, đó là một bộ hướng dẫn được đề xuất được sử dụng để tạo ra các ứng dụng và dịch vụ an toàn. Một nhà phân tích bảo mật có thể làm việc với nhóm phát triển phần mềm để đảm bảo thực hành bảo mật được kết hợp vào vòng đời phát triển phần mềm. Nếu, ví dụ, một trong các nhóm đối tác của bạn đang tạo một ứng dụng di động mới, sau đó bạn có thể được yêu cầu tư vấn về chính sách mật khẩu hoặc đảm bảo rằng mọi dữ liệu người dùng đều được bảo mật và quản lý đúng cách.

That ends our introduction to CISSP's eight security domains. Challenge yourself to better understand each of these domains and how they affect the overall security of an organization. While they may still be a bit unclear to you this early in the program, these domains will be discussed in greater detail in the next course. See you there!

Điều đó kết thúc phần giới thiệu của chúng tôi về Tám miền bảo mật của CISSP. Thử thách bản thân để hiểu rõ hơn về từng điều kiện tên miền này và cách chúng ảnh hưởng an ninh tổng thể của một tổ chức. Mặc dù chúng có thể vẫn còn một chút bạn chưa

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

rõ điều này ngay từ đầu chương trình, những lĩnh vực này sẽ được thảo luận trong chi tiết hơn trong khóa học tiếp theo. Hẹn gặp bạn ở đó!

2.3. Determine the type of attack – Xác định kiểu tấn công

Previously, you learned about the eight Certified Information Systems Security Professional (CISSP) security domains. The domains can help you better understand how a security analyst's job duties can be organized into categories. Additionally, the domains can help establish an understanding of how to manage risk. In this reading, you will learn about additional methods of attack. You'll also be able to recognize the types of risk these attacks present.

Trước đây, bạn đã tìm hiểu về tám miền bảo mật Chuyên gia Bảo mật Hệ thống Thông tin được Chứng nhận (CISSP). Các miền có thể giúp bạn hiểu rõ hơn về cách sắp xếp nhiệm vụ công việc của nhà phân tích bảo mật thành các danh mục. Ngoài ra, các lĩnh vực này có thể giúp thiết lập sự hiểu biết về cách quản lý rủi ro. Trong bài đọc này, bạn sẽ tìm hiểu về các phương pháp tấn công bổ sung. Bạn cũng sẽ có thể nhận ra các loại rủi ro mà các cuộc tấn công này mang lại.



Attack types

Các kiểu tấn công

Password attack

A **password attack** is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Tấn công mật khẩu

Tấn công bằng mật khẩu là một nỗ lực nhằm truy cập các thiết bị, hệ thống, mạng hoặc dữ liệu được bảo mật bằng mật khẩu. Một số hình thức tấn công mật khẩu mà bạn sẽ tìm hiểu sau trong chương trình chứng chỉ là:

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- Lực lượng vũ phu
- Bàn cầu vòng

Các cuộc tấn công mật khẩu thuộc lĩnh vực an ninh mạng và truyền thông.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Some forms of social engineering attacks that you will continue to learn about throughout the program are:

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB (Universal Serial Bus) baiting
- Physical social engineering

Social engineering attacks are related to the security and risk management domain.

Tấn công kỹ thuật xã hội

Kỹ thuật xã hội là một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc vật có giá trị. Một số hình thức tấn công kỹ nghệ xã hội mà bạn sẽ tiếp tục tìm hiểu trong suốt chương trình là:

- Lừa đảo
- đập phá
- Vishing
- Lừa đảo trực tuyến
- Đánh bắt cá voi
- Lừa đảo trên mạng xã hội
- Thỏa hiệp email doanh nghiệp (BEC)

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- Tấn công hồ tưới nước
- Bẫy USB (Universal Serial Bus)
- Kỹ thuật xã hội vật lý

Các cuộc tấn công kỹ thuật xã hội có liên quan đến lĩnh vực quản lý rủi ro và bảo mật.

Physical attack

A **physical attack** is a security incident that affects not only digital but also physical environments where the incident is deployed. Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

Physical attacks fall under the asset security domain.

Tấn công vật lý

Tấn công vật lý là một sự cố bảo mật không chỉ ảnh hưởng đến môi trường kỹ thuật số mà còn cả môi trường vật lý nơi sự cố được triển khai. Một số hình thức tấn công vật lý là:

- Cáp USB độc hại
- Ổ đĩa flash độc hại
- Nhân bản và lướt thẻ

Các cuộc tấn công vật lý thuộc lĩnh vực bảo mật tài sản.

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates [artificial intelligence and machine learning](#) technology to conduct attacks more efficiently. Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

Trí tuệ nhân tạo đối nghịch

Trí tuệ nhân tạo đối nghịch là một kỹ thuật thao túng [trí tuệ nhân tạo và học máy](#) công nghệ để tiến hành các cuộc tấn công hiệu quả hơn. Trí tuệ nhân tạo đối nghịch thuộc cả lĩnh vực an ninh mạng và truyền thông cũng như lĩnh vực quản lý danh tính và quyền truy cập.

Supply-chain attack

A **supply-chain attack** targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them. Supply-chain attacks can fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.

Tấn công chuỗi cung ứng

Cuộc **tấn công chuỗi cung ứng** nhắm vào các hệ thống, ứng dụng, phần cứng và/hoặc phần mềm để xác định lỗ hổng nơi phần mềm độc hại có thể được triển khai. Vì mọi mặt hàng được bán đều trải qua quy trình có sự tham gia của bên thứ ba, điều này có nghĩa là vi phạm an ninh có thể xảy ra ở bất kỳ điểm nào trong chuỗi cung ứng. Những cuộc tấn công này rất tốn kém vì chúng có thể ảnh hưởng đến nhiều tổ chức và cá nhân làm việc cho chúng. Các cuộc tấn công chuỗi cung ứng có thể thuộc một số lĩnh vực, bao gồm nhưng không giới hạn ở các lĩnh vực bảo mật và quản lý rủi ro, kiến trúc và kỹ thuật bảo mật cũng như các lĩnh vực hoạt động bảo mật.

Cryptographic attack

A **cryptographic attack** affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

Cryptographic attacks fall under the communication and network security domain.

Tấn công mật mã

Một **cuộc tấn công bằng mật mã** ảnh hưởng đến các hình thức liên lạc an toàn giữa người gửi và người nhận dự định. Một số hình thức tấn công mật mã là:

- Sinh nhật
- Va chạm
- Hạ cấp

Các cuộc tấn công mật mã thuộc lĩnh vực bảo mật mạng và truyền thông.

Key takeaways

The eight CISSP security domains can help an organization and its security team fortify against and prepare for a data breach. Data breaches range from simple to complex and fall under one or more domains. Note that the methods of attack discussed are only a few of many. These and other types of attacks will be discussed throughout the certificate program.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Bài học chính

Tám miền bảo mật CISSP có thể giúp tổ chức và nhóm bảo mật của tổ chức củng cố và chuẩn bị cho việc vi phạm dữ liệu. Vi phạm dữ liệu có phạm vi từ đơn giản đến phức tạp và thuộc một hoặc nhiều miền. Lưu ý rằng các phương pháp tấn công được thảo luận chỉ là một vài trong số rất nhiều phương pháp tấn công khác. Những kiểu tấn công này và các kiểu tấn công khác sẽ được thảo luận trong suốt chương trình chứng chỉ.

Resources for more information

To view detailed information and definitions of terms covered in this reading, visit the [National Institute of Standards and Technology \(NIST\) glossary](#).

Pro tip: If you cannot find a term in the NIST glossary, enter the appropriate search term (e.g., “cybersecurity birthday attack”) into your preferred search engine to locate the definition in another reliable source such as a .edu or .gov site.

Tài nguyên để biết thêm thông tin

Để xem thông tin chi tiết và định nghĩa của các thuật ngữ được đề cập trong bài đọc này, hãy truy cập [Thuật ngữ của Viện Tiêu chuẩn và Công nghệ Quốc gia \(NIST\)](#).

Mẹo chuyên nghiệp: Nếu bạn không thể tìm thấy thuật ngữ trong bảng thuật ngữ NIST, hãy nhập thuật ngữ tìm kiếm thích hợp (ví dụ: “cuộc tấn công sinh nhật an ninh mạng”) vào công cụ tìm kiếm ưa thích của bạn để tìm định nghĩa trong một nguồn đáng tin cậy khác, chẳng hạn như trang web .edu hoặc .gov .

2.4. Understand attackers – Hiểu kẻ tấn công

Previously, you were introduced to the concept of threat actors. As a reminder, a **threat actor** is any person or group who presents a security risk. In this reading, you’ll learn about different types of threat actors. You will also learn about their motivations, intentions, and how they’ve influenced the security industry.

Trước đây, bạn đã được giới thiệu khái niệm về các tác nhân đe dọa. Xin nhắc lại, **tác nhân đe dọa** là bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật. Trong bài đọc này, bạn sẽ tìm hiểu về các loại tác nhân đe dọa khác nhau. Bạn cũng sẽ tìm hiểu về động cơ, ý định của họ và cách họ ảnh hưởng đến ngành bảo mật.

Threat actor types

Các loại tác nhân đe dọa

Advanced persistent threats

Advanced persistent threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

- Damaging critical infrastructure, such as the power grid and natural resources

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

- Gaining access to intellectual property, such as trade secrets or patents

Các mối đe dọa liên tục nâng cao

Các mối đe dọa liên tục nâng cao (APT) có chuyên môn đáng kể khi truy cập vào mạng của tổ chức mà không được phép. APT có xu hướng nghiên cứu trước các mục tiêu của chúng (ví dụ: các tập đoàn lớn hoặc tổ chức chính phủ) và có thể không bị phát hiện trong một thời gian dài. Ý định và động cơ của họ có thể bao gồm:

- Làm hư hại cơ sở hạ tầng quan trọng, như lưới điện và tài nguyên thiên nhiên
- Đạt được quyền truy cập vào tài sản trí tuệ, chẳng hạn như bí mật thương mại hoặc bằng sáng chế

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

- Sabotage
- Corruption
- Espionage
- Unauthorized data access or leaks

Mối đe dọa nội bộ

Các mối đe dọa nội bộ lạm dụng quyền truy cập được ủy quyền của họ để lấy dữ liệu có thể gây hại cho tổ chức. Ý định và động cơ của họ có thể bao gồm:

- Sự phá hoại
- tham nhũng
- gián điệp
- Truy cập hoặc rò rỉ dữ liệu trái phép

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

- Demonstrations
- Propaganda
- Social change campaigns
- Fame

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Những kẻ tấn công

Những kẻ tấn công là những kẻ đe dọa được thúc đẩy bởi một chương trình nghị sự chính trị. Họ lạm dụng công nghệ kỹ thuật số để đạt được mục tiêu của mình, có thể bao gồm:

- Biểu tình
- Tuyên truyền
- Chiến dịch thay đổi xã hội
- Danh tiếng

Hacker types

A **hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

- Authorized hackers are also called ethical hackers. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.
- Semi-authorized hackers are considered researchers. They search for vulnerabilities but don't take advantage of the vulnerabilities they find.
- Unauthorized hackers are also called unethical hackers. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Note: There are multiple hacker types that fall into one or more of these three categories.

New and unskilled threat actors have various goals, including:

- To learn and enhance their hacking skills
- To seek revenge
- To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay.

There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Các loại tin tặc

Hacker là bất kỳ người nào sử dụng máy tính để truy cập **vào** hệ thống máy tính, mạng hoặc dữ liệu. Họ có thể là người mới bắt đầu hoặc chuyên gia công nghệ tiên tiến, những người sử dụng kỹ năng của mình vì nhiều lý do. Có ba loại tin tặc chính:

- Tin tặc được ủy quyền còn được gọi là tin tặc có đạo đức. Họ tuân theo quy tắc đạo đức và tuân thủ pháp luật để tiến hành đánh giá rủi ro tổ chức. Họ được thúc đẩy để bảo vệ mọi người và tổ chức khỏi các tác nhân đe dọa độc hại.
- Tin tặc bán ủy quyền được coi là nhà nghiên cứu. Họ tìm kiếm các lỗ hổng nhưng không tận dụng được các lỗ hổng mà họ tìm thấy.
- Hacker trái phép còn được gọi là hacker phi đạo đức. Họ là những kẻ đe dọa độc hại không tuân theo hoặc tôn trọng luật pháp. Mục tiêu của họ là thu thập và bán dữ liệu bí mật để thu lợi tài chính.



Lưu ý: Có nhiều loại hacker thuộc một hoặc nhiều loại trong số ba loại này.

Những kẻ đe dọa mới và không có kỹ năng có nhiều mục tiêu khác nhau, bao gồm:

- Để học hỏi và nâng cao kỹ năng hack của họ
- Để tìm cách trả thù
- Để khai thác các điểm yếu về bảo mật bằng cách sử dụng phần mềm độc hại, tập lệnh lập trình hiện có và các chiến thuật khác

Các loại tin tặc khác không bị thúc đẩy bởi bất kỳ mục đích cụ thể nào ngoài việc hoàn thành công việc mà họ đã ký hợp đồng. Những loại tin tặc này có thể được coi là tin tặc phi đạo đức hoặc có đạo đức. Họ được biết là làm cả những công việc bất hợp pháp và hợp pháp để được trả lương.

Cũng có những hacker tự coi mình là người cảnh giác. Mục tiêu chính của họ là bảo vệ thế giới khỏi những tin tặc phi đạo đức.

Key takeaways

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Threat actors are defined by their malicious intent and hackers are defined by their technical skills and motivations. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.

Bài học chính

Các tác nhân đe dọa được xác định bởi mục đích xấu của chúng và tin tặc được xác định bởi các kỹ năng và động cơ kỹ thuật của chúng. Hiểu được động cơ và ý định của họ sẽ giúp bạn chuẩn bị tốt hơn để bảo vệ tổ chức của mình và những người mà tổ chức đó phục vụ khỏi các cuộc tấn công độc hại do một số cá nhân và nhóm này thực hiện.

Resources for more information

To learn more about how security teams work to keep organizations and people safe, explore the [Hacking Google](#) series of videos.

Tài nguyên để biết thêm thông tin

Để tìm hiểu thêm về cách các nhóm bảo mật làm việc để giữ an toàn cho tổ chức và mọi người, hãy khám phá [Hack Google](#) loạt video.

2.5. Test your knowledge: The eight CISSP security domains – Kiểm tra kiến thức của bạn: Tám miền bảo mật CISSP

3. Review: The evolution of cybersecurity – Đánh giá: Sự phát triển của an ninh mạng

3.1. Wrap-up – Gợi lại

Wrap-up

This concludes our brief introduction to some of the most influential security attacks throughout history and CISSP's eight security domains. Let's review what we've discussed.

Gợi lại

Điều này kết thúc phần giới thiệu ngắn gọn của chúng tôi về một số người có ảnh hưởng nhất các cuộc tấn công bảo mật trong suốt lịch sử và tám lĩnh vực bảo mật của CISSP. Hãy xem lại những gì chúng ta đã thảo luận.

First, we covered viruses, including the Brain virus and the Morris worm, and discussed how these early forms of malware shaped the security industry. We also discussed how many attacks today are variants of these early examples. Understanding previous attacks is critical for security professionals who are working to protect organizations and people from possible future variants.

Đầu tiên, chúng tôi đề cập đến các loại vi-rút, bao gồm vi-rút Brain và sâu Morris, và thảo luận về cách những dạng phần mềm độc hại ban đầu này đã định hình ngành bảo mật như thế nào. Chúng tôi cũng thảo luận về số lượng cuộc tấn công ngày nay là biến thể của những ví dụ ban đầu này. Hiểu các cuộc tấn công trước đó là rất quan trọng đối

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

với các chuyên gia bảo mật, những người đang làm việc để bảo vệ các tổ chức và con người khỏi các biến thể có thể xảy ra trong tương lai.

We also discussed social engineering and threat actor motives by learning about the LoveLetter attack and the Equifax data breach. These incidents showed the widespread impacts and associated costs of more recent security breaches in the digital age.

Chúng tôi cũng thảo luận về kỹ thuật xã hội và động cơ của tác nhân đe dọa bằng cách tìm hiểu về cuộc tấn công LoveLetter và vụ vi phạm dữ liệu Equifax. Những sự cố này cho thấy tác động lan rộng và chi phí liên quan đến các vi phạm an ninh gần đây hơn trong thời đại kỹ thuật số.

Finally, we introduced CISSP's eight security domains and how they can be used to categorize different areas of focus within the security profession.

Cuối cùng, chúng tôi đã giới thiệu tám miền bảo mật của CISSP và cách chúng có thể được sử dụng để phân loại các lĩnh vực trọng tâm khác nhau trong ngành bảo mật.

I hope you're feeling confident about your foundational security knowledge! Learning the history of security can allow you to better understand the current industry. CISSP's eight security domains provide a way to organize the work of security professionals.

Tôi hy vọng bạn cảm thấy tự tin về kiến thức bảo mật cơ bản của mình! Tìm hiểu lịch sử bảo mật có thể cho phép bạn hiểu rõ hơn về hiện tại ngành công nghiệp. Tám miền bảo mật của CISSP cung cấp một cách để tổ chức công việc của các chuyên gia an ninh.

Remember, every security professional is essential. Your unique point of view, professional background, and knowledge are valuable. So, the diversity you bring to the field will further improve the security industry as you work to keep organizations and people safe.

Hãy nhớ rằng, mọi chuyên gia bảo mật đều cần thiết. Quan điểm độc đáo, nền tảng chuyên môn và kiến thức của bạn rất có giá trị. Vì vậy, sự đa dạng mà bạn mang đến cho lĩnh vực này sẽ tiếp tục cải thiện ngành bảo mật khi bạn nỗ lực giữ an toàn cho các tổ chức và mọi người.

3.2. Glossary terms from module 2 – Thuật ngữ trong học phần 2

Glossary terms from module 2

Terms and definitions from Course 1, Module 2

Thuật ngữ trong học phần 2

Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 2

Adversarial artificial intelligence (AI): A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

Trí tuệ nhân tạo đối nghịch (AI): Một kỹ thuật vận dụng trí tuệ nhân tạo (AI) và công nghệ máy học (ML) để tiến hành các cuộc tấn công hiệu quả hơn

Business Email Compromise (BEC): A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Thỏa hiệp email doanh nghiệp (BEC): Một loại tấn công lừa đảo trong đó tác nhân đe dọa mạo danh một nguồn đã biết để đạt được lợi ích tài chính

CISSP: Certified Information Systems Security Professional is a globally recognized and highly sought-after information security certification, awarded by the International Information Systems Security Certification Consortium

CISSP: Chuyên gia bảo mật hệ thống thông tin được chứng nhận là chứng chỉ bảo mật thông tin được công nhận trên toàn cầu và được săn đón nhiều, do Hiệp hội chứng nhận bảo mật hệ thống thông tin quốc tế trao tặng

Computer virus: Malicious code written to interfere with computer operations and cause damage to data and software

Virus máy tính: Mã độc được viết nhằm can thiệp vào hoạt động của máy tính và gây hư hỏng dữ liệu, phần mềm

Cryptographic attack: An attack that affects secure forms of communication between a sender and intended recipient

Tấn công mật mã: Một cuộc tấn công ảnh hưởng đến các hình thức liên lạc an toàn giữa người gửi và người nhận dự định

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

Hacker: Bất kỳ người nào sử dụng máy tính để truy cập vào hệ thống máy tính, mạng hoặc dữ liệu

Malware: Software designed to harm devices or networks

Phần mềm độc hại: Phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng

Password attack: An attempt to access password secured devices, systems, networks, or data

Tấn công mật khẩu: Nỗ lực truy cập các thiết bị, hệ thống, mạng hoặc dữ liệu được bảo mật bằng mật khẩu

Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software

Lừa đảo: Việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại

Physical attack: A security incident that affects not only digital but also physical environments where the incident is deployed

Tấn công vật lý: Một sự cố bảo mật không chỉ ảnh hưởng đến môi trường kỹ thuật số mà còn cả môi trường vật lý nơi sự cố được triển khai

Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

Kỹ thuật xã hội vật lý: Một cuộc tấn công trong đó tác nhân đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Module 2: The evolution of cybersecurity

Phần 2: Sự phát triển của an ninh mạng

Kỹ thuật xã hội: Một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc tài sản có giá trị

Social media phishing: A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

Lừa đảo trên mạng xã hội: Một kiểu tấn công trong đó kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của họ trên các trang mạng xã hội trước khi bắt đầu cuộc tấn công

Spear phishing: A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

Phishing lừa đảo: Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể, dường như bắt nguồn từ một nguồn đáng tin cậy

Supply-chain attack: An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

Tấn công chuỗi cung ứng: Một cuộc tấn công nhắm vào các hệ thống, ứng dụng, phần cứng và/hoặc phần mềm để xác định lỗ hổng nơi phần mềm độc hại có thể được triển khai

USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

USB baiting: Một cuộc tấn công trong đó kẻ đe dọa có chiến lược để lại một thẻ USB chứa phần mềm độc hại để nhân viên tìm và cài đặt nhằm vô tình lây nhiễm vào mạng

Virus: refer to “computer virus”

Virus: tham khảo “virus máy tính”

Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

Vishing: Việc khai thác giao tiếp bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết

Watering hole attack: A type of attack when a threat actor compromises a website frequently visited by a specific group of users

Tấn công Watering Hole : Một kiểu tấn công khi tác nhân đe dọa xâm phạm một trang web thường được một nhóm người dùng cụ thể truy cập

3.3. Module 2 challenge – Thử thách module 2

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Module 3: Protect against threats, risks, and vulnerabilities – Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

You will learn about security frameworks and controls, which are used to mitigate organizational risk. You'll cover principles of the CIA triad and various National Institute of Standards and Technology (NIST) frameworks. In addition, you'll explore security ethics.

Bạn sẽ tìm hiểu về các khuôn khổ và biện pháp kiểm soát bảo mật được sử dụng để giảm thiểu rủi ro cho tổ chức. Bạn sẽ đề cập đến các nguyên tắc của bộ ba CIA và các khuôn khổ khác nhau của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Ngoài ra, bạn sẽ khám phá đạo đức bảo mật.

Learning Objectives

- Define security frameworks and controls
- Define the CIA triad and NIST CSF
- Discuss how the CIA triad and NIST CSF are used to develop procedures and processes to address security threats, risks, and vulnerabilities
- Explain security ethics

Mục tiêu học tập

- Xác định khung bảo mật và kiểm soát
- Xác định bộ ba CIA và NIST CSF
- Thảo luận cách sử dụng bộ ba CIA và NIST CSF để phát triển các thủ tục và quy trình nhằm giải quyết các mối đe dọa, rủi ro và lỗ hổng bảo mật
- Giải thích đạo đức bảo mật

1. Frameworks and controls – Frameworks và kiểm soát

1.1. Welcome to module 3 – Chào mừng đến với module 3

Welcome to module 3

Hi there, glad to have you back! You're halfway done with the first course, so you're making great progress.

Chào mừng đến với mô-đun 3

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Xin chào, rất vui vì bạn đã trở lại! Bạn đã hoàn thành được một nửa khóa học đầu tiên, vì vậy bạn đang tiến bộ rất nhiều.

In this section, we'll discuss how organizations protect themselves from threats, risks, and vulnerabilities by covering key principles such as: frameworks, controls, and ethics. To help you better understand how this relates to the role of a security analyst, we'll use an analogy.

Trong phần này, chúng ta sẽ thảo luận về cách các tổ chức tự bảo vệ mình khỏi các mối đe dọa, rủi ro và các lỗ hổng bằng cách đề cập đến các nguyên tắc chính như: khuôn khổ, biện pháp kiểm soát và đạo đức. Để giúp bạn hiểu rõ hơn điều này liên quan như thế nào đến vai trò của nhà phân tích bảo mật, chúng ta sẽ sử dụng một sự tương tự.

Imagine you want to plant a garden. You research, plan, prepare, and purchase materials while considering all the things that could potentially present a risk to your garden. You establish a plan to pull weeds, spray for bugs, and water your plants regularly to prevent issues or incidents. But as the days go by, unexpected problems arise. The weather has been unpredictable and pests have been aggressively trying to infiltrate your garden.

Hãy tưởng tượng bạn muốn trồng một khu vườn. Bạn nghiên cứu, lập kế hoạch, chuẩn bị, và mua vật liệu trong khi xem xét tất cả những thứ có thể có khả năng gây nguy hiểm cho khu vườn của bạn. Bạn lập kế hoạch nhổ cỏ, phun thuốc trừ sâu, và tưới nước cho cây thường xuyên để ngăn ngừa các vấn đề hoặc sự cố. Nhưng ngày tháng trôi qua, những vấn đề bất ngờ nảy sinh. Thời tiết diễn biến khó lường và sâu bệnh đang tích cực cố gắng xâm nhập vào khu vườn của bạn.

You start implementing better ways to safeguard your garden by installing a surveillance camera, building a fence, and covering your plants with a canopy to keep your garden healthy and growing. Now that you have a better idea about the threats to your garden and how to keep your plants safe, you establish better policies and procedures to continuously monitor and safeguard your garden.

Bạn bắt đầu thực hiện những cách tốt hơn để bảo vệ khu vườn của mình bằng cách lắp đặt camera giám sát, xây hàng rào và che phủ cây của bạn bằng một tán cây để giữ cho khu vườn của bạn khỏe mạnh và phát triển. Bây giờ bạn đã có ý tưởng tốt hơn về các mối đe dọa đối với khu vườn của bạn và làm thế nào để giữ cho cây trồng của bạn được an toàn, bạn thiết lập các chính sách và thủ tục tốt hơn để liên tục theo dõi và bảo vệ khu vườn của bạn.

In this way, security resembles a garden. It's an evolving industry that will challenge you to make continuous improvements to policies and procedures that help protect your organization and the people it serves.

Theo cách này, an ninh giống như một khu vườn. Đó là một ngành đang phát triển sẽ thách thức bạn thực hiện liên tục cải tiến các chính sách và thủ tục giúp bảo vệ tổ chức của bạn và những người mà nó phục vụ.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

To that end, we'll introduce security frameworks and controls and explain why they're important. We'll also cover core components and specific examples of frameworks and controls, including the Confidentiality, Integrity, and Availability Triad, or CIA Triad. We'll end with the discussion about the ethics of security and share a few notable ethical concerns in the security field.

Để đạt được mục đích đó, chúng tôi sẽ giới thiệu các khung bảo mật và kiểm soát và giải thích tại sao chúng quan trọng. Chúng tôi cũng sẽ đề cập đến các thành phần cốt lõi và các ví dụ cụ thể về khung và kiểm soát, bao gồm tính bảo mật, tính toàn vẹn và Bộ ba sẵn có hoặc Bộ ba CIA. Chúng ta sẽ kết thúc bằng cuộc thảo luận về đạo đức của an ninh và chia sẻ một số mối quan tâm đạo đức đáng chú ý trong lĩnh vực bảo mật.

Evolving security practices may seem a little abstract, but many of us use them every day. For example, I use security keys, which are a type of security control, as a second form of authentication to access my accounts. The keys ensure that only I can access my accounts, even if a password has been compromised. By improving confidentiality, they also assure me that the integrity of my accounts is intact.

Các biện pháp bảo mật ngày càng phát triển có vẻ hơi trừu tượng, nhưng nhiều người trong chúng ta sử dụng chúng hàng ngày. Ví dụ: tôi sử dụng khóa bảo mật, một loại kiểm soát bảo mật, như một hình thức xác thực thứ hai để truy cập vào tài khoản của tôi. Các khóa đảm bảo rằng chỉ tôi mới có thể truy cập vào tài khoản của mình, ngay cả khi mật khẩu đã bị xâm phạm. Bằng cách cải thiện tính bảo mật, họ cũng đảm bảo với tôi rằng tính toàn vẹn của tài khoản của tôi vẫn nguyên vẹn.

Having processes and procedures in place to organize security efforts and make informed decisions is important for any organization. I'm so excited to get started, and I hope you are too!

Có sẵn các quy trình và thủ tục để tổ chức các nỗ lực bảo mật và đưa ra quyết định sáng suốt là quan trọng đối với bất kỳ tổ chức nào. Tôi rất háo hức được bắt đầu và tôi hy vọng bạn cũng vậy!

1.2. Introduction to security frameworks and controls – Giới thiệu về khung bảo mật và kiểm soát

Introduction to security frameworks and controls

Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start?

Giới thiệu về khung bảo mật và kiểm soát

Hãy tưởng tượng bạn đang làm việc như một nhà phân tích chứng khoán và nhận được nhiều cảnh báo về hoạt động đáng ngờ trên mạng. Bạn nhận ra rằng bạn sẽ cần phải

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

thực hiện các biện pháp an ninh bổ sung để giữ những cảnh báo này trở thành sự cố nghiêm trọng. Nhưng bạn bắt đầu ở đâu?

As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls.

Là một nhà phân tích, bạn sẽ bắt đầu bằng việc xác định tài sản và rủi ro quan trọng của tổ chức bạn. Sau đó bạn sẽ thực hiện các khuôn khổ và biện pháp kiểm soát cần thiết.

In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks.

Trong video này, chúng ta sẽ thảo luận về cách các chuyên gia bảo mật sử dụng các khuôn khổ để liên tục xác định và quản lý rủi ro. Chúng tôi cũng sẽ đề cập đến cách sử dụng kiểm soát an ninh để quản lý hoặc giảm thiểu rủi ro cụ thể.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.

Khung bảo mật là hướng dẫn được sử dụng để xây dựng kế hoạch để giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư. Khung bảo mật cung cấp một cách tiếp cận có cấu trúc để thực hiện vòng đời bảo mật. Vòng đời bảo mật là một loạt các chính sách không ngừng phát triển và các tiêu chuẩn xác định cách tổ chức quản lý rủi ro, tuân theo các hướng dẫn đã được thiết lập, và đáp ứng sự tuân thủ quy định hoặc pháp luật.

There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

Có một số khung bảo mật có thể được sử dụng để quản lý các loại hình tổ chức khác nhau và rủi ro tuân thủ quy định. Mục đích của khung bảo mật bao gồm việc bảo vệ thông tin nhận dạng cá nhân, được gọi là PII, đảm bảo thông tin tài chính, xác định điểm yếu về bảo mật, quản lý rủi ro tổ chức, và điều chỉnh bảo mật với mục tiêu kinh doanh.

Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

Các khung có bốn thành phần cốt lõi và nhiều chúng sẽ cho phép bạn quản lý tốt hơn các rủi ro tiềm ẩn. Thành phần cốt lõi đầu tiên là xác định và ghi lại các mục tiêu bảo mật. Ví dụ: một tổ chức có thể có mục tiêu là phù hợp với Quy định bảo vệ dữ liệu chung của EU, còn được gọi là GDPR. GDPR là luật bảo vệ dữ liệu được thiết lập để trao cho công dân châu Âu nhiều quyền kiểm soát hơn trên dữ liệu cá nhân của họ. Một nhà phân tích bảo mật có thể được yêu cầu xác định và ghi lại lĩnh vực mà một tổ chức không tuân thủ GDPR.

The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.

Thành phần cốt lõi thứ hai là thiết lập hướng dẫn để đạt được mục tiêu an ninh. Chẳng hạn, khi triển khai hướng dẫn để đạt được sự tuân thủ GDPR, tổ chức của bạn có thể cần phát triển chính sách mới về cách xử lý yêu cầu dữ liệu từ người dùng cá nhân.

The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.

Thành phần cốt lõi thứ ba của khung bảo mật là thực hiện các quy trình bảo mật mạnh mẽ. Trong trường hợp GDPR, một nhà phân tích bảo mật làm việc cho một công ty truyền thông xã hội có thể giúp thiết kế các thủ tục để đảm bảo tổ chức tuân thủ các yêu cầu dữ liệu người dùng đã được xác minh. Một ví dụ về loại yêu cầu này là khi người dùng cố gắng cập nhật hoặc xóa thông tin hồ sơ của họ.

The last core component of security frameworks is monitoring and communicating results. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.

Thành phần cốt lõi cuối cùng của khuôn khổ bảo mật là theo dõi và thông báo kết quả. Ví dụ, bạn có thể theo dõi mạng nội bộ của tổ chức bạn và báo cáo một vấn đề bảo mật tiềm ẩn ảnh hưởng đến GDPR cho người quản lý hoặc nhân viên tuân thủ quy định của bạn.

Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls.

Bây giờ chúng tôi đã giới thiệu bốn thành phần cốt lõi của khung bảo mật, chúng ta hãy buộc tất cả chúng lại với nhau. Các khung cho phép các nhà phân tích làm việc cùng với các thành viên khác của đội an ninh để ghi lại, thực hiện và sử dụng các chính sách và các thủ tục đã được tạo ra. Điều cần thiết đối với một nhà phân tích cấp đầu vào là phải hiểu quá trình này vì nó ảnh hưởng trực tiếp công việc họ làm và cách họ cộng tác với người khác. Tiếp theo, chúng ta sẽ thảo luận về các biện pháp kiểm soát bảo mật.

Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

Kiểm soát an ninh là biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể. Ví dụ: công ty của bạn có thể có một hướng dẫn yêu cầu tất cả nhân viên phải hoàn thành đào tạo về quyền riêng tư để giảm nguy cơ vi phạm dữ liệu. Là một nhà phân tích chứng khoán, bạn có thể sử dụng một công cụ phần mềm để tự động chỉ định và theo dõi cái nào nhân viên đã hoàn thành khóa đào tạo này.

Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk.

Các khuôn khổ và biện pháp kiểm soát bảo mật được quan trọng để quản lý an ninh cho tất cả các loại tổ chức và đảm bảo rằng mọi người đều thực hiện phần việc của mình để duy trì mức độ rủi ro thấp.

Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves.

Hiểu mục đích của họ và làm thế nào chúng được sử dụng cho phép các nhà phân tích hỗ trợ các mục tiêu bảo mật của tổ chức và bảo vệ những người mà nó phục vụ.

In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users.

Trong các video tiếp theo, chúng ta sẽ thảo luận về một số framework nổi tiếng và những nguyên tắc mà nhà phân tích cần phải lưu ý để giảm thiểu rủi ro và bảo vệ dữ liệu và người dùng.

1.3. Secure design – Thiết kế an toàn

Secure design

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Hi, welcome back! Previously, we discussed frameworks and controls in general. In this video, you'll learn about specific frameworks and controls that organizations can voluntarily use to minimize risks to their data and to protect users. Let's get started!

Thiết kế an toàn

Xin chào, chào mừng trở lại! Trước đây, chúng ta đã thảo luận về các khuôn khổ và điều khiển nói chung. Trong video này, bạn sẽ tìm hiểu về các khuôn khổ và biện pháp kiểm soát cụ thể mà các tổ chức có thể tự nguyện sử dụng để giảm thiểu rủi ro đối với dữ liệu của họ và để bảo vệ người dùng. Bắt đầu nào!

The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. CIA stands for confidentiality, integrity, and availability.

Bộ ba CIA là một mô hình nền tảng giúp thông báo cách các tổ chức xem xét rủi ro khi thiết lập hệ thống và chính sách bảo mật. CIA là viết tắt của bí mật, tính toàn vẹn và tính sẵn sàng.

Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

Tính bí mật có nghĩa là chỉ những người dùng được ủy quyền mới có thể truy cập vào tài sản hoặc dữ liệu cụ thể. Ví dụ: kiểm soát truy cập nghiêm ngặt xác định ai nên và không nên có quyền truy cập vào dữ liệu, phải được đặt ra để đảm bảo dữ liệu bí mật vẫn được an toàn.

Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

Tính toàn vẹn có nghĩa là dữ liệu được chính xác, xác thực và đáng tin cậy. Để duy trì tính toàn vẹn, các chuyên gia bảo mật có thể sử dụng một hình thức bảo vệ dữ liệu như mã hóa để bảo vệ dữ liệu khỏi bị giả mạo.

Availability means data is accessible to those who are authorized to access it. Let's define a term that came up during our discussion of the CIA triad:

Tính sẵn sàng có nghĩa là dữ liệu được có thể truy cập được đối với những người được phép truy cập nó. Hãy định nghĩa một thuật ngữ xuất hiện trong cuộc thảo luận của chúng tôi về bộ ba CIA:

asset.

tài sản.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

An asset is an item perceived as having value to an organization.

Tài sản là một vật phẩm được coi là có giá trị đối với một tổ chức.

And value is determined by the cost associated with the asset in question.

Và giá trị được xác định bởi chi phí liên quan đến tài sản được đề cập.

For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content. As you may remember, earlier in the course, we discussed frameworks and controls in general. Now, we'll discuss a specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

Ví dụ: một ứng dụng lưu trữ dữ liệu nhạy cảm, chẳng hạn như số an sinh xã hội hoặc tài khoản ngân hàng, là tài sản có giá trị đối với một tổ chức. Nó mang lại nhiều rủi ro hơn và do đó đòi hỏi phải kiểm soát an ninh chặt chẽ hơn đến một trang web chia sẻ nội dung tin tức có sẵn công khai. Như bạn có thể nhớ, trước đó trong khóa học, chúng tôi đã thảo luận về các khuôn khổ và biện pháp kiểm soát nói chung. Bây giờ, chúng ta sẽ thảo luận về một framework cụ thể được phát triển bởi National Institute of Standards and Technology (NIST) có trụ sở tại Hoa Kỳ. Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) cũng được gọi là NIST CSF. Khung an ninh mạng NIST là một khuôn khổ tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và thực tiễn tốt nhất để quản lý rủi ro an ninh mạng.

It's important to become familiar with this framework because security teams use it as

Điều quan trọng là phải làm quen với khuôn khổ này bởi vì đội an ninh sử dụng nó như

a baseline to manage short and long-term risk. Managing and mitigating risks and protecting an organization's assets from threat actors are key goals for security professionals. Understanding the different motives a threat actor may have, alongside identifying your organization's most valuable assets is important. Some of the most dangerous threat actors to consider are disgruntled employees. They are the most dangerous because they often have access to sensitive information and know where to find it. In order to reduce this type of risk, security professionals would use the principle of availability, as well as organizational guidelines based on frameworks to ensure staff members can only access the data they need to perform their jobs.

cơ sở để quản lý rủi ro ngắn hạn và dài hạn. Quản lý và giảm thiểu rủi ro và bảo vệ tài sản của một tổ chức từ các tác nhân đe dọa là mục tiêu chính của các chuyên gia bảo mật. Hiểu các động cơ khác nhau của một kẻ đe dọa có thể có, cùng với việc xác định tổ chức

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

của bạn tài sản có giá trị nhất là quan trọng. Một số tác nhân đe dọa nguy hiểm nhất cần xem xét là những nhân viên bất mãn. Chúng nguy hiểm nhất vì chúng thường có truy cập thông tin nhạy cảm và biết tìm nó ở đâu. Để hạn chế loại rủi ro này, các chuyên gia bảo mật sẽ sử dụng nguyên tắc sẵn có, cũng như các hướng dẫn tổ chức dựa trên các khuôn khổ để đảm bảo nhân viên chỉ có thể truy cập dữ liệu họ cần để thực hiện công việc của mình.

Threat actors originate from all across the globe, and a diverse workforce of security professionals helps organizations identify attackers' intentions. A variety of perspectives can assist organizations in understanding and mitigating the impact of malicious activity. That concludes our introduction to the CIA triad and NIST CSF framework, which are used to develop processes to secure organizations and the people they serve. You may be asked in an interview if you know about security frameworks and principles. Or you may be asked to explain how they're used to secure organizational assets. In either case, throughout this program, you'll have multiple opportunities to learn more about them and apply what we've discussed to real-world situations. Coming up, we'll discuss the ethics of security. See you soon!

Các tác nhân đe dọa có nguồn gốc từ khắp nơi trên thế giới, và lực lượng lao động đa dạng gồm các chuyên gia bảo mật giúp các tổ chức xác định ý định của kẻ tấn công. Nhiều quan điểm khác nhau có thể hỗ trợ các tổ chức trong hiểu biết và giảm nhẹ tác động của hoạt động độc hại. Điều đó kết thúc phần giới thiệu của chúng tôi về bộ ba CIA và khuôn khổ NIST CSF, được sử dụng để phát triển các quy trình nhằm đảm bảo an toàn cho các tổ chức và những người mà họ phục vụ. Bạn có thể được hỏi trong một cuộc phỏng vấn nếu bạn biết về các khuôn khổ và nguyên tắc bảo mật. Hoặc bạn có thể được yêu cầu giải thích chúng như thế nào được sử dụng để bảo đảm tài sản của tổ chức. Trong cả hai trường hợp, trong suốt chương trình này, bạn sẽ có nhiều cơ hội để tìm hiểu thêm về họ và áp dụng những gì chúng ta đã thảo luận vào các tình huống thực tế. Sắp tới chúng ta sẽ thảo luận đạo đức của an ninh. Hẹn sớm gặp lại!

1.4. Controls, frameworks, and compliance – Kiểm soát, khuôn khổ và tuân thủ

Controls, frameworks, and compliance

Previously, you were introduced to security frameworks and how they provide a structured approach to implementing a security lifecycle. As a reminder, a security lifecycle is a constantly evolving set of policies and standards. In this reading, you will learn more about how security frameworks, controls, and compliance regulations—or laws—are used together to manage security and make sure everyone does their part to minimize risk.

Kiểm soát, khuôn khổ và tuân thủ

Trước đây, bạn đã được giới thiệu về các khung bảo mật và cách chúng cung cấp cách tiếp cận có cấu trúc để triển khai vòng đời bảo mật. Xin nhắc lại, vòng đời bảo mật là một tập hợp các chính sách và tiêu chuẩn không ngừng phát triển. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cách các khung bảo mật, biện pháp kiểm soát và quy định tuân

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

thủ—hoặc luật—được sử dụng cùng nhau để quản lý bảo mật và đảm bảo mọi người thực hiện phần việc của mình để giảm thiểu rủi ro.

How controls, frameworks, and compliance are related

The **confidentiality, integrity, and availability (CIA) triad** is a model that helps inform how organizations consider risk when setting up systems and security policies.

CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.

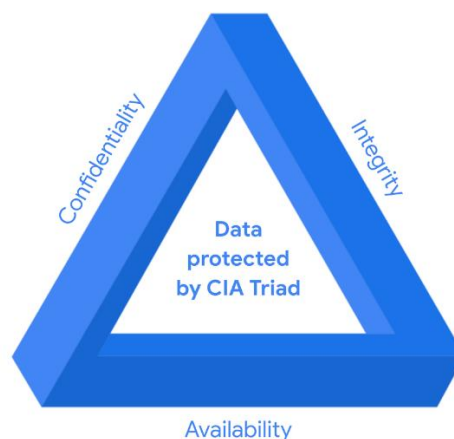
As you may recall, security controls are safeguards designed to reduce specific security risks. So they are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements.

Các biện pháp kiểm soát, khuôn khổ và sự tuân thủ có liên quan như thế nào

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

CIA là ba nguyên tắc cơ bản được các chuyên gia an ninh mạng sử dụng để thiết lập các biện pháp kiểm soát thích hợp nhằm giảm thiểu các mối đe dọa, rủi ro và lỗ hổng.

Như bạn có thể nhớ lại, kiểm soát bảo mật là các biện pháp bảo vệ được thiết kế để giảm các rủi ro bảo mật cụ thể. Vì vậy, chúng được sử dụng cùng với các khuôn khổ để đảm bảo rằng các mục tiêu và quy trình bảo mật được triển khai chính xác và các tổ chức đáp ứng các yêu cầu tuân thủ quy định.



Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

1. Identifying and documenting security goals

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

Compliance is the process of adhering to internal standards and external regulations.

Khung bảo mật là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư. Chúng có bốn thành phần cốt lõi:

1. Xác định và ghi lại các mục tiêu bảo mật
2. Thiết lập các nguyên tắc để đạt được mục tiêu bảo mật
3. Thực hiện các quy trình bảo mật mạnh mẽ
4. Giám sát và truyền đạt kết quả

Tuân thủ là quá trình tuân thủ các tiêu chuẩn nội bộ và các quy định bên ngoài.

Specific controls, frameworks, and compliance

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. The more aligned an organization is with compliance, the lower the risk.

Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

Note: Specifications and guidelines can change depending on the type of organization you work for.

In addition to the [NIST CSF](#) and [NIST RMF](#), there are several other controls, frameworks, and compliance standards that are important for security professionals to be familiar with to help keep organizations and the people they serve safe.

Các biện pháp kiểm soát, khuôn khổ và tuân thủ cụ thể

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) là cơ quan có trụ sở tại Hoa Kỳ, phát triển nhiều khuôn khổ tuân thủ tự nguyện mà các tổ chức trên toàn thế giới có thể sử dụng để giúp quản lý rủi ro. Tổ chức càng tuân thủ chặt chẽ thì rủi ro càng thấp.

Ví dụ về các khung bao gồm Khung bảo mật không gian mạng NIST (CSF) và Khung quản lý rủi ro NIST (RMF).

Lưu ý: Các thông số kỹ thuật và nguyên tắc có thể thay đổi tùy thuộc vào loại tổ chức mà bạn làm việc.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Ngoài việc [NIST CSF](#) và [NIST RMF](#), có một số biện pháp kiểm soát, khuôn khổ và tiêu chuẩn tuân thủ khác rất quan trọng mà các chuyên gia bảo mật cần phải làm quen để giúp giữ an toàn cho các tổ chức và những người mà họ phục vụ.

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.

Ủy ban Điều tiết Năng lượng Liên bang - Tập đoàn Độ tin cậy Điện Bắc Mỹ (FERC-NERC)

FERC-NERC là quy định áp dụng cho các tổ chức làm việc trong lĩnh vực điện lực hoặc có liên quan đến lưới điện Hoa Kỳ và Bắc Mỹ. Những loại tổ chức này có nghĩa vụ chuẩn bị, giảm thiểu và báo cáo mọi sự cố an ninh tiềm ẩn có thể ảnh hưởng tiêu cực đến lưới điện. Về mặt pháp lý, họ cũng được yêu cầu phải tuân thủ các Tiêu chuẩn về độ tin cậy của Bảo vệ cơ sở hạ tầng quan trọng (CIP) do FERC xác định.

The Federal Risk and Authorization Management Program (FedRAMP®)

FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings. Its purpose is to provide consistency across the government sector and third-party cloud providers.

Chương trình quản lý rủi ro và ủy quyền liên bang (FedRAMP®)

FedRAMP là chương trình của chính phủ liên bang Hoa Kỳ nhằm tiêu chuẩn hóa việc đánh giá, ủy quyền, giám sát và xử lý các dịch vụ đám mây và sản phẩm. Mục đích của nó là cung cấp sự nhất quán trong toàn bộ khu vực chính phủ và các nhà cung cấp đám mây bên thứ ba.

Center for Internet Security (CIS®)

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs.

Trung tâm An ninh Internet (CIS®)

CIS là một tổ chức phi lợi nhuận tập trung vào nhiều lĩnh vực. Nó cung cấp một bộ điều khiển có thể được sử dụng để bảo vệ hệ thống và mạng khỏi các cuộc tấn công. Mục

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

đích của nó là giúp các tổ chức thiết lập một kế hoạch phòng thủ tốt hơn. CIS cũng cung cấp các biện pháp kiểm soát hữu ích mà các chuyên gia bảo mật có thể tuân theo nếu xảy ra sự cố bảo mật.

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach.

Quy định chung về bảo vệ dữ liệu (GDPR)

GDPR là quy định dữ liệu chung của Liên minh Châu Âu (EU) nhằm bảo vệ việc xử lý dữ liệu của cư dân EU và quyền riêng tư của họ trong và ngoài lãnh thổ EU. Ví dụ: nếu một tổ chức không minh bạch về dữ liệu họ đang nắm giữ về một công dân EU và lý do họ nắm giữ dữ liệu đó, thì đây là hành vi vi phạm có thể dẫn đến phạt tiền đối với tổ chức. Ngoài ra, nếu xảy ra vi phạm và dữ liệu của công dân EU bị xâm phạm, họ phải được thông báo. Tổ chức bị ảnh hưởng có 72 giờ để thông báo cho công dân EU về hành vi vi phạm.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud.

Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)

PCI DSS là một tiêu chuẩn bảo mật quốc tế nhằm đảm bảo rằng các tổ chức lưu trữ, chấp nhận, xử lý và truyền thông tin thẻ tín dụng thực hiện trong một môi trường an toàn. Mục tiêu của tiêu chuẩn tuân thủ này là giảm gian lận thẻ tín dụng.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' **Protected Health Information (PHI)** is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it's a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance.

Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế (HIPAA)

HIPAA là luật liên bang Hoa Kỳ được thành lập năm 1996 để bảo vệ thông tin sức khỏe của bệnh nhân. Luật này cấm chia sẻ thông tin của bệnh nhân mà không có sự đồng ý của họ. Nó được điều chỉnh bởi ba quy tắc:

1. Sự riêng tư
2. Bảo vệ
3. Thông báo vi phạm

Các tổ chức lưu trữ dữ liệu bệnh nhân có nghĩa vụ pháp lý phải thông báo cho bệnh nhân về hành vi vi phạm vì nếu **Thông tin sức khỏe được bảo vệ (PHI)** của bệnh nhân bị lộ, điều đó có thể dẫn đến hành vi trộm cắp danh tính và gian lận bảo hiểm. PHI liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân, cho dù đó là kế hoạch chăm sóc hay thanh toán cho việc chăm sóc. Cùng với việc hiểu HIPAA như một luật, các chuyên gia bảo mật cũng cần phải làm quen với Liên minh tin cậy thông tin y tế (HITRUST®), đây là một khuôn khổ bảo mật và chương trình đảm bảo giúp các tổ chức đáp ứng tuân thủ HIPAA.

International Organization for Standardization (ISO)

ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

Tổ chức Tiêu chuẩn hóa Quốc tế (ISO)

ISO được tạo ra để thiết lập các tiêu chuẩn quốc tế liên quan đến công nghệ, sản xuất và quản lý xuyên biên giới. Nó giúp các tổ chức cải thiện quy trình và thủ tục của họ trong việc giữ chân nhân viên, lập kế hoạch, lãng phí và dịch vụ.

System and Organizations Controls (SOC type 1, SOC type 2)

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

- Associate
- Supervisor
- Manager
- Executive
- Vendor
- Others

They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Kiểm soát hệ thống và tổ chức (SOC loại 1, SOC loại 2)

Hội đồng tiêu chuẩn kiểm toán của Viện Kế toán Công chứng® Hoa Kỳ (AICPA) đã phát triển tiêu chuẩn này. SOC1 và SOC2 là một loạt báo cáo tập trung vào chính sách truy cập người dùng của tổ chức ở các cấp tổ chức khác nhau, chẳng hạn như:

- Kết hợp
- Người giám sát
- Giám đốc
- Điều hành
- Người bán
- Người khác

Chúng được sử dụng để đánh giá mức độ tuân thủ tài chính và mức độ rủi ro của tổ chức. Chúng cũng bao gồm tính bảo mật, quyền riêng tư, tính toàn vẹn, tính khả dụng, bảo mật và an toàn dữ liệu tổng thể. Kiểm soát thất bại trong các lĩnh vực này có thể dẫn đến gian lận.

Pro tip: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act.

Mẹo chuyên nghiệp : Có một số quy định thường xuyên được sửa đổi. Bạn được khuyến khích cập nhật các thay đổi và khám phá thêm các khuôn khổ, biện pháp kiểm soát và tuân thủ. Hai gợi ý nghiên cứu: Đạo luật Gramm-Leach-Bliley và Đạo luật Sarbanes-Oxley.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

United States Presidential Executive Order 14028

On May 12, 2021, President Joe Biden released an executive order related to improving the nation's cybersecurity to remediate the increase in threat actor activity. Remediation efforts are directed toward federal agencies and third parties with ties to U.S. [critical infrastructure](#). For additional information, review the [Executive Order on Improving the Nation's Cybersecurity](#).

Sắc lệnh hành pháp của Tổng thống Hoa Kỳ 14028

Vào ngày 12 tháng 5 năm 2021, Tổng thống Joe Biden đã ban hành lệnh hành pháp liên quan đến việc cải thiện an ninh mạng của quốc gia nhằm khắc phục sự gia tăng hoạt động của các tác nhân đe dọa. Các nỗ lực khắc phục được hướng tới các cơ quan liên bang và các bên thứ ba có quan hệ với Hoa Kỳ [cơ sở hạ tầng quan trọng](#). Để biết thêm thông tin, hãy xem lại [Sắc lệnh hành pháp về cải thiện an ninh mạng quốc gia](#).

Key takeaways

In this reading you learned more about controls, frameworks, and compliance. You also learned how they work together to help organizations maintain a low level of risk.

As a security analyst, it's important to stay up-to-date on common frameworks, controls, and compliance regulations and be aware of changes to the cybersecurity landscape to help ensure the safety of both organizations and people.

Bài học chính

Trong bài đọc này, bạn đã tìm hiểu thêm về các biện pháp kiểm soát, khuôn khổ và sự tuân thủ. Bạn cũng đã học được cách họ làm việc cùng nhau để giúp các tổ chức duy trì mức độ rủi ro thấp.

Là một nhà phân tích bảo mật, điều quan trọng là phải luôn cập nhật các khuôn khổ, biện pháp kiểm soát và quy định tuân thủ chung cũng như nhận thức được những thay đổi trong bối cảnh an ninh mạng để giúp đảm bảo an toàn cho cả tổ chức và con người.

1.5. Heather: Protect sensitive data and information – Heather: Bảo vệ dữ liệu và thông tin nhạy cảm

Heather: Protect sensitive data and information

Hello, my name is Heather and I'm the Vice President of Security Engineering at Google. PII has been an important topic on the internet since the beginning of the internet. And we have been talking about increasingly sophisticated ways to protect that data over time. When we think about collecting PII on behalf of another person, we should make sure we're very deliberate about how it's handled and where it's stored, and that we understand where it's stored all the time. Depending on what kind of role you're in, you might also need to protect that data to comply with regulation or law. And so, it's important to understand how the data relates to some of those

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

obligations. If an organization fails to meet their obligations, a number of things might happen. First, you might see a government regulator become more interested in understanding the practices around how a company is handling data. Secondly, consumers, customers, businesses may actually begin to directly inquire of the company how they're handling data. And this may become part of the customer relationship and increasingly important if that data is very sensitive. And third, the last consequence is legal action. And it's not uncommon for us to see victims of cybersecurity incidents now suing companies for mishandling their data. You can keep up to date with compliance, regulation and laws around PII by consulting the relevant website in the jurisdiction that you have a question for. Many government websites now post the laws, regulations, and compliance requirements for data that's being handled. The regulations and laws that govern how PII can be handled are very complex, all over the world, countries, states, counties are regulating it at different levels. It's important to understand and to be aware that these laws exist. However, if you need to ask a question about a specific law, it's important to seek advice from legal counsel for that particular jurisdiction. It may be very different than the jurisdiction that you're in.

Heather: Bảo vệ dữ liệu và thông tin nhạy cảm

Xin chào, tên tôi là Heather và Tôi là Phó Chủ tịch Kỹ thuật Bảo mật tại Google. PII đã là một chủ đề quan trọng trên internet kể từ khi có Internet. Và chúng ta đã nói về những cách ngày càng phức tạp để bảo vệ dữ liệu đó theo thời gian. Khi chúng tôi nghĩ đến việc thu thập PII thay mặt cho người khác, chúng ta nên đảm bảo rằng chúng ta rất cân nhắc về cách xử lý và nơi nó được lưu trữ và chúng tôi luôn biết nó được lưu trữ ở đâu. Tùy thuộc vào vai trò của bạn, bạn cũng có thể cần bảo vệ dữ liệu đó để tuân thủ quy định hoặc pháp luật. Và vì vậy, điều quan trọng là phải hiểu dữ liệu liên quan như thế nào đến một số trong số đó nghĩa vụ. Nếu tổ chức không thực hiện được nghĩa vụ của mình, một số điều có thể xảy ra. Đầu tiên, bạn có thể thấy cơ quan quản lý của chính phủ quan tâm nhiều hơn đến nhiều các thực tiễn xung quanh cách một công ty xử lý dữ liệu. Thứ hai, người tiêu dùng, khách hàng, doanh nghiệp có thể thực sự bắt đầu để trực tiếp hỏi công ty cách họ xử lý dữ liệu. Và điều này có thể trở thành một phần của mối quan hệ khách hàng và ngày càng quan trọng nếu dữ liệu đó rất nhạy cảm. Và thứ ba, hậu quả cuối cùng là hành động pháp lý. Và không có gì lạ khi chúng ta chứng kiến những nạn nhân của an ninh mạng sự cố hiện đang kiện các công ty vì xử lý sai dữ liệu của họ. Bạn có thể cập nhật các quy định, tuân thủ và luật pháp xung quanh PII bằng cách tham khảo trang web có liên quan trong khu vực pháp lý mà bạn có thắc mắc. Nhiều trang web của chính phủ hiện nay đăng các luật, quy định và yêu cầu tuân thủ đối với dữ liệu đang được xử lý. Các quy định và luật chi phối cách xử lý PII rất phức tạp, trên toàn thế giới, các quốc gia, tiểu bang, các quận đang điều chỉnh nó ở các cấp độ khác nhau. Điều quan trọng là phải hiểu và nhận thức được rằng những luật này tồn tại. Tuy nhiên, nếu bạn cần đặt câu hỏi về một luật cụ thể, điều quan trọng là tìm kiếm lời khuyên từ cố vấn pháp lý cho khu vực pháp lý cụ thể đó. Nó có thể rất khác so với khu vực pháp lý mà bạn đang ở.

1.6. Test your knowledge: Frameworks and controls – Kiểm tra kiến thức của bạn: Khung và điều khiển

2. Ethics in cybersecurity – Đạo đức trong an ninh mạng

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

2.1. Ethics in cybersecurity – Đạo đức trong an ninh mạng

Ethics in cybersecurity

In security, new technologies present new challenges. For every new security incident or risk, the right or wrong decision isn't always clear.

Đạo đức trong an ninh mạng

Trong lĩnh vực bảo mật, các công nghệ mới đặt ra những thách thức mới. Đối với mọi sự cố hoặc rủi ro an ninh mới, quyền hoặc quyết định sai lầm không phải lúc nào cũng rõ ràng.

For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization.

Ví dụ: hãy tưởng tượng bạn đang làm việc với tư cách là nhà phân tích bảo mật cấp thấp và bạn đã nhận được cảnh báo rủi ro cao. Bạn điều tra cảnh báo và phát hiện dữ liệu đã được chuyển giao mà không được phép.

You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do?

Bạn làm việc chăm chỉ để xác định ai đã thực hiện chuyển khoản và phát hiện ra đó là một trong những người bạn ở nơi làm việc của bạn. Bạn làm nghề gì?

Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality.

Về mặt đạo đức, với tư cách là một chuyên gia bảo mật, công việc của bạn là luôn không thiên vị và duy trì an ninh và bảo mật.

While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow. In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times.

Mặc dù việc muốn bảo vệ một người bạn là điều bình thường, bất kể người dùng được đề cập là ai, trách nhiệm và nghĩa vụ của bạn là tuân thủ các chính sách và giao thức mà bạn đã được đào tạo để tuân theo. Trong nhiều trường hợp, các nhóm bảo mật được giao quyền truy cập nhiều hơn vào dữ liệu và thông tin hơn những nhân viên khác. Các chuyên gia bảo mật phải tôn trọng đặc quyền đó và luôn hành động có đạo đức.

Security ethics are guidelines for making appropriate decisions as a security professional. As another example, if you as an analyst have the ability to grant

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

yourself access to payroll data and can give yourself a raise, just because you have access to do so, does that mean you should? The answer is no. You should never abuse the access you've been granted and entrusted with.

Đạo đức bảo mật là hướng dẫn cho đưa ra quyết định phù hợp với tư cách là một chuyên gia bảo mật. Một ví dụ khác, nếu bạn với tư cách là nhà phân tích có khả năng cấp cho mình quyền truy cập vào dữ liệu bảng lương và có thể tự tăng lương chỉ vì bạn có quyền truy cập để làm vậy điều đó có nghĩa là bạn nên làm vậy? Câu trả lời là không. Bạn không bao giờ nên lạm dụng quyền truy cập mà bạn đã được cấp và giao phó.

Let's discuss ethical principles that may raise questions as you navigate solutions for mitigating risks. These are confidentiality, privacy protections, and laws.

Hãy thảo luận về các nguyên tắc đạo đức có thể đặt ra câu hỏi khi bạn định hướng giải pháp giảm thiểu rủi ro. Đó là tính bảo mật, bảo vệ quyền riêng tư và luật pháp.

Let's begin with the first ethical principle, confidentiality. Earlier we discussed confidentiality as part of the CIA triad. Now let's discuss how confidentiality can be applied to ethics. As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe. For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend.

Hãy bắt đầu với nguyên tắc đạo đức đầu tiên, tính bảo mật. Trước đó chúng ta đã thảo luận về vấn đề bảo mật như một phần của bộ ba CIA. Bây giờ hãy thảo luận về cách áp dụng tính bảo mật vào đạo đức. Là một chuyên gia bảo mật, bạn sẽ gặp phải vấn đề độc quyền hoặc thông tin cá nhân, chẳng hạn như PII. Nghĩa vụ đạo đức của bạn là giữ thông tin đó bí mật và an toàn. Ví dụ: bạn có thể muốn giúp đỡ đồng nghiệp bằng cách cung cấp máy tính truy cập hệ thống bên ngoài các kênh được ghi chép phù hợp. Tuy nhiên, hành vi vi phạm đạo đức này có thể gây ra những hậu quả nghiêm trọng, bao gồm khiển trách, mất danh tiếng nghề nghiệp của bạn và hậu quả pháp lý cho cả bạn và bạn của bạn.

The second ethical principle to consider is privacy protections. Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person.

Nguyên tắc đạo đức thứ hai cần xem xét là bảo vệ quyền riêng tư. Bảo vệ quyền riêng tư có nghĩa là bảo vệ thông tin cá nhân khỏi sử dụng trái phép. Ví dụ: hãy tưởng tượng bạn nhận được email cá nhân sau giờ kể từ khi người quản lý của bạn yêu cầu số điện thoại nhà của đồng nghiệp. Người quản lý của bạn giải thích rằng họ không thể truy cập cơ sở

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

dữ liệu nhân viên vào lúc này, nhưng họ cần thảo luận một vấn đề khẩn cấp với người đó.

As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical. In situations like this, it can be difficult to know what to do. So, the best response is to adhere to the policies and procedures set by your organization.

Là nhà phân tích bảo mật, vai trò của bạn là tuân theo các chính sách và thủ tục của công ty bạn, trong ví dụ này nêu rõ rằng thông tin nhân viên được lưu trữ trong cơ sở dữ liệu an toàn và không bao giờ được truy cập hoặc chia sẻ ở bất kỳ định dạng nào khác. Vì vậy, việc truy cập và chia sẻ thông tin cá nhân của nhân viên sẽ là phi đạo đức. Trong những tình huống như thế này, thật khó để biết phải làm gì. Vì vậy, cách ứng phó tốt nhất là tuân thủ các chính sách và thủ tục do tổ chức của bạn đặt ra.

A third important ethical principle we must discuss is the law. Laws are rules that are recognized by a community and enforced by a governing entity.

Nguyên tắc đạo đức quan trọng thứ ba mà chúng ta phải thảo luận là luật pháp. Pháp luật là những quy định được cộng đồng thừa nhận và được thực thi bởi một cơ quan quản lý.

For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data.

Ví dụ, hãy xem xét một nhân viên tại bệnh viện đã được đào tạo để xử lý PII và SPII để tuân thủ. Nhân viên có các tập tin chứa dữ liệu bí mật không bao giờ được để lại không được giám sát, nhưng nhân viên đó lại đến trễ cuộc họp. Thay vì khóa các tập tin trong một khu vực được chỉ định, các tập tin được để trên bàn của nhân viên, không được giám sát. Khi nhân viên trở lại, các tập tin bị thiếu. Nhân viên vừa vi phạm nhiều quy định tuân thủ và hành động của họ là phi đạo đức và bất hợp pháp, vì sự sơ suất của họ có thể dẫn đến việc mất dữ liệu bệnh nhân và bệnh viện tư nhân.

As you enter the security field, remember that technology is constantly evolving, and so are attackers' tactics and techniques. Because of this, security professionals must continue to think critically about how to respond to attacks.

Khi bạn bước vào lĩnh vực bảo mật, hãy nhớ rằng công nghệ không ngừng phát triển, và chiến thuật và kỹ thuật của kẻ tấn công cũng vậy. Vì điều này, các chuyên gia bảo mật phải tiếp tục suy nghĩ chín chắn về làm thế nào để đáp ứng với các cuộc tấn công.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Having a strong sense of ethics can guide your decisions to ensure that the proper processes and procedures are followed to mitigate these continually evolving risks.

Có ý thức đạo đức tốt có thể hướng dẫn các quyết định của bạn để đảm bảo rằng các quyết định đúng đắn quy trình và thủ tục được tuân thủ để giảm thiểu những rủi ro liên tục phát triển này.

2.2. Ethical concepts that guide cybersecurity decisions – Các khái niệm đạo đức hướng dẫn các quyết định về an ninh mạng

Ethical concepts that guide cybersecurity decisions

Previously, you were introduced to the concept of security ethics. **Security ethics** are guidelines for making appropriate decisions as a security professional. Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data. Having a strong sense of ethics can help you navigate your decisions as a cybersecurity professional so you're able to mitigate threats posed by threat actors' constantly evolving tactics and techniques. In this reading, you'll learn about more ethical concepts that are essential to know so you can make appropriate decisions about how to legally and ethically respond to attacks in a way that protects organizations and people alike.

Các khái niệm đạo đức hướng dẫn các quyết định về an ninh mạng

Trước đây, bạn đã được giới thiệu khái niệm về đạo đức bảo mật. **Đạo đức bảo mật** là những hướng dẫn để đưa ra quyết định phù hợp với tư cách là một chuyên gia bảo mật. Có đạo đức đòi hỏi các chuyên gia bảo mật phải không thiên vị và duy trì tính bảo mật và bảo mật của dữ liệu riêng tư. Việc có ý thức đạo đức cao có thể giúp bạn định hướng các quyết định của mình với tư cách là một chuyên gia an ninh mạng để bạn có thể giảm thiểu các mối đe dọa do các chiến thuật và kỹ thuật không ngừng phát triển của các tác nhân đe dọa gây ra. Trong bài đọc này, bạn sẽ tìm hiểu thêm về các khái niệm đạo đức cần biết để có thể đưa ra quyết định phù hợp về cách ứng phó hợp pháp và có đạo đức trước các cuộc tấn công theo cách bảo vệ các tổ chức cũng như mọi người.

Ethical concerns and laws related to counterattacks

United States standpoint on counterattacks

In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others. You can only defend. The act of counterattacking in the U.S. is perceived as an act of vigilantism. A vigilante is a person who is not a member of law enforcement who decides to stop a crime on their own. And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm. Lastly, if the threat actor in question is a state-sponsored hacker, a counterattack can lead to serious international implications. A **hactivist** is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel.

Những lo ngại về đạo đức và luật pháp liên quan đến phản công

Quan điểm của Hoa Kỳ về các cuộc phản công

Tại Hoa Kỳ, việc triển khai một cuộc phản công nhằm vào tác nhân đe dọa là bất hợp pháp vì các luật như Đạo luật Lừa đảo và Lạm dụng Máy tính năm 1986 và Đạo luật Chia sẻ Thông tin An ninh Mạng năm 2015, cùng nhiều luật khác. Bạn chỉ có thể phòng thủ. Hành động phản công ở Mỹ được coi là hành động cảnh giác. Người cảnh giác là người không phải là thành viên của cơ quan thực thi pháp luật và quyết định tự mình ngăn chặn tội phạm. Và bởi vì những kẻ đe dọa là tội phạm, các cuộc phản công có thể dẫn đến sự leo thang hơn nữa của cuộc tấn công, có thể gây ra nhiều thiệt hại và tổn hại hơn. Cuối cùng, nếu tác nhân đe dọa được đề cập là một kẻ tấn công được nhà nước bảo trợ, thì một cuộc phản công có thể dẫn đến những tác động quốc tế nghiêm trọng. Hactivist là người sử dụng hack để đạt được mục tiêu chính trị. Mục tiêu chính trị có thể là thúc đẩy sự thay đổi xã hội hoặc sự bất tuân dân sự.

Vì những lý do này, những cá nhân duy nhất ở Hoa Kỳ được phép phản công là nhân viên chính phủ liên bang hoặc quân nhân được phê duyệt.

International standpoint on counterattacks

The International Court of Justice (ICJ), which updates its guidance regularly, states that a person or group can counterattack if:

- The counterattack will only affect the party that attacked first.
- The counterattack is a direct communication asking the initial attacker to stop.
- The counterattack does not escalate the situation.
- The counterattack effects can be reversed.

Organizations typically do not counterattack because the above scenarios and parameters are hard to measure. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control. Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.

To learn more about specific scenarios and ethical concerns from an international perspective, review updates provided in the [Tallinn Manual online](#).

Quan điểm quốc tế về phản công

Tòa án Công lý Quốc tế (ICJ), nơi thường xuyên cập nhật hướng dẫn của mình, tuyên bố rằng một người hoặc một nhóm có thể phản công nếu:

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

- Cuộc phản công sẽ chỉ ảnh hưởng đến bên tấn công trước.
- Cuộc phản công là một cuộc giao tiếp trực tiếp yêu cầu kẻ tấn công ban đầu dừng lại.
- Cuộc phản công không làm tình hình leo thang.
- Hiệu ứng phản công có thể bị đảo ngược.

Các tổ chức thường không phản công vì các kịch bản và thông số trên rất khó đo lường. Có rất nhiều điều không chắc chắn về việc điều gì là hợp pháp và điều gì không hợp pháp, và đôi khi rất khó kiểm soát những kết quả tiêu cực. Các hành động phản công thường dẫn đến kết quả tồi tệ hơn, đặc biệt khi bạn không phải là chuyên gia giàu kinh nghiệm trong lĩnh vực này.

Để tìm hiểu thêm về các tình huống cụ thể và các mối lo ngại về đạo đức từ góc độ quốc tế, hãy xem lại các thông tin cập nhật được cung cấp trong [Hướng dẫn sử dụng Tallinn trực tuyến](#).

Ethical principles and methodologies

Because counterattacks are generally disapproved of or illegal, the security realm has created frameworks and controls—such as the confidentiality, integrity, and availability (CIA) triad and others discussed earlier in the program—to address issues of confidentiality, privacy protections, and laws. To better understand the relationship between these issues and the ethical obligations of cybersecurity professionals, review the following key concepts as they relate to using ethics to protect organizations and the people they serve.

Các nguyên tắc và phương pháp đạo đức

Bởi vì các cuộc phản công thường bị phản đối hoặc bất hợp pháp, lĩnh vực bảo mật đã tạo ra các khuôn khổ và biện pháp kiểm soát—chẳng hạn như bộ ba bí mật, tính toàn vẹn và tính khả dụng (CIA) và những vấn đề khác đã được thảo luận trước đó trong chương trình—để giải quyết các vấn đề về bảo mật, bảo vệ quyền riêng tư và luật pháp. Để hiểu rõ hơn mối quan hệ giữa những vấn đề này và nghĩa vụ đạo đức của các chuyên gia an ninh mạng, hãy xem lại các khái niệm chính sau đây vì chúng liên quan đến việc sử dụng đạo đức để bảo vệ các tổ chức và những người mà họ phục vụ.

Confidentiality means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of respect for privacy to safeguard private assets and data.

Tính bảo mật có nghĩa là chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài sản hoặc dữ liệu cụ thể. Tính bảo mật liên quan đến đạo đức nghề nghiệp có nghĩa là cần phải có sự tôn trọng cao đối với quyền riêng tư để bảo vệ tài sản và dữ liệu riêng tư.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Privacy protection means safeguarding personal information from unauthorized use. Personally identifiable information (PII) and sensitive personally identifiable information (SPII) are types of personal data that can cause people harm if they are stolen. **PII** data is any information used to infer an individual's identity, like their name and phone number. **SPII** data is a specific type of PII that falls under stricter handling guidelines, including social security numbers and credit card numbers. To effectively safeguard PII and SPII data, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals.

Bảo vệ quyền riêng tư có nghĩa là bảo vệ thông tin cá nhân khỏi việc sử dụng trái phép. Thông tin nhận dạng cá nhân (PII) và thông tin nhận dạng cá nhân nhạy cảm (SPII) là các loại dữ liệu cá nhân có thể gây hại cho mọi người nếu chúng bị đánh cắp. **Dữ liệu PII** là bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân, như tên và số điện thoại của họ. **Dữ liệu SPII** là một loại PII cụ thể tuân theo các nguyên tắc xử lý chặt chẽ hơn, bao gồm số an sinh xã hội và số thẻ tín dụng. Để bảo vệ hiệu quả dữ liệu PII và SPII, các chuyên gia bảo mật có nghĩa vụ đạo đức trong việc bảo mật thông tin cá nhân, xác định các lỗ hổng bảo mật, quản lý rủi ro tổ chức và điều chỉnh bảo mật cho phù hợp với mục tiêu kinh doanh.

Laws are rules that are recognized by a community and enforced by a governing entity. As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization. To do this:

- You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law.
- Be transparent and just, and rely on evidence.
- Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise.
- Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.

As an example, consider the **Health Insurance Portability and Accountability Act (HIPAA)**, which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed.

Luật pháp là những quy tắc được cộng đồng thừa nhận và được thực thi bởi một cơ quan quản lý. Là một chuyên gia bảo mật, bạn sẽ có nghĩa vụ đạo đức để bảo vệ tổ chức của mình, cơ sở hạ tầng nội bộ và những người có liên quan đến tổ chức. Để làm điều này:

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

- Bạn phải không thiên vị và thực hiện công việc của mình một cách trung thực, có trách nhiệm và với sự tôn trọng cao nhất đối với pháp luật.
- Hãy minh bạch và công bằng, và dựa vào bằng chứng.
- Đảm bảo rằng bạn luôn đầu tư vào công việc mình đang làm để có thể giải quyết các vấn đề phát sinh một cách phù hợp và có đạo đức.
- Luôn cập nhật thông tin và cố gắng nâng cao kỹ năng của mình để có thể đóng góp vào việc cải thiện bối cảnh mạng.

Ví dụ: hãy xem xét **Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA)**, là luật liên bang của Hoa Kỳ được thiết lập để bảo vệ thông tin sức khỏe của bệnh nhân, còn được gọi là PHI hoặc thông tin sức khỏe được bảo vệ. Luật này cấm chia sẻ thông tin của bệnh nhân mà không có sự đồng ý của họ. Vì vậy, với tư cách là một chuyên gia bảo mật, bạn có thể giúp đảm bảo rằng tổ chức mà bạn làm việc tuân thủ cả nghĩa vụ pháp lý và đạo đức trong việc thông báo cho bệnh nhân về hành vi vi phạm nếu dữ liệu chăm sóc sức khỏe của họ bị lộ.

Key takeaways

As a future security professional, ethics will play a large role in your daily work. Understanding ethics and laws will help you make the correct choices if and when you encounter a security threat or an incident that results in a breach.

Bài học chính

Là một chuyên gia bảo mật trong tương lai, đạo đức sẽ đóng một vai trò lớn trong công việc hàng ngày của bạn. Hiểu rõ đạo đức và luật pháp sẽ giúp bạn đưa ra những lựa chọn đúng đắn nếu và khi bạn gặp phải mối đe dọa an ninh hoặc sự cố dẫn đến vi phạm.

2.3. Practice: Ethics for cybersecurity professionals – Thực hành: Đạo đức dành cho chuyên gia an ninh mạng

Practice: Ethics for cybersecurity professionals

Explore a number of scenarios that you might encounter as a security analyst, and consider how you would respond to security incidents based on your understanding of security ethics.

Thực hành: Đạo đức dành cho chuyên gia an ninh mạng

Khám phá một số tình huống mà bạn có thể gặp phải với tư cách là nhà phân tích bảo mật và xem xét cách bạn sẽ ứng phó với các sự cố bảo mật dựa trên hiểu biết của bạn về đạo đức bảo mật.

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng



| Scenario | Response |
|---|--|
| You work for a hospital as a security analyst. | Initiate a counter-attack |
| One day, you log into your work computer and see a ransom note displayed on your screen. Access to files and applications is locked. | Use a self-developed decryptor tool to stop the attack Immediately contact your supervisor |
| You realize this is a ransomware attack. | Contact government agencies for assistance |
| A doctor you work with claims to have laptop performance issues, so you try to identify the problem. | Immediately secure the patient files Submit a formal complaint to Health and Human Services |
| As you're working, you notice the doctor's laptop has unsecured patient files visible on-screen instead of within the medical practice's secure software. | Publicly shame the doctor for not following proper procedures Assume the doctor knows about the issue and do nothing |
| You work for a medical device company as an entry-level security analyst. | Take the laptops home and perform a factory reset |
| Your supervisor has asked you to securely dispose of old developer laptops, and tells you they may contain PII (personally identifiable information). | Dispose of the laptops without properly erasing the data Store the laptops in an area designated for old equipment Remove the laptop hard drives and irreversibly erase all data |
| You work as an entry-level analyst for a pharmaceutical company. | Confront the user directly regarding non-compliance with internal ethical standards |
| You receive SIEM tool alerts about unusual employee activity. | Tell your supervisor and take no other action |
| You check their account activity and | |

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

observe them copying confidential files to an external folder linked to an unknown destination.

Follow provided procedures to address the issue.

Report the incident to the company's security personnel

| Tình huống | |
|--|---|
| <p>Bạn làm việc cho một bệnh viện với tư cách là nhà phân tích bảo mật.</p> <p>Một ngày nọ, bạn đăng nhập vào máy tính ở cơ quan và thấy thông báo đòi tiền chuộc hiển thị trên màn hình. Quyền truy cập vào các tập tin và ứng dụng bị khóa.</p> <p>Bạn nhận ra đây là một cuộc tấn công ransomware.</p> | <p>Bắt đầu phản công</p> <p>Sử dụng công cụ giải mã tự phát triển để ngăn chặn cuộc tấn công</p> <p>Hãy liên hệ ngay với người giám sát của bạn</p> <p>Liên hệ với các cơ quan chính phủ để được hỗ trợ</p> |
| <p>Một bác sĩ làm việc cùng bạn tuyên bố rằng máy tính xách tay có vấn đề về hiệu suất, vì vậy bạn cố gắng xác định vấn đề.</p> <p>Khi đang làm việc, bạn nhận thấy máy tính xách tay của bác sĩ có các tệp bệnh nhân không bảo mật hiển thị trên màn hình thay vì trong phần mềm bảo mật của phòng khám y tế.</p> | <p>Bảo mật ngay lập tức hồ sơ bệnh nhân</p> <p>Gửi khiếu nại chính thức tới Bộ Y tế và Dịch vụ Nhân sinh</p> <p>Công khai xấu hổ vì bác sĩ không tuân thủ đúng quy trình</p> <p>Giả sử bác sĩ biết về vấn đề này và không làm gì cả</p> |
| <p>Bạn làm việc cho một công ty thiết bị y tế với vai trò là nhà phân tích bảo mật cấp độ đầu vào.</p> <p>Người giám sát của bạn đã yêu cầu bạn tiêu hủy an toàn các máy tính xách tay cũ của nhà phát triển và cho bạn biết rằng chúng có thể chứa PII (thông tin nhận dạng cá nhân).</p> | <p>Mang máy tính xách tay về nhà và thực hiện khôi phục cài đặt gốc</p> <p>Vứt bỏ máy tính xách tay mà không xóa dữ liệu đúng cách</p> <p>Cất giữ máy tính xách tay ở khu vực dành riêng cho thiết bị cũ</p> <p>Tháo ổ cứng máy tính xách tay và xóa tất cả dữ liệu không thể phục hồi</p> |
| <p>Bạn làm việc như một nhà phân tích cấp đầu vào cho một công ty dược phẩm.</p> <p>Bạn nhận được thông báo từ công cụ SIEM về hoạt động bất thường của nhân viên.</p> | <p>Đối đầu trực tiếp với người dùng về việc không tuân thủ các tiêu chuẩn đạo đức nội bộ</p> <p>Hãy nói với người giám sát của bạn và không thực hiện hành động nào khác</p> |

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

| | |
|--|--|
| Bạn kiểm tra hoạt động tài khoản của họ và quan sát thấy họ sao chép các tệp bí mật vào một thư mục bên ngoài được liên kết đến một đích đến không xác định. | Thực hiện theo các thủ tục được cung cấp để giải quyết vấn đề. |
|--|--|

2.4. Holly: The importance of ethics as a cybersecurity professional – Holly: Tầm quan trọng của đạo đức với tư cách là một chuyên gia an ninh mạng

Holly: The importance of ethics as a cybersecurity professional

Hi, I'm Holly and I'm a Cloud Security Architect with Google Cloud. At the beginning of my adult career, I sold hosiery while I was going to school. That led me into an opportunity to work in banking, which then led me into an opportunity to work in telecommunications. From there I managed to get myself into a security vendor and learn security. Part of the way that I was able to change from my original half of my tech career being a database administrator to getting into cybersecurity was through getting certificates like you're doing today. Those really helped me gain credibility with potential employers when I didn't have the experience in this particular field yet. Ethics are really the crux of cybersecurity, you need to be able to be ethical in all of your actions in order to be a cybersecurity professional. Examples of unethical behavior are usually honestly just slight laziness, people taking shortcuts and not really thinking about the consequences of their actions. So, certainly when people share passwords to systems or give out private information, or look into systems for their own personal information or purposes about people they know or about celebrities. One of the most difficult situations that I ever faced in my technology career related to ethics was shortly after 9/11, my boss's boss's boss came to me with a bunch of keywords that were clearly related to the attack in New York and asked me to query the database that I administered that had everybody's text messages in it for the entire telecommunications company without anything in writing and without a court order. I was in a very uncomfortable position to tell someone that much senior than me that I wasn't comfortable doing that. I suggested that he bring something in writing to me to do that and he found someone else who did it for him. When you're faced with one of these difficult decisions, it's good to think about what would be the consequences of your decision. My encouragement to those of you out here taking this program is that the rewards that you get from helping to protect your company or your users or your organization from cyber criminals is really great. We get to be the good guys and help protect our industry and our customers from cyber attacks and cyber criminals. That's rewarding.

Holly: Tầm quan trọng của đạo đức với tư cách là một chuyên gia an ninh mạng

Xin chào, tôi là Holly và tôi là Kiến trúc sư bảo mật đám mây của Google Cloud. Khi bắt đầu sự nghiệp trưởng thành của tôi, Tôi đã bán hàng dệt kim khi còn đi học. Điều đó dẫn tôi đến cơ hội làm việc trong ngành ngân hàng, sau đó dẫn tôi vào cơ hội làm việc trong lĩnh vực viễn thông. Từ đó tôi đã có thể dần thân vào một nhà cung cấp bảo mật và tìm hiểu bảo mật. Một phần trong cách mà tôi có thể sự thay đổi so với nửa đầu sự nghiệp công nghệ của tôi một quản trị viên cơ sở dữ liệu để tham gia an ninh mạng là thông qua

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

việc nhận được chứng chỉ giống như bạn đang làm ngày hôm nay. Những điều đó thực sự đã giúp tôi có được sự tin nhiệm với những nhà tuyển dụng tiềm năng khi tôi không còn có kinh nghiệm trong lĩnh vực cụ thể này. Đạo đức thực sự là mấu chốt của an ninh mạng, bạn cần có khả năng có đạo đức trong tất cả hành động của bạn để trở thành một chuyên gia an ninh mạng. Ví dụ về hành vi phi đạo đức là nói thật thì thường chỉ hơi lười biếng thôi, mọi người đi đường tắt và thực sự không phải vậy suy nghĩ về hậu quả của hành động của họ. Vì vậy, chắc chắn khi mọi người chia sẻ mật khẩu với hệ thống hoặc cung cấp thông tin cá nhân, hoặc xem xét các hệ thống cho thông tin cá nhân của riêng họ hoặc mục đích về những người họ biết hoặc về những người nổi tiếng. Một trong những tình huống khó khăn nhất mà tôi từng gặp phải sự nghiệp công nghệ của tôi liên quan đến vấn đề đạo đức ngay sau ngày 11/9, sếp của sếp sếp của tôi đã đến gặp tôi với một loạt từ khóa rõ ràng liên quan đến vụ tấn công ở New York và yêu cầu tôi truy vấn cơ sở dữ liệu mà tôi được quản lý có tin nhắn văn bản của mọi người trong đó toàn bộ công ty viễn thông mà không có bất cứ điều gì bằng văn bản và không có lệnh của tòa án. Tôi đang ở trong một tình thế rất khó chịu để nói một người cao cấp hơn tôi nhiều rằng tôi không thấy thoải mái khi làm điều đó. Tôi đề nghị anh ấy mang thứ gì đó bằng văn bản để tôi làm điều đó và anh ấy đã tìm được người khác làm việc đó cho anh ta. Khi bạn phải đối mặt với một trong những quyết định khó khăn này, thật tốt khi nghĩ về điều gì sẽ xảy ra hậu quả của quyết định của bạn. Sự khuyến khích của tôi dành cho những người trong số các bạn ở đây đang tham gia chương trình này là phần thưởng mà bạn nhận được từ việc giúp bảo vệ công ty hoặc người dùng của bạn hoặc tổ chức của bạn khỏi tội phạm mạng thực sự tuyệt vời. Chúng ta trở thành người tốt và giúp đỡ bảo vệ ngành công nghiệp của chúng tôi và khách hàng của chúng tôi khỏi các cuộc tấn công mạng và tội phạm mạng. Đó là bổ ích.

2.5. Use ethics to make decisions – Sử dụng đạo đức để đưa ra quyết định

Use ethics to make decisions

You've been introduced to security ethics, including specific examples of how ethics are applied in the workplace. Now, it's your turn to share a bit of your experience and exchange ideas with other learners in the course.

Sử dụng đạo đức để đưa ra quyết định

Bạn đã được giới thiệu về đạo đức bảo mật, bao gồm các ví dụ cụ thể về cách áp dụng đạo đức tại nơi làm việc. Bây giờ, đến lượt bạn chia sẻ một chút kinh nghiệm của mình và trao đổi ý kiến với những người học khác trong khóa học.

Option 1: Your example can be related to a work, academic, and/or volunteer setting and should focus on a time when you chose an ethical course of action.

For this discussion prompt, consider the following:

- What was the situation?
- How did you use ethics to make a decision?
- What was the impact and/or result of your decision?

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Tùy chọn 1: Ví dụ của bạn có thể liên quan đến môi trường làm việc, học tập và/hoặc tình nguyện và nên tập trung vào thời điểm bạn chọn một hành động có đạo đức.

Đối với lời nhắc thảo luận này, hãy xem xét những điều sau:

- Tình hình là gì?
- Bạn đã sử dụng đạo đức để đưa ra quyết định như thế nào?
- Tác động và/hoặc kết quả của quyết định của bạn là gì?

Option 2: Your example can be related to a work, academic, and/or volunteer setting and should focus on a time when someone else chose an ethical course of action.

For this discussion prompt, consider the following:

- What was the situation?
- How did the person use ethics to make a decision?
- What was the impact and/or result of the person's decision?

Please write one to two paragraphs in response to one of the discussion options (150–250 words). Then, visit the [discussion forums](#) and, applying what you've learned, comment on at least two posts from other learners.

Participation is optional

Tùy chọn 2: Ví dụ của bạn có thể liên quan đến môi trường làm việc, học tập và/hoặc tình nguyện và nên tập trung vào thời điểm người khác chọn một hành động có đạo đức.

Đối với lời nhắc thảo luận này, hãy xem xét những điều sau:

- Tình hình là gì?
- Người đó đã sử dụng đạo đức để đưa ra quyết định như thế nào?
- Tác động và/hoặc kết quả của quyết định của người đó là gì?

Vui lòng viết một đến hai đoạn văn để phản hồi một trong các phương án thảo luận (150–250 từ). Sau đó, hãy ghé thăm [diễn đàn thảo luận](#) và áp dụng những gì bạn đã học, bình luận về ít nhất hai bài đăng của những người học khác.

Việc tham gia là tùy chọn

2.6. Test your knowledge: Ethics in cybersecurity – Kiểm tra kiến thức của bạn: Đạo đức trong an ninh mạng

3. Review: Protect against threats, risks, and vulnerabilities – Đánh giá: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

3.1. Wrap-up – Gợi lại

Wrap-up

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

You are now better prepared to understand and help make decisions regarding assessing and managing risks. Let's review what we've covered.

Bây giờ bạn đã chuẩn bị tốt hơn để hiểu và giúp đỡ đưa ra quyết định liên quan đến việc đánh giá và quản lý rủi ro. Hãy xem lại những gì chúng tôi đã đề cập.

We discussed security frameworks and controls and how they're used to develop processes and procedures that protect organizations and the people they serve. We also discussed core components of frameworks, such as identifying security goals and establishing guidelines to achieve those goals.

Chúng tôi đã thảo luận về các khuôn khổ bảo mật và các điều khiển và cách chúng được sử dụng để phát triển các quy trình và thủ tục mà bảo vệ các tổ chức và những người mà họ phục vụ. Chúng tôi cũng thảo luận về các thành phần cốt lõi của khung, chẳng hạn như xác định các mục tiêu bảo mật và thiết lập các hướng dẫn để đạt được các mục tiêu đó.

Then, we introduced specific frameworks and controls, including the CIA triad and the NIST CSF, and how they are used to manage risk.

Sau đó, chúng tôi đã giới thiệu các khuôn khổ và biện pháp kiểm soát cụ thể, bao gồm cả bộ ba CIA và NIST CSF, và cách chúng được sử dụng để quản lý rủi ro.

And finally, we discussed security ethics, including common ethical issues to consider, such as confidentiality, privacy protections, and laws.

Và cuối cùng, chúng tôi đã thảo luận về đạo đức bảo mật, bao gồm các vấn đề đạo đức chung để xem xét, chẳng hạn như tính bảo mật, bảo vệ quyền riêng tư và luật pháp.

You're almost there, only one more section to go in this course. Coming up, you'll learn about common tools and programming languages used by security analysts to protect organizational operations. Hope you're as excited as I am to keep going!

Bạn gần như ở đó rồi, chỉ có một phần nhiều hơn để đi trong khóa học này. Tiếp theo, bạn sẽ tìm hiểu về các công cụ phổ biến và ngôn ngữ lập trình được sử dụng bởi các nhà phân tích bảo mật để bảo vệ hoạt động của tổ chức. Hy vọng bạn cũng hào hứng như tôi để tiếp tục!

3.2. Glossary terms from module 3 – Thuật ngữ trong học phần 3

Glossary terms from module 3

Terms and definitions from Course 1, Module 3

Thuật ngữ trong học phần 3

Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 3

Asset: An item perceived as having value to an organization

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

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

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

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

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

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

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

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

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

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

Hactivist: A person who uses hacking to achieve a political goal

Hactivist: Người sử dụng hack để đạt được mục tiêu chính trị

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal law established to protect patients' health information

Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA): Luật liên bang của Hoa Kỳ được thiết lập để bảo vệ thông tin sức khỏe của bệnh nhân

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

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

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

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

Privacy protection: The act of safeguarding personal information from unauthorized use

Bảo vệ quyền riêng tư: Hành động bảo vệ thông tin cá nhân khỏi việc sử dụng trái phép

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual

Thông tin sức khỏe được bảo vệ (PHI): Thông tin liên quan đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân

Module 3: Protect against threats, risks, and vulnerabilities

Phần 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng

Security architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

Kiến trúc bảo mật: Một loại thiết kế bảo mật bao gồm nhiều thành phần, chẳng hạn như các công cụ và quy trình, được sử dụng để bảo vệ tổ chức khỏi các rủi ro và các mối đe dọa bên ngoài

Security controls: Safeguards designed to reduce specific security risks

Kiểm soát bảo mật: Các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể

Security ethics: Guidelines for making appropriate decisions as a security professional

Đạo đức bảo mật: Hướng dẫn đưa ra quyết định phù hợp với tư cách là chuyên gia bảo mật

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

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

Security governance: Practices that help support, define, and direct security efforts of an organization

Quản trị bảo mật: Các hoạt động giúp hỗ trợ, xác định và chỉ đạo các nỗ lực bảo mật của một tổ chức

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Thông tin nhận dạng cá nhân nhạy cảm (SPII): Một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn

3.3. Module 3 challenge – Thử thách module 3

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Module 4: Cybersecurity tools and programming languages –Các công cụ an ninh mạng và ngôn ngữ lập trình

You'll discover common tools used by cybersecurity analysts to identify and mitigate risk. You'll learn about security information and event management (SIEM) tools, network protocol analyzers, and programming languages such as Python and SQL.

Bạn sẽ khám phá các công cụ phổ biến được các nhà phân tích an ninh mạng sử dụng để xác định và giảm thiểu rủi ro. Bạn sẽ tìm hiểu về các công cụ quản lý sự kiện và thông tin bảo mật (SIEM), bộ phân tích giao thức mạng và các ngôn ngữ lập trình như Python và SQL.

Learning Objectives

- Identify common tools used by entry-level security analysts
- Identify the purposes of commonly used tools
- Identify commonly used programming languages and how entry-level security analysts interact with those languages
- Discuss how entry-level security analysts use tools and programming languages to mitigate risk

Mục tiêu học tập

- Xác định các công cụ phổ biến được sử dụng bởi các nhà phân tích bảo mật cấp đầu vào
- Xác định mục đích của các công cụ thường được sử dụng
- Xác định các ngôn ngữ lập trình thường được sử dụng và cách các nhà phân tích bảo mật cấp đầu vào tương tác với các ngôn ngữ đó
- Thảo luận cách các nhà phân tích bảo mật cấp đầu vào sử dụng các công cụ và ngôn ngữ lập trình để giảm thiểu rủi ro

1. Important cybersecurity tools – Các công cụ an ninh mạng quan trọng

1.1. Welcome to module 4 – Chào mừng đến với module 4

Welcome to module 4

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Welcome to the final section of this course! Here, we'll be introducing tools and programming languages that are commonly used in the security field. They are essential for monitoring security in an organization because they enhance efficiency by automating tasks. Although we're only introducing these concepts and tools at this point, later in the program, you'll have opportunities to use them in a variety of hands-on activities.

Chào mừng đến với mô-module 4

Chào mừng bạn đến với phần cuối cùng của khóa học này! Ở đây chúng tôi sẽ giới thiệu các công cụ và các ngôn ngữ lập trình được thường được sử dụng trong lĩnh vực an ninh. Chúng rất cần thiết cho việc giám sát an ninh trong một tổ chức vì chúng nâng cao hiệu quả bằng cách tự động hóa các nhiệm vụ. Mặc dù chúng tôi chỉ giới thiệu những khái niệm và công cụ này vào thời điểm này, phần sau của chương trình, bạn sẽ có cơ hội sử dụng chúng trong nhiều hoạt động thực hành khác nhau.

In the following videos, you'll learn about security information and event management, or SIEM, tools. You'll also be introduced to other tools such as playbooks and network protocol analyzers.

Trong các video tiếp theo, bạn sẽ tìm hiểu về thông tin bảo mật và công cụ quản lý sự kiện hoặc SIEM. Bạn cũng sẽ được giới thiệu các công cụ khác như playbook và máy phân tích giao thức mạng.

Then, you'll learn about the Linux operating system and security-related tasks that are initiated through programming languages, such as SQL and Python.

Sau đó, bạn sẽ tìm hiểu về hệ điều hành Linux và các nhiệm vụ liên quan đến bảo mật được bắt đầu thông qua ngôn ngữ lập trình như SQL và Python.

For me, SQL is one of the most useful tools. It allows me to explore all the different data sources we collect, and it allows my team to analyze the data for trends.

Đối với tôi, SQL là một trong những công cụ hữu ích nhất. Nó cho phép tôi khám phá tất cả các nguồn dữ liệu khác nhau mà chúng tôi thu thập, và nó cho phép nhóm của tôi phân tích dữ liệu để tìm xu hướng.

Take your time going through the videos and if you need to, re-watch them. Also know that these tools will be discussed in much more detail, and you will be able to practice them firsthand, later in the certificate program.

Hãy dành thời gian xem qua các video và nếu bạn cần, hãy xem lại chúng. Cũng biết rằng những công cụ này sẽ được thảo luận chi tiết hơn nhiều, và bạn sẽ có thể thực hành chúng trực tiếp, sau này trong chương trình chứng chỉ.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

While every organization has their own set of tools and training materials that you'll learn to use on the job, this program will provide you with foundational knowledge that will help you succeed in the security industry. Let's get started!

Mặc dù mỗi tổ chức đều có bộ công cụ và tài liệu đào tạo mà bạn sẽ học cách sử dụng trong công việc, chương trình này sẽ cung cấp cho bạn với kiến thức nền tảng sẽ giúp bạn thành công trong ngành bảo mật. Bắt đầu nào!

1.2. Common cybersecurity tools – Các công cụ an ninh mạng phổ biến

Common cybersecurity tools

As mentioned earlier, security is like preparing for a storm. If you identify a leak, the color or shape of the bucket you use to catch the water doesn't matter. What is important is mitigating the risks and threats to your home, by using the tools available to you.

Như đã đề cập trước đây, an ninh giống như chuẩn bị cho một cơn bão. Nếu bạn xác định được rò rỉ, màu sắc hoặc hình dạng của xô bạn dùng để hứng nước không thành vấn đề. Điều quan trọng là giảm thiểu rủi ro và mối đe dọa đối với ngôi nhà của bạn, bằng cách sử dụng các công cụ có sẵn cho bạn.

As an entry-level security analyst, you'll have a lot of tools in your toolkit that you can use to mitigate potential risks.

Là một nhà phân tích bảo mật cấp đầu vào, bạn sẽ có rất nhiều công cụ trong bộ công cụ của bạn mà bạn có thể sử dụng để giảm thiểu rủi ro tiềm ẩn.

In this video, we'll discuss the primary purposes and functions of some commonly used security tools. And later in the program, you'll have hands-on opportunities to practice using them. Before discussing tools further, let's briefly discuss logs, which are the source of data that the tools we'll cover are designed to organize.

Trong video này, chúng ta sẽ thảo luận mục đích và chức năng chính của một số công cụ bảo mật thường được sử dụng. Và sau đó trong chương trình, bạn sẽ có cơ hội thực hành để thực hành sử dụng chúng. Trước khi thảo luận thêm về các công cụ, hãy thảo luận ngắn gọn về nhật ký, đó là nguồn dữ liệu các công cụ chúng tôi sẽ đề cập đến được thiết kế để sắp xếp.

A log is a record of events that occur within an organization's systems. Examples of security-related logs include records of employees signing into their computers or accessing web-based services. Logs help security professionals identify vulnerabilities and potential security breaches.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Nhật ký là bản ghi lại các sự kiện xảy ra trong hệ thống của một tổ chức. Ví dụ về nhật ký liên quan đến bảo mật bao gồm hồ sơ về nhân viên đăng nhập vào máy tính của họ hoặc truy cập các dịch vụ dựa trên web. Nhật ký giúp các chuyên gia bảo mật xác định các lỗ hổng bảo mật và các lỗ hổng bảo mật tiềm ẩn.

The first tools we'll discuss are security information and event management tools, or SIEM tools. A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. The acronym S-I-E-M may be pronounced as 'sim' or 'seem', but we'll use 'sim' throughout this program. SIEM tools collect real-time, or instant, information, and allow security analysts to identify potential breaches as they happen.

Các công cụ đầu tiên chúng ta sẽ thảo luận là thông tin bảo mật và công cụ quản lý sự kiện, hoặc công cụ SIEM. Công cụ SIEM là một ứng dụng thu thập và phân tích dữ liệu nhật ký để theo dõi những hoạt động quan trọng trong một tổ chức. Từ viết tắt SIEM có thể được phát âm là 'sim' hoặc 'có vẻ', nhưng chúng ta sẽ sử dụng 'sim' trong suốt chương trình này. Các công cụ SIEM thu thập thông tin theo thời gian thực hoặc tức thời, và cho phép các nhà phân tích bảo mật xác định các vi phạm tiềm năng khi chúng xảy ra.

Imagine having to read pages and pages of logs to determine if there are any security threats. Depending on the amount of data, it could take hours or days. SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of risks and threats. Next, let's go over examples of commonly used SIEM tools: Splunk and Chronicle.

Hãy tưởng tượng bạn phải đọc hết trang này đến trang khác của nhật ký để xác định xem có bất kỳ mối đe dọa bảo mật nào không. Tùy thuộc vào lượng dữ liệu, có thể mất hàng giờ hoặc hàng ngày. Các công cụ SIEM giảm lượng dữ liệu mà nhà phân tích phải xem xét bằng cách cung cấp thông báo cho loại rủi ro và mối đe dọa cụ thể. Tiếp theo, hãy xem qua các ví dụ về các công cụ SIEM thường được sử dụng: Splunk và Chronicle.

Splunk is a data analysis platform, and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data.

Splunk là một nền tảng phân tích dữ liệu, và Splunk Enterprise cung cấp giải pháp SIEM. Splunk Enterprise là một công cụ lưu trữ được sử dụng để lưu giữ, phân tích và tìm kiếm dữ liệu nhật ký của tổ chức.

Another SIEM tool is Google's Chronicle. Chronicle is a cloud-native SIEM tool that stores security data for search and analysis. Cloud-native means that Chronicle allows for fast delivery of new features.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Một công cụ SIEM khác là Chronicle của Google. Chronicle là một công cụ SIEM dựa trên nền tảng đám mây lưu trữ dữ liệu bảo mật để tìm kiếm và phân tích. Cloud-native có nghĩa là Chronicle cho phép cung cấp nhanh chóng các tính năng mới.

Both of these SIEM tools, and SIEMs in general, collect data from multiple places, then analyze and filter that data to allow security teams to prevent and quickly react to potential security threats.

Cả hai công cụ SIEM này và SIEM nói chung đều thu thập dữ liệu từ nhiều nơi, sau đó phân tích và lọc dữ liệu đó để cho phép đội an ninh ngăn chặn và nhanh chóng phản ứng với các mối đe dọa an ninh tiềm ẩn.

As a security analyst, you may find yourself using SIEM tools to analyze filtered events and patterns, perform incident analysis, or proactively search for threats. Depending on your organization's SIEM setup and risk focus, the tools and how they function may differ, but ultimately, they are all used to mitigate risk.

Là một nhà phân tích chứng khoán, bạn có thể thấy mình đang sử dụng các công cụ SIEM để phân tích các sự kiện và mẫu được lọc, thực hiện phân tích sự cố, hoặc chủ động tìm kiếm các mối đe dọa. Tùy thuộc vào thiết lập SIEM và trọng tâm rủi ro của tổ chức bạn, các công cụ và cách chúng hoạt động có thể khác nhau, nhưng cuối cùng, tất cả chúng đều được sử dụng để giảm thiểu rủi ro.

Other key tools that you will use in your role as a security analyst, and that you'll have hands-on opportunities to use later in the program, are playbooks and network protocol analyzers.

Các công cụ quan trọng khác mà bạn sẽ sử dụng trong vai trò của bạn là một nhà phân tích bảo mật, và bạn sẽ được thực hành cơ hội sử dụng sau này trong chương trình, là các sổ tay và bộ phân tích giao thức mạng.

A playbook is a manual that provides details about any operational action, such as how to respond to an incident. Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred. Playbooks can pertain to security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end.

Playbook là một cuốn sách hướng dẫn cung cấp thông tin chi tiết về bất kỳ hành động vận hành nào, chẳng hạn như cách ứng phó với một sự cố. Playbook, khác nhau tùy theo từng tổ chức, hướng dẫn các nhà phân tích cách xử lý sự cố an ninh trước đó, trong và sau khi nó xảy ra. Playbook có thể liên quan đến bảo mật hoặc đánh giá tuân thủ, quản lý quyền truy cập, và nhiều nhiệm vụ tổ chức khác yêu cầu một quá trình được ghi lại từ đầu đến cuối.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Another tool you may use as a security analyst is a network protocol analyzer, also called packet sniffer. A packet sniffer is a tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include tcpdump and Wireshark.

Một công cụ khác bạn có thể sử dụng như nhà phân tích bảo mật là người phân tích giao thức mạng, còn được gọi là gói sniffer. Trình nghe lén gói tin là một công cụ được thiết kế để thu thập và phân tích lưu lượng dữ liệu trong mạng. Máy phân tích giao thức mạng phổ biến bao gồm tcpdump và Wireshark.

As an entry-level analyst, you don't have to be an expert in these tools. As you continue through this certificate program and get more hands-on practice, you'll continuously build your understanding of how to use these tools to identify, assess, and mitigate risks.

Là một nhà phân tích cấp đầu vào, bạn không cần phải là chuyên gia về những công cụ này. Khi bạn tiếp tục đi qua chương trình chứng chỉ này và được thực hành thực hành nhiều hơn, bạn sẽ liên tục xây dựng sự hiểu biết của mình về cách sử dụng những công cụ này để xác định, đánh giá, giảm thiểu rủi ro.

1.3. Tools for protecting business operations – Công cụ bảo vệ hoạt động kinh doanh

Tools for protecting business operations

Previously, you were introduced to several technical skills that security analysts need to develop. You were also introduced to some tools entry-level security analysts may have in their toolkit. In this reading, you'll learn more about how technical skills and tools help security analysts mitigate risks.

Công cụ bảo vệ hoạt động kinh doanh

Trước đây, bạn đã được giới thiệu một số kỹ năng kỹ thuật mà các nhà phân tích bảo mật cần phát triển. Bạn cũng đã được giới thiệu một số công cụ mà các nhà phân tích bảo mật cấp đầu vào có thể có trong bộ công cụ của họ. Trong bài đọc này, bạn sẽ tìm hiểu thêm về cách các kỹ năng và công cụ kỹ thuật giúp các nhà phân tích bảo mật giảm thiểu rủi ro.

An entry-level analyst's toolkit

Every organization may provide a different toolkit, depending on its security needs. As a future analyst, it's important that you are familiar with industry standard tools and can demonstrate your ability to learn how to use similar tools in a potential workplace.

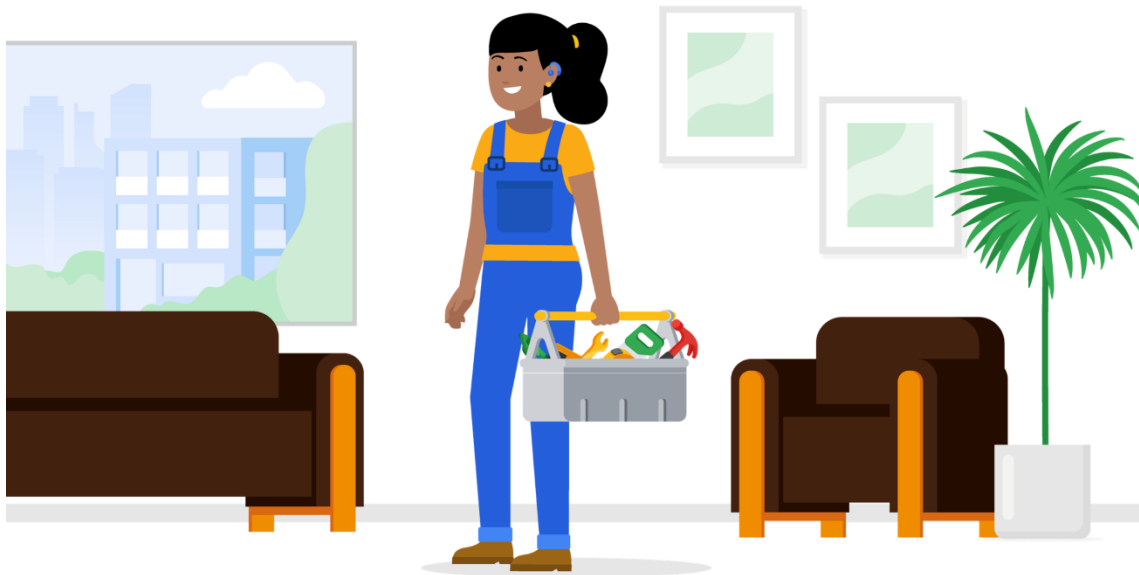
Bộ công cụ dành cho nhà phân tích cấp đầu vào

Mỗi tổ chức có thể cung cấp một bộ công cụ khác nhau, tùy thuộc vào nhu cầu bảo mật của tổ chức đó. Là một nhà phân tích trong tương lai, điều quan trọng

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

là bạn phải quen thuộc với các công cụ tiêu chuẩn ngành và có thể chứng minh khả năng học cách sử dụng các công cụ tương tự ở nơi làm việc tiềm năng.



Security information and event management (SIEM) tools

A **SIEM tool** is an application that collects and analyzes log data to monitor critical activities in an organization. A **log** is a record of events that occur within an organization's systems. Depending on the amount of data you're working with, it could take hours or days to filter through log data on your own. SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of threats, risks, and vulnerabilities.

SIEM tools provide a series of dashboards that visually organize data into categories, allowing users to select the data they wish to analyze. Different SIEM tools have different dashboard types that display the information you have access to.

SIEM tools also come with different hosting options, including on-premise and cloud. Organizations may choose one hosting option over another based on a security team member's expertise. For example, because a cloud-hosted version tends to be easier to set up, use, and maintain than an on-premise version, a less experienced security team may choose this option for their organization.

Công cụ quản lý sự kiện và thông tin bảo mật (SIEM)

Công cụ **SIEM** là một ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng trong một tổ chức. Nhật **ký** là bản ghi các sự kiện xảy ra trong hệ thống của tổ chức. Tùy thuộc vào lượng dữ liệu bạn đang làm việc, có thể mất hàng giờ hoặc vài ngày để tự lọc dữ liệu nhật ký. Các công cụ

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

SIEM giảm lượng dữ liệu mà nhà phân tích phải xem xét bằng cách đưa ra cảnh báo về các loại mối đe dọa, rủi ro và lỗ hổng cụ thể.

Các công cụ SIEM cung cấp một loạt trang tổng quan giúp sắp xếp dữ liệu thành các danh mục một cách trực quan, cho phép người dùng chọn dữ liệu họ muốn phân tích. Các công cụ SIEM khác nhau có các loại bảng thông tin khác nhau hiển thị thông tin bạn có quyền truy cập.

Các công cụ SIEM cũng đi kèm với các tùy chọn lưu trữ khác nhau, bao gồm cả tại chỗ và trên nền tảng đám mây. Các tổ chức có thể chọn tùy chọn lưu trữ này thay vì tùy chọn lưu trữ khác dựa trên chuyên môn của thành viên nhóm bảo mật. Ví dụ: vì phiên bản được lưu trữ trên đám mây có xu hướng dễ thiết lập, sử dụng và bảo trì hơn phiên bản tại chỗ nên nhóm bảo mật ít kinh nghiệm hơn có thể chọn tùy chọn này cho tổ chức của họ.

Network protocol analyzers (packet sniffers)

A **network protocol analyzer**, also known as a **packet sniffer**, is a tool designed to capture and analyze data traffic in a network. This means that the tool keeps a record of all the data that a computer within an organization's network encounters. Later in the program, you'll have an opportunity to practice using some common network protocol analyzer (packet sniffer) tools.

Máy phân tích giao thức mạng (bộ phân tích gói)

Trình **phân tích giao thức mạng**, còn được gọi là **trình thám thính gói**, là một công cụ được thiết kế để nắm bắt và phân tích lưu lượng dữ liệu trong mạng. Điều này có nghĩa là công cụ này lưu giữ bản ghi tất cả dữ liệu mà máy tính trong mạng của tổ chức gặp phải. Ở phần sau của chương trình, bạn sẽ có cơ hội thực hành sử dụng một số công cụ phân tích giao thức mạng (bộ thu thập gói) phổ biến.

Playbooks

A **playbook** is a manual that provides details about any operational action, such as how to respond to a security incident. Organizations usually have multiple playbooks documenting processes and procedures for their teams to follow. Playbooks vary from one organization to the next, but they all have a similar purpose: To guide analysts through a series of steps to complete specific security-related tasks.

For example, consider the following scenario: You are working as a security analyst for an incident response firm. You are given a case involving a small medical practice that has suffered a security breach. Your job is to help with the forensic investigation and provide evidence to a cybersecurity insurance company. They will then use your investigative findings to determine whether the medical practice will receive their insurance payout.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

In this scenario, playbooks would outline the specific actions you need to take to conduct the investigation. Playbooks also help ensure that you are following proper protocols and procedures. When working on a forensic case, there are two playbooks you might follow:

- The first type of playbook you might consult is called the **chain of custody** playbook. Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. As a security analyst involved in a forensic analysis, you will work with the computer data that was breached. You and the forensic team will also need to document who, what, where, and why you have the collected evidence. The evidence is your responsibility while it is in your possession. Evidence must be kept safe and tracked. Every time evidence is moved, it should be reported. This allows all parties involved to know exactly where the evidence is at all times.
- The second playbook your team might use is called the **protecting and preserving evidence** playbook. Protecting and preserving evidence is the process of properly working with fragile and volatile digital evidence. As a security analyst, understanding what fragile and volatile digital evidence is, along with why there is a procedure, is critical. As you follow this playbook, you will consult the **order of volatility**, which is a sequence outlining the order of data that must be preserved from first to last. It prioritizes volatile data, which is data that may be lost if the device in question powers off, regardless of the reason. While conducting an investigation, improper management of digital evidence can compromise and alter that evidence. When evidence is improperly managed during an investigation, it can no longer be used. For this reason, the first priority in any investigation is to properly preserve the data. You can preserve the data by making copies and conducting your investigation using those copies.

Playbooks

Cẩm **nang** là một cẩm nang cung cấp thông tin chi tiết về mọi hành động vận hành, chẳng hạn như cách ứng phó với sự cố bảo mật. Các tổ chức thường có nhiều sổ tay ghi lại các quy trình và thủ tục để nhóm của họ tuân theo. Sách hướng dẫn của mỗi tổ chức có thể khác nhau nhưng tất cả đều có mục đích giống nhau: Hướng dẫn các nhà phân tích thực hiện một loạt các bước để hoàn thành các nhiệm vụ cụ thể liên quan đến bảo mật.

Ví dụ: hãy xem xét tình huống sau: Bạn đang làm nhà phân tích bảo mật cho một công ty ứng phó sự cố. Bạn được giao một vụ việc liên quan đến một cơ sở y tế nhỏ đã bị vi phạm an ninh. Công việc của bạn là hỗ trợ điều tra pháp y và cung cấp bằng chứng cho một công ty bảo hiểm an ninh mạng. Sau đó, họ sẽ sử dụng kết quả điều tra của bạn để xác định xem cơ sở y tế có nhận được khoản thanh toán bảo hiểm của họ hay không.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Trong trường hợp này, cẩm nang sẽ phác thảo những hành động cụ thể mà bạn cần thực hiện để tiến hành điều tra. Sách hướng dẫn cũng giúp đảm bảo rằng bạn đang tuân theo các giao thức và quy trình phù hợp. Khi giải quyết một vụ án pháp y, có hai cuốn sách bạn có thể làm theo:

- Loại cẩm nang đầu tiên bạn có thể tham khảo được gọi là cẩm **nang về chuỗi quyền giám hộ**. Chuỗi hành trình sản phẩm là quá trình ghi lại việc sở hữu và kiểm soát bằng chứng trong suốt vòng đời của sự cố. Với tư cách là nhà phân tích bảo mật tham gia phân tích điều tra, bạn sẽ làm việc với dữ liệu máy tính đã bị vi phạm. Bạn và nhóm pháp y cũng sẽ cần ghi lại ai, cái gì, ở đâu và tại sao bạn có bằng chứng thu thập được. Bằng chứng là trách nhiệm của bạn khi nó thuộc quyền sở hữu của bạn. Bằng chứng phải được giữ an toàn và theo dõi. Mỗi lần bằng chứng được di chuyển, nó phải được báo cáo. Điều này cho phép tất cả các bên liên quan biết chính xác bằng chứng ở đâu vào mọi lúc.
- Cẩm nang thứ hai mà nhóm của bạn có thể sử dụng được gọi là cẩm nang **bảo vệ và bảo quản bằng chứng**. Bảo vệ và lưu giữ bằng chứng là quá trình xử lý hợp lý các bằng chứng kỹ thuật số dễ vỡ và dễ thay đổi. Với tư cách là một nhà phân tích bảo mật, việc hiểu rõ bằng chứng kỹ thuật số dễ vỡ và dễ biến động là gì, cùng với lý do tại sao cần có một quy trình, là rất quan trọng. Khi làm theo cẩm nang này, bạn sẽ tham khảo thứ **tự biến động**, là một trình tự phác thảo thứ tự dữ liệu phải được lưu giữ từ đầu đến cuối. Nó ưu tiên dữ liệu dễ thay đổi, là dữ liệu có thể bị mất nếu thiết bị được đề cập tắt nguồn, bất kể lý do. Trong khi tiến hành điều tra, việc quản lý bằng chứng kỹ thuật số không đúng cách có thể làm tổn hại và thay đổi bằng chứng đó. Khi bằng chứng được quản lý không đúng cách trong quá trình điều tra, nó sẽ không thể được sử dụng nữa. Vì lý do này, ưu tiên hàng đầu trong bất kỳ cuộc điều tra nào là bảo quản dữ liệu đúng cách. Bạn có thể bảo toàn dữ liệu bằng cách tạo các bản sao và tiến hành điều tra bằng cách sử dụng các bản sao đó.

Key takeaways

In this reading, you learned about a few tools a security analyst may have in their toolkit, depending on where they work. You also explored two important types of playbooks: chain of custody and protecting and preserving evidence. However, these are only two procedures that occur at the beginning of a forensic investigation. If forensic investigations interest you, you are encouraged to further explore this career path or security practice. In the process, you may learn about forensic tools that you want to add to your toolkit. While all of the forensic components that make up an investigation will not be covered in this certificate program, some forensic concepts will be discussed in later courses.

Bài học chính

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Trong bài đọc này, bạn đã tìm hiểu về một số công cụ mà nhà phân tích bảo mật có thể có trong bộ công cụ của họ, tùy thuộc vào nơi họ làm việc. Bạn cũng đã khám phá hai loại sách vở quan trọng: chuỗi hành trình sản phẩm và bảo vệ và bảo quản bằng chứng. Tuy nhiên, đây chỉ là hai thủ tục xảy ra khi bắt đầu cuộc điều tra pháp y. Nếu các cuộc điều tra pháp y khiến bạn quan tâm, bạn được khuyến khích khám phá thêm về con đường sự nghiệp hoặc hoạt động bảo mật này. Trong quá trình này, bạn có thể tìm hiểu về các công cụ pháp y mà bạn muốn thêm vào bộ công cụ của mình. Mặc dù tất cả các thành phần pháp y tạo nên một cuộc điều tra sẽ không được đề cập trong chương trình chứng chỉ này, nhưng một số khái niệm pháp y sẽ được thảo luận trong các khóa học sau.

Resources for more information

The Google Cybersecurity Action Team's [Threat Horizon Report](#) provides strategic intelligence for dealing with threats to cloud enterprise.

The Cybersecurity & Infrastructure Security Agency (CISA) has a list of [Free Cybersecurity Services and Tools](#). Review the list to learn more about open-source cybersecurity tools.

Tài nguyên để biết thêm thông tin

Nhóm hành động an ninh mạng của Google [Báo cáo chân trời mối đe dọa](#) cung cấp thông tin chiến lược để đối phó với các mối đe dọa đối với doanh nghiệp trên nền tảng đám mây.

Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) có một danh sách [Các công cụ và dịch vụ an ninh mạng miễn phí](#). Xem lại danh sách để tìm hiểu thêm về các công cụ an ninh mạng nguồn mở.

1.4. Explore: Tools and their purposes – Khám phá: Công cụ và mục đích của chúng

| Description | Tool |
|--|-----------|
| Application that collects and analyzes log data to monitor an organization's critical activities | SIEM tool |
| A manual that provides details about what actions to take | Playbook |
| A record of events that occur within an organization's systems | Log |
| A tool used to visually communicate information or data | Dashboard |

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

| Tình huống | Tool |
|---|-----------|
| Ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng của tổ chức | SIEM tool |
| Hướng dẫn cung cấp chi tiết về những hành động cần thực hiện | Playbook |
| Bản ghi các sự kiện xảy ra trong hệ thống của tổ chức | Log |
| Một công cụ được sử dụng để truyền đạt thông tin hoặc dữ liệu một cách | Dashboard |

1.5. Test your knowledge: Important cybersecurity tools – Kiểm tra kiến thức của bạn: Các công cụ an ninh mạng quan trọng

2. Core cybersecurity knowledge and skills – Kiến thức và kỹ năng an ninh mạng cốt lõi

2.1. Introduction to Linux, SQL, and Python – Giới thiệu về Linux, SQL và Python

Introduction to Linux, SQL, and Python

As we discussed previously, organizations use a variety of tools, such as SIEMs, playbooks, and packet sniffers to better manage, monitor, and analyze security threats. But those aren't the only tools in an analyst's toolkit. Analysts also use programming languages and operating systems to accomplish essential tasks.

Giới thiệu về Linux, SQL và Python

Như chúng ta đã thảo luận trước đây, các tổ chức sử dụng nhiều công cụ khác nhau, chẳng hạn như SIEM, playbook và trình nghe lén gói để quản lý tốt hơn, theo dõi và phân tích các mối đe dọa bảo mật. Nhưng đó không phải là công cụ duy nhất trong bộ công cụ của nhà phân tích. Các nhà phân tích cũng sử dụng ngôn ngữ lập trình và hệ điều hành để thực hiện các nhiệm vụ thiết yếu.

In this video, we'll introduce you to Python and SQL programming, and the Linux operating system. All of which you'll have an opportunity to practice using later in the certificate program.

Trong video này, chúng tôi sẽ giới thiệu cho bạn về Python và Lập trình SQL và hệ điều hành Linux. Tất cả những điều đó bạn sẽ có cơ hội thực hành sử dụng sau này trong chương trình chứng chỉ.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Organizations can use programming to create a specific set of instructions for a computer to execute tasks. Programming allows analysts to complete repetitive tasks and processes with a high degree of accuracy and efficiency. It also helps reduce the risk of human error, and can save hours or days compared to performing the work manually. Now that you're aware of what programming languages are used for, let's discuss a specific and related operating system called Linux, and two programming languages: SQL and Python.

Các tổ chức có thể sử dụng lập trình để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ. Lập trình cho phép các nhà phân tích hoàn thành các nhiệm vụ lặp đi lặp lại và các quy trình có độ chính xác và hiệu quả cao. Nó cũng giúp giảm nguy cơ lỗi của con người và có thể tiết kiệm giờ hoặc ngày so với việc thực hiện công việc một cách thủ công. Bây giờ bạn đã biết những gì ngôn ngữ lập trình được sử dụng cho, hãy thảo luận một hệ điều hành cụ thể và có liên quan được gọi là Linux và hai ngôn ngữ lập trình: SQL và Python.

Linux is an open-source, or publicly available, operating system. Unlike other operating systems you may be familiar with, for example MacOS or Windows, Linux relies on a command line as the primary user interface. Linux itself is not a programming language, but it does allow for the use of text-based commands between the user and the operating system. You'll learn more about Linux later in the program.

Linux là một mã nguồn mở, hoặc hệ điều hành có sẵn công khai. Không giống như các hệ điều hành khác mà bạn có thể quen thuộc, ví dụ như MacOS hoặc Windows, Linux dựa vào dòng lệnh làm giao diện người dùng chính. Bản thân Linux không phải là ngôn ngữ lập trình, nhưng nó cho phép sử dụng lệnh dựa trên văn bản giữa người dùng và hệ điều hành. Bạn sẽ tìm hiểu thêm về Linux sau này trong chương trình.

A common use of Linux for entry-level security analysts is examining logs to better understand what's occurring in a system. For example, you might find yourself using commands to review an error log when investigating uncommonly high network traffic.

Việc sử dụng Linux phổ biến cho các nhà phân tích bảo mật cấp đầu vào là kiểm tra nhật ký để tốt hơn hiểu những gì đang xảy ra trong một hệ thống. Ví dụ, bạn có thể thấy mình sử dụng lệnh để xem lại nhật ký lỗi khi điều tra lưu lượng truy cập mạng cao bất thường.

Next, let's discuss SQL. SQL stands for Structured Query Language. SQL is a programming language used to create, interact with, and request information from a database. A database is an organized collection of information or data. There may be millions of data points in a database. So an entry-level security analyst would use SQL to filter through the data points to retrieve specific information.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Tiếp theo, hãy thảo luận về SQL. SQL là viết tắt của Ngôn ngữ truy vấn có cấu trúc. SQL là ngôn ngữ lập trình được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu. Cơ sở dữ liệu là một bộ sưu tập có tổ chức của thông tin hoặc dữ liệu. Có thể có hàng triệu điểm dữ liệu trong cơ sở dữ liệu. Vì vậy, một nhà phân tích bảo mật cấp đầu vào sẽ sử dụng SQL để lọc qua các điểm dữ liệu để lấy thông tin cụ thể.

The last programming language we'll introduce is Python. Security professionals can use Python to perform tasks that are repetitive and time-consuming and that require a high level of detail and accuracy.

Ngôn ngữ lập trình cuối cùng chúng tôi sẽ giới thiệu là Python. Các chuyên gia bảo mật có thể sử dụng Python để thực hiện các tác vụ lặp đi lặp lại và tốn thời gian và điều đó đòi hỏi độ chi tiết và độ chính xác cao.

As a future analyst, it's important to understand that every organization's toolkit may be somewhat different based on their security needs. The main point is that you're familiar with some industry standard tools because that will show employers that you have the ability to learn how to use their tools to protect the organization and the people it serves.

Là một nhà phân tích tương lai, điều quan trọng là phải hiểu điều đó bộ công cụ của mọi tổ chức có thể hơi khác nhau dựa trên nhu cầu bảo mật của họ. Điểm chính là bạn đã quen thuộc với một số công cụ tiêu chuẩn ngành vì điều đó sẽ hiển thị khả năng tuyển dụng mà bạn có khả năng học cách sử dụng công cụ của họ để bảo vệ tổ chức và những người mà nó phục vụ.

You're doing great! Later in the course, you'll learn more about Linux and programming languages, and you'll practice using these tools in security-related scenarios.

Bạn đang làm rất tốt! Ở phần sau của khóa học, bạn sẽ tìm hiểu thêm về Linux và ngôn ngữ lập trình và bạn sẽ thực hành sử dụng các công cụ này trong các tình huống liên quan đến bảo mật.

2.2. Use tools to protect business operations – Sử dụng công cụ để bảo vệ hoạt động kinh doanh

Use tools to protect business operations

Previously, you were introduced to programming, operating systems, and tools commonly used by cybersecurity professionals. In this reading, you'll learn more about programming and operating systems, as well as other tools that entry-level analysts use to help protect organizations and the people they serve.

Sử dụng công cụ để bảo vệ hoạt động kinh doanh

Trước đây, bạn đã được giới thiệu về lập trình, hệ điều hành và các công cụ thường được các chuyên gia an ninh mạng sử dụng. Trong bài đọc này, bạn sẽ tìm hiểu thêm về

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

lập trình và hệ điều hành, cũng như các công cụ khác mà các nhà phân tích cấp cơ sở sử dụng để giúp bảo vệ các tổ chức và những người mà họ phục vụ.

Tools and their purposes

Công cụ và mục đích của chúng

Programming

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. Security analysts use programming languages, such as Python, to execute automation. **Automation** is the use of technology to reduce human and manual effort in performing common and repetitive tasks. Automation also helps reduce the risk of human error.

Another programming language used by analysts is called Structured Query Language (SQL). **SQL** is used to create, interact with, and request information from a database. A **database** is an organized collection of information or data. There can be millions of data points in a database. A **data point** is a specific piece of information.

Lập trình

Lập trình là một quá trình có thể được sử dụng để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ. Các nhà phân tích bảo mật sử dụng các ngôn ngữ lập trình, chẳng hạn như Python, để thực hiện tự động hóa. **Tự động hóa** là việc sử dụng công nghệ để giảm bớt nỗ lực của con người và thủ công trong việc thực hiện các nhiệm vụ thông thường và lặp đi lặp lại. Tự động hóa cũng giúp giảm nguy cơ lỗi của con người.

Một ngôn ngữ lập trình khác được các nhà phân tích sử dụng được gọi là Ngôn ngữ truy vấn có cấu trúc (SQL). **SQL** được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu. **Cơ sở dữ liệu** là một tập hợp thông tin hoặc dữ liệu có tổ chức. Có thể có hàng triệu điểm dữ liệu trong cơ sở dữ liệu. Điểm **dữ liệu** là một phần thông tin cụ thể.

Operating systems

An **operating system** is the interface between computer hardware and the user. Linux®, macOS®, and Windows are operating systems. They each offer different functionality and user experiences.

Previously, you were introduced to **Linux** as an open-source operating system. Open source means that the code is available to the public and allows people to make contributions to improve the software. Linux is not a programming language; however, it does involve the use of a command line within the operating system. A **command** is an instruction telling the computer to do something. A **command-line** interface is a text-based user interface that uses commands to interact with the computer. You will learn more about Linux, including the Linux kernel and GNU, in a later course.

Các hệ điều hành

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Hệ **điều hành** là giao diện giữa phần cứng máy tính và người dùng. Linux®, macOS® và Windows là các hệ điều hành. Mỗi loại đều cung cấp chức năng và trải nghiệm người dùng khác nhau.

Trước đây, bạn đã được làm quen với **Linux** như một hệ điều hành nguồn mở. Nguồn mở có nghĩa là mã có sẵn cho công chúng và cho phép mọi người đóng góp để cải thiện phần mềm. Linux không phải là ngôn ngữ lập trình; tuy nhiên, nó liên quan đến việc sử dụng dòng lệnh trong hệ điều hành. Lệnh là một lệnh yêu cầu máy **tính** làm một việc gì đó. Giao diện **dòng lệnh** là giao diện người dùng dựa trên văn bản sử dụng các lệnh để tương tác với máy tính. Bạn sẽ tìm hiểu thêm về Linux, bao gồm nhân Linux và GNU, trong khóa học sau.

Web vulnerability

A **web vulnerability** is a unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment.

To stay up-to-date on the most critical risks to web applications, review the [Open Web Application Security Project \(OWASP\) Top 10](#).

Lỗ hổng web

Lỗ hổng web là một lỗ hổng duy nhất trong ứng dụng web mà kẻ đe dọa có thể khai thác bằng cách sử dụng mã hoặc hành vi độc hại để cho phép truy cập trái phép, đánh cắp dữ liệu và triển khai phần mềm độc hại.

Để luôn cập nhật những rủi ro nghiêm trọng nhất đối với các ứng dụng web, hãy xem lại [Dự án bảo mật ứng dụng web mở \(OWASP\) Top 10](#).

Antivirus software

Antivirus software is a software program used to prevent, detect, and eliminate malware and viruses. It is also called anti-malware. Depending on the type of antivirus software, it can scan the memory of a device to find patterns that indicate the presence of malware.

Phần mềm diệt virus

Phần mềm chống vi-rút là một chương trình phần mềm được sử dụng để ngăn chặn, phát hiện và loại bỏ phần mềm độc hại và vi-rút. Nó còn được gọi là chống phần mềm độc hại. Tùy thuộc vào loại phần mềm chống vi-rút, nó có thể quét bộ nhớ của thiết bị để tìm các mẫu cho biết sự hiện diện của phần mềm độc hại.

Intrusion detection system

An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. The system scans and analyzes network packets, which carry small amounts of data through a network. The small amount of data makes the detection process easier for an IDS to identify potential threats to sensitive

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

data. Other occurrences an IDS might detect can include theft and unauthorized access.

Hệ thống phát hiện xâm nhập

Hệ thống phát hiện xâm nhập (IDS) là một ứng dụng giám sát hoạt động của hệ thống và cảnh báo về những xâm nhập có thể xảy ra. Hệ thống quét và phân tích các gói mạng, mang một lượng nhỏ dữ liệu qua mạng. Lượng dữ liệu nhỏ giúp quá trình phát hiện của IDS dễ dàng hơn trong việc xác định các mối đe dọa tiềm ẩn đối với dữ liệu nhạy cảm. Các trường hợp khác mà IDS có thể phát hiện có thể bao gồm trộm cắp và truy cập trái phép.

Encryption

Encryption makes data unreadable and difficult to decode for an unauthorized user; its main goal is to ensure confidentiality of private data. **Encryption** is the process of converting data from a readable format to a cryptographically encoded format.

Cryptographic encoding means converting plaintext into secure ciphertext.

Plaintext is unencrypted information and **secure ciphertext** is the result of encryption.

Note: Encoding and encryption serve different purposes. Encoding uses a public conversion algorithm to enable systems that use different data representations to share information.

Mã hóa

Mã hóa làm cho dữ liệu không thể đọc được và khó giải mã đối với người dùng trái phép; mục tiêu chính của nó là đảm bảo tính bảo mật của dữ liệu riêng tư. **Mã hóa** là quá trình chuyển đổi dữ liệu từ định dạng có thể đọc được sang định dạng được mã hóa bằng mật mã. **Mã hóa mật mã** có nghĩa là chuyển đổi bản rõ thành bản mã an toàn. **Bản rõ** là thông tin không được mã hóa và **bản mã an toàn** là kết quả của mã hóa.

Lưu ý: Mã hóa và mã hóa phục vụ các mục đích khác nhau. Mã hóa sử dụng thuật toán chuyển đổi công khai để cho phép các hệ thống sử dụng các cách trình bày dữ liệu khác nhau để chia sẻ thông tin.

Penetration testing

Penetration testing, also called pen testing, is the act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. It is a thorough risk assessment that can evaluate and identify external and internal threats as well as weaknesses.

Kiểm tra thâm nhập

Kiểm tra thâm nhập, còn gọi là kiểm tra bút, là hành động tham gia vào một cuộc tấn công mô phỏng giúp xác định các lỗ hổng trong hệ thống, mạng, trang web, ứng dụng và quy trình. Đó là một đánh giá rủi ro kỹ lưỡng có thể đánh giá và xác định các mối đe dọa bên ngoài và bên trong cũng như các điểm yếu.

Key takeaways

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

In this reading, you learned more about programming and operating systems. You were also introduced to several new tools and processes. Every organization selects their own set of tools. Therefore, the more tools you know, the more valuable you are to an organization. Tools help security analysts complete their tasks more efficiently and effectively.

Bài học chính

Trong bài đọc này, bạn đã tìm hiểu thêm về lập trình và hệ điều hành. Bạn cũng đã được giới thiệu một số công cụ và quy trình mới. Mỗi tổ chức chọn bộ công cụ của riêng mình. Do đó, bạn càng biết nhiều công cụ thì bạn càng có giá trị đối với tổ chức. Công cụ giúp các nhà phân tích bảo mật hoàn thành nhiệm vụ của mình hiệu quả và năng suất hơn.

2.3. Test your knowledge: Core cybersecurity knowledge and skills – Kiểm tra kiến thức của bạn: Kiến thức và kỹ năng cốt lõi về an ninh mạng

2.4. Create a cybersecurity portfolio – Tạo danh mục đầu tư an ninh mạng

Create a cybersecurity portfolio

Throughout this certificate program, you will have multiple opportunities to develop a professional cybersecurity portfolio to showcase your security skills and knowledge.

In this reading, you'll learn what a portfolio is and why it's important to develop a professional cybersecurity portfolio. You'll also learn about options for creating an online or self-hosted portfolio that you can share with potential employers when you begin to look for cybersecurity jobs.

Tạo danh mục đầu tư an ninh mạng

Trong suốt chương trình chứng chỉ này, bạn sẽ có nhiều cơ hội phát triển danh mục an ninh mạng chuyên nghiệp để thể hiện các kỹ năng và kiến thức về bảo mật của mình.

Trong bài đọc này, bạn sẽ tìm hiểu danh mục đầu tư là gì và tại sao việc phát triển danh mục đầu tư an ninh mạng chuyên nghiệp lại quan trọng. Bạn cũng sẽ tìm hiểu về các tùy chọn để tạo danh mục đầu tư trực tuyến hoặc tự lưu trữ mà bạn có thể chia sẻ với các nhà tuyển dụng tiềm năng khi bắt đầu tìm kiếm việc làm về an ninh mạng.

What is a portfolio, and why is it necessary?

Cybersecurity professionals use portfolios to demonstrate their security education, skills, and knowledge. Professionals typically use portfolios when they apply for jobs to show potential employers that they are passionate about their work and can do the job they are applying for. Portfolios are more in depth than a resume, which is typically a one-to-two page summary of relevant education, work experience, and accomplishments. You will have the opportunity to develop a resume, and finalize your portfolio, in the last course of this program.

Danh mục đầu tư là gì và tại sao nó cần thiết?

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Các chuyên gia an ninh mạng sử dụng danh mục đầu tư để thể hiện kiến thức, kỹ năng và kiến thức về bảo mật của họ. Các chuyên gia thường sử dụng danh mục đầu tư khi họ nộp đơn xin việc để cho các nhà tuyển dụng tiềm năng thấy rằng họ đam mê công việc và có thể làm được công việc mà họ đang ứng tuyển. Danh mục đầu tư có chiều sâu hơn sơ yếu lý lịch, thường là bản tóm tắt từ một đến hai trang về trình độ học vấn, kinh nghiệm làm việc và thành tích có liên quan. Bạn sẽ có cơ hội phát triển sơ yếu lý lịch và hoàn thiện danh mục đầu tư của mình trong khóa học cuối cùng của chương trình này.

Options for creating your portfolio

There are many ways to present a portfolio, including self-hosted and online options such as:

- Documents folder
- Google Drive or Dropbox™
- Google Sites
- Git repository

Các tùy chọn để tạo danh mục đầu tư của bạn

Có nhiều cách để trình bày portfolio, bao gồm các tùy chọn tự lưu trữ và trực tuyến như:

- Documents folder
- Google Drive hoặc Dropbox™
- Trang web Google
- Git repository

Option 1: Documents folder

Description: A documents folder is a folder created and saved to your computer's hard drive. You manage the folder, subfolders, documents, and images within it.

Document folders allow you to have direct access to your documentation. Ensuring that your professional documents, images, and other information are well organized can save you a lot of time when you're ready to apply for jobs. For example, you may want to create a main folder titled something like "Professional documents." Then, within your main folder, you could create subfolders with titles such as:

- Resume
- Education
- Portfolio documents
- Cybersecurity tools
- Programming

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Setup: Document folders can be created in multiple ways, depending on the type of computer you are using. If you're unsure about how to create a folder on your device, you can search the internet for instructional videos or documents related to the type of computer you use.

Tùy chọn 1: Thư mục tài liệu

Mô tả: Thư mục tài liệu là thư mục được tạo và lưu vào ổ cứng máy tính của bạn. Bạn quản lý thư mục, thư mục con, tài liệu và hình ảnh trong đó.

Thư mục tài liệu cho phép bạn có quyền truy cập trực tiếp vào tài liệu của mình. Việc đảm bảo rằng các tài liệu, hình ảnh chuyên nghiệp và thông tin khác của bạn được sắp xếp hợp lý có thể giúp bạn tiết kiệm rất nhiều thời gian khi sẵn sàng nộp đơn xin việc. Ví dụ: bạn có thể muốn tạo một thư mục chính có tiêu đề như “Tài liệu chuyên nghiệp”. Sau đó, trong thư mục chính, bạn có thể tạo các thư mục con có tiêu đề như:

- Bản tóm tắt
- Giáo dục
- Tài liệu danh mục đầu tư
- Công cụ an ninh mạng
- Lập trình

Thiết lập: Thư mục tài liệu có thể được tạo theo nhiều cách, tùy thuộc vào loại máy tính bạn đang sử dụng. Nếu không chắc chắn về cách tạo thư mục trên thiết bị của mình, bạn có thể tìm kiếm trên Internet các video hướng dẫn hoặc tài liệu liên quan đến loại máy tính bạn sử dụng.

Option 2: Google Drive or Dropbox

Description: Google Drive and Dropbox offer similar features that allow you to store your professional documentation on a cloud platform. Both options also have file-sharing features, so you can easily share your portfolio documents with potential employers. Any additions or changes you make to a document within that folder will be updated automatically for anyone with access to your portfolio.

Similar to a documents folder, keeping your Google Drive or Dropbox-based portfolio well organized will be helpful as you begin or progress through your career.

Setup: To learn how to upload and share files on these applications, visit the Google Drive and Dropbox websites for more information.

Tùy chọn 2: Google Drive hoặc Dropbox

Mô tả: Google Drive và Dropbox cung cấp các tính năng tương tự cho phép bạn lưu trữ tài liệu chuyên môn của mình trên nền tảng đám mây. Cả hai tùy chọn cũng có tính năng chia sẻ tệp, vì vậy bạn có thể dễ dàng chia sẻ tài liệu danh mục đầu tư của mình với các nhà tuyển dụng tiềm năng. Mọi bổ sung hoặc thay đổi bạn thực hiện đối với tài liệu trong thư mục đó sẽ được cập nhật tự động cho bất kỳ ai có quyền truy cập vào danh mục đầu tư của bạn.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Tương tự như thư mục tài liệu, việc sắp xếp tốt danh mục đầu tư dựa trên Google Drive hoặc Dropbox của bạn sẽ hữu ích khi bạn bắt đầu hoặc tiến bộ trong sự nghiệp của mình.

Thiết lập: Để tìm hiểu cách tải lên và chia sẻ tệp trên các ứng dụng này, hãy truy cập trang web Google Drive và Dropbox để biết thêm thông tin.

Option 3: Google Sites

Description: Google Sites and similar website hosting options have a variety of easy-to-use features to help you present your portfolio items, including customizable layouts, responsive webpages, embedded content capabilities, and web publishing.

Responsive webpages automatically adjust their content to fit a variety of devices and screen sizes. This is helpful because potential employers can review your content using any device and your media will display just as you intend. When you're ready, you can publish your website and receive a unique URL. You can add this link to your resume so hiring managers can easily access your work.

Setup: To learn how to create a website in Google Sites, visit the Google Sites website.

Tùy chọn 3: Trang web Google

Mô tả: Google Sites và các tùy chọn lưu trữ trang web tương tự có nhiều tính năng dễ sử dụng để giúp bạn trình bày các mục danh mục của mình, bao gồm bố cục có thể tùy chỉnh, trang web phản hồi, khả năng nội dung được nhúng và xuất bản web.

Các trang web đáp ứng tự động điều chỉnh nội dung của chúng để phù hợp với nhiều loại thiết bị và kích thước màn hình. Điều này rất hữu ích vì các nhà tuyển dụng tiềm năng có thể xem lại nội dung của bạn bằng bất kỳ thiết bị nào và phương tiện của bạn sẽ hiển thị đúng như bạn dự định. Khi đã sẵn sàng, bạn có thể xuất bản trang web của mình và nhận một URL duy nhất. Bạn có thể thêm liên kết này vào sơ yếu lý lịch của mình để người quản lý tuyển dụng có thể dễ dàng truy cập công việc của bạn.

Thiết lập: Để tìm hiểu cách tạo trang web trong Google Sites, hãy truy cập trang web Google Sites.

Option 4: Git repository

Description: A Git repository is a folder within a project. In this instance, the project is your portfolio, and you can use your repository to store the documents, labs, and screenshots you complete during each course of the certificate program. There are several Git repository sites you can use, including:

- GitLab
- Bitbucket™
- GitHub

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Each Git repository allows you to showcase your skills and knowledge in a customizable space. To create an online project portfolio on any of the repositories listed, you need to use a version of Markdown.

Setup: To learn about how to create a GitHub account and use Markdown, follow the steps outlined in the document [Get started with GitHub](#).

Tùy chọn 4: Kho Git

Mô tả: Kho lưu trữ Git là một thư mục trong một dự án. Trong trường hợp này, dự án là danh mục đầu tư của bạn và bạn có thể sử dụng kho lưu trữ của mình để lưu trữ tài liệu, phòng thí nghiệm và ảnh chụp màn hình mà bạn hoàn thành trong mỗi khóa học của chương trình chứng chỉ. Có một số trang lưu trữ Git mà bạn có thể sử dụng, bao gồm:

- GitLab
- Bitbucket™
- GitHub

Mỗi kho lưu trữ Git cho phép bạn thể hiện các kỹ năng và kiến thức của mình trong một không gian có thể tùy chỉnh. Để tạo danh mục dự án trực tuyến trên bất kỳ kho lưu trữ nào được liệt kê, bạn cần sử dụng phiên bản Markdown.

Thiết lập: Để tìm hiểu về cách tạo tài khoản GitHub và sử dụng Markdown, hãy làm theo các bước được nêu trong tài liệu [Bắt đầu với GitHub](#).

Portfolio projects

As previously mentioned, you will have multiple opportunities throughout the certificate program to develop items to include in your portfolio. These opportunities include:

- Drafting a professional statement
- Conducting a security audit
- Analyzing network structure and security
- Using Linux commands to manage file permissions
- Applying filters to SQL queries
- Identifying vulnerabilities for a small business
- Documenting incidents with an incident handler's journal
- Importing and parsing a text file in a security-related scenario
- Creating or revising a resume

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Note: Do not include any private, copyrighted, or proprietary documents in your portfolio. Also, if you use one of the sites described in this reading, keep your site set to “private” until it is finalized.

Dự án danh mục đầu tư

Như đã đề cập trước đó, bạn sẽ có nhiều cơ hội trong suốt chương trình chứng chỉ để phát triển các hạng mục để đưa vào danh mục đầu tư của mình. Những cơ hội này bao gồm:

- Soạn thảo một tuyên bố chuyên nghiệp
- Tiến hành kiểm tra an ninh
- Phân tích cấu trúc mạng và bảo mật
- Sử dụng lệnh Linux để quản lý quyền truy cập tệp
- Áp dụng bộ lọc cho truy vấn SQL
- Xác định lỗ hổng cho doanh nghiệp nhỏ
- Ghi lại sự cố bằng nhật ký của người xử lý sự cố
- Nhập và phân tích cú pháp tệp văn bản trong trường hợp liên quan đến bảo mật
- Tạo hoặc sửa đổi sơ yếu lý lịch

Lưu ý: Không đưa bất kỳ tài liệu riêng tư, có bản quyền hoặc độc quyền nào vào danh mục đầu tư của bạn. Ngoài ra, nếu bạn sử dụng một trong các trang web được mô tả trong bài đọc này, hãy đặt trang web của bạn ở chế độ “riêng tư” cho đến khi hoàn tất.

Key takeaways

Now that you’re aware of some options for creating and hosting a professional portfolio, you can consider these as you develop items for your portfolio throughout the certificate program. The more proactive you are about creating a polished portfolio, the higher your chances of impressing a potential employer and obtaining a new job opportunity in the cybersecurity profession.

Bài học chính

Bây giờ bạn đã biết về một số tùy chọn để tạo và lưu trữ danh mục đầu tư chuyên nghiệp, bạn có thể xem xét những tùy chọn này khi phát triển các mục cho danh mục đầu tư của mình trong suốt chương trình chứng chỉ. Bạn càng chủ động tạo ra một danh mục đầu tư bóng bẩy thì bạn càng có cơ hội gây ấn tượng với nhà tuyển dụng tiềm năng và có được cơ hội việc làm mới trong ngành an ninh mạng.

2.5. Portfolio Activity: Draft a professional statement – Hoạt động danh mục đầu tư: Soạn thảo một tuyên bố chuyên nghiệp

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

2.6. Portfolio Activity Exemplar: Draft a professional statement – Ví dụ về hoạt động danh mục đầu tư: Dự thảo một tuyên bố chuyên nghiệp

3. Review: Cybersecurity tools and programming languages – Đánh giá: Các công cụ an ninh mạng và ngôn ngữ lập trình

3.1. Wrap-up – Gợi lại

Wrap-up

That completes the introduction to security tools and programming languages!

Gợi lại

Vậy là đã hoàn tất phần giới thiệu về các công cụ bảo mật và ngôn ngữ lập trình!

In this section of the course, we covered SIEM tools such as Splunk and Chronicle. We also discussed how SIEM tools are used by security analysts to complete different tasks.

Trong phần này của khóa học, chúng tôi đã đề cập đến các công cụ SIEM như Splunk và Chronicle. Chúng tôi cũng thảo luận về cách các nhà phân tích bảo mật sử dụng các công cụ SIEM để hoàn thành nhiệm vụ khác nhau.

Then, we discussed other tools such as playbooks and network protocol analyzers, also called packet sniffers.

Sau đó, chúng tôi thảo luận về các công cụ khác như sách hướng dẫn và máy phân tích giao thức mạng, còn được gọi là bộ dò tìm gói.

Finally, we introduced the Linux operating system and the programming languages SQL and Python.

Cuối cùng, chúng tôi đã giới thiệu hệ điều hành Linux và các ngôn ngữ lập trình SQL và Python.

Remember, the tools we discussed take time to understand completely. But having a basic understanding of these tools can help you get a job in the security field and progress in your career!

Hãy nhớ rằng, các công cụ chúng ta đã thảo luận cần có thời gian để hiểu hoàn toàn. Nhưng hiểu biết cơ bản về những công cụ này có thể giúp bạn có được một công việc trong lĩnh vực an ninh và thăng tiến trong sự nghiệp của bạn!

3.2. Glossary terms from module 4 – Thuật ngữ trong phần 4

Glossary terms from module 4

Terms and definitions from Course 1, Module 4

Thuật ngữ trong học phần 4

Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 4

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Phần mềm chống vi-rút: Một chương trình phần mềm được sử dụng để ngăn chặn, phát hiện và loại bỏ phần mềm độc hại và vi-rút

Database: An organized collection of information or data

Cơ sở dữ liệu: Một tập hợp thông tin hoặc dữ liệu có tổ chức

Data point: A specific piece of information

Điểm dữ liệu: Một phần thông tin cụ thể

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

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

Linux: An open-source operating system

Linux: Một hệ điều hành nguồn mở

Log: A record of events that occur within an organization's systems

Nhật ký: Bản ghi các sự kiện xảy ra trong hệ thống của tổ chức

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network

Trình phân tích giao thức mạng (trình thám thính gói): Một công cụ được thiết kế để thu thập và phân tích lưu lượng dữ liệu trong mạng

Order of volatility: A sequence outlining the order of data that must be preserved from first to last

Thứ tự biến động: Trình tự phác thảo thứ tự dữ liệu phải được bảo toàn từ đầu đến cuối

Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks

Lập trình: Một quy trình có thể được sử dụng để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ

Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence

Bảo vệ và lưu giữ bằng chứng: Quá trình xử lý đúng đắn các bằng chứng kỹ thuật số dễ vỡ và dễ thay đổi

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

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

Quản lý sự kiện và thông tin bảo mật (SIEM) : Ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng trong một tổ chức

SQL (Structured Query Language): A query language used to create, interact with, and request information from a database

SQL (Ngôn ngữ truy vấn có cấu trúc): Ngôn ngữ truy vấn được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu

3.3. Module 4 challenge – Thử thách module 4

4. Congratulations on completing Course 1! – Chúc mừng bạn đã hoàn thành Khóa 1!

4.1. Course wrap-up – Tóm tắt khóa học

Course wrap-up

Congratulations on completing the first course! We've come so far and covered so much about a really exciting industry.

Tóm tắt khóa học

Congratulations on completing the first course! We've come so far and covered so much about a really exciting industry.

I find cybersecurity to be exciting because it's dynamic. There are always new puzzles to solve, and the work of protecting our users is worthwhile.

Tôi thấy an ninh mạng rất thú vị vì nó năng động. Luôn có những câu đố mới để giải và công việc bảo vệ người dùng của chúng tôi là đáng giá.

Before we move on, let's take a moment to celebrate and reflect on what we've covered. First, we introduced core security concepts, including what security is and why it matters. We also discussed what an entry-level security analyst does and some skills related to the role.

Trước khi tiếp tục, chúng ta hãy dành một chút thời gian để ăn mừng và suy ngẫm về những gì chúng tôi đã đề cập. Đầu tiên, chúng tôi giới thiệu các khái niệm bảo mật cốt lõi, bao gồm bảo mật là gì và tại sao nó quan trọng. Chúng tôi cũng đã thảo luận về những gì một nhà phân tích bảo mật cấp đầu vào làm và một số kỹ năng liên quan đến vai trò.

Then, we transitioned to eight security domains, which include security and risk management, asset security, and security operations.

Sau đó, chúng tôi chuyển sang tám miền bảo mật, bao gồm bảo mật và quản lý rủi ro, bảo đảm tài sản và hoạt động bảo đảm.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

Next, we highlighted security frameworks and controls. Specifically, the CIA triad model and the NIST Cybersecurity Framework.

Tiếp theo, chúng tôi nêu bật các khuôn khổ và biện pháp kiểm soát bảo mật. Cụ thể, mô hình bộ ba của CIA và Khung an ninh mạng NIST.

Finally, we explored common tools and programming languages used by security analysts, such as SIEMs, playbooks, SQL, and Python.

Cuối cùng, chúng tôi khám phá các công cụ phổ biến và ngôn ngữ lập trình được sử dụng bởi các nhà phân tích bảo mật, chẳng hạn như SIEM, sách hướng dẫn, SQL và Python.

I hope you're proud of the work you've done so far. No matter what direction you take in the security industry, everything you've learned lays the foundation for the next phase of your career. And, as you move through this program, you'll have the chance to develop your skills further.

Tôi hy vọng bạn tự hào về công việc bạn đã làm cho đến nay. Bất kể hướng nào bạn tham gia vào ngành an ninh, mọi thứ bạn đã học đều nằm ở đó nền tảng cho giai đoạn tiếp theo trong sự nghiệp của bạn. Và khi bạn chuyển qua chương trình này, bạn sẽ có cơ hội phát triển kỹ năng của mình hơn nữa.

In the next course, we'll provide more details about several of the topics introduced in this course.

Trong khóa học tiếp theo, chúng tôi sẽ cung cấp thêm chi tiết về một số chủ đề được giới thiệu trong khóa học này.

Hi, I'm Ashley, and I will be guiding you through the next course of this certificate program. We'll discuss security domains and business operations in greater detail.

Xin chào, tôi là Ashley và tôi sẽ hướng dẫn bạn thông qua khóa học tiếp theo của chương trình chứng chỉ này. Chúng ta sẽ thảo luận về các lĩnh vực bảo mật và hoạt động kinh doanh một cách chi tiết hơn.

I'm so glad I was able to be here for the beginning of your journey. You're off to a great start. I'm excited for you to reach your goal of joining the security industry!

Tôi rất vui vì tôi có thể ở đây để bắt đầu cuộc hành trình của bạn. Bạn đang có một khởi đầu tuyệt vời. Tôi rất vui khi bạn tiếp cận mục tiêu của bạn là tham gia vào ngành bảo mật!

4.2. Course 1 glossary – Thuật ngữ khóa 1

[Course 1 glossary](#)

4.3. Your Course 1 learning journey – Hành trình học tập khóa 1 của bạn

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

4.4. Get started on the next course – Bắt đầu khóa học tiếp theo

Get started on the next course

Congratulations on completing Course 1 of the Google Cybersecurity Certificate: **Foundations of Cybersecurity**! In this part of the program, you learned about possible career paths and key skills for cybersecurity professionals. You were also introduced to foundational cybersecurity terms and concepts that you will continue to explore throughout the certificate program.

Bắt đầu khóa học tiếp theo

Chúc mừng bạn đã hoàn thành Khóa 1 của Chứng chỉ An ninh mạng của Google: **Nền tảng của An ninh mạng** ! Trong phần này của chương trình, bạn đã tìm hiểu về con đường sự nghiệp khả thi và các kỹ năng chính dành cho chuyên gia an ninh mạng. Bạn cũng đã được giới thiệu các thuật ngữ và khái niệm cơ bản về an ninh mạng mà bạn sẽ tiếp tục khám phá trong suốt chương trình chứng chỉ.



The Google Cybersecurity Certificate has eight courses:

Chứng chỉ An ninh mạng của Google có tám khóa học:

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities. *(This is the course you just completed. Well done!)*
1. **Nền tảng của an ninh mạng** - Khám phá nghề an ninh mạng, bao gồm các sự kiện quan trọng dẫn đến sự phát triển của lĩnh vực an ninh mạng và tầm quan trọng liên tục của nó đối với hoạt động của tổ chức. Tìm hiểu về vai trò và trách nhiệm an ninh mạng cấp cơ bản. *(Đây là khóa học bạn vừa hoàn thành. Làm tốt lắm!)*
2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
2. **Chơi an toàn: Quản lý rủi ro bảo mật** — Xác định cách các chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh cũng như khám phá các công cụ an ninh mạng phổ biến.
3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.
3. **Kết nối và bảo vệ: Mạng và bảo mật mạng** - Hiểu rõ về các lỗ hổng cấp độ mạng và cách bảo mật mạng.

Module 4: Cybersecurity tools and programming languages

Phần 4: Các công cụ an ninh mạng và ngôn ngữ lập trình

4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
4. **Công cụ giao dịch: Linux và SQL** - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
5. **Tài sản, mối đe dọa và lỗ hổng bảo mật** - Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.
6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
6. **Báo động: Phát hiện và ứng phó** - Hiểu vòng đời ứng phó sự cố và thực hành sử dụng các công cụ để phát hiện và ứng phó với sự cố an ninh mạng.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
7. **Tự động hóa các tác vụ an ninh mạng bằng Python** — Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.
8. **Đưa nó vào hoạt động: Chuẩn bị cho các công việc về an ninh mạng** — Tìm hiểu về phân loại sự cố, leo thang và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.