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.

# **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

# **Các công cụ an ninh mạng quan trọng**

## **Chào mừng đến với Module 4**

|  |
| --- |
| **Welcome to module 4**  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 vàcác ngôn ngữ lập trình đượcthường được sử dụng trong lĩnh vực an ninh.Chúng rất cần thiết cho việc giám sát an ninh trongmột tổ chức vì chúng nâng caohiệu quả bằng cách tự động hóa các nhiệm vụ.Mặc dù chúng tôi chỉ giới thiệunhững khái niệm và công cụ này vào thời điểm này,phần sau của chương trình,bạn sẽ có cơ hội sử dụng chúng trongnhiều 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 vàcông cụ quản lý sự kiện hoặc SIEM.Bạn cũng sẽ được giới thiệu các công cụ khác nhưplaybook 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 vàcác nhiệm vụ liên quan đến bảo mật được bắt đầu thông quangôn 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 phátất 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 videovà nếu bạn cần, hãy xem lại chúng.Cũng biết rằng những công cụ này sẽđược thảo luận chi tiết hơn nhiều,và bạn sẽ có thể thực hành chúngtrực tiếp, sau này trong chương trình chứng chỉ.

|  |
| --- |
| 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 vàtài liệu đào tạo mà bạn sẽ học cách sử dụng trong công việc,chương trình này sẽ cung cấp cho bạnvới kiến ​​thức nền tảng sẽgiúp bạn thành công trong ngành bảo mật.Bắt đầu nào!

## **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 bạndùng để hứng nước không thành vấn đề.Điều quan trọng là giảm thiểu rủi ro vàmối 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 trongbộ công cụ của bạn mà bạn có thểsử 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 luậnmục đích và chức năng chínhcủa một số công cụ bảo mật thường được sử dụng.Và sau đó trong chương trình,bạn sẽ có cơ hội thực hànhđể 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 liệucác 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. |

Nhật ký là bản ghi lại các sự kiệnxảy ra trong hệ thống của một tổ chức.Ví dụ về nhật ký liên quan đến bảo mật bao gồm hồ sơ vềnhân viên đăng nhập vào máy tính của họhoặc truy cập các dịch vụ dựa trên web.Nhật ký giúp các chuyên gia bảo mật xác địnhcác 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 làthông tin bảo mật và công cụ quản lý sự kiện,hoặc công cụ SIEM.Công cụ SIEM là một ứng dụng thu thập vàphân tích dữ liệu nhật ký để theo dõinhững 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 mậtxác 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 củanhật 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 cóxem xét bằng cách cung cấp thông báo choloại 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 tự 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. |

Một công cụ SIEM khác là Chronicle của Google.Chronicle là một công cụ SIEM dựa trên nền tảng đám mâylưu trữ dữ liệu bảo mật để tìm kiếm và phân tích.Cloud-native có nghĩa là Chroniclecho 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 đềuthu thập dữ liệu từ nhiều nơi,sau đó phân tích và lọc dữ liệu đó để cho phépđội an ninh ngăn chặn và nhanh chóngphản 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 đểphân 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 trongvai trò của bạn là một nhà phân tích bảo mật,và bạn sẽ được thực hànhcơ hội sử dụng sau nàychương 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 dẫncung 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 cáchxử lý sự cố an ninh trước đó,trong và sau khi nó xảy ra.Playbook có thể liên quan đến bảo mật hoặcđánh giá tuân thủ, quản lý quyền truy cập,và nhiều nhiệm vụ tổ chức khácyêu cầu một quá trình được ghi lại từ đầu đến cuối.

|  |
| --- |
| 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 nhưnhà 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 đểthu thập và phân tích lưu lượng dữ liệu trong mạng.Máy phân tích giao thức mạng phổ biếnbao 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 quachương trình chứng chỉ này và được thực hành thực hành nhiều hơn,bạn sẽ liên tục xây dựng sự hiểu biết của mình vềcách sử dụng những công cụ này để xác định,đánh giá, giảm thiểu rủi ro.

## **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. |

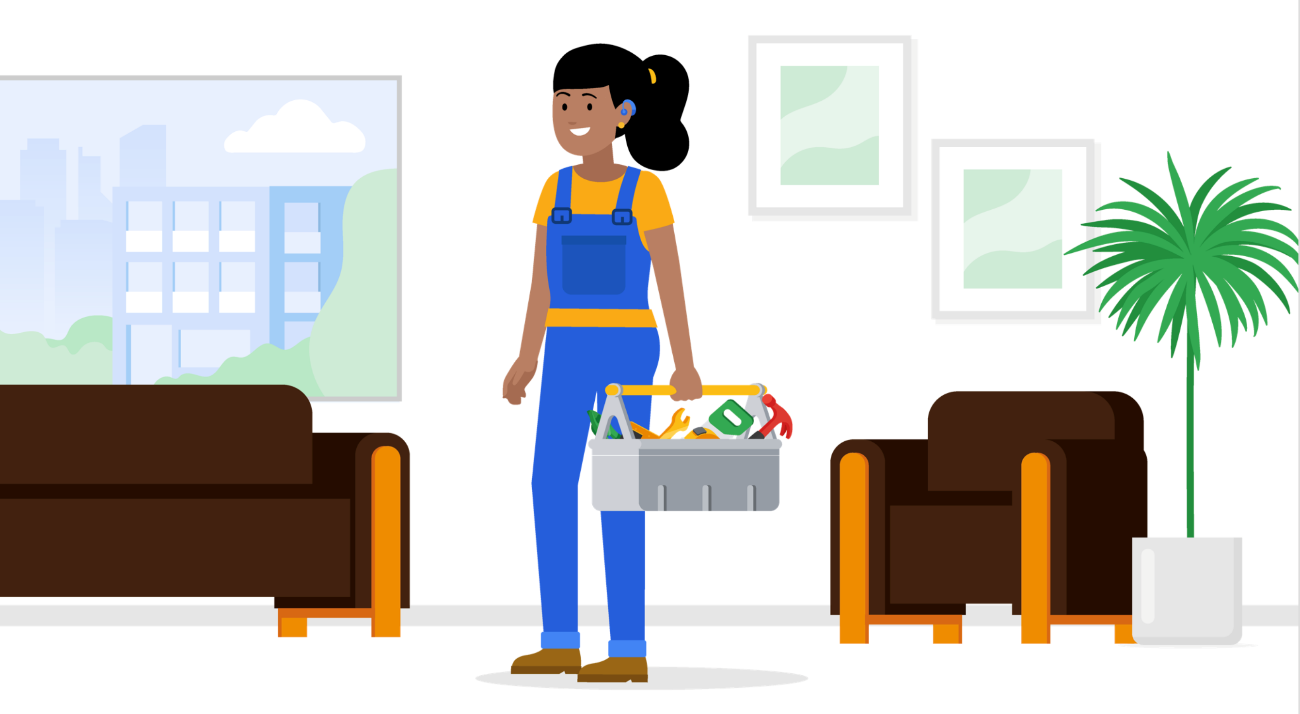
**Công cụ bảo vệ hoạt động kinh doanh**

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 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 dashboardsthat visually organize data into categories, allowing users to select the data they wish to analyze. Different SIEM toolshave 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 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.  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.

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**

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](https://services.google.com/fh/files/blogs/gcat_threathorizons_full_sept2022.pdf) 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](https://www.cisa.gov/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](https://services.google.com/fh/files/blogs/gcat_threathorizons_full_sept2022.pdf)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](https://www.cisa.gov/free-cybersecurity-services-and-tools). Xem lại danh sách để tìm hiểu thêm về các công cụ an ninh mạng nguồn mở.

## **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 |

|  |  |
| --- | --- |
| **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 |

## **Kiểm tra kiến thức của bạn: các công cụ an ninh mạng quan trọng**

# **Kiến thức và kỹ năng an ninh mạng cốt lõi**

## **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 vàhệ 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 vàLập trình SQL và hệ điều hành Linux.Tất cả những điều đó bạn sẽ có cơ hội thực hànhsử dụng sau này trong chương trình chứng chỉ.

|  |
| --- |
| 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 ramột bộ hướng dẫn cụ thểđể máy tính thực hiện các tác vụ.Lập trình cho phép các nhà phân tíchhoàn thành các nhiệm vụ lặp đi lặp lại vàcác quy trình có độ chính xác và hiệu quả cao.Nó cũng giúp giảm nguy cơ lỗi của con người và có thểtiết kiệm giờ hoặc ngàyso với việc thực hiện công việc một cách thủ công.Bây giờ bạn đã biết những gìngôn ngữ lập trình được sử dụng cho,hãy thảo luậnmột hệ điều hành cụ thể và có liên quan được gọi làLinux 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, hoặchệ 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 lệnhlàm giao diện người dùng chính.Bản thân Linux không phải là ngôn ngữ lập trình,nhưng nó cho phép sử dụnglệnh dựa trên văn bản giữa người dùngvà 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 chocác nhà phân tích bảo mật cấp đầu vào làkiểm tra nhật ký để tốt hơnhiểu những gì đang xảy ra trong một hệ thống.Ví dụ, bạn có thểthấy mình sử dụng lệnh để xem lạinhật ký lỗi khi điều tralưu 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. |

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 chứccủa 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 đểlọc qua các điểm dữ liệuđể 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 dụngPython để thực hiện các tác vụlặp đi lặp lại và tốn thời gian và điều đóđòi 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 đóbộ công cụ của mọi tổ chức có thểhơi khác nhau dựa trên nhu cầu bảo mật của họ.Điểm chính là bạn đã quen thuộc vớimột số công cụ tiêu chuẩn ngành vì điều đó sẽ hiển thịnhà tuyển dụng mà bạn có khả năng học cách sử dụngcông cụ của họ để bảo vệtổ 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 vàngôn ngữ lập trình và bạn sẽ thực hànhsử dụng các công cụ này trong các tình huống liên quan đến bảo mật.

## **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 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 pointsin 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** interfaceis 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**

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](https://owasp.org/www-project-top-ten/). |

**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](https://owasp.org/www-project-top-ten/).

|  |
| --- |
| **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 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**  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.

## **Kiểm tra kiến thức của bạn: Kiến thức và kỹ năng cốt lõi về an ninh mạng**

## **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?**

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   **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.

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   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](https://docs.google.com/document/d/13nqRTU4H14NFytodh_tbafXthjNRD7aWU_4Cjq7pKG8/template/preview#heading=h.m08l38wqbrm0). |

**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](https://docs.google.com/document/d/13nqRTU4H14NFytodh_tbafXthjNRD7aWU_4Cjq7pKG8/template/preview#heading=h.m08l38wqbrm0).

|  |
| --- |
| **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   **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.

## **Hoạt động danh mục đầu tư: Soạn thảo một tuyên bố chuyên nghiệp**

## **Ví dụ về hoạt động danh mục đầu tư: Dự thảo một tuyên bố chuyên nghiệp**

# **Đánh giá: Các công cụ an ninh mạng và ngôn ngữ lập trình**

## **Gói lại**

|  |
| --- |
| **Wrap-up**  That completes the introduction to security tools and programming languages! |

**Gói 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 thànhnhiệm 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 vàmáy 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 trìnhSQL 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 bạncó được một công việc trong lĩnh vực an ninh và thăng tiến trong sự nghiệp của bạn!

## **Thuật ngữ trong module 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**

|  |
| --- |
| **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

|  |
| --- |
| **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

## **Thử thách module 4**

# **Chúc mừng bạn đã hoàn thành Khóa 1!**

## **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 vàcông 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 đểăn 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 gìmột nhà phân tích bảo mật cấp đầu vàolàm 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.

|  |
| --- |
| 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 CIAvà 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 vàngôn ngữ lập trình được sử dụng bởicác 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 nàobạn tham gia vào ngành an ninh,mọi thứ bạn đã học đều nằm ở đónền 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 vềmột 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 bạnthông qua khóa học tiếp theo của chương trình chứng chỉ này.Chúng ta sẽ thảo luận về các lĩnh vực bảo mật vàhoạt 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 thểhãy ở đây để bắt đầu cuộc hành trình của bạn.Bạn đang có một khởi đầu tuyệt vời.Tôi rất vui khi bạn tiếp cậnmục tiêu của bạn là tham gia vào ngành bảo mật!

## **Thuật ngữ khóa 1**

[**Course 1 glossary**](Course%201%20glossary.docx)

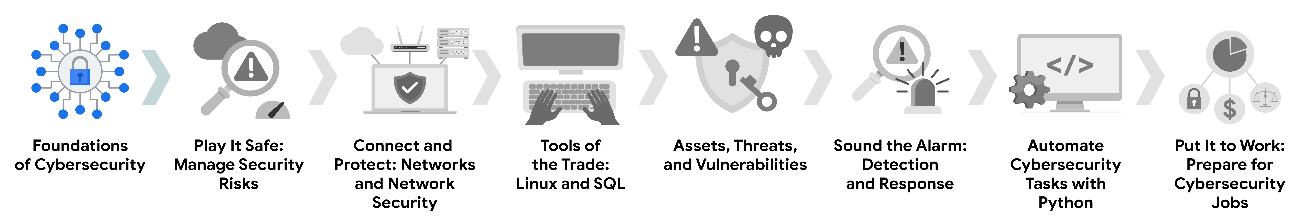
## **Hành trình học tập khóa 1 của bạn**

## **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!)*

|  |
| --- |
| 1. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. |

1. **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.

|  |
| --- |
| 1. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks. |

1. **Kết nối và bảo vệ: Mạng và bảo mật mạng** - Hiểu rõ về các lỗ hổng cấp độ mạng và cách bảo mật mạng.

|  |
| --- |
| 1. **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. |

1. **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.

|  |
| --- |
| 1. 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.** |

1. **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.

|  |
| --- |
| 1. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents. |

1. **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.

|  |
| --- |
| 1. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks. |

1. **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.

|  |
| --- |
| 1. **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. **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.