Important Cybersecurity tools

- Welcome to week 4
- Common cybersecurity tools
- Tools for protecting business operations

Welcome to week 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.

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.

Then, you'll learn about the Linux operating system and security-related tasks that are initiated through programming languages, such as SQL and 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.

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.

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!

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.

As an entry-level security analyst, you'll have a lot of tools in your toolkit that you can use to mitigate potential risks.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

A person with a toolkit with different tools inside

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.

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.

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.

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.

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.