

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.

Revision #1

Created 2023-06-03 00:02:37 UTC by naruzkurai

Updated 2023-06-03 04:51:01 UTC by naruzkurai