**Industry-Leading SIEM Tools for Security Analysts**

Organizations utilize SIEM (Security Information and Event Management) tools to monitor, analyze, and defend against security threats. These tools come in various types and offer unique features to meet the diverse security needs of organizations.

**1. Types of SIEM Tools**

Organizations can choose from three main types of SIEM solutions depending on their operational and security requirements:

**Self-Hosted SIEM Tools**

* **Description:**  
  Installed and operated on an organization’s **own infrastructure** (e.g., physical servers).
* **Management:**  
  Managed and maintained by the organization's **IT department**.
* **Ideal Use Case:**  
  Organizations that need to maintain **physical control over confidential data** for compliance or security reasons.

**Cloud-Hosted SIEM Tools**

* **Description:**  
  Managed and maintained by the **SIEM provider** and accessed via the internet.
* **Advantages:**  
  Reduces the need for organizations to invest in and maintain their own infrastructure.
* **Ideal Use Case:**  
  Organizations adopting **cloud-first** strategies or those without the resources to maintain physical servers.

**Hybrid SIEM Tools**

* **Description:**  
  A combination of **self-hosted** and **cloud-hosted** solutions.
* **Advantages:**  
  Allows organizations to leverage **cloud benefits** (e.g., scalability and availability) while maintaining **control over sensitive data**.
* **Ideal Use Case:**  
  Organizations that handle a mix of **on-premise** and **cloud-based services**.

**2. Commonly Used SIEM Tools**

**Splunk**

Splunk is a widely used data analysis platform that offers both self-hosted and cloud-hosted SIEM solutions:

* **Splunk Enterprise:**
  + Self-hosted.
  + Provides **real-time analysis** and **alerting** by retaining, analyzing, and searching log data.
  + Ideal for organizations that require an on-premise solution.
* **Splunk Cloud:**
  + Cloud-hosted.
  + Used to **collect, monitor, and analyze log data** in hybrid or cloud-only environments.
  + Ideal for businesses transitioning to or operating fully in the **cloud**.

**Google Chronicle**

* **Type:** Cloud-native SIEM tool.
* **Key Features:**
  + Designed to take full advantage of cloud computing capabilities like **scalability, flexibility, and availability**.
  + Offers **log monitoring**, **data analysis**, and **data collection** for robust threat detection and response.
* **Ideal Use Case:** Organizations looking for a **cloud-native SIEM tool** with advanced analytics for large-scale environments.

**3. Why SIEM Tools Are Critical**

The cybersecurity landscape is constantly evolving, and threat actors are developing new methods to breach systems. SIEM tools provide critical functionalities, including:

* **Centralized Data Collection:** Gathering and consolidating logs from multiple sources for comprehensive monitoring.
* **Real-Time Alerts:** Detecting and flagging suspicious activities as they occur.
* **Threat Analysis:** Analyzing data to identify vulnerabilities and potential breaches.
* **Scalability:** Adapting to meet growing organizational needs.

**4. Key Takeaways**

The choice of SIEM tools depends on the organization’s infrastructure, compliance requirements, and operational goals. Tools like **Splunk Enterprise**, **Splunk Cloud**, and **Google Chronicle** provide diverse options to meet a wide range of needs.

In the upcoming sections of the program, you’ll gain hands-on experience with **Splunk Cloud** and **Google Chronicle**, which will help you develop the skills needed to operate these tools effectively as a security analyst. Stay tuned!

# More about cybersecurity tools

Previously, you learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, you’ll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

## Open-source tools

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.

Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

## Proprietary tools

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

### ****Common misconceptions****

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they’re identified.

## Examples of open-source tools

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

### ****Linux****

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It’s used to communicate with the hardware of a computer and manage software applications.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

### ****Suricata****

Suricata is an open-source network analysis and threat detection software.  Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it’s free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

## Key takeaways

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and proprietary tools in more depth.