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.

Revision #1
Created 2023-06-14 09:11:01 UTC by naruzkurai
Updated 2023-06-14 09:11:07 UTC by naruzkurai