Open source intelligence

Cyber attacks can sometimes be prevented with the right information, which starts with knowing where your systems are vulnerable. Previously, you learned that the CVE® list and scanning tools are two useful ways of finding weaknesses. But, there are other ways to identify vulnerabilities and threats.

In this reading, you'll learn about open-source intelligence, commonly known as OSINT. OSINT is the collection and analysis of information from publicly available sources to generate usable intelligence. It's commonly used to support cybersecurity activities, like identifying potential threats and vulnerabilities. You'll learn why open-source intelligence is gathered and how it can improve cybersecurity. You'll also learn about commonly used resources and tools for gathering information and intelligence.

Information vs intelligence

The terms intelligence and information are often used interchangeably, making it easy to mix them up. Both are important aspects of cybersecurity that differ in their focus and objectives.

Information refers to the collection of raw data or facts about a specific subject. *Intelligence*, on the other hand, refers to the analysis of information to produce knowledge or insights that can be used to support decision-making.

For example, new information might be released about an update to the operating system (OS) that's installed on your organization's workstations. Later, you might find that new cyber threats have been linked to this new update by researching multiple cybersecurity news resources. The analysis of this information can be used as intelligence to guide your organization's decision about installing the OS updates on employee workstations.

In other words, intelligence is derived from information through the process of analysis, interpretation, and integration. Gathering information and intelligence are both important aspects of cybersecurity.

Intelligence improves decision-making

Businesses often use information to gain insights into the behavior of their customers. Insights, or intelligence, can then be used to improve their decision making. In security, open-source information is used in a similar way to gain insights into threats and vulnerabilities that can pose risks to an organization.

OSINT plays a significant role in **information security (InfoSec)**, which is the practice of keeping data in all states away from unauthorized users.

For example, a company's InfoSec team is responsible for protecting their network from potential threats. They might utilize OSINT to monitor online forums and hacker communities for discussions about emerging vulnerabilities. If they come across a forum post discussing a newly discovered weakness in a popular software that the company uses, the team can quickly assess the risk, prioritize patching efforts, and implement necessary safeguards to prevent an attack.

Here are some of the ways OSINT can be used to generate intelligence:

- To provide insights into cyber attacks
- To detect potential data exposures
- To evaluate existing defenses
- To identify unknown vulnerabilities

Collecting intelligence is sometimes part of the vulnerability management process. Security teams might use OSINT to develop profiles of potential targets and make data driven decisions on improving their defenses.

OSINT tools

There's an enormous amount of open-source information online. Finding relevant information that can be used to gather intelligence is a challenge. Information can be gathered from a variety of sources, such as search engines, social media, discussion boards, blogs, and more. Several tools also exist that can be used in your intelligence gathering process. Here are just a few examples of tools that you can explore:

- VirusTotal
- is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content.
- MITRE ATT&CK®
- is a knowledge base of adversary tactics and techniques based on real-world observations.
- OSINT Framework
- is a web-based interface where you can find OSINT tools for almost any kind of source or platform.
- Have I been Pwned
- is a tool that can be used to search for breached email accounts.

There are numerous other OSINT tools that can be used to find specific types of information. Remember, information can be gathered from a variety of sources. Ultimately, it's your

responsibility to thoroughly research any available information that's relevant to the problem you’re trying to solve.

Key takeaways

Gathering information and intelligence are important aspects of cybersecurity. OSINT is used to make evidence-based decisions that can be used to prevent attacks. There’s so much information available, which is why it's important for security professionals to be skilled with searching for information. Having familiarity with popular OSINT tools and resources will make your research easier when gathering information and collecting intelligence.

Revision #1
Created 2023-08-15 18:45:25 UTC by naruzkurai
Updated 2023-08-15 18:47:56 UTC by naruzkurai