Cybersecurity incident detection methods

Security analysts use detection tools to help them discover threats, but there are additional methods of detection that can be used as well.

Previously, you learned about how detection tools can identify attacks like data exfiltration. In this reading, you'll be introduced to different detection methods that organizations can employ to discover threats.

Methods of detection

During the **Detection and Analysis Phase** of the incident response lifecycle, security teams are notified of a possible incident and work to investigate and verify the incident by collecting and analyzing data. As a reminder, **detection** refers to the prompt discovery of security events and **analysis** involves the investigation and validation of alerts.

As you've learned, an intrusion detection system (IDS) can detect possible intrusions and send out alerts to security analysts to investigate the suspicious activity. Security analysts can also use security information and event management (SIEM) tools to detect, collect, and analyze security data.

You've also learned that there are challenges with detection. Even the best security teams can fail to detect real threats for a variety of reasons. For example, detection tools can only detect what security teams configure them to monitor. If they aren't properly configured, they can fail to detect suspicious activity, leaving systems vulnerable to attack. It's important for security teams to use additional methods of detection to increase their coverage and accuracy.

Threat hunting

Threats evolve and attackers advance their tactics and techniques. Automated, technology-driven detection can be limited in keeping up to date with the evolving threat landscape. Human-driven detection like threat hunting combines the power of technology with a human element to discover hidden threats left undetected by detection tools.

Threat hunting is the proactive search for threats on a network. Security professionals use threat hunting to uncover malicious activity that was not identified by detection tools and as a way to do further analysis on detections. Threat hunting is also used to detect threats before they cause damage. For example, fileless malware is difficult for detection tools to identify. It's a form of

malware that uses sophisticated evasion techniques such as hiding in memory instead of using files or applications, allowing it to bypass traditional methods of detection like signature analysis. With threat hunting, the combination of active human analysis and technology is used to identify threats like fileless malware.

Note: Threat hunting specialists are known as threat hunters. Threat hunters perform research on emerging threats and attacks and then determine the probability of an organization being vulnerable to a particular attack. Threat hunters use a combination of threat intelligence, indicators of compromise, indicators of attack, and machine learning to search for threats in an organization.

Threat intelligence

Organizations can improve their detection capabilities by staying updated on the evolving threat landscape and understanding the relationship between their environment and malicious actors. One way to understand threats is by using **threat intelligence**, which is evidence-based threat information that provides context about existing or emerging threats.

Threat intelligence can come from private or public sources like:

- **Industry reports**: These often include details about attacker's tactics, techniques, and procedures (TTP).
- **Government advisories:** Similar to industry reports, government advisories include details about attackers' TTP.
- **Threat data feeds**: Threat data feeds provide a stream of threat-related data that can be used to help protect against sophisticated attackers like **advanced persistent threats (APTs)**. APTs are instances when a threat actor maintains unauthorized access to a system for an extended period of time. The data is usually a list of indicators like IP addresses, domains, and file hashes.

It can be difficult for organizations to efficiently manage large volumes of threat intelligence. Organizations can leverage a *threat intelligence platform* (TIP) which is an application that collects, centralizes, and analyzes threat intelligence from different sources. TIPs provide a centralized platform for organizations to identify and prioritize relevant threats and improve their security posture.

Note: Threat intelligence data feeds are best used to add context to detections. They should not drive detections completely and should be assessed before applied to an organization.

Cyber deception

Cyber deception involves techniques that deliberately deceive malicious actors with the goal of increasing detection and improving defensive strategies.

Honeypots are an example of an active cyber defense mechanism that uses deception technology. Honeypots are systems or resources that are created as decoys vulnerable to attacks with the purpose of attracting potential intruders. For example, having a fake file labeled *Client Credit Card Information - 2022* can be used to capture the activity of malicious actors by tricking them into accessing the file because it appears to be legitimate. Once a malicious actor tries to access this file, security teams are alerted.

Key takeaways

Various detection methods can be implemented to identify and locate security events in an environment. It’s essential for organizations to use a variety of detection methods, tools, and technologies to adapt to the ever evolving threat landscape and better protect assets.

Resources for more information

If you would like to explore more on threat hunting and threat intelligence, here are some resources:

- An informational repository about threat hunting fromThe ThreatHunting Project
- Research on state-sponsored hackersfrom Threat Analysis Group (TAG)

Revision #1
Created 2023-09-13 15:07:30 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai