Google Cloud

IoCs for threat detection

So far, you've learned that threat hunting is an approach security operations teams can use to protect organizations against threats. As a reminder, **threat hunting** is the proactive method of identifying previously unknown threats within a network. In this reading, you'll compare the differences between reactive and proactive strategies for incident detection. You'll also explore indicators of compromise, and their importance in detecting threats.

Reactive and proactive strategies

The proliferation of cloud deployment introduces new attack vectors. These attack vectors can be leveraged by malicious actors who are continuously improving their tactics and techniques to gain access to systems, maintain access, and evade detection. Relying on security tools alone is not enough to detect and prevent threats. Traditional security solutions like SIEM and IDS tools often use a reactive approach to detect known security threats through signatures and patterns. With traditional security solutions, the first sign of a security threat happens when an alert is generated while the threat is still in progress.

A reactive approach to security may be effective for low severity threats, but, when it comes to serious threats like advanced persistent threats (APTs), it's not enough. APTs are notorious for their sophisticated levels of expertise, which they use to compromise systems, bypass detection, and maintain persistence. For this reason, APTs can reside in their victim's systems for an extended period of time before being detected. This is known as **dwell time,** or the number of days an attacker is present in a victim's environment before being detected. Typically, a longer dwell time is likely to result in more damage to an organization.

Threat hunting is a strategy that can be used to detect and prevent sophisticated attacks. Threat hunting uses a proactive approach to search for unknown threats – primarily driven by human judgment – to understand the attacker's motivations. By using a proactive approach, security operations teams can remediate potential incidents before they have the chance to cause harm to an organization. Security operations teams can consider implementing threat hunting processes to complement their security strategies, and identify gaps in their security solutions.

Threat hunting best practices

Threat hunting is similar to incident response because it requires a methodology in the form of outlined plans, processes, and procedures. Unlike incident response, the focus of threat hunting is to identify threats that were previously undetected. Here are some best practices to consider when creating a threat hunting program:

- **Define the scope**: Defining the scope of your threat hunt ensures that you focus your time and resources on the most critical areas in your environment. You can utilize threat modeling to identify assets, their vulnerabilities, and the criticality of their vulnerabilities.
- **Know your threat landscape**: Before you can start threat hunting, you need to know which types of threats your organization is most likely to encounter. Threat hunters leverage threat intelligence data and research the observed tactics, techniques, and procedures (TTPs) of threat actors. They use their research to formulate a hypothesis to narrow down the scope of the threat hunt. A hypothesis defines a specific and testable statement about the threat. Knowing what a “normal” landscape looks like is key. For example, having an understanding of which applications are authorized, what the

typical login locations and times are, and how to conduct network utilization can help you identify when things are functioning as intended.

- **Leverage a variety of tools and techniques**: Use a combination of techniques to drive your threat hunting like threat intelligence, analytics, manual analysis, and threat hunting frameworks.
- **Collaborate with others**: Cloud environments are complex and dynamic, which is why communicating with others teams and departments is necessary in threat hunting. By doing so, you'll gain a more complete picture of the threat landscape.

Indicators of compromise (IoC)

Threat hunting can be organized around searching for **indicators of compromise** (IoC), or observable evidence that suggests signs of a potential security incident. This includes artifacts that are known as malicious, like malware, hashes, domains, filenames, and IP addresses.

IoC can also include:

- Unusual inbound or outbound network traffic
- Irregularities in the geographic area of network traffic origin or destination
- Unknown applications found on a system
- Unusual administrator or privileged account activity
- Increased activity for access requests, or incorrect log-ins
- Unusually high database read volume
- Increased requests for the same file
- Suspicious registry and/or system file changes
- Unusual Domain Name Serves (DNS) activity
- Suspicious file hashes, or inconsistencies in file hashes for known system files

Key takeaways

It's impossible to detect and mitigate every single threat in an environment. But, having different defensive approaches in place can help you detect threats early on, so you can minimize the damage done. Threat hunting is becoming an effective approach that many organizations can leverage to discover threats in their systems early on. Being familiar with the processes involved in threat hunting can help you counter threat actors, and protect assets.

Resources for more information

Here are a few resources that can help you learn more about threat hunting:

- Google Cloud podcast about threat hunting in the cloud
- Strategic threat hunting In the cloud
- Event threat detection rules