Threat Hunting Fundamentals

Threat Hunting Definition

The median duration between an actual security breach and its detection, otherwise termed "dwell time", is usually several weeks, if not months. This implies a potential adversarial presence within a network for a span approaching three weeks, a duration that can be significantly impactful.

This alarming fact underscores the growing inefficacy of traditional, defense-oriented cybersecurity tactics. In response, we advocate for a paradigm shift towards a proactive, offensive strategy – the initiation of threat hunting.

`Threat hunting` is an active, human-led, and often hypothesis-driven practice that systematically combs through network data to identify stealthy, advanced threats that evade existing security solutions. This strategic evolution from a conventionally reactive posture allows us to uncover insidious threats that automated detection systems or external entities such as law enforcement might not discern.

The principal objective of threat hunting is to substantially reduce dwell time by recognizing malicious entities at the earliest stage of the cyber kill chain. This proactive stance has the potential to prevent threat actors from entrenching themselves deeply within our infrastructure and to swiftly neutralize them.

The threat hunting process commences with the identification of assets – systems or data – that could be high-value targets for threat actors. Next, we analyze the TTPs (Tactics, Techniques, and Procedures) these adversaries are likely to employ, based on current threat intelligence. We subsequently strive to proactively detect, isolate, and validate any artifacts related to the abovementioned TTPs and any anomalous activity that deviates from established baseline norms.

During the hunting endeavor, we regularly employ Threat Intelligence, a vital component that aids in formulating effective hunting hypotheses, developing counter-tactics, and executing protective measures to prevent system compromise.

Key facets of threat hunting include:

- An offensive, `proactive` strategy that prioritizes threat anticipation over reaction, based on hypotheses, attacker TTPs, and intelligence.
- An offensive, `reactive` response that searches across the network for artifacts related to a `verified` incident, based on evidence and intelligence.
- A solid, practical comprehension of threat landscape, cyber threats, adversarial TTPs, and the cyber kill chain.
- Cognitive empathy with the attacker, fostering an understanding of the adversarial mindset.
- A profound knowledge of the organization's IT environment, network topology, digital assets, and normal activity.
- Utilization of high-fidelity data and tactical analytics, and leveraging advanced threat hunting tools and platforms.

The Relationship Between Incident Handling & Threat Hunting

So, how does threat hunting intersect with the various phases of Incident Handling?

- In the `Preparation` phase of incident handling, a threat hunting team must set up robust, clear rules of engagement. Operational protocols must be established, outlining when and how to intervene, the course of action in specific scenarios, and so forth. Organizations may choose to weave threat hunting into their existing incident handling policies and procedures, obviating the need for separate threat hunting policies and procedures.
- During the `Detection & Analysis` phase of incident handling, a threat hunter's acumen is indispensable. They can augment investigations, ascertain whether the observed indicators of compromise (IoCs) truly signify an incident, and further, their adversarial mindset can help uncover additional artifacts or IoCs that might have been missed initially.
- In the `Containment, Eradication, and Recovery` phase of incident handling, the role of a hunter can be

Go to Questions

Table of Contents

Threat Hunting & Threat Intelligence Fundamentals

Threat Hunting Fundamentals

The Threat Hunting Process

Threat Hunting Glossary

Threat Intelligence Fundamentals

Threat Hunting With The Elastic Stack

Hunting For Stuxbot

Let's Go Hunting

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

diverse. Some organizations might expect hunters to perform tasks within the Containment, Eradication, and Recovery stages. However, this is not a universally accepted practice. The specific roles and responsibilities of the hunting team will be stipulated in the procedural documents and security policies.

- Regarding the `Post-Incident Activity` phase of incident handling, hunters, with their extensive expertise spanning various IT domains and IT Security, can contribute significantly. They can proffer recommendations to fortify the organization's overall security posture.

We tried to shed light on the symbiotic relationship between incident handling and threat hunting. Whether these processes should be integrated or function independently is a strategic decision, contingent upon each organization's unique threat landscape, risk, etc.

A Threat Hunting Team's Structure

The construction of a threat hunting team is a strategic and meticulously planned process that requires a diverse range of skills, expertise, and perspectives. It is crucial that each member of the team offers a unique set of competencies that, when combined, provide a holistic and comprehensive approach to identifying, mitigating, and eliminating threats.

The ideal threat hunting team composition typically includes the following roles:

- `Threat Hunter`: The core role within the team, threat hunters are cybersecurity professionals with a deep understanding of the threat landscape, cyber adversaries' Tactics, Techniques, and Procedures (TTPs), and sophisticated threat detection methodologies. They proactively search for Indicators of Compromise (IoCs) and are proficient in using a variety of threat hunting tools and platforms.
- `Threat Intelligence Analyst`: These individuals are responsible for gathering and analyzing data from a variety of sources, including open-source intelligence, dark web intelligence, industry reports, and threat feeds. Their job is to understand the current threat landscape and predict future trends, providing valuable insights to threat hunters.
- `Incident Responders`: When threat hunters identify potential threats, incident responders step in to manage the situation. They investigate the incident thoroughly and they are also responsible for containment, eradication, and recovery actions, and they ensure that the organization can quickly resume normal operations.
- `Forensics Experts`: These are the team members who delve deep into the technical details of an incident. They are proficient in digital forensics and incident response (DFIR), capable of analyzing malware, reverse engineering attacks, and providing detailed incident reports.
- `Data Analysts/Scientists`: They play a pivotal role in examining large datasets, using statistical models, machine learning algorithms, and data mining techniques to uncover patterns, correlations, and trends that can lead to actionable insights for threat hunters.
- `Security Engineers/Architects`: Security engineers are responsible for the overall design of the organization's security infrastructure. They ensure that all systems, applications, and networks are designed with security in mind, and they often work closely with threat hunters to implement tools and techniques that facilitate threat hunting, as well as kill-chain defenses.
- `Network Security Analyst`: These professionals specialize in network behavior and traffic patterns. They understand the normal ebb and flow of network activity and can quickly identify anomalies indicative of a potential security breach.
- `SOC Manager`: The Security Operations Center (SOC) manager oversees the operations of the threat hunting team, ensuring smooth coordination among team members and effective communication with the rest of the organization.

When Should We Hunt?

In the realm of cybersecurity, threat hunting should not be seen as a sporadic or reactionary practice, but rather as a sustained, forward-thinking activity. Nevertheless, there are specific instances that call for an immediate and intense threat hunting operation. Here's a more intricate breakdown of these instances:

- `When New Information on an Adversary or Vulnerability Comes to Light`: The cybersecurity landscape is always evolving, with fresh intel on potential threats and system vulnerabilities being uncovered regularly. If there's a newly discovered adversary or a vulnerability associated with an application that our network utilizes, this calls for an immediate threat hunting session. It's imperative to decipher the adversary's modus operandi and scrutinize the vulnerability to evaluate the possible risk to our systems. For instance, if we stumble upon a previously unknown vulnerability in a widely utilized

application, we'd promptly kickstart a threat hunting initiative to seek out any signs of exploitation.

- `When New Indicators are Associated with a Known Adversary`: Often, cybersecurity intelligence sources release new Indicators of Compromise (IoCs) tied to specific adversaries. If these indicators are associated with an adversary known for targeting networks akin to ours or if we've been a past target of the same adversary, we need to launch a threat hunting initiative. This aids in detecting any traces of the adversary's activities within our system, allowing us to ward off potential breaches.
- `When Multiple Network Anomalies are Detected`: Network anomalies might sometimes be harmless, caused by system glitches or valid alterations. However, several anomalies appearing concurrently or within a short period might hint at a systemic issue or an orchestrated attack. In such cases, it's crucial to carry out threat hunting to pinpoint the root cause of these anomalies and address any possible threats. For instance, if we observe odd network traffic behavior or unexpected system activities, we'd initiate threat hunting to probe these anomalies.
- `During an Incident Response Activity`: Upon the detection of a confirmed security incident, our Incident Response (IR) team will concentrate on containment, eradication, and recovery. Yet, while the IR process is in motion, it's vital to simultaneously conduct threat hunting across the network. This enables us to expose any connected threats that might not be readily visible, understand the full extent of the compromise, and avert further harm. For example, during a confirmed malware infiltration, while the IR team is dealing with the infected system, threat hunting can assist in identifying other potentially compromised systems.
- `Periodic Proactive Actions`: Beyond the scenarios mentioned above, it's crucial to note that threat hunting should not be simply a reactive task. Regular, proactive threat hunting exercises are key to discovering latent threats that may have slipped past our security defenses. This guarantees a continual monitoring strategy, bolstering our overall security stance and minimizing the prospective impact of an attack.

In a nutshell, the ideal time for threat hunting is always the present. A proactive stance on threat hunting lets us detect and neutralize threats before they can inflict substantial damage.

The Relationship Between Risk Assessment & Threat Hunting

Risk assessment, as an essential facet of cybersecurity, enables a comprehensive understanding of the potential vulnerabilities and threat vectors within an organization. In the context of threat hunting, risk assessment serves as a key enabler, allowing us to prioritize our hunting activities and focus our efforts on the areas of greatest potential impact.

To begin with, risk assessment entails a systematic process of identifying and evaluating risks based on potential threat sources, existing vulnerabilities, and the potential impact should these vulnerabilities be exploited. It involves a series of steps including asset identification, threat identification, vulnerability identification, risk determination, and finally, risk mitigation strategy formulation.

In the threat hunting process, the information gleaned from a thorough risk assessment can guide our activities in several ways:

- `Prioritizing Hunting Efforts`: By recognizing the most critical assets (often referred to as 'crown jewels') and their associated risks, we can prioritize our threat hunting efforts on these areas. Assets could include sensitive data repositories, mission-critical applications, or key network infrastructure.
- `Understanding Threat Landscape`: The threat identification step of the risk assessment allows us to understand the threat landscape better, including the Tactics, Techniques, and Procedures (TTPs) used by potential threat actors. This understanding assists us in developing our hunting hypotheses, which are essential for proactive threat hunting.
- `Highlighting Vulnerabilities`: Risk assessment helps to highlight vulnerabilities in our systems, applications, and processes. Knowing these weaknesses enables us to look for exploitation indicators in these areas. For instance, if we know a particular application has a vulnerability that allows for privilege escalation, we can look for anomalies in user privilege levels.
- `Informing the Use of Threat Intelligence`: Threat intelligence is often used in threat hunting to identify patterns of malicious behavior. Risk assessment helps inform the application of threat intelligence by identifying the most likely threat actors and their preferred methods of attack.
- `Refining Incident Response Plans`: Risk assessment also plays a critical role in refining Incident Response (IR) plans. Understanding the likely risks helps us anticipate and plan for potential breaches, ensuring a swift and effective response.
- `Enhancing Cybersecurity Controls`: Lastly, the risk mitigation strategies derived from risk assessment

can directly feed into enhancing existing cybersecurity controls and defenses, further strengthening the organization's security posture.

The technicalities of employing risk assessment for threat hunting include the use of advanced tools and techniques. These range from automated vulnerability scanners and penetration testing tools to sophisticated threat intelligence platforms. For instance, SIEM (Security Information and Event Management) systems can be used to aggregate and correlate events from various sources, providing a holistic view of the organization's security status and aiding in threat hunting.

In essence, risk assessment and threat hunting are deeply intertwined, each augmenting the other to create a more robust and resilient cybersecurity posture. By regularly conducting comprehensive risk assessments, we can better focus our threat hunting activities, thereby reducing dwell time, mitigating potential damage, and enhancing our overall cybersecurity defense.

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 1 Threat hunting is used ... Choose one of the following as your answer: "proactively", "reactively", "proactively and reactively".

proactively and reactively

Submit

+ 1 Threat hunting and incident handling are two processes that always function independently. Answer format: True, False.

False

Submit

+ 1 Threat hunting and incident response can be conducted simultaneously. Answer format: True, False.

True

Submit

Next

Mark Complete & Next

Powered by HACKTHEBOX