The Threat Hunting Process

Below is a brief description of the threat hunting process:

- `Setting the Stage`: The initial phase is all about planning and preparation. It includes laying out clear targets based on a deep understanding of the threat landscape, our business's critical requirements, and our threat intelligence insights. The preparation phase also encompasses making certain our environment is ready for effective threat hunting, which might involve enabling extensive logging across our systems and ensuring threat hunting tools, such as SIEM, EDR, IDS, are correctly set up. Additionally, we stay informed about the most recent cyber threats and familiarize ourselves with threat actor profiles.
    - `Example`: During the planning and preparation phase, a threat hunting team might conduct in-depth research on the latest threat intelligence reports, analyze industry-specific vulnerabilities, and study the tactics, techniques, and procedures (TTPs) employed by threat actors. They may also identify critical assets and systems within the organization that are most likely to be targeted. As part of the preparation, extensive logging mechanisms can be implemented across servers, network devices, and endpoints to capture relevant data for analysis. Threat hunting tools like SIEM, EDR, and IDS are configured to collect and correlate logs, generate alerts, and provide visibility into potential security incidents. Additionally, the team stays updated on emerging cyber threats by monitoring threat feeds, subscribing to relevant security mailing lists, and participating in information sharing communities.
- `Formulating Hypotheses`: The next step involves making educated predictions that will guide our threat hunting journey. These hypotheses can stem from various sources, like recent threat intelligence, industry updates, alerts from security tools, or even our professional intuition. We strive to make these hypotheses testable to guide us where to search and what to look for.
    - `Example`: A hypothesis might be that an attacker has gained access to the network by exploiting a particular vulnerability or through phishing emails. This hypothesis could be derived from recent threat intelligence reports that highlight similar attack vectors. It could also be based on an alert triggered by an intrusion detection system indicating suspicious network traffic patterns. The hypothesis should be specific and testable, such as "An advanced persistent threat (APT) group is leveraging a known vulnerability in the organization's web server to establish a command-and-control (C2) channel."
- `Designing the Hunt`: Upon crafting a hypothesis, we need to develop a hunting strategy. This includes recognizing the specific data sources that need analysis, the methodologies and tools we'll use, and the particular indicators of compromise (IoCs) or patterns we'll hunt for. At this point, we might also create custom scripts or queries and utilize dedicated threat hunting tools.
    - `Example`: The threat hunting team may decide to analyze web server logs, network traffic logs, DNS logs, or endpoint telemetry data. They define the search queries, filters, and correlation rules to extract relevant information from the collected data. The team also leverages threat intelligence feeds and open-source intelligence (OSINT) to identify specific indicators of compromise (IoCs) associated with the suspected threat actor or known attack techniques. This may involve crafting custom scripts or queries to search for IoCs or using specialized threat hunting platforms that automate the process.
- `Data Gathering and Examination`: This phase is where the active threat hunt occurs. It involves collecting necessary data, such as log files, network traffic data, endpoint data, and then analyzing this data using the predetermined methodologies and tools. Our goal is to find evidence that either supports or refutes our initial hypothesis. This phase is highly iterative, possibly involving refinement of the hypothesis or the investigation approach as we uncover new information.
    - `Example`: The threat hunting team might examine web server access logs to identify unusual or unauthorized access patterns, analyze network traffic captures to detect suspicious communications with external domains, or investigate endpoint logs to identify anomalous behavior or signs of

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

compromise. They apply data analysis techniques such as statistical analysis, behavioral analysis, or signature-based detection to identify potential threats. They might employ tools like log analyzers, packet analyzers, or malware sandboxes to extract information from the collected data and uncover hidden indicators of compromise.

- `Evaluating Findings and Testing Hypotheses`: After analyzing the data, we need to interpret the results. This could involve confirming or disproving the hypothesis, understanding the behavior of any detected threats, identifying affected systems, or determining the potential impact of the threat. This phase is crucial, as it will inform the next steps in terms of response and remediation.
    - `Example`: The threat hunting team might discover a series of failed login attempts from an IP address associated with a known threat actor, confirming the hypothesis of an attempted credential brute-force attack. They might also find evidence of suspicious outbound network connections to known malicious domains, supporting the hypothesis of a command-and-control (C2) communication channel. The team conducts deeper investigations to understand the behavior of the identified threats, assess the scope of the compromise, and determine the potential impact on the organization's systems and data.
- `Mitigating Threats`: If we confirm a threat, we must undertake remediation actions. This could involve isolating affected systems, eliminating malware, patching vulnerabilities, or modifying configurations. Our goal is to eradicate the threat and limit any potential damage.
    - `Example`: If the threat hunting team identifies a compromised system communicating with a C2 server, they may isolate the affected system from the network to prevent further data exfiltration or damage. They may deploy endpoint protection tools to remove malware or perform forensic analysis on the compromised system to gather additional evidence and determine the extent of the breach. Vulnerabilities identified during the threat hunting process can be patched or mitigated to prevent future attacks. Network configurations can be adjusted to restrict unauthorized access or to strengthen security controls.
- `After the Hunt`: Once the threat hunting cycle concludes, it's crucial to document and share the findings, methods, and outcomes. This might involve updating threat intelligence platforms, enhancing detection rules, refining incident response playbooks, or improving security policies. It's also vital to learn from each threat hunting mission to enhance future efforts.
    - `Example`: Once the threat hunting cycle concludes, the team documents the findings, methodologies, and outcomes of the investigation. They update threat intelligence platforms with newly discovered indicators of compromise (IoCs) and share relevant information with other teams or external partners to enhance the collective defense against threats. They may improve detection rules within security tools based on the observed attack patterns and refine incident response playbooks to streamline future incident handling. Lessons learned from the hunt are incorporated into security policies and procedures, and training programs are adjusted to enhance the organization's overall security posture.
- `Continuous Learning and Enhancement`: Threat hunting is not a one-time task, but a continuous process of learning and refinement. Each threat hunting cycle should feed into the next, allowing for continuous improvement of hypotheses, methodologies, and tools based on the evolving threat landscape and the organization's changing risk profile.
    - `Example`: After each threat hunting cycle, the team reviews the effectiveness of their hypotheses, methodologies, and tools. They analyze the results and adjust their approach based on lessons learned and new threat intelligence. For example, they might enhance their hunting techniques by incorporating machine learning algorithms or behavioral analytics to detect more sophisticated threats. They participate in industry conferences, attend training sessions, and collaborate with other threat hunting teams to stay updated on the latest attack techniques and defensive strategies.

Threat hunting is a delicate balance of art and science. It demands technical prowess, creativity, and a profound understanding of both the organization's environment and the broader threat landscape. The most successful threat hunting teams are those that learn from each hunt and constantly hone their skills and processes.

The Threat Hunting Process VS Emotet

Let's see how the abovementioned threat hunting process could have been applied to hunt for emotet malware within an organization.

- `Setting the Stage`: During the planning and preparation phase, the threat hunting team extensively researches the Emotet malware's tactics, techniques, and procedures (TTPs) by studying previous attack campaigns, analyzing malware samples, and reviewing threat intelligence reports specific to Emotet. They gain a deep understanding of Emotet's infection vectors, such as malicious email attachments or links, and the exploitation of vulnerabilities in software or operating systems. The team identifies critical assets and systems that are commonly targeted by Emotet, such as endpoints with administrative privileges or email servers.

- `Formulating Hypotheses`: Hypotheses in the context of Emotet threat hunting might be based on known Emotet IoCs or patterns observed in previous attacks. For example, a hypothesis could be that Emotet is using a new phishing technique to distribute malicious payloads via compromised email accounts. This hypothesis could be derived from recent threat intelligence reports highlighting similar Emotet campaigns or based on alerts triggered by email security systems detecting suspicious email attachments. The hypothesis should be specific, such as "Emotet is using compromised email accounts to send phishing emails with malicious Word documents containing macros."

- `Designing the Hunt`: In the design phase, the threat hunting team determines the relevant data sources and collection methods to validate or invalidate the Emotet-related hypotheses. They may decide to analyze email server logs, network traffic logs, endpoint logs, or sandboxed malware samples. They define search queries, filters, and correlation rules to extract information related to Emotet's specific characteristics, such as email subject lines, attachment types, or network communication patterns associated with Emotet infections. They leverage threat intelligence feeds to identify Emotet-related IoCs, such as known command-and-control (C2) server addresses or file hashes associated with Emotet payloads.

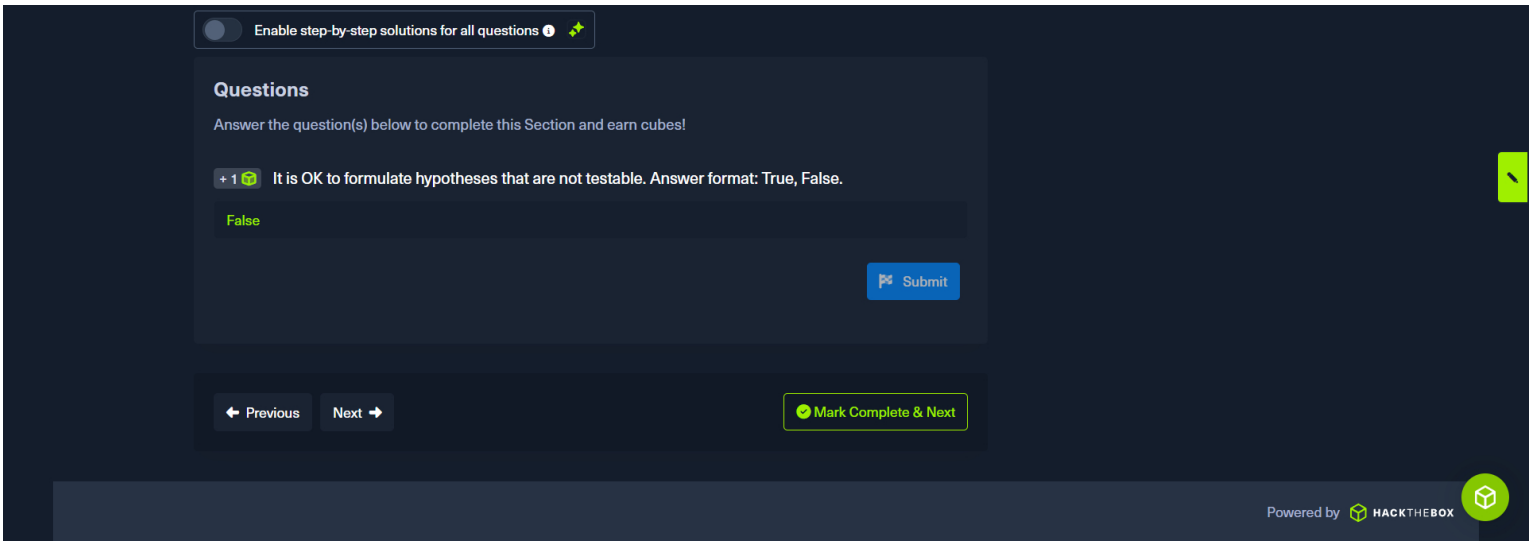
- `Data Gathering and Examination`: During the active threat hunting phase, the team collects and analyzes data from various sources to detect Emotet-related activities. For example, they might examine email server logs to identify patterns of suspicious email attachments or analyze network traffic captures to detect communication with known Emotet C2 servers. They apply data analysis techniques, such as email header analysis, network traffic pattern analysis, or behavioral analysis, to identify potential Emotet infections. They utilize tools like email forensics software, network packet analyzers, or sandbox environments to extract relevant information from the collected data and uncover hidden indicators of Emotet activity.

- `Evaluating Findings and Testing Hypotheses`: In this phase, the team evaluates the findings from data analysis to confirm or refute the initial Emotet-related hypotheses. For example, they might discover a series of emails with similar subject lines and attachment types associated with Emotet campaigns, confirming the hypothesis of ongoing Emotet phishing activities. They might also find evidence of network connections to known Emotet C2 servers, supporting the hypothesis of an active Emotet infection. The team conducts deeper investigations to understand the behavior of the identified Emotet infections, assess the scope of the compromise, and determine the potential impact on the organization's systems and data.

- `Mitigating Threats`: If Emotet infections are confirmed, the team takes immediate remediation actions. They isolate affected systems from the network to prevent further spread of the malware and potential data exfiltration. They deploy endpoint protection tools to detect and remove Emotet malware from compromised systems. Additionally, they analyze compromised email accounts to identify and remove unauthorized access. They patch or mitigate vulnerabilities exploited by Emotet to prevent future infections. Network configurations are adjusted to block communication with known Emotet C2 servers or malicious domains.

- `After the Hunt`: Once the Emotet threat hunting cycle concludes, the team documents their findings, methodologies, and outcomes. They update threat intelligence platforms with new Emotet-related IoCs and share relevant information with other teams or external partners to enhance their collective defense against Emotet. They improve detection rules within security tools based on the observed Emotet attack patterns and refine incident response playbooks to streamline future incident handling. Lessons learned from the Emotet hunt are incorporated into security policies and procedures, and training programs are adjusted to enhance the organization's overall defenses against Emotet and similar malware.

- `Continuous Learning and Enhancement`: Threat hunting for Emotet is an ongoing process that requires continuous learning and improvement. After each Emotet threat hunting cycle, the team reviews the effectiveness of their hypotheses, methodologies, and tools. They analyze the results and adjust their approach based on lessons learned and new Emotet-related threat intelligence. For example, they might enhance their hunting techniques by incorporating advanced behavior-based detection mechanisms or machine learning algorithms specifically designed to identify Emotet's evolving TTPs. They actively participate in industry conferences, attend training sessions, and collaborate with other threat hunting teams to stay updated on the latest Emotet attack techniques and defensive strategies.


Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
+ 1
It is OK to formulate hypotheses that are not testable. Answer format: True, False.
False
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX