Threat Hunting: Strategic Approaches and Capabilities to Uncover Hidden Threats

What is Threat Hunting?

Threat hunting is the discovery of malicious artifacts, activity or detection methods not accounted for in passive monitoring capabilities. Essentially, threat hunting is the process of identifying unknown threats that otherwise would be hiding in your network and on your endpoints, lying in wait to further expand access and/or steal sensitive data.

Successful threat hunting usually involves creating hypotheses based on attacker TTPs and using these to find unusual patterns or indicators that traditional security measures might miss. This proactive method also helps create special markers and behavioral signs, improving the ability to detect threats in real-time.

- Recommended Reading: Mastering Threat Hunting: Your Edge Against Hidden Cyber Threats

Quick Stats

Here are some industry stats to illustrate the urgency and effectiveness of cyber threat hunting:

21 days

is the average dwell time of cyber threats

57%

of breaches involving undetected TTPs

3.5 million

is the Projected global cybersecurity talent gap

45%

increase in ROI for organizations investing in dedicated threat hunting capabilities

Three Strategic Approaches for Threat Hunt

Retrospective Discovery

This approach leverages new internal or external intelligence (i.e. new IOC) to look back across the environment to see if a threat exists that was not previously detected.

Artifact Discovery

Statistical analysis approach, using machine learning to collate, aggregate and crunch the data to find abnormalities (i.e. identify the least used user agent string over the last 30 days and analyze why that is)

Activity Discovery

This type of threat hunting is where analysts identify patterns of behaviors (TTPs) that could be malicious.

Why is Threat Hunting Important?

Threat hunting is derived from a shift in the approach by security professionals on how to address risks within the organization. Previously, the focus was on building defense-in-depth and quickly reacting to suspicious activity – a “Vulnerability-Centric” approach.

More organizations are beginning to shift their approach to ensure greater visibility within the environment and proactively look for anomalous activity based on various profiles and behaviors of attacks, attackers, and their tools. This detection-based paradigm shift is considered a “Threat-Centric” approach of which threat hunting is a core component.

Threat hunting provides organizations with a method for taking a proactive approach to the identification of sophisticated, unknown threats… threats that have evaded preventative and signature-based detection methods. As research has shown, the average dwell time (where an attacker is hunkered down inside a network before being discovered) is measured in months.

Threat hunting is a way to find attackers inside the network before they have had the opportunity to cause real damage – either by disrupting operations or stealing sensitive data. Additionally, threat hunting can be used to create new behavioral tactics, techniques, and procedures (TTPs) that can be added to existing detection methods/rules/tools/and intelligence. A threat hunting endeavor will help identify activity that may have gone unnoticed over time or across the infrastructure.

Threat Hunting vs. Threat Intelligence

Threat hunting and threat intelligence are usually seen as related but separate activities in cybersecurity. Both help improve security by being proactive, but they have different goals:

Threat hunting

involves actively looking for unknown threats in your system, using hypotheses to find specific behaviors or artifacts indicative of malicious activity. Cyber threat hunting is a proactive, hands-on activity usually done by specialized teams.

Threat intelligence

involves gathering, processing, and analyzing data about existing threats, like IOCs, TTPs, and attack trends. This information helps the threat-hunting process by giving details on the latest methods used by attackers.

While threat intelligence provides information about known threats, threat hunting uses that information/data to find unknown or undetected elements within a company's systems.

Where to Start Threat Hunting?

Before threat hunting can begin, a prioritized set of questions must be determined as these will drive the hunt. You also must understand your infrastructure and your data as that will impact what types of threat hunting activities you can conduct. Also important is understanding the expertise on hand as that will impact threat hunting as well. Threat hunting is an advanced, but highly beneficial capability that requires the right people, technology and data to help answer the critical hypotheses that are created.

Catch the Threats that Other Tools Miss

Explore Fidelis Security's Active Threat Detection Using proprietary algorithms developed by Fidelis Security's expert threat hunters! ***What This Datasheet Covers:***

- Introduction to Active Threat Detection
- Capabilities
- Advantages

Download Datasheet

Effective Threat-Hunting Tools

In 2024, using the right tools for threat-hunting is very important for proactive and efficient defense. Here are four key tools to consider:

1. Extended Detection and Response (XDR)

XDR is not a singular threat-hunting tool; it's an integrated security platform that gathers information from various places like endpoints, networks, and cloud environments, and puts it all together in one place.

Fidelis Elevate® is an example of an XDR solution that helps find threats by correlating data from these different areas, making it easier to understand and quicker to investigate. XDR supports threat hunters by making detection centralized, speeding up responses, and giving a comprehensive context that allows for more accurate and efficient threat-hunting.

2. Managed Detection and Response (MDR)

MDR services offers expert-led threat monitoring, detection, and incident response, providing continuous protection and support. It is especially useful for companies facing cybersecurity talent gaps or those needing robust threat-hunting capabilities around the clock.

3. Security Information and Event Management (SIEM)

SIEM solutions collect log data from across the network, allowing for better detection and

understanding of advanced threats and complex attack patterns. By integrating with SIEM platforms, Fidelis Network® improves threat detection and response by providing more comprehensive visibility and useful information about what's happening on the network.

4. Security Analytics

Security analytics tools use machine learning and behavioral analysis to find unusual activities and give useful information about potential threats. These tools are important for discovering sophisticated, low-and-slow attacks that traditional security might overlook.

5. Endpoint Detection and Response (EDR)

EDR tools focus on endpoint visibility, helping teams to detect, investigate, and respond to threats fast. Fidelis Endpoint® provides real-time monitoring, automatic response, and forensic analysis, letting security teams identify lateral movement and protect devices from complex attacks.

These tools provide a strong base for successful threat hunting, improving visibility and strengthening an organization's capability to find and respond to complex threats.

What are Key Capabilities to Look for in a Threat Hunting Capability?

Threat hunting requires the right expertise, along with the tools and data, so the first thing to determine is if that expertise is on staff, to be hired, or to be outsourced. Often times organizations will look to outsource their threat hunting capability through a Managed Detection and Response provider.

Important capabilities and data to effectively conduct threat hunting activities include the following:

People Skills

Threat hunting requires a unique skillset that combines multiple disciplines of security infrastructure, threat intelligence, malware analysis, data analytics and forensics, and creativity.

Threat hunters should have:

- An understanding of both networks and how operating systems (OS) work in an infrastructure.
- A background or understanding of analytic tradecraft, including the ability to create hypotheses and test those against assumptions (including biases).
- An understanding of how attacker TTPs from both a process and/or tool perspective.

Threat Hunting Process

A threat hunting process should begin by defining the level of importance that cyber risk has upon the business, what potential threats could occur and how those threats would create risk. Existing tools and teams should be used to profile the infrastructure and ensure that the profile stays up-to-date. Part of the threat hunting process also includes determining what information you need to collect and for how long, as well as what must be analyzed to ensure proactive

threat analysis. By focusing on the areas within the Pyramid of Pain, you can gain the greatest impact, while minimizing alert fatigue.

Once your threat hunting process is defined, create a set of rules to identify the risk or threat and metrics to address efficiency (i.e. how many alerts are generated by a new rule versus how many tickets are closed by analysts).

Use the profile of the environment and the information collected to address the following questions:

- What can be automated versus what should be analyzed?
- What should be the focus in terms of intel sources?
- How are you incorporating the analysis process and cross-verifying with the information, such as the MITRE ATTACK framework?

By having a strong documentation and feedback process for the threat hunting activity, you can leverage the postmortem of the activity and results to further refine the process and the Cyber Threat Intelligence (CTI) IOCs.

Technology

The third pillar of being ready to conduct threat hunting exercises is having the right technology in place. If possible, ensure security solutions can collect metadata from multiple layers in real-time. Oftentimes a SIEM will provide a repository of raw logs but may lack the capabilities or will be over-subscribed to allow for hunting activities to occur within a specific timeframe.

Key capabilities to look for in a solution that will enable threat hunting include the ability to:

- Ingest and store metadata from network and cloud traffic, as well as endpoint activity for real-time threat detection and retrospective analysis.
- Overlay that rich metadata with threat intelligence and run scripts to capture specific data for visibility and context.
- Import live data from various sources (i.e. network traffic and endpoint activity) into a solution where correlation of real-time and historical activity can occur to enhance visibility and validate the activity.
- Provide visibility across the cyber terrain to validate against the current environment.
- Leverage a deception layer that can be used to provide context or validation of activity.
- Foster the analyst’s creativity to help identify anomalous activity with an extensible query solution for hosts.
- Quickly pull forensic images of memory or the hard drive for further analysis.

Frequently Ask Questions

What frameworks support threat hunting?

The MITRE ATT&CK and Pyramid of Pain frameworks are commonly used to help recognize tactics, techniques, and procedures (TTPs) and prioritize threat-hunting efforts. Both frameworks offer a systematic way to understand and tackle the actions of adversaries and the most important areas of risk.

What are common challenges in threat hunting?

Threat hunting has challenges like limited resources, alert fatigue, and a need for highly skilled professionals. As more threats use AI, it becomes harder to tell legitimate activities from malicious ones, underscoring the importance of advanced tools and well-trained analysts.

How often should threat hunting be conducted?

The frequency of threat hunting depends on an organization’s risk tolerance, available resources, and the threat landscape. Many organizations conduct continuous threat hunting, while others do so on a periodic basis, such as monthly or quarterly, based on their specific needs.