Threat Hunting Done Right

Breaking Through Industry Misconceptions and Identifying Emerging Threats Systematically

The Critical Role of Threat Hunting

At a time when many security leaders see their teams struggling to keep pace with their organization's threat detection and response needs, proactive threat hunting often becomes a goal that is perpetually just out of reach.

Even if the budget exists, it's challenging to find and retain the specialized talent required for threat hunting. And even if resources are onboarded, they are often absorbed into daily emergencies as part of the interrupt-driven world of security operations.

But in today's climate, threat hunting is no longer a luxury. In fact, threat hunting, when done correctly, provides a better return than most other security investments. As an industry, we now know without a doubt that even the most complete and mature set of security controls and detection methods will be evaded at some point. It's just a matter of when.

An effective threat hunting function will identify adversaries who evade an organization's security controls faster. Reducing this dwell time will, in turn, reduce the likelihood that adversaries will achieve their objectives and cause negative business outcomes. The solution is taking an approach where Offense Fuels Defense – thinking like an adversary while defending like a guardian.

More specifically, threat hunting enhances defensive security by:

- Enriching threat intelligence with the latest adversary tactics and techniques.
- Providing insights that enable continuous improvement of detection methods.
- Revealing atomic indicators of compromise that can inform changes to security policy enforcement and alerting strategies.
- Reducing the percentage of incidents that escalate to crisis level.

But success with threat hunting requires a clear understanding of what it is and what it isn't. The security vendor community often makes this confusing by using the term to describe things that aren't truly threat hunting.

The goal of this guide is to help organizations cut through this noise and create a threat hunting function that is comprehensive, effective, and seamlessly integrated with an equally effective detection and response motion.

- Jeremy Wiedner, Principal Analyst

What Threat Hunting Isn't:

Before we explore the intricacies of threat hunting, let's take a moment to review what it isn't.

Threat hunting is not:

- Responding to a detected threat to discover the scope of the compromise and develop strategies to contain, evict, and remediate it.
  This is Incident Response.
- Investigating an alert from a security tool to determine if it is valid or a false positive.
  This is Security Analysis.
- Gathering and producing information about threat actors and their tactics, techniques, procedures, and infrastructure.
  This is Threat Intelligence.
- Adding a list of known indicators of compromise such as IP addresses, hashes, domains, URLs, etc. to a tool and looking for hits within specific time window.
  This is Retroactive Investigation.

To be fair, there are some areas of overlap in the methodologies, skills, and technologies required to perform these functions. But often, security vendors will frame elements of these functions that happen to complement their product as threat hunting, which can create confusion and undermine efforts to build a comprehensive and effective threat hunting function.

Four Essential Pillars of Effective Threat Hunting

Now that we've level-set on what threat hunting isn't, let's dig into what it is, referencing guidance from the **National Institute of Standards and Technology (NIST)** as a starting point. Control number RA-10 in NIST Special Publication 800-53 Revision 5 provides the following definition of threat hunting:

Control:

a. Establish and maintain a cyber threat hunting capability to:
   1. Search for indicators of compromise in organizational systems; and
   2. Detect, track, and disrupt threats that evade existing controls; and

b. Employ the threat hunting capability [Assignment: organization-defined frequency].

Discussion:

Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies. Indications of compromise include unusual

The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses.

network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

For the purposes of our discussion, let's focus on four key concepts in this guidance:

1. ...threats that evade existing controls...
2. ...active means of cyber defense... proactively searching...
3. ...measurably improve the speed and accuracy of organizational responses.
4. ...leverage existing threat intelligence...

These concepts represent the four essential pillars of an effective threat hunting function.

01.

Address Threats that Evade Existing Controls

Threat hunting assumes compromises will be undetected as threat actors evade existing security controls such as firewalls, intrusion detection/prevention systems (IDS/IPS), web application firewalls (WAF's), and endpoint detection and response (EDR) systems. In these cases, security teams must rely on threat hunting to find unknown unknowns or stated differently, the compromises they don't know they don't know about.

02.

Search for Threats Proactively

A proactive threat hunting function must be human -led and hypothesis-driven. While automation can be used as a force multiplier, true hypothesis-based threat hunting moves beyond the unfocused, automated scans that many managed detection and response (MDR) providers perform and ensures that every hunt is guided by:

1. Well-defined motives
2. Specific hypotheses that will be validated
3. Clear completion and success criteria

Doing this well requires dedicated resources with sufficient time to focus on proactive threat hunting. This doesn't mean that the specialized expertise of threat hunters can't ever be called on for other needs. But it's critical to give them focused blocks of time that are exclusively dedicated to threat hunting.

03.

Improve Response Speed and Accuracy Measurable

Building on the point above, it's important not to allow threat hunting efforts to turn into an unbounded research project. They need to produce measurable results. The primary security metric that threat hunting can directly impact is time from initial compromise to detection, often referred to as dwell time. Over time, threat hunting efforts should also have a positive impact on the time it takes to contain, evict, and remediate compromises.

04.

Leverage Existing Threat Intelligence

Without structure, threat hunting can feel like looking for a needle in a haystack. It can be hard to know where to start. It's not as simple as collecting a batch of data or logs and scrolling through it. The signals that matter will be lost in the noise, if threat hunters don't zone out from boredom first. An effective threat hunting strategy must leverage existing threat intelligence to focus efforts where the impact on risk is greatest and identify the specific tactics, techniques, and procedures to

look for. The goal is to extend beyond the telemetry that is inbound from security controls, which would restrict the basis for the hypothesis. Instead, it needs to draw on federated data sources that relate to the organization, based on factors like industry, supply chain, and market profile, and incorporate this federated intelligence into the threat hunt. This positions the threat hunter more as an attacker would, from the outside in.

Understanding these principles also makes it possible to arrive at a more digestible definition of true threat hunting.

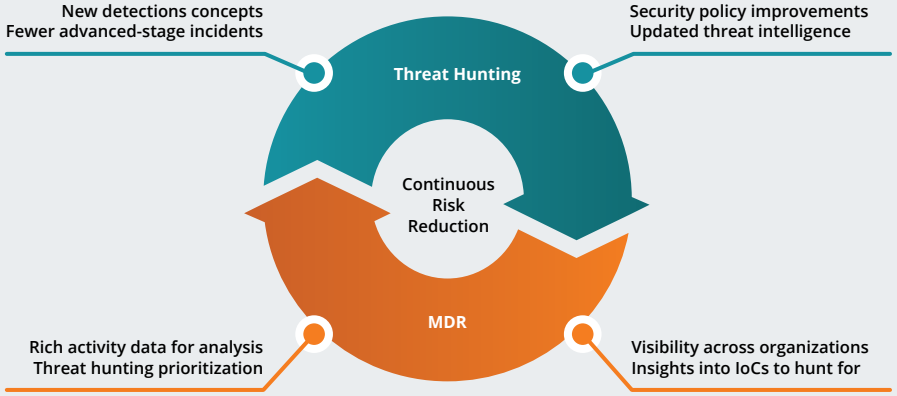
Threat Hunting:
An accurate and concise definition

Threat hunting is a proactive, human-led pursuit guided by threat intelligence that seeks to discover adversary activity, either current or historical, that has evaded existing security controls. Its goals are to reduce dwell time, minimize the negative impact to the business impacts , of security incidents, reduce the attack surface, and improve overall security posture.

Threat Hunting, MDR, and the Risk Reduction Flywheel

At CyberMaxx, we work closely with organizations across diverse industries to implement highly effective managed detection and response (MDR) models. One key thing that sets us apart is our belief that offensive and defensive security play equally important—and highly complementary—roles in risk mitigation.

The relationship between threat hunting and MDR is a perfect example of this concept in action.



MDR / Threat Hunting Relationship

Proactive threat hunting makes MDR more effective by:

- Discovery of new emerging threats and detections for them.
- Reducing the number of situations where the security operations team is blindsided by threats that have escalated to advanced stages.
- Identifying opportunities to improve security policies and controls based on observed threats.
- Enriching the threat intelligence available to the MDR team.

Threat Hunting, MDR, and the Risk Reduction Flywheel (Cont'd)

Similarly, MDR improves the effectiveness of threat hunting by:

- Making large sets of security event data available to support threat hunting efforts.
- Providing zero-latency response capabilities for compromises discovered during threat hunting.
- Identifying trends that appear across multiple customer environments.

This symbiotic relationship produces a flywheel effect where security team effectiveness improves continuously as threat hunting and MDR generate momentum for each other.

Anatomy of a Successful Threat Hunt

Most of the day-to-day work that threat hunters perform identifies areas of risk that have not yet been exploited by threat actors. This is ideal since it:

1. Allows risk mitigation steps to be taken before negative business impacts occur
2. Contributes lessons learned into MDR detection models.

But when active compromise situations are discovered, the impact of tightly integrated threat hunting and MDR functions really shines. Here is an example of how the process works with the CyberMaxx Threat Hunting and MDR teams.

The Hunt

While conducting a hunt for T1087.002 Account Discovery: Domain Account, a known attack method defined in MITRE ATT&CK®, the hunter identified what appeared to be hands-on keyboard activity as well as installation of AnyDesk via a PowerShell script. The hunter then isolated the host on which the commands were run, created a ticket, and escalated it to the client with a phone call. Once off the phone with the client, the hunter initiated the threat response process within the CyberMaxx SOC.

The Response

The threat response team then investigated further and was able to determine that there was no further activity, as isolating the host removed access from the adversary. They were also able to determine that initial access came from an email and attached malicious OneNote document that launched cmd.exe and powershell.exe after being clicked on by the user. Based on the investigation, they were able to "rollback" the machine to a known good state prior to the user clicking on the malicious document. The investigation found the initial compromise happened 31 days prior to being discovered by the hunter.

The Research and Applied Learning

Once the investigation was complete, all information was turned over to the Cyber Threat Intelligence & Research team, along with the malicious OneNote file. Through their investigation of the information provided they determined this intrusion would have eventually deployed Nokoyawa ransomware. They were then able to work with the CyberMaxx detection engineers to create three new detections that protect not just the affected client but all other MDR clients.

The Business Impact

The zero-latency response by the SOC between identification of the threat and engagement of the threat response process was able to contain and mitigate the threat before it became a full-scale ransomware event. This saved the client from a costly Incident Response engagement along with the associated negative business impact of a ransomware incident.

Elevate Your Team's Threat Hunting Capability Today

Whether an organization is building its own in-house threat hunting function or engaging a third-party specialist like CyberMaxx, here are four closing thoughts that should be considered throughout the journey:

Ensure that all stakeholders are aligned on a clear definition of threat hunting

Focus conversations with security vendors on desired outcomes rather than the vendor's product capabilities

Find opportunities to integrate threat hunting with detection and response in ways that allow each set of resources to focus on their role while achieving bi-directional benefits

Measure the effectiveness of threat hunting efforts, starting with the impact on dwell time

At CyberMaxx, we're always here to help.

Our threat hunting and MDR services provide access to elite security talent and best practices with a superior ROI to building these capabilities in-house. We also follow the principles described above to help our customers unlock the combined value of an integrated approach to threat hunting and MDR.

Ready to take the first step? **Talk to an expert** to learn more.