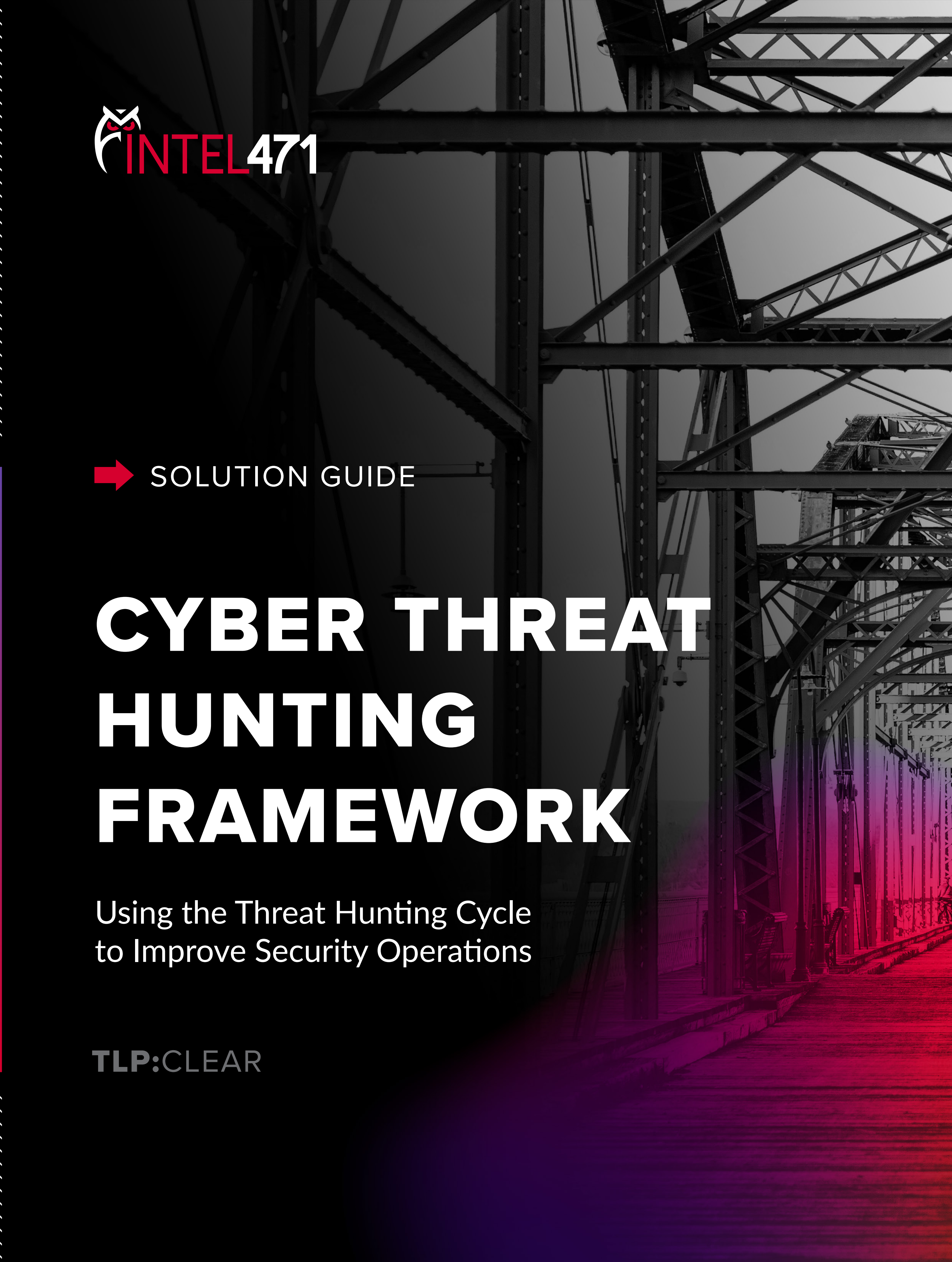


INTEL471

SOLUTION GUIDE

CYBER THREAT HUNTING FRAMEWORK

Using the Threat Hunting Cycle to Improve Security Operations

TLP:CLEAR

TABLE OF CONTENTS

INTRODUCTION

Security teams are faced with the reality that sometimes, adversaries are going to compromise an environment. A user may click on a link in a phishing email that leads to the download of malware that's not caught by endpoint detection software. A threat actor may exploit an unpatched vulnerability in an internet-facing appliance. Compromised credentials could lead to an attacker taking over a highly privileged account, lending access to a domain controller.

> *The threat hunt team's primary objective is to identify undetected threats, close gaps that improve security posture, and develop new capabilities to prevent future breaches.*

However, not all is immediately lost, even when threats gain access and use advanced techniques to evade detection. Behavioral threat hunting provides an opportunity to identify and disrupt the threat actor before they can burrow deeper into an environment and become harder to remove. By cutting short attacker "dwell time" — how long a threat remains undetected in an environment — behavioral threat hunting can stop a serious security incident from escalating into a 'front-page' crisis.

Intel 471's Threat Hunting Framework seeks to provide operational and technical guidance, derived from the collective experience of our dedicated hunt teams and on the shoulders of giants that came before them, who have served in some of the largest organizations around the globe.

This paper explores some of the key obstacles to building a behavioral threat hunting capability and how to overcome them. The framework aims to help security leaders understand the goals of threat hunting, key concepts, prerequisites and benefits, contributions to security operations, and capabilities at different maturity levels.

BUSINESS CHALLENGES

From a business perspective, one of the most critical challenges organizations are faced with are skills shortages for their threat hunting program, which are often heavily reliant on only a few, highly skilled and technical resources. Fluctuations in staffing at these organizations can have direct operational impacts on threat hunting at a time when more organizations treat it as a strategic security capability.

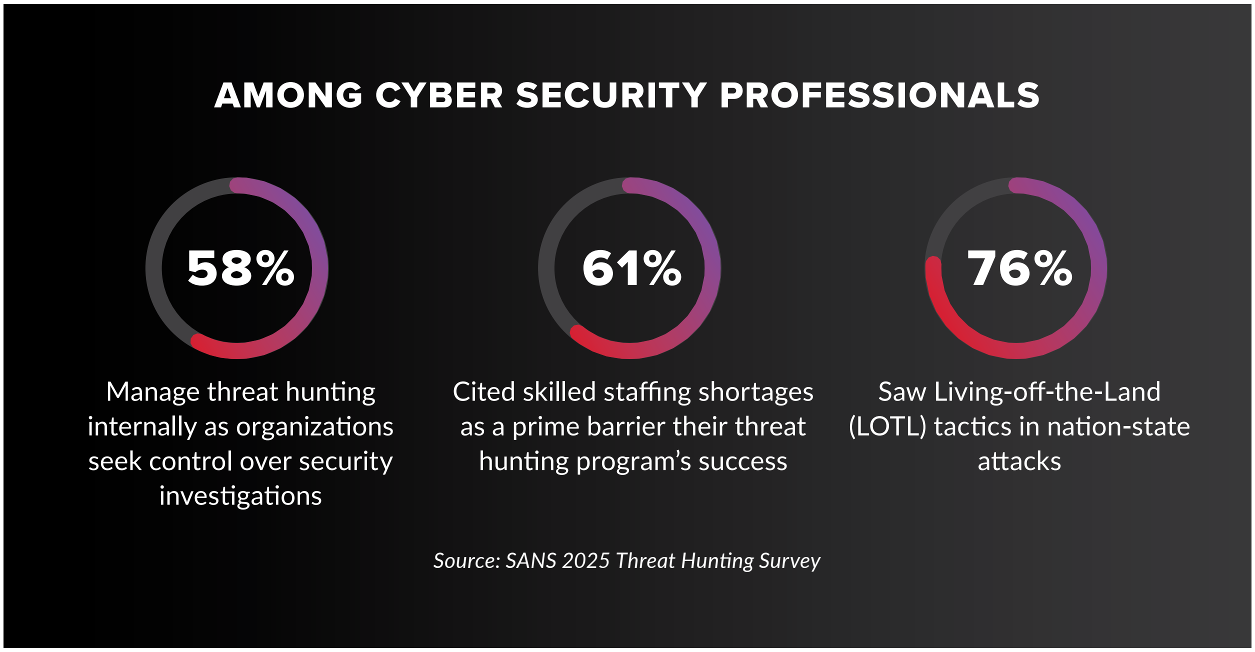
Another challenge organizations grapple with is identifying metrics that demonstrate the value that threat hunting brings to security operations, which can make it difficult for organizations to realize the business value and for the program to secure further funding.

With ongoing skills shortages, and the challenge in measuring hunt success metrics, threat hunting capabilities are often overlooked in favor of traditional security operations or are outsourced where a capability is desired but not yet a strategic priority.

The *SANS 2025 Threat Hunting Survey* found that 61 percent of respondents cited skilled staffing shortages as the primary obstacle to their threat hunting program's success. Skills shortages have been a persistent challenge for many years. However this year SANS identified several key trends that indicate threat hunting has become a strategic priority for combating cyber adversaries who increasingly use advanced tactics to evade endpoint detection and response (EDR) and other detection-based defenses. The importance of threat hunting has become clearer as new regulations have made proactive cyber risk management and digital resilience a responsibility for senior executives and board members.

The survey found the number of organizations that fully outsource threat hunting dropped from 37% in 2024 to 30% in 2025. Meanwhile, a lot more organizations that do have a threat hunting capability now choose to manage the program and scope of hunts internally — up from 46% a year ago to a clear majority at 58% today. The SANS Institute concluded this large shift towards in-house threat hunting capabilities indicated organizations were now prioritizing internal expertise, visibility, and operational control over their threat hunting investigations.

Another major trend that has made threat hunting a strategic priority are adversary tactics. Living-off-the-Land (LOTL) tactics, which use native operating system tools and components to evade detection, was the "most prevalent tactic across all adversary groups, reinforcing the need for behavior-based threat hunting." Some 76% of organizations saw LOTL behaviors in nation-state attacks while LOTL also surged to 49% of ransomware attacks — up from 42% last year.



AMONG CYBER SECURITY PROFESSIONALS

58% Manage threat hunting internally as organizations seek control over security investigations

61% Cited skilled staffing shortages as a prime barrier their threat hunting program's success

76% Saw Living-off-the-Land (LOTL) tactics in nation-state attacks

Source: SANS 2025 Threat Hunting Survey

TECHNICAL CHALLENGES

From a technical perspective, organizations face a number of obstacles establishing a threat hunting capability.

One of the most common technical challenges is a so-called data deficit. Even organizations with mature SOC teams can find the depth and breadth of security event and telemetry data is insufficient to support threat hunting operations. Security teams often discover this when they realize their existing security controls may not provide sufficient data coverage to support more advanced threat hunting.

The ongoing skills shortage also manifests itself as a technical issue for organizations. This remains a challenge as more organizations embark on their threat hunting journey and discover the need for not only skilled personnel and resources to develop operational capabilities, but frameworks, methodologies, and tools to support well-defined hunt processes and enable effective and reliable hunts.

Despite these significant challenges, there are strategies to enable reliable, repeatable, and robust hunting capabilities at different stages of hunt program maturity.

Before exploring threat hunting, however, it is valuable to first examine the definition of threat hunting and the role that it plays in a mature security operations team.

THREAT HUNTING SECURITY OPERATIONS

THREAT HUNTING DEFINED

Threat hunting is a methodology for *identifying* cyber threats that have infiltrated systems undetected. There are tools to help threat hunting teams, but it is not a technology or solution. The threat hunting team's primary objective is to **identify unknown and undetected threats, close security gaps** that improve security posture, and **develop new capabilities** that prevent future breaches. This definition has two critical components:

Threat hunting must be iterative. A hunt (the commonly accepted term for activity carried out by these teams) has value in its execution, but only for the duration of its execution. Once the hunt is complete, any subsequent malicious activity may remain unidentified. Therefore, hunts need to be carried out in an iterative fashion based on the prevalence of the technique, and the relative risk to the organization.

Threat hunting must be proactive. The objective of threat hunting is, ultimately, to identify previously undetected malicious activity in an environment. This objective is accomplished through a variety of analysis methods, especially those involving behavioral and statistical analysis. This process, however, absolutely does not rely on searching through an environment using atomic indicators of compromise (IOC). That practice belongs strictly to the domain of traditional security operations, not threat hunting.

THE RISING ROLE OF BEHAVIORAL THREAT HUNTING

A combination of forces, including new cyber regulations and evolving advanced threats, are driving more organizations to adopt proactive cyber risk management measures. Wider threat actor usage of advanced techniques to evade detection have also made it imperative for organizations to proactively identify and disrupt threats already inside their environment and continually improve security posture to prevent future breaches.

This proactive approach can be achieved with structured behavioral threat hunting, which is a formalized search for the tactics, techniques, and procedures (TTPs) used by actors that are a high risk to the organization. Threat hunters identify TTPs in internal and external CTI and build "hunt content" in the form of queries to search for evidence of TTPs and behaviors in security logs within the organization's endpoint detection and response (EDR/XDR), security information and event management (SIEM) platform, or a data lake on platforms. The hunt team also identifies and addresses system misconfigurations and blindspots that hinder threat hunting. Findings discovered during the course of iterative threat hunts result in several "outputs" (discussed below), which contribute to new mitigations that close security gaps and provide key inputs to new capabilities that support the security operation's mission to efficiently catch threats using automated detections.

An important question hunt program leaders often consider is which of several hunt methodologies to adopt for their program and whether their available skill resources can support it. The SANS 2025 Threat Hunt Survey found 45% of organizations had adopted a formal methodology while 38% had not. While no single methodology dominates the landscape, SANS noted that many organizations are using frameworks such as TaHiTI, an approach to intelligence-driven structured threat hunting that establishes a hunt-intelligence feedback loop; the Pyramid of Pain, which clarified the value of threat hunting durable TTPs versus ephemeral historical indicators of compromise (IOCs); and MITRE ATT&CK, which many teams use to visualize their defensive coverage of TTPs.

Regardless of methodology, what matters is that hunts are consistent, rigorous, and repeatable. Organizations can overcome skills shortages and drive their hunt methodology by pairing internal hunt teams with externally created behavioral hunt content. This is comparable to enhancing detection-based defenses with new custom detections, but instead uses external hunt content to improve a human-led team's mission to find and disrupt undetected threats.

External hunt content can come from a variety of sources. Security platform vendors often provide platform-specific hunt queries. There are also freely available machine-readable hunt queries. Some organizations extend hunt team capabilities with dedicated hunt content platforms, such as HUNTER from Intel 471, which contains a library of pre-built queries for multiple platforms with CTI contextualization and human-readable documentation to support team usage.

Pairing threat hunt teams with a library of hunt queries offers teams the flexibility to divide threat hunter and analyst resources among different priorities to increase hunt cadence, improve response times to emerging threats, and expand their defensive threat coverage. A simple example is allocating more experienced hunters to creating novel hunts for threats unique to their environment while assigning other members, such as mid-tier analysts, to recurring behavioral hunts for frequently seen TTPs using ready-made pre-validated hunts. Performing a higher number of proactive and recurring hunts across an environment prevents future threats and reduces visibility gaps.

THREAT HUNTING OUTPUTS

☑ INTELLIGENCE FEEDBACK LOOP

Threat hunting and threat intelligence are vital for each other. CTI can contextualize hunt findings. New CTI on an adversary's TTPs may broaden the scope of a hunt and refine the hunt hypothesis or spark new ideas for future hunts. Hunts can provide contextualized signal generation and new CTI data, improving the feedback loop between the hunt and intelligence teams. Threat hunting also provides threat emulation and foundational content for new detections — the result of moving "unknown" threats discovered during a hunt to "known" threats that the SOC can automatically trap and stop in the future.

☑ NEW THREAT DETECTIONS

Upon discovery of a previously unknown threat within an environment, threat hunters and incident responders will analyze the activity and tool sets. This analysis should ultimately result in the development of threat detection content..

☑ INDICATORS OF COMPROMISE (IOC) CREATION

While threat hunting does not rely on traditional IOCs, threat hunting identifies and collects IOCs that are deployed into traditional security controls, threat intelligence platforms (TIPs), signatures, or used for immediate blocking.

☑ RED TEAM ENHANCEMENT

A less obvious output of threat hunting is as a source of research for red team engagements. Threat hunting activities can serve as real-world inspiration for red team adversary methodologies, as well as to test threat detection content creation.

☑ RUNBOOKS AND MITIGATIONS

Other output of threat hunting is enhanced documentation which often takes the form of runbooks and mitigation recommendations. This documentation often serves two purposes. First, they form the basis for operational processes and methodologies used on repeated hunts. Secondly, they should serve as guides for incident response analysts to investigate any identified behaviors during the threat hunt campaign. This ensures that analysts investigating are provided with consistent analysis methodologies and remediation guidelines. These runbooks and mitigation recommendations become mission critical for the successful deployment of threat hunting operations.

☑ DRIVE INCIDENT RESPONSE ENGAGEMENTS

Another obvious output of successful hunts will be new incident response engagements. It can be tempting to amalgamate traditional incident response with threat hunting. Indeed, both teams draw on many similar skill sets. However, if an organization has a dedicated incident response team and processes, the threat hunt team should direct any identified malicious activity to incident response teams.

Threat hunting can enhance incident response with detailed threat hunt documentation, runbooks, mitigations, and post-incident hunting content and supplemental context and intelligence.

REQUIREMENTS FOR THREAT HUNTING

Threat hunting, as a capability, has certain requirements, much like other cybersecurity disciplines. While some would assert the need for a particular technology or brand, the reality is that threat hunting is primarily a methodology that has a set of prerequisites around technological and personnel parameters. It should be noted that a lack in one area doesn't prohibit threat hunting, but it may hinder it.

EMULATION & VALIDATION

Threat hunting is a critical aspect of modern cybersecurity, as it enables organizations to identify and respond to attacks before they cause significant damage. However, to be effective, threat hunting needs to be supported by robust and reliable testing capabilities. Emulation and validation are essential components in the threat hunting process, as they allow organizations to test and validate their defenses before and after they are implemented.

Emulation and validation enable organizations to simulate an attacker's behavior in a controlled environment, allowing them to identify and address vulnerabilities, improve their incident response procedures, and measure the effectiveness of their security controls. By using these capabilities, organizations can enhance their threat intelligence, as they gain valuable insights into the tactics and techniques used by advanced adversaries.

Moreover, emulation and validation can help organizations demonstrate compliance with industry standards and regulations, by providing proof that their security controls are functioning as intended. This is particularly important for organizations that are subject to strict regulatory requirements, as it can help them avoid costly penalties and fines.

Emulation and validation capabilities are a pre-requisite for effective threat hunting. By simulating an attack, organizations can validate their defenses, improve their incident response procedures, and enhance their threat intelligence. This, in turn, helps organizations to protect themselves against cyber threats and maintain compliance with industry standards and regulations.

TECHNOLOGICAL PRE-REQUISITES

One of the primary questions often asked during the research phases for organizations looking to establish threat hunting teams is, “What technological prerequisites are needed for threat hunting?”

TOOL AND DEPLOYMENT GAPS

Threat hunting at its core depends on visibility at the network and host level. You can’t hunt for what you can’t see and not all systems are built or deployed to generate required logs for threat hunting. The more granular the data and visibility, the better it is for hunters to examine data for an adversary’s known behaviors. Technological gaps that can impede threat hunting center on the capabilities of the security tool itself and how the technology is deployed.

Some environments may not have network proxies deployed, or network intrusion detection signatures (IDS) or NetFlow data isn’t being captured on the correct network segment. Another example is where a SIEM platform cannot correlate or aggregate data, which can make threat hunting extremely difficult when attempting to filter relevant data from thousands of logs.

BREADTH AND DEPTH

Threat hunting requires both breadth and depth of data. This data is often generated by endpoint agents that record changes to the state of a system or appliance that records network traffic.

STORAGE

An effect of greater visibility is more data. Organizations often find their storage needs increase dramatically as they integrate prolific log sources. Today, organizations can store terabytes or even petabytes of security log and telemetry data for incident response purposes. Guidance on log retention by national authorities emphasizes that it can take 18 months to discover a cyber incident and 200 days for malware to manifest into harm.

ANALYSIS PLATFORM

A minimum requirement for threat hunting is a platform for data aggregation and correlation. These platforms allow threat hunters to examine data from a number of different angles. For threat hunting, security information and event (SIEM) platforms or a data analytics platform is more critical than dedicated threat hunting platforms. The most important requirement is that the platform supports multiple methods for analysts to enrich, correlate and visualize data.

PERSONNEL PREREQUISITES

Another question organizations frequently ask when establishing a threat hunting capability is “What type of people do I need for threat hunting?”

Many security leaders considering this question are often also weighing up how to develop structured hunt processes and build a team in the face of hiring difficulties. A good place to start solving this question is by **defining the key goals of threat hunting** and **breaking down the core skills of a threat hunter into parts**. The goal is to build a successful threat hunt team rather than building a team of ideal threat hunters.

The goal is to build a successful threat hunt team rather than building a team of ideal threat hunters.

A key advantage for any individual threat hunter is an extensive knowledge of the mechanics of an operating system (Windows, Linux, macOS and mobile platforms), especially for hunters engaged in structured or hypothesis-based hunting. The team should have a deep knowledge of adversary TTPs and a comprehensive awareness of the organization’s IT environment. The team also benefits from members who have **industry specific experience** and **organizational knowledge**. These members are more likely to know where to spend their hunting efforts searching for threats and the options they have to prevent adversary tactics. As a team, they must understand the organization’s critical process chains, privileged access, network access, architecture, applications, defense technologies, and incident response.

The team should have a combination of strengths across **four main skill sets.** Expertise from each domain can guide the hunt team on its mission. These include:

1. **Offensive mindset** needs can be met by security researchers or intelligence analysts who have studied how an attacker can use systems and bypass controls to achieve their goals.

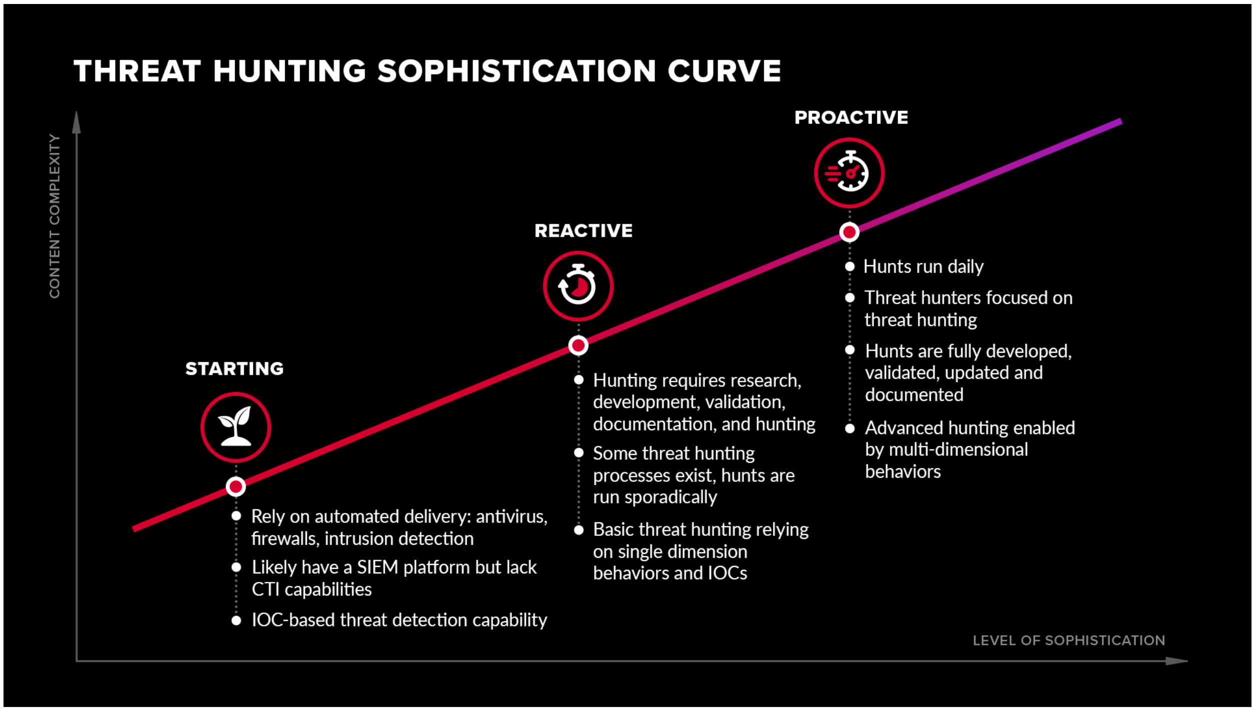
2. **Security architecture** knowledge can be covered by a network engineer or application security specialist — a person who understands how systems interconnect, what controls exist, and whether controls can be configured to close gaps.
3. **Data analysis skills** can be specific to information security or from outside of the field. This person is vital for identifying patterns and anomalies from large datasets of endpoint and network logs.
4. **Organizational and core systems knowledge** can come from a veteran who may have built the technologies hunters are defending.

Team Maturity and Operational Awareness. The hunt team also needs the maturity to understand that not finding threats on every hunt is not a failure; identifying and closing gaps and creating new capabilities are core parts of hunting that help prepare the organization for attacks in the future.

The hunt team works closely with threat intelligence to identify emerging threats for new hunts. It also supports the security operations (SecOps) team's mission by enriching threat findings to identify characteristics that can be used to create **new, high-fidelity detections.** This creation transitions threats from the "unknown" to "known" threats, which SecOps can efficiently trap with detections in the future. The hunt team should already be stalking adversary behaviors where detections are not possible.

HUNT TEAM MATURITY

Threat hunting has become a critical component of modern cybersecurity defenses, as organizations are constantly facing evolving threats in the ever-changing threat landscape. Threat hunting is the process of proactively seeking out threats that have evaded initial detection by security systems. As organizations mature in their threat hunting capabilities, they are able to better identify and respond to security incidents in a more efficient manner. In this section, we will explore the three levels of threat hunting maturity and how organizations can maximize their threat hunting efforts.


THREAT HUNTING SOPHISTICATION CURVE
CONTENT COMPLEXITY
LEVEL OF SOPHISTICATION
STARTING
Rely on automated delivery: antivirus, firewalls, intrusion detection
Likely have a SIEM platform but lack CTI capabilities
IOC-based threat detection capability
REACTIVE
Hunting requires research, development, validation, documentation, and hunting
Some threat hunting processes exist, hunts are run sporadically
Basic threat hunting relying on single dimension behaviors and IOCs
PROACTIVE
Hunts run daily
Threat hunters focused on threat hunting
Hunts are fully developed, validated, updated and documented
Advanced hunting enabled by multi-dimensional behaviors

STARTING

The first level of threat hunting maturity is “Ad Hoc.” Organizations in this category rely heavily on automated alerting, generated from security controls such as antivirus, firewalls, and intrusion detection and prevention systems. These organizations will also likely have a platform for log and data aggregation, such as a security information and event management (SIEM) platform but will have no true threat intelligence capability. The challenges for organizations at this level include finding and retaining talent, developing threat hunting processes, dedicating time to threat hunting efforts, and centralizing management of threat hunting efforts.

REACTIVE

The second level of threat hunting maturity is "Reactive." Organizations in this category have developed sufficient visibility into their environment to conduct mature threat hunting, but their focus is primarily on reactive efforts, such as responding to emerging threats. They will typically be capable of producing their own organization-specific threat intelligence and will employ more advanced analysis methodologies, such as structured or hypothesis-based hunting. However, they may still lack the time and resources to fully mature to true proactive threat hunting. The challenges for organizations at this level include further developing threat hunting processes, dedicating time to hunting, and centralizing management of threat hunting efforts.

PROACTIVE

The third level of threat hunting maturity is "Proactive." Organizations in this category have largely addressed the staffing-related issues found in the previous two categories and are able to develop their own hunting content, queries, and threat detection content. These organizations are often able to publish their findings and develop community content used by organizations in lesser classifications. The challenges for organizations at this level include time, as the sheer number of hunts required to be researched, developed, and actioned exceeds the amount of time available. Additionally, there is still a requirement to further the management of threat hunting activities, such as providing concrete evidence of a return on investment and routinely communicating the value that threat hunting plays in their organization.

To maximize their threat hunting efforts, organizations should strive to reach the proactive level of threat hunting maturity. This requires a dedicated effort to develop the necessary skills and processes, as well as the investment in the right tools and resources. It also requires a strong commitment to threat hunting as a critical component of their overall security strategy. By leveraging the right tools, acquiring the necessary skills, and making threat hunting a regular part of their security program, organizations can maximize their threat hunting efforts and take full advantage of this critical practice.

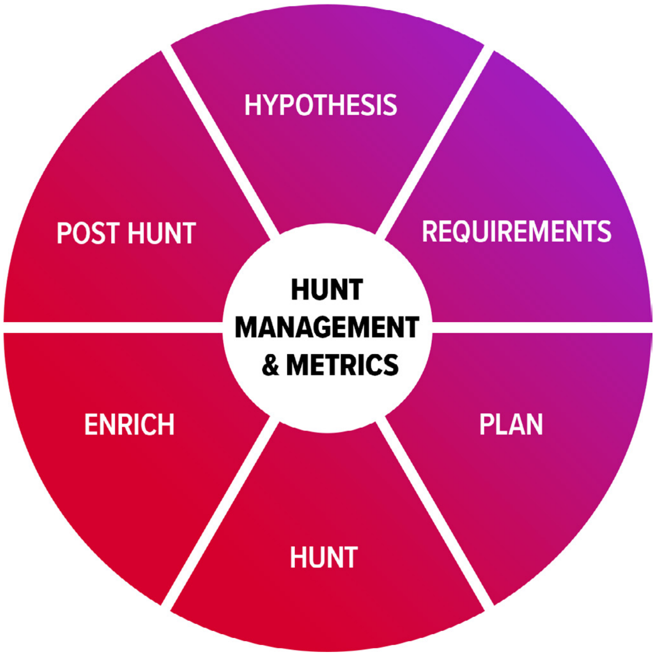
Threat hunting maturity is a critical component of modern cybersecurity defenses. By understanding the three levels of threat hunting maturity, organizations can better assess their own threat hunting capabilities and take steps to maximize their efforts. Whether an organization is just getting started or is already well into their threat hunting journey, there is always room for improvement and growth. By dedicating the time and resources to threat hunting, organizations can stay ahead of the curve and avoid missed opportunities.

THREAT HUNTING CYCLE

Threat hunting, like many disciplines in the cyber security field, should aspire to be consistent, rigorous, and repeatable. This is because while hunting on its own is valuable, the true value is derived from repeated hunts where organizations have confidence that the activities being conducted are both consistent and thorough.

Compare a hunt to a scan of a system by an antivirus agent. The value the antivirus agent provides is not merely the result of single scan, but the continuous protection it affords an organization. Threat hunting, from a security and value perspective, is no different.

Therefore, in order to conduct hunts that are consistent, rigorous, and repeatable, it is beneficial to establish and adhere to a cycle which is similar to the many existing cycles established in various cyber security sub-disciplines, such as the incident response preparedness cycle, the threat intelligence cycle, or the security analysis cycle. Several past publications have proposed cycles referred to variously as “The Hunting Loop,” or “The Threat Hunting Lifecycle,” and while these cycles have tremendous merit, Intel 471 has synthesized these cycles, as well making modifications to address existent limitations in other cycles, into what we call, eponymously, the Threat Hunting Cycle.



Threat Hunting Cycle

HYPOTHESIS

Hypothesis-based hunting is covered in more detail in the following sections, however it is important to understand that the hypothesis aims to describe a particular area for inquiry and investigation and need not exclusively be a scientific hypothesis.

These hypotheses may originate from a variety of sources, including the organization's cyber threat intelligence, such as malware indicators, known and exploited vulnerabilities, intelligence-driven purple team engagements, previously reported incidents, and threat hunters themselves.

EXAMPLE OF A HYPOTHESIS

A hypothesis could be a formal statement:

- Increasingly, attackers have concealed their command and control (C2) traffic in encrypted TLS/SSL, however through volumetrics, frequency, and statistical analysis, it is possible to identify anomalous covert channels.

However, it could also simply be an area for investigation:

- Parse, output, and identify all User-Agent Strings (UAS) observed across an environment to identify statistical anomalies.

REQUIREMENTS

The next step in the Threat Hunting Cycle is for organizations to develop the requirements necessary to prove or disprove the hypothesis. These requirements may be quite obvious initially — for example, observing the user-agent strings across an environment would require either HTTP metadata from net flow or endpoint security controls. However, in the development of requirements it is likely that organizations will discover specific technological limitations or even blind spots (i.e. recording of net flow data is limited to specific ports, or that the endpoint agent only stores historical data for 13 days).

These identified limitations and blind spots will need to be adapted and overcome for the purposes of the hunt (i.e. perhaps expanding the number of ports HTTP metadata is available for, to include widely abused ports, or doing sequential pulls of endpoint logs every 12 days) but they should also be noted and investigated during the Feedback phase in order to ensure ongoing improvement.

WHAT SHOULD I HAVE FOR REQUIREMENTS?

- Determine if the hunt requires network visibility? Endpoint visibility? Or both.
- Identify the log sources that would allow hunters to identify the activity.
- Consider the tools that could be used to gather more in-depth information.
- Determine any special skillset requirements you have for the hunt (for example, the expertise of a data scientist).
- Document technical limitations and blind spots, but also how you would overcome them.

PLAN

Hunt teams must develop a formal, written, plan (often referred to simply as a "hunt plan") where the particulars of the hunt are laid out. While there is no formal format for these plans they should also act as a living document that can be used moving forward both for the coordination of the existing hunt amongst multiple team members, as well as a guide for future hunts.

This plan should clearly lay out the established hypothesis, the technological and operational requirements, the time frame for the hunt (i.e. quarterly, monthly, etc.), additional support from external teams that hunters may require; the actions that will be carried out during the hunt in the form of playbooks; analysis and validation methodologies employed in the form of runbooks; the agreed method of incident reporting should a compromise be identified; and, a crucial point that is often overlooked, a record of points for improvement from previous hunts and efforts or changes in methodology or technology to address those points. This last point prevents situations from developing where activities are carried out of habit.

HUNT

The Hunt phase is where the actual execution, laid out in the hunt plan, is carried out. This step will vary depending upon the sources of data, analysis methodologies, and additional roadblocks or challenges that are encountered. Any findings (e.g. true positive and negative, as well as false positive and negative) or challenges experienced by the hunt team, during the Hunt phase, should be recorded in the hunt plan, as it will serve as the basis for the documentation produced.

ENRICH

The Enrich phase is a step that is often forgotten altogether. The role of the enrichment process is as important as the Hunt phase itself. During the Enrich phase, positive identifications of previously unknown malicious activity will be analyzed for attributes which can be detected in the future, and detection content based on some aspect of the attack, tool, or malware (e.g. communication patterns or infrastructure, or pro grammatical behaviors or attributes) needs to be created. This process ensures that moving forward, detections of identified and known threats are carried out by traditional security operations capabilities, and not wasting a hunt team's time on known threats.

However, detection content is not the only output of the Enrich phase. Additionally, new documentation of the newly created threat detection content (especially analysis and validation steps), and findings regarding the environment (especially around identified false positives and negatives) should be created, and existing documentation should be enriched with the findings. This process ensures that threat hunting serves to improve the overall processes in the security operations cycle.

POST HUNT

The Post Hunt phase is the final component of the Threat Hunting Cycle, and it's essential for continuous improvement and the development of a mature threat hunting capability. One of the most critical elements of this phase is feedback, which should be sought not only from the threat hunters themselves but also from the support teams involved in the hunt and the recipients of the hunting outputs, such as incident response, threat intelligence, security analysts, and business focused stakeholders. This ensures that all parties can identify the strengths that should be preserved and the weaknesses that must be improved.

REPORTING & METRICS

Another important element of the Post Hunt phase are reporting and metrics. Demonstrating the value and impact of threat hunting to upper management and business stakeholders can be challenging, especially as the outcomes of a successful hunt may not always be immediately apparent or measurable. Reporting provides tactical information to readers and gives teams the ability to show key outcomes and benefits that were achieved during a single hunt, even if no bad actors or malicious activity were found within an environment during a hunt.

Another dimension to the successful communication of value that threat hunting provides are metrics. Metrics allow security leadership to provide operations and strategic information about the overall value that threat hunting has provided to the organization. While the individual metrics that an organization may vary significantly based on stakeholder requirements, a key area of consideration should be hunt outcomes.

HOW TO MEASURE A HUNT'S SUCCESS WHEN "BAD" ISN'T FOUND

- Increased visibility and understanding of the environment
- Identification of visibility gaps and misconfigurations
- Improved incident response readiness
- Enhanced security posture
- Better correlation of data
- Enhance the knowledge of the team
- Test incident response plans.

A successful threat hunt outcome can be determined by a variety of factors, including increased visibility and understanding of the environment, identification of visibility gaps and misconfigurations, improved incident response readiness, enhanced security posture, better correlation of data, enhancement of the team's knowledge, testing of the incident response plan, and enhancement of the team's knowledge of the environment. Therefore, even a hunt that doesn't result in positive threat identification can be viewed as a successful outcome that can help an organization better understand and protect against future potential threats.

Hunt metrics, generally, and outcomes specifically can help organizations show the holistic value of threat hunting to an organization and how hunting has helped to improve the overall posture of the organization against the modern threat landscape.

CENTRALIZED HUNT MANAGEMENT AND METRICS TOOLS

As teams grow, they need tooling to perform consistent and repeatable processes that improve structured threat hunting methodology, which helps hunt teams stay ahead of undetected threats and evolving adversary behaviors. To achieve this, the program should also consistently measure metrics that demonstrate risk reduction from the hunt program, such as threats and TTPs identified, mitigations implemented, new automated detections derived from hunts, and hunt-driven improvements to security posture and network visibility.

A key feature of the HUNTER platform is the **Hunt Management Module**, a centralized hunt management tool for tracking and measuring key hunt performance metrics, coordinating collaborative hunts, and managing hunt queries. Threat hunting teams use the module to document findings, collect analyst notes, and share runbooks and mitigations. It also provides threat hunt reporting that can be easily exported and shared.

The Hunt Management Module helps organizations adopt a hybrid approach to hunt content, allowing teams to bring their own custom hunt packages to the HUNTER platform. The "Bring Your Own Hunt" support in the Hunt Management Module allows your threat hunters to leverage the same methodology used for HUNTER packages, each of which include the behavioral query logic, deployment requirements, emulation and validation files, up-to-date CTI, threat actor profiles, hunt documentation, runbooks, and recommended mitigations. This can be more effective and less cumbersome than spreadsheets, wikis, or general-purpose content management tools.

While hunting itself can take time, teams at all hunt maturity levels struggle to create new and up-to-date hunt content with the threat contextualization hunters need to coordinate with incident response or the security operations center (SOC). Organizations building in-house hunt capabilities overcome this with an external threat hunt content platform that serves either as a foundation for new hunting capabilities or to augment and unblock constraints on producing new hunts for teams with mature hunt capabilities. Hunt content platforms contain a robust library of pre-validated "hunt packages" for most observed TTPs that the security community tracks. Packages should support query languages for widely-used security and data analysis platforms. This enables teams to bypass the research and development phase for most behaviors and begin the search for previously undetected threats in their environment.

HUNTING IN ACTION

Many organizations seeking to begin developing — or mature existing — hunt capabilities are likely to ask the simple, and yet pointed, question: “How do I hunt?”

The answer to that question, however, is as varied as the number of people one asks it to, and perhaps even more so. With that being said, there are conceptual models developed to group types of hunting together.

STRUCTURED HUNTING

Structured hunting, otherwise known as hypothesis-based hunting, is a category that is based on a central hypothesis about attackers and their associated tactics, techniques, and procedures (TTP). This type of hunting is typically reserved for hunt teams in more mature, proactive, organizations. Unlike the Hypothesis phase of the Threat Hunting Cycle, hypothesis-based hunting is developed strictly around a scientific hypothesis, that is a formal statement which must be falsifiable, and is often driven by organizations’ threat intelligence capabilities, but may also be informed by a hunter’s skillset and experience.

UNSTRUCTURED HUNTING

Unstructured hunting, often referred to as data-based hunting, is a category which is not based on a central hypothesis but rather on observable data. This style of hunting is often where organizations that have not yet started hunting, or who conduct ‘reactive hunting’ start their hunting activities, and it may employ analytical constructs such as “the principle of least seen,” and use techniques such as stacking, clustering and others, as described below.

THREAT HUNTING TACTICS

There are a number of tactics that threat hunters use for both structured and unstructured hunting. While this list is not exhaustive, it is meant to provide some insight into tactics threat hunters often use in their hunts. Note that none of these tactics are exclusive, and several can, and should, be used in tandem as seen in the TaHiTI methodology.

INTELLIGENCE-DRIVEN

Intelligence-driven hunting is a tactic used in structured hunting whereby hunters use reporting from internal and external threat intelligence providers in order to develop a hypothesis. This type of hunting will rely very heavily on the quality of intelligence reporting generated and consumed by organizations. When a new vulnerability or attack technique is released, threat intelligence reporting will document the attack, and that will often form the basis for a new hypothesis.

TARGET-DRIVEN

Target-driven hunting is a tactic that acknowledges that hunters have both limited time and resources, and that while attackers may gain access through a number of avenues, their ultimate targets are often similar: specific networking infrastructure and large data repositories. Therefore, when reviewing hunt plans, for organizations with limited resources, these targets should be prioritized.

TECHNIQUE-DRIVEN

Technique-driven hunting is a tactic for hunting that seeks to concentrate on one, or a series of, techniques that attackers are likely to employ. These techniques are often, but not always, derived from the MITRE ATT&CK framework, and seek to uncover all usage of that technique in the environment, regardless of whether it is legitimate or not. This tactic relies heavily on threat hunters' skills and experience with the various operating systems within the environment.

THREAT HUNTING TECHNIQUES

Similar to the described tactics, threat hunters frequently employ various techniques for structured, and especially unstructured, hunting. This list is most certainly not exhaustive but may serve to illustrate methods threat hunters may use during an active hunt.

☑ VOLUME ANALYSIS

Volumetric analysis looks at the volume of a particular activity in relation to all other activities. While this method is often thought of in terms of network traffic, it can be applied more broadly to any activity on a system, such as the number of processes with unusual paths, the number of particular users' activities across an environment, or any other aspect which can be sufficiently measured and visualized.

EXAMPLES COULD INCLUDE:

- How much data did endpoints send out of the network?
- Which endpoint sent the most data?
- What external IP had the greatest number of blocked connections?
- Which systems have had the longest sessions?
- What systems have had the most AV alerts?

☑ FREQUENCY ANALYSIS

Frequency analysis is like volumetric analysis. Instead of volume, it examines frequency of an occurrence. This technique is most often applied to network traffic at both the network and host levels. Hunters will use it to identify anomalous patterns often found in malware beacons.

☑ CLUSTERING ANALYSIS

Clustering analysis is a method of statistical analysis. This technique will often look at both network- and host-based characteristics. Clustering will group data around a particular set of characteristics in aggregate. This technique is often aided by statistical analysis tools. Clustering can help identify things such as outliers such as an uncommon numbers of occurrences of a common behavior

☑ GROUPING ANALYSIS

Grouping analysis is similar to clustering analysis, but instead of clustering based on a an aggregate of various characteristics, grouping seeks to group the data based on the occurrence of specific simultaneous conditions. Grouping analysis can often reveal previously unknown tools or actor behaviors.

EXAMPLES OF CHARACTERISTICS THAT YIELD RESULTS WHEN GROUPED INCLUDE:

- Outbound network source — This shows hosts that may be bypassing web content filtering.
- Domain Name Servers — This will reveal hosts that may be using non-standard DNS servers.

☑ STACK COUNTING (STACKING)

Stack counting, or more simply "stacking," is an analytical method which can be effectively used against finite data sets (i.e. a particular business unit, department, organizational function) and involves aggregating and counting the number of times a condition is observed, with the intent of identifying statistical extremes in either direction. An example which often yields results is looking at the directory that key Windows files are observed in. This can identify, for example, binaries masquerading as legitimate files.

EXAMPLES OF DATA THAT CAN BE EFFECTIVELY STACKED INCLUDE:

- User Agent Strings
- High (ephemeral) port numbers
- Specific file names and their locations
- Installed programs across an organization
- Process names and execution paths across a department

LONG-TERM BENEFITS OF THE HUNT

Threat hunting is a proactive and systematic approach to identifying and mitigating potential threats to an organization's network, systems, and data. When executed correctly, threat hunting can provide a number of long-term benefits to organizations, and can help to ensure that they remain secure against a wide range of threats. These benefits can be grouped into three key categories:

1 DRIVING STRATEGIC DECISIONS:

One of the key benefits of threat hunting is that it provides organizations with valuable information and insights that they can use to make informed and strategic decisions about their security posture. As organizations conduct regular proactive threat hunting, they will validate the effectiveness of their existing security tools and identify any visibility gaps that exist within their network. These gaps can be categorized into two major groups: visibility gaps (which are often identified during the validation process) and technology gaps, where an organization routinely needs access to specific technological capabilities that it doesn't possess.

By identifying these gaps, organizations can make informed decisions about what technological capabilities and visibilities should take priority in order to best protect their network and assets. This can help to ensure that they are able to stay ahead of emerging threats, and can provide peace of mind knowing that their network is protected against a wide range of potential threats.

2 IDENTIFYING CURRENT/FUTURE THREATS:

As threat hunt teams mature, they will begin to categorize their hunting efforts into two primary groups: targeted threat behaviors and continuous threat behaviors. Targeted threat behaviors are specific to a particular threat or adversary, and are designed to answer a specific question such as "have we been impacted by this specific threat?" On the other hand, continuous threat behaviors are suspicious or malicious behaviors that are exhibited by multiple threats.

By hunting for both targeted and continuous threat behaviors, organizations can stay ahead of the curve when it comes to identifying and mitigating potential threats. This can help to ensure that they are able to stay ahead of emerging threats, and can provide peace of mind knowing that their network is protected against a wide range of potential threats.

3 MAXIMIZING ROI ON PEOPLE/TECHNOLOGY:

Finally, threat hunting helps organizations to maximize the return on investment from both people and technology. From a people perspective, threat hunting utilizes individual skills and talents, especially highly technical security resources. However, it is important to note that institutional knowledge from other technical groups (such as account management or system administration) can also be highly valuable and can help to ensure that individuals wanting to further develop their careers are given the opportunity to do so.

In terms of technology, threat hunting enables organizations to maximize the capabilities of their security tools by using the telemetry data to its fullest extent possible. This can help to ensure that organizations are getting the most out of their investments, and can provide peace of mind knowing that their network is protected against a wide range of potential threats.

In conclusion, the long-term benefits of threat hunting are many, and can help organizations to stay ahead of emerging threats, make informed and strategic decisions about their security posture, and maximize the return on investment from both people and technology. By conducting regular proactive threat hunting, organizations can ensure that their network is protected against a wide range of potential threats and can provide peace of mind knowing that their security is in good hands.

CONCLUSION

As the threat landscape continues to evolve, and adversaries carry on developing their overall tradecraft, organizations are aware of the growing limitations posed by traditional security practices. As a result, more organizations are looking to threat hunting as a means of further maturing their overall security operations, and therefore, the requirement to understand what threat hunting is (and equally, what it isn't!), and the role hunting plays in the overall security processes are more important than ever.

Threat hunting as a capability does not supplant traditional security operations. Rather, it serves as a vital component of the overall security apparatus. Threat hunting not only detects hidden threats but also to improve threat detection content, provides security playbooks and runbooks, and is a key input for threat intelligence, incident response and red/purple team engagements.

Intel 471's HUNTER is a key tool for enhancing and amplifying threat hunt team capabilities at all hunt maturity levels. HUNTER is a threat hunting content and centralized hunt management platform that helps threat hunters proactively identify unknown and undetected threats before they manifest into a more serious event.

At the heart of the platform is an expanding library of hundreds of "hunt packages." These packages contain intelligence-driven threat hunt queries that allow security teams to query their SIEMs, XDRs, EDRs, or other logging platforms and security tools to hunt for suspicious activity that could indicate a compromise. The pre-validated queries empower security teams to jump immediately into threat hunting and spend less time crafting queries and more on investigations and remediation. This provides scale and efficiency, allowing for more hunts, an increase in hunt cadence, and improved response times for emerging threats. The queries are derived from Intel 471's cyber threat intelligence (CTI), which collects real-time malware indicators and the tactics, techniques, and procedures (TTPs) of threat actors.

The platform contains a suite of tools for managing hunts across teams, documenting findings and mitigations, measuring key hunt performance metrics, and providing MITRE ATT&CK technique gap analysis.

EXPERIENCE HUNTER THREAT HUNT PACKAGES

Discover how HUNTER can take your threat hunting team to the next level. Sign up for the HUNTER Community Edition to gain free access for one month to dozens of pre-validated hunt packages written for your security and data platforms.

The HUNTER platform offers:

- Behavioral threat hunting packages that identify adversary activity based on TTPs, not IOCs
- Coverage of emerging threats, including ransomware, malware, and weaponized CVEs, mapped to MITRE ATT&CK
- Threat emulation and validation through custom cyber attack simulations
- Analyst-focused runbooks with transparent threat intelligence, remediation steps, and clear guidance
- A straightforward SaaS platform, no deployment or downloads required

You can join the HUNTER Community on our web site at intel471.com or scan the QR code below.

Test our intelligence-driven threat hunting!

Get your Community Edition account in our HUNTER platform.

ABOUT INTEL 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting.

Learn more at intel471.com.

Our customers' eyes and ears outside the wire.

INTEL471

CONTACT INFO

800.833.1471
sales@intel471.com
www.intel471.com

FOLLOW US!

in intel471
intel471Inc
▶ intel471_Inc
f intel471
@intel471Inc