CYBORG SECURITY

THREAT HUNTING FRAMEWORK

TABLE OF CONTENTS

CYBORG SECURITY

INTRODUCTION

> **"HUNTING IS NOT A SPORT. IN A SPORT, BOTH SIDES SHOULD KNOW THEY'RE IN THE GAME."**
>
> **– PAUL RODRIGUEZ**

'Threat hunting' is a concept that has gained tremendous traction within the cyber security community. Organizations have realized that while traditional security controls and analysis have served as a cornerstone for an organization's cyber security compliance, they are no longer sufficient to mitigate operational risks.

This is especially true given the ever-increasing attack surfaces of these organizations, as well as the increase in number and capability of cyber adversaries. This reality has necessitated a paradigm shift from reactive to proactive security, and as a result, organizations have increasingly focused on threat hunting to fill this realized gap.

However, despite this increase in demand for processes, people, and technologies to enable threat hunting across environments, many organizations continue to struggle with the establishment of sustainable threat hunting capabilities which are able to operate in a rigorous, and repeatable, manner. This struggle is often fed by a litany of business and technical challenges, some of which are unique to threat hunting, but many of which are common to security practices as a whole.

CYBORG SECURITY

BUSINESS CHALLENGES

From a business perspective, one of the most critical challenges organizations are faced with are skills shortages for threat hunting.

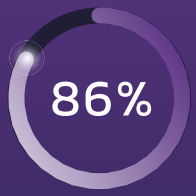
This means that many organizations are unable to locate resources to stand up a threat hunting capability; and, for organizations that are able to conduct threat hunting operations, their programs are largely reliant on only a few, highly skilled and technical resources. This often means that any fluctuation in manning can have direct operational impacts. Skill shortage, however, is not the only business-related challenge to threat hunting.

Another challenge organizations grapple with is the inherently uncertain nature of threat hunting. This uncertainty can often make it a challenge to appropriately measure the value that threat hunting brings to security operations, which in turn can make is difficult to realize the return-on-investment (ROI) for organizations.

With ongoing skills shortages for most organizations, and the challenge in measuring ROI for organizations, a common outcome of this is that threat hunting teams are often seconded to, or forgone altogether in favor of, ongoing traditional security operations.

AMOUNG CYBER SECURITY PROFESSIONALS

Currently run or intend to run threat hunting operations as part of their security strategy.



Believe the human elements and analyst input is essential to defend their organization from cyber attacks.

Claim their lack of skilled staff is their primary barrier to sucessful security operations.

SANS 2020 Threat Hunting Survey

TECHNICAL CHALLENGES

From a technical perspective, the number of impediments organizations face to establishing a threat hunting capability are considerable.

One of the most common technical challenges is a so-called data deficit. Organizations, dependent upon their current SOC maturity, often find that the depth, breadth, quality, and quantity of their data is insufficient to support threat hunting operations. This challenge can be compounded as security teams come to realize that their existing security controls may not provide sufficient coverage to support more advanced threat hunting.

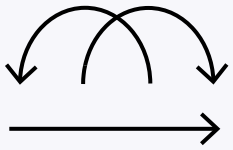
The ongoing skill shortage also manifests itself as a technical issue for organizations. This is especially true as the number of resources with the depth of experience to develop operational capabilities and conduct threat hunting operations continues to remain very low. The result is often a lack direction and focus for threat hunting operations which typically results in a lack of defined processes, as well as ineffective and unreliable hunts.

Despite these significant challenges that organizations continue to encounter, there is both a demand, and a need, for mature, reliable, repeatable and robust hunting capabilities in many organizations. Cyborg Security'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. Before exploring threat hunting, however, it is valuable to first examine the definition of, and the role that, threat hunting plays in a mature security operations team.

THREAT HUNTING SECURITY OPERATIONS

A DEFINITION OF THREAT HUNTING

At its simplest, threat hunting is an iterative and proactive process whereby threat hunters seek out anomalous activity, artifacts, and behaviors within an environment with the objective of identifying previously unknown and undetected threats. 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.

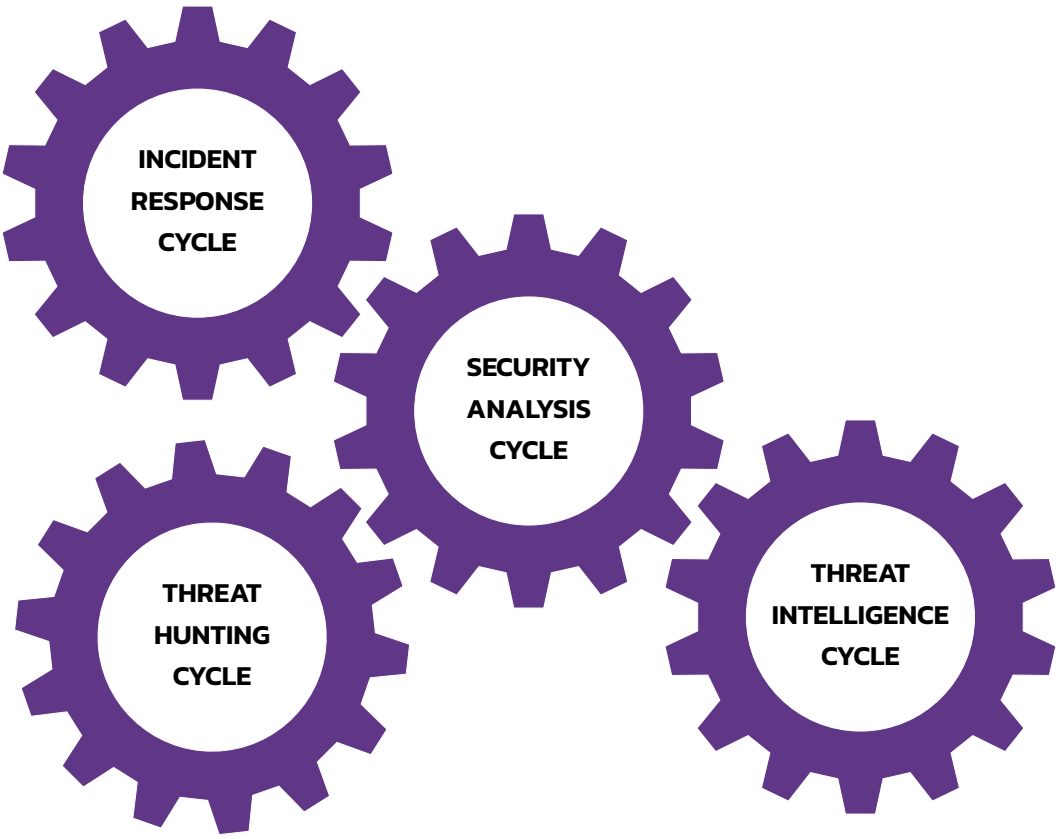
CYBORG SECURITY

THE ROLE OF THREAT HUNTING

The role that threat hunting plays for security teams and organizations also presents challenges. This is because the role of threat hunting within the security operations milieu as a whole, and what the expected outcomes of threat hunting are, are often poorly understood.

Threat hunting is sometimes erroneously portrayed as an elite capability that is operationally segregated from other disciplines. This however can result in ineffectual threat hunting. The threat hunting capability of an organization should be tightly integrated with traditional security operations as well as other disciplines like threat intelligence and incident response, as it relies significantly on these other disciplines for inputs.

Additionally, the outputs of threat hunting, especially detection of malicious activity and richer understanding of an enterprise environment, will serve as inputs for other security teams.



THREAT HUNTING OUTPUTS

THREAT DETECTION CONTENT CREATION

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, the output of threat hunting can absolutely contribute to the collection and deployment of IOCs into traditional security controls, threat intelligence platforms (TIPs), signatures, or for immediate blocking.

PLAYBOOK AND RUNBOOK CREATION OF ENRICHMENT

Other output of threat hunting is enhanced documentation which often takes the form of playbooks and runbooks. These playbooks and runbooks often serve two purposes. First, they form the basis for operational processes and methodologies used on repeated hunts. Second, and perhaps more crucially, they should serve as guides for security analysts to investigate the threat detection content that was also created. This ensures that analysts investigating the threat detection content are provided with consistent analysis methodologies and remediation guidelines. These playbooks and runbooks become mission critical for the successful deployment of threat detection content.

RED TEAM ENGAGEMENTS

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 methodologies, as well as to test threat detection content creation.

THREAT INTELLIGENCE REPORTING

Another valuable output of threat hunting is the incorporation of the findings within existing threat intelligence reporting. One of the most critical sources of threat intelligence is existing threat hunt and incident response data from within an organization. This data can then be enriched and contextualized through the threat intelligence process.

INCIDENT RESPONSE ENGAGEMENT

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 often draw on similar skill sets. However, if an organization has a dedicated incident response team and processes, any identified malicious activity as a result of hunts should be directed towards those teams.

Organizations often rely on threat hunters for their ability to detect previously unknown and unidentified threats, threat hunting also serves as an invaluable input and resource for organizations' existing security operations. To that end, threat hunting should serve as a rising tide which lifts all boats within an organization, and not remain a lake of knowledge unto itself.

CYBORG SECURITY

PRE-REQUISITES TO THREAT HUNTING

Threat hunting, as a capability, has certain pre-requisites much like most disciplines in cyber security. While some would assert the need for a particular technology or brand, the reality is the pre-requisites for threat hunting typically can be grouped into the categories of technological pre-requisites, and personnel pre-requisites. It should be noted that while we have referred to them as pre-requisites, a lack in a specific 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.

CYBORG SECURITY

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 pre-requisites are needed for threat hunting?”

IT IS SIMPLE, BUT COMPLICATED

The answer to this can be both simple and complicated at the same time. It can be a simple answer because at the core of threat hunting is visibility into an environment at both the network- and host-levels. The greater in granularity the visibility is, the simpler it will be for threat hunters to examine data and uncover suspicious or malicious activity. However, the answer will almost certainly be complicated as well. This is because how organizations will accomplish this is ultimately dependent upon a number of unique variables. This will include compatibility with current technologies and platforms, available budget, and operational and legal concerns.

BREADTH AND DEPTH

Another important technical factor is that threat hunting doesn’t simply require a breadth of data, but a significant depth as well. This data is often generated by endpoint agents which record changes to the state of a system or appliance that record network traffic.

STORAGE

With this increased visibility, another key consideration is capacity and duration of log storage. Organizations will often find that their storage needs increase dramatically as they integrate these new prolific log sources. And as threat hunting often requires large data sets, this will result in organizations needing to plan for long term storage of data with relatively rapid data access.

ANALYSIS PLATFORM

Another minimum consideration is some form of collation and correlation platform. These platforms allow threat hunters to examine data from a number of different perspectives. While some organizations may be tempted to focus on dedicated threat hunting platforms, the reality is that tools like a security information and event management (SIEM) or big data platforms can be sufficient. Additionally, they can be supplemented with free and open-source analysis tools for things like data visualization. The key is that the platform should present multiple methods for analysts to enrich, correlate and visualize data. Beyond those capabilities, the selection of such a platform will reside with the organization using it.

CYBORG SECURITY

PERSONNEL PRE-REQUISITES

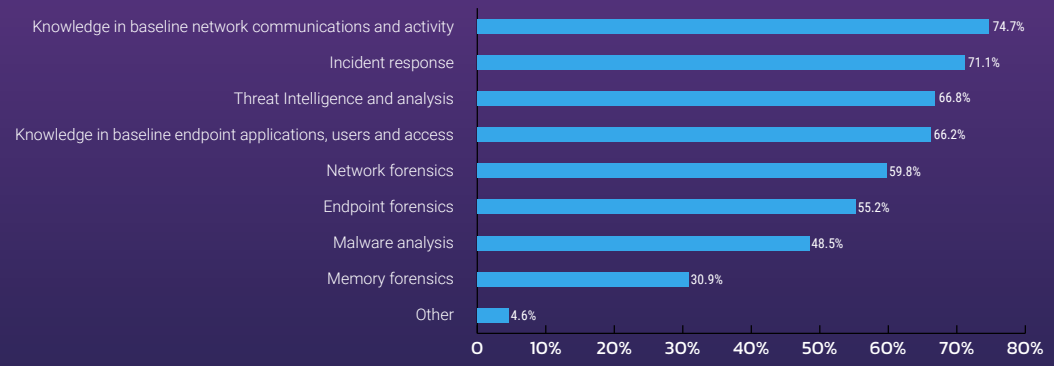
Another question which is frequently asked by organizations looking to establish a threat hunting capability is “what type of people do I need for threat hunting?”

The answer, here, is similar to that in the section on technological pre-requisites in that the answer can both incredibly simple and frustratingly complex. At the core of a threat hunter is an extensive knowledge of the mechanics of an operating system (typically Windows and Linux, but with a growing need for macOS and mobile platforms), especially for hunters engaged in structured or hypothesis-based hunting.

However, the answer can also be quite complex, as the broader the experience of a candidate is in various sub-disciplines (and indeed other disciplines altogether) the richer the capability of the team.

For instance, those with strong mathematical backgrounds will prove valuable for statistical analysis; or those with programming backgrounds will likely be able to provide tool development, as well as augmenting teams’ abilities to understand more niche programming concepts. Another often overlooked component for threat hunters is institutional knowledge. For example, a former system administrator in the organization may provide critical insight into expected behaviors for both users and systems, and may be able to augment a team’s capability significantly. All of this is to say that while at its core threat hunting requires an extensive experience with the target operating systems and the organization as a whole, additional, and diverse experiences are also highly desirable.

PROFESSIONAL BACKGROUNDS COMPANIES VALUE IN THEIR THREAT HUNTING TEAM MEMBERS



SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters

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 detect 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.

HUNTING OPERATIONS	CHALLENGES	WINS
NOT STARTED	▸ Talent ▸ Process ▸ Time ▸ Centralized Management	Where to Start ▸ Hunt Packages ▸ Intel Sources ▸ Technical Notes ▸ Mitigation/Response Action
REACTIVE	▸ Process ▸ Time ▸ Centralized Management	Emerging Threats ▸ Threat Collections ▸ MITRE Tagged Behaviors ▸ Contextualized Metadata Tagging
PROACTIVE	▸ Time ▸ Centralized Management	Augementation ▸ 24/48 Hour Turn Around ▸ 20+ Hunt Packages/Month ▸ 180 Day Hunt Package Review ▸ Planning/Reporting Hunt Module

CYBORG SECURITY

NOT STARTED

The first level of threat hunting maturity is “Not Started.” Organizations in this category rely exclusively on traditional security controls and technologies to drive daily operations. They will likely 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 manning-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.

CYBORG SECURITY

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.

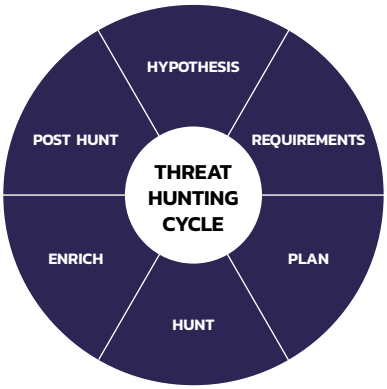
Threat hunting maturity is a critical component of modern cybersecurity defenses. By understanding the three levels of threat hunting maturity, organizations can better assess their own threat hunting capabilities and take steps to maximize their efforts. Whether an organization is just getting started 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,”[ii] or “The Threat Hunting Lifecycle,”[iii] and while these cycles have tremendous merit, Cyborg Security has synthesized these cycles, as well making modifications to address existent limitations in other cycles, into what we call, eponymously, the Threat Hunting Cycle.



CYBORG SECURITY

HYPOTHESIS

While we will touch on hypothesis-based hunting in the following sections, it is important to understand that the Hypothesis step is more simplistic. It aims to describe a particular area for inquiry and investigation and need not exclusively take the form of an explicit, scientific, hypothesis.

These hypotheses may originate from a variety of sources, including the existing threat intelligence capabilities of an organization, known and reported vulnerabilities, previous red team engagements, previously reported incidents, and of course, most importantly, the skills and experience of the threat hunters.

EXAMPLE OF HYPOTHESIS

A hypothesis, in this case, 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 overcame 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.

CYBORG SECURITY

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 "because that is how they have always been done."

HUNT

The next phase, referred to as 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.

CYBORG SECURITY

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 (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.

CYBORG SECURITY

REPORTING & METRICS

Another important component 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, and
- Test incident response plans.

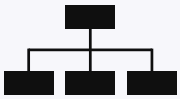
A successful threat hunt outcome can be determined by a variety of factors, including increased visibility and understanding of the environment, identification of visibility gaps and misconfigurations, improved incident response readiness, enhanced security posture, better correlation of data, enhancement 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.

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).[iv] 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.[v] 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.

CYBORG SECURITY

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.[vi]

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.[vii] 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.[viii] 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.[ix] 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.[x] 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.[xi] 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:

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.

CYBORG SECURITY

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.

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 as a result, the requirement to understand what threat hunting is (and equally, what it isn't!), and the role hunting plays in the overall security processes is more important than ever.

Equally critical, however, is also to understand that threat hunting as a capability does not supplant traditional security operations. Rather it serves as a vital component of the overall security apparatus and should serve not only to detect hidden threats but also to improve the capabilities of existing security teams, especially in the areas of threat detection content creation, documentation in the form of playbooks and runbooks, as well as serving as an input for threat intelligence, incident response and red team engagements.

CYBORG SECURITY

STANDING ON THE SHOULDERS OF GIANTS

Threat hunting, both as a process and as a discipline, must be iterative, building on the knowledge and experience of those who came before and those who stand should-to-shoulder with us. As such, Cyborg Security, Inc. would like to acknowledge and thank those who have worked to further the field and industry of threat hunting, and whose pre-eminent work influenced and helped shape the Threat Hunting Framework.

Amongst those individuals and their contributions to threat hunting which Cyborg Security has drawn on to compose this include:

- **David J. Bianco** – one of the forefathers of threat hunting, and whose contributions to cyber security field are too innumerable to count.
- **Ely Kahn** – the co-founder of the threat hunting and security analytics platform SQRRL (acquired by AWS).

Cyborg Security would also like to thank all threat hunters, many of whom have toiled tirelessly in the log data in search of "the bad," for their significant and ongoing contributions to the field of threat hunting, as a whole.

HOW HUNTER HELPS

The HUNTER Platform from Cyborg Security is a powerful tool designed to help organizations detect and respond to cybersecurity threats. It is specifically built for threat hunters, providing them with all the tools, resources, and support they need to identify, track, and mitigate threats effectively. Here are some of the ways HUNTER helps organizations perform threat hunting:

One of the key features of the HUNTER Platform is its vast library of threat hunting content. This includes hunting queries, playbooks, and other resources that are designed to help organizations get started with threat hunting. The platform also offers advanced search capabilities, allowing users to search across different data sources to identify potential threats.

The Platform also provides detailed reports on hunting activities, including the number of hunts conducted, the types of threats detected, and the outcomes of those hunts. These reports help security teams understand the impact of their hunting efforts and demonstrate the ROI of threat hunting to key stakeholders within the organization.

The HUNTER Platform offers a centralized location for managing all aspects of the threat hunting process, from creating and deploying queries, to tracking hunting progress, to reporting on outcomes. This enables security teams to easily manage their hunting efforts and collaborate more effectively.

The HUNTER Platform is a comprehensive solution for threat hunting that provides organizations with the necessary tools, resources, and support to effectively detect and respond to cybersecurity threats. Its advanced features, reporting capabilities, and management tools make it an essential tool for any organization looking to improve its threat hunting efforts.

SEE HUNTER IN ACTION

Get started hunting for FREE! Get a Community Account on the HUNTER Platform at cyborgsecurity.com!

CYBORG SECURITY

ABOUT CYBORG SECURITY

Cyborg Security is a cybersecurity company that provides threat hunting solutions through the HUNTER Platform. They specialize in proactive threat hunting and offer a range of customizable hunting packages to meet the unique needs of their clients. Cyborg Security is focused on empowering security teams with the tools and resources they need to effectively detect and respond to threats.

CONTACT INFO

407.562.1124
info@cyborgsecurity.com
www.cyborgsecurity.com

FOLLOW US!

Cyborg-Security
@CyborgSecInc
Cyborg Security
Cyborg Security
@CyborgSecInc
Cyborg Security

REFERENCES

[i] https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper. pdf, retrieved 23 July 2020

[ii] ibid

[iii] https://www.huntsmansecurity.com/blog/how-to-improve-security-monitoring-in-your-soc/, retrieved 23 July 2020

[iv] https://medium.com/@jshlbrd/structured-task-driven-threat-hunting-e8941cbeaa49, retrieved 10 July 2020

[v] ibid.

[vi] https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf, retrieved 01 August 2020

[vii] https://www.sans.org/reading-room/whitepapers/threathunting/practical-model-conducting-cyber-threat-hunting-38710, retrieved 4 March 2020

[viii] https://medium.com/@sroberts/incident-response-is-dead-long-live-incident-response-5ba1de664b95, retrieved 23 July 2020

[ix] https://www.threatq.com/mitre-attack-framework-maturity/, retrieved 30 July 2020

[x] https://awakesecurity.com/glossary/threat-hunting/, retrieved 24 July 2020

[xi] https://www.fireeye.com/blog/threat-research/2012/11/indepth-data-stacking.html, retrieved 24 July 2020

CYBORG SECURITY