A Guide to Cyber Threat Hunting
What is Cyber Threat Hunting?

SANS defines threat hunting as a focused and iterative approach to searching out, identifying, and understanding adversaries internal to the defender's networks.

Cybercriminals are extremely adept at obtaining access undetected. It’s pretty common for an organization to be unaware of an intrusion for days, weeks, or even months.

As the number of successful cyberattacks continues to soar, it’s time to take a proactive stance to detect them. When automated or preventative controls fail — and they will — organizations must rely on a detective control competency that delivers a multi-disciplinary threat hunting capability across the enterprise.

You can’t simply sit back and wait for an automated alert to let you know you've been breached. You need to actively seek out potentially malicious behavior on your network.

That’s why we’re seeing a shift to a more proactive approach that we call cyber threat hunting.

Read this Cyber Threat Hunting Guide to learn:

- Who you’re hunting for and the techniques they use
- The essential tools of a threat hunter
- How threat hunting will benefit your organization
- How to leverage all the advantages of threat hunting with a Managed Detection and Response (MDR) service provider
The Adversaries

When threat hunting, you must first understand the adversaries you’re facing. While their techniques may be very similar, what motivates them can be very different. Understanding these motivations can provide you with a better understanding of where and when a cyber attacker may strike or when an unwitting accomplice takes measures that present undue risk to the organization. If you can determine who would want to do you harm and what you have that’s valuable to them, you can better protect your business.

Malicious Insider
An insider attack that is malicious in nature, and is typically perpetrated by disgruntled, troubled, or just greedy insiders. This is a targeted attack, motivated by financial gain or grievance.

Inadvertent Insider
Not all insider threats are malicious. Sometimes people just make mistakes, or fall victim to common social engineering tactics, such as phishing, vendor spoofing, or pretexting.

Hacker
Hackers are opportunistic, and typically get a thrill from gaining access to secured systems. They are looking to prove themselves, and do it for bragging rights.

Cybercriminals
Cybercriminals are opportunistic and are motivated by financial gain. The growth of cybercrime-as-a-service (CaaS) means little technological expertise is needed to become a very successful cybercriminal today.

Cyber Hacktivist
Hacktivist attacks are targeted, and are often perpetrated to promote a political agenda or a social change, such as free speech, human rights, or freedom of information.

Cyber Terrorist
Cyber terrorists are motivated by a political, religious, or ideological cause. The goal is to intimidate a government or a section of the public, and they can interfere with critical infrastructure.
Anatomy of a Cyberattack

Hackers are people, so in order to successfully hunt for threats, you need to think like they do by understanding the tricks and techniques that are commonly used. This intellectual capital can provide mature threat hunters with an advantage because they share common skills and traits with their unethical counterparts.

Unfortunately, cybercriminals don’t follow a specific play book. There isn’t a single process or simple path of execution when perpetrating an attack. Nor is there a silver bullet for detecting that attack.

Nevertheless, it’s instructive to have an understanding of how a typical attack unfolds. Just keep in mind that hackers can skip steps, add steps, and even backtrack.

The Progression of a Typical Cyberattack

Research
Before launching an attack, cybercriminals try to gather as much publicly available information about the target organization and its network as possible. This can include, network ranges, IP addresses, and domain/host names. Part of the reconnaissance may include looking for email addresses of key players in the organization (IT manager, CFO, etc.) that could be used in a phishing attack during the exploit phase.

Penetrate
Now the attacker is ready to engage with the intended target and subvert the perimeter defenses.
This is often achieved through a phishing attack or another common attack vector (see page 5).
But hackers also have other tools that can be used to gain entry. These include port scanners, vulnerability exploitation tools, traffic monitoring tools, password crackers, and encryption tools.

Expand
Once in, an attacker will employ a technique called pivoting, where they use a compromised device to access other devices that would not otherwise be accessible.
This lateral movement optimizes transparency into available network assets in order to obtain high-value, sensitive information.
Various techniques are deployed to escalate privileges and gain system administrator credentials.

Exploit
Once an attacker finds what they are looking for, they take the final steps to achieve their goal.
Successful outcomes include:
• Gaining administrative access
• Opening Command and Control communications
• Achieving persistence
• Denying access to systems
• Exfiltrating data
• Destroying data
• Covering their tracks
Common Attack Vectors

Now let’s take a closer look at how hackers can gain access to a computer or network server. While hackers have a lot of tools in their arsenal, these attack vectors are some of the most common ways for cybercriminals to deliver a payload and exploit system vulnerabilities.

**Phishing**

An email disguised as a legitimate message, enticing recipient to open an infected attachment or click a link that takes them to an infected website. Phishing accounts for 90 percent of all successful cyberattacks.

**Malware**

Malicious code that disrupts computer operations, gathers sensitive information, or gains unauthorized access. There are various types of malware. They differ in infection and propagation characteristics (see page 6).

**Drive-By-Downloads**

Malware inadvertently downloaded from a legitimate site that has been compromised without any action from the user. It typically takes advantage of vulnerabilities in the user’s operating system or other program.

**Denial-of-Service**

An attempt to make a machine or network resource unavailable for its intended use. It often consumes more computer resources than a device can handle or disrupts by disabling communication services.

**Domain Shadowing**

If a hacker can obtain domain registrar credentials, they can add host records to an organization’s DNS records, then try to redirect visitors to these malicious, but trusted, IPs.

**Malvertising**

These are online ads that are owned by cybercriminals. Malicious software is downloaded onto the user’s systems when they click the ad, which can be on any site, including popular sites visited regularly.
Common Types of Malware

Malware exists in many forms and presents different intention objectives in order to compromise target hosts. Short for malicious software, it is software, script, or code commonly used by hackers to disrupt computer operations, gather sensitive information, or gain unauthorized access to computer systems and mobile devices. It’s easy for attackers to create their own malware or purchase malware toolkits, many of which have user-friendly interfaces that make it simple for unskilled attackers to create customized malware.

Malware categories are based on infection and propagation characteristics, and it’s possible to combine characteristics of multiple categories into a hybrid malware code. Here are a few of the most common types of malware.

- **Ransomware**: Malicious file encryption that can prevent you from using your computer or mobile device, opening your files, or running certain applications.
- **Trojan**: Poses as a legitimate application. Typically connects to a Command and Control server, allowing the attacker to take control of the infected machine.
- **Worm**: A piece of malicious code that is designed to spread from one computer to another by exploiting known vulnerabilities. It replicates itself in order to spread to other computers.
- **Virus**: Upon execution, a virus replicates itself by modifying other computer programs and inserting its own code. Viruses are designed to be destructive.
- **Bots**: Snippets of code designed to automate tasks and respond to instruction. An entire network of compromised devices is a botnet, which can be used to launch a distributed denial-of-service (DDoS) attack.
- **Rootkit**: A Rootkit is a collection of malicious software that allows access to unauthorized users. Once installed, it becomes possible to hide the intrusion, as well as to maintain privileged access.
- **Spyware**: Spyware is designed to gather data from a computer or other device and forward it to a third-party without the consent or knowledge of the user.
- **Keylogger**: Keylogger is software that can record all information that is typed on a keyboard, giving attackers access to sensitive information like passwords or credit cards.
Common Delivery Channels

Opening a phishing email isn’t enough to get a user infected with ransomware. So how does malware typically get delivered?

Quite simply, users must open the infected attachment or click the link that takes them to a compromised website.

Here are some common methods that hackers use to deliver malware once an action is taken.

**Windows Macros**
Macro are codes embedded within another program to automate repetitive tasks. Hiding malicious macros inside Microsoft Office® programs, like Microsoft Word®, used to be the prevailing technique for launching attacks. Though Microsoft has since developed security features that greatly reduce the use of macro-based malware, the technique is still in use. Malware is installed when the recipient opens the infected document.

**Exploit Kits**
An exploit kit is a software system that runs on web servers with the purpose of identifying software vulnerabilities in a client’s machine and exploiting the discovered vulnerabilities. It’s a tool that hackers use to break in, similar to picking a lock. Once installed, the kit uploads and executes a variety of malicious code. They are sold in cybercriminal circles, often with vulnerabilities already loaded onto them, and are extremely easy to use.

**Fileless Malware / Non-Malware**
Fileless malware is not really fileless, it just isn’t an executable file (.exe). When you are compromised using this technique, there isn’t a malicious program sitting on your computer. It operates by using legitimate programs, typically PowerShell, for malicious purposes. A malicious encoded script can be decoded by PowerShell, and then reach out to a Command and Control server without writing any files to the local hard drive.
“Cyber threat hunting is the next step in the evolution to combat an increasing array of sophisticated threats from attackers.”
— Crowd Research Partners

Tools of the Hunter

Comprehensive and effective threat hunting is the result of leveraging enterprise network traffic in a contextual setting in order to pinpoint areas of concern (at best) and compromise (at worst). Technology alone is not an adequate control. This exercise requires the skill-set and professional expertise of highly-trained threat hunting specialists coupled with a quality methodology.

According to the SANS Threat Hunting Survey, threat hunting tools driven by trained analysts can help increase the scalability and accuracy of threat hunting operations. Core technical skill sets and knowledge areas are also key to a successful threat hunting team.

Tier 1 rankings for the security operation skills required for threat hunting analysts reported in the SANS survey are detailed below. According to the survey, digital forensics and incident response are also important, and considered Tier 2 skills for threat hunters. These skills help them identify and extract new threat intelligence and use it to identify threats using their Tier 1 skills.
Security Operations Skills: Tier 1 Rankings

Log Analysis and Use of Analytics Tools
Maximizing network transparency and analyzing logs of all network devices is essential for the threat hunter. This can be a time consuming task due to the huge volume of data. A process is required to aggregate, correlate, and normalize logs, then perform contextual and behavioral analysis in order to detect advanced threats.

Knowledge of Baseline Network Activity
Once a baseline of network traffic is established, threat hunters develop an understanding of network events that are expected and authorized. Network activity baselines are a constantly shifting target as new technologies are introduced and new user behavior originates. Continually refining the baseline of what constitutes approved network traffic minimizes false positives so threat hunters can focus on uniqueness and confirm malicious or benign intent.

Threat Analysis and Use of Threat Intelligence
Threat hunters need to be able to examine behavioral attributes of network users and place activity in the appropriate context in order to detect advanced threats. An awareness and understanding of the latest developments in the external threat environment is a critical piece of a mature threat hunting methodology that requires regular and consistent attention.

Understanding of Baseline Endpoint Apps, Users, and Access
Most cyberattacks originate at an endpoint as the result of a phishing attack, so analyzing endpoint data enables fast incident detection and response. Hunters can zero in on unique and potentially suspicious activity, then confirm an infection using forensic-quality data.
“Persistent and focused adversaries are already in many enterprises. They present a security challenge that requires dedicated and empowered threat hunters who know what adversaries are capable of so they can sniff them out of the network as early as possible, close the gaps and create repeatable processes that can be followed for future hunts.”

Indicators of a Cyberattack

Equipped with powerful data mining technologies and leveraging a sophisticated methodology, threat hunters begin their search for indicators of compromise (IOC) and indicators of attack (IOA). These are network diagnostics representing forensic evidence or attacker activity that identify if a threat is imminent or has already proven successful. They serve as breadcrumbs leading the threat hunter to areas of concern as early as possible.

IOCs and IOAs are varied and numerous. Here are the top 10 as reported by Dark Reading.

1. Unusual Outbound Network Traffic

2. Anomalies In Privileged User Account Activity

3. Geographical Irregularities

4. Log-in Irregularities and Failures

5. Swells In Database Read Volume

6. HTML Response Sizes

7. Large Numbers Of Requests For The Same File

8. Mismatched Port-Application Traffic

9. Suspicious Registry Or System File Changes

10. DNS Request Anomalies
Benefits of Cyber Threat Hunting

So why should you consider adding cyber threat hunting to your cybersecurity strategy? It’s effective! The SANS 2017 Threat Hunting Survey found that 60 percent of organizations using threat hunting tactics are recognizing measurable improvements in cybersecurity performance indicators. Of significance, 91 percent of those cited measuring improvement in both the speed and accuracy of response and in attack surface exposure.

Here are the improvements respondents of the survey attributed to threat hunting.

- **91%** Improved the speed and accuracy of response.
- **91%** Reduced attack surface exposure and hardened network endpoints.
- **88%** Reduced dwell time (infection to detection).
- **87%** Reduced time to containment (detect / prevent lateral movement).
- **84%** Reduced actual breaches based on number of incidents detected.
- **83%** Reduced exposure to external threats.
- **78%** Reduced resources (e.g., staff hours, expenses) spent on response.
- **74%** Reduced frequency and number of malware infections.

“The inability to detect advanced threats and find expert security staff to assist with threat mitigation are the top two challenges SOCs are facing. As a result, about four in five respondents stated their SOC does not spend enough time searching for emerging and advanced threats.”

—Threat Hunters Strikes Back: The SANS 2017 Threat Hunting Survey
Unfortunately, that same SANS study also found that while many organizations understand the need to adopt threat hunting practices, it's not an easy task to undertake.

Many IT and security teams are already stretched thin, so it can be difficult to effectively focus on hunting. Plus it takes a highly-trained professional to successfully hunt for threats and avoid the diminishing returns that come with going down rabbit holes. Threat hunters need to understand what they are reviewing and be able to read the context clues to piece an attack together.

These experts are hard to find and expensive to retain. Plus, the cybersecurity workforce shortage is projected to hit 1.8 million by 2022 [Source: ISC2], so it will become even more difficult to find hunters moving forward.

Now more than ever, an increasing number of organizations are looking to specialized cybersecurity service providers, like Managed Threat Detection and Response (MDR) service providers, to fill this gap. See page 11 for details!
Cyber Threat Hunters for Hire

In theory, maturing your incident detection and response capabilities with the incorporation of a sound threat hunting methodology makes sense. Practically speaking, this can be a daunting task, especially if you’re faced with limited budgets and competing priorities.

As a result, many organizations are turning to Managed Threat Detection and Response (MDR) service providers that utilize threat hunting techniques for a reliable and cost-effective solution. Partnering with the right MDR provider can allow a business to focus on their core competencies and still leverage all the cybersecurity advantages an in-house threat hunting team brings to the table for this critical functional responsibility, including:

Security Expertise
Advanced threat detection cannot happen by algorithm alone. Incorporating the expertise of highly-skilled professionals is a must. These cybersecurity professionals are in short supply. MDR service providers should allow organizations to benefit from cybersecurity domain expertise without the need to invest in training, development, or headcount.

Threat Intelligence
Access to real-time cyber threat intelligence is a critical aspect of minimizing risk exposures. Keeping up-to-date with the rapid pace of change in the external threat environment is an on-going and time-consuming responsibility. Many organizations don’t have the time or resources to devote to the task, which makes MDR providers who offer this service an attractive alternative.

24/7 Monitoring
Cyberattacks can happen at any time. As soon as something suspicious is detected, it’s reassuring knowing that a skilled professional is available for immediate confirmation, interpretation, and guidance to assist with the response effort. An MDR service provider should give you access to a 24/7 security operations center (SOC), at a fraction of the cost of building one in-house.

Compliance
Daily log analysis — which is part of any sound threat detection methodology — is also an integral part of complying with a number of cybersecurity compliance standards. It’s very difficult to keep up with the sheer volume of data to review. While not all MDR providers offer this, finding one that does, can take this burden off the organization, and save a great deal of time and money.

Incident Confirmation and Containment
When an incident occurs, organizations need to know what happened, the extent of the damage, and how to drive an effective resolution effort. Partnering with an MDR provider that can confirm when an incident occurs, explain the details of what happened, and suggest remediation recommendations will improve your response capabilities immensely.
Struggling with the day-to-day demands of threat hunting? Explore nDiscovery!

While threat hunting may be a new buzz word circulating throughout the cybersecurity world, the concept of incorporating skilled professionals in a threat hunting capacity is not new. In fact, for more than a decade, nDiscovery™ has successfully employed this methodology to detect incidents before they become breaches.

nDiscovery combines human expertise with the latest threat intelligence and advanced data analytics to quickly and accurately detect threats across the entire enterprise environment. When nDiscovery confirms an incident, organizations are notified in minutes with exact details of what happened, which files are affected, and what you should do about it.

Learn more at www.tylertech.com/nDiscovery.
nDiscovery Managed Threat Detection

Daily analysis of network traffic, including log monitoring and endpoint analysis, is the only way to stay on top of the evolving threat landscape. Many organizations struggle with this task because of gaps in technology, manpower, or expertise.

nDiscovery offers all the features you need to overcome these challenges and cost-effectively protect your network with confidence.

**All the Benefits You Need, At a Low Cost**

<table>
<thead>
<tr>
<th>Feature</th>
<th>nDiscovery</th>
<th>MSSP</th>
<th>SIEM</th>
<th>Cloud Log Mgt</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNOLOGY: A foundation for effective data collection &amp; processing.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>METHODOLOGY: A proven process for reliable, consistent detection.</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>HUMAN EXPERTISE: Expert analysis and a go-to resource for answers.</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>THREAT HUNTING: Uncovers activity missed by automated systems.</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>CROSS INDUSTRY METRICS: Active threat intelligence center for better insight.</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>INDEPENDENT OVERSIGHT: Offers transparency &amp; removes conflict of interest.</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>COST OF OWNERSHIP: An in-house security expert is expensive.</td>
<td>$</td>
<td>$$$</td>
<td>$$$</td>
<td>$</td>
</tr>
</tbody>
</table>

nDiscovery is a subscription-based service. Licensing is determined by type of device and the size of your environment.
**About Tyler Technologies**

Tyler Technologies is a leading provider of end-to-end information management solutions and services for local governments. Tyler partners with clients to empower the public sector — cities, counties, schools, and other government entities — to become more efficient, more accessible, and more responsive to the needs of their constituents. Tyler’s client base includes more than 15,000 local government offices in all 50 states, Canada, the Caribbean, Australia, and other international locations. In 2017, Forbes ranked Tyler on its “Most Innovation Growth Companies” list, and Fortune included Tyler on its “100 Fastest-Growing Companies” list. More information about Tyler Technologies, headquartered in Plano, Texas, can be found at tyler.com.