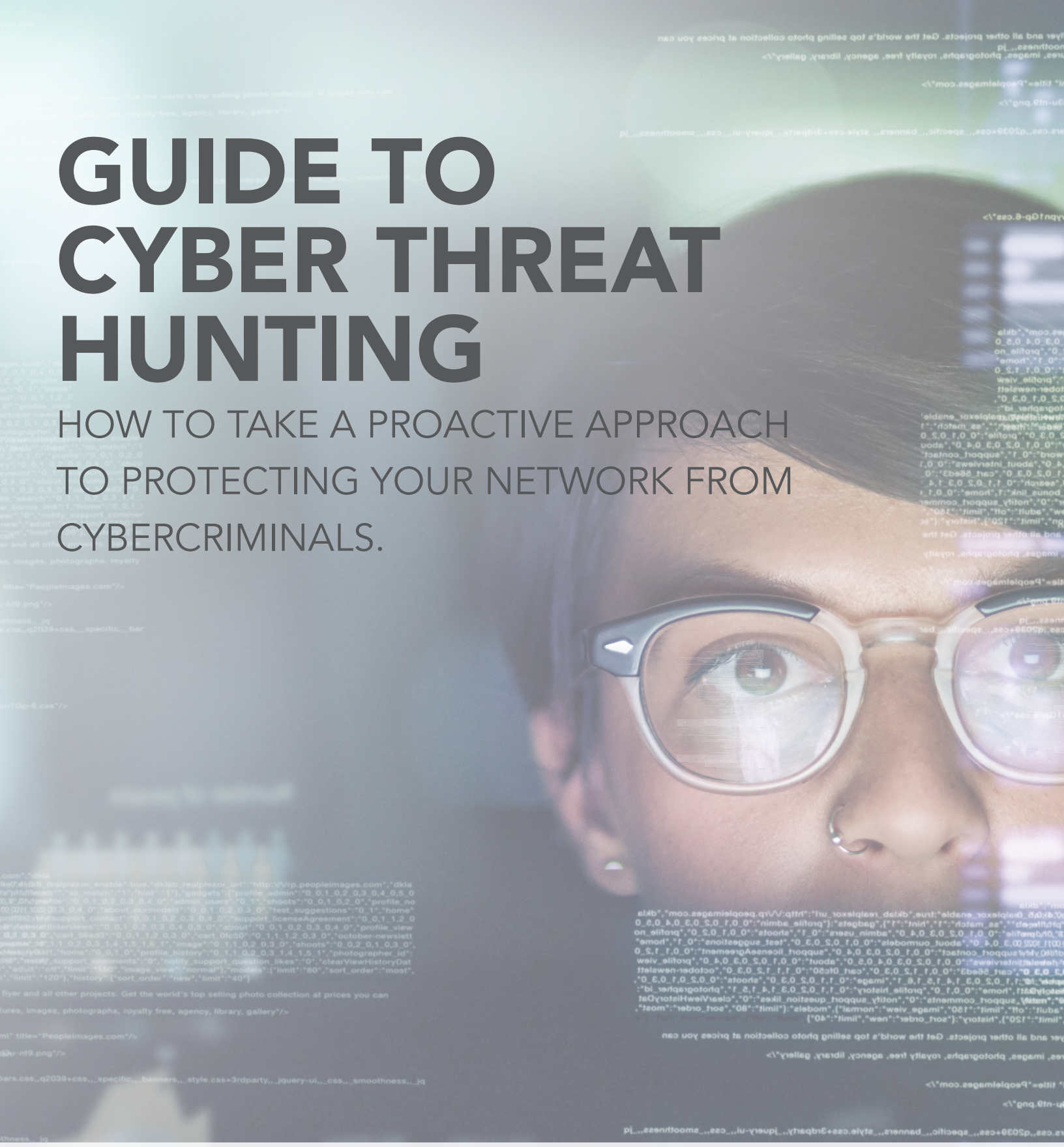
GUIDE TO CYBER THREAT HUNTING

HOW TO TAKE A PROACTIVE APPROACH TO PROTECTING YOUR NETWORK FROM CYBERCRIMINALS.



tyler technologies

tylertech.com

GET PROACTIVE

Cybercriminals can evade traditional defenses, compromising an infrastructure within minutes or hours. Study after study shows that it takes organizations weeks, even months, to uncover an intruder.

As the number of successful cyberattacks continues to soar, it's no longer enough to rely on passive forms of threat detection.

You can't sit back and wait for an automated alert to let you know you've been breached. You need to continually hunt down potentially malicious behavior on your network.

Read this Guide to Cyber Threat Hunting 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

> "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." [1]

1 Lee, R. & Lee, R.M. (2016). The Who, What, Where, When, Why and How of Effective Threat Hunting. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/membership/36785

tyler technologies

WHAT IS CYBER THREAT HUNTING?

[1] *A Practical Model for Conducting Cyber Threat Hunting* defines threat hunting as the proactive, analyst-driven process to search for attacker tactics, techniques, and procedures within an environment.

It's a method employed by highly trained cybersecurity analysts of thoroughly scrutinizing network traffic and datasets to find advanced persistent threats that evade existing security defenses.

"Cyber threat hunting is the next step in the evolution to combat an increasing array of sophisticated threats from attackers." [3]

It's extremely effective. A [2] SANS Threat Hunting Survey found that 60% of organizations using threat hunting tactics are recognizing measurable improvements in cybersecurity performance indicators, including:

- 91% Improved 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 (i.e., staff hours, expenses) spent on response
- 74% Reduced frequency/number of malware infections

1 Gunter, D. (2018). A Practical Model for Conducting Cyber Threat Hunting. Retrieved from https://www.sans.org/whitepapers/threathunting/paper/38710
2 Lee, R. & Lee, R.M. (2017). The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey. Retrieved from https://www.malwarebytes.com/pdf/white-papers/SANS_Report-The_Hunter_Strikes_Back_2017.pdf
3 2017 Threat Hunting Report, Crowd Research Partners. (2017). Retrieved from https://cybersecurity-insiders.com/wp-content/uploads/2017/02/2017-threat-hunting-report.pdf

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. Sometime 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.

CYBERCRIMINAL

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, i.e., free speech, human rights, or freedom of information. Anonymous is well-known for their hacktivist activities.

CYBER TERRORIST

These targeted attacks 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.

*Motivations aside, these regular network activities, typically administrative and maintenance-related in nature, often conspire to introduce excessive security exposure that is at odds with the organization's level of risk tolerance.

tyler technologies

"88% of hackers can break into their desired system and get through cyber security defenses in 12 hours or less... and it only takes another 12 hours for 81% of hackers to find and take valuable data." [1]

ANATOMY OF A CYBER ATTACK

Hackers are people, so in order to successfully hunt for threats, you need to think like they do – understand 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.

1 The Black Report 2017, Nuix.
Retrieved from https://www.information-age.com/cyber-security-hackers-perspective-123464671

THE PROGRESSION OF A TYPICAL CYBER ATTACK

RESEARCH

Before launching an attack, cybercriminals gather as much publicly available information about the target organization and its network as possible. This often includes, network ranges, IP addresses, and domain/hosts 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. Hackers have many 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. 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 & Control (C&C) communications
- Achieving persistence
- Denying access to systems
- Exfiltrating data
- Destroying data
- Covering their tracks

tyler technologies

"The top benefits organizations derive from threat hunting include improved detection of advanced threats (64%), followed closely by reduced investigation time (63%), and saved time not having to manually correlate events (59%)." [1]

COMMON TYPES OF MALWARE

Malware exists in many forms and presents different intention objectives in order to compromise target host(s). Short for "malicious software," it is software, script, or code commonly used by hackers to disrupt computer operation, 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 that you should be aware of.

1 2018 Threat Hunting Report, Alert Logic.
Retrieved from https://www.alertlogic.com/resources/industry-reports/2018-threat-hunting-report

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 & control (C&C) server, allowing the attacker to take control of the infected machine.

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.

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.

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

A software that can record all information that is typed on a keyboard, giving attackers access to sensitive information like passwords or credit cards.

tyler technologies

"The threat landscape is changing. The last wave of data breaches prove the need for a proactive approach to security. Applying the right strategies can help threat hunters beat attackers in their own game." [2]

COMMON ATTACK VECTORS

Here are some of the most common ways for cybercriminals to deliver a payload and exploit system vulnerabilities.

PHISHING

An email that entices the recipient to open an infected attachment or click a malicious link. [1] Phishing accounts for 90% of all cyberattacks.

DRIVE-BY-DOWNLOADS

Malware inadvertently downloaded from a compromised website; typically takes advantage of operating system or program vulnerabilities.

DOMAIN SHADOWING

If a hacker obtains domain registrar credentials, they can add host records to an organization's DNS records, then to redirect visitors to these malicious IPs.

MALWARE

Malicious code that disrupts operation, gathers information, or gains access. Various malware strains differ in infection and propagation characteristics.

DENIAL-OF-SERVICE (DOS)

An attempt to make a computer or network unavailable; often consumes more computer resources than it can handle or disables communication services.

MALVERTISING

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, even popular sites visited regularly.

1 2019 Phishing Statistics and Email Fraud Statistics. (2019). Retrieved from https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html
2 Threat Hunting Strategies for 2020. (2019). Retrieved from https://securityboulevard.com/2019/11/threat-hunting-strategies-for-2020

COMMON DELIVERY CHANNELS

Opening a phishing email usually isn't enough to get a user infected with malware. Typically users must open an infected attachment or click a malicious link that takes them to a compromised website. Once action is taken, the malware is delivered.

Following are three common malware delivery channels.

WINDOWS MACROS

Macros are codes embedded within another program to automate repetitive tasks. Hiding malicious macros inside Microsoft Office™ programs, like Word, used to be the prevailing technique for launching attacks. Though Microsoft has since developed security features that greatly reduces 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 – like 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 PC. 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 (C&C) server without writing any files to the local hard drive.

TOOLS OF THE HUNTER

Effective threat hunting leverages network traffic in a contextual setting to pinpoint areas of concern and compromise. 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.

Here's a brief rundown of the Tier 1 security operation skills required for threat hunting analysts as reported by 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." (Lee, 2017)

LOG ANALYSIS AND USE OF ANALYTICS TOOLS

Log analysis of all network devices is essential. The huge volume of data makes it a time-consuming task. A process is required to aggregate, correlate, and normalize logs, then contextual and behavioral analysis can be performed.

KNOWLEDGE OF BASELINE NETWORK ACTIVITY

Threat hunters must understand events that are expected and authorized. Continually refining this baseline 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 must place activity in the appropriate context, so it's critical they understand the latest developments in the external threat environment. This requires consistent attention.

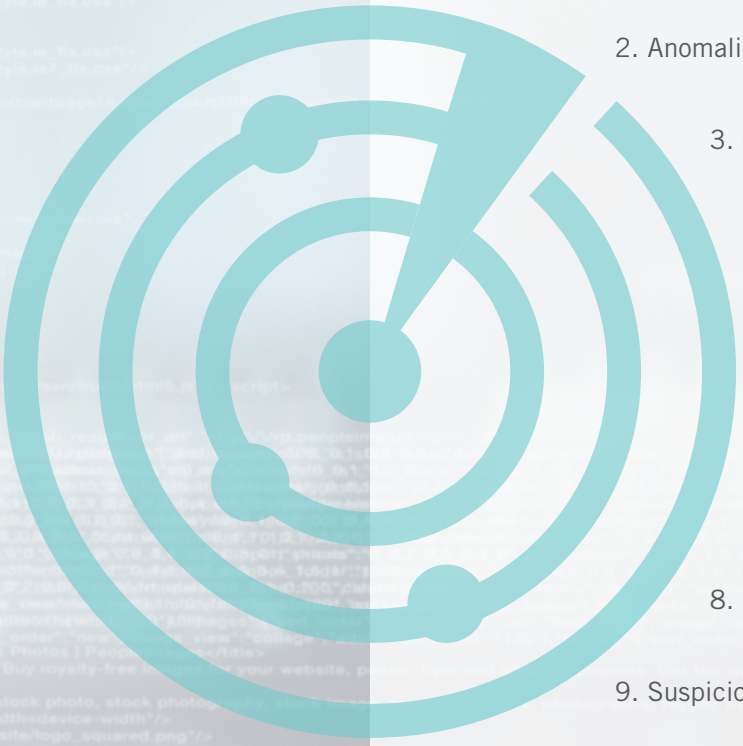
UNDERSTANDING OF ENDPOINT APPS, USERS, AND ACCESS

Most cyberattacks originate at an endpoint as the result of a phishing attack, so analyzing endpoint data enables fast incident detection and response.

INDICATORS OF A COMPROMISE AND ATTACK

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 [1]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

1 Chickowski, E. (2013). Top 15 Indicators of Compromise.
Retrieved from https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?

tyler technologies

THREAT HUNTERS FOR HIRE

"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." (Lee, 2017)

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.

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, [1] the cybersecurity workforce shortage is projected to hit 1.8 million by 2022, 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.

1 Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022. (2017). Retrieved from https://blog.isc2_blog/2017/02/cybersecurity-workforce-gap.html

FINDING THE RIGHT PARTNER

Partnering with the right MDR provider allows you to focus on your core competencies and still leverage all the cybersecurity advantages an in-house threat hunting team brings to the table, including:

SECURITY EXPERTISE

An MDR service providers should allow organizations to benefit from cybersecurity domain expertise without the need to invest in training, development, or headcount.

THREAT INTELLIGENCE

Many organizations don't have the time or resources to devote to keeping up to date with the rapidly changing external threat environment the task, which makes MDR providers who offer this service an attractive alternative.

24/7 MONITORING

Cyberattacks can happen at any time. 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. Partnering with an MDR that offers log analysis can ensure compliance.

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. Partner with an MDR provider that can confirm an incident, explain what happened, and suggest remediation recommendations.

Explore Tyler Detect!

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.

For more than a decade, Tyler Detect™ has successfully employed this methodology to detect incidents before they become breaches.

Tyler Detect combines human expertise with the latest threat intelligence and advanced data analytics to quickly and accurately detect threats across the entire enterprise environment.

When Tyler Detect 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 TylerTech.com/TylerDetect

tyler technologies

About Tyler Cybersecurity

Information security has always been a top priority at Tyler. Tyler has taken that focus to the next level by offering Tyler Cybersecurity, products and services supported by a team of experts dedicated to protecting their clients since 2002. By partnering with Tyler Cybersecurity, our clients realistically and cost-effectively protect their information assets while maintaining a balance of productivity and operational effectiveness.

Tyler Technologies (NYSE: TYL) provides software and services to transform communities. Tyler's solutions connect data and processes across disparate systems, allowing clients to gain actionable insights for solving problems. We are proud to deliver effective cybersecurity solutions to help protect our communities.

Tyler was also named to Forbes' "Best Midsize Employers" list in 2018 and recognized twice on its "Most Innovative Growth Companies" list. More information about Tyler Technologies, headquartered in Plano, Texas, can be found at tylertech.com.

CYBERSEC-THHUNTG-TL-13322-0120

tyler technologies