CyberProof®

MANAGED THREAT INTELLIGENCE

EVERYTHING YOU NEED TO KNOW

Looking strictly at the statistics, it may seem like companies are doomed to always lose the cyber security battle. According to the FBI, the cost of cybercrime in the US was $3.5 billion in 2019. However, the actual toll was probably much higher, since exploits and intrusions frequently are not noticed. In fact, a New Zealand-based security firm, Emsisoft, estimated that in 2019, ransomware alone cost the US more than $7.5 billion. Looking more globally at the cost of cybercrime, independent researcher Cybersecurity Ventures expects global costs to grow by 15 percent per year over the next five years – reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

But the outlook doesn't have to be so bleak. To close the gap on cyber security, we have to shift from traditionally reactive processes to more proactive tactics and strategies.

WHAT IS MANAGED THREAT INTELLIGENCE?

The first step to understanding the value of managed threat intelligence is having a firm grasp on threat intelligence, itself. Threat intelligence as a practice has grown significantly in recent years, bolstering cyber security strategies against increasingly sophisticated attacks.

Threat intelligence has become such a crucial piece of cyber security because it helps you proactively determine which threats represent the greatest risks to your business. The information generated by these practices offers insight into the threats that have, will, or are currently targeting the organization, its employees and customers. These threats could potentially lead to loss of revenue, diminished brand reputation, the destabilization of operations, and more. Having this knowledge enables you to identify and prioritize the most likely causes of trouble so you can dedicate your available resources where they will be most effective.

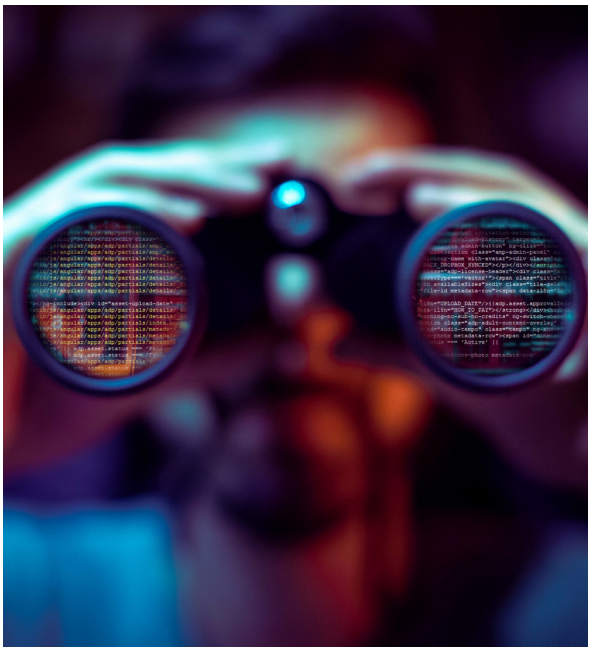
The problem for many companies is that threat intelligence professionals can be difficult to come by and employing them in-house can be challenging for a cyber security budget that is already stretched to its limits. It's possible to simply purchase threat intelligence data, but who is going to provide the analysis and translate that into actionable remediation.

This is where managed threat intelligence fills a gap. When you invest in targeted threat intelligence services, you ensure that the most important key to success is addressed—that the intel generated is actionable.

THE STEPS OF MANAGED THREAT INTELLIGENCE

Successfully managed threat intelligence will provide deep insight into the context security engineers need to properly protect valuable assets and systems. That means knowing which specific threats are targeting your industry, who is behind them, what their motivations are, and what kinds of systems they're exploiting.

The most efficient way to implement targeted threat intelligence services is to have actionable data fed directly to your security operations center. But when you're just starting with managed threat intelligence, it may not be clear how insights are generated. To identify and prepare for cyber threats that would otherwise take advantage of your valuable resources and data, providers will roughly follow the intelligence lifecycle laid out by the FAS:



Direction

Whether it's an automated system built on machine learning and artificial intelligence or less sophisticated services, the provider must set objectives based on essential elements of information (EEIs) that will factor into actionable threat intel. This includes the type of threat, the actors involved, where the threat will occur, etc.

Collection

Each provider will have a unique set of sources for gathering threat intelligence. The quality of data fed into the threat intelligence system is critical to overall success.

Processing

Data gathered from all sources must be processed and prepared for further analysis. That might mean decrypting information, sorting data based on relevance, or translating text.

Analysis

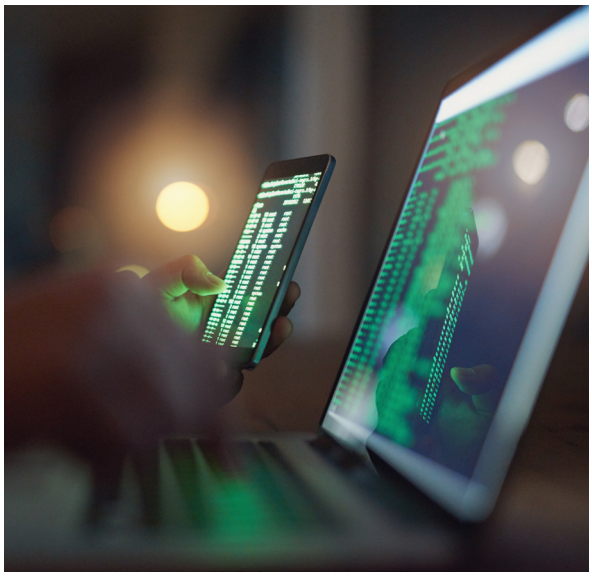
Bringing together the data from all sources and analyzing it as a whole is the critical component of managed threat intelligence. This is where actionable insights into patterns and trends should be identified.

Dissemination

Threat intelligence shouldn't be delivered as a set of raw data. Expect reports and assessments that provide detailed next steps for proactive cyber security.

Feedback

Data generated by managed threat intelligence providers should be fed back into the backend systems to continuously improve insights.



The approach that a managed threat intelligence provider takes to these steps will make or break their ability to protect your business. That's why it's so important to choose the right provider and solutions. And while each step is important, the collection stage can often prove to be the difference maker.

KEY SOURCES FOR MANAGED THREAT INTELLIGENCE

A managed threat intelligence provider is only as good as the data it can collect. Like any data analysis system, threat intelligence follows the garbage in, garbage out principle. That's why it's so important to assess the sources a managed threat intelligence provider monitors to generate your insights.

While every service will have its own set and combination of sources, a few main categories include:

IOC Sharing

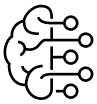
Sharing indicators of compromise (IOC) across the industry is a critical practice for uncovering more insights in system log entries and files that indicate malicious activity. When these IOCs are documented openly, it's easier to identify issues regarding network traffic anomalies, compromised user privileges, suspicious file changes, and more.

Open Source Feeds

Openly available information is a critical source for threat intelligence platforms. Everything from traditional media outlets to social media posts, cyber security forums, popular blogs, and more can be mined for intelligence. These feed fuel practices like brand monitoring and help identify domain squatting issues.

In-House Threat Intelligence

When working with a managed threat services provider, you benefit from the insights they deliver to other customers. The more data the provider can collect from other customers, the more their internal algorithms and security analysts will learn about the threat landscape. This, in turn, will give you more actionable insights to protect your business.



Deep and Dark Web Intelligence

It's essential that your managed threat intelligence provider can go beyond open source information to analyze what's going on in deep and dark web forums. Collecting information from things like Telegram hacker groups, QQs, IRCs, and a variety of marketplaces, forums, and file sharing platforms will provide an opportunity to identify stolen assets, emerging threat vectors, exploit kit analyses, and other tools and techniques of attackers. These are highly exclusive communities, so having a managed threat intelligence provider that can crack them is invaluable.

The expectation should be that a managed threat intelligence provider can think like a hacker. Deploying different crawlers and automated systems to collect information from a wide variety of sources is the first step. The better the data input, the more benefits you'll get out of targeted threat intelligence services.

BENEFITS OF FINDING THE RIGHT MANAGED THREAT INTELLIGENCE PROVIDER

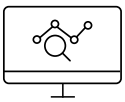
The truth about cyber security is that it's simply not possible to defend against every potential threat. You don't have the time, money, or human resources to handle every possible attack scenario. In theory, this is the benefit of making threat intelligence part of your cyber security strategy—to narrow the possibilities and make it clear where to invest resources.

But when you invest in managed threat intelligence and find the right partner, there are additional benefits beyond resource prioritization. Targeted threat intelligence services will maximize cost efficiency while ensuring you stay on top of the latest threats, become more proactive in cyber security, and gain a deeper understanding of your company's overall cyber risk.

KEEPING UP WITH EMERGING THREATS

Attackers come up with new and more sophisticated threats faster than software vendors can patch vulnerabilities. In the last three years, between 12,000 and 17,000 new vulnerabilities have emerged annually, giving attackers low-hanging fruit to compromise networks.

Managed threat intelligence services ensure you can keep up with the often-overwhelming volume of threats to your business. This includes everything from new techniques to vulnerabilities, zero-day code, potential targets, and known bad actors. Having a managed provider take care of this doesn't just free up internal resources—it helps you gain deeper insights than a limited internal team could.



MAKING CYBER SECURITY MORE PROACTIVE

Adding threat intelligence to an existing cyber security strategy won't automatically make you more proactive in dealing with attacks. In fact, sinking too much time and resources into threat intelligence internally can ultimately hurt the business if it takes away from other areas of cyber security.

Managed threat intelligence services cut out the guesswork to streamline the path to proactive cyber security. You'll know that the insights you gain are actionable and accurate, helping you to understand the goals of hackers, anticipate attacks before, and respond accordingly before the business is compromised.

UNDERSTANDING CYBER RISK

Managed threat intelligence isn't just about identifying a wider variety of potential attack vectors. The right partner should also provide deeper insight into the overall cyber risk that your company faces. This means keeping board members, c-level leaders, stakeholders, and business users informed about the latest threats and repercussions that they could have for the business. These insights are derived not just from internal data, but from the data collected regarding other companies in your industry with similar characteristics.

THREE LEVELS OF MANAGED THREAT INTELLIGENCE

Threat intelligence can't just be a question of what information is received. Rather, the best-managed threat intelligence providers will make sure the information is used properly. To do so, targeted threat intelligence services become fully integrated with security operations, combining complete data access with top analytical talent and a dedicated, intuitive threat intelligence platform.

However, actionable insights aren't the same for all threat intelligence stakeholders. The information provided to executive-level stakeholders won't be the same as more technical people. That's why managed threat intelligence is broken down into three distinct levels—strategic, tactical, and operational. The most comprehensive targeted threat intelligence services will encompass all three.

Level 1

STRATEGIC THREAT INTELLIGENCE

This is the broadest category of threat intelligence that is typically tailored to non-technical audiences, whether that means business users or executives who need to understand the company's cyber risk.

The main objective here is to deliver a detailed analysis of current and projected future risks to the business. Not only that, but strategic threat intelligence aims to outline the possible outcomes of individual threats to help leaders prioritize their responses.

Level 2

TACTICAL THREAT INTELLIGENCE

This level is where managed threat intelligence providers start to dig into TTP analyses. These outlines of tactics, techniques, and procedures of threat actors are meant for more technical audiences, such as a networking team that needs to understand its vulnerabilities based on the latest ways that attackers are compromised companies.

The insights generated at a tactical level will help security teams predict upcoming attacks and identify at the earliest possible stages. When managed threat intelligence providers can deliver detailed reports about the correlation between attacker targets and network vulnerabilities, technical teams can prioritize their resources most efficiently.

Level 3

OPERATIONAL THREAT INTELLIGENCE

The most technical level of threat intelligence is operational, where specific details about individual attacks and campaigns are shared. Insights delivered by threat intelligence experts at this level include the nature, intent, and timing of emerging threats. Without a targeted threat intelligence services provider, this is the most difficult type of information to obtain. Most often it is gathered through deep and dark web forums that in-house teams can't access.

Operational threat intelligence is used by threat hunters and red teams to improve the overall security posture of an organization. These are the stakeholders who take threat intelligence insights and use it to make the shift from reactive to proactive cyber security.

OPTIMIZING MANAGED THREAT INTELLIGENCE WITH SEEMO

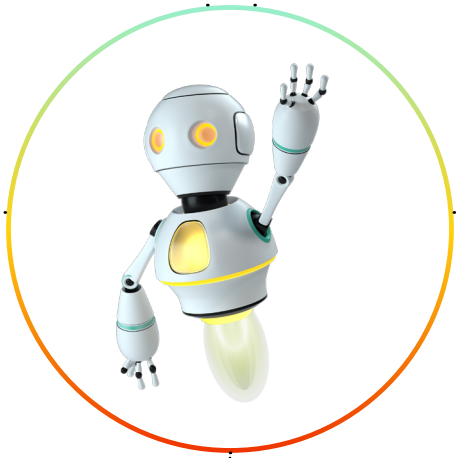
In recent years, the focal point of data intelligence innovation has been the combination of big data, machine learning, and artificial intelligence. And it should come as no surprise that these technologies promise to transform cyber security.

The reality is that massive volumes of raw data from internal and external sources outmatch any traditional SOC's ability to process and detect every potential IOC. When combined with human intelligence (HUMINT) and Open Source Intelligence (OSINT), AI-powered cyber security tools can optimize efficiency and help security operations teams address the most pressing threats. This is why our managed threat intelligence services are built around SeeMo, our virtual analyst.

SeeMo is an intelligence driven, machine learning BOT that helps automate and improve the efficiency of various activities within the CDC platform. SeeMo helps enrich event data, proactively queries external sources, and responds to analyst requests to provide contextualized and actionable information. This is achieved by leveraging the native integration and machine learning capabilities of the BOT.

SeeMo can also automate many repeatable Tier 1 and Tier 2 activities, reduce false positives, enrich events, and accelerate response times. Some of the capabilities SeeMo provide include, but are not limited to:

- Automatically extract observables and actionable information contained in security events
- Enrich events by proactively fetching information from external sources such as VirusTotal, X-Force, etc.



- Enable execution of CLI commands to fetch specific information from integrated sources
- Automatically create incidents based on alerts and their contexts without human intervention
- Automatically execute non-intrusive steps in digitized playbooks

SeeMo's main benefits are the fast creation and deployment of analysis agents without complex integration or versioning of the software. These agents support smart automation of security operations and proactive threat detection while supporting main threat intelligence players—analysts, threat hunters, and red teams—to execute rapid response processes.

The most effective managed threat intelligence providers enable the right combination of AI and expert cyber security experience. Algorithms are only as effective as the time and effort that goes into improving and perfecting them—and SeeMo gives you the necessary capabilities on both ends.

CyperProof managed threat intelligence services take care of the monitoring, detection, response, and resolution of any cyber threat you may face, so your company can recover fast and stay safe. It's the perfect combination of human intelligence and AI-powered cyber security that will facilitate your shift from outdated, reactive processes to more effective proactive defenses.

When you're ready to take advantage of advanced, cost efficient managed threat intelligence services, contact us for a free demo and learn more about CyberProof managed security services.

ABOUT CYBERPROOF

CyberProof is a security services company that helps organizations to intelligently manage incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats. We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

For more information, see: www.cyberproof.com

LOCATIONS

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum