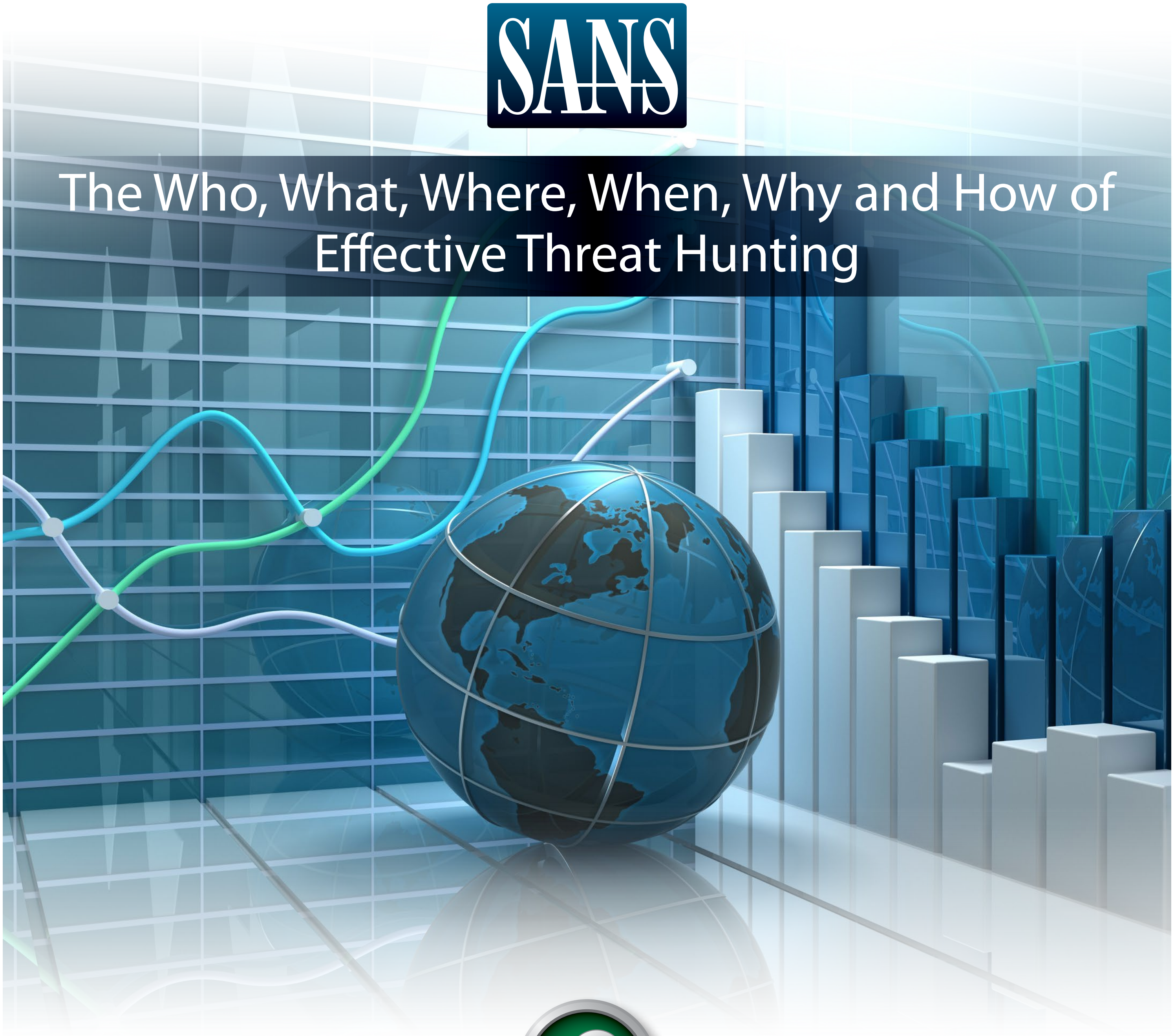
The Who, What, Where, When, Why and How of Effective Threat Hunting

The Who, What, Where, When, Why and How of Effective Threat Hunting



A SANS Whitepaper

Written by Robert M. Lee and Rob Lee

February 2016

Sponsored by
Sqrrl

Executive Summary

The chances are very high that hidden threats are already in your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Having a perimeter and defending it are not enough because the perimeter has faded away as new technologies and interconnected devices have emerged. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools by, for example, making their attacks look like normal activity.

Prevention systems and tools help reduce opportunities for adversaries and enable analysts to operate more effectively. The key, however, is to constantly look for attacks that get past security systems and to catch intrusions in progress rather than after attackers have completed their objectives and done worse damage to the business. This process is referred to as "cyber threat hunting."[1] Many organizations today do some type of formal or informal hunting. For example, rather than waiting for the "you've been breached" notification, they are intermittently or constantly searching through their own networks for evidence of threat activity.

This paper will explain *what* threat hunting is (and what it is not), *why* it is needed, *when* threat hunting is appropriate, *where* it fits into maturity efforts, *how* to get started and *who* should do the hunting.

[1] "Cyber Threat Hunting (1): Intro," Samuel Alonso blog, Jan. 21, 2016, https://samuelalonsog.wordpress.com/2016/01/21/cyber-threat-hunting-1-intro

What, Why, When and Where

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

What Is Threat Hunting?

Threat hunting is aptly focused on threats. And to be a threat, an adversary must have three things: the intent, capability and opportunity to do harm.[2,3,4] Threat hunters focus their search on adversaries who have those three characteristics and who are already within the networks and systems of the threat hunters' organization, where they have authority to collect data and deploy countermeasures.

Many security personnel will feel that they have been doing this type of activity, at least in part, since long before the term *threat hunting* emerged. And in many cases, that is true. The recent focus on threat hunting is not about rebranding what many defenders have endeavored to do over the years; it is about placing an appropriate, dedicated focus on the effort by analysts who purposely set out to identify and counteract adversaries that may already be in the environment. Threat hunting requires some specific analytic skills, such as familiarity with the enterprise and the ability to generate and investigate hypotheses. Hunting benefits from analysts using automation to make these hunts faster, easier, more frequent and more accurate. (Automation will be discussed later in the paper.)

The formal process of threat hunting should not be confused with an attempt to prevent adversaries from breaching the environment or for defenders to eliminate vulnerabilities in the network.

Why Hunt?

Threats are human. It is the adversaries, not just their tools, such as malware, that interest threat hunters. These adversaries are persistent and flexible and often evade network defenses. The threats are often identified as advanced persistent threats (APTs), not just because of the capabilities that the adversaries wield, but also because of their ability to initiate and maintain long-term operations against targets.

Focused and funded adversaries will not be countered by security boxes on the network alone. And threat hunters are not simply waiting to respond to alerts or indicators of compromise (IOCs). They are actively searching for threats to prevent or minimize damage.

[2] Air University, "Strategy to Tactics: BIA for Actionable Insights on Adversary Behavior," September 2007, www.au.af.mil/bia/methodology.htm

[3] Anind Dey, Boicho Kokinov, David Leake and Roy Turner, "Modeling and Using Context: 5th International and Interdisciplinary Conference," Paris, France, 2005

[4] Peter D. Gasper, "Cyber Threat to Critical Infrastructure 2010-2015," Idaho National Laboratory, September 2008

When Do You Hunt?

As we said earlier, threat hunting already occurs at many levels in organizations—mostly ad hoc in nature and based on hunches by analysts familiar with the environment. The challenge for many organizations is to make threat hunting an achievable and repeatable process that returns value.

The most significant part of this challenge is to organically integrate threat hunting into existing workflows so that it complements current security efforts. Threat hunting is often appropriately performed by organizations of various levels of security maturity. However, to fully take advantage of threat hunting, organizations must invest in the security infrastructure that is needed to use threat hunting tools and practices properly.

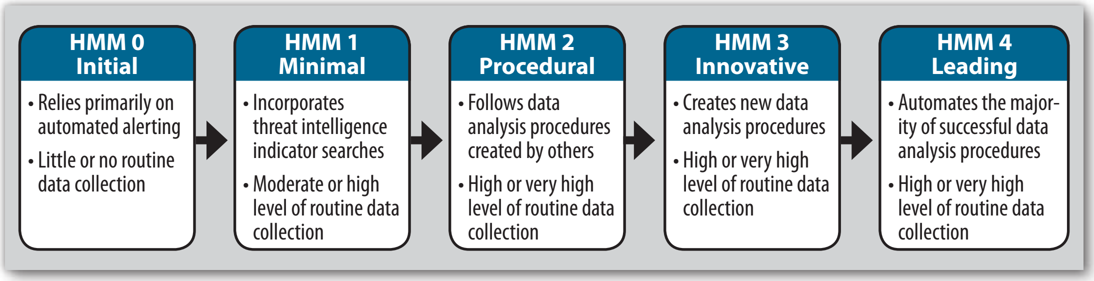
Bringing threat hunting into maturity requires a security stance that includes the tools, people, processes and buy-in from decision makers that enable defenders to hunt. The organization should set ground rules regarding roles, responsibilities and the way in which threat hunting will be used. For example, the hunt team should not be seen as a one-stop shop for taking care of every issue on the network. For that reason, the organization must make threat hunting part of its overall security strategy and enact it and understand it from the top down.

To fully take advantage of threat hunting, organizations must invest in the security infrastructure that is needed to use threat hunting tools and practices properly.

Simply put, threat hunting is accessible to all, but an organization must be mature enough to get a proper return on investment from it and make it a repeatable and consistent process. Several models are available that can help organizations assess their security maturity.

The Hunting Maturity Model

This model focuses on three important concepts for hunting:[5] Organizations need to be mindful of the quality of data they collect, the tools used to access and analyze the data, and the skills of the analysts who do the hunting. The Hunting Maturity Model puts forth five different categories of an organization's hunting capability: initial, minimal, procedural, innovative and leading (see Figure 1).



HMM 0 Initial
- Relies primarily on automated alerting
- Little or no routine data collection

HMM 1 Minimal
- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collection

HMM 2 Procedural
- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM 3 Innovative
- Creates new data analysis procedures
- High or very high level of routine data collection

HMM 4 Leading
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Figure 1. The Hunting Maturity Model (HMM)[6]

[5] David Bianco, "A Simple Hunting Maturity Model," Enterprise Detection & Response blog, Oct. 15, 2015, http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

[6] David Bianco, "A Simple Hunting Maturity Model," Enterprise Detection & Response blog, Oct. 15, 2015.

The chief takeaway from this model is to understand that threat hunting is not a single state but a progression. Organizations should attempt to maximize their data collection, efficiently analyze the data and then leverage their analysts appropriately. Properly using hunters' talents with this model means that automation should replace repeatable tasks, and machine learning should focus hunters on prioritized data and analysis.

Scaling Your Program

The Sliding Scale of Cyber Security is similar to the Hunting Maturity Model in many ways, but it defines five phases of investments that organizations can make to contribute to cyber security. These five sliding phases—architecture, passive defense, active defense, intelligence and offense—are visualized in Figure 2.

Threat hunting is not a single state but a progression.

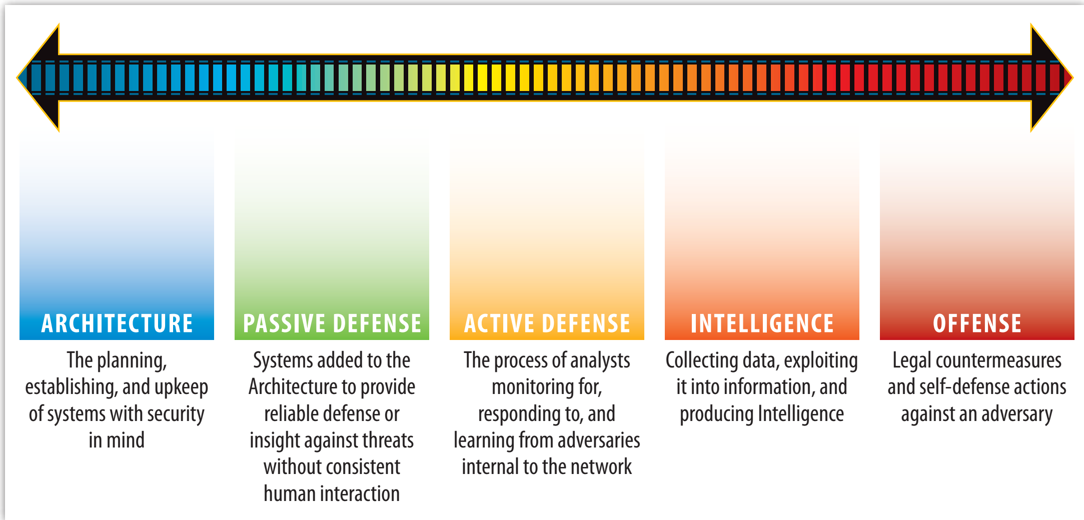

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 2. The Sliding Scale of Cyber Security[7]

In the figure, **architecture** refers to all aspects of design, including the network and its systems, and therefore this phase encompasses addressing vulnerabilities. **Passive defenses** are those tools and systems added to the architecture that give insight into the network or provide some aspect of security without constant human interaction, such as firewalls, intrusion detection systems and endpoint security solutions. **Active defense** covers a wide array of activities relating to analysts monitoring for threats, responding to them, learning from them and leveraging that information internal to their environment.[8]

[7] "The Sliding Scale of Cyber Security," SANS Reading Room, August 2015, www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240, p. 2, Figure 1.

[8] Despite popular misconceptions, active defense has nothing to do with sending out "hack-back" files, which beacon back from adversary networks, or creatively hardening systems. Those actions would fall into the offense, intelligence or passive defense categories, respectively.

Where Threat Hunting Fits In

Threat hunting is contained within the active defense category and integrates some of the best products of intelligence. **Intelligence** is the process and product resulting from collecting data, turning it into information and analyzing potentially competing sources of information to produce useful knowledge. The last category, **offense**, relates to countermeasures that organizations or states may take for self-defense purposes according to their laws.[9]

Organizations performing security operations are already hunting today (usually informally) regardless of where they are in their security maturity. However, as appropriate investments are made along the scale—such as monitoring infrastructure to enable active defense actions such as threat hunting—the hunt team produces significantly more output. In that way, threat hunting is an activity that continually provides increasing value to organizations as they grow in their maturity.

Infrastructure First

The Sliding Scale of Cyber Security is an easy way to see how the effectiveness of threat hunting can be limited if the security maturity of an organization cannot support it. For example, if the architecture is incorrectly maintained and full of vulnerabilities while the passive defenses are not tuned properly, the network will have a number of issues that make it difficult to accurately hunt for threats. As a result, noise, such as that made by basic malware, could be generated on the network, which can obscure the real data needed in a hunt. With proper investments in a robust and defensible network, threat hunting becomes significantly easier and will have a higher return on investment

[9] SANS does not recommend organizations invest in or perform offense. The original purpose of the sliding scale was to note that investing in offense is an extremely poor decision when investments can be made in the other four categories to return a better value toward security. Offense should be reserved for national and policy purposes, not for a misconstrued notion that it will yield significant cyber security benefits.

Once an organization has a sound understanding of the position threat hunters are to take, it needs to consider how they are to get started. As with most good analysis-driven processes, threat hunting should almost always start with a question, such as, "How could a threat evade current passive defenses?" This is because threat hunting is an analyst-driven process that is meant to address issues outside of what a single alert or indicator can reveal. Importantly, the questions you start with must also be testable.

How to Hunt

Start with a good hypothesis about threats that might be in the organization, the best places in the organization to go hunting and how threats might take advantage of users or business processes to bypass security appliances. As an example, hunters can consider crown jewels analysis: They identify the assets and information that are most vital to the organization's mission so that they can prioritize their efforts, use passive defenses and hardening techniques to reduce their risk, and generate hypotheses about what an adversary could do to compromise the assets. In the crown jewels example, hunters combine an understanding of their environment with a hypothesis of what the adversary might do.

Organizations that are ready to hunt must focus on two key areas: what data is available to search and how to sort through it.

Organizations that are ready to hunt must focus on two key areas: what data is available to search and how to sort through it.

What to Search: Analysts need a lot of data to look through. A concept familiar to anyone who has worked in incident response is that without evidence, forensics cannot do much. The same applies to threat hunting. Hunters need the data that will allow them to pivot from individual pieces of data into links and correlations that will ultimately reveal the threat. No amount of skilled personnel or expensive tools can make up for a lack of data gathered from the environment, such as flow records, logs, alerts, system events, digital images, memory dumps and other information gathered from throughout the entire organization. Investments in the architecture and passive defense phases of the Sliding Scale of Cyber Security can ensure that data is readily available on demand.

How to Search: It is pointless for analysts to blindly look through the data; they need search and visualization tools to help them. Analysts who are already threat hunting know that data science is important to being able to hunt effectively.[10] IOCs, alerts and other information are useful, but the most effective hunters have access to machine-learning and analytics tools, with visual displays to sort this information and help answer their questions and pinpoint abnormal behaviors across large data sets.

[10] "Cyber Hunting: 5 Tips to Bag Your Prey," InformationWeek, March 26, 2015, www.darkreading.com/risk/cyber-hunting-5-tips-to-bag-your-prey/a/d-id/1319634

How to Focus: Analysis often works best when data is enriched with helpful contextual information and data visualization identifies links between data sets. For example, analysts are most effective when they can look past individual alerts to identify patterns and abnormalities. Tailored analytics and machine learning make this possible, and automation helps. Features in tools such as visual link analysis can help analysts identify an adversary's larger effort inside the organization even against a backdrop of network noise and with large data sets to filter through.

How Much to Automate: Despite common misconceptions, threat hunting cannot be fully automated. Much of the process and any repeatable steps—searching for known signs of a threat on the network, reusing new threat data and performing other machine-learning tasks, for example—can and should be automated, but there will always be a need for analysts who have instincts and inquisitive minds. What is powerful about threat hunting is that it pits human defenders against human adversaries. The key is to find the right analysts and empower them.

Hunters are curious. They are passionate. They are skilled at leveraging multiple tools and understanding and pushing the limits of those tools.

Who Are the Right People to Hunt?

Even if they operate in dual-hatted roles such as incident responder/threat hunter or security operations center analyst/threat hunter, threat hunters must be dedicated to actively pursuing adversaries. These defenders add the most value when they are fixated on true threats and not restricted to responding to alerts or network maintenance issues such as patching vulnerabilities.

In a team structure, threat hunters work alongside other network and security teams in the organization, not in competition with them. Many hunting teams are positioned inside of a security operations center or as part of a computer security incident response team.

Hunters are curious. They are passionate. They are skilled at leveraging multiple tools and understanding and pushing the limits of those tools. Most important, hunters are innovative analysts who understand their threat landscape and their organization well enough to ask the right questions and find the answers. In a lot of ways, automated tools should reflect this behavior in human threat hunters, replicate it and automate it to act as agent on behalf of the threat hunter behind the keyboard.

[11] "Enhancing Intrusion Analysis through Data Visualization," SANS Institute InfoSec Reading Room, Feb. 9, 2015, www.sans.org/reading-room/whitepapers/detection/enhancing-intrusion-analysis-data-visualization-35757

Hunters should embody a mix of active defense skills and intelligence analyst tradecraft. Consider a hunter who has experience performing enterprise security as well as incident response. The enterprise security skills give the hunter knowledge about tools in the environment that can generate good logs and insight, as well as understanding about their limitations. The incident response skills inform the defender about what data can be requested from incident responders and what realistic recommendations to make after uncovering a new threat.

With intelligence analyst tradecraft, the defender will also be adept at forming hypotheses, analyzing competing sources of information to prioritize the best hypothesis and searching for and tracking adversaries over the course of a campaign. Additionally, the hunter should know the value and limitations of intelligence, as well as the pitfalls that can occur with common logical fallacies and biases, such as anchoring and congruence bias,[12] so that precious resources aren't wasted chasing down false leads.

A good hunter will possess a varied background and a passion for uncovering threats that can complement the overall effort.

As an example, the Hunting Maturity Model (HMM) level 0 focuses on automated alerts and routine data collection. These alerts may come from prevention systems on the network, such as a firewall or intrusion prevention system. This is a reactive approach; it is not hunting. Once they have moved beyond HMM level 0, teams can begin the proactive hunting process.

As analysts expand their skills, they become better at generating hypotheses and asking the right questions regarding what adversaries may be on the network and where they are hiding. They move up the HMM levels to begin incorporating threat data and IOCs. Defenders who begin to understand the tactics, techniques and procedures of adversaries and have access to data from throughout their environment will be able to follow data analysis procedures (HMM 2) and even create their own procedures (HMM 3). All hunters should aspire to reach HMM 4, which automates previously successful hunts.

While there is no single combination of correct skills for a hunter, a good hunter will possess a varied background and a passion for uncovering threats that can complement the overall effort.

[12] Analysts should attempt to defeat biases. Doing this requires familiarity with the definitions and existence of these biases. For a useful list, see https://en.wikipedia.org/wiki/Cognitive_bias.

Hunting as Active Defense

Especially skilled hunters (of the more mature organizations) will also be familiar with the security models that can be applied to the active defense and intelligence categories of the Sliding Scale of Security Maturity. Expert hunters know when and how to use these models as they apply to their organizations, but they do not rely solely upon them. While models are meant to help analysts structure data and their responses, they should never be allowed to limit a defender's options or creativity in an exceptional situation. Nonetheless, models can serve as a great catalyst for even the most senior analysts.

Two cyber threat intelligence models that have been widely used in the industry tie directly into the Hunting Maturity Model shown previously in Figure 1. These models, the Cyber Kill Chain and the Diamond Model of Intrusion Analysis, help to identify intrusions and look past the idea of a single intrusion and toward an identification and understanding of adversaries' campaigns. Both of these feed into the Active Cyber Defense Cycle.

The Cyber Kill Chain[13] is an adaptation of the U.S. military's kill chain process, which attempts to identify the phases of action adversaries take to achieve their goals. The Kill Chain has been used in a variety of ways. One of its most important uses is in detailing the phases of individual intrusions, extracting indicators for each phase and identifying patterns across multiple intrusions. Defenders can combine key indicators, such as the human aspect of intrusions, and related intrusions into a grouping representing an adversary's campaign.

The Diamond Model of Intrusion Analysis directly complements this kill chain analysis.[14] It is often used for generating intelligence, as opposed to the consumption of it, so it exists outside the scope of this paper but is worthy of study for those interested in the topic. The Diamond Model helps analysts structure indicators observed in the Cyber Kill Chain to define and understand adversary campaigns. This ability to group intrusions into campaigns allows threat hunters to counter adversaries' efforts over long periods of time instead of countering single intrusions.

[13] Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceedings of the 6th International Conference on Information Warfare and Security, 2011

[14] Sergio Caltagirone, Andrew Pendergast and Christopher Betz, "The Diamond Model of Intrusion Analysis," Active Response, July 2013

The Active Cyber Defense Cycle takes the threat intelligence generated from the use of the first two models and puts it into context of an active defense.[15] This model is used to ingest threat intelligence and identify and respond to threats while taking advantage of defender strengths. The model consists of four phases that are meant to act as a continual process: threat intelligence consumption, asset identification and network security monitoring, incident response, and threat and environment manipulation. The cycle's strong suit is that defenders can evolve through interactions with adversaries while leveraging their knowledge of the environment.

These interactions with adversaries feed back into the Cyber Kill Chain and the Diamond Model, creating a back-and-forth process that allows for the generation and consumption of threat intelligence. It is in this process that effective hunting models can be realized and utilized.

Figure 3 shows how these three models come together for generating and consuming intelligence to support the threat hunting process.

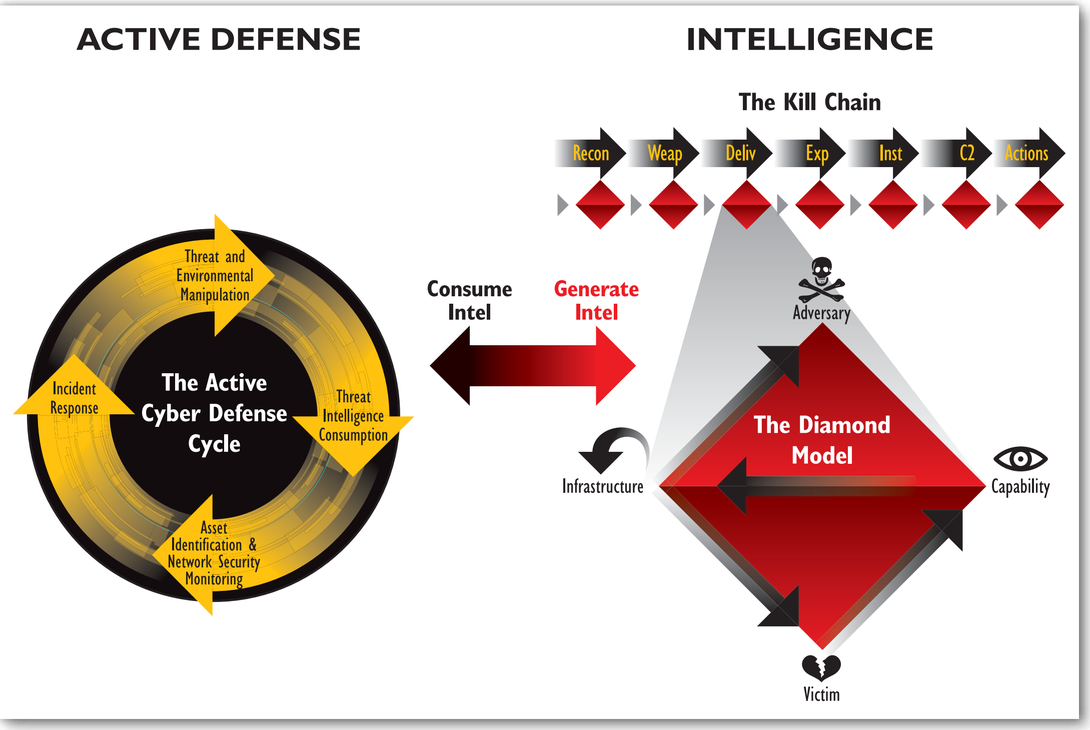


Figure 3. The Continual Process of Generating and Consuming Intelligence for Hunting Threats

Adding in the Hunting Maturity Model (as shown previously in Figure 1) as a measure of maturity for hunting makes this process an analyst-driven and successful effort.

[15] "The Sliding Scale of Cyber Security," SANS Institute InfoSec Reading Room, August 2015, www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Automating the Hunt

With automation, defenders do not have to start their search process over from the beginning every time they hunt an adversary. Most analysts are familiar with using self-made scripts or open-source tools, but professional tools and services are emerging to help hunt down threats in enterprise networks.

With automation, defenders do not have to start their search process over from the beginning every time they hunt an adversary.

What makes adversaries advanced is their ability to understand the target, have consistency across their actions and possess the logistics and coordination to carry out long-term campaigns. These same principles must be applied to threat hunting technologies: They should enable defenders to understand their environments, have consistency across the start of their hunts and possess the logistics and coordination to hunt and counter adversaries over time.

When choosing the appropriate platform for threat hunting, look at specific elements of automation, how they incorporate various data sources, and their ability to identify and correlate patterns and to fully investigate and uncover adversary activity. These force multipliers combined with the right people ensure a successful, long-term security process in any organization.

Conclusion

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.

The overall goal should be to build an approach tailored to the organization as well as its threat landscape. Waiting until the attack cycle is complete and then responding to the threat is costly and dangerous—the damage has been done, data has been lost and the costs to repair are high. The key is to create a threat hunting capability that can take in the threat information as early in the kill chain as possible, analyze and act upon it with accuracy, and reutilize the lessons learned.

Threat hunting is a proactive approach to identifying adversaries rather than reactively waiting for an alert to go off. Most organizations are doing threat hunting to some degree today. An understanding of their own hunting maturity will help guide organizations that need to grow these capabilities. At that point, organizations need to empower threat analysts with the right training, datasets and automated platforms to become analysis-driven defenders.

Threat Hunting

https://www.linkedin.com/company/threathunting
https://www.twitter.com/threathunting_

About the Authors

Robert M. Lee, a SANS certified instructor and author of the "ICS Active Defense and Incident Response" and "Cyber Threat Intelligence" courses, is the founder of Dragos Security LLC, a critical infrastructure cyber security company, where he focuses on control system traffic analysis, incident response and threat intelligence research. He has performed defense, intelligence and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Author of *SCADA and Me* and a nonresident National Cybersecurity Fellow at New America, focusing on critical infrastructure cyber security policy issues, Robert was named EnergySec's 2015 Energy Sector Security Professional of the Year.

Rob Lee is the curriculum lead and author for digital forensic and incident response training at the SANS Institute. With more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyberforensics branch, and a computer forensic and security software development team. He also worked for a leading incident response service provider and co-authored *Know Your Enemy: Learning About Security Threats*, 2nd Edition.

Sponsor

SANS would like to thank this paper's sponsor:

sqrrl

Last Updated: April 2nd, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS New Orleans 2020	New Orleans, LAUS	Jun 08, 2020 - Jun 13, 2020	Live Event
SANS Las Vegas Summer 2020	Las Vegas, NVUS	Jun 08, 2020 - Jun 13, 2020	Live Event
SANSFIRE 2020	Washington, DCUS	Jun 13, 2020 - Jun 20, 2020	Live Event
SANS Chennai 2020	Chennai, IN	Jun 22, 2020 - Jun 27, 2020	Live Event
SANS Pittsburgh 2020	Pittsburgh, PAUS	Jun 22, 2020 - Jun 27, 2020	Live Event
SANS Silicon Valley - Cupertino 2020	Cupertino, CAUS	Jun 22, 2020 - Jun 27, 2020	Live Event
SANS Cyber Defence Canberra 2020	Canberra, AU	Jun 29, 2020 - Jul 11, 2020	Live Event
Cyber Defence Japan 2020	Tokyo, JP	Jun 29, 2020 - Jul 11, 2020	Live Event
SANS Perth 2020	Perth, AU	Jun 29, 2020 - Jul 03, 2020	Live Event
SANS Chicago Spring 2020	OnlineILUS	Jun 01, 2020 - Jun 06, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced