Interested in learning more about security?

SANS Institute InfoSec Reading Room

Scalable Methods for Conducting Cyber Threat Hunt Operations

Information Security professionals commonly agree that organizations cannot prevent 100% of all cyber attacks. For this reason, organizations are encouraged to practice defense in depth so that if any one security measure fails, another will reduce the exposure and mitigate the impact. However, despite investing countless sums of money, manpower, and time into developing and maintaining a robust security infrastructure, organizations still struggle to identify and respond to cyber intrusions in a timely manner. Cyber T...

Scalable Methods for Conducting Cyber Threat Hunt Operations

GIAC (GSEC) Gold Certification

Author: Michael C. Long II, mrlong0124@gmail.com
Advisor: Adam Kliarsky
Accepted: July 11th 2016

Abstract

Information Security professionals commonly agree that organizations cannot prevent 100% of all cyber attacks. For this reason, organizations are encouraged to practice defense in depth so that if any one security measure fails, another will reduce the exposure and mitigate the impact. However, despite investing countless sums of money, manpower, and time into developing and maintaining a robust security infrastructure, organizations still struggle to identify and respond to cyber intrusions in a timely manner. Cyber Threat Hunt Teams have recently emerged as a proactive defense asset capable of methodically detecting and responding to advanced persistent threats that evade traditional rule or signature-based security solutions. This paper describes scalable methods and practices to plan and conduct cyber threat hunt operations throughout the enterprise.

1. Introduction

Dr. Eric Cole of SANS Institute stated three absolute facts regarding information security: "1) an organization cannot prevent all attacks; 2) an organization's network is going to be compromised; and 3) 100% security does not exist" (Cole, 2016). This statement reflects a harsh problem that large organizations struggle to address: despite investing overwhelming amounts of resources in developing, maintaining, and enhancing their organization's information security, they will inevitably be victims of cyber intrusions. This is not to marginalize the importance of maintaining a robust information security architecture, but to highlight that traditional signature-based security solutions are not sufficient to identify and respond to intrusions conducted by advanced persistent threats, particularly those who have lingered in networks in excess of years.

Data collected by the Sqrrl Security Analytics Company suggests that organizations struggle to identify intrusions in a timely manner. "On average it takes 205 days before an organization is able to find a malicious actor hidden in their systems" (Sqrrl Whitepaper, 2016). The reality is that organizations cannot afford to wait that long. In an era where cyber intrusions occur in minutes, the security of the organization depends on rapid identification and response actions. How then does an organization with robust information security processes enhance their capabilities to identify advanced adversaries in their network? Recently, organizations have begun proactively searching for advanced adversaries in their networks through a process known as Cyber Threat Hunting.

Cyber Threat Hunting is a "focused and iterative approach to searching out, identifying and understanding adversaries internal to the defender's networks" (Lee & Lee, 2016). While traditional security solutions are reliant on pre-established rules and algorithms, cyber threat hunting "pits human defenders against human adversaries" (Lee & Lee, 2016). Threat hunting is based on the premise that organizations do not have to wait for an automated alert before responding to a threat. Threat hunting recognizes that intrusions revolve around human threats, and by that token, it takes a human being to understand and dynamically respond to subtle indicators of compromise. Threat Hunters

accomplish this by analyzing large quantities of disparate data sources in order to make inferences and correlations that ultimately lead to the identification of advanced adversaries, who are otherwise likely to remain undetected.

According to Dr. Cole's survey of 494 participants, "nearly 86% of organizations are involved in threat hunting today, albeit informally, as more than 40% do not have a formal threat-hunting program in place" (Cole, 2016). Furthermore, of the organizations performing threat hunting, "less than 3% follow any formal, published, external methodology" (Cole, 2016). These figures indicate that organizations understand the value offered by Threat Hunters; however, they are struggling to integrate threat hunting as a formal capability within their information security program. Without a tested, verifiable, and repeatable methodology, threat hunting becomes far less effective and consistent. The objective of this research is to offer a scalable methodology for organizations to utilize to conduct cyber threat hunt operations in the enterprise.

1.1 Overview of the Threat Hunting Methodology

The Sqrrl Security Analytics Company provides a broad framework for conducting cyber threat hunt operations. This framework includes four specific steps that are performed cyclically (Sqrrl Whitepaper, 2016):

1. Create a Hypothesis
2. Investigate via Tools and Techniques
3. Uncover new Patterns and Tactics, Techniques, and Procedures (TTPs)
4. Inform and Enrich Analytics

These steps describe the essence of conducting cyber threat hunt operations; however, specific details such as planning, implementation, and specific TTPs are left to the organization to determine. This research will incorporate and expand upon the Sqrrl Threat Hunting framework to offer organizations specific guidance on conducting threat hunt operations.

Michael C. Long II, mrlong0124@gmail.com

The following table depicts this methodology with specific tasks to be performed while conducting threat hunt operations. This methodology will be examined in detail in the sections that follow.

Cyber Threat Hunt Methodology	
Create Hypothesis	• Analyze Threat Intelligence • Evaluate Threats and Vulnerabilities • Formulate Hypothesis
Investigate via Tools and Techniques	• Log Analysis • Network Analysis • Host Analysis
Uncover New Patterns and TTPs	• Intrusion Discovery and Response • Attack Tree Analysis
Inform and Enrich Analytics	• Develop Automated Hunt Techniques • Generate Threat Intelligence • Enhance Security Posture

Figure 1. Cyber Threat Hunt Methodology

2. Threat Hunting Prerequisites

Cyber threat hunting is an advanced practice that requires a significant investment of personnel, equipment, and time. "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" (Lee & Lee, 2016). Foundational security policies and practices should be thoroughly established and routinely followed before adopting cyber threat hunting. Furthermore, senior leadership must have an understanding of the value that threat hunting brings to an organization and extend their support to the program.

Michael C. Long II, mrlong0124@gmail.com

Before an organization commits to cyber threat hunting, they need to assess their available personnel, security assets, and information security maturity.

2.1 Threat Hunt Personnel

Organizations need to assess their staff and determine how they can allocate personnel for threat hunting. According to Dr. Cole's survey, only 28% of organizations have a threat hunting program with assigned staff (Cole, 2016). Other organizations were reported as utilizing existing personnel from areas such as Computer Security Incident Response Teams or Security Operations Centers. Regardless, when deciding how to staff cyber Threat Hunters, organizations should plan around a framework of capabilities, and apply it based on the size of their network and the numbers and experience of their personnel. Broadly speaking, a threat hunting teams can be characterized by four key roles with supporting and complementary skill sets:

1. Supervisory
2. Host Hunt
3. Network Hunt
4. Threat Intelligence Analyst

The supervisory role serves as the primary command and control node responsible for planning and execution of threat hunt operations. This role interfaces with key leadership, conducts mission planning, and prioritizes and synchronizes tasks of subordinate Threat Hunters.

Host Hunters examine information systems and endpoints for indicators of compromise. Host hunters will benefit from teams with diverse expertise and skills in areas such as host intrusion analysis, system administration, incident response, and malware analysis.

Network Hunters are the network based counterpart to Host Hunters. Network Hunters focus on examining network activity via network flow, packet analysis, and network device logs. Network Hunters will have experience in network intrusion analysis, network device administration, incident response, and Network IDS/IPS.

Michael C. Long II, mrlong0124@gmail.com

The Threat Intelligence Analyst will consume and generate threat intelligence that drives hunt operations. Threat Intelligence Analysts are instrumental to the success of a hunt operation. In essence, the Threat Intelligence Analyst will examine threat intelligence from private and public sources and identify threats that are relevant to their organization. This information will be fed to the Threat Hunters in order to focus their efforts and increase the likelihood of identifying advanced intruders in their network. During threat hunting operations, the Threat Intelligence Analyst will track and correlate indicators of compromise found by Host and Network Hunt personnel. They will also consolidate the results of the Host and Network hunts and produce a cohesive product that documents the results of the threat hunting team and simultaneously enriches existing threat intelligence analytics.

The roles and responsibilities of a typical Threat Hunting Team are summarized in Figure 2.

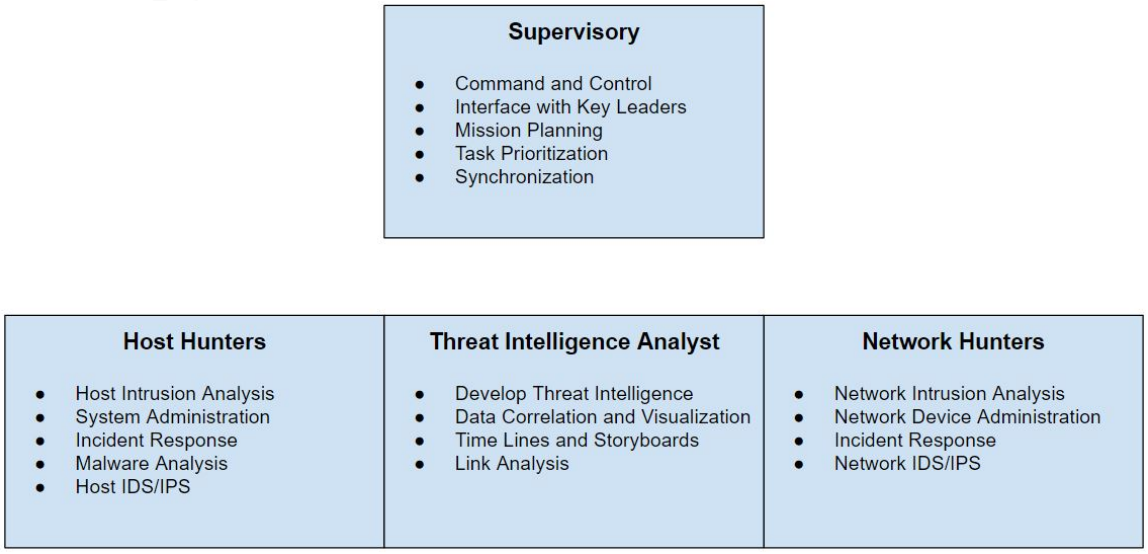

Figure 2. Threat Hunt Organization

One issue new threat hunt teams struggle with is that personnel are pulled from existing positions, such as IT/security or incident response. For the greatest return on

investment, organizations should utilize personnel whose primary responsibility is threat hunting. While this requires greater investment from the organization, dedicated personnel ensure threat hunting operations are executed routinely with consistent quality. Furthermore, threat hunting is an activity that becomes more effective over time as Threat Hunters gain greater insight and intuition regarding the activities on their network. Organizations should avoid tasking other IT/security staff with threat hunting as "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" (Lee & Lee, 2016).

2.2 Information Security Assets and Capabilities

Organizations need to ensure that they have adequate security assets in place to support 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” (Lee & Lee, 2016). Successful threat hunting requires a wide assortment of tools and sensors to collect, aggregate, and analyze data for indicators of compromise. "Data collection should be expanded to include as many data sources as you can handle, from netflow to DNS logs, in addition to data enrichment sources such as threat intelligence" (Sqrrl Whitepaper, 2016). The success of threat hunting is proportional to the amount of data the Threat Hunters may leverage in pursuit of adversaries, as well as the access they are afforded. Threat Hunters require vast amounts of information derived from logs, sensors, etc. and also require uninhibited access to examine systems for indicators of compromise. At a minimum, Threat Hunters need platforms that facilitate centralized logging, network activity monitoring, endpoint protection, and data collection and aggregation.

2.3 Organizational Maturity

For Threat Hunters to be effective, they have to be engaged in threat hunting on a regular basis. “They need to get to the point where they have the skills and capability to launch hunts automatically and on a regular basis, without waiting first to see an IOC”

(Cole, 2016, p. 1). This end state requires a mature information security program. To assess maturity, organizations should examine the CIS Critical Security Controls for Effective Cyber Defense (Center for Internet Security, 2015). The Critical Security Controls offers a comprehensive list of tasks that should be performed in order to build a robust and effective information security program. Once these tasks are executed routinely and effectively, organizations may consider adding threat hunting as an additional capability to further enhance their security.

CIS Critical Security Controls for Effective Cyber Defense	
CSC 1:	Inventory of Authorized and Unauthorized Devices
CSC 2:	Inventory of Authorized and Unauthorized Software
CSC 3:	Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
CSC 4:	Continuous Vulnerability Assessment and Remediation
CSC 5:	Controlled Use of Administrative Privileges
CSC 6:	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7:	Email and Web Browser Protections
CSC 8:	Malware Defenses
CSC 9:	Limitation and Control of Network Ports, Protocols, and Services
CSC 10:	Data Recovery Capability
CSC 11:	Secure Configurations for Network Devices such as Firewall Routers, and Switches
CSC 12:	Boundary Defense
CSC 13:	Data Protection
CSC 14:	Controlled Access Based on the Need to Know
CSC 15:	Wireless Access Control
CSC 16:	Account Monitoring and Control

Michael C. Long II, mrlong0124@gmail.com

CSC 17:	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18:	Application Software Security
CSC 19:	Incident Response and Management
CSC 20:	Penetration Tests and Red Team Exercises

Figure 3. CIS Critical Security Controls for Effective Cyber Defense

3. Planning Threat Hunting Operations

3.1 Preparation

Adequate preparation is essential to the success of any operation. Successful threat hunting first depends on thoroughly understanding the operating environment. Threat Hunters need to have a deep understanding of the authorized assets, configurations, and critical data located on their network. Threat Hunters need to have processes in place to ensure acquisition and preservation of baselines documenting system configurations and changes. Current and historic baselines serve as a means of monitoring and comparing changes over time. Threat Hunters need to automate the collection and storage of this information, preferably in a database to facilitate queries and data aggregation. Finally, Threat Hunters need to ensure that senior management understands and approves of the hunt program. This will ensure that hunt activities have the support they require and that they are in synch with the organization's security goals and priorities.

3.2 Mission Analysis

"Threat hunting is an analyst-driven process that is meant to address issues outside of what a single alert or indicator can reveal" (Lee & Lee, 2016). Threat Hunting Operations should be preceded with an analysis of threats. For an adversary to be considered a threat, it must have three things: intent, capability and opportunity to do harm (Homeland Security, 2008). Threat Hunting is conducted on the basis that cyber threats are fundamentally human threats. Effective threat hunting entails understanding

the human threat. Threat Hunting Operations should be preceded with a review of threat intelligence, whether that means examining data related to historic breaches/incidents, reviewing logs and alerts, or examining open source intelligence for threats specific to the organization. This information is used to focus Threat Hunters and ultimately give them direction needed to hunt for adversaries who are already within their network.

3.3 Creating a Hypothesis

A foundation built on threat intelligence transitions into a defining characteristic of threat hunting: a hypothesis. Simply speaking, threat hunting starts with a question: What threats may be in the organization? How would the adversary infiltrate the organization? What would their objectives be? These questions enable Threat Hunters to develop a specific and measurable hypothesis grounded in an understanding of the threat which will ultimately drive the hunt operation.

For a hypothesis to be effective, it has to be testable. An example hypothesis could state that executive management is at an elevated risk of compromise from state-sponsored actors who seek trade secret information. Threat hunters could then evaluate possible threat vectors such as spear phishing. “Phishing, as a leading action of Cyber-espionage, provides a number of advantages—the time to compromise can be extremely quick and attackers can target specific people” (Verizon, 2016). Threat Hunters could identify potential footholds, pivot points, and user credentials that are likely to be compromised following initial intrusion. This information culminates in providing Threat Hunters key people, systems, and techniques that adversaries are likely to exploit in order to complete their objectives. The end result is that Threat Hunters have specific guidance and direction in order to efficiently conduct threat hunting operations.

4. Investigate Via Tools and Techniques

With a hypothesis derived from risk and threat intelligence, Threat Hunters proceed to resolve their hypothesis by investing via tools and techniques. "Hypotheses are investigated via various tools and techniques, including Linked Data Analysis and

visualizations. Effective tools will leverage both raw and linked data analysis techniques such as visualizations, statistical analysis, or machine learning to fuse disparate cybersecurity datasets." (Sqrrl Whitepapers, 2016). To emphasize scalable practices, this methodology breaks down threat hunt operations into three key techniques that are performed concurrently and synergistically: log analysis, network analysis, and host analysis.

4.1 Log Analysis

Log analysis is a task that is performed by both host and network hunters, albeit with respect to their areas of focus. Effective log analysis offers Threat Hunters a detailed understanding of events occurring in their network and on their systems. The NIST Guide to Computer Security Log Management recommends collecting a diverse set of logs such as firewalls, routers, IDS/IPS, etc. (Kent & Souppaya, 2006). Diverse collections of logs enable Threat Hunters to holistically scrutinize activity on their network and correlate and visualize subtle indicators of compromise. Log analysis often serves as a starting point for follow-on investigations by Network and Host Hunters.

The challenge with log analysis involves balancing log generation, quantity, and retention limitations. However, an accurate understanding of cyber threats should prioritize the type, quantity, and turnover of collected logs. Regardless of organizational requirements, for an adversary to maintain persistent access to a system after reboot, they inevitably have to modify or add user/group accounts, processes, and listening ports (Cole, 2015). This provides an opportunity for Threat Hunters efficiently identify indicators of compromise by focusing on three key areas: log integrity, object access, and changes to processes and listening ports.

Advanced adversaries commonly cover their tracks by modifying or deleting log entries. Monitoring the integrity of logs can aid in rapidly identifying threat actors on the network. Threat hunters should scrutinize instances where all logs are purged, and where local logs differ from centralized logging utilities such as Syslog, Splunk, or ELK. Threat

Hunters can compare the logs of their target systems with those of the centralized solution and verify that data has not been altered or purged altogether.

Perhaps the most important factor in log analysis entails monitoring the activity and behavior of privileged users and groups. "63% of confirmed data breaches involved weak, default, or stolen passwords" (Verizon, 2016). As administrative access is often a prerequisite to follow on adversary exploitation, administrative access must be closely monitored and verified by Threat Hunters. Threat Hunters should also expand their search to high-value users, such as C-level executives, IT/IA personnel, and finance and human resources, who are likely targets of advanced adversaries.

Advanced threats are fundamentally information driven. “90% of Cyberespionage breaches capture trade secrets or proprietary information” (Verizon, 2016). In conjunction with monitoring privileged users and groups, Threat Hunters need to closely monitor access attempts to their critical data and resources. Casual users typically do not have a significant amount of failed access attempts and have relatively predictable access behavior. Threat Hunters should utilize their logs to scrutinize the number of accessed objects, the frequency of access, and success or failures of access. This will enable Threat Hunters to effectively hone in on anomalies that can lead to the identification of additional indicators that may be linked to advanced adversaries.

Persistent access to systems is required for sustained exploitation of an organization’s information assets. While advanced threats can obfuscate their activities through means such as rootkits, they inherently have to sustain access to their targets to continue to operate. This implicitly requires that adversaries modify a system’s listening ports and processes. Logging can be useful to identify instances of new processes and open ports, particularly when examining processes that were started by privileged users.

4.2 Network Analysis

The focus of Network Threat Hunters is network activity monitoring and analysis. Network analysis poses challenges due to encryption, bandwidth, storage, and processing limitations, and an increasingly clever adversary. Despite these limitations, network

analysis offers Threat Hunters a scalable means to identify and react to advanced adversaries in the network (Bejtlich, 2013). When used in conjunction with log and host analysis, Threat Hunters can achieve a holistic and comprehensive examination of their systems for adversary presence.

Network Threat Hunters analyze a diverse set of network activities, such as packet captures and network flow, network IDS/IPS alerts, and network device logs. While organizational requirements will dictate the specific sources of network information, Threat Hunters should focus their analysis on examining four key network characteristics: the number of outbound network connections, the duration of connections, the amount of data exchanged, and the frequency of connections. When a host is compromised, these characteristics will nearly always deviate from normal user activity in a significant way (Cole, 2015). Using capabilities such as network flow analysis, protocol analysis, and statistical analysis, Threat Hunters can visualize and identify anomalous hosts in their network based on the way that they communicate. This can serve as a springboard to allow Threat Hunters to identify compromised hosts and by extension adversaries on their network. The suspect IP addresses can then be correlated against the findings of Host Threat Hunters as well as the network as a whole.

4.3 Host Analysis

Host Threat Hunters focus on examining the behavior and configuration of host systems. This is accomplished by comparing configurations against established baselines, reviewing alerts from security solutions such as anti-virus and host IDS/IPS, and verifying integrity of the filesystem. Threat Hunters continuously verify the state of these data sets and compare them against historic reporting, preferably in a way that supports data visualization.

As indicated in the Log Analysis section, adversaries inevitably modify a system's users/groups, processes, and network connections. Host Threat Hunters should focus on these areas by comparing current configurations to established baselines and norms. In conjunction with historical comparisons, Host Threat Hunters should closely

monitor and scrutinize the status and activities of privileged users and groups. For example, Host Threat Hunters should observe logon periods of privileged users and hunt for anomalies that deviate from traditional user behavior.

5. Uncover New Patterns and TTPs

Threat Hunt teams may be inclined to focus their efforts on hunting for basic indicators of compromise such as malicious hashes, IP addresses, and filesystem artifacts. While this may result in some quick wins, it is trivial for advanced adversaries to modify these indicators. Instead, as Threat Hunters should focus on understanding the overarching TTPs that produced in the indicator through a process known as attack tree analysis. Attack tree analysis entails modeling what steps an adversary may perform to breach the organization's systems (Schneier, 1999). Models such as the Lockheed Martin Cyber Kill Chain or the Mandiant Attack Lifecycle can be helpful to determine where in the attack tree an adversaries' activities occurred.

Adversary Action	Techniques, Tactics, and Procedures
Reconnaissance	• Port scanning, harvesting email addresses, etc.
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim vic email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code on the victim system
Installation	• Installing malware on the asset

Michael C. Long II, mrlong0124@gmail.com

Command and Control	• Command channel for remote manipulation of victim
Actions on Objectives	• Intruders accomplish their original goal

Figure 5. Lockheed Martin Cyber Kill Chain

By determining where a respective indicator fits within the attack tree, Threat Hunters can identify information gaps and then attempt to resolve them through additional investigative techniques. As Threat Hunters uncover the adversary attack tree, they achieve a holistic view of the adversaries' TTPs, which augments follow on hunts and enhances the organization's overall information security posture.

Threat Hunters receive the greatest return on their efforts by focusing on uncovering adversary TTPs. "TTPs reflect an attacker's behavior, and behavior requires a significant time and monetary investment to modify" (Sqrrl Blog, 2015). In practice, this means detecting and combatting techniques such as Pass-the-Hash attacks rather than uncovering artifacts incident to adversaries who conduct those attacks. By focusing on detecting and responding to adversary TTPs, Threat Hunters gain an advantage by operating directly on adversary behaviors, rather than adversary toolsets (Sqrrl Blog, 2015).

Uncovering new patterns and TTPs enables Threat Hunters to evolve their information security processes as well as the threat hunt program itself. "As defenders catalog observations about attackers' TTPs, weak points in their defenses, and any obstructions in the investigative workflow, they can streamline response times and offset the challenge of persistence" (Sqrrl Blog, 2015). As Threat Hunters continue uncovering new TTPs, their results feed back into their existing processes and systems, refining their detection, response actions, and efficiency. When incorporated with data visualization, threat intelligence, and machine learning techniques, this process enables Threat Hunters to stay one step ahead of attackers.

Michael C. Long II, mrlong0124@gmail.com

6. Inform and Enrich Analytics

A defining characteristic of Cyber Threat Hunting is that "successful hunts form the basis for informing and enriching automated analytics" (Sqrrl Whitepapers, 2016). As Threat Hunters discover effective methods of identifying adversary TTPs during hunts, they should develop automated solutions to counter the TTPs throughout the organization's network. "There are many ways this can be done, including developing a saved search to run regularly, creating new analytics using tools like Sqrrl, Apache Spark, R, or Python, or by even providing feedback to a supervised machine learning algorithm confirming that an identified pattern is malicious" (Sqrrl Whitepapers, 2016). This enables Threat Hunters to continue conducting operations to uncover new adversary TTPs.

Threat Hunters should also contribute to the body of threat intelligence. As Threat Hunter examinations reveal new adversary TTPs, they need to feed their findings into existing monitoring systems. As this process continues, Threat Hunters mature beyond generic hypothesis-driven hunts to hunts driven by threat intelligence. This results in more efficient hunts and greater organizational security.

7. Conclusion

Traditional rule-based defensive solutions are not enough to enable defenders to quickly identify and respond to advanced persistent threats. While traditional defense in depth practices are important to safeguarding the network, they do not address the issue of latent adversaries who remain in the organization's network. Cyber Threat Hunting aims to address the issue of identifying advanced adversaries by adopting a preemptive and deliberate methodology of routinely hunting for intruders on the network.

While many organizations perform threat hunting in some capacity, 40% of those surveyed by Eric Cole do not have a formal threat hunting methodology (Cole, 2016). This research incorporated the threat hunting framework provided by Sqrrl and expanded upon it to offer specific guidance on implementing and conducting threat hunt operations in a way that can scale across disparate organizations.

Michael C. Long II, mrlong0124@gmail.com

Guidance was offered on organizing a threat hunting team into four distinct roles: Host Threat Hunters, Network Threat Hunters, Threat Intelligence Analysts, and Supervisory. These four roles are developed into a functional Threat Hunter team after carefully assessing the organization's existing assets and maturity. Fundamentally, Threat Hunters require vast amounts of information in order to leverage analytics, visualizations, and machine learning to uncover advanced threats in the network.

Threat Hunters begin to operate after performing mission analysis. They begin with a hypothesis: where would an adversary be within the network? What would their objectives be? This hypothesis should be grounded in risk analysis, threat intelligence, and organizational priorities. With a documented hypothesis, Threat Hunters begin the hunt by investigating via tools and techniques.

During this phase, Threat Hunters divide responsibilities between Host and Network Threat Hunters, and a Threat Intelligence Analyst. As these Threat Hunters operate, they focus on identifying adversaries and uncovering new Patterns and TTPs. Their findings are fed back into the threat hunt cycle, which has the effect of informing and enriching analytics. As Threat Hunters discover successful techniques, they create automated solutions that can be deployed throughout their enterprise. The cycle then comes full circle as the results from the previous hunt inform and enrich the next.

Threat hunting can be a viable method for reducing the time it takes to identify adversaries in the network. By conducting deliberate and iterative threat hunts, organizations maintain a higher state of readiness and potentially dramatically enhance their information security posture.

Michael C. Long II, mrlong0124@gmail.com

References

Bejtlich, R. (2013). *The Practice of Network Security Monitoring*. San Francisco, CA: No Starch Press.

Center for Internet Security. (2015, October 15). Critical Security Controls for Effective Cyber Defense Version 6.0. Retrieved June 18, 2016, from https://www.cisecurity.org/critical-controls.cfm

Cole, E. (2016, April). Threat Hunting: Open Season on the Adversary. Retrieved June 2, 2016, from https://sqrrl.com/media/Survey_Threat-Hunting-2016_Sqrrl-1.pdf?submissionGuid=351af157-b8cf-428d-a92b-96368c8e7bf6

Homeland Security. (2008, September). DHS Risk Lexicon. Retrieved July 5, 2016, from https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

Kent, K., & Souppaya, M. (2006, September). Guide to Computer Security Log Management. National Institute of Standards and Technology (NIST) Special Publication 800-92. Retrieved June 27, 2016, from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Lee, R., Lee, R. M., & Maldonado, L. (2016). *Threat Hunting* [Video file]. Retrieved from https://vimeo.com/sqrrldata/review/154213694/eef1c5a649?submissionGuid=9d93b83c-2914-487d-8cf9-df55fd27b7f1

Lee, R. M., & Lee, R. (2016, February). The Who, What, Where, When, Why and

How of Effective Threat Hunting. Retrieved June 1, 2016, from https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

Schneier, B. (1999, December). Attack Trees. Retrieved July 3, 2016, from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Sqrrl Blog. (2015, July 23). A Framework for Cyber Threat Hunting Part 1: The Pyramid of Pain. Retrieved July 2, 2016, from http://blog.sqrrl.com/a-framework-for-threat-hunting-part-1-the-pyramid-of-pain

Sqrrl Whitepaper. (2016). What is a Threat Hunting Platform? Retrieved June 13, 2016, from https://sqrrl.com/media/THP-White-Paper.pdf?submissionGuid=5afae1ef-4b62-4499-bfad-b5828b194638

Sqrrl Whitepaper. (2016). A Framework for Cyber Threat Hunting. Retrieved June 13, 2016, from http://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf?submissionGuid=ea14adfd-ef1a-4016-80ed-421732d5a44a

Verizon. (2016). Verizon 2016 Data Breach Investigations Report. Retrieved June 14, 2016, from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Michael C. Long II, mrlong0124@gmail.com

Last Updated: March 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Boston Spring 2018	OnlineMAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced