Prescriptive Risk Solutions, LLC

April 2017

CISO Series on Today's Critical Issues

Cyber Threat Hunting

By Tari Schreider C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author

Prescriptive Risk Solutions, LLC.

EC-Council

http://ciso.eccouncil.org/

What is Cyber Threat Hunting?

If you are tired of the suspense of waiting for the bad actors to come to you, consider going to them. A rapidly emerging practice is cyber threat hunting. As the name implies, some organizations have gone on the offensive and have begun to hunt down bad actors seeking evidence of their malicious activity within their network. Threat hunting leverages cyber intelligence, threat analytics and security information and event management solutions to hunt advisories. Cyber threat hunting is “what’s next” for your security operations (SecOps).

A 2016 SANS Institute survey of nearly 500 participants on threat hunting reveal that nearly 86% of organizations are involved in some form of threat hunting today, albeit informally. According to the survey author Dr. Eric Cole, respondents are still figuring out exactly what a threat-hunting program should look like, how to attract the right skills and how to automate their hunting processes.

Rather than focusing on the noise of attacks crashing the gates of your firewall, hunting focuses on what may already be happening inside your network. Identifying lateral or east-west movement of attackers searching your devices to gain access privileges is where the big game is now. Many prominent attacks have occurred when attackers have been inside the network for months if not years.

You must face a reality of life today, hackers or insiders with ill intent already live behind your firewall searching your network for vulnerabilities to exploit.

CYBER THREAT HUNTING APPROACHES

Cyber threat hunting efforts range from informal manual efforts to sophisticated big data-driven approaches. However, all share a common goal, stay one-step ahead of the hackers to be there waiting when they arrive. Hunting has been around in various incarnations for ten years and has matured from advanced IDS signatures to automated solutions that actively and aggressively seek out and destroy malware left by attackers.

CYBER THREAT HUNTING TOOLS

Taking the right guns and ammo with you on a hunt is tantamount to the hunt's success. You will need weapons that can detect stealth attacks that move slowly and laterally through our network. These tools use different techniques to bag their quarry. For example, Sqrrl relies on SIEM data, endpoint devices and outside threat feeds to detect network behaviors missed by conventional security dashboards. Infocyte HUNT on the other hand dispatches dissolving agents to all endpoints on the network to report suspicious activity. Then there are products like Endgame, which deploy permanent agents with the power to destroy threats.

The following table lists leading threat hunting tools on the market:

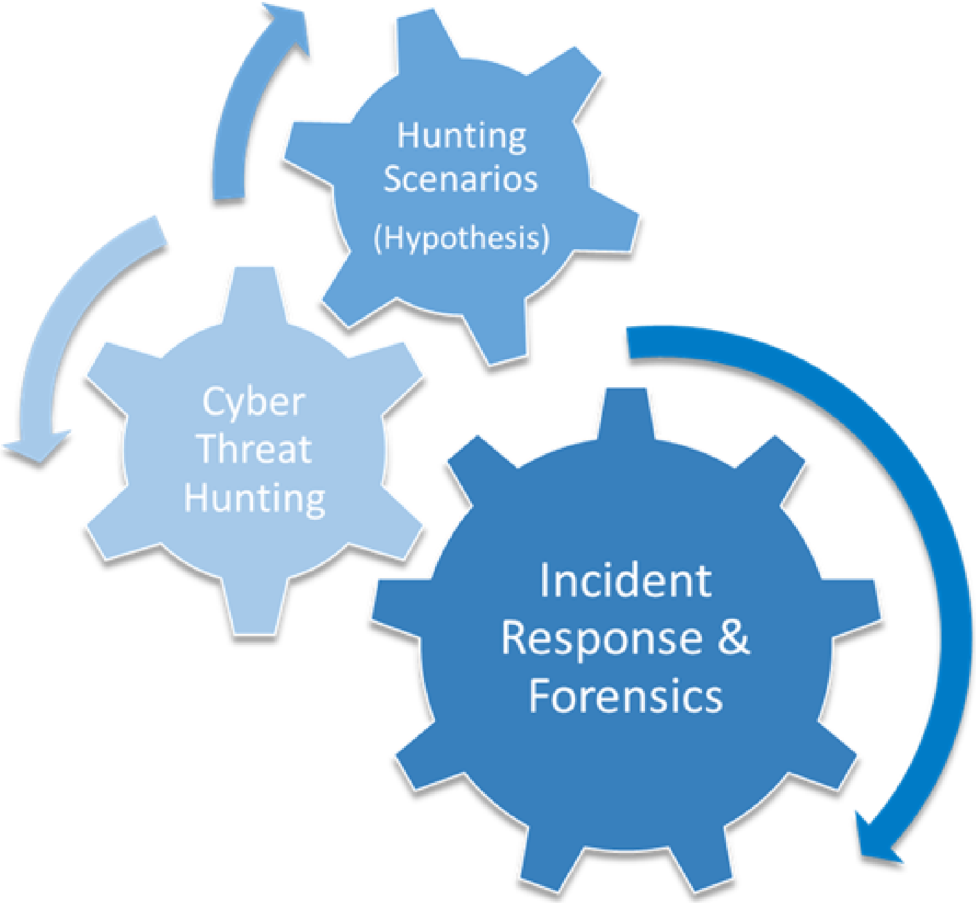
COMPANY	PRODUCT
Carbon Black	Cb Repsonse
Endgame	Endgame
Infocyte, Inc.	Infocyte HUNT
Nuix	Nuix Insight Analytics & Intelligence
Sqrrl Data Inc.	Sqrrl Enterprise

Excerpted and adapted from The Manager's Guide to Cybersecurity Law: Essentials for Today's Business, Copyright ©2017, Rothstein Associates Inc. Used with permission.

Cyber Threat Hunting Model

Hunting cyber threats is complex, time and resource consuming as well as expensive. It is best to create a model or framework with rules of engagement to limit the scope of your hunting and follow a disciplined approach. You need to remember that not every hunt will yield big game, sometimes the game just does not show up.

The following is a basic cyber threat hunting model you can use to draft your approach:



Excerpted and adapted from The Manager's Guide to Cybersecurity Law: Essentials for Today's Business, Copyright ©2017, Rothstein Associates Inc. Used with permission.

HERE ARE THE ROLES OF EACH COMPONENT OF THE MODEL:

- **Hunting Scenarios –** Here you will narrow your quarry to increase the chances of success of your hunt. Use your threat intelligence to identify the specific bad actor you feel is targeting your industry or technology. Declare the timeframe you will spend hunting before you move on to a secondary target. Develop hypotheses to stage your hunts. For example, I think bad actors are exfiltrating financial data. You will also identify the tools you will use for the hunt here.

- **Cyber Threat Hunting –** Determine your hunting strategy, specifically where you will focus your hunting. If your hypothesis is the bad actor is exfiltrating financial information, go to your financial database to search for indictors of compromise. If your hypothesis is, hackers are laterally looking for servers to compromise seeking to exploit a specific vulnerability, go look at your vulnerable servers. This way you can cut them off at the pass.

- **Incident Response & Forensics –** If your hunt is successful, you will need to bag your prey. This will include activating your first responders to remove malware, change passwords, drop connections, etc. You will need to follow your incident response plan as if you were under attack, why, because you are!

Cyber threat hunting product provider, Sqqrl has published an excellent framework and model of **cyber hunting maturity**. This and other the SANS Reading Room suggestions I provided at the end of the white paper should give you ample examples to build your own cyber hunting approach.

PENETRATION TESTING VS. CYBER THREAT HUNTING

To some there may be confusion between penetration testing and cyber threat hunting. The fastest way to clear up the ambiguity of these terms is to think of cyber threat hunting as an offensive measure. Penetration testing reviles how an attacker could enter your network; cyber threat hunting tells you if they are already in.

I see penetration testing as a methodology with specific phases followed to yield results (e.g., reconnaissance, enumeration, exploitation). Cyber threat hunting is tradecraft alike to that used by spies. You can also think of it as the difference between what could happen and what is happening.

Cyber Threating Hunting Using Your SIEM

Your SIEM could be an effective tool to perform cyber threat hunting. However, you will need to shift your thinking that attackers announce their presence through alerts to your SIEM. It often does not work this way. Hunting is proactive and iterative; detecting adversaries who work hard to evade detection requires persistence and discipline.

Nonetheless, SIEMs are an integral part of your security operations center (SOC), which you have made a significant investment in time and money, so you definitely should use it to hunt attackers.
By now, all SIEM providers have published a white paper on using their SIEM to hunt cyber attackers. Their basic premise is that aggressors of your network use and leave behind advanced malware. Subsequently, SIEMs can detect unknown files and executables as well as perform contextualization of content flow with network traffic to identify exfiltration.

SIEMs can be effective in hunting when an organization uses a sandbox to detain and study malware. The SIEM monitors the activities of the malware establishing a baseline of indicators of compromise (IoC) that can be used to “hunt back” through logs to identify IoC.

I suggest you exploit the full potential of your SIEM before investing in a cyber threat hunting solution. Once satisfied with your efforts to leverage your SIEM investment, evaluate integrating cyber threat hunting solutions to complement your SIEM and move your SOC to the next level of maturity.

THE THREAT HUNTING PROJECT

The Threat Hunting Project curates cyber threat hunting information from blogs, conference presentations, white papers, etc. in the interest of promoting the practice. Their annotated reading list is the best place to get smart on cyber threat hunting quickly.

Excerpted and adapted from The Manager’s Guide to Cybersecurity Law: Essentials for Today’s Business, Copyright ©2017, Rothstein Associates Inc. Used with permission.

LEARNING MORE ABOUT CYBER THREAT HUNTING

The following are excellent sources of cyber threat hunting background information:

- ✓ Scalable Methods for Conducting Cyber Threat Hunt Operations
- ✓ The Who, What, Where, When, Why and How of Effective Threat Hunting
- ✓ Generating Hypotheses for Successful Threat Hunting

Conclusion

Cyber threat hunting is one of the newer active defense or offensive cybersecurity disciplines. The cost and requirement for skilled resources to perform cyber threat hunting places it out of reach for many companies. Before embarking on anything new, it is always best to exploit existing cyber countermeasures such as your SIEM.

Early cyber threat hunting market entry providers have some great solutions, but there are decidedly different approaches. If you go this route, you will want an approach you are most comfortable. Begin learning as much as you can about cyber threat hunting before going out on your first hunt to make sure you don't go hunting elephants with a peashooter.

Excerpted and adapted from The Manager's Guide to Cybersecurity Law: Essentials for Today's Business, Copyright ©2017, Rothstein Associates Inc. Used with permission.

ABOUT THE AUTHOR

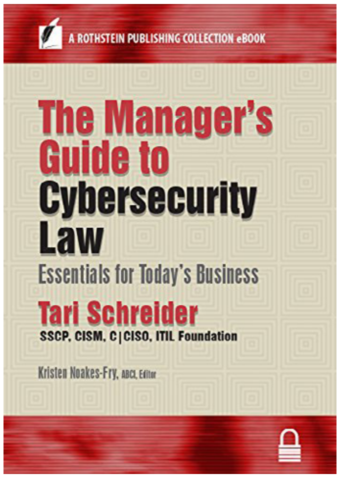
TARI SCHREIDER

C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author
Prescriptive Risk Solutions, LLC.
Atlanta, GA - Cheyenne, WY

www.prescriptiverisksolutions.com
tari@prescriptiverisksolutions.com

M: Atlanta – 678.595.2818
M: Cheyenne – 307.215.1330



A ROTHSTEIN PUBLISHING COLLECTION eBOOK

The Manager's Guide to Cybersecurity Law

Essentials for Today's Business

Tari Schreider

SSCP, CISM, C|CISO, ITIL Foundation

Kristen Noakes-Fry, ABCI, Editor

The Manager's Guide to Cybersecurity Law

Qualifies for Five (5) EC-Council ECUs.

Excerpted and adapted from The Manager's Guide to Cybersecurity Law: Essentials for Today's Business, Copyright ©2017, Rothstein Associates Inc. Used with permission.