Brought to you by:

vmware®

Threat Hunting

for dummies®
A Wiley Brand

Prepare to hunt

Gain the upper hand

Become a master hunter

VMware Threat Analysis Unit

VMware Security
2nd Special Edition

About VMware

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As a trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda.

To learn more, visit www.vmware.com/security.

Threat Hunting

VMware Security 2nd Special Edition

by VMware Threat Analysis Unit

for dummies®
A Wiley Brand

Threat Hunting For Dummies®, VMware Security 2nd Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

ISBN 978-1-119-88704-1 (pbk); ISBN 978-1-119-88705-8 (ebk)

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Client Account Manager: Cynthia Tweed

Production Editor: Pradesh Kumar

Special Help: Faithe Wempen

Table of Contents

INTRODUCTION 1
About This Book 1
Icons Used in This Book 2
Beyond the Book 2

CHAPTER 1: **Understanding Threat Hunting** 3
Looking at Today's Security Threats 3
What motivates cyberattackers? 4
What methods do cyberattackers use? 4
What is assumption of breach? 6
Defining Threat Hunting 7
What threats are hunted 7
Why you need threat hunting 8
Identifying the Tools and Techniques 9
Coexistence 9
Humans and machines 9
Details and the big picture 10
Intruders and signs of intrusion 10
Data exploration 11
Computing and the business 11
Knowing the battlefield 12

CHAPTER 2: **Preparing to Hunt** 13
People: Creating the Culture 13
Building the team 13
Making time to threat hunt 15
Training 15
Putting processes in place 16
Technology: Putting the Necessary Tools in Place 17
Achieving complete endpoint visibility 17
Achieving complete network visibility 18
Gathering threat intelligence 18
Integrating your information 19
Using data correlation and analytics tools 19
People and Technology: Knowing Your Environment 20
Differentiating between normal and abnormal 20
Knowing your high-value targets 20
Anticipating how you'll be attacked 20

CHAPTER 3: **The Hunt** 23
Understanding the Mentality of the Hunt 23
Planning for the Hunt 24
Outlining the Hunt Chain 26
Where and how to start 26
Filtering out legitimate activity 27
Hunt for suspicious activity 27
Deeper investigation 28
Scope the impact 29
Remediate 29
Update defenses 29

CHAPTER 4: **Becoming a Master Hunter** 31
Raising the Bar 31
Becoming Embedded in the Environment 32
Performing Research 33
Developing Intuition 34
Educated hunches 35
OODA 35
Strong opinions, loosely held 36
Developing Your Own Tools and Custom Integrations 36
Setting Land Mines 37
Taking the Threat Hunting Challenge 38

CHAPTER 5: **Ten Tips for Effective Threat Hunting** 39
Know Your Environment 39
Think Like an Attacker 40
Develop the OODA Mindset 40
Devote Sufficient Resources to the Hunt 41
Deploy Endpoint Intel across the Enterprise 41
Supplement Endpoint Intel with Network Intel 42
Collaborate across IT 42
Keep Track of Your Hunts 43
Hone Your Security Skills 44
Be Aware of Attack Trends 44

Introduction

In recent years, cyberattacks have increased by 300 percent. That's partly due to the rise of rogue nation-states and cyber cartel activity, as well as the wider availability of knowledge, tools, and technologies that lower the barrier to entry for hackers and increase overall attack success rates.

And here's a fact that should concern you: According to Atlas VPN, the economy of scale of the dark web is greater than that of Silicon Valley, totaling $1.5 trillion in revenue annually. This means that for organizations like yours, cyberattacks are an inevitable part of doing business, requiring greater investment and rigor in cyber defenses that can better keep pace with the changing threat landscape.

"Set it and forget it" defensive capabilities are a relic of the past. You need to be able to combat the ever-changing set of tactics, techniques, and procedures (TTPs) that hackers employ to infiltrate and carry out their attack objectives. You also need to be able to identify the custom malware attackers are deploying, as well as spot the sophisticated techniques they're using to ensure they can burrow into your organization and operate freely.

You also need to be able to fight counter incident response tactics, which try to thwart your attempts to ensure attackers can't maintain persistence. If an attacker can keep a foothold in your organization, they can use it to launch additional attacks against you and, subsequently, all your constituents.

This is where threat hunting comes into play. *Threat hunting* is the practice of proactively identifying early-stage attack activity — from an attacker getting ready to target your organization to an attacker preparing to launch the next phase of their attack from a hidden position (or persistent foothold) already established within your network. Carbon Black EDR can help you build the capacity you need to swiftly detect and respond to attackers, turning the tables and using their TTPs against them to ensure they can't achieve their objectives.

About This Book

Threat Hunting For Dummies, VMware Security Special Edition, introduces the concept of threat hunting and its role in protecting your organization's systems and information. After reading this book, you'll better understand how threat hunting works and why it's needed. You'll see that threat hunting is an essential component of any organization's security program.

Threat hunting requires specific tools and technology, but a successful program requires far more. It requires collaboration across IT and the business; a desire to make needed improvements to keep attackers out; environmental understanding, threat intelligence feeds, and ways to differentiate between what's expected and what's not.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way:

REMEMBER

Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.

WARNING

Watch out! This information tells you to steer clear of bad practices that leave you vulnerable, cost you big bucks, or suck your time.

TECHNICAL STUFF

This icon indicates technical information that's probably most interesting to technology planners and architects.

TIP

If you see a Tip icon, pay attention — you're about to find out how to save some aggravation and time.

Beyond the Book

This book is full of information that you can use to understand how to get your threat hunting program off the ground or take your existing program to a higher level. If you want to learn more than what's covered in these pages, you can find additional resources at `www.vmware.com/security/threat-analysis-unit-tau.html`.

IN THIS CHAPTER

- » Understanding today's security threats
- » Introducing the practice of threat hunting
- » Looking into the tools and techniques of threat hunting

Chapter 1 Understanding Threat Hunting

There's a story of a famous criminal who was asked why he robbed banks. His answer was simple and elegant: Because that's where the money is. Cybercriminal organizations today are no different. They steal information because they profit from it.

Threat hunting, though not actually a new concept, is now one of the hottest topics in the security industry. Passively waiting for evidence of intrusions is no longer cutting it. Instead, as the name suggests, threat *hunting* is all about proactively searching for would-be intruders and signs of potential future intrusions.

Looking at Today's Security Threats

You'd have to be living under a rock not to be aware of the scourge of security breaches that occur every day. Breaches have become so commonplace in the news that everyone almost seems numb to them. And yet, the ever-growing number of breaches makes you wonder if breaches can be avoided at all.

What motivates cyberattackers?

Organizations face security threats from cyber cartels, nation-states, and hackers for hire, as well as rogue attackers fueled by their own agendas. Some of their motivations include

- **Financial gain:** Hackers steal information that they can use for direct or indirect financial gain. For example, they steal credit card numbers to make purchases or gain access to medical records to commit Medicare fraud.
- **Political statement:** Hackers and "hacktivists" attack sites to make a political statement. A good recent example is the 2022 declaration by members of the Anonymous hacking group to get involved in the military conflict between Ukraine and Russia by defacing and bringing down some of Russia's government websites.
- **Theft of intellectual property:** Whether sponsored by nation-states bent on stealing military or industrial secrets or competitors seeking market advantage, hackers steal plans for weapons, aircraft, and commercial and consumer products.
- **Disruption of critical infrastructure:** Hackers disrupt or sabotage manufacturing, electric power generation and distribution, water supplies, and transportation systems, attempting to create chaos and anarchy.
- **Revenge:** Disgruntled personnel can cause all kinds of problems. When organizations fire or lay off personnel who have intimate knowledge about system access, these people may use that information to retaliate.
- **Fame:** Hackers are recognized and respected by their peers for compromising high-visibility or high-value sites, particularly those that take pride in how good their security is. Hackers like to humble these organizations.

Regardless of the motive, the end result is the same: the compromise of sensitive data or disruption of business operations, and sometimes both.

What methods do cyberattackers use?

Hackers will use everything in their arsenal to infiltrate your organization and maintain a consistent presence they can use to carry out their attacks. They're constantly developing advanced techniques designed to evade detection and make it increasingly difficult for existing security controls to defend against, such as custom and zero-day malware. However, they also rely on tried-and-true tactics that often still work due to the complexity and distributed, dynamic nature of today's digital enterprise. It takes only one vulnerability, one open port, or one person to fall for their scheme for an attacker to be successful. Because your organization's attack surface is constantly changing and expanding, it's essential to remain vigilant against both old and new threat vectors, such as:

- **Unauthorized access:** Attackers will gain access to resources in the network through the Remote Desktop Protocol (RDP), which enables a user to connect to another computer over a network connection; living off the land attack techniques that use legitimate binary for malicious purposes; and weaponized documents infected with malware/ransomware/malicious code, which may be part of a phishing attack. After they have access, they exfiltrate, encrypt, and destroy.
- **Stealthy malware:** Some malware is designed to evade detection tools that look for known attack patterns (called *signatures*). Hackers are increasingly taking the time to create custom, targeted malware that has never been seen before and can slip by defenses undetected.

  TECHNICAL STUFF

  One of the main techniques used by malware today is known as *polymorphism.* Malware re-encrypts or repackages itself for each new victim's computer, making every infected system appear to be unique. This thwarts antivirus software's main technique of detection by signature.
- **Hacking the people:** Intruders use various methods for tricking personnel into unwittingly granting them access to their workstations or the organization's network itself. This is most often accomplished via phishing emails that trick users into opening attachments or visiting websites. The result? Malware installed on endpoints that attackers consider a beachhead into the organization's networks. This malware can install keyloggers (short for *keystroke logging* and also called *keyboard capturing*) to steal login credentials, which gives intruders access to more systems and applications.
- **Hacking the systems:** This method is fast and doesn't involve human intervention. An attacker sends messages to

target systems in search of exploitable vulnerabilities, such as unpatched systems, unsafe security configurations, and default login credentials. Brute force attacks through password guessing are often quite successful because many people use easily guessed passwords to protect their systems and infrastructure.

- **Recruiting insiders:** Sometimes a lucrative alternative, intruders will attempt to "turn" a trusted insider into a spy for the dark side, enlisting insiders to provide secrets or access to internal systems.

Attackers will often employ a path of least resistance to break into an organization, but no matter how they can get in, they consider it a win. For you, it's the beginning of a compromise that could range from an irritant to an incident that threatens the ongoing viability of your organization.

What is assumption of breach?

Information security professionals used to put all their chips toward incident prevention. With the right defenses, security professionals believed they could keep any attacker from being able to compromise their defenses and get to the crown jewels — whatever they might be.

Prevention is ideal, but detection is a must.

Attackers, patient and resourceful, soon discovered that they could get into virtually any organization provided they followed time-proven techniques of research, reconnaissance, stealthy intrusion, and quiet exfiltration. This led to the modern philosophy of information security — *assumption of breach.* Assumption of breach simply means that you must accept the very real possibility that intruders are already inside your networks and systems, regardless of your defenses and your ability (or inability) to detect them. Much like it's almost impossible to say that a program is entirely free of vulnerabilities, not many people can confidently and correctly say that there are or have been no intruders in their networks. To think otherwise is foolish.

REMEMBER

Just because you can't see the obvious signs of intruders or technology hasn't alerted you to their presence doesn't mean they aren't there. The absence of security alerts only means that security mechanisms haven't been configured correctly or don't have all the context needed to indicate a threat.

Defining Threat Hunting

Threat hunting is the pursuit of indicators of compromise (IOCs) within public and private cloud servers, endpoints, and networks that may be symptomatic of a compromise, intrusion, or data exfiltration. Though the concept of threat hunting isn't new, the practice of threat hunting is for many organizations.

REMEMBER

With threat hunting, you proactively scour your organization to "find evil" instead of waiting for technology to alert you.

TIP

When threat hunting, you look for anomalies that don't typically surface. To do this effectively, you need solutions that provide highly granular visibility into every endpoint's and server's operating system — things like launched processes, command-line arguments, mechanisms of persistence, opened files, and network communications. Solutions such as Carbon Black EDR are tailor-made to hunt threats in all the endpoints across an enterprise. At the network layer, NSX Network Detection and Response provides network sandboxing, traffic analysis, and intrusion prevention system (IPS) capabilities that detect anomalous network activities and lateral movements of threat actors.

What threats are hunted

Threat hunting is systematic and requires patience and analytical skills. Threat hunters must continually look for indicators of an intrusion or an attacker's presence. Threat hunting needs to be instilled as a process that security teams make and schedule time for. The types of threat attributes that are hunted include the following:

- **Processes:** Hunters look for processes with certain names, file paths, checksums, and network activity. They want to find processes that make changes to registry entries, have specific child processes, access certain software libraries, have specific SHA-256 hashes, make specific registry key modifications, and include known bad files.

  TECHNICAL STUFF

  The SHA-256 hash, also known as a *checksum* for a file, is a 256-bit value (like a fingerprint of the file). This feature can be useful both for comparing files and ensuring their integrity.
- **Binaries:** Hunters look for binaries with certain checksums, filenames, hashes, paths, metadata, specific registry modifications, and other characteristics that indicate a threat.

- **Network activity:** Hunters look for network activity to specific domain names and Internet Protocol (IP) addresses or inbound connections from unauthorized sources, such as a beacon, backdoor, or command-and-control (C2) server, that shouldn't be allowed.
- **Registry key modifications:** Hunters can look for specific registry key additions and modifications that are abnormal.

TIP

Pay special attention to registry run key modifications, a common persistence mechanism.

REMEMBER

Threat hunting isn't about just finding "evil" within your systems. Instead, it's about anything that could be evidence that evildoers leave behind on your systems. With threat hunting, you're looking for things that IOC-based detection wouldn't catch.

Why you need threat hunting

The definition of insanity is doing the same thing over and over and expecting a different result. Many organizations may work in this insanity pattern because they continue to use passive intrusion detection, which clearly isn't working (hence, the word *passive*).

REMEMBER

Attackers' initial objectives generally include stealing valid login credentials that they can use to perpetrate their attack. With valid credentials, attackers are virtually insiders that can blend their malicious actions with the normal activities of the organizations' networks, systems, and applications. But, unlike the personnel whose login credentials they've stolen, attackers use these credentials to carry out search-and-steal (or search-and-destroy) missions, using tools and techniques that end users don't use. These are the anomalies that threat hunters should be *actively* looking for.

Instead of passive intrusion detection, you need threat hunting for the following reasons:

- **Malware stealth:** Passive intrusion detection doesn't work because of the stealthy techniques used by cybercriminal organizations and the malware they produce. Today's malware can easily evade antivirus software through evasion techniques that enable it to change its colors like a chameleon.
- **Evolving attack vectors:** Attackers are innovating at a furious rate, which results in new forms of attack being developed regularly.

- **Dwell time:** You can't afford to wait weeks or months to learn about incidents. From the moment of intrusion, the cost, damage, and impact from a breach grow by the hour. The average time to detection of 287 days is no longer acceptable.

Your stakeholders will want to know what your organization is doing to seek out and detect the advanced attacks, with a skilled human being on the other side. Threat hunting is one of the answers.

REMEMBER

Threat hunting is becoming a part of infosec table stakes: the essential tools and practices that all organizations require. Threat hunting will soon be a part of the information protection that customers, regulators, and the legal system expect.

Identifying the Tools and Techniques

Threat hunting is a combination of tools and techniques. Tools provide highly detailed information across endpoints; how these tools are used constitutes the techniques that separate the beginner from the master threat hunter. Check out Chapter 4 for more on becoming a master hunter.

Coexistence

Passive incident detection and threat hunting can and should coexist. Organizations shouldn't rely solely on threat hunting for their detection. Automated systems such as IPSs, intrusion detection systems (IDSs), data loss prevention (DLP) systems, firewalls, and web filters are still needed because of their capability to detect (and sometimes block) malicious activity.

Humans and machines

Modern cybercrime is perpetrated by combining evolved technologies with the skills and intuition of a human attacker. Threat hunting is the unification of human and machine that enables defenders to fight back. Humans and technology need to form hunt teams, like an elite U.S. Navy SEALS team or a tiger team. In war, your elite forces lead and provide intelligence that helps other teams make decisions to prevent actions and respond faster.

Details and the big picture

Threat hunting means simultaneously looking at the big picture and at the details. This process is carried out with tools that perform detailed queries about specific activities taking place across hundreds or thousands of endpoint systems.

Some people think threat hunting is just setting up and getting alerts from an IDS or an endpoint detection and response (EDR) solution. This is *not* threat hunting. Setting up EDR solutions to look for a specific behavior can be an outcome or the postmortem *after* a hunt so you never hunt for the same thing twice, but you have to get dirty with the data you collect. This means digging into detailed data with the knowledge of what's normal and abnormal in the environment. This is how evil activity is tracked down.

Intruders and signs of intrusion

Threat hunting isn't necessarily about finding the intruders themselves. It's about looking for evidence of their activities. This isn't necessarily looking for bad, but *signs* of bad — like looking for the getaway car versus the thief with the big bag of money.

UNDERSTANDING THE UNIFIED KILL CHAIN

The National Institute of Standards and Technology (NIST) created the Cybersecurity Framework (CSF) to provide organizations guidance on how to establish a mature cybersecurity strategy capable of assessing, improving, and delivering on key security metrics. It's often recognized as a security best practice, offering a functional starting place that your organization can use to build and measure your cybersecurity strategy in alignment with compliance and regulatory standards.

Specific to threat hunting, your security operations centers (SOCs) can use the unified kill chain laid out by NIST CSF and other frameworks (for example, the MITRE ATT&CK framework) to understand the methodology used by intruders throughout an attack's life cycle. This will help you effectively identify evidence of an attacker at any point in their attack campaign, so you can take steps to defend your networks.

The phases of the NIST CSF's cyberattack life cycle include the following:

1. **Do reconnaissance.**

   The attacker selects a target, researches it, and tries to identify vulnerabilities they can potentially exploit.

2. **Weaponize.**

   The attacker selects or develops an exploit (such as malware) that they intend to use on the target system or network.

3. **Deliver.**

   The attacker delivers the exploit to the target system or network.

4. **Exploit.**

   The delivered exploit (code) is triggered and executed on the target system or network.

5. **Install.**

   The attacker installs remote access software that provides a presence and allows them to control the target system or network.

6. **Command and control.**

   The attacker uses remote access mechanisms to establish a C2 channel with the compromised system or network.

7. **Act on objectives.**

   The attacker uses this foothold to carry out the overall objectives of their attack, which could be stealing information, destroying information, disrupting systems or networks, or moving laterally to infect other targets and launch other attacks.

Data exploration

A threat hunter is a data explorer. Hunters follow their instincts and are patient but act with urgency in the chase.

Computing and the business

A threat hunter understands computing at a detailed level. They understand operating system internals and the detailed workings of applications and tools. For instance, a threat hunting team may be seeking signs of intrusions, but to do so effectively, it must understand how its business applications work and how its personnel uses them.

WHAT THREAT HUNTING IS *NOT*

Like many practices, the term *threat hunting* is ascribed to all sorts of activities. Threat hunting is the proactive pursuit of evidence of intrusions. Threat hunting is *not* any of the following:

- **Acquiring or analyzing threat intelligence:** This isn't threat hunting, but it can be a good starting point for a hunt.
- **Installing tools and waiting for alerts:** Installing a tool and waiting for it to alert isn't hunting, despite what vendors may claim. Threat hunting is humans finding bad actors by leveraging technology and data to analyze activity and artifacts.
- **Reporting on incidents or intrusions:** This is an after-the-fact activity; threat hunting is the pursuit of bad actors *before* incidents get out of hand.
- **Doing incident forensics:** It's important to know what happened in an incident, but incident forensics is about understanding what happened in the past, not what's taking place now or preventing future events.

Knowing the battlefield

Endpoints and networks are critical to threat hunting. They're the battleground of modern cyber wars. If you don't have endpoint and network visibility, it's hard to have a meaningful or conclusive hunt. The endpoint and network are where you find the tracks in the mud, holding the keys to the tactics attackers are using and the data and information they're after.

REMEMBER

Threat hunting isn't passive monitoring of events; it's the proactive pursuit of intruders and the evidence they leave behind.

IN THIS CHAPTER

- **Assembling your threat hunting team**
- **Acquiring and integrating threat hunting tools**
- **Discovering what normal is all about in your organization**

Chapter 2 Preparing to Hunt

You've decided to be proactive: Instead of sitting back passively and waiting for attackers to set off alarms, you're going to pursue them like a cheetah in the bush hunts for its next meal. You know the attackers are out there; they're trying to break in, and they may be succeeding. The challenge is to start hunting them to find the shreds of evidence they invariably leave behind. In this chapter, you discover what it takes to build a hunting team and start finding attackers.

People: Creating the Culture

Putting together a threat hunting team requires the right people, given the right time, training, and processes for success.

Building the team

The people on your threat hunting team should be knowledgeable about the internals of the operating systems (OSes) found in your endpoints. Most endpoints will likely run Microsoft Windows, but your team should also include experts in macOS, Linux, and Kubernetes (K8). Your threat hunters need to know how these OSes work at a detailed level, including the following:

- OS process tree structure
- Files used by the OS
- Registry used by the OS (Windows only)

In addition, your threat hunting team should be comfortable with basic networking concepts, including the type of network flows per application/service that can be expected. These include, but are not limited to:

- Microsoft Active Directory
  - Kerberos
  - Lightweight Directory Access Protocol (LDAP)
  - Network Basic Input/Output System (NetBIOS)
  - Server Message Block (SMB)
- Domain Name System (DNS)
  - Address (A)
  - Canonical name (CNAME)
  - Nonexistent domain name (NXDOMAIN)
  - Text (TXT)
- Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS)
  - GET method
  - PATCH method
  - POST method
  - Transport Layer Security (TLS)
- Secure Shell (SSH)
- Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol 3 (POP3)
  - Internet Message Access Protocol (IMAP)

This level of expertise is important because adversaries operate within these domains and make subtle changes to the OS or application. Threat hunters need to understand what to look for and what "normal" looks like so anomalies will be more apparent. They must understand what's normal at the business-application and human-activity level, because it's not just about packets on the network and processes in the OS.

REMEMBER

Anomalies are the primary sign that malware is lurking in endpoints or other network devices.

After you know what expertise is needed, you must figure out who has these expert skills and work on bringing them onto the threat hunting team. Depending on the size of the organization, this team may be one person or an entire crew, and wherever you get them from, you'll need to figure out how to reallocate roles and responsibilities, so you don't leave other teams shorthanded. For instance, you might identify one or more talented systems engineers or analysts from your security operations center (SOC). This team is usually known for passively monitoring security events.

Making time to threat hunt

Unless you have an unlimited budget to build your threat hunting team, you probably need to carve out time from the work schedules of existing staff for threat hunting. Depending on how large or small your organization is, the number of hours a week you need to spend in actual threat hunting may vary. In part, it depends a lot on your security posture and your risk tolerance.

TIP

Start by dedicating two to four hours a week to hunting. When you see results from your hunts, adjust as needed. The important thing is getting results from your hunts and tweaking existing tools to maximize return on investment (ROI). It's all about allocating time and committing yourself to results.

Training

Your threat hunters need to have passion! They *must* think like predators and have a hunger to hunt adversaries. After that important characteristic comes other trained skills such as:

- **OS internals:** This skill is critical for threat hunters. They need to understand not only the rules and practices of process management but also the file system operation and network communication in each OS in use.
- **Endpoint application behavior:** Your threat hunters must understand how any locally used applications function on your endpoints.
- **Network application behavior:** It's important for your threat hunters to identify abnormal network activity and question it.

- **Threat hunting tools:** Your threat hunters must be able to use the tools at their disposal, so they can hunt effectively.
- **Incident response procedures:** Your threat hunters need to know what steps to take when they discover signs of intrusion and how to preserve that evidence for potential future legal proceedings.

REMEMBER

It's not enough to equip your threat hunters with the skills and tools to find their prey; they also need to know what to do when they catch them.

Putting processes in place

Threat hunting needs to be a structured, long-term effort. But first, there must be a vision for what threat hunting is about in an organization and how it works with other IT security processes including the following:

- **Establish endpoint baselines.** Continuously hone your threat hunters' knowledge of what constitutes "normal" in your endpoints, so anomalies can be recognized more quickly.
- **Identify network baselines.** Equip your threat hunters with tools that support the identification of abnormal network behavior in comparison to an established "normal" baseline.
- **Improve hunting tools, practices, and skills.** Identify ways to make hunts better over time, and enable new threat hunters to learn from the seasoned warriors on your team. This is partly about tribal knowledge, but you also need to maintain knowledge base, so each new threat hunter can stand on the shoulders of their predecessors.
- **Improve response.** Identify ways to respond to threats with containment and remediation more quickly and accurately.
- **Improve skills.** Your threat hunters need to improve their skills and knowledge, and not just from on-the-job-experience. Offer continuing education on ethical hacking, system and network internals, and incident response.
- **Automate.** Provide systems and tools to automate the hunt where possible, so you can scale without necessarily increasing your headcount.

REMEMBER

Threat hunters must understand what's "normal" in *your* organization so they can quickly identify anomalies that may be signs of intrusions. The local context that humans have makes all the difference in detection.

Technology: Putting the Necessary Tools in Place

Threat hunting isn't just done with people or machines. Without the right tools in place, your threat hunters are going on a safari with nothing. Without threat hunting tools, there's no hunt.

Achieving complete endpoint visibility

Endpoints are today's battleground where intrusions into enterprises begin. Endpoints are the attackers' crown jewels, and they use them to gain entry into your environment. Although the data that attackers are looking for lives on servers, access to servers starts with endpoints.

Endpoint visibility is the ability to capture, in detail, the activities going on inside of *every* endpoint. If your organization allows bring your own device (BYOD), you have to achieve this visibility on all the devices, apps, and users.

Information about every process, including its parents and children, should be included, as well as every file that's created, read, written, and removed, and any corresponding network activity. This information must be available to be queried across the entire organization, so your threat hunters can quickly understand what anomalous activity is going on at any place and time.

Another very important aspect of endpoint visibility is *retrospection.* This is the ability to hunt back in time. For example, you should be able to mine the data for suspicious activity that took place not just yesterday, but last week, last month, and maybe even earlier.

TIP

VMware Security uses Carbon Black Endpoint Detection and Response (EDR) to provide the endpoint visibility that enterprises need for effective threat hunting. This tool helps you understand in detail what's going on in endpoint systems, including malware attacks.

REMEMBER

Complete visibility is needed for all networks and endpoints. Otherwise, attackers will be able to target unprotected network assets and endpoints to get into your environment without notice.

Achieving complete network visibility

Visibility at the network level is key to identifying potentially malicious activity. This can include how traffic flows through your environment and who (or what) is connecting to different networked resources. Baselines can help threat hunters uncover abnormal activity such as risky unauthorized access, lateral movement, and command-and-control (C2) traffic, indicative of an attacker operating in your environment.

Intrusion detection systems (IDSs), intrusion prevention systems (IPSs), network traffic analysis, network sandboxing, web filtering, firewall logs, and passive DNS tools are all good sources for obtaining this vital network data. To get a complete picture of the threats your organization is facing, your threat hunters must analyze the data from these tools to understand what's going on in the network and correlate it to suspicious endpoint data.

Gathering threat intelligence

Threat intelligence feeds inform your threat hunters of the new tools and techniques that attackers are using against other organizations, as well as the domains and Internet Protocol (IP) ranges they may be using. Threat intel feeds are often high volume and are delivered in structured formats such as Structured Threat Information Expression (STIX), Open Indicators of Compromise (OpenIOC), and Cyber Observable Expression (CybOX), all designed to be fed into your security information and event management (SIEM) system or other threat management platform.

TIP

The bigger your net, the greater your chances of catching an attacker. The VMware Threat Analysis Unit casts its nets far and wide, analyzing terabytes of data, millions of artifacts, and billions of events, to uncover threats as they emerge, so threat hunters can catch attackers in their environment.

TIP

NSX Network Detection and Response (NDR) provides indicators of compromise (IOCs) based on encounters within the network. Plus, it consumes IOCs from VMware's global network threat feeds to maximize the attack activity it can uncover.

Integrating your information

REMEMBER

Threat hunting is a human activity. A high volume of information is probably available in your environment about threats and activities, but it takes a human to find the meaning in it. To make the most of this information, your team must understand the tools and look for ways to integrate them.

One great example is the fusion of EDR/NDR data, SIEM data, and threat intel feeds. By themselves, each is useful, but when fused together, they're far more valuable. For instance, threat intel feeds often use STIX, Trusted Automated Exchange of Intelligence Information (TAXII), or CybOX for structuring this data. Application programming interfaces (APIs) for these are available so you can consume this data and get it into your other systems.

Furthermore, having integration with the MITRE ATT&CK framework will enrich the quality of the data and streamline your response activities. This also helps SOC analysts to speak the same language during the threat hunting process.

Using data correlation and analytics tools

Because threat and event data come in from many different places, you must be able to analyze and correlate events to make sense of what's going on in your environment. The tool of choice is SIEM.

SIEM systems are made for event correlation and analytics, and they do a pretty good job. Organizations often use them as a central repository for log and event data from network devices, firewalls, OSes, and applications. SIEM is often the storage for everything going on in the environment, together with the ability to make sense of it.

TIP

Using NSX NDR can help because it focuses on threat campaigns rather than just isolated anomalous events. VMware's AI-based correlation engine generates high-fidelity, highly accurate alerts that provide authoritative context to speed up forensics. This enables SOC teams to focus their attention on a small subset of relevant events instead of digging through thousands of anomalies.

NSX NDR automatically enriches threat data with MITRE tactics and techniques.

People and Technology: Knowing Your Environment

Successful threat hunters need to know as much about your environment as possible to better sense what's normal and abnormal. As they proceed in their threat hunts, they develop an unmatched intimate familiarity with your environment.

Differentiating between normal and abnormal

The key to threat hunting is knowing what's normal so that anything abnormal will stand out and be noticed. Because of this, threat hunters spend a good part of their time observing and becoming familiar with normal, routine events in their environments.

However, threat hunting takes more than just observation. Threat hunters also need to be familiar with their organization's architecture: networks, systems, tools, and applications. They need to understand that architecture independently of their threat hunting, because anything they might observe in their environment may or may not be normal in the first place.

WARNING

Occasionally, threat hunters discover things that aren't necessarily security incidents, but insiders exercising poor judgment.

Knowing your high-value targets

In goal-oriented sports, teams defend goals against the opposing team and try to prevent them from scoring. In threat hunting, threat hunters need to identify the "goals" — in other words, the *high-value targets* (HVTs), both the ones that are likely to be attacked and the ones that are less so. They also need to understand *how* attackers might go about attacking them. Depending on the attackers and their objectives, HVTs could be information, like customer or employee data, or critical assets, such as public-facing web servers.

Anticipating how you'll be attacked

Just as a cheetah anticipates the next move of its prey, threat hunters need to know how attackers are likely to try to get into their environments using IOCs. This is part gut feel and part knowing your environment:

- **Architecture:** Attackers will try to discover the weak spots in your organization's architecture and data flows. This helps them discover whatever valuable data they're looking for and how to get it out unnoticed.
- **Security posture:** Attackers will attack your organization's weak spots. They discover them through simple techniques like port scanning to find unpatched and vulnerable systems. Consequently, your threat hunters need to know where the organization's weak spots are because attackers are going to find them and exploit them.
- **People:** The security culture of your organization is a great indicator of vulnerability. Attackers might not have ready access to security awareness training or other aspects of your organization's security awareness program, but attackers will be able to gauge how easy it is to lure your employees into clever social engineering, phishing, and spear-phishing campaigns, whether they're purely online or on-site.
- **Threat intel:** Understanding how attackers are going after other organizations gives your threat hunters a better idea of how they may go after yours. They'll get creative and be unpredictable at times, but attackers are people, too — creatures of habit and apt to use tools and techniques they're used to and that have worked for them in the past. Because organizations tend to protect themselves in similar ways, attackers are likely to attack in similar ways.

One of the best ways to test your theories about what attackers may try to do and how well your defenses will hold up against those tactics, techniques, and procedures (TTPs) is to use breach and attack simulation (BAS). A BAS mimics real attack activity, running complex attack scenarios to enable you to see what an attacker can get away with within your environment. This helps threat hunting teams look for and shut down similar activity across your network and endpoints, as well as uncover potential gaps and weaknesses that need to be addressed.

REMEMBER

Your threat hunters need to know your environment inside and out. How does everything work? Where are the gaps and weak spots, and where are the risks? They need to think like attackers so they can better anticipate their threats and stop attacks early.

TIP

Open frameworks such as MITRE ATT&CK can help out here. You can leverage TTPs associated with advanced persistent threat (APT) groups who may pose a specific threat to your industry vertical, and hunt for evidence that your organization is being targeted.

IN THIS CHAPTER

- **Getting inside the thought process of a threat hunter**
- **Setting up for a hunt**
- **Understanding the Hunt Chain**

Chapter 3 The Hunt

After you've assembled and trained your threat hunting team and acquired the tools they need, it's time to send them out hunting. This chapter explores the thought processes that prepare a threat hunter for a successful hunt, as well as a proven methodology for threat hunting called the *Hunt Chain.* Created by VMware Security, the Hunt Chain methodology provides a framework for the entire threat hunting process.

Understanding the Mentality of the Hunt

A threat hunter knows how systems work, how attackers think and act, and how to use tools to find and go after them. They take it as a personal challenge and point of pride to unearth attack activity and root out attackers who may be hiding in your environment. Your organization has its weak spots — every company does. That may give cybercriminals an easy way in, but it doesn't give them the right to be there. Threat hunters know best where attackers will strike, and they're ready and waiting for them.

Your threat hunters will

- Proactively uncover security incidents and evidence of attack activity within your environment.

- Improve the speed of your threat response by identifying the specific attack tactics, techniques, and procedures (TTPs) attackers used, so effective remediation actions can be taken.
- Reduce investigation time by providing insights into the scope of the attack — identifying the expanse and reach of the attack activity.
- Provide vital knowledge on all your endpoints and networks, reducing the unknown and filling in critical details (for example, how data flows and how endpoints are used) that can be used to uncover weaknesses, predict where attackers will target, and bolster defenses.
- Improve overall security operations center (SOC) efficiency, helping focus efforts and resources on the activities that matter most.
- Minimize damage and overall risk to the organization by actively identifying threats.

Week in and week out, threat hunters add to their knowledge, skills, and tools. With the right resources, each new query becomes another automatic threat detector, so the hunter slowly gains ground and denies attackers access to more and more of your organization's attack surface. That way, a threat hunter needs to never hunt for the same thing twice. Instead, they can continue to evolve to combat the new and innovative ways attackers will target your organization.

Constantly reading and learning about new exploits, threat hunters will test out new hunches and see whether attackers are trying these new techniques (using breach and attack simulation [BAS] and other tools) to make sure they can be ready.

Planning for the Hunt

For the first few weeks of threat hunting, a threat hunter becomes oriented to the environment and masters the tools used and how they're configured. Soon it will be time for the threat hunter to venture out on individual campaigns — probing deeper and further than before.

The overall practice of threat hunting is continuous, but it's broken up into individual missions called *hunts.* A hunt can last a few hours to several days — it depends on the objectives of the particular hunt. A hunt should have one or more objectives — narrowly focused at times, but not too broad either (or it might not ever really get completed). Some example hunt objectives include the following:

- **Hunting for specific threats:** A threat hunter may have read about some specific new threat, such as Hermetic malware, and will look broadly in the environment for signs of it.
- **Hunting for attacks against specific vulnerabilities:** A threat hunter dives into high-value systems with one or more known unpatched vulnerabilities to see whether attackers are trying to exploit them.
- **Hunting for attacks against specific high-value targets (HVTs):** Here, the threat hunter dives deeply into the operation of a specific asset (or a small number of them), learning more about how it operates and looking for signs of reconnaissance or intrusion.
- **Hunting for advanced persistent threat (APT) group behavior:** Here the hunter focuses on specific ATP group behaviors as defined by MITRE, to identify activities that be associated with a known ATP group.

Threat hunters generally concentrate their attention on endpoints and networks with tools such as Carbon Black Endpoint Detection and Response (EDR) and NSX Network Detection and Response (NDR), which provide detailed forensic data. Depending on the hunt's objective, the threat hunter may try to triangulate attack evidence using additional tools that can corroborate or provide incremental signs of compromise, such as an intrusion detection system (IDS) or intrusion prevention system (IPS), web proxy filter, or network firewall.

REMEMBER

Threat hunting is not only about detecting malware but also about the abnormal usage of legitimate tools (such as PowerShell and Enhanced Mitigation Experience Toolkit [EMET]) and accounts.

TIP

Keep notes on your threat hunting experiences. Over a long period of time, hunts may all become a blur, but with good records, you can go back and familiarize yourself with past hunts. These records might be highly structured and include hunt objectives, logs, traffic, activities searched for, and analytics. Or they might be more like a narrative describing a hunt. I like the hybrid approach — a combination of both. In the future, if you embark on a similar hunt, you could peruse your records and use them as a springboard.

Outlining the Hunt Chain

VMware Security has developed a methodology called the Hunt Chain, which is a series of activities that constitutes a formal threat hunt. The overall chain is depicted in Figure 3-1. The following sections explain what you see in this diagram.

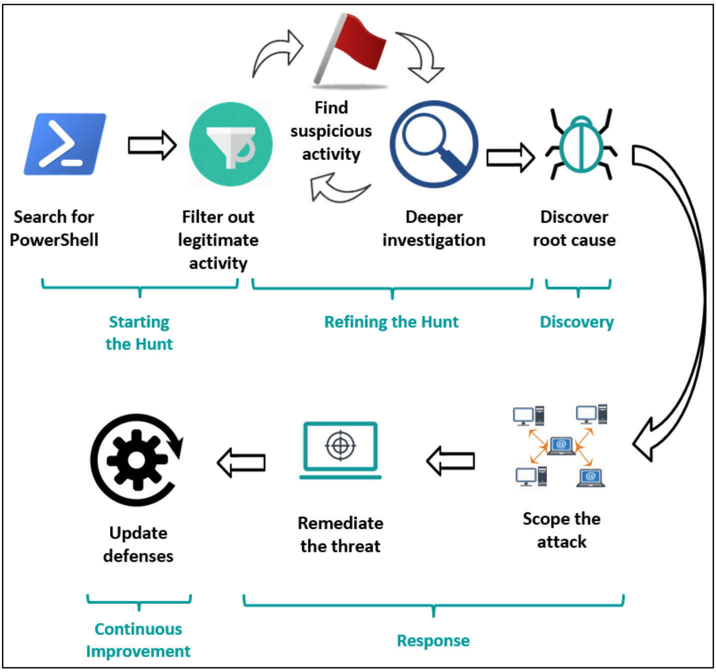

FIGURE 3-1: The VMware Security Hunt Chain.

Where and how to start

A threat hunt starts with the collection of data directly or indirectly related to its objective. When developing an objective, the threat hunter needs to know what data will be mined to achieve the hunt's objective. Typically, this data will include both endpoint and network information to ensure the hunt is comprehensive when complete. VMware's NDR is constantly gathering data from the networks it protects, which can help guide the hunt's starting point by focusing efforts on network anomalies already found by machine learning (ML)–based data analytics.

TIP

Define the objectives and scope of a hunt *before* the hunt begins. This will help you quantify success and know when the hunt is completed. Without clear objectives, a hunt is more of a fishing trip that could go on and on.

Focusing on network anomalies, such as the use of outdated or unusual protocols in the context of your network, is a good starting point for a hunt. It's also helpful to pay attention to potential "policy violation" activity, such as the use of The Onion Router (Tor), Domain Name System (DNS) over Hypertext Transfer Protocol Secure (HTTPS), or BitTorrent activity.

Filtering out legitimate activity

As threat hunters begin observing the target environment, they begin observing activities. By using their knowledge about the operating system (OS) and application(s) that are in your environment by design, they can begin to filter out legitimate activity and expose anomalous activity to investigate. One by one, as activities are explained, anything that remains is potentially due to attackers and their actions.

Hunt for suspicious activity

After legitimate activity is filtered out, threat hunters will look at everything that remains to determine whether it's suspicious. For example, if your organization utilizes PowerShell as a part of your endpoint management tools, a threat hunter could use this knowledge to filter out all its legitimate uses and investigate anything that remains. The hunter will look to determine if there are additional legitimate use cases or if the use of PowerShell is part of an attack.

From a network perspective, hunters could look at connection volumetry to identify anomalies that could be indicative of a threat. For instance, spikes to an Amazon S3 bucket could indicate a previously unknown network backup or a data exfiltration attempt. Until the hunter verifies precisely what it is, it should be treated as an unexplained data exfiltration that poses a risk to your environment. In the same vein, the presence of unusual account enumeration activities or a failed Kerberos authentication could indicate that credentials have been compromised or might simply represent a cached set of invalid credentials. It's important to note that threat hunts don't always turn up activity indicating intrusion; nonetheless, threat hunters must identify any anomalies and then investigate them to determine whether they are legitimate or represent a real risk.

TECHNICAL STUFF

PowerShell is a command-line shell and scripting language. It could be likened to a new and improved version of command line and batch files.

Deeper investigation

Any activity that remains unexplained must be investigated. During the investigation, threat hunters may need to solicit help from experts in your organization on the OS, applications, data flows, use cases, or other aspects of the anomalous activity. Sometimes the investigation will discover aspects of legitimate activities that were previously unknown; other times it will discover aspects of an environment that represent the improper implementation of a system.

For example, a threat hunter may find persistent temp files that contain credit card numbers that were supposed to be encrypted but weren't. This could be considered an artifact of an attacker scraping credit card numbers out of an application or a simple misconfiguration. A deeper investigation is needed to determine which it is.

Another example would be the identification of Remote Desktop Protocol (RDP) sessions using the legacy Microsoft Train Simulator (MSTS) hash cookie authentication. This could be attack activity, but it could also be a legitimate but legacy interaction. Only by inspecting the metadata within the connection (such as usernames and RDP session environmental settings) can the threat hunter tell whether the activity is a risk. They may also need to look at what other network or OS activities can be found in relation to the host and what workload was posted and what happened prior to the anomalous encounter. This portion of the Hunt Chain is iterative: As threat hunters investigate anomalies, they filter out legitimate activities and then resume hunting for illegitimate activities.

Scope the impact

When anomalous activity is observed and confirmed to be an attack, the threat hunter continues to investigate to see where and how the attack originated and proceeded. This is essentially a root cause analysis. Depending on the attack, it may narrow into an initial intrusion, but it may also branch out into an investigation that could indicate a broader attack on more systems.

Remediate

After the total extent of an attack is known, the threat hunter contributes to the remediation effort, often joined by appropriate colleagues such as systems engineers, network engineers, security engineers, software developers, and maybe others. The specific activities vary depending on the nature of the attack, but the general objectives are to:

- Remove malware and restore all altered and removed files to their original state.
- Update configurations, permissions, and software versions to prevent a similar attack in the future.
- Apply security patches or other mitigation measures to prevent similar attacks.

Update defenses

The organization must update its defenses to ensure that similar attacks are blocked, or at least require greater effort on the part of attackers. Updating includes automating systems to look for (and potentially address) what your threat hunters found. The range of activities may include

- Creating new or updated firewall and/or IPS rules
- Generating new or updated alerts within your security incident and event management (SIEM) system
- Improving incident response procedures

- Applying updates to your infrastructure, application, or security architecture
- Making changes to your application development, testing, quality assurance (QA), or quality control (QC) tools and processes
- Creating new alerting rules in your EDR, NDR, or similar tools

The investment in threat hunting tools and personnel is mostly wasted if there isn’t a feedback loop incorporated that turns lessons learned into better defenses. A threat hunt doesn’t find just outside attackers, but also insider threats. A traitor is every bit as much of an enemy as an outside adversary. The goal is to put into action what the threat hunt turned up to improve your security and reduce your risks.

TIP

The results of a threat hunt will give a threat hunter a lot of ideas for future hunts. If you’re fishing in a pond and you find a hot spot where fish are biting, you’re going to go back to that spot next time.

IN THIS CHAPTER

- Strengthening your organization's overall posture
- Embedding yourself in the environment
- Designing better hunting techniques through research
- Honing your hunter intuition
- Engineering your own tools and custom integrations
- Laying traps for attackers
- Learning more through training

Chapter 4 Becoming a Master Hunter

After you've been threat hunting in an environment for six months, a year, or more, you're going to become a senior in most circles. You're expanding your skills and knowledge, you're building and using tools, and you've begun to mentor others. You're becoming a master threat hunter. Or you *want* to be. Read on to discover how to grow your expertise so you can get there.

Raising the Bar

As a master threat hunter, your hunt findings strengthen your organization's overall posture. How? Here are some examples:

- **Improved defenses:** As you chase down intruders and deny their return, you're closing down one vulnerability after another. Over time, this begins to severely limit the available techniques that can be used for successful intrusions.

- **More detection:** You've updated your defenses based on what you've learned from previous incidents. Each time you catch an intruder, you're able to catalogue these new attack vectors to immediately gain visibility into subsequent attempts.
- **Infrastructure familiarity:** As you've been chasing intruders all over your organization's environment, you've become intimately familiar with it — perhaps more so than its own designers and engineers. As an expert in defense, you've been able to impart several useful suggestions to tighten things up from an architectural perspective. You also understand where the organization may be weak in detection or response capabilities and can offer suggestions for additional tools that could enable a better overall defense.
- **Better instincts:** As you gain experience threat hunting in your environment, you begin to build an instinct for noticing abnormal activity and predicting how the next intruders might attempt to strike. And you'll be there to catch them when they do.

This continuous improvement is partly about your organization and its improved defenses, and the rest is about your growing prowess as a black belt threat hunter.

REMEMBER

Achieving master threat hunter status doesn't signify *arrival.* Instead, it represents your outlook and your discipline. You know the enemies and how they work, and you're determined to always be learning so that you can be one step ahead of them and anticipate their next moves. It requires constant vigilance and focus.

Becoming Embedded in the Environment

With the hunting tools at your disposal and your ability to look deeply into any server or endpoint in the organization, you're certainly embedded in the technical environment. The focus here should be on how you work with others in the organization. Although threat hunting can *sometimes* be depicted as the activities of a solitary threat hunter surrounded by the cool glow of monitors, long hours after dark hunting for evil, a threat hunter is more often than not a collaborator, known across IT and involved in its many varied teams.

That's right: You need to work with teams across *all* of IT and DevOps as they discuss the business of the day and their current projects. To defend your organization's environment, you must work closely with these teams as they build and run the IT environment. Mainly this is because you need to:

- **Understand what they built.** As you observe system operation, interaction, and data movement, you must work with people who understand how systems were designed, built, and implemented. This knowledge helps you better distinguish anomalies from legitimate operations.
- **Understand what they're building.** Given that most IT environments grow organically, you must be involved in this change. As you work with teams in IT and build trust with them, they'll tell you more about their projects — the new things they're building.

  There are two reasons you need to be involved:

  - You need to understand how their new systems work, so your understanding of what's normal is accurate.
  - You may need to advise them to make design enhancements based on your knowledge of the current threats and adversaries facing the organization today, so those new systems will be more secure by design. What a concept, right?

REMEMBER

Your relationships with the teams in IT serve you well. As you work with these teams over months and years, your role as a subject matter expert will foster trust, and these teams will rely on you to provide them with accurate and reasonable guidance for improving the environment's defenses. They'll be more apt to take your advice and incorporate more and better security practices into the new projects they're working on. And this is why you're there — to help everyone in IT build and administer systems and networks that have better defenses.

Performing Research

One of the keys to being a master threat hunter is your insatiable desire to learn more. You want to know about the newest exploit or that latest tool. As you dive into this field, the more you know, the more you want to learn, so you do some of your own research. You need to run your own experiments to see how things work, so you build your own lab environments and test ranges. This process can include probing the malware you've captured to play with an exploit kit you found or reviewing experimental changes in systems to make them more resistant to attacks.

You might also be building newer and more complex queries with your threat hunting toolsets and trying to see if there are any new "hits" against a data set containing a new batch of attack vectors. You might not have a crystal ball, but as you gain experience, you'll constantly be thinking of new ways that intruders can try to penetrate your environment — and how you can stop them.

Pragmatically, your research helps you design better hunting techniques to validate your suspicions. You know where the weak points are, and it's up to you to discover new ways to watch them. These methods include new traps, new triggers, and new filters that you can use to tighten down your environment a bit more. And sometimes, on that very rare occasion, your research might even lead to your discovering that rare holy grail of all vulnerabilities: a previously unknown zero-day. It's at times like this when all the late nights of wrestling with your environment and trying to probe it for security weaknesses pay off. That feeling of elation and satisfaction that you've found a vulnerability that no one else has ever thought of before is the greatest rush!

Developing Intuition

A master threat hunter develops a sixth sense when it comes to the hunt: After enough time, they see attack patterns emerge out of a collection of seemingly unrelated data points. They begin to recognize reconnaissance and the intended activities behind the exploit and dropper tools that adversaries are using. At times, this can even lead to the threat hunter being able to predict what intruders might do next so they can be stopped.

Another perspective on intuition is this: The threat hunter can also put themselves in the shoes of the attacker, see the environment as a potential target, and anticipate their next move. Thinking like an attacker separates the master threat hunters from the rest.

Educated hunches

Threat hunting isn't just about taking blind leaps; it's also about making educated hunches — educated perhaps by new pieces of intelligence that showed up in a threat feed or something you recently read about, like a new exploit in the wild. You can follow leads in other ways, as well, which include reviewing indicators from monitoring tools like an intrusion prevention system (IPS) that can alert personnel to traffic and discovering low-reputation Internet Protocol (IP) addresses or endpoint antimalware sandboxes firing off notifications about an application pivoting in a way that it shouldn't.

OODA

Intuition is also about OODA: Observe, orient, decide, act. This is the military's way of responding to situations in combat operations. You're a threat hunter; you're in combat as well — on the cyber battlefield. An example of OODA applied would go something like this:

1. **Observe.** Collect data from sensors on your endpoints and events in the network.
2. **Orient.** Discern what this data means in context. How does this information relate to other information and what could it mean? Could command-and-control (C2) traffic be occurring, or could one of your endpoints be under attack from a ransomware variant?
3. **Decide.** After you have a clear picture of an incident, the next step is to determine a course of action. Typically, this is the containment phase in which your incident response strategy will kick in. Only after the breach has been scoped should you proceed to the eradication and subsequent recovery and feedback stages to prevent similar intrusions from recurring.
4. **Act.** Execute the plan to shut down the intrusion, harden the organization's security posture, and enhance detection. Repeat.

Many times your hunts may return "empty," and no intrusion will be discovered that leverages that particular vulnerability, but the knowledge created is incredibly valuable. You now have a series of processes and detection mechanisms that serve to harden your organization against future potential incursions.

Strong opinions, loosely held

One way to grow in knowledge about the systems and data in an environment is to mentally build a model representing how they work and interact together. The same principle holds true as you learn how an attacker might attack an organization: You can study and develop models that represent how these actors operate.

As you continue to develop your security acumen, you may notice a tendency to stand inordinately firm in certain beliefs and opinions, like "Operating systems *always* open files like this" or "Intruders would *never* attack this program."

The mental models in your subconscious are what help you understand complex topics and navigate them with ease. However, although these constructs can be helpful to simplify certain concepts, you must never become too entrenched in a certain way of thinking because you blind yourself to new ways of thinking. This case holds doubly true in the security field where, especially with new technology, the only constant is change. You must be open to changing your understanding about things when new information comes in. This is known as *strong opinions, loosely held,* which is the safety valve that helps you recognize new facts that may change the way you think about things — like how operating systems and applications do what they do and how attackers do what they do.

WARNING

If you cling to your time-honored beliefs too tightly, your hunts may suffer and not only might you return with no prey, but you could also *become* the prey.

Developing Your Own Tools and Custom Integrations

Master threat hunters don't just rely on the tools and interfaces handed to them by vendors. Instead, they view these resources as a starting point and work to engineer ways to extend and correlate the data and capabilities of these tools to build a system in which the whole is greater than the sum of its parts:

- **Custom data collection scripts and analyst tools:** Master threat hunters may, from time to time, need to write their own scripts to collect or analyze data. One example of this could be writing a simple Windows Management Instrumentation (WMI) script to collect various instances of persistence in the Windows Registry. Another could be building a Python utility to generate analytics on a set of metrics to discover anomalous data points. Typically, master threat hunters are no strangers to leveraging powerful instruments like pivot tables and regular expressions to twist collections of data for a specific purpose.

- **Custom integrations:** The environment may have a lot of tools, many of which may have application programming interfaces (APIs) or interfaces that you can use to acquire or distribute information. For instance, a trigger in an endpoint detection tool could activate the creation of a new IPS or firewall rule used to block a particular network connection. Or, information from a threat feed could be filtered and fed into a tool to update its own rules that could then action a ticket over to the help desk or even isolate a system on the network.

Master hunters aren't just clever operators — they're also builders. Often, they act as both the problem finder and the problem solver. They must be able to understand not only how new attacks work but also how to "stitch together" the various pieces of information available in the environment to enhance visibility and defenses.

Setting Land Mines

A master threat hunter thinks ahead and anticipates what a known or a potential adversary might do. In this scenario, hunters can set land mines for attackers. These methods attempt to attract attackers so that an alarm can be raised to alert security that illegitimate activity may be occurring in the environment.

When using incident detection and response tools, this means setting up queries for events that *might* happen. Again, this is where it's critical to fuel your passion to learn about new, clever attack vectors. As you continue to develop your mental cyber armory, you'll learn how to probe sections of the environment where you previously didn't have visibility.

In addition to your standard hunting tools, you can leverage other more advanced resources, such as *honeypots,* to lure malicious actors into attacking a decoy target loaded with intrusion detection monitoring sensors. Instead of housing legitimate data, a honeypot is built to impersonate critical assets while having extremely sensitive monitoring and alerting configured.

In certain organizations, you might even go one step further to create *honey accounts,* which contain one or more honeypots, set up user accounts that follow certain naming conventions for VIP users, and monitor for any access attempts (meanwhile, the VIP users are assigned other legitimate logins).

Taking the Threat Hunting Challenge

Threat hunting has emerged as an essential practice for organizations to proactively avert destructive attacks. As practitioners on the front lines of today's cyberwar, continuously testing and developing your organization's skills to protect from dangerous attacks is crucial. But attackers are frequently innovating past your defenses.

How can you hone your security skills and stay steps ahead of attackers?

VMware's Threat Hunting Challenge, which can be played virtually or in person, offers a unique method of gamified training that enables players to get hands-on experience in threat hunting with VMware Carbon Black Cloud. During the Challenge, you learn how to:

- Identify and detect processes making malicious outbound connections or unauthorized modifications in real time.
- Respond to attacks by stopping malicious processes, banning hashes, and isolating marginalized hosts.
- Detect future suspicious activity and receive early warning signs to move security procedures and policies forward.

Become a proactive threat hunter with the VMware Threat Hunting Challenge. You no longer have the luxury of waiting for threats to identify themselves — you need to hunt them down. For more information on threat hunting from the VMware Threat Analysis Unit, visit `https://blogs.vmware.com/security/threat-analysis-unit`.

IN THIS CHAPTER

- » Knowing your environment
- » Thinking like an attacker
- » Collaborating across IT
- » Identifying the latest attack trends
- » Keeping track of your hunts
- » Honing your security skills

Chapter 5
Ten Tips for Effective Threat Hunting

Given the dire consequences of failure, it's critical that your threat hunting program succeed. Organizations that start a threat hunting program have success in mind, but are they able to achieve it? The ten tips in this chapter will help your organization and its threat hunters be effective and successful.

Know Your Environment

The purpose of threat hunting is to discover abnormal activities that point directly to reconnaissance and attacks. To recognize activities that aren't normal, you must understand what *is* normal. You must become familiar with the architecture overall — and at a detailed level — in order to understand the vulnerabilities and weaknesses that attackers could target.

Understanding your environment involves deep and wide exploration of the technical environment: networks, systems, and applications. But it's more than that — it's also imperative that a threat hunter build relationships with key personnel inside and outside of IT.

Why build relationships? These people help threat hunters better understand normal activity versus anomalous activity. When a threat hunter finds a problem, it's not always an attacker; sometimes it's an unsafe practice. Without a trusting relationship between threat hunters and others, threat hunters can't be effective change agents to help the organization make key security improvements and keep its house in order.

TIP

You can find more information about knowing your environment and understanding what's normal in Chapter 2.

Think Like an Attacker

A threat hunter's mission is to quickly find signs of intrusion, so attacks can be stopped and their effects can be mitigated to minimize damage. But instead of adopting the mindset of always chasing attackers, better threat hunters anticipate their next move.

In a threat hunt, this process involves looking for things that attackers *might* do. With tools like Carbon Black Endpoint Detection and Response (EDR) and NSX Network Detection and Response (NDR), threat hunters can set up triggers that fire when an attacker does those things. This practice is also known as laying *tripwires,* which are triggers that a threat hunter sets up, anticipating an attacker's move, and alerting personnel if such a move is ever made.

TIP

For more information, check out Chapter 4.

Develop the OODA Mindset

Observe, orient, decide, act (OODA). This is how the military thinks about combat operations. Threat hunters are soldiers in today's cyberwars, so it makes sense to think about threat hunting in this way.

OODA is a mental discipline that keeps threat hunters from acting impulsively. In the cyberwar arena, acting before thinking can blunt a threat hunter's effectiveness.

TIP

Read more about OODA and its detailed steps in Chapter 4.

Devote Sufficient Resources to the Hunt

Threat hunting can be a great idea that goes sour if there aren't enough resources to properly carry it out. This includes both personnel and the tools and systems on which to run them. Here's a breakdown of what's needed:

- **Personnel:** One or more trained and/or experienced threat hunters. These individuals must have a deep understanding of the inner workings of operating systems, plus subsystems such as web servers, database management systems, and application servers. And perhaps most important of all, they must have a thorough and growing familiarity with the inner workings of the organization, as well as its applications, networks, and users.
- **Tools:** You don't go on a safari without appropriate equipment, and you can't do a threat hunt without threat hunting tools. This includes Carbon Black EDR and NSX NDR, which are installed on every endpoint and network and provide a step-by-step detailed forensic history of every activity. The real power of Carbon Black EDR and NSX NDR is their central querying capabilities, wherein a threat hunter can create and store queries, asking about whether certain detailed events have occurred anywhere in the environment.
- **Infrastructure:** Of course, threat hunting does require some systems resources. This includes management consoles, and it may also include a "test range" where advanced threat hunters can experiment with suspected malware in a safe environment. Here, hunters can hone their skills with "live fire" and also hone their hunting skills in production environments.

TIP

For more information on threat hunting resources, turn to Chapter 2.

Deploy Endpoint Intel across the Enterprise

In cyberwarfare, defenders must protect all endpoints all the time, but attackers only need to be successful one time. This principle underscores the urgent need for an organization to cover not just a subset of endpoints with advanced threat hunting tools, such as Carbon Black EDR, but all endpoints.

WARNING

Leaving some endpoints unguarded creates blind spots where organizations are unable to detect or remediate attacks. This is why it's so important for an organization to cover all endpoints.

Supplement Endpoint Intel with Network Intel

Endpoints are the hills on the cyberwarfare battleground. Endpoints are the principal focus of attacks, but they are by no means the only place to find information about intruders. In addition to endpoint tools, it's often useful to have network-centric visibility by using tools, such as

- Data loss prevention (DLP) systems
- Firewalls
- Intrusion detection systems (IDSs)
- Intrusion prevention systems (IPSs)
- Network traffic analysis (NTA)
- Web application firewalls (WAFs)

These tools provide a network-centric view of activities that may help a threat hunter corroborate attack patterns and activities. Collecting additional intel from the network and other sources is a part of the observe and orient parts of OODA (see "Develop the OODA Mindset," earlier in this chapter).

Collaborate across IT

Threat hunting isn't just about technology. The essential ingredient in threat hunting is having strategic relationships with key personnel in the IT organization. Better threat hunters work with systems engineers, network engineers, endpoint engineers, service desks, and application developers in different ways:

- **Understanding normal:** As threat hunters build their knowledge of environments, they're in dialogue with key IT personnel to hone their understanding of how systems and applications function.

- **Remediation of vulnerabilities:** While searching for intruders, threat hunters also encounter weaknesses in the design and implementation of applications, systems, and networks. Relationships built on trust enable threat hunters to convey the need to fix those weaknesses.
- **Remediation of incidents:** When threat hunters find signs of intrusion, they need to work with key IT personnel to correctly diagnose intrusions and remediate them effectively and completely with minimal impact.

TIP

The OODA methodology applies perfectly here. Using their relationships across IT, they collect information (observe), and work with others to understand it (orient), before acting on it (decide and action). For more information, turn to Chapter 4.

With relationships based on trust, IT personnel are more likely to cooperate with threat hunters to reduce risks in the organization.

TIP

Turn to Chapter 4 to learn more about working with IT and others in the business.

Keep Track of Your Hunts

Even a single threat hunt can have more details than most people can remember. But over time, when a single threat hunter has performed 10, 20, 30, or more threat hunts, the details quickly become a blur.

REMEMBER

For this reason, threat hunters should document each threat hunt. Better threat hunters include important high-level business information with each hunt — most notably, the *reason* for the hunt in the first place.

A detailed history of threat hunts helps a threat hunter better understand, at any level of detail, the ground that's already been covered, what's been looked at, and what's been overlooked. And although it's important to sometimes revisit old hunts (meaning repeating a prior threat hunt if the threat hunter suspects intrusions since last time), IT environments quickly change over time, potentially leading to new intrusions by using methods examined earlier.

Hone Your Security Skills

Cybersecurity innovation is occurring at a dizzying pace. Seasoned threat hunters know this and take time out from the hunt to evolve and hone their skills through:

- **Technical training:** The SANS Institute (`www.sans.org`) and other organizations provide high-quality technical training in attack and defense techniques.
- **Conferences:** Local gatherings such as BSides (`www.securitybsides.com`), as well as national and international conferences like RSA Conference (`www.rsaconference.com`), Black Hat (`www.blackhat.com`), and DEF CON (`https://defcon.org`), provide tremendous networking and education opportunities.
- **In-person and virtual training:** Visit a cyber range to advance your threat hunting skills. This is an excellent way to get invaluable hands-on experience in a simulated environment that will further equip you to discover and mitigate today's most advanced cyber threats. For a list of cyber ranges around the world, go to `https://cybersecurityventures.com/10-hot-cyber-range-companies-to-watch-in-2020`.

TIP

To find out more about training, turn to Chapter 4.

Be Aware of Attack Trends

Threat hunters can't exist on intellectual islands. They need to be continually aware of the techniques cybercriminal organizations use against other organizations. Only with this knowledge can a threat hunter anticipate attacks and be able to find them. Want to know more about this subject? Turn to Chapter 4.

REMEMBER

This book is a good "getting started" resource, but you can also find a lot of great training and resources online. Threat hunters can find valuable information on the VMware Security Blog at `https://blogs.vmware.com/security`.

Eliminate advanced threats that are hiding in your environment

This book introduces the advanced cybersecurity practice of threat hunting and its role in protecting your organization. You'll learn how threat hunting works, why it's an essential component in an organization's security program, and how you can master the discipline to improve your organization's security and advance your career. Because, in today's environment, if you rely only on passive, automated threat detection, you'll always be a step behind threat actors.

Inside…

- How to strengthen your organization's security posture
- How to develop invaluable security skills
- Ways to learn more through training
- Ten simple tips for more effective hunting
- Understand threat hunting

vmware®

The **VMware Threat Analysis Unit** comprises leading minds in cybersecurity research and analysis. 260+ cybersecurity research publications across three decades. 100+ threat researchers and 30+ data scientists with a PhD #1 and #2 most published cybersecurity researchers in academia. Winners of DEF CON Capture the Flag.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-88704-1
Not For Resale

9 781119 887041

for dummies®
A Wiley Brand