LEARNING MADE EASY

Carbon Black by Broadcom Special Edition

Threat Hunting

for dummies®
A Wiley Brand

Understand threat hunting

Develop your threat hunting skills

Gain the upper hand

Compliments of

Carbon Black. by Broadcom

Peter H. Gregory

Threat Hunting

Carbon Black by Broadcom Special Edition

by Peter H. Gregory

for dummies®
A Wiley Brand

Threat Hunting For Dummies®, Carbon Black by Broadcom Special Edition

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

ISBN 978-1-394- 34991-3 (pbk); ISBN 978-1-394- 34992-0 (ePDF);
ISBN 978-1-394- 34993-7 (ePub)

Publisher's Acknowledgments

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Managing Editor:
Sunanda Jayakumar

Client Account Manager:
Cynthia Tweed

Content Refinement Specialist:
Bharaneedharan Murthy

Table of Contents

Introduction

Adversaries, and cybercriminal organizations in particular, are building tools and using techniques that are becoming so difficult to detect that organizations are having a hard time knowing that intrusions are taking place. Passive techniques of watching for signs of intrusion are less and less effective. Environments are complicated, and no technology can find 100 percent of malicious activity, so humans have to "go on the hunt."

Threat hunting is the proactive technique that's focused on the pursuit of attacks and the evidence that attackers leave behind when they're conducting reconnaissance, attacking with malware, or exfiltrating sensitive data. Instead of just hoping that technology flags and alerts you to the suspected activity, you apply human analytical capacity and understanding about environment context to more quickly determine when unauthorized activity occurs. This process allows attacks to be discovered earlier with the goal of stopping them before intruders are able to carry out their attack objectives.

Until there were tools available that could give analysts a data-centric view of what was going on in their environments, all organizations had were the time-proven, but no-longer-effective, log review techniques for discovering that the horse escaped from the barn yesterday, last week, or even last year. Carbon Black Endpoint Detection & Response (EDR) is one of these data-centric tools. More than that, Carbon Black EDR is an industry-leading tool that puts wheels on the threat hunting bus and gives threat hunters the upper hand in today's cyberwars.

About This Book

Threat Hunting For Dummies, Carbon Black by Broadcom Special Edition, introduces the concept of threat hunting and the role it plays in the protection of your organization's systems and information. Many organizations have yet to start a threat hunting program, so this book explains what threat hunting is for and

how to get a program off the ground. You will better understand how threat hunting works and why it's needed. It will become apparent to you that threat hunting is an essential component in an organization's security program.

While threat hunting requires specific tools and technology, a successful program requires far more: motivated, trained personnel; collaboration across IT and the business; a desire to make needed improvements to keep attackers out; local context, environmental understanding, and differentiation between what's expected and not.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of what each one means:


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 things that may leave you vulnerable, cost you big bucks, suck your time, or be bad practices.


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 to take your existing program to a higher level. But if you want to learn

more than what's covered in these pages, here are some resources that can help:

- **How to feel more secure about EDR ebook:** Shopping around for yet another tool to add to your security stack can be daunting. This guide helps you find the EDR vendor that's best aligned to your cybersecurity needs. Go to `docs.broadcom.com/doc/how-to-feel-more-secure-about-edr-ebook`.
- **4 Questions To Ask Before Investing in EDR:** Before investing, asking the right questions can save you from getting stuck with an EDR that can't keep up. Visit `www.security.com/product-insights/4-questions-ask-investing-edr`.
- **The latest threat intel from Symantec and Carbon Black:** Their global threat intelligence teams provide unparalleled analysis and commentary on the cyberthreats you should be looking out for today. Check out `www.security.com/threat-intelligence`.

IN THIS CHAPTER

- Understanding today's security threats
- Introducing the practice of threat hunting
- Looking into the benefits 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, while 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. You can't just sit back and wait for obvious signs of an intrusion. 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 to not 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, ever-growing breaches make you wonder if breaches can be avoided at all.

This section shows you what motivates attackers and some of the methods they use to carry out these attacks.

What motivates cyberattacks?

Organizations face security threats from several types of actors with different motivations:

- **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 they gain access to medical records to commit Medicare fraud.
- **Political statement:** Hackers and "hacktivists" attack sites to make a political statement. A good example is the hacking group Anonymous that stated, in 2016, that it would attack the website of United States presidential candidate Donald Trump.
- **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. For example, when organizations fire or lay off personnel who have intimate knowledge about access to systems, these people may use that information to wreak havoc on the company.
- **Fame:** In the hacker community, hackers are recognized and respected for compromising high-visibility or high-value sites, particularly those that take pride on how good their security is. Hackers like to humble these organizations.

However, the end result is the same: compromise of sensitive data or disruption of business operations, and sometimes both. The actors behind the threats include cybercriminal organizations, nation-states, and hackers for hire.

What are the attack methods?

Attackers seem to have little trouble getting into organizations' networks and systems. Looking at this from a big-picture perspective, attackers gain access through different avenues:

- **Stealthy malware:** The primary method of intrusion today is stealthy malware. Designed to evade detection by antivirus software and other tools, today's malware employs advanced evasion techniques, which are difficult to detect.

  

  The main technique used by malware today is known as *polymorphism.* Malware reencrypts or repackages itself for each new victim computer, making every infected system appear to be unique. This thwarts antivirus's main technique of detection by signature largely obsolete.

- **Hacking the people:** Intruders use various methods for tricking personnel into unwittingly granting intruders access to their workstations or the organization's network itself. Techniques used here generally involve pretexting in the form of phishing emails that trick users into opening attachments or visiting websites. The result? Malware that's 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 logon credentials. Other techniques include brute force attacks through password guessing. This technique is 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 prove to range from an irritant to an incident that threatens the ongoing viability of your organization.

Understanding Assumption of Breach

Information security professionals used to put all of 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.

This didn't work out very well.

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, similarly, 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 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 detected intrusion.

Defining Threat Hunting

Threat hunting is, quite simply, the pursuit of abnormal activity on servers and endpoints that may be signs of compromise, intrusion, or exfiltration of data. Though the concept of threat hunting

isn't new, for many organizations the very idea of threat hunting is. The common mindset regarding intrusions is to simply wait until you know they're there. Typically, though, this approach means that you'll be waiting an average of 220 days between the intrusion and the first time you hear about it. And even then, it's typically an external party such as law enforcement or a credit card company that's telling you.

REMEMBER

With threat hunting, you use humans to go "find stuff" versus waiting for technology to alert you. Don't sit back and wait for a knock on the door. Proactively chase down signs that intruders are present or *were* present in the recent past. What are you looking for when you're threat hunting? You look for anomalies — things that don't usually happen.

TIP

To do this effectively, you need tools that give you highly granular visibility into the goings-on in the operating systems of every endpoint and server — things like processes that are launched, files that are opened, and network communications that take place. Tools such as Carbon Black EDR are tailor made for effective threat hunting across an enterprise.

Defining the Threats That Are Hunted

Threat hunting is systematic. Threat hunters need to be continually looking for anything that could be evidence of intrusion. 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 are looking 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 MD5 hashes, make specific registry key modifications, and include known bad files.

  The MD5 hash, also known as *checksum* for a file, is a 128-bit value (like a fingerprint of the file). You can get two identical hashes of two different files. This feature can be useful both for comparing the files and their integrity control.

TECHNICAL STUFF

- **Binaries:** Here hunters look for binaries with certain checksums, file names, paths, metadata, specific registry modifications, and many other characteristics.
- **Network activity:** This threat attribute includes network activity to specific domain names and IP addresses.
- **Registry key modifications:** Hunters can look for specific registry key additions and modifications.


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 indicators of compromise (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. These attackers are virtually insiders that seek out "live off the land" activities of organizations' networks, systems, and applications. But like 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 is able to easily evade antivirus software through polymorphic 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 that are 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 and by the day. The average time to detection of 220 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 the answer.


REMEMBER

Threat hunting is becoming a part of infosec table stakes: the essential tools and practices required by all organizations. Threat hunting will soon be a part of the due care for information protection expected by customers, regulators, and the legal system.

The Evolution of Threat Hunting

Threat hunting is a combination of tools and techniques. Tools provide highly detailed information across endpoints; how these tools are used constitute 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; instead, current techniques are still important. Automated systems such as intrusion prevention systems (IPS), data loss prevention (DLP) systems, firewalls, and web filters are still needed because of their capability to detect (and sometimes block) malicious activity.

Man and machine

Modern cybercrime is perpetrated by combining the skills and intuition of an attacker with evolved technologies. Threat hunting is the unification of man and machine that allows defenders to

fight back. Man and technology need to form hunt teams, like an elite navy SEALS team or a tiger team. In war, you don't send in the regular infantry to capture a leader; instead, you use your elite forces and advanced drones.

Science and art

Threat hunting is part science and part art form. The science part of threat hunting is the vast amount of detailed information available from all endpoints. The art form in threat hunting is the use of instinctive cat-and-mouse techniques in pursuit of signs of intrusion, no matter how small.

Details and big picture

Threat hunting means looking at the big picture and at the details — at the same time. This process is carried out through tools that can be used to perform very detailed queries about specific activities, which take place across hundreds or thousands of endpoint systems.

Some people think threat hunting is using an intrusion detection system (IDS) and just getting alerts — or setting up endpoint detection and response (EDR) solutions to look for a specific behavior or indicator and getting an alert. This is *not* threat hunting. Setting up EDR solutions to look for a specific behavior can be an outcome or the post-mortem *after* a hunt so that 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; instead, 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.

Data exploration

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

UNDERSTANDING THE KILL CHAIN MODEL

Developed by Lockheed Martin, the Kill Chain Model accurately depicts the methodology used by intruders as a means for information security professionals to better understand attack techniques so they can defend their networks. By using the Kill Chain Model, the threat hunter is looking for evidence at any point in the intruder's campaign. The steps in this model are as follows:

- **Reconnaissance:** The intruder selects a target, researches it, and attempts to identify vulnerabilities in the target network.
- **Weaponization:** A weapon, typically malware, is selected or developed for use on the target system.
- **Delivery:** The weapon is delivered to the target system.
- **Exploitation:** The weapon's code is triggered, which exploits a vulnerability on the target system.
- **Installation:** The attacker installs components that permit permanent control of the target system.
- **Command and control:** This is an attacker's remote control capability, whether mechanized or hands on keyboards.
- **Actions on objective:** Attackers work to carry out the overall objective of the attack whether it's stealing information, destroying information, or disrupting systems or networks.

Computing and the business

A threat hunter understands computing at a detailed level. He understands 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.

Knowing the battlefield

Endpoints are critical to threat hunting: The endpoint is the battleground in modern cyber wars. If you don't have endpoint

visibility, it's really hard for you to have a meaningful or conclusive hunt. The endpoint is where you find the tracks in the mud, and the endpoint holds the keys to the data and information that attackers are after.

REMEMBER

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

WHAT THREAT HUNTING IS *NOT*

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

- **Acquiring or analyzing threat intelligence:** While this is useful to do, 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 through the leveraging of technology and data to be able to analyze activity and artifacts.
- **Reporting on incidents or intrusions:** This is an after-the-fact activity; whereas, threat hunting is the pursuit of bad actors before incidents get out of hand.
- **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.

IN THIS CHAPTER

- Assembling your threat hunting team
- Acquiring and integrating threat hunting tools
- Learning 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 several different aspects. This section contains the essentials as you begin this effort.

Team composition

The people on your threat hunting team should be knowledgeable about the internals of the operating systems (OS) found in your endpoints. Mainly this system will likely be Microsoft Windows, but it may also include Apple Mac OS and perhaps Linux. What

I mean by OS internals expertise is this: 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)

Expertise at this level of detail is important because malware operates within these domains and makes subtle changes to the OS here. Threat hunters need to understand what to look for and what "normal" looks like (understanding what's normal at the business-application and human-activity level — it's not just about packets on the network and processes in the OS), so anomalies will be more apparent. And remember, it's anomalies that are the primary sign that malware is lurking in endpoints.

After you know what expertise is needed, it's time to figure out who has these expert skills and work on bringing them into 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 short-handed. 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 passive monitoring of security events.

Making time to threat hunt

Unless Daddy Warbucks has tossed you a new bag of money 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, how many 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 with two to four man hours a week that are dedicated to hunting. When you see results from your hunts, adjust as needed. The important thing is getting results from your hunts so that they show a return on that time investment. It's all about allocating the 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 the following:

- **Operating system internals:** This skill is critical for threat hunters. They need to not only understand the rules and practices of process management but also the file system operation and network communication in each operating system in use.
- **Endpoint application behavior:** It's important for your threat hunters to understand how any locally used applications function on your endpoints.
- **Threat hunting tools:** Your threat hunters need to thoroughly understand how to use the tools at their disposal, so they will be effectively hunting for attackers.
- **Incident response procedures:** Your threat hunters need to understand what steps they need to take when they discover signs of intrusion in your systems and then they need 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.

Put 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 and IT security processes. An essential part of this is a means for learning several things, including the following:

- **Endpoint baselines:** You need to continuously hone your threat hunters' knowledge of what constitutes "normal" in your endpoints, so anomalies can be more quickly recognized.
- **Improving hunting tools, practices, and skills:** You want your hunts to become better over time, and you want your new threat hunters to be able to quickly learn from the seasoned warriors on your team. In part, this is about tribal

knowledge, but it also needs to include a knowledgebase, so each new threat hunter can stand on the shoulders of his or her predecessors.

- **Improving response:** Finding prey requires response that includes containment and remediation. Mainly, this means doing these things more accurately and also more quickly.
- **Improving skills:** Your threat hunters need to improve their skills and knowledge, not just from threat hunting itself, but from continuing education on ethical hacking, system and network internals, and incident response.

REMEMBER

It's essential for your threat hunters to 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: Getting the Necessary Tools in Place

Threat hunting is a man-machine activity — you can't do it with just people or just 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.

Complete endpoint visibility

Endpoints are today's battleground where intrusions into enterprises begin. Endpoints are the attackers' crown jewels, and they're used to make a landing into your environment. Endpoints are everything. And while 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 those machines, too.
- Include information about every process, including its parents and children, as well as every file that's created, read, written, and removed, plus network activity. This information

needs to be able to be queried across the entire organization, so your threat hunters can quickly understand what anomalous activity is going on at anyplace and at any time.

- Another very important aspect of endpoint visibility is known as *retrospection,* which is the ability to hunt back in time. For example, you mine the data for suspicious activity that took place not just yesterday, but last week, last month, or even earlier.

TIP

Carbon Black uses its Endpoint Detection & Response (EDR) solutions to provide the endpoint visibility that enterprises need for effective threat hunting. These tools help you understand in detail what's going on in endpoint systems, including malware attacks.

REMEMBER

Complete visibility is needed on *every* endpoint. Otherwise, attackers may be able to single out unprotected endpoints and get into your environment without notice.

Obtaining the necessary network event data

In addition to endpoint visibility (see the preceding section), having access to network event data is essential. Sometimes the first sign of intrusion is in the command and control (C&C) network traffic from a bot that has already compromised an endpoint. Intrusion prevention systems (IPS), web filtering, firewall logs, and netflow tools are good sources for obtaining this data. Threat hunters need to be able to reference one or more of these tools from time to time to better understand what's going on in the network.

Threat intelligence gathering

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 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) and 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

Carbon Black provides more than 20 threat intel feeds to its customers, helping them to automatically detect and respond to new threats.

Integrating your information

Remember that threat hunting is a man-machine activity. In many respects, there is a high volume of information on threats and activities in your environment. To make the most of this information, you want to understand what tools you're using and where there may be opportunities to integrate them.

One great example is the fusion of your endpoint data, SIEM data, and threat intel feeds. By themselves, they're useful, but when fused together, they're far more valuable. For instance, threat intel feeds often use STIX, TAXII, or CybOX for structuring this data. APIs for these are available so that you can consume this data and get it into your other systems.

Data correlation and analytics tools

Because threat and event data is coming in from a lot of different places, you need to be able to perform event correlation and analytics 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. They're often used as a central repository for log and event data from network devices, firewalls, operating systems, and applications. It's the storage for everything going on in your environment, together with the ability to make sense of it.

People and Technology: Know Your Environment

Successful threat hunters need to know as much about your environment as possible, so they can better sense what's normal and what's abnormal. But as they proceed in their threat hunts, in many respects they begin to have a more intimate familiarity with your environment than anyone else.

What's normal and what's 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 more familiar with normal, routing 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. Mainly, they need to understand this independently of their threat hunting, because anything they might observe in the environment may or may not be normal in the first place. What your threat hunters find and consider normal includes things that are there but aren't allowed.

WARNING

Occasionally, threat hunters discover things that aren't necessarily security incidents; instead, they're insiders with poor judgment.

Know 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 know what the goals are. Depending on the attackers and their objectives, this could be information like customer or employee data, or it could be critical assets such as public facing web servers. Threat hunters need to know all these high-value targets (HVTs) — the likely ones and those less so. And, they need to understand *how* attackers might go about attacking them.

Anticipate 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. This is part gut feel and part knowing your environment:

- **Architecture:** Attackers are going to try and figure out the weak spots in an 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 are going to go for an 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 an organization is a great indicator of vulnerability. While attackers might not have ready access to security awareness training or other aspects of an organization's security awareness program, 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. While they will get creative and be unpredictable at times, attackers are people too — creatures of habit and apt to use tools and techniques they're used to and what has worked for them in the past. Because organizations tend to protect themselves in similar ways, attackers are likely to attack in similar ways.

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.

IN THIS CHAPTER

- Getting inside the thought process of a threat hunter and a new hunt
- Setting up for a hunt
- Understanding the Carbon Black Hunt Chain

Chapter 3
The Hunt

When the threat hunting team and tools have been acquired and trained, it's time to go 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 Carbon Black, the Hunt Chain methodology depicts the entire threat hunting process.

The Mentality of the Hunt

Maybe you've been familiar with operating system (OS) internals for a long time, and you've been inside the proverbial machine. Maybe you've even written some of your own tools and exploits. You're reading about cybercrime and what hackers do these days, and you're mad as heck, and you're not going to take it anymore! It's time for the chase and to put cybercriminals on the defense. Make them run.

This description is the mental attitude of a threat hunter: He knows how systems work, how attackers think and act, and how to use tools to go after them, find them, and kick them out. Your organization has its weak spots — sure. Every company does.

That may give cybercriminals an easy way in, but it doesn't give them the right. You know where they'll strike, and you'll be waiting for them.

The primary objective of threat hunting is asset and information protection through the following:

- Knowledge of systems, networks, exploits
- Knowledge of the enterprise applications, how they work, where the treasures are, and how the data flows
- Knowledge of endpoints, how they work, and how they're used

Week in and week out, a threat hunter adds to his knowledge, skills, and tools. With the right tools, such as Carbon Black EDR, each new query becomes another automatic threat detector, so the hunter slowly gains ground and denies attackers access to more and more attack surface. That way, a threat hunter needs to never hunt for the same thing twice. But at the same time, attackers' tools improve, and more exploits are discovered, so it's a tug of war between threat hunters and their adversaries. Constantly reading and learning about new exploits, threat hunters test out new hunches and see whether attackers are trying these new techniques and, if so, what they look like.

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 indeed 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 exploits:** A threat hunter may have read about some specific new exploits, such as Locky, 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 attempting 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.

Threat hunters generally concentrate their attention on endpoints with tools such as Carbon Black EDR, which provides detailed forensic data on endpoints. Depending on the hunt's objective, the threat hunter may be triangulating attack evidence by using additional tools, such as an intrusion prevention system (IPS), web proxy filter, or next-gen firewall to identify signs of compromise.

REMEMBER

Threat hunting is not only about detecting malware but also the abnormal usage of legitimate tools (such as PowerShell and 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, traffics, 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.

The Carbon Black Hunt Chain

Carbon Black 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. This section explains the different aspects of the Hunt Chain.

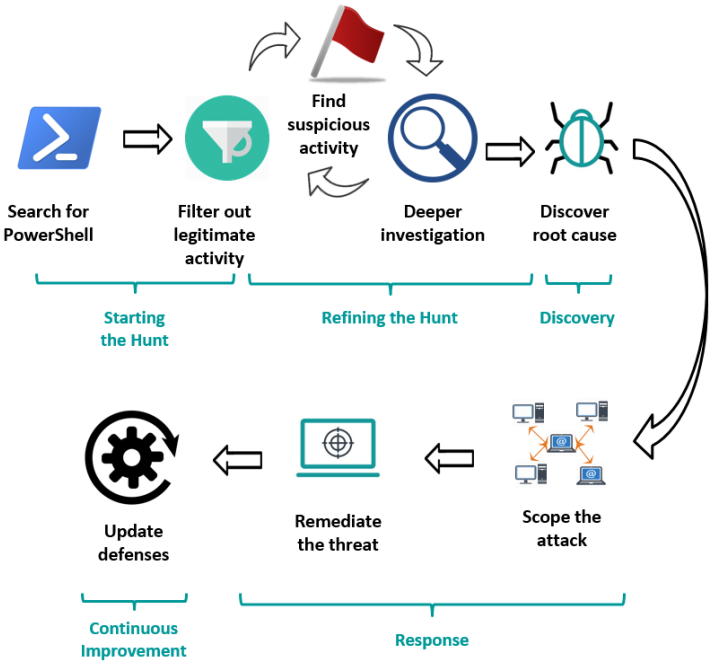

FIGURE 3-1: The Carbon Black Hunt Chain.

Where and how to start

A threat hunt starts with the collection of data that's directly or indirectly related to its objective. When developing an objective, the threat hunter needs to know what data will be mined in order to achieve the hunt's objective.

Define objectives and the scope for a hunt *before* the hunt begins to 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.

Filtering out legitimate activity

As threat hunters begin observing the target environment, they begin observing activities. By using their knowledge about the OS and application(s) in the target environment, they begin to filter out legitimate activity, leaving only anomalous activity to investigate. One by one, as those activities are explained, all that remains, if anything, are attackers and their actions.

Hunt for suspicious activity

During the hunt, the threat hunter observes data and filters out known legitimate activity. Anything that remains could be suspicious. For example, an organization might utilize PowerShell as a part of its endpoint management tools. PowerShell is a command line shell and scripting language; you could liken it to the new and improved version of command line and batch files. A threat hunter can use this knowledge to filter out all of the organization's legitimate use cases for PowerShell. If any uses of PowerShell remain, they either belong to additional legitimate use cases or attacks. Remember that threat hunts don't always turn up activity indicating intrusion.

Deeper investigation

Activities that remain unexplained are investigated further. The threat hunter may need to solicit help from experts on the OS, applications, data flows, use cases, or other aspects of the anomalous activity. Oftentimes, the threat hunter discovers aspects of legitimate activities that were previously unknown.

Sometimes the threat hunter discovers aspects of an environment that represent improper implementation of a system. For example, a threat hunter may find persistent temp files containing credit card numbers, where the files were supposed to be encrypted but weren't. This may have been considered an artifact of an attacker scraping credit card numbers out of an application.

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, which — depending on the attack — may narrow into an initial intrusion, but it may also branch out into an investigation into what could be a broader attack on more systems.

Remediate

After the total extent of an attack is known, the threat hunter — often together with appropriate colleagues (system engineers,

network engineers, security engineers, software developers, and maybe others) — contributes to the remediation effort. The specific activities vary, depending on the nature of the attack, but the general principles are

- 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 to prevent similar attacks

Update defenses

The organization needs to update its defenses so similar attacks require greater effort on the part of attackers. Updating includes automating systems to look for what you found. The range of activities may include

- New or updated firewall and IPS rules
- New or updated alerts in a security incident and event management (SIEM) system
- Improved incident response procedures
- Updates to infrastructure, application, or security architecture
- Changes in application development, testing, quality assurance (QA) or quality control (QC) tools, and processes
- New alerting rules in Carbon Black EDR or similar endpoint detection and response tools

The investment in threat hunting tools and personnel is mostly wasted if there isn't a feedback loop incorporated that illuminates lessons learned and updates defenses. A threat hunt doesn't just find outside attackers; insider threats can also be discovered in a threat hunt. A traitor is every bit an enemy as an outside adversary.


TIP

The results of a threat hunt will also give the threat hunter a lot of ideas for future hunts. If you're fishing in a pond and 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, too, 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. Being an expert in defense, you've been able to impart several useful suggestions to tighten things up from an architectural perspective. You also will have an understanding of where the organization may be weak in detection or response capabilities and be able to offer suggestions for additional tools that could be used to allow for a better overall defense.
- **Better instincts:** As you gain experience threat hunting in your environment, you begin to build an instinct for discerning abnormal activity as well as the way in which the next intruders might attempt 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.* Rather, 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.

Be 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 needs to be about how you work with others in the organization. While 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, more often than not, a threat hunter is 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 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 need to work with people who understand how systems were designed, built, and implemented. This knowledge helps you better distinguish anomalies from legitimate operations.
- **You need to 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.

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 dataset 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 you 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, and it's just incredible.

Developing Intuition

A master threat hunter develops a "sixth sense" when it comes to the hunt: After enough time, he sees attack patterns emerge out of a collection of seemingly unrelated data points. He begins 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 himself in the shoes of the attacker and see the environment as a potential target and anticipate the next move by the attacker given this understanding of how he sees you. Thinking like an attacker separates the master threat hunters from the rest.

Educated hunches

Threat hunting isn't just all 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 IPs 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:

- **Observe:** Collect data from sensors on your endpoints and events in the network.
- **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 (C&C) traffic be occurring, or could one of your endpoints be under attack from a ransomware variant?
- **Decide:** Make a decision about what to do. After you have a clear picture regarding 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.

- **Act:** Execute the plan to shut down the intrusion, harden the organization's security posture, and enhance detection. Repeat.

While many times your hunts might return "empty" and no intrusion will be discovered that leverages that particular vulnerability, the knowledge created is incredibly valuable because you've created 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:

- Operating systems always open files like this.
- 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, while 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 from 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 you may not only return with no prey, but also you could *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 just 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 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:** Chances are there are a lot of tools in the environment, many of which may have APIs or interfaces that can be used 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'll act as both the problem finder and the problem solver. They must be able to not only understand how new attacks work but how to "stitch" together the various pieces of information available in the environment to enhance visibility and defenses.

Setting Landmines

A master threat hunter thinks ahead and anticipates what a known or a potential adversary might do. In this scenario, hunters can set landmines 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. This is again 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,* in an attempt to lure malicious actors into attacking a decoy target loaded with intrusion detection monitoring sensors. Instead of actually 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 contains one or more honeypots, and 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).

SANS and Other Training

The SANS Institute uses the very best experts — the journeymen (and women) in the security world — as speakers at SANS conferences and instructors at SANS training events. Engineers, analysts, architects, and fellow hunters are among SANS speakers and instructors.

Sure, courses on threat hunting from SANS are terrific, but you shouldn't stop there. Also consider one or more of these courses:

- Security courses
  - **SEC401:** Security Essentials Bootcamp Style
  - **SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling
  - **SEC511:** Continuous Monitoring and Security Operations
  - **SEC542:** Web App Penetration Testing and Ethical Hacking
  - **SEC503:** Intrusion Detection In-Depth
  - **SEC561:** Immersive Hands-On Hacking Techniques
  - **SEC617:** Wireless Ethical Hacking, Penetration Testing, and Defenses
  - **SEC660:** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
- Forensics courses
  - **FOR408:** Windows Forensic Analysis
  - **FOR508:** Advanced Digital Forensics and Incident Response
  - **FOR610:** Reverse Engineering Malware: Malware Analysis Tools and Techniques

This list is but a small sampling of the courses available. You can find a complete list at `www.sans.org/courses`. I urge you to challenge yourself and add to your skills and knowledge through continual exploration and learning, as a master threat hunter would do.

In addition to participating in academic security training, you can embed yourself within the security community. This immersion will ensure that you're constantly being exposed to the latest defensive (and offensive) techniques in the industry. To get you started, here is a short list of must-attend conferences:

- **Black Hat USA:** `blackhat.com`
- **DEF CON:** `www.defcon.org/index.html`
- **DerbyCon:** `www.derbycon.com`
- **InfoSec World:** `infosecworld.misti.com`
- **RSA Conference:** `www.rsaconference.com`
- **ShmooCon:** `shmoocon.org`
- **BSides:** `www.securitybsides.com`

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

Consider the fact that attackers don't think of *their* success as optional. Given that, effectiveness and success of a threat hunting program are critical. Organizations that start a threat hunting program have success in mind, but are they able to achieve it? The ten tips in this chapter help your organization and its threat hunters be effective and successful.

Know Your Environment

The purpose of threat hunting is the discovery of abnormal activities that point directly to reconnaissance and attacks. To recognize activities that aren't normal, it's first important to understand what's normal. Furthermore, it's important to become familiar with the architecture overall and at a detailed level to understand where vulnerabilities and weaknesses are that could be targeted by attackers.

Understanding one's 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 also build relationships with key personnel in 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, but 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. You can find more information on knowing your environment and understanding what's normal in Chapter 2.

Think Like an Attacker

A threat hunter's mission is to find signs of intrusion, and quickly, so attacks can be stopped and their effects mitigated to minimize damage. But rather than 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 EDR, threat hunters can set up triggers that fire when an attacker ever 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. For more information, check out Chapter 4.

Develop the OODA Mindset

Observe. Orient. Decide. Act. This is how the military thinks about combat operations. Threat hunters are soldiers in the cyberwars, so it makes sense to think about threat hunting in this way. The steps to OODA are as follows:

- Observe
- Orient
- Decide
- Act

OODA is mental discipline that keeps threat hunters from acting impulsively. In the cyberwar arena, acting before thinking can blunt a threat hunter's effectiveness. 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 as well as tools and systems to run them on. Further, it includes personnel who know how to carry out threat hunts. Here's a breakdown on what's needed:

- **Personnel:** One or more trained and/or experienced threat hunters. These people have a deep understanding on 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 need to have a thorough and growing familiarity of 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, which is installed on every endpoint and provides a step-by-step detailed forensic history of every activity on every endpoint. The real power of Carbon Black EDR is its central querying capability, 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.

If you need more information on threat hunting resources, Chapter 2 is the place to go.

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.

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. While they're the principle focus of attacks by intruders, endpoints are by no means the only place where information about intruders can be found. In addition to endpoint tools, it's often useful to have network-centric visibility by using tools, such as

- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Netflow
- Web filters
- Firewalls
- Data loss prevention (DLP) systems

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 Observe and Orient (for more info, see the earlier section "Develop the OODA Mindset" or flip back to Chapter 4).

Collaborate across IT

Threat hunting isn't just about technology. *The* essential ingredient in threat hunting is 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'll be in dialogue with key IT personnel to hone their understanding on 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), work with others to understand it (Orient), before acting on it (Decide and Action). For more info, see Chapter 4.

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

Innovation in the cybersecurity arms race is occurring at a dizzying pace. Seasoned threat hunters know this, and they take time out from the hunt to 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, as well as national and international conferences like RSA, Black Hat, and DEFCON, provide tremendous networking and education opportunities.

Chapter 4 expands the topic of training if this is something you want to learn more about.

Be Aware of Attack Trends

Threat hunters can't exist on intellectual islands. Instead, they need to be continually aware of the techniques used by cybercriminal organizations 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? See Chapter 4.


TIP

While this book is a good "getting-started"-type resource, you can find a lot of great training and resources online. One place where threat hunters can learn from each other is the Carbon Black Community, at `https://community.broadcom.com/carbonblack/home`.

Eliminate hidden threats in your environment

If you only rely on passive, automated threat detection, you'll always be one step behind threat actors. Advanced threats could be hiding in your environment – but you can hunt them down! This book shares demystifies the practice of threat hunting so that you can advance your security program and better protect your organization. You'll learn how threat hunting works, why it's an essential component in your organization's security program, and how you can master the discipline to improve the security of your organization and advance your career.

Inside...

- See why threat hunting is necessary to combat today's threats
- Assemble your team with the right mindset and toolkit
- Think like an attacker and stay one step ahead
- Take command of the fundamentals and hone your skills
- Strengthen your organization's security posture

Carbon Black.
by Broadcom

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

ISBN: 978-1-394-34991-3
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.