LEARNING MADE EASY

Palo Alto Networks Special Edition

XDR

for dummies®
A Wiley Brand

Find out what XDR is — and what it isn't

Break the attack chain with XDR

Explore XDR use cases

Brought to you by

CORTEX XDR
BY PALO ALTO NETWORKS

Lawrence Miller

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

XDR

Palo Alto Networks Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

XDR For Dummies®, Palo Alto Networks Special Edition

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

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.

ISBN 978-1-119-85169-1 (pbk); ISBN 978-1-119-85170-7 (ebk)

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
Business Development Representative: Cynthia Tweed
Production Editor: Mohammed Zafar

Introduction

Year after year, the challenge of securing critical data intensifies as the rapid adoption of trends such as cloud computing, the Internet of Things (IoT), and digital transformation increase the risk to companies' sensitive data. At the same time, threat actors take advantage of many of these same technology trends to expand the power and scale of ever more sophisticated attacks.

Security teams have deployed tools, implemented processes, and hired staff to respond to new threats as they've emerged, but they're outnumbered and outgunned. But continually bolting new capabilities onto existing systems quickly creates a mess of poorly integrated tools that require a lot of scarce time, energy, and skill to use. Static processes that don't adapt to rapidly changing trends and environments — such as cloud and remote work — quickly become stale and ineffective. And security analysts are charged with the near-impossible task of triaging a never-ending deluge of security alerts, but they often receive limited training and equally limited tools. The combination of too many alerts and too little context causes security teams to lose visibility and control. Ultimately, the company becomes even more at risk as a result.

Extended detection and response (XDR) has emerged as a response to this complexity. XDR is a category of threat detection, investigation, and response solutions that work together across all threat vectors in a company's infrastructure — including network, endpoint, cloud, and identity — rather than just one aspect of the infrastructure. By building integration directly into the architecture, XDR tools by design deliver threat insights and recommendations that optimize how security teams operate.

About This Book

XDR For Dummies helps you get up to speed on the XDR category of security solutions and what it means for your company. This book consists of five chapters that explore the following:

- The current state of detection and response, including threats, limitations, and challenges (Chapter 1)

- What XDR is and what it isn't (Chapter 2)
- How XDR breaks the attack life cycle to stop attacks (Chapter 3)
- Different XDR use cases (Chapter 4)
- Must-have XDR capabilities and features (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you work for an organization that's looking for a better way to improve the effectiveness of its security strategy, specifically its detection and response capabilities. Perhaps you're an IT executive such as a chief information security officer (CISO), chief information officer (CIO), or chief technology officer (CTO), or a VP or director of security. Or perhaps you're a network or security architect or engineer. As such, this book is written for technical readers with a general understanding of modern security operations concepts and technologies.

If any of these assumptions describes you, this is the book for you! If none of these assumptions describes you, keep reading anyway — XDR is a must-know technology, and your team will thank you for becoming an X-pert on XDR!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

The Remember icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! The Technical Stuff icon explains the jargon beneath the jargon and is the stuff nerds are made of.

TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

I can only cover so much in this short book, so if you find yourself at the end of it, thinking, "Gosh, this was an amazing book! Where can I learn more?," head to `www.paloaltonetworks.com/cortex/cortex-xdr`.

IN THIS CHAPTER

- Seeing the urgent need for a better approach to security
- Understanding the limitations of traditional detection and response tools
- Addressing alert fatigue and the security skills gap

Chapter 1
Looking at the Current State of Threat Detection and Response

In this chapter, I explain how modern threats have evolved to become potentially more destructive; why traditional approaches to prevention, detection, and response aren't sufficient; and how alert fatigue and the cybersecurity skills shortage increase risk for your organization.

Surveying the Modern Threat Landscape

Lately, data breaches and ransomware attacks have become so frequent that they practically warrant their own news segment alongside weather, sports, and traffic. The fact that these security events are commonplace, however, doesn't make them any less dangerous. Every minute that an active threat actor operates within your environment, tremendous damage occurs.

WARNING

According to the Ponemon Institute, from 2020 to 2021, the average cost of a data breach increased by 10 percent to $4.24 million. This was the largest single-year cost increase in the last seven years.

Of course, you already know and live this reality, and you work hard to detect threats and respond as quickly and effectively as possible — before data loss can occur. However, this is an uphill battle in the face of increasingly advanced tactics, techniques, and procedures (TTPs) used by threat actors. Attackers can now compromise an environment almost at will, without using traditional methods such as file-based malware. Instead, they will use methods that compromise authorized system files, insert attacks into a device's registry, or maliciously use utilities like PowerShell. The increase of novel and more evasive attack methods has driven the need for new strategies and tactics for detection and response, in addition to threat prevention.

REMEMBER

An organization's ability to stay on top of the modern threat landscape requires effective tools and a team of capable security analysts. Unfortunately, having the proper balance of technology and skilled experts tends to be the exception for most organizations, rather than the rule.

Recognizing the Limitations of Traditional Technologies and Approaches

While your security teams strive to prevent successful attacks against your organization, you have to prepare for the inevitable reality that no environment is completely secure. Eventually, a threat will gain entry into your environment.

A dizzying array of logging, detection, and response tools have come to market to help security teams find threats. Each of these tools has strengths and weaknesses and can be useful against attacks — such as known file-based malware incidents or attacks that are designed to defeat just one part of the infrastructure. Most of these tools, however, are tuned for a single purpose, and none is particularly well suited to handling sophisticated threats on its own.

WARNING

ESG Research found that 66 percent of organizations feel their threat detection and response effectiveness is limited because it's based on multiple independent point tools.

In the following sections, I take a closer look at some of the more common logging, detection, and response tools used by security teams, and fill you in on their challenges and limitations.

Endpoint detection and response

Endpoint detection and response (EDR) is a category of tools used to detect and investigate threats on endpoint devices. EDR tools typically provide detection, analysis, investigation, and response capabilities.

EDR first emerged in 2013 to help forensic investigations requiring very detailed endpoint telemetry to reverse-engineer malware and understand exactly what a threat actor did on a compromised device.

EDR tools monitor events generated by endpoint agents to look for suspicious activity. The alerts that EDR tools create help security operations analysts identify, investigate, and remediate incidents. EDR tools also collect telemetry data on suspicious activity and may enrich the data with other contextual information from correlated events. Through these functions, EDR is instrumental in shortening response times for incident response teams.

However, EDR alone can't provide enterprise threat detection due to its sole focus on the endpoint. It doesn't offer visibility into network traffic of devices without installing agents on network and networked devices — such as routers, switches, servers, Internet of Things (IoT) devices, bring your own device (BYOD), and industrial control system (ICS) — and cloud resources such as workloads, cloud networks, and platform as a service (PaaS) offerings.

Endpoint protection platform

An *endpoint protection platform* (EPP) is a software agent installed on endpoint devices to prevent file-based malware attacks and detect malicious activity. EPP is the evolution of traditional host-based antivirus and anti-malware solutions and is generally considered to be the first line of defense on an endpoint.

Detection capabilities across EPP solutions vary, but most use some combination of detection and prevention techniques, including the following:

- Static indicators of compromise (IOCs; that is, signature-based detection)

- *Whitelisting* (allowing) or *blacklisting* (blocking) applications, Uniform Resource Locators (URLs), ports, and addresses
- Behavioral analysis and machine learning
- Sandboxing to explode (or test) suspected threats, such as executables

An EPP solution should be cloud-managed to enable the continuous monitoring and collection of activity data, along with the ability to take remote remediation actions whether the endpoint is being used on the corporate network or remotely. In addition, EPP solutions are cloud-data assisted. In other words, the endpoint agent doesn't have to maintain a local database of all known IOCs; instead, the endpoint agent can check a cloud resource to find the latest verdicts on objects that it's unable to classify and leverage real-time threat intelligence.

EPP is designed purely to prevent or control and, hence, is not focused on detecting or collecting information to defend against modern attacks. Most EPP platforms also lack the response capabilities necessary to investigate incidents. As a result, EPP alone does not provide the essential features to stop modern attacks.

Security information and event management

Security information and event management (SIEM) software tools provide near-real-time collection, correlation, and analysis of security events, as well as notification of security alerts generated by various network devices and applications.

Many organizations allocate large portions of their security budgets to SIEM tools to gather logs from disparate security devices and server environments. SIEMs were initially designed primarily as log collectors for compliance reporting purposes. Over time, their usage expanded to threat detection, and SIEMs are now the central alert repository for many security operations centers (SOCs).

A SIEM centralizes alerts and aggregates log data by parsing and normalizing it. Security teams get to see the log data all in one place, but it typically isn't pieced together meaningfully, and the frontline analysts charged with making sense of it often can't use

the tools that contain the richer source data to validate alerts. Overall, SIEMs lack the depth of analysis for key data sources, such as endpoint data and network data, and they can be challenging to deploy, configure, and maintain, in part because they lack this out-of-the-box knowledge.

Network detection and response and user and entity behavior analytics

Network detection and response (NDR) and *user and entity behavior analytics* (UEBA) tools represent a newer class of security analytics tools that have emerged to address the challenges SIEM has in detecting unknown attacks. These tools use machine learning to develop a baseline of activity from the gathered telemetry and then look for atypical actions that may indicate malicious behavior. These technologies allow organizations to identify previously unknown attacks by recognizing unusual traffic patterns.

However, these tools also have their limitations. Network-based products are limited to the network and can't monitor or track local events, such as process information gathered on the endpoints. NDR also has very limited depth; if EDR is deep and narrow, NDR is wide and shallow.

REMEMBER

The complexity of modern attacks requires analysis of multiple data sources to identify and confirm malicious activity. Layering on one-dimensional tools adds significant expense for security teams, creates potential blind spots, and requires a lot of manual effort on the part of security analysts to switch between consoles and make sense of an attack.

Too Many Alerts, Too Little Time and Staff

Detection and prevention tools generate thousands of alerts every day — far exceeding the volume that security teams are staffed to effectively handle. These alerts come from many disconnected sources, leaving security analysts to piece the puzzle together (see Figure 1-1).

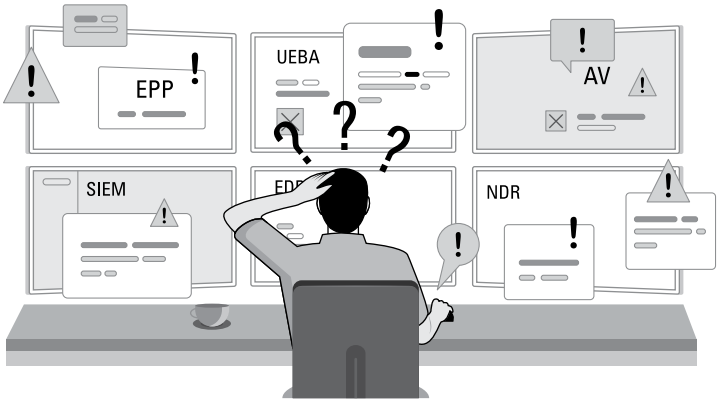

FIGURE 1-1: Siloed tools slow down investigation and response.

Analyzing a potential threat generally requires a number of steps:

1. Reviewing available log data to start piecing together what may have occurred
2. Manually comparing data against threat intelligence sources to determine if indicators are known to be malicious
3. Looking for related events using IOCs to determine if the alert is part of a larger attack.
4. Gathering context around the incident, including the systems, hosts, assets, resources, IP addresses, and files associated with each alert.
5. Constructing a timeline and identifying the root cause of an alert.
6. Checking whether new information links to alerts are being handled by other team members to coordinate efforts
7. Evaluating whether the alert needs to be escalated, discarded, or quickly remediated and closed out

All these steps take a lot of time and multiple tools to complete in a traditional SOC — and that's just triage. The net result is that analysts only have time to address the "highest-priority" alerts they come across each day; meanwhile, a disconcerting number of "lower-priority" alerts aren't addressed at all. And without the proper context to classify an alert as "high" or "low," the SOC may actually be missing what's really important and/or chasing issues that aren't really critical.

WHAT DOES A SOC TEAM DO?

Security operations teams big and small share some key functions. A traditional model for many SecOps teams and SOCs divides these functions into a tiered analyst structure, based on level of experience. Here are the primary responsibilities of those tiers:

- **Tier 1 — Triage:** This is where the majority of security analyst hours are typically spent. Tier 1 analysts are generally the least experienced analysts, and their primary function is to monitor event logs for suspicious activity. When they feel that something needs further investigation, they gather as much context from as many sources as they can into a report in the form of an incident that includes the user, the host, the IP address, and any related IOCs, and escalate the incident to Tier 2.
- **Tier 2 — Investigation:** Tier 2 analysts dig deeper into the suspicious activity to determine the nature of the threat and the extent to which it has infiltrated the environment, which includes building a timeline to understand the sequencing and correlating events to determine root cause. They must perform further investigation to understand how far the attack has gone. These analysts then coordinate a response to remediate the issue. This is a higher-impact activity that often requires more analyst experience.
- **Tier 3+ — Threat hunting:** These are the most experienced analysts, who support complex incident response and spend any remaining time looking through forensic and telemetry data for threats that may not have been identified as suspicious by detection software. The average company spends the least amount of time on threat-hunting activities, because the activities of Tier 1 and Tier 2 consume so many analyst resources.

Although this model may be the most common, it isn't necessarily ideal. Most people are not well suited to monitoring logs all day. Alert fatigue is real, and threats slip through among all the noise generated by the myriad sensors in a SOC. It can be hard to retain analysts to perform this task — they'd much rather be contributing meaningfully to investigations (and may have new and innovative approaches that are never revealed because they don't have the technical skills required for legacy investigation processes). Far too little time is spent on threat hunting and process improvement, because the majority of resource hours are spent uncovering and mitigating threats.

Further, security analysts who are responsible for alert triage are often left with insufficient context to determine the real risk that an attack presents to the organization. So, the alert is escalated to a higher-level group for further validation, requiring even more time, labor, and resources — creating inefficiencies at all levels.

REMEMBER

Most enterprises receive thousands of alerts from a multitude of monitoring solutions, but more noise is counterproductive. Advanced detection isn't about *more* alerts; it's about *better,* more actionable alerts. Achieving this kind of advanced detection requires integration of all the detection technologies in use, as well as sophisticated analytics that analyze endpoint, network, and cloud data to find and validate adversary activity in your environment.

Even with better and more comprehensive tools for threat detection, dealing with alerts — and possible incidents — requires further validation and triage from skilled responders. Unfortunately, not enough of these security practitioners are out there, and this significant skills gap impacts the ability of organizations to keep pace with attackers (see Figure 1-2).

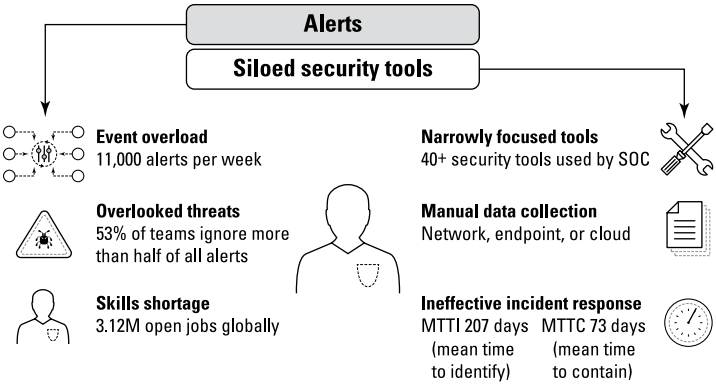

FIGURE 1-2: The many challenges of a security analyst.

Threat actors use highly automated tools and techniques to find vulnerabilities and gain initial access to your environment. This further exacerbates the skills gap because attackers are able to scale their automated toolkits faster and more affordably than

organizations can add skilled security personnel. So, you need to look for tools that can

- Make your less-experienced personnel more effective and efficient
- Automate detection of complex threats
- Simplify investigations
- Help analysts to improve their skills

TIP

In its 2020 *Cybersecurity Workforce Study*, the International Information Systems Security Certification Consortium, or (ISC)², reports a shortage of 3.12 million skilled cybersecurity professionals globally. According to Cyberseek, more than 300,000 cybersecurity job openings exist in the United States today — a number expected to grow substantially in the coming years.

Many companies choose to outsource their detection and response functions, either entirely or in part, to managed security service providers (MSSPs) or managed detection and response (MDR) vendors. Outsourcing this function is common (and considered best practice in many cases), particularly for teams with smaller security budgets or organizations that don't have the desire or resources to manage their own security. However, organizations that want comprehensive visibility and control shouldn't be stuck outsourcing their security simply because their tools are inadequate. It's also worth noting that the technology stack is just as important for an outsourced security team; vendors using legacy tools will wrestle with the same inefficiencies that plague in-house security teams.

What's really needed is a set of technologies to reduce the total number of alerts while at the same time allowing less-experienced analysts to assess threats efficiently and confidently on their own, ensuring that only high-fidelity alerts are escalated to more senior analysts.

IN THIS CHAPTER

- Starting with ironclad threat prevention to reduce noise
- Ensuring end-to-end visibility in your environment
- Reducing manual investigations to accelerate and improve incident response
- Maximizing the value of your security investments

Chapter 2
Defining XDR

Extended detection and response (XDR) is a new approach to threat detection and response. The term *XDR* was coined in 2018 by Nir Zuk, chief technology officer (CTO) and cofounder of Palo Alto Networks. The basic reason for creating XDR was to stop attacks more efficiently, detect attacker techniques and tactics that can't be prevented, and help security operations center (SOC) teams better respond to threats that require investigation.

The *X* in XDR stands for *extended,* but it really represents any data source, because it's not efficient or effective to look at individual components of an environment in isolation. XDR brings a proactive approach to threat detection and response, delivering visibility across all your data while applying analytics and automation to address today's increasingly sophisticated threats.

In this chapter, you learn what XDR is and the key requirements of an XDR solution.

Ensuring Robust Threat Prevention

The foundation for XDR is ironclad threat prevention. An XDR solution should accurately block more than 99 percent of threats that can be blocked automatically in real or near-real time — without manual verification. With best-in-class threat prevention, your team can focus on identifying and stopping more sophisticated and stealthy attacks instead of wasting time investigating every potential threat that gets past your defenses.

To defeat endpoint threats, you need a robust solution with integrated next-generation antivirus (NGAV) that can detect and block every stage of an attack — from the initial exploit and malware installation to the illicit actions executed by a threat actor running malware. Every layer of defense must be intelligent enough to defeat a threat actor's evasion techniques and continuously adapt to stop the latest threats.

TIP

Look for the following NGAV capabilities in an XDR solution:

- Machine learning–based local analysis and threat prevention
- Behavior-based threat prevention for dynamic analysis of running processes
- Exploit prevention by exploit technique
- Known threat prevention based on threat intelligence, such as file hashes
- Automated integration with a cloud-based malware prevention service, with analysis reports and minimum 100MB file-size support
- Zero-delay signatures to rapidly deliver protection and share threat intelligence
- Reverse shell protection capability
- Transparent threat detection engine updates
- Security profiles and exceptions
- Ad hoc and scheduled scanning of endpoints
- Protection against malware, ransomware, and fileless attacks
- Single lightweight agent for endpoint protection, detection, and response

Your XDR solution should also reduce your attack surface and safeguard sensitive data with endpoint protection features, including the following:

- Host firewall
- Disk encryption
- USB device control
- Customizable prevention rules

Finally, your XDR solution should be compatible with a network security client for endpoints to provide secure remote access, threat prevention, and URL filtering.

Providing Complete Visibility and Detection

Visibility and detection are critical for threat mitigation. If you can't *see* a threat, you can't identify it or investigate it and you certainly can't stop it. Threat actors leverage the cloud and machine learning to wage massive, multifaceted attacks that allow them to establish persistence and exfiltrate valuable data and intellectual property. This means XDR must have robust visibility and detection capabilities, including the following:

- **Broad visibility and contextual understanding:** Siloed point products lead to siloed data — and that's not effective. You can't possibly hope to defend against attacks effectively if you aren't at least as nimble in your own environment as threat actors are. XDR must have visibility and detection capabilities across your entire environment, integrating telemetry from your endpoints, networks, and cloud environments. Moreover, it must be able to correlate these data sources to understand how various events are linked and when a certain behavior is (or isn't) suspicious based on context (see Figure 2-1).

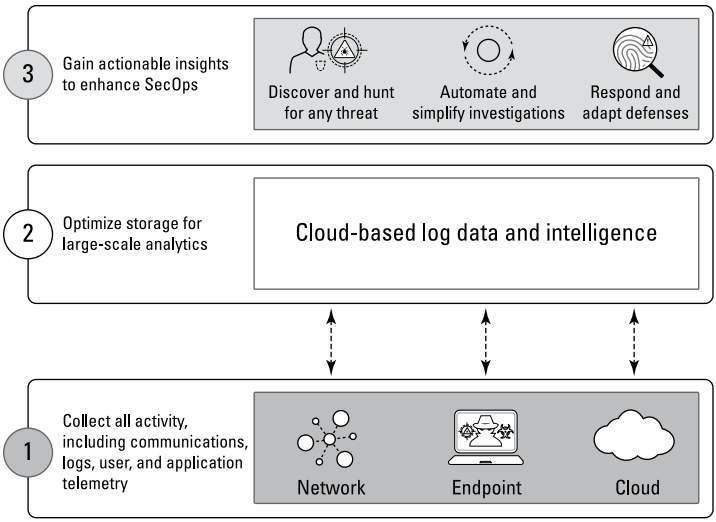

FIGURE 2-1: XDR breaks the traditional silos of detection and response.

- **Data retention:** Attackers are patient and persistent. They know they're harder to detect if they move slowly, waiting out the log retention periods of the detection technologies they're up against. XDR shouldn't make this easy for them. Your detection systems need to collect, correlate, and analyze data from the network, endpoint, and cloud within a single repository, offering 30 days or more of historical retention.
- **Analysis of both internal and external traffic:** Traditional detection techniques focus primarily on external attackers, providing an incomplete view of potential threat actors. Detection can't solely look for attacks coming from beyond the perimeter. It also has to profile and analyze internal threats to look for anomalous and potentially malicious behavior and identify credential misuse.
- **Integrated threat intelligence:** You must be equipped to deal with unknown attacks. One method of balancing the scales is leveraging known attacks that other organizations see first. Detection needs to rely on threat intelligence gathered across a global network of enterprises. When an organization within the extended network identifies an attack, you can use the knowledge gained from that initial attack to identify subsequent attacks within your own environment.

- **Customizable detection:** Protecting your organization presents unique challenges associated with specific systems, different user groups, and various threat actors. Detection systems must also be highly customizable based on the specific needs of your environment. These challenges require an XDR solution that supports both custom and predefined detections.
- **Machine learning–based detection:** With attacks that don't look like traditional malware, such as those that compromise authorized system files, utilize scripting environments, and attack the registry, detection technology needs to use advanced analytical techniques to analyze all the collected telemetry. These approaches include supervised and semi-supervised machine learning.

TIP

Look for an XDR solution that addresses the following key visibility and detection requirements:

- Behavioral analytics to profile behavior and detect anomalies indicative of an attack by analyzing network traffic, endpoint events, and user events over time
- Supervised and unsupervised machine learning capabilities
- Predefined and customizable behavior-based detection rules
- Custom rules that can retroactively detect attacks
- Granular alert exclusions for optional tuning of endpoint, network, cloud, or third-party alerts
- Shared threat intelligence to distribute crowdsourced threat intelligence from a cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services
- Ability to consume threat intelligence feeds from third-party sources in JavaScript Object Notation (JSON) and comma-separated values (CSV) formats
- Detection of attack techniques across the attack life cycle, including discovery, lateral movement, command and control, and exfiltration
- Demonstrated ability to detect attacker tactics and techniques through MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) evaluations

- Tagging of MITRE ATT&CK tactics and techniques in alerts and detection rules
- Asset management with rogue device discovery
- Vulnerability assessment
- Host inventory with detailed user, system, and application information

Accelerating Investigation and Response

When you're alerted to potential threats in your environment, you have to be able to quickly triage and investigate those threats. Doing this effectively — especially during an attack that touches multiple parts of your environment — is where traditional detection and response systems fail. XDR solutions can dramatically improve this process with investigation and response capabilities that include the following:

- **Correlation and grouping of related alerts and telemetry data:** When it comes to attacks against your organization, time is of the essence. By the time you receive a threat alert, the attacker is already hard at work carrying out their mission and achieving their objectives in your environment. You need to be able to quickly understand the attack and its full causality chain. This means your XDR tool must first reduce noise by automatically grouping related alerts and effectively prioritizing the events that most urgently require your attention. Then your XDR tool must be able to build a timeline of the attack, stitching together activity logs from your network, endpoint, and cloud environments. By visualizing the activity and sequencing events, the root cause of the threat can be determined, and the potential damage and scope can be assessed (see Figure 2-2).

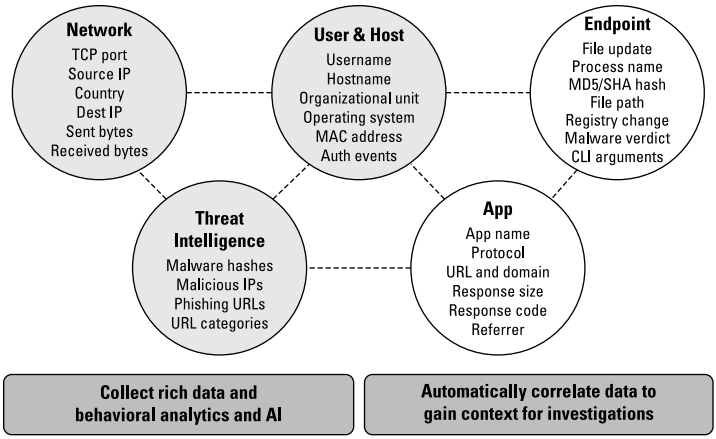

FIGURE 2-2: XDR collects data from any source, correlating and stitching it together for better detection and hunting.

- **Swift investigation into incidents with instant access to all forensic artifacts, events, and threat intelligence in one location:** Quickly pinpoint attacker activity by reviewing key artifacts such as event logs, registry keys, browser history, and much more. Single-purpose agents for forensics, endpoint protection, and detection and response can bog down performance and add complexity. To resolve an incident, you need to find the entry point and track down remnants — even if adversaries tried to cover their tracks.
- **Consolidated user interfaces with the ability to pivot quickly:** When they start digging into alerts, your security analysts need a streamlined work environment that enables them to understand the root cause of alerts from any source with a single click. Analysts shouldn't have to waste time switching between multiple different tools.
- **Manual and automated threat hunting:** An increasing number of organizations proactively hunt for active adversaries, allowing their analysts to develop attack hypotheses and look for relevant activity within the environment. Supporting threat hunting requires powerful search capabilities to look for evidence to prove the hypotheses, as well as integrated threat intelligence to search for activity already seen within the extended network. This threat

intelligence should be integrated and automated in a way that makes it clear whether a threat has been seen before without requiring tons of manual analyst work (for example, opening 30 different browser tabs to search numerous threat intelligence feeds for a known malicious IP address).

- **Coordinated response:** After threat activity has been detected and investigated, the next step is efficient and effective remediation and policy enforcement. Your system must be able to coordinate a response to active threats and prevent future attacks across your network, endpoint, and cloud environments. This includes communication between prevention technologies (that is, an attack blocked on the network automatically updates the policies on the endpoints), either natively or built through application programming interfaces (APIs). It also includes the ability for an analyst to take response actions directly through the XDR interface.

TIP

Look for the following investigation and response capabilities in an XDR solution:

- Automated root cause analysis of any alert, including network alerts, if endpoint data is available
- Visualization of the chains of execution leading up to an alert
- Timeline analysis view to see all actions and alerts on a timeline
- Querying for indicators of compromise (IOCs) and endpoint behaviors, online and offline hosts, network traffic logs from firewalls, and authentication logs from identity management providers
- Advanced querying language with support for wildcards, regular expressions, JSON, data aggregation, field and value manipulation, merging of data from disparate sources, and data visualization
- Ability for an analyst to easily pivot between views with granular filtering and sorting of query results
- Automatic aggregation of relevant Internet Protocol (IP) or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations and block access to malicious IP addresses or domains

- Identification of whether an event was blocked by an endpoint agent, firewall, or another prevention technology and remote ability to view, suspend, or terminate running processes or download binaries
- Automated stitching of security alerts, such as firewall alerts, to endpoint data
- Noise cancellation and removal of non-significant binaries and dynamic-link libraries (DLLs) from chain
- SOC analyst context of tactics, techniques, and procedures (TTPs) to utilize knowledge gained to help in future investigations
- Integration with security orchestration, automation, and response (SOAR) and security information and event management (SIEM) solutions
- Incident scoring allowing ranking and prioritization of high-risk incidents to swiftly zero in on the most critical threats; creating incident scores based on alert attributes, including the users or hosts in an alert
- Quarantining malicious files and removing them from their working directories
- Swiftly finding and deleting files across your organization in real time by indexing endpoint files
- Directly accessing endpoints to run Python, PowerShell, or system commands or scripts; reviewing and managing active processes; and viewing, deleting, moving, or downloading files

Improving Security Effectiveness

XDR significantly reduces the overall costs of handling incidents. It also minimizes financial damage and loss by improving threat coverage. This means increasing the efficiency and effectiveness of your security team to help prevent or overcome staffing shortages, improving the integration between your existing tools to extend their value, and strengthening your prevention efficacy over time with scalable infrastructure and artificial

intelligence (AI). To meet these criteria, XDR must have the following capabilities:

- **Data ingestion from any source:** Every organization today has a mixed bag of disparate, siloed security tools. The more an XDR solution is able to have visibility into data from each of those different tools, the more comprehensive the security it will be able to provide. The best XDR solutions will have the flexibility to ingest data from the other tools in your environment to maximize both value and effectiveness.
- **Scalable storage and compute:** Given the persistence of today's threat actors, you don't want to discard telemetry that may provide important forensic evidence of attacker activity in "low and slow" attacks that may last for months or even years. You also need the analytics horsepower to be able to utilize all this telemetry effectively. Cloud-based XDR platforms provide this practically unlimited accessibility and scale.
- **Improvement over time:** Detecting increasingly sophisticated attacks requires embedded AI and machine learning, as well as automation and orchestration to reduce manual efforts and enable security analysts to be more effective and efficient. XDR solutions should learn from experience, reducing future risk and continually strengthening prevention by applying knowledge gained through detection, investigation, and response.
- **Simplified deployment:** Security teams should be able to quickly install XDR agents to all their endpoints, including Windows, macOS, Linux, Chrome OS, and Android systems. XDR agents need to protect all digital assets, including mobile devices and private, public, hybrid, and multi-cloud environments. To ensure security scales along with cloud workloads, XDR solutions should support frictionless Kubernetes deployment.
- **Reporting and dashboards:** Security teams need to be able to understand and communicate the organization's security posture and operational metrics. XDR solutions should be capable of providing better security outcomes and summarizing the state of security through intuitive and customizable reports and dashboards.

FRIEND OR FAUX? DEFINING TRUE XDR

XDR is gaining acceptance and traction in the industry by the analyst community, security vendors, and end users at large, but like other security solution categories, it comes in a range of "flavors." And because some XDR "flavors" are simply a rebranding of endpoint detection and response (EDR), vendors don't necessarily share the same capabilities. It pays to pay attention.

So, how can you distinguish between the various options available on the market to determine whether a solution is true XDR as opposed to another vendor hopping on the XDR bandwagon? The following specifications, though not exhaustive, can help separate the winners from the wannabes.

A true XDR solution:

- Should be able to take in, normalize, and process data from all data sources (including third-party data sources)
- Should provide stitching of data, not just a simple correlation of data
- Is cloud native and can effectively scale to an infinite degree
- Natively stitches together network, endpoint, identity, and cloud data into a single "story" or integrated log record for cross-data analytics
- Applies intelligent, advanced logic to show the complete story of an incident in a single view
- Automatically maps evidence and artifacts to the MITRE ATT&CK framework
- Provides a built-in capability to perform deep forensic analysis
- Is backed by world-class security research and security services teams

Does the solution take a prevention-first approach?

XDR is "extended detection and response," and its strength lies in the ability to interoperate at a deep level of integration with devices that can block, disrupt, and contain threats and attacks before any

(continued)

(continued)

damage occurs. The most important of these devices are next-generation network firewalls and endpoints because the network represents the complete record of communications and endpoints and how users interact with all applications and data.

Does the solution base detections only on the endpoint?

Can the solution detect attacks based on identity, cloud, and network data, including between unmanaged devices? Some "XDR" vendors will say they see network data when what they really mean is network traffic collected from endpoint agents.

A true XDR will allow any data to be correlated with threat activity and tagged with MITRE ATT&CK TTPs to help provide a more detailed picture of adversarial movement.

Does the solution have native investigation and response capabilities?

A true XDR:

- Uses security analytics to automate response recommendations
- Allows for native response actions on the endpoint
- Can support, but does not require, integrations with other tools like SOAR for response
- Enables response across endpoint network and cloud enforcement points instead of endpoint only
- Allows native support for ad-hoc searching across all third-party data sources using analyst-optimized investigative and hunting methods
- Optimizes triage and investigations by surfacing all related malicious artifacts, hosts, users, and correlated alerts, mapped to MITRE ATT&CK
- Can provide smart recommendations for targeted response actions based on MITRE ATT&CK

IN THIS CHAPTER

- Taking a closer look at the attack life cycle
- Exploring an example of a multifaceted attack

Chapter 3
Breaking the Attack Life Cycle with XDR

Threat actors have evolved from direct attacks against a high-value server or asset ("shock and awe") to a patient, multistep process that blends exploits, malware, stealth, and evasion in a coordinated network attack ("low and slow").

In this chapter, you learn about the attack life cycle and how extended detection and response (XDR) helps you break the life cycle to stop attacks against your environment. This chapter outlines a general representation of the common stages of an attack. Many security teams have adopted the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework to help them track threats at various stages of an attack. A true XDR should be able to detect every step an adversary makes and map each step to MITRE ATT&CK tactics and techniques to simplify investigations.

Understanding the Attack Life Cycle

The attack life cycle illustrates the sequence of events (or steps) that an attacker goes through to infiltrate a network and exfiltrate (or steal) valuable data. These steps include the initial vulnerability exploit, malware installation, command and control, lateral movement, and exfiltration (see Figure 3-1).

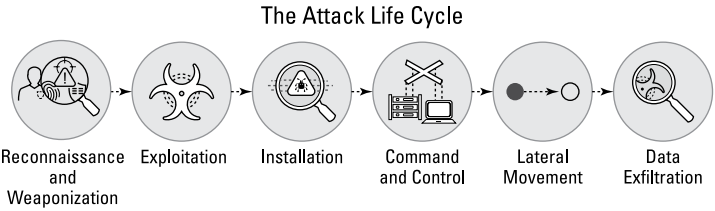

FIGURE 3-1: Successful attacks require multiple steps.

TIP

If you can detect steps earlier in the life cycle, you can stop attackers from executing later stages of an attack. The following sections take a closer look at the attack life cycle and how XDR helps you break that life cycle.

Reconnaissance

Threat actors meticulously plan their attacks. They research, identify, and select targets, often extracting public information from targeted employees' social media profiles or from corporate websites, which can be useful for social engineering and phishing schemes. Attackers also use various tools to scan for network vulnerabilities, services, and applications that they can exploit, such as network analyzers, network vulnerability scanners, password crackers, port scanners, and web application vulnerability scanners.

XDR breaks the life cycle during reconnaissance through continuous monitoring and inspection of network traffic flows to detect and prevent unauthorized port and vulnerability scans, host sweeps, and other suspicious activity.

Weaponization

Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a Microsoft Word document or email message. Or, for highly targeted attacks, attackers may customize deliverables to match the specific interests of an individual within the target organization. Attackers next try to deliver their weaponized payload to a target endpoint, for example, via email, instant messaging (IM), drive-by download (in which an end user's web browser is redirected to a web page that automatically downloads malware to the endpoint in the background), or infected file share.

Breaking the life cycle at this phase of an attack is challenging because weaponization typically occurs within the attacker's

network. However, analysis of artifacts (both malware and weaponizer) can provide important threat intelligence to enable effective zero-day protection when delivery is attempted. XDR provides visibility into all network traffic to effectively block malicious or risky websites, applications, and Internet Protocol (IP) addresses, and prevent known and unknown malware and exploits.

Exploitation

After a weaponized payload is delivered to a target endpoint, it must be triggered. An end user may unwittingly trigger an exploit, for example, by clicking a malicious link or opening an infected attachment in an email, or an attacker may remotely trigger an exploit against a known server vulnerability on the target network.

Breaking the life cycle at this phase of an attack requires XDR capabilities including the following:

- Vulnerability and patch management
- Malware detection and prevention
- Threat intelligence (including known and unknown threats)
- Blocking risky, unauthorized, or unneeded applications and services
- Logging and monitoring all network, endpoint, and cloud activity

An effective XDR agent prevents known, zero-day, and unpatched vulnerabilities by blocking the exploitation techniques attackers use to manipulate applications. Although there are thousands of exploits, they typically rely on a small set of exploitation techniques that change infrequently. By blocking these techniques, XDR prevents exploitation attempts before endpoints can be compromised (see Figure 3-2).

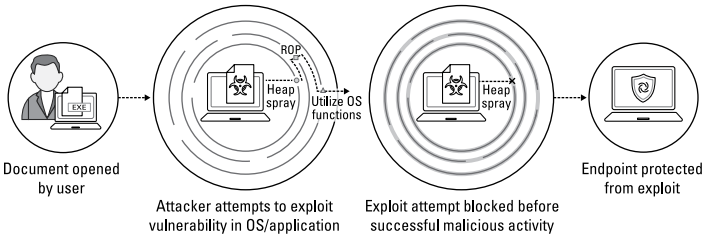

FIGURE 3-2: An advanced XDR solution focuses on exploit techniques and behaviors rather than the exploits themselves.

Installation

Next, an attacker will escalate privileges on the compromised endpoint (for example, by establishing remote shell access and installing rootkits or other malware). With remote shell access, the attacker has control of the endpoint and can execute commands in privileged mode from a command-line interface (CLI), as if physically sitting in front of the endpoint. The attacker will then move laterally across the target's network, executing attack code, identifying other targets of opportunity, and compromising additional endpoints to establish persistence.

The key to breaking the life cycle at this phase of an attack is to prevent installation on the endpoint and limit or restrict the attackers' lateral movement within the network. XDR leverages endpoint detection and response (EDR) and endpoint protection platform (EPP) technologies to prevent installation. XDR also monitors and inspects all traffic between zones or segments in a Zero Trust model and provides granular control of applications that are allowed in the environment.

Command-and-control

Threat actors establish encrypted communication channels back to command-and-control servers across the Internet. This approach allows them to modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, as well as evade any new security countermeasures that the organization may try to deploy if attack artifacts are discovered. Communication is essential to an attack because it enables the attacker to remotely direct the attack and execute the attack objectives. Command-and-control traffic has to be resilient and stealthy for an attack to succeed.

Breaking the life cycle at this phase of an attack requires the following:

- Inspecting all network traffic (including encrypted communications)
- Blocking outbound command-and-control communications with anti-command-and-control signatures (along with file and data pattern uploads)

- Blocking all outbound communications to known malicious Uniform Resource Locators (URLs) and IP addresses
- Blocking novel attack techniques that employ port evasion methods
- Preventing the use of anonymizers and proxies on the network
- Monitoring the Domain Name System (DNS) for malicious domains and countering with DNS sinkholing or DNS poisoning
- Redirecting malicious outbound communications to honeypots to identify or block compromised endpoints and analyze attack traffic

Lateral movement and exfiltration

Attackers often have multiple, different attack objectives, including data theft; destruction or modification of critical systems, networks, and data; and denial of service (DoS). This last stage of the life cycle can also be used by an attacker to advance the early stages of the attack against another target. For example, an attacker may compromise a company's extranet to breach a business partner that is the primary target. These types of supply chain attacks became headline news in 2020 with the SolarWinds attack.

Breaking the life cycle at this stage requires XDR tools that can automatically detect and prevent data exfiltration and other malicious or unauthorized actions.

Looking at an Attack Example

To help visualize all the steps of the attack life cycle and their role in an attack, let's take a closer look at a hypothetical attack. In Figure 3-3, a threat actor executes the following steps to attack a target:

1. Exploitation.

   The attacker exploits bugs on the web server to take control of the server.

2. Installation.

   The attacker uses the control of the server to install mimikatz and get access to admin credentials.

3. Command-and-control.

   The attacker installs additional malware and remote access tools to establish persistence and command-and-control communications.

4. Lateral movement.

   The adversary moves laterally across the network, compromises multiple endpoints, and accesses private and public cloud applications.

5. Access and exfiltration.

   The attacker looks at the configuration files on the server, finds the backend database location, queries the database, and saves the results to a local file. Collected data is uploaded to an "authorized" or "sanctioned" cloud storage location. The attacker then deletes the file that contains the data from the database, clears the local logs, and closes the session.

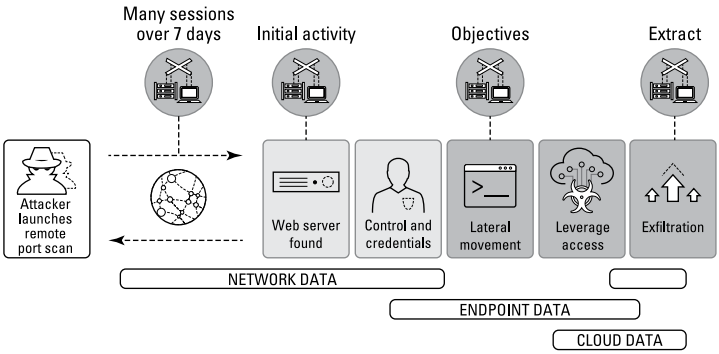

FIGURE 3-3: XDR can uniquely stop these advanced, multistep attacks because it collects data from every source and can detect and stop attack tactics other tools miss.

An XDR platform gathers and analyzes multiple types of data to detect and stop adversary tactics across the attack life cycle.

IN THIS CHAPTER

- Detecting threat activity with XDR
- Managing and validating alerts
- Accelerating investigations and response
- Enabling proactive threat hunting

Chapter 4
Exploring XDR Use Cases

In this chapter, I introduce the most common use cases to help your organization improve its detection and response capabilities, including detection, alert triage and validation, automation of investigations and response, and threat hunting.

Detection

To stop successful cyberattacks, you should focus on detecting attacks at each stage of the attack life cycle. Extended detection and response (XDR) uses machine learning to discover the unique characteristics of your organization, allowing it to differentiate between threat activity and normal activity, beyond what's possible with manual analysis or static correlation rules. This machine learning fuels advanced analytics, profiling, and behavioral threat detection. Through this comprehensive detection, an XDR solution improves the ability to detect nefarious activity, including targeted attacks, malicious insiders, and more.

Targeted attacks

Attackers try to blend their activities in with legitimate usage at every stage in the attack life cycle. With XDR's ability to collect data from any source for detection and automatically stitch together key security data for advanced cross-data analytics, you can detect the stealthiest attacks. With analytics, you can

profile user behavior and pinpoint anomalous behavior, such as an attacker's attempts to compromise devices and move laterally on the network, looking for and exfiltrating sensitive data.

Malicious insiders

Malicious insiders use their trusted credentials and access to steal corporate data without being detected. XDR addresses this threat by looking for anomalies in user behavior and activity (see Figure 4-1). XDR solutions can streamline analysis by presenting a 360-degree view of each user with a clear risk score.

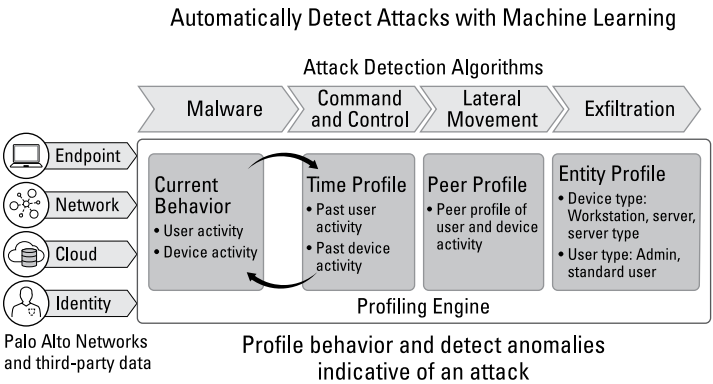

FIGURE 4-1: Behavioral analytics discover anomalies at the user, application, and device level.

Inadvertent risk

Well-meaning employees can inadvertently expose organizations to undue risk through abuse and misuse of authorized access. An XDR solution allows organizations to follow security best practices by monitoring user activity and identifying risky behavior to detect when an employee is violating security policies — whether inadvertently or not.

Compromised endpoints

Attackers often use malware to infiltrate targeted networks by compromising an endpoint and moving laterally through the network. XDR brings security data together across networks and endpoints to look for anomalous traffic generated by malware and other nefarious activity. This security data also provides the means to investigate across the environment to determine the extent of the attack.

For example, if a threat actor adds a new value to the Autorun registry key, an XDR solution could detect the new Autorun value and generate an alert with a clear description of this suspicious activity, including rich investigative context with the MITRE ATT&CK tactic and technique. The XDR solution could even determine which process added the Autorun value and the sequence of events that led to the update to provide a complete story of the attack.

REMEMBER

XDR detects active attacks with unparalleled precision and increases the ability of security teams to:

- Detect malicious activity from both internal and external resources by finding patterns among activity happening on the network, at endpoints, and within the cloud.
- Utilize cutting-edge analytical techniques on significant amounts of security data to identify abnormal activity without increasing the level of false positives.
- Leverage internal response and external threat intelligence to learn from past attacks and make that experience accessible to less sophisticated analysts, improving the performance of the entire security team.

Alert Triage and Investigation

XDR solutions simplify alert triage and analysis by revealing the root cause of alerts, making them much faster to investigate. If only endpoint data is available, then the endpoint root cause is presented. If network and endpoint data are available, then the XDR platform can associate network activity with endpoint events automatically. For example, not only does XDR determine which endpoint executable was responsible for a network alert, it can figure out which application launched the executable.

Given the challenges presented by the security skills gap discussed in Chapter 1, XDR improves the ability of a less experienced analyst to detect and validate a potential attack by grouping alerts into incidents and, within those incidents, summarizing activities or actions into tags that add context. This flexibility ensures that knowledge is captured and leveraged for the entire team.

XDR produces a timeline of the events leading to the alert and provides integrated threat intelligence. All of this allows analysts

to understand the root cause of an alert, the exact nature of the threat, and what action to take.

Here's how XDR helps simplify incident analysis and investigations:

1. Assessment.

   The process starts with the XDR solution evaluating both external alerts (such as from third-party security tools) and internally generated alerts (based on rules and other indicators) to determine potentially suspicious behavior.

2. Prioritization.

   The XDR tool then automatically groups those alerts into incidents, assigning a priority level to each incident in order to direct analysts to the incidents that pose the greatest threat. Analysts can click into each incident and see the full list of alerts, devices, associated threat intelligence, and other context to help understand the full extent of the alert.

3. Analysis.

   XDR provides a visual attack chain (see Figure 4-2), leveraging the various sources of telemetry to collect anything and everything that's relevant to the incident and providing additional context, causality, and to ensure faster and better analysis. The attack chain shows the steps an attacker took by revealing the sequence of processes that led to the final attack step. Besides displaying the associated alerts, including an EPP alert for the XDR agent, it also identifies the root cause.

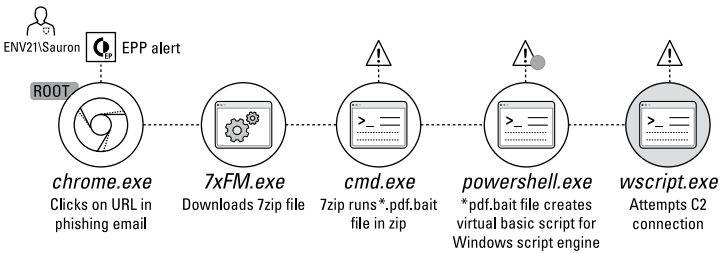

FIGURE 4-2: An example of a visualized attack chain using XDR.

4. Enrichment.

   The attack chain is then enriched with additional contextual information, including a play-by-play view of how the alert was generated; its root cause; other involved endpoint, network, and cloud devices; and the reputation of all forensic artifacts.

With thousands of alerts coming through each day, automating the triage process and providing analysts with enriched contextual information is the only way to manage the volume. With XDR, security teams can focus their time and energy where it will have the greatest impact — on remediating alerts with the potential to cause the most damage.

REMEMBER

With XDR, analysts have an increased ability to:

- Cut down on their alert backlog with incident management, intelligent alert grouping, and investigative context.
- Dramatically reduce the chance of a missed attack.
- Analyze alerts to improve detection, as well as ensure that downstream productivity and defenses are not adversely impacted.
- Apply new behavioral triggers to improve triage times, and optionally transform detection rules into prevention rules for closed-loop prevention.

Automated and Simplified Investigations and Response

After an alert has been triaged and prioritized, a more in-depth investigation is warranted. The automation of XDR accelerates the investigation process of any alert or hunting campaign, eliminating time-consuming manual tasks by providing a clear picture of the threat, performing root-cause analysis, verifying reputation, and resolving attack attribution.

XDR tools begin by aggregating all telemetry within a security data repository, such as a cloud data lake (see Figure 4-3). To reduce investigation time, the XDR solution can correlate and group alerts from across detection tools into a small number of accurate, actionable incidents, including information about the user, application, and device. XDR can also aid forensics investigations by interrogating endpoints to determine which process or executable initiated an attack.

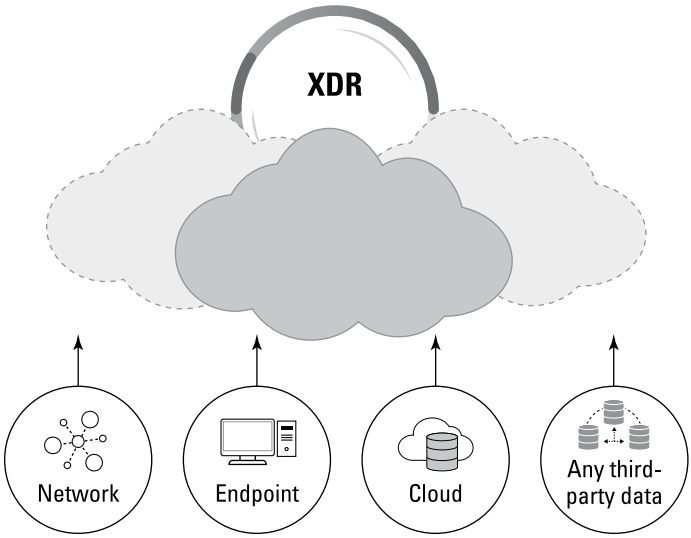

FIGURE 4-3: XDR tools stitch together data from different sensors in a cloud-based data repository.

To dig deeper into the incident, an XDR solution then determines whether the endpoint process is malicious. It does this by integrating with threat intelligence sources and services to analyze the process. An XDR solution makes it easy for security analysts to verify attacks by presenting all the information they need in a single interface.

XDR tools can also adapt defenses, applying knowledge from previous incidents and hunting campaigns to automatically prevent the successful recurrence of any threat previously found. This "assisted learning" allows early detection of attacks based on what has already been seen in the environment.

After the threat has been validated, incident responders can then choose from dozens of remote response and remediation techniques to stop the attack, prevent follow-on attacks, restore damaged or deleted files, and more. Response options include isolating endpoints, blocking, deleting, or quarantining files, reverting files and registry to a clean state, directly accessing endpoints, and executing scripts. The security team will become highly efficient, require less training, reduce the burden on more experienced incident responders, and minimize incident resolution times.

REMEMBER

With XDR, incident responders have an increased ability to:

- Find stealthy threats faster by leveraging threat intelligence and behavioral analytics.
- Simplify and speed up investigation and response by providing deep and extensive searches of telemetry gathered from networks, endpoints, and the cloud.

Threat Hunting

XDR solutions improve your threat-hunting capabilities through both automated and ad-hoc identification of malicious activity across your environment. Threat hunters can perform advanced queries and get instant results. Some examples of how XDR provides the necessary capabilities to support different methods of threat hunting include

- **Intel-based:** This is the most common type of threat hunting exercise, where the hunter has been given a clue about a potential threat before looking for it. Whether it's a lead from threat intelligence, newfound indicator of compromise (IOC), tip from someone within the organization, or mere suspicion, the complexity of intel-based threat hunting will depend on the level of detail the intel provides. Drawing from an integrated data source that is linked to multiple threat intelligence providers, an XDR solution can manually import artifacts or IOCs from different standards to provide fast and robust search results.
- **Leadless-based:** A close second in terms of common approaches to threat hunting, leadless is where the hunter uses their own or sought-after knowledge of how a computer, application, user, data, or network is meant to be used and aims to identify anomalous or abnormal use. This type of advanced threat hunting is typically left to the most experienced team members who use techniques such as data carving and analytics to achieve results. An XDR solution simplifies this process by building these advanced techniques into its interface, allowing hunters of any experience level to leverage these techniques without scripts, additional tools, or the need to learn a new query language.

- **Outcome-based:** In this approach, the hunter looks into past quarantined alerts, completed investigations, or any other resolved threats and uses these to identify variants of the threat, potential new threats, or open attack vectors. A quality XDR solution can automatically and continuously incorporate outcome-based threat hunting directly into the workflow of security alerts and incident handling. Lessons learned from every investigation are applied to ensure you don't get hit by repeat attacks.
- **Compliance-based:** This threat-hunting approach is focused on ensuring compliance with internal, industry, and government requirements by performing routine searches that indicate noncompliance, such as sensitive data stored on unauthorized systems or escalation of privileges by admin users. An XDR solution can be configured to alert security analysts of this type of activity and provide a means to quickly investigate the situation.
- **Machine learning–based:** Machine learning systems baseline the typical behaviors of an organization to understand what's normal and what isn't. Using large-scale analytics, XDR solutions use machine learning to monitor behaviors and identify anomalies that deviate from these baselines. These behavioral indicators of compromise (BIOCs) pick up on many stealthy threats that an analyst may not be able to identify manually and are continually optimized over time to improve the machine learning model. This form of threat hunting represents the ultimate time savings for analysts and is critical for optimizing security outcomes.

REMEMBER

With XDR, threat hunters have an increased ability to:

- Take advantage of network, endpoint, and cloud data for searches and analysis.
- Leverage automation to hunt across all network, endpoint, and cloud activity.
- Use highly configurable searches and wizards to find both internal and external threats identified by traditional IOCs and BIOCs stored within your threat library.
- Remediate attacks via integration with security controls.

IN THIS CHAPTER

- Ensuring robust threat prevention and complete visibility
- Simplifying investigations with analytics, machine learning, coordinated response, and orchestration features
- Maximizing flexibility with a full protection suite
- Looking at third-party validation, innovative road maps, and total value

Chapter 5
Ten Key XDR Capabilities and Features

Extended detection and response (XDR) enables organizations to prevent successful cyberattacks and simplify and strengthen their security processes using a proactive approach to threat detection and response. XDR stops modern attacks by gathering and analyzing data from any source. It unifies prevention, detection, investigation, and response to deliver unparalleled security and operational efficiency.

This chapter lays out ten "must-haves" to look for in an XDR solution for your organization. It also explains how Cortex XDR, the industry's first extended detection and response platform, delivers these essential features.

Best-in-Class Endpoint Threat Prevention

Protecting your organization starts with best-in-class endpoint threat prevention that blocks known and unknown malware, ransomware, fileless attacks, and exploits.

REMEMBER

Cortex XDR provides everything you need for threat prevention, detection, and response with a single agent managed from the cloud. It safeguards your endpoints with industry-best, artificial intelligence (AI)–driven local analysis and behavior-based protection (see Figure 5-1).

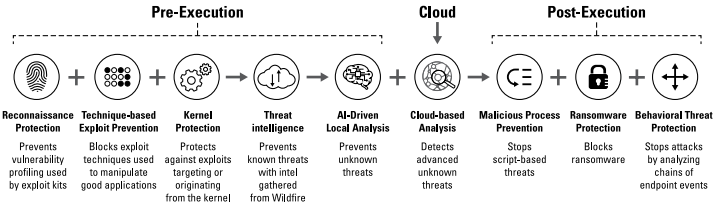

FIGURE 5-1: Cortex XDR provides complete endpoint threat prevention.

Look for next-generation antivirus that provides

- Malware, ransomware, and fileless threat protection
- Cloud-based real-time global threat intelligence
- Local analysis via machine learning
- Behavioral threat protection
- Granular child process protection
- Pre-exploit and technique-based exploit prevention
- Kernel exploit prevention
- Credential theft protection

Flexible Suite of Endpoint Protection Features

You need an easy way to identify and prioritize endpoint risks, reduce your attack surface, and stop data loss. Look for endpoint protection features, including the following:

- **Vulnerability assessment:** Take advantage of vulnerability assessment, application visibility across managed and unmanaged endpoints, and more to get an enterprise-wide view of your digital assets.
- **Host firewall:** Centrally manage inbound and outbound communications on your endpoints from the Cortex XDR management console.
- **Disk encryption:** Apply encryption or decryption policies on your endpoints and view lists of all encrypted drives.
- **Device control:** Monitor and granularly control Universal Serial Bus (USB) access to protect your endpoints.

Extended Visibility across Data Sources

To reduce the risk of a successful attack, you need a holistic approach to detection and response that eliminates blind spots, increases accuracy, and streamlines investigations across all environments, including network, cloud, and endpoint.

TIP

Cortex XDR is the industry's first XDR platform that natively integrates endpoint, network, and cloud data to stop sophisticated attacks. Cortex XDR delivers all the capabilities of network detection and response (NDR), endpoint detection and response (EDR), endpoint protection (EPP), cloud detection and response (CDR), and user and entity behavior analytics (UEBA), as shown in Figure 5-2.

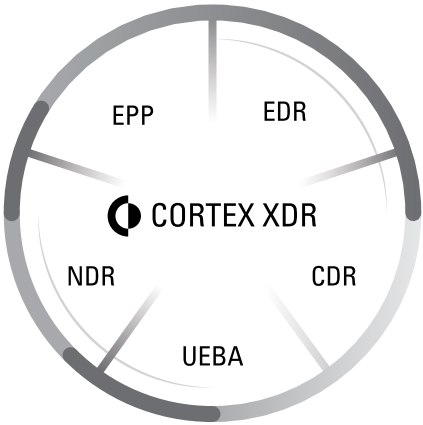

FIGURE 5-2: Cortex XDR gathers and analyzes rich data to deliver the capabilities traditiionally provided by EPP, EDR, NDR, CDR, and UEBA tools.

Simplified Investigations

Today's siloed security tools generate endless alerts with limited context. According to the Ponemon Institute's 2020 *Cost of a Data Breach Report,* the average time to identify and contain a breach is 280 days. To reduce response times, security tools must provide a complete picture of incidents with rich investigative details.

TIP

Cortex XDR simplifies investigations by automatically revealing the root cause, sequence of events, and threat intelligence details of alerts. It reduces investigation time 88 percent by revealing the root cause and rich context of network, endpoint, and cloud alerts, and reduces alerts by 98 percent with intelligent alert grouping and deduplication.

Analytics and Machine Learning

Threat actors leverage cloud and machine learning technologies to increase the scale and effectiveness of their attacks. You need a comprehensive set of machine learning and analytics techniques to stay ahead of rapidly evolving threats and counter sophisticated attacks.

REMEMBER

Cortex XDR provides

- AI-driven local analysis to block malware
- Behavioral analytics to detect intrusions and active attacks
- Global analytics to improve detection accuracy and coverage

Coordinated Response

After you identify threats in your environment, you need to contain them quickly. Your team needs integrated and flexible response options to shut down attacks rapidly and effectively before they can do more damage. An XDR solution must enable your team to remotely stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists, such as bad domains, through tight integration with enforcement points.

TIP

Cortex XDR lets your security team instantly eliminate network, endpoint, and cloud threats from one console.

Automation of Security Tasks

Manual tasks and processes slow down incident response and increase the cost of security operations. Executing a range of response actions natively to the endpoint and to other key enforcement points, XDR solutions can swiftly contain threats. Advanced SOCs may require processes that include decision logic and workflow orchestration controlled by playbooks and include range of actions across a wide range of security and IT tools from different vendors. A full-featured security automation and orchestration solution that provides orchestration logic and has extensive partner integrations and prebuilt content and playbooks can address these requirements. Therefore, look for an XDR solution that tightly integrates with an industry-leading SOAR platform.

REMEMBER

Cortex XDR tightly integrates with Cortex XSOAR for complete threat intelligence management and offers more than 750 partner integrations and 680 content packs so you can take your security operations to the next level.

Independent Testing and Validation

When choosing an XDR solution, you should always review third-party testing, analyst validation, and customer testimonials to get an independent and objective perspective.

TIP

Cortex XDR has achieved exceptional test results including achieving the best combined detection and protection in the MITRE ATT&CK round 3 evaluation, and a "Strategic Leader" rating in the AV-Comparatives Endpoint Prevention and Response (EPR) test. Garnering praise from customers and reviewers alike, Cortex XDR can be trusted to protect your endpoints and data.

Rapid Pace of Innovation

To outpace fast-moving adversaries, look for vendors that continuously strengthen or expand their products' capabilities.

TIP

Cortex XDR continues to redefine how security operations teams address complex modern threats and drive greater efficiencies. By tackling the system integration problem of gathering, integrating, and analyzing data and coupling that with the ability to kick off highly optimized and automated workflows, XDR helps solve the challenges of detection, investigation, and response at scale in a consolidated manner.

Unparalleled Return on Investment

When selecting a key element of your security infrastructure, you want to make sure it will provide real value that can be easily demonstrated for your stakeholders.

REMEMBER

Cortex XDR lowers total cost of ownership (TCO) by 44 percent, on average, compared to traditional tools, by:

- Leveraging your existing security tools as sensors for detection and response
- Eliminating on-premises log servers with cloud deployment
- Simplifying operations with data stitching, alert grouping, and root cause analysis

Improve your security operations effectiveness with extended detection and response (XDR)

Security teams face a dizzying array of threats, from ransomware to fileless attacks and data breaches. However, the biggest headache for many security analysts is not the endless number of attacks that dominate news headlines, but rather the repetitive tasks they must perform every day as they triage events and attempt to whittle down an endless backlog of alerts. Extended detection and response (XDR) is a new approach to threat detection, investigation, and response that integrates and analyzes data from any source.

Inside…

- Recognize limitations in current approaches
- Address cybersecurity staff shortages
- Ensure robust threat prevention
- Enable complete visibility
- Automate investigations and response
- Improve security effectiveness
- Protect network, endpoint, and cloud resources

paloalto NETWORKS

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

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

ISBN: 978-1-119-85169-1
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.