XDR: Extended Detection and Response

Everything you need to know about the market category that is unifying data silos and reshaping security operations

paloalto NETWORKS | CORTEX XDR BY PALO ALTO NETWORKS

Table of Contents

Introduction

Year after year, the challenge of securing critical data intensifies. Evolving technology trends, including the recent growth in cloud and IoT adoption, continue to expand the enterprise cyberattack surface and make companies' sensitive data more vulnerable to sophisticated attackers. At the same time, adversaries use those exact tools to increase their own power and scale, allowing them to efficiently wage repeated attacks—and they only need to succeed once. Future technologies threaten to exacerbate both of these problems.

Security teams have deployed tools, processes, and staffing models to respond to new threat vectors as they have emerged, but they are outnumbered and outgunned. The consequence of continually bolting new capabilities onto existing systems over time is an eventual mess of poorly integrated tools that require a lot of time, energy, and experience to utilize. Junior analysts are charged with the impossible task of triaging a never-ending stream of security alerts despite limited training and equally limited toolkits. The combination of too many alerts and too little context causes security teams to lose visibility and become less agile than their adversaries. Ultimately, the company becomes even more vulnerable as a result.

"XDR" emerged as a market category in response to this complexity, the basic premise being a simple one: XDR is a category of threat detection, investigation, and response solutions that work across all threat vectors in a company's infrastructure (i.e., network, endpoint, and cloud), rather than just one piece thereof. By increasing integration, XDR tools also increase visibility and insight for both for the machine learning models powering them and the security analysts using them.

> **"Cybercrime is the greatest threat to every company in the world."**
>
> **Source: Ginni Rometty, CEO, IBM**

About This Guide

Need to get up to speed on the XDR category and what it means for your company? You've come to the right place. We will define XDR, describing its key capabilities, applicable use cases, and impact on key security operations functions. By the end of this guide, you will have a clear understanding of what XDR is and what it is not; the advantages it has over legacy detection and response tools; which capabilities to look for when evaluating XDR solutions; and how XDR can help to simplify and improve your security operations.

The Challenge

Reports of data breaches and attacks from sophisticated adversaries have become so frequent that society has become numb to them. In the business world, it's become an accepted reality and running joke that "you have adversaries in your environment, whether you know it or not." The fact that adversaries are commonplace does not, however, make them less dangerous. The truth is that every minute an active adversary operates within your environment, untold damage occurs. As a security operations professional, you already know this and doubtless work hard to detect attacks and respond as quickly and effectively as possible—before data loss can occur.

This is an uphill battle in the face of increasingly advanced attacks and tactics used by adversaries. Attackers can now compromise devices without using file-based malware at all. Sophisticated attackers use different approaches, such as compromising authorized system files, inserting attacks into a device's registry, or using utilities like PowerShell maliciously. This has driven the need for new methods of detection.

Almost 4 million digital records are stolen from breaches every day.

Source: Cybersecurity Ventures

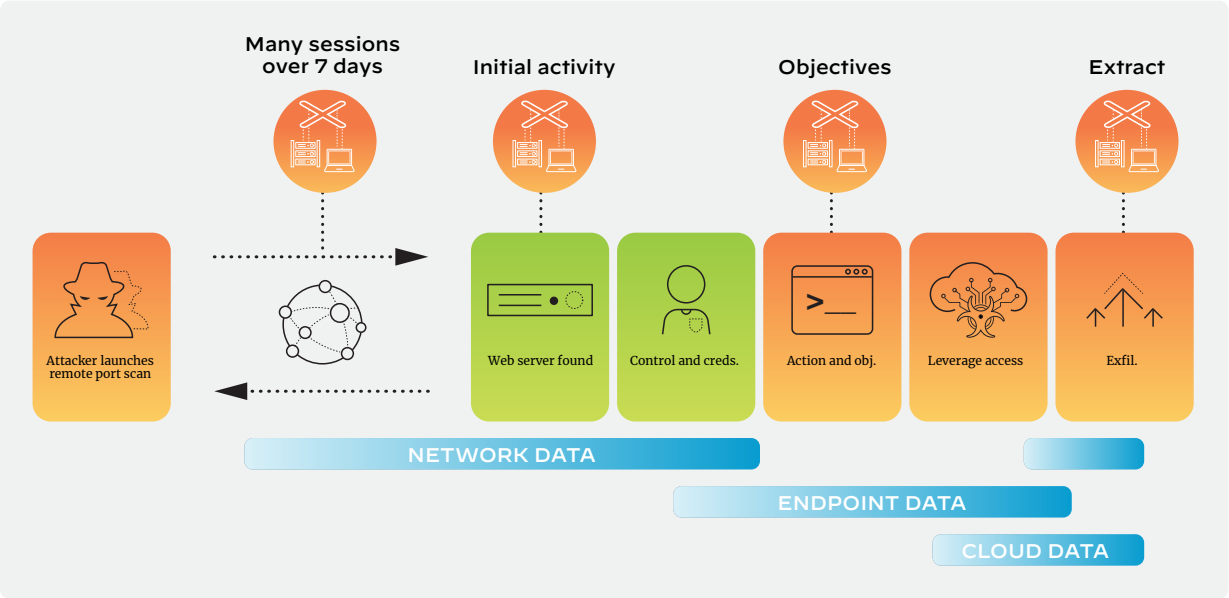

Figure 1: Example of a multi-stage attack

Further complicating matters is the continued investment in new technologies like the cloud and internet of things (IoT) to move faster, increase agility, and use data in new ways. Each of these new technologies gives attackers additional ways to enter and exploit your infrastructure. Your security team must employ the best prevention possible, optimize the ability to locate adversaries, decrease the time those adversaries dwell in your environment, and accelerate the response to the incident.

The Elusive Balance

An organization's ability to achieve these objectives relies on two things: effective tools and a team of capable security analysts. Unfortunately, having the proper balance of technology and human capital tends to be the exception rather than the rule.

Detection and prevention technologies generate hundreds or thousands of alerts per day—far exceeding the amount security teams are staffed to handle. These alerts come from many disconnected sources, leaving analysts to piece the puzzle together. Analysis of a potential threat generally requires a number of steps:

1) Review available log data to start piecing together what may have occurred.

2) Manually compare against threat intelligence sources to determine if indicators are known to be malicious.

3) Find information gaps and search for available data that may indicate additional steps in the attack.

4) Check if new information links to alerts being handled by other team members to coordinate efforts.

5) Evaluate whether the alert needs to be escalated, discarded, or quickly remediated and closed out.

69% of organizations don't trust their anti-virus software to block threats to their environments.

Source: Ponemon Institute

All of these steps traditionally take a lot of time and multiple tools to complete—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.

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

Many organizations attempt to use APIs to integrate their detection and response data. This generally involves using an expensive SIEM as the centerpiece of their security operations, which aggregates log data by parsing and normalizing it, thus stripping away much of the valuable context. Security teams get to see the log data in one place, but it 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.

Other companies choose to outsource their detection and response functions, entirely or in part, to either managed security service providers (MSSP) or even more threat-focused managed detection and response (MDR) vendors. There's nothing wrong with outsourcing this function, particularly for organizations with smaller security budgets or 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 sophisticated analysts to efficiently and confidently assess threats on their own, ensuring that only fully validated alerts are escalated to more senior analysts.

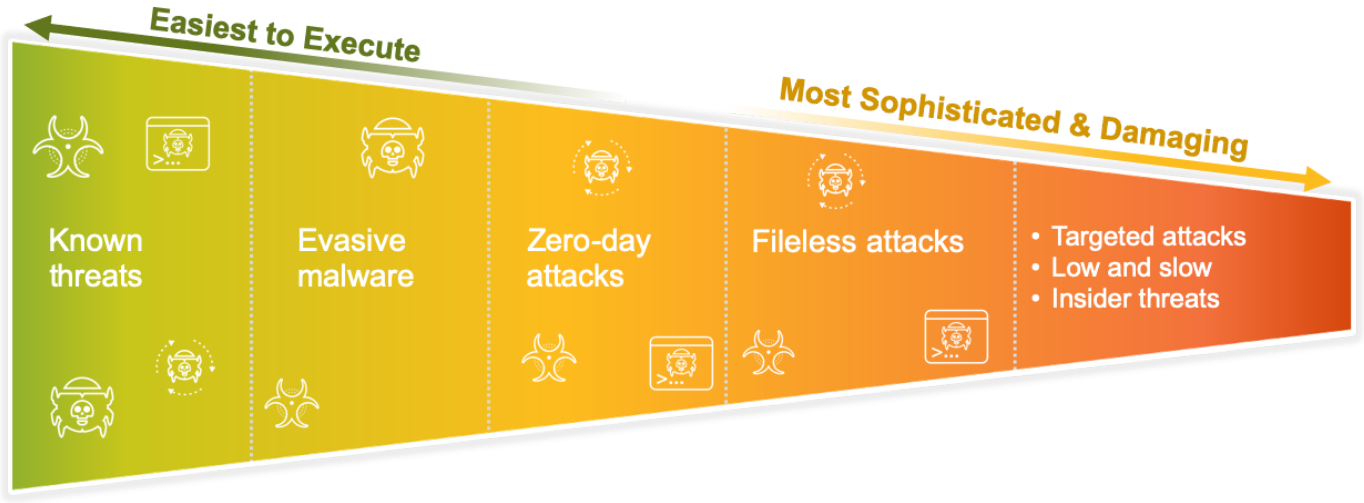

Figure 2: Detection and response tools are designed to stop sophisticated attacks

Technologies for Detection and Response

While the ultimate goal remains preventing successful attacks, organizations must plan for the reality that some percentage of crafty attackers will find their way into their infrastructure and accomplish their objectives. An array of logging, detection, and response tools has come to market to help security teams find threats that have managed to circumvent prevention. Each of these tools has strengths and weaknesses, and can be useful against simple attacks, such as known file-based malware scenarios or attacks that threaten just one part of the infrastructure. Most of them, however, are tuned for a single purpose, and none is particularly well-suited to handle complex campaigns on its own. For those reasons, security teams primarily rely on the detection and response tools described in the sections that follow.

EDR

Gartner definition: *The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems. EDR solutions must provide the following four primary capabilities:*

- *Detect security incidents*
- *Contain the incident at the endpoint*
- *Investigate security incidents*
- *Provide remediation guidance*

IDC predicts a compound annual growth rate of 9.9% in security spending through 2022.

Source: Worldwide Security Spending Guide, IDC

Endpoint detection and response (EDR) first emerged in 2013 to help forensic investigations requiring very detailed endpoint telemetry to reverse engineer malware and understand exactly what the attacker did on a compromised device.

EDR alone cannot 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 devices (IoT, BYOD, ICS, as well as switches, routers, servers, etc.) and cloud resources (e.g., workloads, cloud networks, PaaS). Further, companies use many unmanaged endpoint devices that cannot support EDR agents, providing potential attackers with unmonitored entry points.

SIEM

Gartner definition: *Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).*

Many organizations allocate large portions of their security budgets to SIEM tools to gather logs from security devices (IDS/FW) and server environments (event logs). 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.

Gartner data indicates that security is a top driver of IT spending, and detection and response is the top category of security spending.

Source: Gartner

SIEM centralizes alerts from many security and network devices and alerts on common attacks. Looking to the SIEM for advanced detection is challenging because the SIEM can only look for specific attacks using rules enumerated in the system. If a sophisticated attacker uses a new pattern, a SIEM will likely miss the attack. Moreover, the logs driving SIEM-based analysis don't provide the context required to validate alerts, as much of the contextual data is lost in normalization. Therefore, other systems are required to determine if a device is really compromised or data is being exfiltrated.

NTA and UEBA

Gartner definitions:

Network traffic analysis (NTA) uses a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks. NTA tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NTA tools detect abnormal traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NTA solutions can also monitor east/west communications by analyzing network traffic or flow records that it receives from strategically placed network sensors.

User and entity behavior analytics (UEBA) offers profiling and anomaly detection based on a range of analytics approaches, usually using a combination of basic analytics methods (e.g., rules that leverage signatures, pattern matching and simple statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic and data repositories) to discover potential incidents.

Finally, a newer class of security analytics tools, including NTA and UEBA, 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.

These tools also have their limitations. Network-based products are limited to the network and cannot monitor or track local events, such as process information gathered on the endpoints. NTA also has very limited depth; if EDR is deep and narrow, NTA is wide and shallow. UEBA tools are heavily reliant on third-party logs to monitor and detect network and endpoint-based security threats. The UEBA then analyzes these threats to assign risk scores to users. However, if the third-party tools fail in their detections, or aren't logging a certain piece of infrastructure, then the UEBA is rendered ineffective.

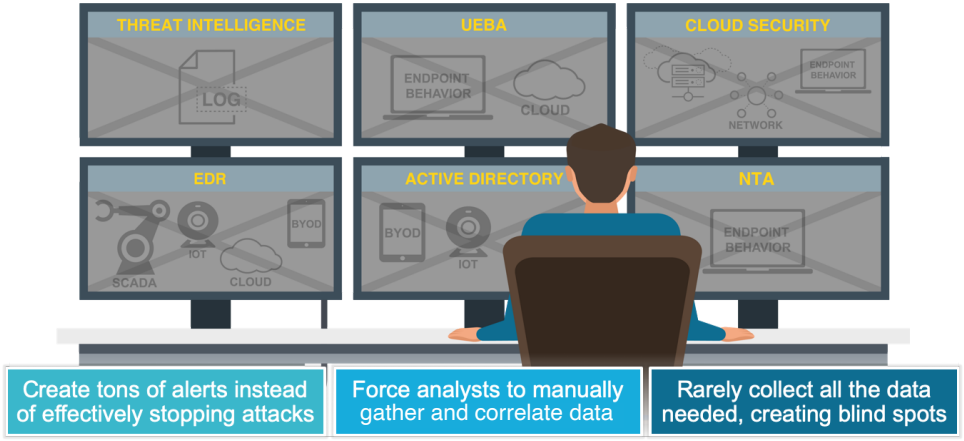

Figure 3: Siloed tools slow down investigation and response

CORTEX XDR BY PALO ALTO NETWORKS

The Bottom Line

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 software applications and make sense of an attack. 451 Research has found that 76% of security teams initiate at least a quarter of their attacks through manual threat hunting, indicating that the detection technologies and processes they have in place to surface attacks are not delivering against the objective. Unless you have full visibility and analysis of all the components in your environment, you could be missing threats.

Addressing the Security Skills Gap

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, there are not enough of these security practitioners, and this significant skills gap impacts the ability of organizations to keep pace with attackers.

Adversaries now utilize highly automated attacks to find vulnerabilities and gain initial presence in your environment. This further exacerbates the skills gap as attackers are able to scale their automated toolkits faster and more affordably than organizations can add skilled security personnel. Thus, you need to look for tools that make your less experienced personnel more effective and efficient, automating repetitive tasks, simplifying investigations, and helping analysts to improve their skills.

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

Source: ESG

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

Tactical detection and response solutions have not solved the problem of finding advanced attackers. Organizations still get hacked and data is lost, so whatever skills an enterprise can field need to work more effectively and efficiently.

There are over 300,000 available cybersecurity job openings in the US today—a number expected to grow substantially in the coming years.

Source: Cyberseek

Defining XDR

XDR is a new category that has emerged to meet the need for more comprehensive and sophisticated detection and response. Extending to any data source, XDR recognizes that it's not efficient or effective to look at individual components of the infrastructure in isolation. XDR uses machine learning and dynamic analysis techniques to combine capabilities and outcomes associated with SIEM, UEBA, NTA, and EDR.

If XDR is the future of detection and response, it must meet the key challenges that we face on a daily basis. With that in mind, let's define the requirements for XDR based on the challenges identified above.

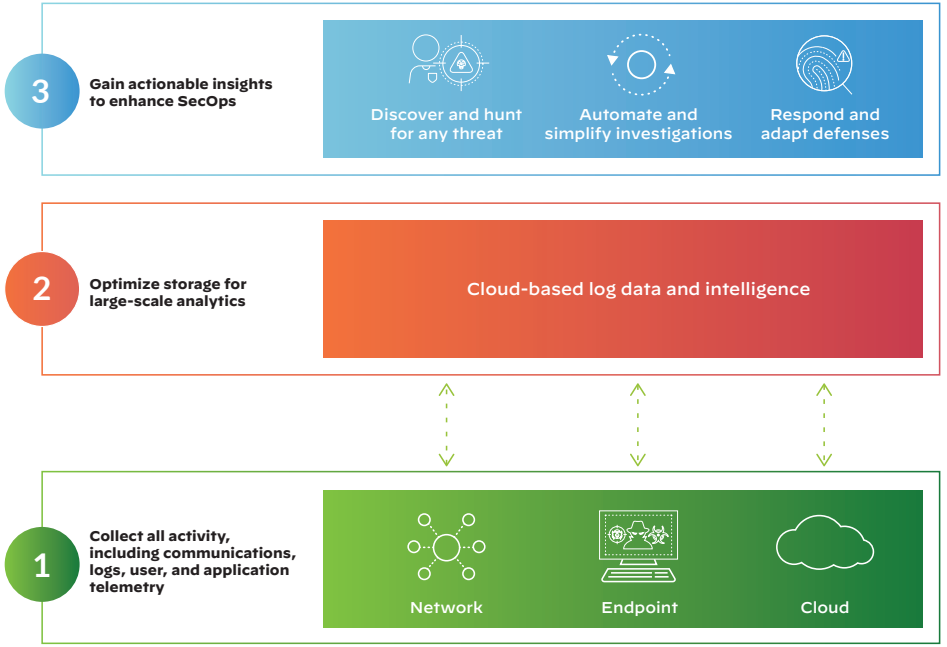

Figure 4: XDR breaks the traditional silos of detection and response

CORTEX XDR BY PALO ALTO NETWORKS

Requirement 1: Find Stealthy Threats Faster with Analytics Across Network, Endpoint, and Cloud

The first step in detection in response is, logically, detection. If you can't see a threat, you can't investigate it; and you certainly can't stop it. Attackers leverage the power of cloud and machine learning to wage multifaceted campaigns that allow them to gain persistence and exfiltrate critical data and intellectual property. This means XDR must have all of the capabilities that follow.

Broad Visibility and Contextual Understanding

Siloed point products lead to siloed data—and that's no longer acceptable. You can't possibly hope to fight attackers effectively if you aren't at least as nimble in your own environment as they 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.

Data Retention

Attackers can be patient. They know they are harder to detect if they move slowly, waiting out the log retention periods of the detection technologies they are up against. XDR should not 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.

88% of hackers believe they can infiltrate a target in less than 12 hours.

Source: Nuix (via NBC)

Analysis of Both Internal and External Traffic

Traditional detection techniques focus primarily on external attackers, providing an incomplete view of potential adversaries. Detection cannot solely look for attacks coming from beyond the perimeter. It **must also profile and analyze internal constituencies** to look for anomalous and potentially malicious behavior to 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 the initial attack to identify subsequent attacks within your organization.

Customizable Detection

Protecting every organization presents unique challenges concerning specific systems, user constituencies, and adversaries. Detection systems must also be highly customizable based on the specific needs of your environment. This involves supporting 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 of the collected telemetry. These approaches include supervised and semi-supervised machine learning.

Only 38% of organizations feel that they are prepared to handle a sophisticated cyberattack.

Source: Cybint

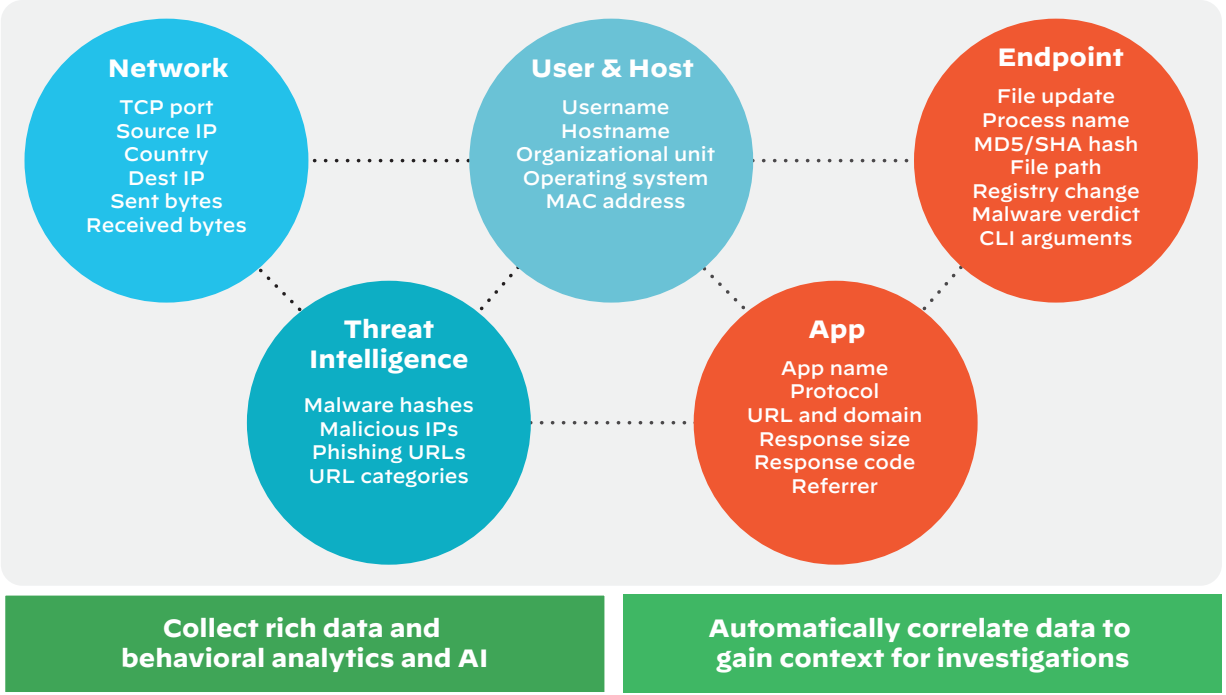

Figure 5: XDR correlates and stitches together rich data

Requirement 2: Simplify Investigation and Response to Known and Unknown Threats

Once you are alert to the potential threats in your environment, you must be able to quickly triage and investigate those threats. Doing this quickly and effectively—especially during an attack that touches multiple parts of your infrastructure—is where traditional detection and response systems fail. XDR solutions can dramatically improve the investigation process. These next sections explain how.

Correlation and Grouping of Related Alerts and Telemetry Data

By the time you receive an alert, the attacker is already hard at work to carry out the mission and achieve an objective. Thus, time is of the essence. You need to be able to quickly understand the attack and its full causality chain. This first means your XDR tool must 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 the network, endpoint, and cloud. By visualizing the activity and sequencing of events, the root cause of the attack can be determined, and the potential damage and proliferation assessed.

Consolidated User Interfaces with the Ability to Pivot

Once they start digging into alerts, the analysts need a **streamlined work environment** that enables them to pivot within the data from any source with a single click. Analysts should not have to waste time switching between two tools, let alone a multitude of 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 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 windows to search numerous threat intelligence feeds for a "bad" IP address.

Orchestration Capabilities

Once attacker activity has been detected and investigated, the next step is efficient and effective enforcement. Your system must be able to orchestrate a coordinated response to active threats and prevent future attacks across network, endpoint, and cloud. This includes communication between prevention technologies (e.g., an attack blocked on the network automatically updates the policies on the endpoints), either natively or built through APIs. It also includes the ability for an analyst to take response actions directly through the XDR interface.

Requirement 3: Improve the ROI of Current and Future Security Investments

XDR should radically advance the return on your security investments. This means improving the efficiency of your team to help avoid and overcome staffing shortages, improving the integration between your existing tools, and strengthening your prevention efficacy over time with scalable infrastructure and artificial intelligence. To meet these criteria, XDR must have these next capabilities.

Security Orchestration

The same attributes that make orchestration important to simplifying investigations also allow it to maximize the ROI of your security stack. Every organization has an installed base of security controls that can be brought to bear in responding to active threats. A key aspect of any detection and response system is to **leverage the investments in these existing controls**, ensuring any response can be undertaken consistently across the enterprise.

Third-Party Data Ingestion

All enterprises have heterogeneous security toolkits. 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 unpredictability of today's adversaries, you don't want to discard telemetry that can provide clues as to attacker activity in slower persistent attacks. This requires sufficient **capacity to store forensic evidence** for months or even years, as well as **analytics horsepower** to be able to utilize all of the telemetry effectively. Cloud-based platforms provide this unrestricted accessibility and scale.

Improvement over Time

Detecting increasingly sophisticated attacks requires embedded artificial intelligence or machine learning as well as automation to reduce manual efforts in order to make scarce security analysts more effective and efficient. XDR solutions should learn from experience, reducing future risk and continually strengthening prevention by applying knowledge gained through detection, investigation, or response.

Reporting and Dashboards

Security teams need to be able to understand and communicate their security posture and operational metrics. Not only must XDR solutions be capable of providing better security outcomes, they must also be able to summarize the state of security through reports and dashboards.

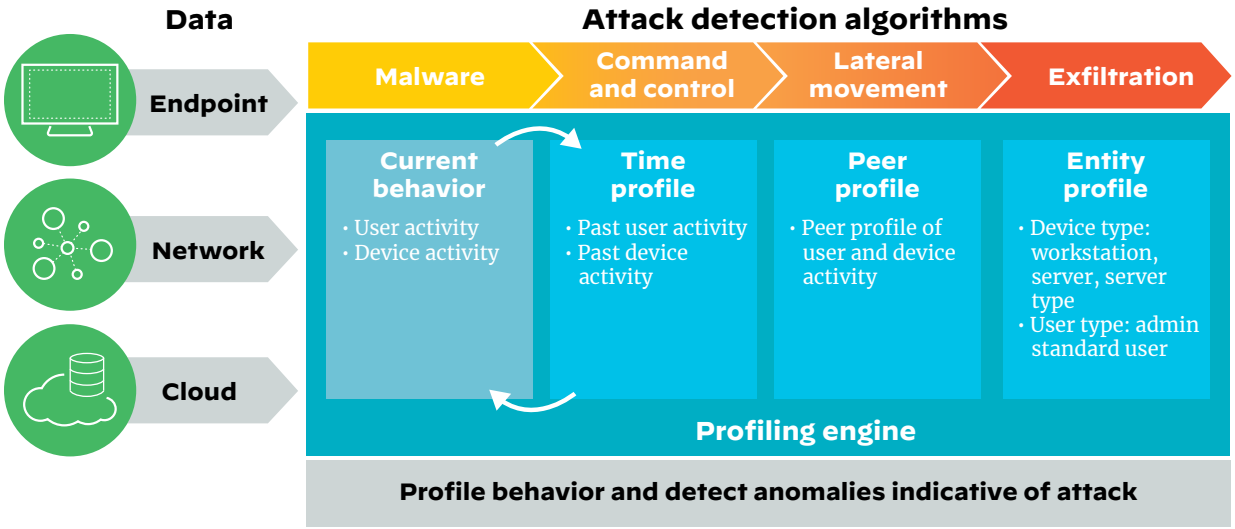

Figure 6: Pinpoint threats unique to your environment with AI

XDR is a new way to think about detection and response, providing a broader view of your environment across networks, endpoints, and the cloud. Using advanced analytics and integrated threat intelligence ensures that both responders and hunters have the information they need at their fingertips to effectively and efficiently pinpoint and address attacker activity.

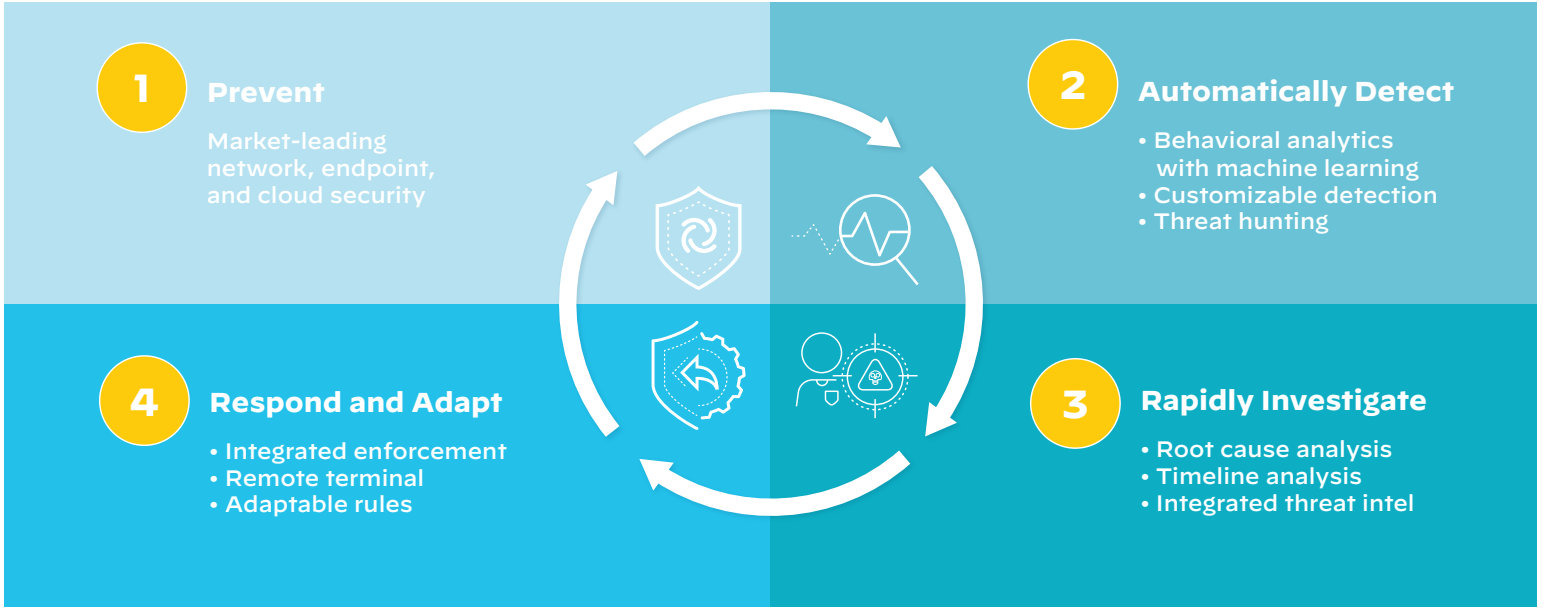

Figure 7: XDR adapts over time to continually improve defenses

Use Cases for XDR

Security operations teams big and small share some key functions. A traditional model for many SecOps teams 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 information as they can 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 penetrated the infrastructure. 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 time on threat hunting activities, as the activities of Tier 1 and Tier 2 consume so many analyst resources.

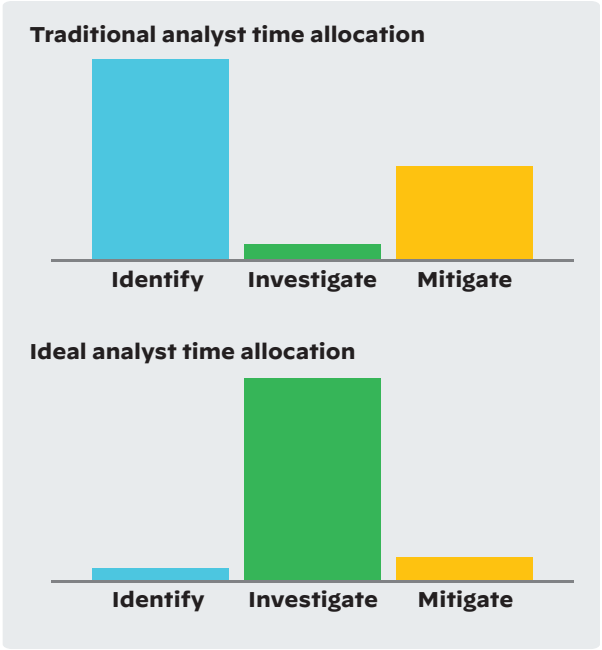

Figure 8: The traditional SOC model does not optimally use analyst time and talent

CORTEX XDR BY PALO ALTO NETWORKS

While this model may be the most common, it is not necessarily ideal. For one thing, most people are not well-suited to monitoring logs all day long. 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). Secondly, far too little time is spent on threat hunting and process improvement, as the majority of resource hours are spent uncovering and mitigating threats.

Now that we've defined XDR, let's take it a level deeper, delving into how it impacts security operations across these tiers and how it can improve this model. We'll break this down by key functions, including detection, alert triage, investigation and response, and threat hunting.

Detection

The ability to prevent data loss rests with the capability of detecting adversaries attempting malicious activity in your environment. XDR uses machine learning to absorb the unique characteristics of your organization, allowing it to differentiate between attacks and harmless activity beyond what is 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 attempt to blend in with legitimate users as they perform reconnaissance and exploit targeted networks. With XDR's ability to perform sophisticated analysis on security data encompassing the network, endpoint, and cloud, you can detect anomalous behavior as attackers compromise devices and move laterally on the network, looking for and exfiltrating customer data and intellectual property.

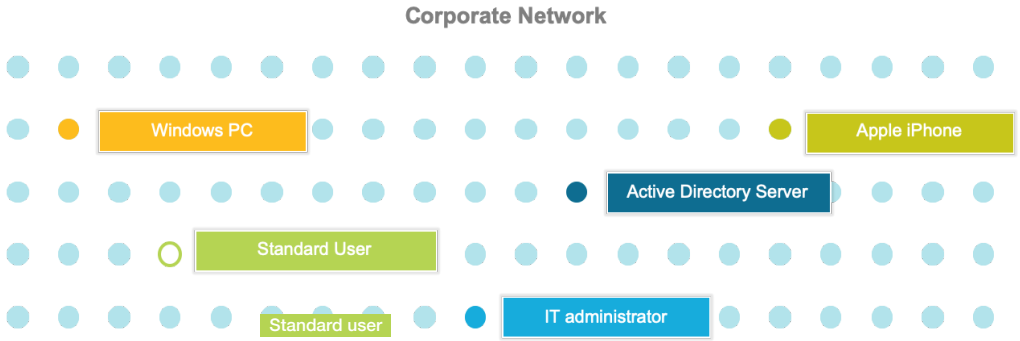

Figure 9: Behavioral analytics discover anomalies at the user, application, and device level

Malicious Insiders

Malicious insiders use their trusted credentials and access to steal significant amounts of corporate data without being detected. XDR addresses this challenge by looking for changes in user behavior and the resulting infrastructure activity, which provides the ability to pinpoint internal reconnaissance and lateral movement.

Inadvertent Risk

Well-meaning employees can inadvertently expose organizations to undue risk through their careless activities. 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—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 malicious activity. This security data also provides the means to investigate across infrastructure to determine the proliferation of the attack campaign.

Given the challenges presented by the security skills gap mentioned previously, 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 knowledge is captured and leveraged for the entire team.

For example, if an adversary adds a new value to the Autorun registry key, an XDR solution could automatically generate a tag creating an action for the analyst called "Executable File Set to Start after Boot;" the type of attack, labeled "Persistence;" and a detailed description like "Process added a new key to the Autorun folder in the Windows Registry; this will ensure an executable or script is run at startup. Review which file and why."

By integrating attack detection algorithms with data collected across network and endpoint as well as cloud, applying a structured detection framework, and continuously learning from both internal responses and external threat intelligence, an XDR solution identifies active attacks with unparalleled precision.

SUMMARY

The benefits of XDR for detection

XDR gives security teams an increased ability 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 Validation

As described previously, security analysts are challenged to triage more security issues both earlier in the process (i.e., reduce dwell time) and by less sophisticated staffers (address the skills gap). The more work that can be done by Tier 1 staff, the more alerts can be handled, and the more attacks detected. Better yet, the more automation that can be built into the triage process, the more effective Tier 1 analysts will be at reviewing and prioritizing security threats that need to be escalated.

Because XDR stitches together network, endpoint, and cloud data, it can automatically determine the root cause of attacks, making them much faster to validate and investigate. For example, not only does XDR determine which endpoint executable was responsible for a network attack, it can figure out which application launched the executable. XDR produces a timeline of the events leading to the attack and provides integrated threat intelligence. All of this allows analysts to understand the root cause of an attack, the exact nature of the threat, and what action to take.

Here's how alert triage and validation works with XDR:

(1) Assessment: The process starts with the XDR solution evaluating both external alerts (from SIEM and other controls) 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 attack.

Palo Alto Networks product usage data shows an average of 50 alerts generated per each security incident. By identifying these related events and grouping them into incidents, XDR can reduce the number of alerts an analyst sees by 98%.

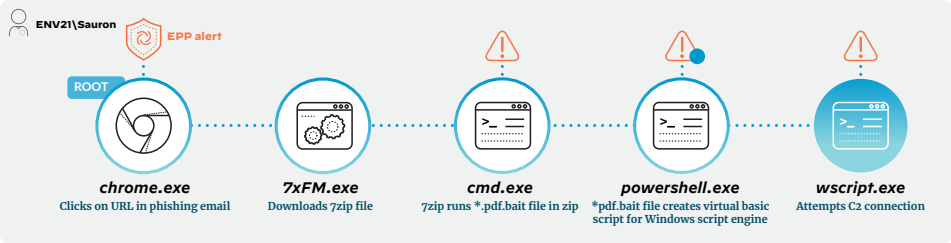

Figure 10: Visualized attack chain using XDR

(3) Analysis: Within each incident, analysts can click further into alerts to access a visual attack chain, leveraging the various sources of telemetry to collect anything and everything that's relevant to the alert to ensure faster and better analysis.

(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.

(5) Validation: The enrichment, analysis, assessment, and prioritization processes all happen automatically before the responder receives the alert for a more formal investigation. XDR uses the history of all previous alerts investigated to add context to the timeline of current alerts, improving prioritization and the speed at which the alert can be validated.

With thousands—sometimes millions—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 attacks with the potential to cause the most damage.

SUMMARY

The benefits of XDR for alert triage and validation

Analysts have an increased ability to:

- Get to more events per day, not just the ones prioritized by security alerting tools or SIEMs.
- Dramatically reduce the chance of a missed alert.
- Analyze false positive alerts to improve detection as well as ensure downstream productivity and defenses are not adversely impacted.
- Apply new behavioral triggers to improve triage times and tighten defenses continually.

Automated and Simplified Investigations and Response

Once an alert has been triaged and prioritized, a more in-depth investigation is warranted. Analysts need context to better understand attacks and how to mitigate them. They need to understand the user, the endpoint information (the process, etc.) the threat intelligence details (e.g., whether a process is known malware), and network details. They should be able to understand the root cause and the timeline of the attack. If they need to manually piece together this information, it will take a while, increasing dwell times and risk. 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 endpoint, network, and cloud telemetry within a security data repository, such as a data lake. 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 eliminate lengthy forensics investigations by interrogating endpoints to determine which process or executable initiated an attack.

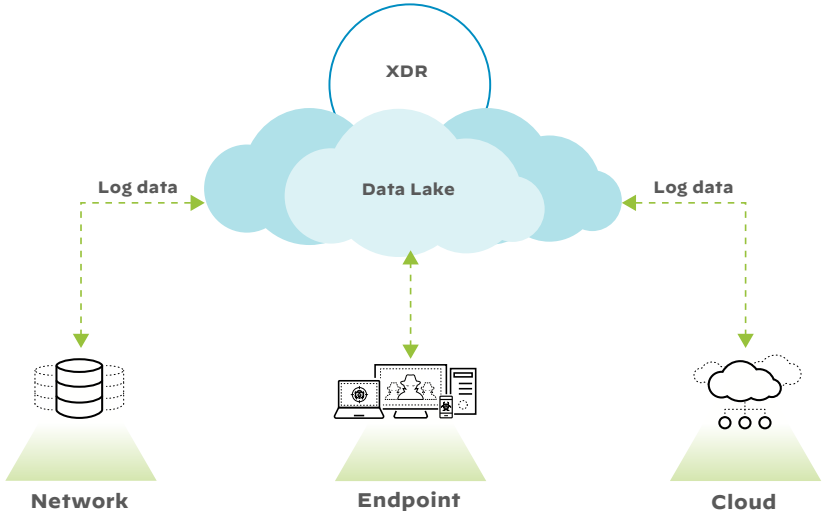

Figure 11: XDR tools stitch together data from different sensors in a cloud-based data lake

CORTEX XDR BY PALO ALTO NETWORKS

To dig deeper into the incident, an XDR solution then ascertains 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 recurrence of any threat found previously. This "assisted learning" allows early detection of attacks based on what has already been seen.

Incident responders can then choose from dozens of remote response and remediation techniques to surgically clean infected systems without business disruption. The security team will become highly efficient, require less training, reduce the burden on more experienced incident responders, and minimize incident resolution times.

SUMMARY

The benefits of XDR for investigations

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 searching of telemetry gathered from networks, endpoints, and the cloud.

Threat Hunting

XDR solutions provide a significant boost to threat hunting capabilities through both automated and ad hoc identification of malicious activity across the infrastructure. Threat hunters can perform advanced queries, gaining instant results with superior precision. Examples of how XDR provides the necessary capabilities to support the different methods of threat hunting follow.

Intel-Based Threat Hunting

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 a lead from threat intelligence, newfound indicator of compromise (IOC), tip from someone within the organization, or mere suspicion, the complexity of tip-based threat hunting will depend on the level of detail the tip 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 Threat Hunting

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 is typically referred to as advanced threat hunting as it is commonly left to the most experienced of 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 UI, 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 Threat Hunting

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 incorporate outcome-based threat hunting directly into the workflow of security alerts and incident handling automatically and continuously. Lessons learned from every investigation are applied to ensure you don't get hit by repeat attacks.

Compliance-Based Threat Hunting

This hunting approach is focused on ensuring compliance with internal, industry, and government policies by performing routine searches that indicate noncompliance, such as sensitive data stored in 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 investigate the situation quickly.

Machine Learning-Based Hunting

Machine learning systems baseline the typical behaviors of an organization to understand what is normal and what is not. 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.

SUMMARY

The benefits of XDR for threat hunting

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 both highly configurable search 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.

Conclusion

Enterprises are in need of foundational changes to their detection and response technologies and processes. Legacy technologies are too rigid and limited, failing to provide either the flexibility or scale to keep pace with today's adversaries. Companies need to work more effectively and efficiently to address the scarcity of qualified security analysts. XDR offers a new way forward, with broader visibility across endpoints, networks, and the cloud, along with more effective machine learning analytics and integrated remediation to fundamentally change threat hunting, detection, investigation, and response.

XDR RFP Checklist

XDR must deliver a wide range of common EDR capabilities to provide efficient and effective security against modern attacks, while also integrating with other key prevention, detection, and response tools across the infrastructure. The following RFP checklist includes requirements within nine key categories to help you evaluate the quality of the platforms you're considering.

Use this checklist as a starting point, and tailor it to your company's needs to ensure you're able to identify vendors that can best support your organization.

Download the spreadsheet version to start your RFP today at go.paloaltonetworks.com/xdrrfp.

1. AV Requirements

- □ ML-based threat prevention
- □ Behavior-based threat prevention
- □ Exploit technique prevention
- □ Signature-based threat prevention
- □ Real-time verdict updates provided by the vendor
- □ Integration with cloud-based malware analysis service
- □ 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 and for detection and response

2. Data Visibility and Logging Requirements

User information

- Domain and distinguished name
- Email address
- Organizational unit
- Phone number

Device information

- MAC address
- Hostname of device
- Domain name
- Distinguished name of host
- Organizational unit
- Operating system
- Operating system version
- Name of firewall, if applicable
- Other names used by firewall configuration, if applicable

Process information

- Process timestamp
- Path and name
- Process ID
- Loaded modules
- Hash values such as MD5 and SHA-256
- Command line arguments
- Signature state

File information for file create, write, access, open, rename, or delete

- Timestamp
- Path and name
- Previous file name and path for file rename events
- Hash values, such as MD5 and SHA-256
- Username

Network activity including outgoing connections, failed connections, and incoming connections

- Timestamp
- Source IP address, destination IP address, source port, and destination port
- Bytes sent and received
- Protocol

- Remote country
- Proxy information
- User
- Integration with next-generation firewalls for complete Layer 7 visibility, including application name
- Connection duration
- Transaction-level data and enhanced information about key protocols, such as DNS, HTTP, DHCP, RPC, ARP, and ICMP

Registry activities such as create key, modify key, delete key, and rename key

- Timestamp
- Key name
- Value and type
- Previous key name for rename events

System events

- User status change event, such as login and logout
- Host status change event
- Agent status change event

Security alerts

- □ URL filtering logs
- □ Firewall threat logs
- □ Endpoint threat logs

Contextual user data

- □ Logged-in user
- □ Typical user of a machine
- □ User creating the process that initiated communication
- □ User group and organizational unit from directory services

3. Data Retention and Coverage Requirements

- □ Visibility into lateral movement across the network and other parts of the infrastructure
- □ Detection and response for threats involving both managed and unmanaged endpoints
- □ Detection and response for threats involving remote users
- □ Detection and response for threats involving cloud servers
- □ Minimum of 30 days of data retention
- □ One year of retention for audit logs of administrative and investigative activity

4. Investigation Requirements

- Automated root cause analysis of any alert, including network alerts, if endpoint data is available
- Ability to view chains of execution leading up to an alert
- Timeline analysis view to see all actions and alerts on a timeline
- Query capability for indicators of compromise (IOCs) and for endpoint behaviors
- Query capability for online and offline hosts
- Ability for an analyst to easily pivot between views
- Granular filtering and sorting of query results
- Identification if an event was blocked by an endpoint agent, a firewall or another prevention technology
- Automated stitching of security alerts, such as firewall alerts, to endpoint data
- Noise cancellation, removal of non-significant binaries and DLLs from chain
- SOC analyst context of TTPs to utilize knowledge gained in future investigations

5. Incident Management Requirements

- Automated reduction of related alerts from various sources into a single incident
- Ability to extract notable artifacts from the alerts and match them with threat intelligence services
- Ability to extract the entities involved in the incidents for ease of view
- Ability to assign incidents to team members

- ☐ Ability to get notifications on incident assignment
- ☐ Ability to add comments
- ☐ Ability to manage the incident lifecycle (new, investigation, closed, handled, etc.)
- ☐ Ability to merge and split incidents
- ☐ Ability to send incident data to third-party case management

6. Threat Intelligence Requirements

- ☐ Ability to alert on known malicious objects on endpoints with IOC rules
- ☐ Automatically scan historic data for IOCs as they are added to the system and raise alerts
- ☐ Integrate with one or more threat intelligence services for threat intelligence tags and additional context on key artifacts
- ☐ Ability to remotely run arbitrary scripts

7. Response Requirements

- ☐ Remote terminal capability
- ☐ UI-based remote terminal, not only CLI
- ☐ Ability to run CMD, PowerShell, and Python commands
- ☐ Ability to run custom scripts
- ☐ Remote isolation of the endpoint
- ☐ Remote file deletion
- ☐ Automatic and manual collection or retrieval of quarantined files and objects

- Remotely suspend or terminate processes
- Ability to view running processes
- File manager with ability to view, download, rename, or move files
- UI task manager

8. Detection, Integration, and Automation Requirements

- Behavioral analytics to profile user and endpoint behavior and detect anomalies indicative of attack
- Supervised and unsupervised machine learning capabilities
- Predefined and customizable behavior-based detection rules
- Custom rules for retroactive threat detection
- Integration with security information and event management (SIEM) solutions
- Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services
- Integration with a security orchestration, automation, and response (SOAR) solution for incident analysis
- Ability to detect reconnaissance and lateral movement attempts

9. System Support and Resource Requirements

- Modular and scalable product
- Cloud-based deployment
- Full auditing for all actions in the system

- ☐ Minimum number of agents required
- ☐ Average CPU usage of less than 3% with all services enabled
- ☐ Agent installation size of less than 50 MB
- ☐ Ability to push agent updates from the management console
- ☐ Ability to run on and protect all macOS and Mac OS X versions released in the last five years
- ☐ Support for Android
- ☐ Support for all major Linux distributions
- ☐ Support for all recent Windows versions, including Windows Server
- ☐ Multi-factor authentication for management
- ☐ Support for non-persistent VDI
- ☐ Support for temporary sessions for machines that repeatedly revert to a snapshot (or image) on which the agent is not installed

10. Managed Service Requirements (Optional)

If your security operations team uses a hybrid or fully outsourced model, consider these additional checklist items to evaluate managed security services:

- ☐ 24/7 year-round monitoring and availability
- ☐ Ability to ingest, prioritize, and triage alerts from all vendors
- ☐ Identification and validation of critical threats in one hour or less

- □ Visibility into data sources that include endpoint device, network packet/session, and cloud packet/session/config
- □ Monitoring and detection of behavioral anomalies on unmanaged devices
- □ Monitoring and detection of behavioral anomalies for users
- □ Continuous threat hunting across managed and unmanaged devices
- □ Tuning of tools to individual customer environments, including custom rules and exceptions
- □ Access to specialists via email, phone, or messaging system (e.g., Slack)
- □ Visibility, communication, and response portal or mobile application
- □ Customer access to tools

3000 Tannery Way
Santa Clara, CA 95054

Main: **+1.408.753.4000**
Sales: **+1.866.320.4788**
Support: **+1.866.898.9087**
www.paloaltonetworks.com

paloalto NETWORKS | CORTEX XDR BY PALO ALTO NETWORKS

Sophisticated cyberattackers can sneak past even the best threat prevention systems to compromise critical data—often in public, damaging ways. Most enterprises have tools to deal with attacks that skirt their initial defenses, but each of these only sees a tiny slice of the IT infrastructure. The tools aren't intelligent or integrated enough to correlate different events over the course of an attack, so they send out alerts for anything remotely suspicious, often hundreds or thousands per day. Security analysts waste time sifting through these alerts for the ones that matter. When real threats slip through the cracks, they frequently go uncovered for months.

That system doesn't work.

Introducing a better category of detection and response tools: XDR. XDR stitches together data from the endpoint, network, and cloud in a robust data lake. Applying advanced machine learning and analytics, it identifies threats and benign events with superior accuracy and gives analysts contextualized information, simplifying and accelerating investigations. Read this e-book to learn more, including:

- Challenges with the current state of detection and response
- Tactical use cases for improving security operations with XDR
- The definition and key requirements of XDR