aws marketplace

(Re)Defining XDR: How to improve threat detection and response in AWS

Learn how to architect an extended detection and response (XDR) strategy with Amazon Web Services (AWS) services and third-party solutions in AWS Marketplace

AWS Marketplace Introduction

Extended detection and response (XDR) is more than a simple integration of multiple sources. An effective XDR strategy can help you build stronger detection capabilities and better response orchestration across device and traffic types. In this whitepaper, SANS instructor Matt Bromiley will break down each component of XDR to provide practical guidance on approaches, tools, and implementation strategies. He will also talk about areas where you can introduce automation in response and remediation activities and provide various examples of use cases for XDR.

Expanding on Bromiley's perspective, AWS Marketplace will share how you can specifically apply these practices to your AWS environment. They will cover relevant AWS Marketplace seller solutions that can help you further expand on this strategy.

The featured solutions for this use case can be accessed in AWS Marketplace:

Palo Alto Networks

CrowdStrike

Humio

Trend Micro

SANS

Analyst Program

Whitepaper

(Re)Defining XDR: How to Improve Threat Detection and Response in AWS

Written by **Matt Bromiley**

July 2021

aws marketplace

Introduction

What it takes to secure an enterprise has changed significantly in just a few years. Enterprises' digital footprints are expanding at a record pace, morphing to include new technologies. Organizations have sought to strengthen their security posture with endpoint or network detection and response capabilities (known as EDR and NDR, respectively).

However, information security analysts now say that the single- or limited-source telemetry provided by EDR and NDR aren't able to encompass the security needs of the modern enterprise. To compensate, some organizations are deploying even more security controls. The result? Security teams are trying to wrangle too many controls. Instead, organizations need an understanding of how controls can work together to build a stronger detection and response program.

In this paper, we are going to focus on exactly that: obtaining an optimal state of enterprise security detection and response. Extended detection and response, often shortened to "XDR," is a relatively recent concept that recognizes that, too often, the myriad security controls organizations deploy are not efficiently cooperating. An effective, well-planned XDR strategy considers the organization's risk profile, its threat landscape, and the technologies it uses.

Furthermore, as you will see in this paper, it is important to ensure your organization is taking advantage of both the detection and response capabilities that an effective XDR strategy offers. Modern technology simply grows at too rapid a pace. For example, within your own organization, think about what has changed in the past 24 months in these areas:

- Number of systems deployed in the cloud versus on premises
- Percentage of environment that is virtualized versus physical hardware
- Size of the workforce using company assets and/or accessing internet-facing services remotely
- New organization-wide projects, such as SD-WAN, that attempt to unify communications

Chances are good that your organization has undergone significant change in a short amount of time. Now think about those areas of change and ask yourself the following question:

> Did our security posture change as well?

Each technological implement your organization undertakes expands both its digital footprint and security posture. The goal of this paper is to help you plan an XDR strategy that enables your security team to minimize risk and gain visibility on *all* the technologies the organization uses.

As you work your way through this paper, we encourage you to use the "Implementation Tips," which appear in the margins, to evaluate your environment and security team. These tips will help you gain insight into where your security posture needs to improve next. Let's get started!

XDR Piece by Piece

Before implementing an XDR strategy, it is worth the effort to analyze each part of the "extended detection and response" label and consider how to incorporate what it represents into your security program. A well-structured XDR strategy can help minimize risks and plan for future implementations.

Typically, *DR products have been endpoint- or network-centric. These EDR and NDR products have been instrumental in forwarding many security postures and detecting and responding to security events. But modern enterprises are much more than simply networks behind central, common firewalls or endpoints on physical, corporate-managed devices. In the following sections, we take a closer look at the components that make up the *X*, *D*, and *R* in *XDR*.

Implementation Tip

Have your team examine your current security posture and discuss known visibility gaps or assumed risks that an XDR strategy could rectify.

X(tended)

The *X*, for *eXtended*, refers to the source or type of telemetry being received. Today, this typically goes far beyond simple endpoint or network telemetry. For example, enterprises now incorporate vast cloud resources, ranging from storage to virtual systems to containerized, short-lived "servers" helping meet traffic demands. Detection and response capabilities for these products do not exist in the traditional formats (but we will cover those next).

As assets moved to the cloud, security teams attempted to maintain visibility by adding data sources. For example, cloud environments offer provider-specific logs. Cloud providers may also offer telemetry, such as Cisco's NetFlow, to give a network-based viewpoint into cloud operations.

Implementation Tip

Begin your XDR strategy by focusing on the technologies your enterprise utilizes. For example, how much of your infrastructure is in the cloud? What are your critical assets and where are they located? Your first XDR telemetry should derive from your perimeter and these sources.

But sometimes a traditional technology deployed in a new type of environment may call for teams to take additional precautions. Consider, for example, a Linux server deployed in a cloud environment. The security team might have the cloud provider logs, which give insight into the back-end operations of that server (system events, user authentications, and so on), as well as a traditional EDR agent, which provides endpoint-specific telemetry such as process and user activity. But this presents a new question for the team to consider: Are both sources necessary?

Data sources are critical to an effective XDR strategy, because they enable defenders to model detection and response around telemetry. However, too much data can easily lead to overconsumption. Like "analysis paralysis," defenders who have to sift through too much data will be unable to effectively detect and respond to unauthorized activity. The same can happen with too much security tooling data. Too many choices and/or too much coverage can create vulnerabilities in an environment, despite being fully "observed."

Implementation Tip

When implementing tooling and visibility, eliminate redundancies and try to ensure full coverage. If two endpoint agents provide similar data, choose the one that best complements your XDR strategy or separate the functionalities of the two agents based on need and reach.

Finally, when assessing coverage and visibility, look for tooling that offers significant coverage of your assets, whether on premises or in the cloud. For example, if you deploy endpoint agents on cloud assets, keep in mind the functionality of those assets and their expected lifetime. Assessments like these might help you realize that an endpoint agent on such an asset is not the right type of coverage. Instead, look to your cloud provider for network data. Detection and response strategies can be built on a steady stream of network data, eliminating concerns about endpoint lifetime. Any asset brought up behind the "wall of visibility" is covered and included in the *DR strategy. We'll discuss this further in the following case study.

Implementation Tip

When assessing visibility, look for tooling and/or data that can help provide the most coverage. For example, network security tooling can cover a large enterprise easily and is much more effective than attempting to deploy and maintain endpoints in every single corner of the enterprise. Conversely, you may not be able to deploy network sensors and so will need individual security mechanisms to help bridge this gap.

Case Study: Unauthorized Traffic in VPC Logs

In perhaps the simplest form of XDR, only endpoint telemetry is gathered. Figure 1 illustrates a small subset of an environment relying on multiple AWS resources in the cloud. It includes Amazon Elastic Compute Cloud (Amazon EC2) clusters for web-facing applications and internal R&D.

One challenge that an organization might face is that the systems within various clusters might have differing timelines. Internet-facing applications, for example, must scale as necessary to meet demand, whereas R&D systems are more permanent to long-term business operations. What is the best monitoring/response approach for the organization to take? Should it aim for 100% coverage via endpoint telemetry, or is there better option?

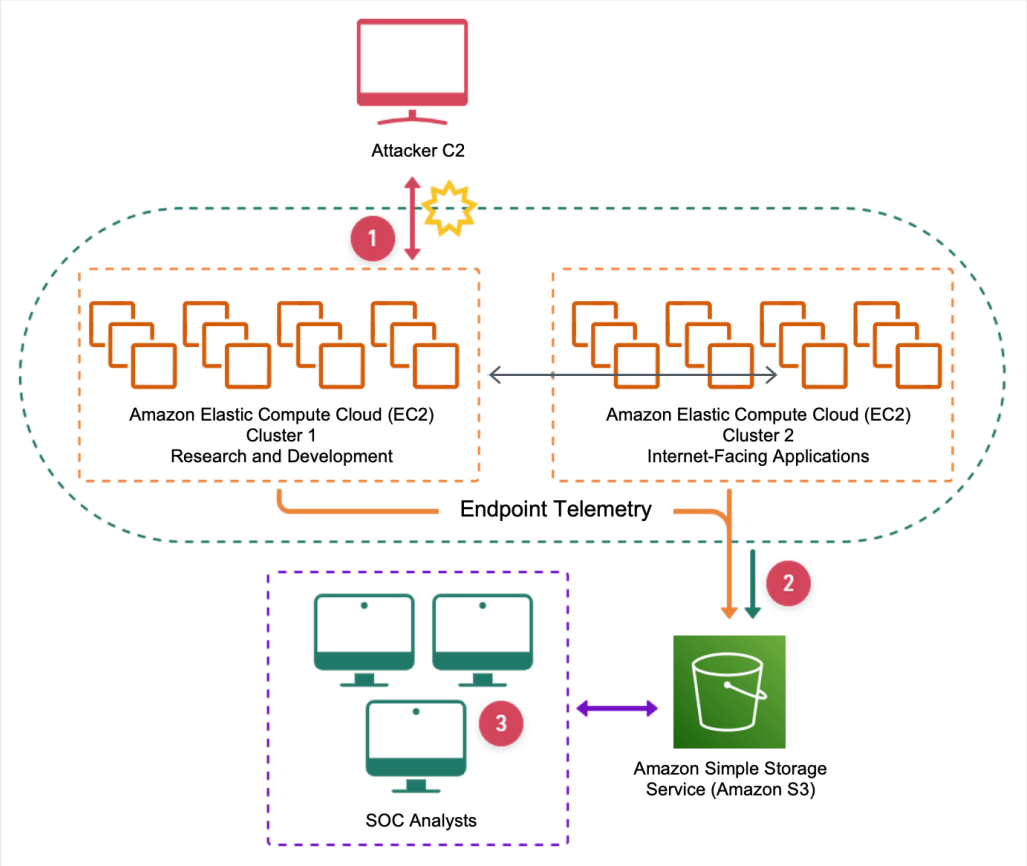


Figure 1. Endpoint Telemetry Only

The solution shown in Figure 1 answers these questions. We can use it to consider an incident in which a security team relies solely on endpoint telemetry. Although tracing Amazon EC2 communications 1 is certainly possible with endpoint data, analysts should determine whether it is the best source of evidence. Furthermore, is endpoint data always available? Instead, SOC analysts 3 would be better served by combining both endpoint and 2 network telemetry (available via Amazon VPC Flow Logs) in a central location. When combined and correlated, they provide not only system activity but also IP traffic moving in and out of all applicable subnets.

[1] This paper mentions product/solution names to provide real-life examples of how cloud security tools can be used. The use of these examples is not an endorsement of any product/solution.

D(etection)

The second element of an *DR implementation is the ability to detect. While the *X* in *XDR* refers to a source of telemetry, the *D* refers to the ability to use that telemetry to detect anomalous or unauthorized activity. Detection in any *DR strategy must be on or close to the source and occur in real time. Consider traditional SOC setups, which afforded only post-activity analysis. They forwarded logs from multiple sources to a single SIEM or log platform, and security analysts needed to parse and normalize that data, craft detections, and wait for alerts to trigger. Unfortunately, while log forwarding can be useful in identifying *some* bad actor activity, the lag time between unauthorized activity and incident team detection is too long.

Implementation Tip

When evaluating an XDR product, consider its ability to allow for customized detection capabilities. Security teams that can craft their own detections with high-fidelity telemetry can customize alerts to meet their environment's unique behaviors.

*DR products include built-in detection capabilities that place defenders *closer* to a security event. When this is coupled with real-time system telemetry, defenders can understand more about an actor's unauthorized activity and techniques. Detections also help defenders gain more technical insight into an actor's overall unauthorized activity, as opposed to a single point in time.

For example, consider an actor who is attempting to download an unauthorized file from an external server, perhaps to assist in the next stage of the attack. A legacy security setup may collect network data into a SIEM and use policies crafted to detect file download activity. But because downloading a file is not inherently malicious, the artifact of file download would likely provide relevant value to an investigation only *after* the actor has fully downloaded and potentially executed the file. This is simply too late.

Implementation Tip

To see a significant decrease in actors' success rates, encourage teams to learn how to write and implement their own detections. This also develops analyst capabilities and allows your team to gain experience in modeling actors' behaviors.

*DR products, on the other hand, provide real-time telemetry and insight into said download activity, including the system processes and accounts used, the external server's IP address, a hostname (if applicable), and other key details. These real-time data points provide immediate insight that allows for defenders to respond faster.

Case Study: Third-Party Supplier Security Event (EDR vs. XDR)

Security teams should not stop at simply adding more telemetry. They should strive to understand business processes so they can build the telemetry around them. Because many organizations use third parties for some of their business processes, here we expand upon the original example by adding third-party integrations 1, as shown in Figure 2. In this case, the organization is utilizing a third party for some IT management.

Security teams should identify and monitor how third parties access the organization's data and resources, for example, via user access or API calls (to name two possibilities). In the scenario described in Figure 2, the security team should incorporate AWS CloudTrail logs 2 or infrastructure logs to help augment endpoint and network detections.

With multiple data sources, security teams 3 can also construct complex detections across multiple datasets. For example, login and endpoint activity can be correlated to show when a user accesses a resource and what actions were taken on that system. Similarly, access to a cloud application can be coupled with network telemetry to provide a complete picture of IP traffic, from external to internal.

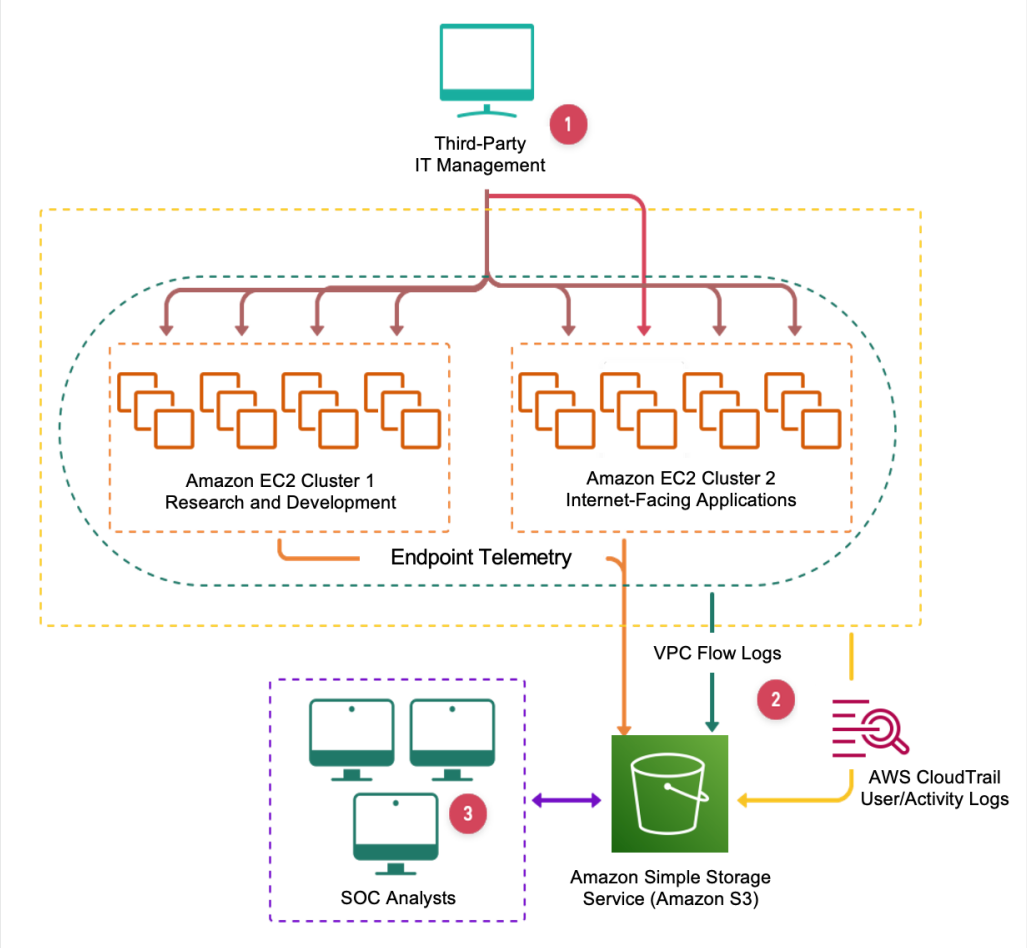


Figure 2. Endpoint Telemetry Plus Multiple Data Sources

R(esponse)

The third element of a successful *DR strategy identifies an organization's ability to respond to a security event, often because of useful telemetry and successful detections. Response is likely the most critical component of any *DR strategy—especially an XDR strategy, which relies on multiple tools and technologies. Put simply, an environment's response capabilities measure how quickly the security team can regain control of an asset, data, user account, or parts of the business.

However, many security tools with superb detection capabilities offer little in response. A strong XDR strategy should look to create a seamless experience for defenders, with detection and response done with the same data and tooling. Needless hopping between tools and data creates too much friction, which actors will seize on.

Implementation Tip

Response involves much more than simply gathering evidence about an incident; it is how you regain control of an asset. Assess tooling response capabilities up front: In the event of an incident, how will this tool help your security team achieve its objectives? If you detect with one and respond with another, it might be worth assessing tools that can do both.

When analyzing the response capabilities of a security tool, your questions should be rooted in your team's requirements and technologies. This begins with an assessment of incident response processes. If anomalous activity is detected, what is the security team's next step? Does it take the resource offline, block it for additional access, or wipe it and completely rebuild it? Does the process change based on technology (which would also change the tooling requirements)?

For example, an organization with a significant cloud footprint should first determine its processes for cloud-borne events. In the event of, say, unauthorized access to a cloud resource, what are the next three to five steps in the team's response? Look for tools that can integrate into your cloud environment and help your team achieve those critical steps.

Implementation Tip

Your response strategy, and thus your tooling requirements, begins with processes. Seek out tooling that helps your team achieve its objectives. Look for congruity between processes, teams, and tools.

Automating Response

As mentioned, implementing strong response in an XDR strategy begins with processes and identifying tooling to help meet those processes. With these in place, security teams increase their control of the environment and gain confidence to protect the various technologies their organization uses. Fortunately, an XDR strategy includes an additional inherent benefit: a quick path to automating detection and response.

Once a strategy begins to mature, teams will find themselves performing the same response tasks again and again. This is *not* inherently bad. Teams repeating tasks is good exercise because it enables them to identify gaps in controls and vulnerabilities in the environment. However, once processes have been ironed out, it is time to free up the security team. Automation helps achieve this.

Implementation Tip

With enough maturity and practice, the security team can begin to automate key parts of the response strategy. Every technology—cloud, endpoint, or network—has response processes your team can automate to defend the environment. Assess how tools can integrate with one another and what automation options are available.

Often done with security orchestration, automation, and response (SOAR) and the use of highly detailed playbooks, automation is where an XDR strategy comes to fruition. With predefined actions and playbooks across multiple points of telemetry, a security team can create intricate, nearly surgical, response approaches. This does not replace the security team. It simply utilizes tooling to emulate the team's already well-defined processes.

The benefit of automated response and a strong XDR strategy is one that keeps the organization secure behind the scenes, regardless of technology deployed. Organizations that understand the technologies they use and how to secure them will find it easy to embrace newer technologies as the business grows. As you will see in the next case study, this is hardly truer than in cloud environments. Loaded with various resources and capabilities, cloud providers offer organizations myriad capabilities with the click of a button. However, this can create opportunities for an actor—unless the organization has already thought ahead.

Implementation Tip

Get your team in the habit of writing response playbooks. This is not additional work—it is breaking down additional processes into technical, actionable steps. Then, when you move to automation, you will already have playbooks ready to go!

Case Study: Cloud IAM Security Playbooks—Integrated Detection and Response

In the final example, we continue building and finding ways for the security team to take advantage of more telemetry and automated, integrated processes. As shown in Figure 3, the security team can utilize integrations from security vendors in AWS Marketplace to automate playbook responses and security actions 2.

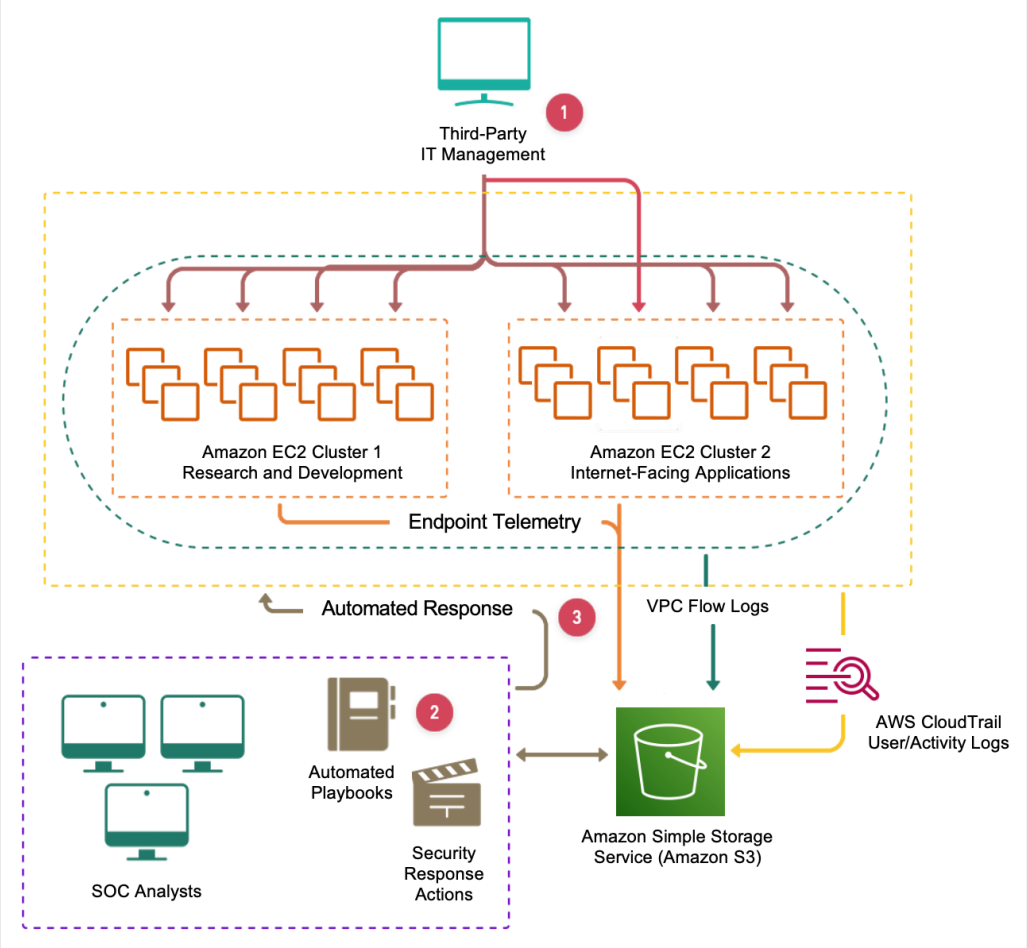


Figure 3. Telemetry Plus Automated, Integrated Responses

Let us consider a full response example: A third-party IT manager has a security event that extends to its customers and networks that it has access to. Typically, a third-party provider has privileged access to customers' environments, and an actor could continue undetected for a lengthy period of time. However, with automated playbooks, anomalous account activity would be detected and responded to automatically.

You may notice that throughout each of the case studies presented, we built upon the previous scenario to incorporate new data, new processes, and new integrations from all that AWS offers. Security teams should constantly do the same by assessing the data that would have the most impact for their detection and response capabilities, integrating and correlating that data, and building automated actions off of it.

Advanced Threat Detection with XDR

In the previous section, we analyzed the key components of XDR. When implemented effectively, an XDR strategy can help an organization secure an ever-expanding technology footprint. However, XDR also presents an inherent benefit to the security team: a way to rethink and revamp detection and response strategies. An optimal XDR strategy includes these considerations. With greater and more granular visibility, the security team is no longer limited in its ability to stop advanced, unauthorized access attempts.

An organization with single- or limited-source telemetry thinks of detections in only that way. An endpoint-centric security posture, for example, relies solely on endpoint detections. Network activity is lost but available for capture. Additionally, the organization's response capabilities are limited to its tooling. An actor can contain or block a system but can do little to impact the network. What happens, though, if an actor successfully evades endpoint security? What has the team's investment yielded at this point? A more sweeping XDR strategy incorporates how attacker techniques can best be detected and responded to.

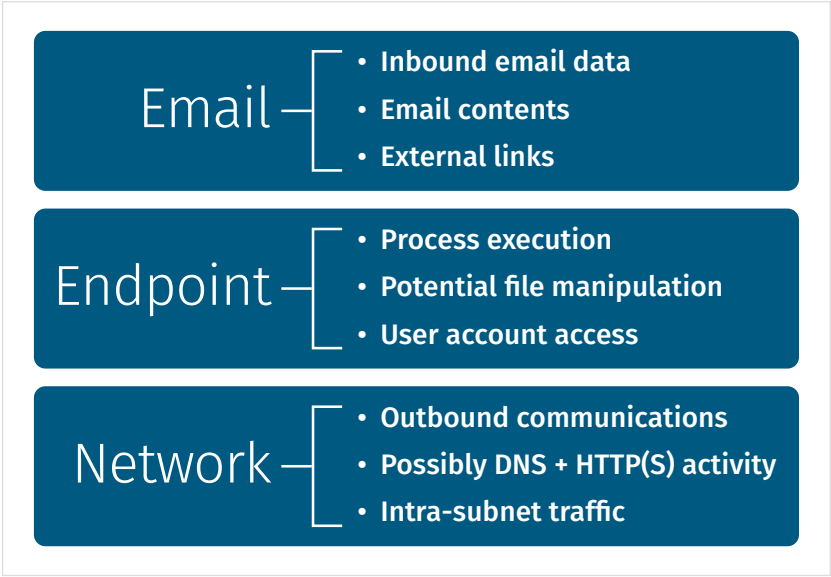


Figure 4. Telemetry Involved in Spearphishing

For example, consider an actor who is attempting to spearphish a victim to gain a foothold in an environment. This type of activity easily involves multiple sources of telemetry, as shown in Figure 4.

Individually, each of these points of telemetry could assist in detecting a spearphishing event. However, if any of the telemetry sources were implemented standalone, an actor need only evade one defense to gain access into the environment. Furthermore, each data point is relevant only at a particular stage of the event. For example, email data is hardly useful if the actor has already gained a foothold and is beaconing back to an Amazon EC2 server.

Conversely, what if your security team utilized all the data points to craft multi-source detections? Let us evaluate this situation again, instead thinking of telemetry in chronological importance, as shown in Figure 5.

Figure 5. Telemetry in Chronological Importance

These seemingly different points of telemetry contribute to the same narrative of the security event. Your team can not only craft better detections, but also rely on the correlated XDR data to understand the incident—and make decisions—much faster. And this is true for myriad techniques that actors are using in the wild. Actors have become skilled at evading single defenses but have displayed an inability to evade multi-source environments for a long period of time.

Multi-source detections are just the beginning. By harnessing and utilizing a wider range of security data, teams can up the ante by combining multi-source detections with high-fidelity threat intelligence. Offering unique and up-to-the-minute insight into actors' activities, threat intelligence data becomes significantly more impactful if an organization can act on *all* the data it receives, rather than a single piece.

Next Steps in XDR

In this whitepaper, we challenged the current notion of detection and response strategies within modern organizations. As we elaborated, many organizations are stuck using single-source security tooling. This limitation unfortunately means that actors need only deploy simple defense evasions to avoid detection. Furthermore, single- or limited-source telemetry does little to fully encompass the modern enterprise. Organizations are much more than endpoints and networks and thus need detection and response capabilities for the other areas of their operations.

The use of XDR is helping meet this need. XDR recognizes that organizations will have multiple sources of security tooling and require a path to combine and correlate data efficiently. This so-called XDR strategy encourages organizations to evaluate their digital footprint and security profile. Their XDR implementation should help provide visibility into the former, while minimizing the latter.

Finally, XDR also creates new opportunities for defenders in an organization. Without visibility or advanced tooling into certain parts of the environment, defenders are limited in what they can implement. An XDR strategy defeats this by not only expanding visibility, but also combining tools and capabilities. For example, your organization's cloud footprint can be combined with automated detection and response, meaning your security team can craft high-fidelity rules and playbooks, and leave them in place. This frees up your team to focus on the challenging aspects of the organization and protecting the critical areas of the business.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensic and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

aws marketplace

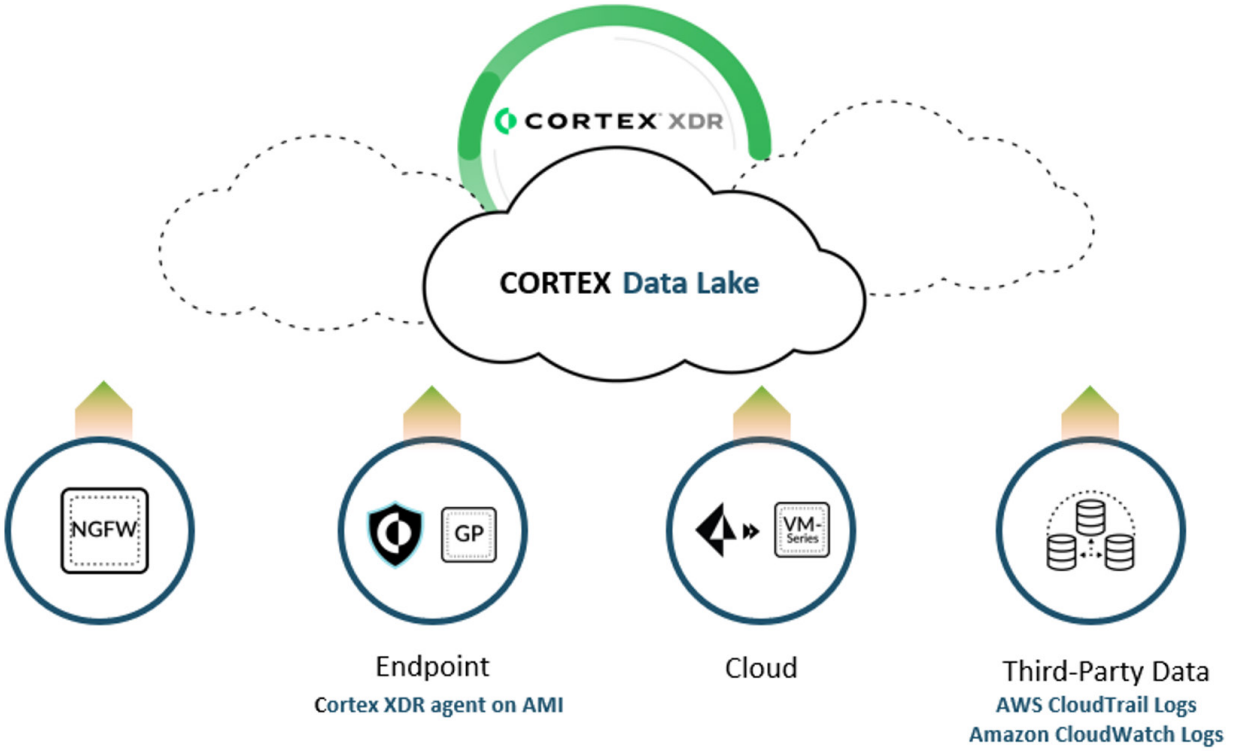
Effective XDR strategies with AWS services and third-party solutions

Network and endpoint detection and response (NDR and EDR) products have been important tenets of organizations' security strategies. As we have seen, however, leveraging an XDR strategy can help reduce information silos while enhancing productivity of security teams. By synthesizing data from sources like Amazon Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail logs, and other services you may already be using, visibility and coverage can be improved. Tools like Palo Alto Networks Cortex XDR are designed to handle these additional datasets and orchestrate responses quickly.

How AWS customers are leveraging Palo Alto Networks as part of their security architecture

Palo Alto Networks Cortex XDR helps organizations prevent security events by unifying prevention, detection, and response with data gathered from networks, endpoints, virtual machines, logs, and other sources.

- **Unified threat prevention, investigation, and response:** Centralized platform brings together data from disparate sources.
- **Accelerate investigation and response times:** Use automated playbooks and machine learning to better manage and response to cases.
- **Reduce total cost of ownership (TCO):** Consolidate separate security tools from separate vendors into the Cortex XDR platform to reduce TCO.



Trend Micro's XDR solution also collects and correlates data from multiple vectors, enabling simplified investigation and response via a single platform. Humio, a CrowdStrike company, offers an observability solution with an extensive set of integrations to collect log data which security teams can use to bring context to their detection and response activities.

Why use AWS Marketplace?

AWS Marketplace is a curated digital catalog that simplifies software discovery, procurement, provisioning, and management. With AWS Marketplace, customers can also utilize features that speed up product evaluation, improve governance and cost transparency, and enhance control over software spend. AWS Marketplace offers third-party solutions across software, data, and machine learning tools that enable builders to find, test, and deploy solutions to expedite innovation.

Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

aws marketplace

How to get started with security solutions in AWS Marketplace

Security teams use AWS native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security posture. The following solutions can help you get started:

paloalto NETWORKS

Palo Alto Networks

CROWDSTRIKE

CrowdStrike

humio A CrowdStrike Company

Humio

TREND MICRO

Trend Micro