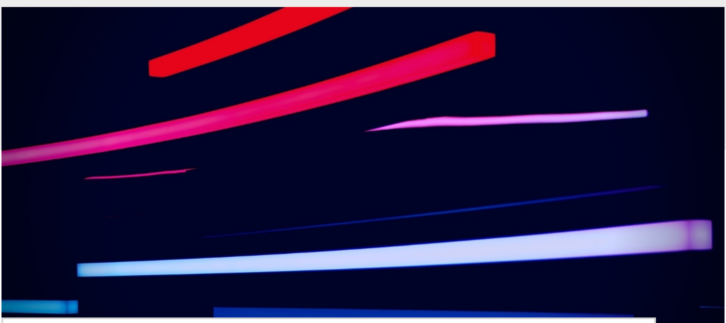

Understanding the Difference Between EDR, SIEM, SOAR, and XDR

October 6, 2021
by Resha Chheda and Michael Leland

The cybersecurity industry is awash with jargon, abbreviations, and acronyms. As sophisticated attack vectors multiply, from endpoints to networks to the cloud, many enterprises are turning to a new approach to counter advanced threats: Extended Detection and Response, giving rise to yet another acronym: XDR. And while XDR has gained a lot of traction this year from industry leaders and the analyst community, XDR is still an evolving concept, and, as such, there is confusion around the topic.

- What is XDR?
- How does XDR differ from EDR?
- Is it the same as SIEM & SOAR?

As a leader in the EDR market and a pioneer in emerging XDR technology, we are often asked to clarify what it means and how it can ultimately help deliver better customer outcomes. This post aims to clarify some common questions around XDR and differences compared to EDR, SIEM, and SOAR.

Understanding the Difference Between EDR, SIEM, SOAR, and XDR
By Resha Chheda & Michael Leland
SentinelOne

What Is EDR?

EDR provides an organization with the ability to monitor endpoints for suspicious behavior and record every single activity and event. It then correlates information to provide critical context to detect advanced threats and finally runs automated response activity such as isolating an infected endpoint from the network in near real-time.

What Is XDR?

XDR is the evolution of EDR, Endpoint Detection, and Response. While EDR collects and correlates activities across multiple endpoints, XDR broadens the scope of detection beyond endpoints to provide detection, analytics, and response across endpoints, networks, servers, cloud workloads, SIEM, and much more.

This provides a unified, single pane of glass view across multiple tools and attack vectors. This improved visibility provides contextualization of these threats to assist with triage, investigation, and rapid remediation efforts.

XDR automatically collects and correlates data across multiple security vectors, facilitating faster threat detection so that security analysts can respond quickly before the scope of the threat broadens. Out-of-the-box integrations and pre-tuned detection mechanisms across multiple different products and platforms help improve productivity, threat detection, and forensics.

> In short, XDR *extends* beyond the endpoint to make decisions based on data from more products and can take action across your stack by acting on email, network, identity, and beyond.

How Is XDR Different From SIEM?

When we talk about XDR, some people think that we are describing a Security Information & Event Management (SIEM) tool in a different way. But XDR and SIEM are two different things.

SIEM collects, aggregates, analyzes, and stores large volumes of log data from across the enterprise. SIEM started its journey with a very broad approach: collecting available log and event data from almost any source across the enterprise to be stored for several use cases. These included governance and compliance, rule-based pattern matching, heuristic/behavioral threat detection like UEBA, and hunting across telemetry sources for IOCs or atomic indicators.

SIEM tools, however, require a lot of fine-tuning and effort to implement. Security teams can also get overwhelmed by the sheer number of alerts that come from a SIEM, causing the SOC to ignore critical alerts. In addition, even though a SIEM captures data from dozens of sources and sensors, it is still a passive analytical tool that issues alerts.

The XDR platform aims to solve the challenges of the SIEM tool for effective detection and response to targeted attacks and includes behavior analysis, threat intelligence, behavior profiling, and analytics.

How Is XDR Different From SOAR?

Security Orchestration & Automated Response (SOAR) platforms are used by mature security operations teams to construct and run multi-stage playbooks that automate actions across an API-connected ecosystem of security solutions. In contrast, XDR will enable ecosystem integrations via Marketplace and provide mechanisms to automate simple actions against 3rd-party security controls.

SOAR is complex, costly, and requires a highly mature SOC to implement and maintain partner integrations and playbooks. XDR is meant to be ‘SOAR-lite’: a simple, intuitive, zero-code solution that provides actionability from the XDR platform to connected security tools.

What Is MXDR?

Managed Extended Detection and Response (MXDR) extends MDR services across the enterprise to get a fully managed solution that includes security analytics and operations, advanced threat hunting, detection and rapid response across endpoint, network, and cloud environments.

An MXDR service augments the customer’s XDR capabilities with MDR services for additional monitoring, investigations, threat hunting, and response capabilities.

Why Is XDR Gaining Traction and Generating Buzz?

XDR replaces siloed security and helps organizations address cybersecurity challenges from a unified standpoint. With a single pool of raw data comprising information from across the entire ecosystem, XDR allows faster, deeper, and more effective threat detection and response than EDR, collecting and collating data from a wider range of sources.

XDR provides more visibility and context into threats; incidents that would not otherwise have been addressed before will surface to a higher level of awareness, allowing security teams to remediate and reduce any further impact and minimize the scope of the attack.

A typical ransomware attack traverses the network, lands in an email inbox, and then attacks the endpoint. Addressing security by looking at each of those independently puts organizations at a disadvantage. XDR integrates disparate security controls to provide automated or one-click response actions across the enterprise security estate such as disabling user access, forcing multi-factor authentication on suspected account compromise, blocking inbound domains and file hashes and more – all via custom rules written by the user or by logic built into the prescriptive response engine.

This comprehensive visibility leads to several benefits, including:

- Reducing Mean Time to Detect (MTTD) by correlating across data sources.
- Reducing Mean Time to Investigate (MTTI) by accelerating triage and reducing time to investigate and scope.
- Reducing Mean time to respond (MTTR) by enabling simple, fast, and relevant automation.
- Improving visibility across the entire security estate.

Moreover, thanks to AI and automation, XDR helps reduce the burden of manual work on security analysts. An XDR solution can proactively and rapidly detect sophisticated threats, increasing the security or SOC team’s productivity and returning a massive boost in ROI for the organization.

Parting Thoughts

Navigating the vendor landscape is challenging for many enterprises, particularly when looking at detection and response solutions. Often the biggest hurdle is understanding what each solution provides, especially when terminologies vary from vendor to vendor and can mean different things.

As with any new technology entering the marketplace, there is a lot of hype, and buyers need to be wise. The reality is, not all XDR solutions are alike. SentinelOne Singularity XDR unifies and extends detection and response capability across multiple security layers, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across the complete technology stack.

If you would like to learn more about the SentinelOne Singularity Platform, contact us or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Massive Attack | Why MSPs Are Prime Targets for Cybercriminals and APTs
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- 6 Real-World Threats to Chromebooks and ChromeOS
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks

©2023 SentinelOne, All Rights Reserved