

SIEM VS XDR VS OPEN XDR


A new cybersecurity acronym has entered the chat. XDR, or Extended Detection and Response, is the latest security technology and method for threat detection. Best summarized as a “NextGen SIEM”, XDR is redefining the process of collecting, normalizing and correlating security data from multiple sources and leveraging security tools to automate immediate response. Because SIEM and XDR appear to be very similar, it is important to highlight the differences.

UNDERSTANDING XDR VS SIEM BY DEFINITION

We explained XDR a little above, but let’s look at Gartner’s definitions of each to highlight the nuances of the two.

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).^[1]

Extended Detection and Response, or XDR, is a unified security and incident response platform that collects and correlates data from multiple proprietary components. The



platform-level integration occurs at the point of deployment rather than being added in later. This consolidates multiple security products into one and may help provide better overall security outcomes. Organizations should consider using this technology to simplify and streamline security.[2]

In summary, XDR is a SIEM alternative that takes the core functions of a SIEM and enhances them with machine learning for a more automated and accurate response.

XDR VS SIEM IN-ACTION

The best way to highlight the tools is by looking at the platform and how XDR earned its name as a “NextGen SIEM”.

XDR takes the core of a SIEM platform and enhances it with machine learning to instantly analyze and correlate large amounts of data. As a result, teams are given the most important, critical alerts first. Let’s look at the four phases of XDR:

Collect: XDR platforms have data collection at their core. Eliminate common problems of too much data, not enough data or no context to incoming data by normalizing data as it enters the system. From there easily reduce, enrich with telemetry and fused into one record. In the end, there is context to what is actually occurring.

Detect: Built to be an early detection warning by mapping out detections of known and unknown behaviors against the cybersecurity kill chain. The rich data collection and correlation put kill chain detection at the foundation of threat detection.

Investigate: With thorough detection, analysts can confidently search the dataset for malicious activity via queries.

Respond: Automate appropriate responses to ensure a secure environment. For example, an event can automatically trigger a ticket within its built-in case management system trigger email, Slack and restful API alerts, automatically send out POF reports and signal firewalls to take appropriate actions.



OPEN XDR VS XDR

Many cybersecurity vendors are throwing XDR around. How do you compare all the different versions? The answer is simple. Most XDR platforms are limited to a specific set of tools, often those produced by the platform creator and select technology partners. Sounds limiting, right?

Open XDR is different. As 'open' suggests, all security tool logs are collected, normalized and correlated for a complete picture of what is going on in your environment. The truly vendor agnostic approach provides superior visibility while improving the ROI on existing security investments.

THE POWER OF BRITEPROTECT MANAGED OPEN XDR

The power of a platform is only as good as its management. BriteProtect addresses the too many tools, too many alerts and not enough people challenge with a 24/7/365 security operations service. BriteProtect's expert process and cybersecurity experts with the powerful co-managed Open XDR platform provides unprecedented protection from the most advanced threats.

[1] <https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem>

[2] <https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/>