WHITE PAPER

Open XDR vs. SIEM

Matching Resources and Business Risk with the Right Solution

STELLAR CYBER®

Gaining visibility and responding to attacks across the entire enterprise infrastructure (endpoints, servers, applications, SaaS, cloud, users, etc.) is a very tall order in today's cybersecurity environment. Enterprises are forced to create complex security stacks consisting of SIEM, UEBA, SOAR, EDR, NDR, TIP and other tools in order to meet this challenge. For many enterprises, SIEM is the main tool for aggregating and analyzing data from the infrastructure. Nearly half of enterprises report that they are not satisfied with their SIEMs[1], but all enterprises will be quick to point out the amount of capital, time and resources they have poured into standing up and maintaining their SIEMs. Open XDR is emerging as a new approach addressing the challenge of gaining visibility and responding to attacks across the entire enterprise infrastructure. In this article, we'll look at how Open XDR and SIEM measure up as security solutions.

Defining Open XDR

Gartner defines XDR, or eXtended Detection and Response, as "a unified security incident detection and response platform that automatically collects and correlates data from multiple **proprietary** security components." This definition, dating back to 2020, does not capture Open XDR as an emerging category of XDR that collects and correlates data from **all existing** security components, not just proprietary or single-vendor ones. So, Open XDR is defined the same as Gartner's XDR definition except that it ends with "**all existing** security components, delivered via an open architecture". The Open vs. Native XDR difference is discussed in detail in another article. In this article, we focus on Open XDR as it compares to SIEM. So Open XDR has the following technical requirements to fulfill the promise of the above definition:

- **Deployability –** Cloud-native microservice architecture for scalability, availability and deployment flexibility
- **Data Fusion –** Centralize, normalize and enrich data across the entire attack surface, including network, cloud, endpoints, applications and identity
- **Detection –** Built-in automated detections through Machine Learning
- **Correlation –** High-fidelity correlated detections across multiple security tools
- **Intelligent Response –** One-click or automated response from the same platform.

Sound similar to SIEM plus a little SOAR? That's because it is. However, there are major architectural differences that allow Open XDR to deliver on many of the promises of SIEMs where SIEMs have fallen short.

Defining SIEM

Gartner defines SIEM, or Security Information and Event Management, as technology that "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." This definition is notably similar to the definition of XDR. Architecture is where the biggest differences lie, but purely definitionally a SIEM was named after its main purpose - to manage information and events. XDR was also named after its main purpose - to detect and respond. This may seem like a minor point, but this difference in business purposes is what drives the architectural approach, and is why SIEMs are so capital-intensive in today's security environment.

Architectures Compared

This comparison focuses only on the differences. There are a number of technical similarities including long-term storage, open integrations with security tools, cloud-nativity, and efficient search and threat-hunting.

However, Open XDR has five key architectural differences from SIEMs:

1. Data is forced into a normalized and enriched state, and this is done before the data are stored in a data lake.
2. Detections and correlation of alerts are automatically driven by AI in Open XDR, not human-written rules as with SIEMs.
3. Incidents are produced from correlated alerts, from which a single response on the same platform is orchestrated, compared to a SIEM, which sends alerts to a different SOAR platform which then performs downstream correlation and response.
4. Many tools required for security operations are unified, such as Big Data Lake, UEBA, SOAR, TIP, NDR or EDR on one platform while many SIEMs only include a Big Data Lake, forcing SIEM users to manually combine many complex tools together by themselves.

Differences 1 and 2 go hand in hand. In order to build and maintain meaningful AI in any industry, the data problem must be solved. In security, that means data must be centralized, normalized and enriched to reduce data complexity. If data is modeled differently at each deployment of a platform, it will be an impossible problem to maintain AI models. XDR forces data to be modeled the same way across each deployment before data lands into a Data Lake; data is only available in its normalized and enriched state. SIEM either provides this as optional functionality or does not provide this feature at all; in the optional case, normalization and enrichment is treated as a post-processing step on raw data that is already stored.

In summary, on technical differences 1 and 2, Open XDR forces normalization and enrichment on data, so it is capable of building meaningful AI that correlates events and alerts together. For the same reasons, SIEM architecture is not able to produce an AI engine of the same fidelity because of its treatment of data. SIEMs will be able to leverage AI, but it will be difficult to scale.

Technical difference 3 comes down to an Open XDR performing correlation and response in the same platform. A higher order construct of an incident (multiple related alerts) is automatically produced in an Open XDR platform, and that is responded to holistically. A SIEM must pass alerts to a SOAR, which must correlate alerts together with rules without the deep context of everything happening

	NOT SCALABLE Heavy Services Required		SCALABLE Little/No Services Required	
Deployment	**SIEM Data**	**SIEM Rules**	**Open XDR Data**	**Open XDR AI Model**
A		**I**		**X**
B		**J**		**X**
C		**K**		**X**

in the environment. Open XDR produces a response just like a SIEM and SOAR does, but the response fidelity is much greater with XDR because it is orchestrated from the same platform performing detections and AI-driven correlations, where all the data is available.

The final technical difference is centered around the approach to building and maintaining the overall security stack. Open XDR was designed to unify all key tools for security operations such that they can be orchestrated from one platform. Many SIEMs offer long lists of plugins and deep levels of customization, but that puts the onus on the users to build and configure their system.

For the enterprise, these technical differences influence the capital, time and resources it takes to run a security platform. SIEMs are open-ended technologies, so they are going to be expensive to operate. Open XDR platforms are security prescriptive technologies, and therefore enterprises will be much more efficient when employing them.

Finally, while not strictly technical differences, two areas where SIEMs have focused much more are on heavy compliance-related storage and use of the same platform for IT Operations. XDR is designed for the outcome of detection and response. It can still meet compliance requirements, but it was not designed for that from the start. IT Operations in the same platform is something that only SIEM can claim, as Open XDR is strictly focused on security.

What About NG-SIEMs?

"Next Gen" anything signals something that is better, not different. NG-SIEMs are better than SIEMs in the hypothetical sense. Open XDR is different from both. NG-SIEMs brought huge advancements in many areas where legacy SIEMs were not keeping up with the demands of today's security environment. Notable improvements are:

- Use of Big Data technologies (no more SIEM constantly falling over)
- Some User and Entity Behavior Analysis (UEBA) through various algorithms
- UI/UX improvements to key workflows like Threat-Hunting
- Native or open integration with SOARs
- Data modeling plugins.

NG-SIEMs certainly close the capability gap between Open XDR and SIEM, but the architectural differences remain the same.

Some Vendors Say They Offer A SIEM *and* An XDR Platform – What Gives?

There are many similarities between SIEM and Open XDR, as noted above. The technical differences are nuanced, but have major implications on business value and capital required to operate. There are two claims vendors are making if they are using both SIEM and Open XDR to describe their product.

The first claim vendors may make is that they may use "SIEM Capabilities" to refer to their Open XDR platform having all the important capabilities of a SIEM - open collection, storage, search, reporting, cloud-native - as a way to describe how Open XDR can be deployed in an enterprise security stack, specifically to replace an existing SIEM.

The second claim vendors may make is to say that their platform is both a SIEM and an Open XDR platform. This is a confusing point likely to ensure that the vendor does not miss out on potential category marketing and can sell a product to customers regardless of whether they are looking for SIEM or Open XDR. As discussed above however, SIEM and Open XDR are different, so the same product cannot be both.

Navigating The Collision Course of XDR And SIEM

XDR is on a collision course with SIEM and SOAR, as noted by Forrester[2]. Enterprises need to approach both technology categories with their long-term business outcomes and available resources in mind. Is high fidelity, automated detection and response out of the box more important? Is the capability of response from the same platform by the same team critical to reduce the attack dwelling time? Is the team short-staffed and/or needs lots of training to run the tool? These are the key questions enterprises must bring to the table when defining their security stack strategy and deciding whether XDR or SIEM is right for them.

[1] 2017 Ponemon SIEM Report

[2] https://www.forrester.com/report/Adapt+Or+Die+XDR+Is+On+A+Collision+Course+With+SIEM+And+SOAR/-/E-RES165775

STELLAR CYBER®

Stellar Cyber's Open XDR platform delivers Everything Detection and Response by ingesting data from all tools, correlating incidents across the entire attack surface, delivering high-fidelity detections, and responding to threats automatically through AI and machine learning. Our intelligent, next-gen security operations platform greatly reduces enterprise risk through early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity. Typically, our platform delivers a 20X improvement in MTTD and an 8X improvement in MTTR.

www.stellarcyber.ai | sales@stellarcyber.ai