exabeam

Guide

SIEM and XDR: A Comparison Guide

A little history on the SIEM

The term "security information and event management" (SIEM) was **coined in 2005** as an evolution of "central log management" (CLM). Since inception, SIEM tool workloads have grown in scope (and complexity) leading to the tools that we know today. SIEMs offer many capabilities and solve a very wide set of problems for security practitioners. Analyst firm, Gartner, has tracked this space in their **SIEM Magic Quadrant** for more than a decade.

And along comes XDR

There's a new item in the security practitioner toolkit, it's called "extended detection and response" or XDR. XDR was **coined in 2018**. XDR tools were designed with a more narrow purpose than SIEMs and have not seen their capabilities morph, like SIEMs, ... just yet. Let's compare SIEM and XDR:

Comparison: Key differences between SIEM and XDR

	SIEM	XDR
Domain coverage	Multi domain coverage: • Threat detection, investigation, and response (TDIR) • Compliance • Centralized storage • Reporting	Single domain coverage: TDIR
Design approach	Designed for customization and "just in case" situations	Designed to be focused on efficient TDIR
Data location	Typically assumes that the data needs to be centralized in the SIEM	Typically assumes that data could be stored anywhere and/or doesn't need to be stored for the long term
Delivery model	Can be on-prem, cloud-delivered or both	Cloud-delivered
Storage requirement	Offers an infinitely scalable storage	Doesn't always offer long-term storage
Detection approach	Typically focuses on correlation-based analytics	Typically offers machine learning-based advanced analytics
Automation approach	Typically offers very flexible orchestration, automation, and playbooks for TDIR and non-TDIR use cases	Typically offers prepackaged, use case–specific TDIR with prescriptive orchestration, automation, and playbooks
GTM motions	Typically replaces or displaces legacy SIEMs, CLMs and/or data lakes	Typically augments legacy SIEMs, CLMs and/or data lakes

SIEM and XDR share *some* common characteristics (e.g., both can do TDIR), but their design philosophies and core capabilities make them different.

Which tool do I need for my organization?

SIEM and XDR are best suited for different situations:

Threat detection and incident response (TDIR)

If the functional coverage is focused only on TDIR across a heterogeneous stack, then XDR might be a better alternative with a shorter time-to-value than a general-purpose tool such as a SIEM.

Log retention, compliance

If the functional coverage goes beyond TDIR, for example including centralized storage, or compliance then a SIEM is in order as the XDR may or may not be able to address these additional requirements.

Behavioral analytics

Those organizations that are looking for an analytics-driven approach, versus a correlation-driven approach to Security Operations, might prefer XDR. While some SIEMs provide behavioral analytics as a feature, few SIEMs were architected with this capability. Behavioral analytics is a core component of the leading XDR offerings.

Start small, grow over time

Fearing the long deployment and complexity of a SIEM, many organizations opt to start small with a specific requirement on TDIR and expand their scope to include compliance or log centralization. These organizations should look for vendors that offer an XDR with an easy upgrade path to a full-featured SIEM, for example by adding storage, compliance packages or non-TDIR dashboarding capabilities.

Conclusion

Regardless of the path you take, your organization should prioritize tools that offer **prepackaged content for common and advanced use cases** delivered at scale with an outcomes-based approach.

While SIEM and XDR appear similar at first glance they actually differ on many key criteria. To learn more about modernizing your SOC visit **https://pages.exabeam.com/modern-soc.html**

Or visit **https://www.exabeam.com/product/** to learn more about what Exabeam offers in each of these categories.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.