Secureworks®

WHITE PAPER

XDR VS. SIEM: A CYBERSECURITY LEADER'S GUIDE

As threats intensify and SecOps teams are called upon to defend digital environments that keep growing in size and complexity, and with a defensible perimeter that has all but disappeared, cybersecurity vendors are responding with a new generation of software and service solutions.

Most notably in 2022, the industry is experiencing the ascent of a new class of solutions called Extended Detection and Response, commonly referred to as XDR.

Because XDR aggregates security data from across the enterprise, some cybersecurity leaders might assume that it is merely an evolved version of Security Information and Event Management (or SIEM). But the truth is, XDR goes far beyond the characteristics of a traditional SIEM, offering tangible value that improves security visibility, operational investigations capabilities, and response actions across the enterprise.

With SecOps teams facing escalating pressures of increased workload and low-fidelity alerts — coupled with a troublesome undersupply of available SecOps talent to help address those demands — cybersecurity leaders should investigate and understand the non-trivial differences between XDR and SIEM.

This guide provides an overview of those differences.

WHAT IS SIEM?

While the acronym "SIEM" was first coined by Gartner in 2005[1], the functional fundamentals of SIEM have been around even longer than that. As early as the 1990's, forward-looking organizations recognized that they needed to consolidate their disparate security logs into a single system to facilitate analysis and fulfill compliance requirements.

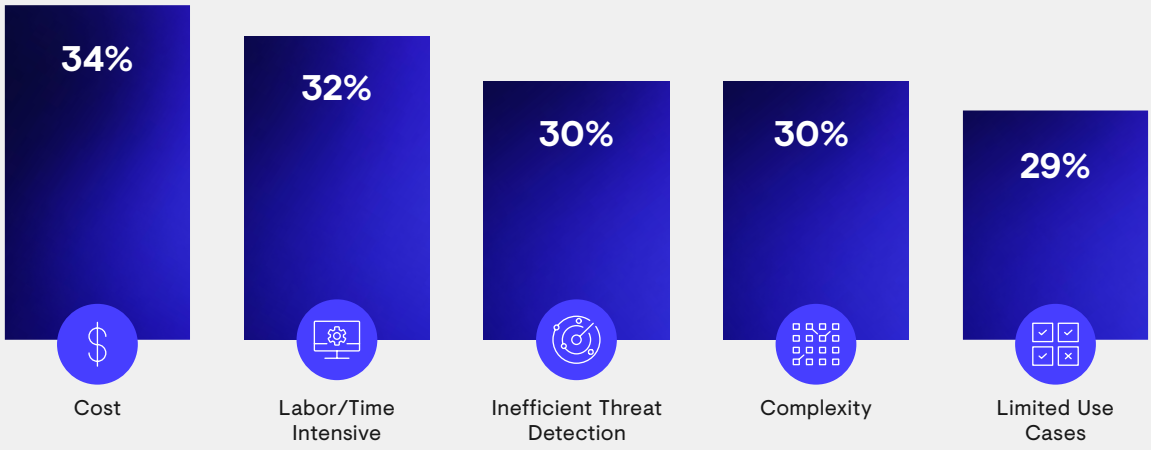
[1]Gartner Research: Innovation Insight for Extended Detection and Response

Not all SIEM solutions are created equal. However, they generally share the following attributes:

- **Log data aggregation** that provides SecOps teams with a consolidated source of telemetry from across the enterprise.
- **Centralized data retention** that maintains a historical record for forensic and compliance purposes with a common retention period, while allowing dispersed logs to flush their caches as frequently as required.
- **Data querying** across systems that helps SecOps staff investigate security logs and alerts in order to search for undiscovered active threats in the environment.
- **Dashboards and reports** enable SecOps to monitor their environments on-demand, comply with auditing requirements, and provide third parties such as MSSPs with the data they need.

Some SIEM solutions also offer data analysis and manipulation tools that help SecOps staff correlate related events, apply filters that improve the noise/signal ratio, and otherwise support forensic investigation.

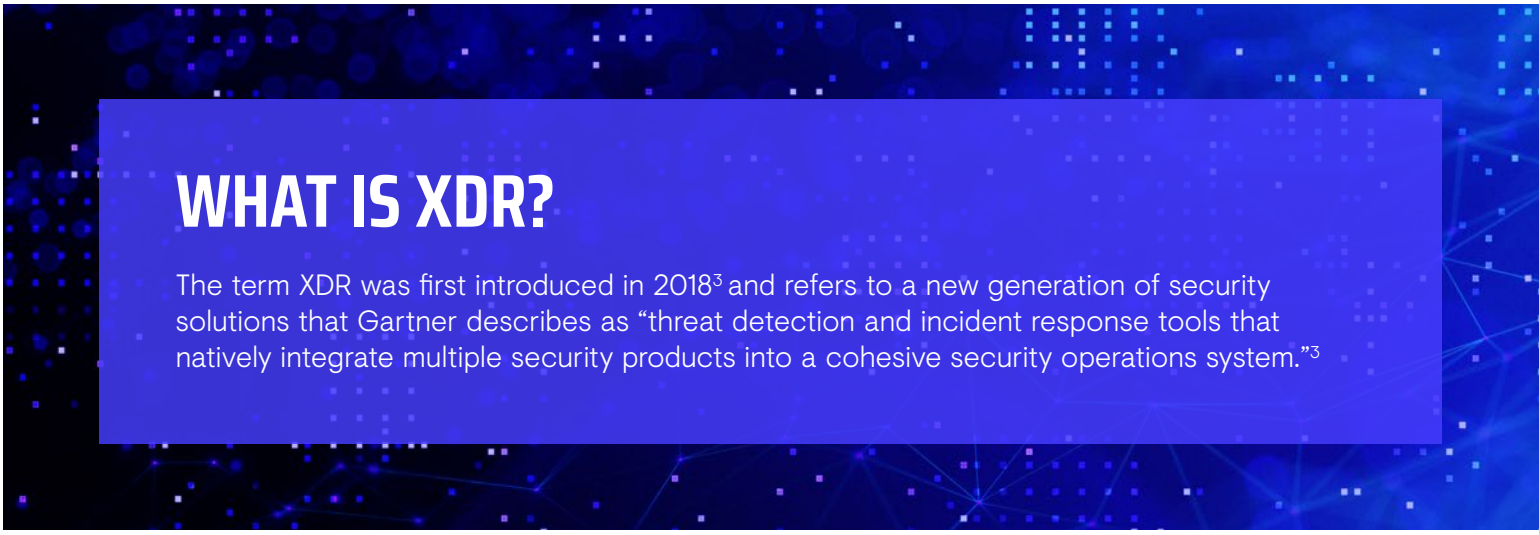
THE MOST CHALLENGING ATTRIBUTES OF SIEM FOR ORGANIZATIONS, ACCORDING TO A SURVEY FROM ESG[2]



What SIEM technology has not historically provided is any built-in ability to correlate an organization's current alert/telemetry data with the known behaviors of threat actors based on current threat intelligence. Without this built-in threat intelligence, conventional SIEM technology also lacks the built-in security workflows to guide SecOps staff through identification, response, and remediation of active threats.

[2]ESG: The Impact of XDR in the Modern SOC

The end-to-end kill chain process is critical for effective risk mitigation but can be lost in an organization relying exclusively on SIEM as their "single pane of glass." No combination of security tools delivers 100 percent invulnerability against breach. But when threat actors can wreak tremendous havoc if they are allowed to work clandestinely for too long, SIEM can leave organizations relying solely on the time, effort, and skills of their SecOps teams, who are often stretched thin. In security terms, this can be a recipe for disaster.



WHAT IS XDR?

The term XDR was first introduced in 2018[3] and refers to a new generation of security solutions that Gartner describes as "threat detection and incident response tools that natively integrate multiple security products into a cohesive security operations system."[3]

Distinctive attributes of XDR-class solutions include:

- **Data aggregation of high-efficacy telemetry** across endpoints, servers, networks, clouds, email, and applications. This data aggregation must also cross firewall, intrusion detection and prevention, and other security controls within the environment.
- **Data analysis and correlation against threat intelligence** that exposes and identifies potentially malicious activity in the environment based on behavioral clues.
- **Ongoing use of machine learning and human intelligence** inputs to continuously improve sensitivity and accuracy of threat detection.
- **Native support for effective incident investigation and response** with built-in security investigation workflows.
- **Integrated access to threat-specific guidance** for remediation, restoration, and enhancement of preventive cyber-defenses.
- **Fully automated and/or automated assistance** for remedial actions, along with threat-specific remediation "playbooks" based on current research and best practices.

[3]Forrester: XDR Defined: Giving Meaning to Extended Detection and Response

XDR thus improves upon traditional EDR (Endpoint Detection and Response) in two critical ways:

1. It goes beyond EDR's endpoint telemetry to include network, cloud, identity, email, and other systems that up until now could only be aggregated via SIEM
2. It transcends EDR's reactive malware detection and antivirus functionality with proactive detection of and accelerated kill-chain response to evolving advanced threats — including and especially those that have breached an organization's endpoint/perimeter defenses.

XDR vs. SIEM

Based on the above descriptions, we can see that SIEM and XDR are functionally distinct and are suited for two very different purposes. Given the emergence of XDR, it is clear that SIEM has limitations and there are specific situations where it should be used, but one is not robust security. The chart below offers a useful side-by-side comparison:

Description	XDR	SIEM
Open platform for aggregating telemetry and security-relevant data from diverse sources	✓	Varies
Complex log storage or governance, risk management, and compliance (GRC) use cases	✗	✓
Long-term data retention for compliance and audit	Varies	✓
Correlates behavioral indicators with threat intelligence to detect & identify advanced threats	✓	✗
Applies both machine learning and ongoing human intelligence to continuously improve and update threat detection and identification	✓	✗
Facilitates collaborative investigations so SecOps teams and their external partners can accelerate urgent kill-chain and remediation processes	✓	✗
Helps SecOps respond to and remediate security issues faster and more efficiently with automated actions and proven playbooks	✓	Add-on Required
Licensing	By Coverage	By Data Volume

Based on this comparison, organizations that have made significant investments in SIEM may still choose to use it for compliance and auditing purposes—especially in verticals such as finance and healthcare that face significant regulatory scrutiny when it comes to safeguarding data.

XDR, on the other hand, is the most powerful platform for mitigating cybersecurity risk in a new era of expanded attack surfaces and diminished security perimeters — especially for organizations that have limited internal SecOps resources and therefore need to aggressively leverage external sources of intelligence and cybersecurity support services.

For organizations that do not have significant investments in SIEM—or that are prepared to retire those investments as part of their strategy to realign/reoptimize allocation of their cybersecurity budgets—XDR can potentially serve double-duty as both the core operational platform for SecOps and the central data repository for compliance/audit reporting without the ongoing investment of maintaining a legacy SIEM platform.

Three other issues are noteworthy regarding any XDR vs. SIEM comparison:

1. Because its licensing is typically based on data volume, **SIEM paradoxically punishes good cybersecurity practices, like defense in depth, with a financial penalty.** That penalty is likely to grow substantially in the coming years as our environments become larger and more diversified—and as we capture greater volumes of historical data. There are also high implementation costs, ongoing tuning and maintenance required, and additional licensing costs. Technology decision-makers should take these long-term licensing costs into account when determining how they can best allocate their budgets to achieve optimal results.
2. While we may view cybersecurity as primarily something we practice within our individual organizations, just the opposite is true. Cybersecurity is inherently a collective activity. We make every other organization we touch more vulnerable when we fail—and we protect every other organization we touch when we succeed. Threat intelligence is also an inherently collective undertaking, since the quality of that intelligence is highly contingent on the extent to which we share what we know.
3. From an overall security standpoint, SIEM is a completely different ecosystem than XDR. SIEMs can have the effect of being isolated, like an island, with myriad security concerns existing just outside the border of the SIEM's sphere of influence. But XDR acts as an interconnected system, with threat intelligence benefiting every angle of the environment – without introducing shared risk or increased costs.

XDR by its very nature facilitates this collective defense by both leveraging and contributing to our shared threat intelligence and by enabling truly collaborative investigation and response. XDR also facilitates collective defense simply by mitigating the exposure of every organization touched by the individual organizations that utilize it.

SIEM, in marked contrast, is inherently self-contained and private, built for log management and not for security investigation and response. SIEM thus does far less to contribute to our collective defense.

WHY IT MATTERS TODAY

A clear understanding of XDR vs. SIEM is not only necessary because of all the attention XDR is now getting in the marketplace, but also because of the new reality organizations face, which include:

- Continuing escalation of the **intensity and sophistication of cyberattacks**
- The ever-expanding **scale and complexity of the environments** SecOps is charged with protecting—especially when it comes to the use of multiple IaaS clouds and a growing number of SaaS applications (for which, like it or not, SecOps teams remain ultimately responsible)
- Severe chronic undersupply of **professional cybersecurity talent, resulting in shorter tenures and continuous turnover**
- The associated pressure to **consistently retain SecOps** staff already in place (by creating a positive work experience, preventing burnout, etc.)
- The continued pressure to ensure robust defenses to keep data and systems secure goes **beyond a compliance checkbox.**
- Greater use of **remote access** as a long-term consequence of the pandemic and work-from-anywhere policies
- **Increased demands from C-level executives** who are more concerned than ever about how breaches can adversely impact business operations, customer relationships, brand value, stock price, etc.—but who also will absolutely not write SecOps a blank check

The disparity between cybersecurity needs and cybersecurity resources, in other words, has reached a tipping point beyond which the status quo will no longer be sufficient.

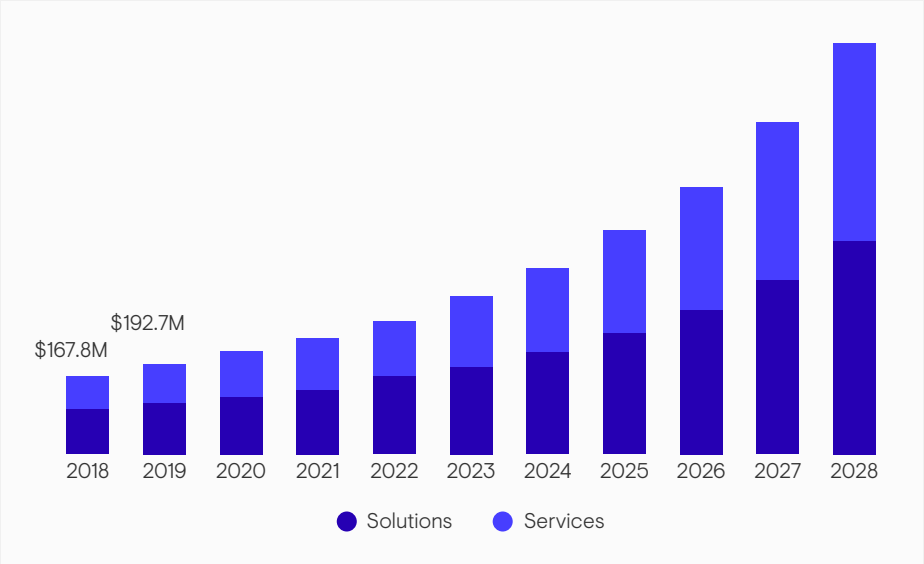
Cybersecurity leaders are therefore going to have to make some hard calls. A clear understanding of what XDR and SIEM both can and cannot do—as well as how they both impact the resource-efficiency of SecOps teams—is essential for anyone who must make the right call for the long-term well-being of the organization they serve.

> As security information and event management (SIEM) technology becomes outdated and less effective, cloud-delivered security analytics platforms that provide custom detections will dictate which providers will lead the pack.[4]
>
> **FORRESTER**

> In response to the growing security skills gap and attacker trends, extended detection and response (XDR) tools, machine learning (ML), and automation capability are emerging to improve security operations productivity and detection accuracy.[5]
>
> **GARTNER**

ESCALATING CYBERSECURITY PRESSURES DRIVE XDR ADOPTION

The XDR market is projected to grow at 19.6% CAGR[6]



[4]The Forrester Wave: Security Analytics Platforms, Q4 2020 report
[5]Top Security and Risk Management Trends June 2020
[6]XDR Market Size, Share & Trends Analysis, Grand View Research, April 2021

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp