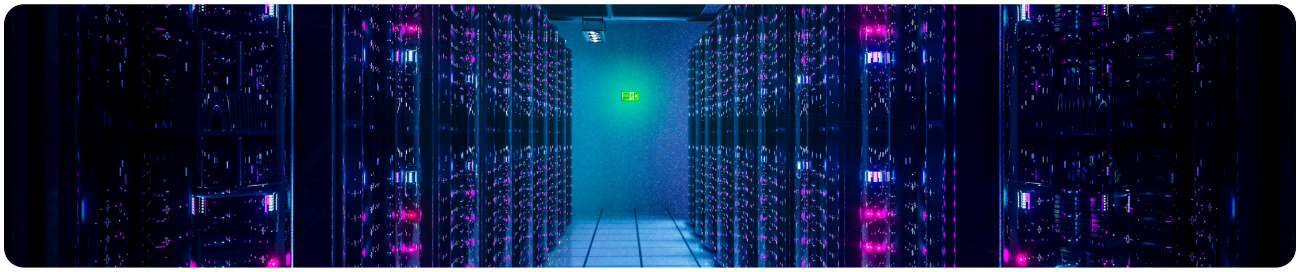
# What is SIEM and Why you Need it



The right SIEM platform can save you time, money, and keep you protected.In today's world, many businesses are finding themselves sandwiched between ever-evolving threats and compliance regulations. And while strict adherence to compliance protocols is a basic tenet of cybersecurity, keeping up with the latest regulations while also monitoring for known threats can be a challenge in and of itself. More challenging still is monitoring for unknown threats like zero-days. That's why choosing the right SIEM platform is so important.

SIEM can help your organization meet regulatory compliance requirements and improve threat detection at the same time. Here's how.

# What is SIEM and What are the Benefits?

- Hollistic overview of your network
- Identify security gaps & compliance violations
- Detailed security reporting

Security Information and Event Management (SIEM) is a staple of any good cybersecurity program. But they also come with the added benefit of helping businesses streamline regulatory compliance.

By consolidating information from different hosts, and sources across your environment, SIEM solutions provide a holistic picture of what is going on across your organization. This is done by carrying out a range of functions such as searching for insecure protocols or unauthorized network connections as well as monitoring log-ins and log-offs. This data is then used to create detailed event logs and alerts, allowing a unified reporting to better identify security gaps and compliance violations.

In addition to maintaining compliance, the right SIEM platform can provide you with a comprehensive overview of malicious threats. The data included in event logs, alerts and automated reports are analyzed in near real-time to give you a big-picture assessment of the overall state of your cybersecurity posture..

secnap

# The Hidden Costs and Drawbacks of SIEM

Unpredictable pricing can be costly

Requires extensive tuning to be effective

While there are a wide variety of SIEM solutions—ranging from those hosted in the Cloud to those hosted on-premises and even hybrid systems— most can be divided into two major categories: stand-alone solutions and managed.

Stand-alone SIEM solutions are typically self-managed, out-of-the-box products that provide your organization with a centralized way to track compliance and monitor threats. Due to the self-managed nature of stand-alone solutions, upfront they can seem like the more cost-effective solution. At least, it appears that way. Many SIEMs are priced unpredictably due to their consumption-based model. And there are also hidden costs when it comes to maintaining a stand-alone SIEM.

The modern SIEM has become overly complex and costly. For the average SMB, the amount of data that is logged and analyzed daily can be staggering. Couple this with having to pay personnel across the three shifts you'll need for 24/7 monitoring, and the economical advantages of stand-alone SIEM start to fade.

However, the real cost of stand-alone SIEM is compromised security. It is important to look for a SIEM that does not require extensive training to implement and use which may leave you in the dark when a real threat occurs. While a stand-alone solution is capable of detecting threats in real-time by manually analyzing event logs, there is typically no built-in way to respond to them. This is especially true for unknown threats.

secnap

# Managed Solutions and the Cost of SaaS

Whereas a stand-alone SIEM is managed by an organization's in-house team, managed solutions are outsourced to a Security Operations Center (SOC) which provides 24/7 threat monitoring. This has a few advantages over the stand-alone model.

First, it reduces the overall workload for your internal team by cutting down the noise and analyzing the logs all while staying ahead of ever-evolving threats. Oftentimes the reason bad actors are successful is due to a misconfiguration or a missed compromise that took place days, weeks, or even months ago. However, because of this, managed solutions are much more expensive than their stand-alone counterparts. For smaller businesses with tighter budgets, they can be cost prohibitive.

Furthermore, while employing the services of a SOC increases your organizations' capacity to respond to threats, the response is reactive rather than proactive due to a reliance on analyzing event logs. With ransomware attacks, phishing schemes, and other threats becoming more advanced, reactive security simply won't cut it.

# CloudJacket™ is the next step in SIEM technology

This is precisely why we created CloudJacket™. Enterprise-level protection, predictable costs, measurable value—without the burden of staffing your own SOC.

**The XDR Platform:** Our technology goes beyond a traditional SIEM. It doesn't just collect logs; it integrates rich security data from across your entire environment (endpoints, cloud, network) to provide the context needed for faster, more accurate threat detection.

**The MDR Service:** This powerful platform is managed by our 24/7 Security Operations Center (SOC). Our analysts don't just react to alerts, they proactively hunt for threats, investigate suspicious activity, and neutralize attacks before they can impact your business.

Our SIEM ingests and correlates alerts from across your environment, but it's our SOC that ensures those alerts don't become your burden. Every alert is reviewed, validated, and triaged by our analysts. Instead of being consumed by monitoring duties, your internal staff sees only what matters: verified, actionable incidents with context and clear next steps. Our approach transforms the SIEM from a stream of raw alerts into a trusted source of intelligence—freeing your team to focus on core priorities, while our SOC manages the day-to-day noise and responds to threats before they escalate.