LOGPOINT

WHY MODERNIZING SIEM CAN HELP MSSPS CAPITALIZE ON A MULTI-BILLION MARKET

Legacy tools are out-of-step with today's managed security business model

The market for security Information and event management (SIEM) solutions was worth USD 6.1 billion in 2022 and is on track to leap from USD 7.13 billion last year to USD 24.79 billion by 2031. **– Skyquest Research, February 2024**

At an annual growth rate of 16.86% (CAGR), it's no surprise that competition in the SIEM space is heating up. Cisco's monumental $28 billion acquisition of Splunk, Thoma Bravo's acquisition of Darktrace, the recent merger of Exabeam and LogRhythm, and the acquisition of IBM's QRadar Cloud software assets by Palo Alto Networks all point to a market teeming with opportunity.

Cybersecurity concerns coupled with the scale of today's threats are key drivers. Both are complicated by the sheer amount of data created and the diverse IT environments security teams have to defend. An effective SIEM capability helps overcome those challenges by providing a central management console for analyzing and acting on security data from across the network.

WHY A SIEM IS VITAL FOR MSSPs

SIEM should be an MSSP's early warning system, helping SOC analysts see across the IT environment and spot behavior that could indicate an attack on a client's network.

But determined threat actors – and the increasingly complex architectures designed to keep them out – make it harder to detect anomalous behavior. Hackers continually locate new vulnerabilities, attack in unison across multiple systems, or develop sophisticated new evasion techniques.

That has costs and consequences. Out of date SIEM tools can leave cyberattacks undetected by even the best SOC analysts until they become catastrophic events and the associated costs are considerable: lengthy remediation, damaged reputation, plus the potential for losing clients and revenue.

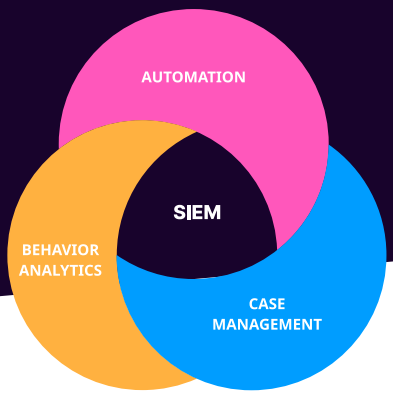
Legacy SIEMs are expensive in other ways too, with pricing based on ingested data volumes, invoices can vary wildly. They can also be technically complex, making them incompatible with AI-led innovation.

In this article we'll explain why modernizing SIEM should be a top priority for future-focused MSSPs.

KEY TAKEAWAYS

1. **Rapidly evolving threats, complex IT environments, and volatile pricing make yesterday's SIEM tools a poor fit for today's MSSPs**
2. **Modernizing SIEM strengthens security, provides new opportunities to sell value-added services, comes at a transparent and predictable cost, and makes onboarding new clients easier**
3. **A modern SIEM solution like Logpoint can also be a basis for innovative new services and AI-driven managed services solutionstesting, and comprehensive detection coverage**

WHERE LEGACY SIEMS FALL SHORT



For MSSPs, the importance of an effective SIEM capability can't be overstated. It's a vital investment in cybersecurity infrastructure – but traditional SIEM pricing is out of step with modern digital business models. Pricing is based on data volumes, meaning the more log data that's ingested, the higher the invoice is going to be for that period.

In a rapidly evolving security environment, temporary data spikes are inevitable, and the long-term trend is for volumes to increase. That makes it hard for MSSPs to stay on-forecast with their SIEM budgets.

The capabilities of legacy SIEM solutions are also out of step with today's rapid-fire threat environment. Built initially for a pre-cloud world of on-premises deployment, many SIEMs are technically closed and limited in the volume of data they can ingest. They operate at a sluggish pace, throw up too many false positives and don't scale easily to the needs of growing MSSPs.

Onboarding new clients and ingesting all their data into a legacy SIEM can take a lot of time – something SOC analysts can't afford to waste when a security alert needs assessment. Legacy SIEMs also struggle to turn all the data they ingest into meaningful threat intelligence, making it harder for MSSPs to capture trends and fine-tune the defense posture in-line with the needs of different clients.

In this article we'll explain why modernizing SIEM should be a top priority for future-focused MSSPs.

LOCKED IN THE PAST

Legacy SIEMs were designed to handle security-related data. SOCs need to correlate alerts with other events that may be occurring across a client's IT environment. In our hybrid world, where employees mix in-office and remote working, use their own devices, and connect everything to cloud services, focusing on security alone is just not fit for purpose.

To manage an expanding threat surface, MSSPs also need to monitor user activity, behavior and application access across SaaS, on premises and mixed environments. Legacy SIEMs lack the capabilities and flexibility to deliver.

Their technical limitations also make yesterday's SIEM tools a poor fit for digital innovation and the demanding data requirements of AI.

THE PROBLEM WITH LEGACY SIEM

Invoice shock: Pricing based on data volumes that can be highly variable

Out-of-date: Designed for the technical requirements of on-premises infrastructure

Complexity: Difficulty handling data ingestion from hybrid environments with multi-layered cyber defenses

Uncertainty: End-of-life solutions with unclear roadmaps

Interoperability: Difficult or impossible to integrate with other cybersecurity tools

Barrier to innovation: Incompatible with digital transformation and AI

HOW MODERNIZING SIEM SUPPORTS MSSP GROWTH

To address today's security challenges, MSSPs need a SIEM solution that gives analysts full visibility of their clients' IT estate, analyzes multitudes of data to identify trends, sorts through alerts to prioritize the most worrying, minimizes false positives and doesn't blow up quarterly budgets.

In terms of capabilities, SIEM should add power to the SOC, helping analysts anticipate the threats might be lurking in anomalous activity and quickly take action to limit clients' vulnerability.

For that, MSSPs need an AI-powered solution that can go beyond simple correlation to analyze all the data clients are generating and identify both right-now and future threats. With a blend of real-time monitoring and predictive modelling, MSSPs gain a clearer picture of client needs enabling them to pinpoint measures and services that could make them safer.

THE BENEFITS OF MODERN SIEM

1. **Pricing based on number of log sources not ingested data volumes**
2. **Collect and analyze event logs and data feeds in real time**
3. **Better protection for clients, improve ability to identifying attacks when they happen**
4. **Extend customer relationships and create innovative new services**
5. **Simplify new client onboarding**
6. **Advanced analytics for threat detection and compliance**
7. **Assess incident severity and business impact**

WHY LOGPOINT IS THE ANSWER

Logpoint delivers a Modern SIEM solution that provides accelerated detection and response to security events. It gives MSSPs a wealth of integrations with market-leading security applications, ensuring it's a flexible fit for the MSSPs business and technology strategy. With Logpoint as the central security solution, SOC analysts can quickly examine the correlation of events and use Threat Intelligence for faster validation.

Logpoint's SIEM software collects and aggregates security data generated throughout the end customer's infrastructure, from host systems and applications, whether on-premises or in the cloud, from networking and security devices like firewalls and routers.

It then identifies, categorizes and analyzes incidents and events to deliver real-time alerts, to the security operations center, enabling efficient analytics across all data sources though user-friendly dashboards.

LogPoint's underlying architecture is entirely flexible and scales linearly for large and complex implementations. It can be deployed in physical or virtual environments, on-premise or in the cloud.

WHAT LOGPOINT DELIVERS

Predictable pricing

Simplified budget management from pricing based on the number of endpoints a client has, rather than the amount of data they generate. You pay as you grow.

Easy onboarding

Interoperable with most client and MSSP IT infrastructure, Logpoint integrates easily. Adding SIEM services for a new or existing client is simple and straightforward.

New revenue streams

MSSPs can extend their client relationships with modular new services for ensuring compliance, enhancing automation, or delivering ore sophisticated analytics around detection and behavior.

AI-driven Network Detection & Response (NDR)

Enhanced visibility and situational awareness to significantly improve your ability to detect, investigate, and respond to cyber threats – ultimately minimizing cyber risk.

Real-time analysis

Collecting and analyzing log data from across a client's IT ecosystem in compliance with industry-specific regulatory mandates and reporting requirements.

Centralized control

Aggregation of data from the entire customer IT infrastructure for different events over multiple machines or across a given period, providing a centralized security console for all clients.

Active threat hunting

Accelerated detection and response for security events and incidents, enabling SOC analysts to become more efficient threat hunters and forensic investigators.

Intelligent automation

Logpoint accelerates alert triage and optimizes SOC analyst time, ensuring that no threat goes unnoticed. MSSPs reduce their clients' cybersecurity risk by applying automated playbooks for rapid investigation, containment, and removal of threats.

Advanced threat intelligence

Real time analysis of security event data from applications, the cloud, and core infrastructure to learn precisely what goes on within the network, capturing trends and recognizing anomalies as they happen.

MSSP SUCCESS STORY:

METCLOUD
GET CONNECTED • CYBER SAFE

METCLOUD is a multi-award-winning UK Sovereign Cloud provider that harnesses sophisticated cyber defense, surveillance, AI and machine learning technologies to deliver a host of advanced MSSP services.

Named Data Centre ICT Systems Vendor of the Year at the 2024 DCS Awards, METCLOUD is a recognized innovator, continually scanning the horizon for emerging threats and trends that will impact its clients' future security needs.

In 2018 the company adopted Logpoint as its SIEM partner. As a European vendor, Logpoint was a perfect fit for the data sovereignty requirements of METCLOUD's critical national infrastructure clients.

Then in 2023 METCLOUD began offering Logpoint Converged SIEM and support services to clients as part of its award-winning sovereign cloud offering. Logpoint technology would also form part of METCLOUD's proprietary AI and Data Analytics services, fully integrated with Logpoint converged SIEM to further accelerate the speed of threat detection and remediation.

> **For data sovereignty reasons we wanted a SIEM that was UK and European focused,** said Ian Vickers, CEO of METCLOUD. **The pricing model was also attractive that gave us centralized control over the software in our own environment. It is a simple, elegant solution that has proven to be very effective.**

Logpoint's technical elegance has also helped METCLOUD innovate. AISOC, its new AI-driven service offering, blends Logpoint SIEM technology with machine learning algorithms to create 'virtual SOCs.' The aim is to democratize access to security operations center capabilities and scale them for the needs and budgets of smaller companies.

> **Cybersecurity is all about having rapid insight into what's going on within customers environments,** adds Vickers. **Logpoint allows us to do that. It's elegant in its dashboard capabilities and integrations with other tools and frameworks. That has been really important for us.**

STRENGTHENING MSSP BUSINESS MODELS

MSSPs face a host of business challenges, from managing a complex threat landscape, to dealing with talent shortages, achieving compliance, scaling capabilities, growing client relationships and controlling costs.

Whether its developing new services or stopping today's threat actors from compromising client systems, modernizing SIEM with Logpoint can be the foundation for a new phase of growth.

Want to learn more?

Please visit www.logpoint.com for further information or email mssp@logpoint.com.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — Logpoint helps organizations and partners protect against cyberattacks and streamline security operations by combining sophisticated technology and a profound understanding of customer challenges. Logpoint's threat detection, investigation, and response solution brings together SIEM, SOAR, case management, and user and entity behavior analysis technologies. It empowers European organizations to achieve security outcomes across any premise through high-quality data, continuously updated security content, flexible deployment options, and industry-best predictable licensing. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification and a SOC 2 Type II compliance. This demonstrates Logpoint's strengthened focus on data protection and data and cybersecurity regulations adherence. For more information, visit **http://www.logpoint.com.**

For more information, visit **www.logpoint.com**