CyberProof®
A UST Company | Better Security, Together.

Google Cloud

# 7 Benefits of Managed SIEM for Google SecOps

## What is SIEM?

> “SIEM (Security Information and Event Management) gives security teams a central place to collect, aggregate, and analyze volumes of data across an enterprise, effectively streamlining security workflows.”[1]

In today's cybersecurity landscape, CISOs are being pulled in dozens of different directions. The rise of Artificial Intelligence is changing both offensive and defensive strategies, and the cybersecurity skills gap has left four million vacancies globally.[2] Security analysts are tasked with keeping tabs on applications, servers, network devices, traffic, and resource utilization, and can no longer manage the growing volume of data without the help of automation. Overall, PWC has found that just 2% of companies are optimizing across nine key cyber resilience best practices.[3]

Driven by this complex organizational landscape, SIEM is now a critical piece of the enterprise security toolset, and includes:

### Log management

Automatically gathering and organizing a wide range of data into a single centralized dashboard.

### Events management

Sorting data to uncover behaviors, patterns, or relationships that may signify a threat, including leveraging historical data.

### Incident response

Providing intelligent and prioritized alerts related to a security event or incident, including audit logs and reporting for compliance.

[1] Microsoft, What is SIEM

[2] WeForum, Cybersecurity Skills Shortage 2024

[3] PWC, Global Digital Trust Insights

# Top Business Benefits of SIEM

## Real-time Security Monitoring and Analytics

*The average Mean-Time-to-Detect (MTTD) for a data breach in 2023 was 204 days.*[4]

By transforming raw data into actionable insights, a SIEM solution supports analysts in uncovering threats before significant damage can impact the business. With continuous monitoring and correlation across multiple security tools at scale, SIEM can handle large data volumes pulled from on-premises, cloud and hybrid sources. Google Cloud SecOps leverages Google's infrastructure to detect threats in near real-time, analyzing telemetry at Google speed and scale.

## Curated Detection and Alert Prioritization

*73% of security experts have missed, ignored, or failed to act on a critical alert.*[5]

A strong SIEM tool will offer curated detections out-of-the-box such as MITRE ATT&CK mapping. This allows analysts to prioritize their alerts and focus on high-risk threats in business context, leveraging expert threat intelligence to reduce MTTD and alleviate the challenge of false positives.

## Enhanced Incident Investigation and Threat Hunting

*93% of CISOs are concerned about dark web threats, but 21% of CISOs have no threat intelligence capabilities at all*[6]

SIEM is a powerful weapon in comprehensive incident investigation and threat hunting, with the ability to analyze and correlate Indicators of Compromise (IaC) across multiple sources. Benefit from high-speed search, workflow automation and integrated threat intelligence to identify and neutralize a wide range of threats faster. Google SecOps uses threat intelligence to detect novel attacks quickly, supporting up to 30,000 alerts per rule for greater coverage without extensive engineering.

## Unified Threat Detection, Investigation, and Response

*SOC teams spend 32% of the day on incidents that pose no threat.*[7]

By coordinating workflows across detection, investigation and response, SIEM facilitates automated processes for the SOC (Security Operations Center), improving overall efficiency and resilience. Look for features such as an incident workbench to foster collaboration, and automated playbooks to help you hit the ground running.

## Optimized Compliance and Reporting

*68% of security teams do not believe they could comply with the SECs's four-day disclosure rule*[8]

Compliance is a growing challenge, and one that organizations can't hope to overcome without a strong strategy. SIEM helps companies to gather and verify compliance data, and meet and exceed requirements such as HIPAA, PCI-DSS and GDPR, with detailed frameworks and audit trails, comprehensive logging, and in-depth reporting tools.

[4] IBM, Cost of a Data Breach 2023 | [5] Security Magazine, June 2024 | [6] Searchlight Cyber, Proactive Defense, 2023 | [7] Morning Consult Report 2023, Security Intelligence | [8] VikingCloud, 2024 Cyber Threat Landscape Report

## Ultimate Scalability and Flexibility

*The number of organizations that maintain minimum viable cyber resilience is down 30% in 2024*[9]

As security environments grow in complexity, SIEM's ability to scale vertically for hardware resources and horizontally to cover increasing server instances is crucial. Google SecOps allows security teams to ingest and analyze data at scale, providing flexibility to handle growing data volumes and complexity. Without the need for major platform modifications, the right SIEM is future-focused, adapting to evolving challenges and technology integrations with ease.

## Cost Management and Operational Efficiency

*51% of CISOs see budget as the biggest barrier to executing their strategy*[10]

SIEM tools offer intelligent data optimization, such as tiering data to reduce storage costs, or selective data ingestion. That means critical security data is always available, without adding unnecessary overheads. Automating manual tasks improves productivity, while centralizing alerts in context reduces alert fatigue for the SOC.

[9] WEF, Global Cybersecurity Outlook, 2024
[10] Stott and May, Cybersecurity in Focus Report, Q4 2023

CyberProof®
A UST Company

Better Security,
Together.

# About CyberProof

Fortify your enterprise with cloud security transformation. CyberProof, a UST company, helps enterprises migrate to cloud-native security operations with advanced Managed Detection & Response services that allow you to protect, detect, and respond to new and existing cyber threats faster and more effectively. Our team of nation-state trained experts together with our AI virtual assistant SeeMo challenge the status quo in the cybersecurity industry with a risk-based approach that helps mitigate the potential threat to your business. Our mission is to empower your organization to anticipate, adapt, and swiftly counter cyber threats – with our global security operations centers, in-depth expertise, and a portfolio of services including Tailored Threat Intelligence, Advanced Threat Hunting, Use Case Management, and more. See: www.cyberproof.com