Managed Google SecOps SIEM & SOAR

The Cost and Resource Advantages of a Managed Approach vs. Running Your Own SIEM In-House

CloudWave

EXECUTIVE SUMMARY

Healthcare organizations face an increasingly hostile cybersecurity landscape, with threat actors specifically targeting hospitals, clinics, and health systems for their valuable patient data and critical operational infrastructure. At the same time, healthcare IT teams are stretched thinner than ever—juggling EHR migrations, regulatory compliance, clinical system support, and cybersecurity with limited staff and constrained budgets.

A Security Information and Event Management (SIEM) platform combined with Security Orchestration, Automation, and Response (SOAR) capabilities is essential to detecting and responding to threats in real time. But the decision of **how** to deploy and operate a SIEM can make or break your security program's effectiveness—and your budget.

Google SecOps

This document outlines the compelling cost and resource advantages of choosing CloudWave's Managed Google SecOps over purchasing, deploying, and running a SIEM solution in-house.

KEY TAKEAWAY

CloudWave's Managed Google SecOps delivers enterprise-grade SIEM and SOAR capabilities without the burden of hiring, training, and retaining a full-time SOC team—**saving healthcare organizations an estimated 40–60% in total cost of ownership** while dramatically improving detection and response times.

THE IN-HOUSE SIEM CHALLENGE

Operating a SIEM solution in-house may seem appealing for the control it offers, but the reality is that most healthcare organizations significantly underestimate the total cost of ownership and operational complexity involved. Here are the key challenges:

STAFFING AND TALENT COSTS

Running a SIEM effectively requires dedicated, specialized staff who can configure the platform, write and tune detection rules, analyze alerts, investigate incidents, and maintain the infrastructure 24/7/365. For most healthcare organizations, this means hiring:

- **SIEM Engineers:** To deploy, configure, integrate data sources, and maintain the platform ($90K–$140K+ per year)
- **SOC Analysts (Tier 1–3):** Minimum of 5–8 FTEs required for 24/7 coverage ($75K–$130K per analyst)
- **Threat Hunters / Detection Engineers:** To write and tune YARA-L or custom rules and investigate advanced threats ($110K–$160K+)
- **A SIEM Manager or Security Operations Lead:** To oversee the program and report to leadership ($130K–$180K+)

When you factor in benefits, training, and turnover costs, the annual staffing cost alone for a small in-house SOC easily exceeds $800K–$1.5M. And in a market where cybersecurity talent is scarce—especially professionals who understand healthcare workflows and compliance—recruiting and retaining this team is an ongoing battle.

> Annual staffing cost alone for a small in-house SOC easily exceeds $800K–$1.5M

INFRASTRUCTURE AND LICENSING

Beyond staffing, in-house SIEM requires significant capital and operational expenditure:

- **SIEM Licensing:** Many traditional SIEM vendors charge based on data ingestion volume, creating unpredicable costs that grow as your environment expands. Enterprise platforms can cost $100K–$400K+ annually
- **Storage and Compute:** Petabyte-scale log storage, retention for compliance (often 12+ months), and the compute resources to correlate and search that data
- **Hardware and Data Center Costs:** On-premises deployments require servers, networking, power, cooling, and physical security
- **Integration and Maintenance:** Connecting all your log sources—EHR systems, medical devices, network infrastructure, cloud services, endpoint agents—and keeping those integrations working through updates and changes

ALERT FATIGUE AND OPERATIONAL BURDEN

One of the most common failures of in-house SIEM is **alert fatigue.** Without expert tuning and automation, SIEM platforms generate thousands of alerts per day—the vast majority of which are false positives. Understaffed teams quickly become overwhelmed, and real threats slip through the noise. Without a SOAR platform to automate triage and response workflows, every alert requires manual investigation, dramatically increasing mean time to detect (MTTD) and mean time to respond (MTTR).

OPPORTUNITY COST

Every dollar and every hour your IT team spends managing a SIEM in-house is a dollar and hour they are not spending on EHR optimization, clinical system support, digital transformation initiatives, or other projects that directly improve patient care and operational efficiency.

THE HEALTHCARE REALITY

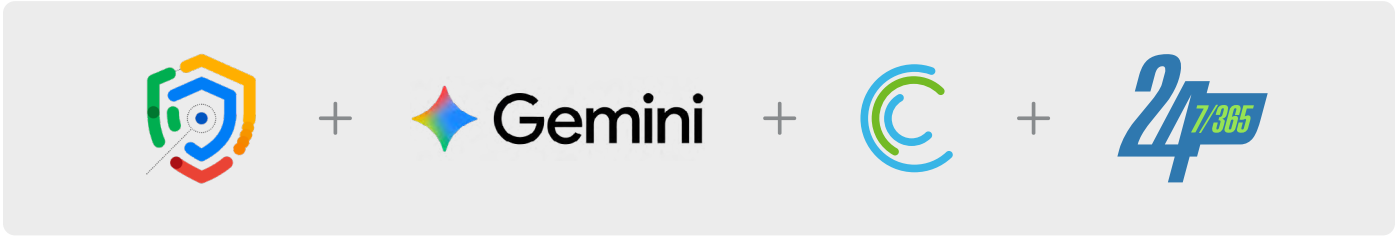
With workforce shortages projected to continue through 2032 and **healthcare system costs rising at double-digit rates**, dedicating scarce IT and security resources to building and maintaining an in-house SOC is an increasingly difficult proposition for healthcare organizations of any size.

THE CLOUDWAVE MANAGED GOOGLE SECOPS ADVANTAGE

CloudWave's Managed Google SecOps combines the power of Google's cloud-native SIEM and SOAR platform with CloudWave's deep healthcare cybersecurity expertise. Rather than building and staffing your own SOC, you get a fully managed security operations capability delivered by a team that understands healthcare inside and out.

WHAT YOU GET

- **Google SecOps SIEM:** Cloud-native, petabyte-scale log ingestion and correlation with 12 months of hot data retention, sub-second search, and 800+ built-in parsers. Named a Leader in the 2025 Gartner Magic Quadrant for SIEM
- **Google SecOps SOAR:** Automated playbooks, case management, and 300+ tool integrations to orchestrate response across your entire security stack
- **Google Threat Intelligence:** Integrated threat intelligence from Mandiant, VirusTotal, and Google's global visibility into the threat landscape
- **Gemini AI:** Built-in AI that helps analysts search data using natural language, create detections, summarize investigations, and respond faster
- **CloudWave's Healthcare SOC Team:** 24/7/365 monitoring, alert triage, investigation, and incident response by analysts who understand clinical workflows, HIPAA requirements, and healthcare-specific threat vectors
- **Healthcare-Tuned Detections:** Custom detection rules tuned for healthcare environments—EHR access patterns, medical device anomalies, HIPAA-sensitive data movements, and more
- **Patient Safety-First Remediation:** Remediation approaches that prioritize continuity of patient care, not just IT containment



COST COMPARISON: IN-HOUSE VS. CLOUDWAVE MANAGED

The following comparison illustrates the estimated annual costs for a mid-size healthcare organization (1,000–5,000 endpoints) operating a SIEM program either in-house or through CloudWave's managed service:

Cost Category	In-House SIEM	CloudWave Managed
SIEM / SOAR Licensing	$150K – $400K+	**Included**
SOC Staffing (24/7 coverage)	$800K – $1.5M+	**Included**
Infrastructure / Storage	$50K – $200K+	**Included**
Threat Intelligence Feeds	$30K – $100K+	**Included**
Training & Certification	$20K – $60K	**Included**
Recruitment & Turnover	$50K – $150K+	**Eliminated**
Estimated Annual Total	**$1.1M – $2.4M+**	**Predictable, Bundled Fee**

Note: In-house estimates are based on industry averages for mid-size healthcare organizations. Actual costs vary by region, organization size, and SIEM vendor selection.

RESOURCE IMPACT: SIDE-BY-SIDE

Dimension	In-House SIEM	CloudWave Managed
Time to Deploy	6–12+ months	**Weeks**
Staff Required	5–8+ dedicated FTEs	**0 dedicated FTEs**
24/7 Coverage	Requires shift staffing	**Built in**
Detection Tuning	Your team's responsibility	**Healthcare-tuned by CloudWave**
SOAR / Automation	Requires additional purchase and setup	**Included with playbooks**
Threat Intelligence	Separate subscription required	**Mandiant + Google TI included**
Data Retention	Limited by your storage budget	**12 months hot data**
Scalability	Requires capacity planning	**Google Cloud scale**
Healthcare Expertise	Only if you can hire it	**Core to CloudWave's DNA**

WHY CLOUDWAVE FOR MANAGED GOOGLE SECOPS

Not all managed SIEM providers are created equal. What sets CloudWave apart is the combination of a world-class technology platform with healthcare-native operational expertise:

- **350+ Healthcare Organizations Served:** CloudWave doesn't dabble in healthcare—it's all we do. Our team understands clinical workflows, HIPAA and HITECH requirements, and the unique threat vectors that target hospitals and health systems
- **Deep MEDITECH and EHR Integration:** We know how to integrate with and monitor the systems that healthcare organizations actually run, including MEDITECH, Epic, Cerner, and other clinical platforms
- **Patient Safety-First Approach:** Our remediation philosophy prioritizes continuity of care. We don't just quarantine a device—we assess the clinical impact first, because in healthcare, an IT decision can be a patient safety decision
- **Predictable, Budget-Friendly Pricing:** No surprise ingestion charges, no data caps, no hidden fees. CloudWave offers predictable managed service pricing that healthcare CFOs can plan around
- **Google's Technology Backbone:** Sub-second search across petabytes of data, AI-powered investigation with Gemini, curated detections maintained by Google's threat researchers, and Mandiant threat intelligence—all delivered as a managed service
- **End-to-End Security Partnership:** CloudWave's managed Google SecOps integrates seamlessly with our broader portfolio of managed EDR/MDR, vCISO advisory services, and compliance support—giving you a unified security partner, not a collection of point tools

THE BOTTOM LINE

Healthcare organizations don't need to choose between robust cybersecurity and fiscal responsibility. CloudWave's Managed Google SecOps lets you achieve both by shifting from a capital-intensive, talent-dependent in-house model to a predictable, expertly managed service that's purpose-built for healthcare.

Reduce Costs

Save 40–60% on total cost of ownership vs. in-house SIEM

Reclaim Resources

Free your IT team to focus on clinical systems and patient care

Strengthen Security

24/7 healthcare-native SOC with Google-scale detection

NEXT STEPS

Ready to see what CloudWave's Managed Google SecOps can do for your organization? Here's how to get started:

1. **Schedule a Discovery Call**
   Our team will assess your current security posture, data sources, and operational requirements
2. **Receive a Custom Proposal**
   We'll provide a tailored scope and predictable pricing based on your environment
3. **Go Live in Weeks**
   CloudWave handles deployment, integration, and tuning so you can start seeing value fast

Let's Talk

Contact CloudWave to learn how Managed Google SecOps can transform your healthcare security operations.

CONTACT US →

© 2026 CloudWave, Inc. All rights reserved. Google SecOps, Google Cloud, Mandiant, and related marks are trademarks of Google LLC. This document is provided for informational purposes only.

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 **gocloudwave.com**

CloudWave