NETENRICH

Netenrich SecOps Operate

Google Cloud
SecOps Delivery Partner

Netenrich SecOps Operate provides continuous, expert-led engineering to ensure Google SecOps is fully operationalized, optimized, and delivers maximum security value year-round. Designed for organizations that require ongoing enhancements, quality assurance, and proactive security improvements, our solutions ensure that your security operations remain efficient and proactive to emerging threats.

Unlike one-time implementations, Netenrich SecOps Operate is designed to sustain, evolve, and optimize your security operations. While Netenrich SecOps Implement gets you started, Netenrich SecOps Operate ensures your SecOps environment continually improves with expert oversight, automation, and evolving threat detection.

What is Google SecOps?

Scale without limits with a cloud-native platform that enhances threat detection, investigation, and response using Google's AI, machine learning, and threat intelligence. The platform proactively uncovers and defends against the latest threats while making everyone more productive with AI and automation.

Key Components Include:

- Chronicle SIEM and SOAR
- Google Threat Intelligence (GTI)
- UEBA
- Google Hunt
- Gemini AI for SecOps
- Mandiant Managed Services
- Unified Data Model (UDM)

Key Benefits

- Continuous security improvement: Regular updates and reviews enhance security posture over time.
- Reduced operational burden: Offload security engineering tasks to Netenrich experts.
- Proactive threat detection and response: Detect evolving threats & achieve rapid response ability
- Optimized Google SecOps investment: Ensure your implementation evolves with your business.
- Scalable and future-proofed security operations: Adapt as your security needs grow.
- Maximize Your SecOps Investment: Netenrich extends and amplifies the success of your initial implementation investment.

Migrate to Google SecOps with ease and confidence

Ready to take your security to the next level with Google Security Operations? You're in the right place. We specialize in seamless migrations from legacy SIEMs such as Splunk and QRadar to Google SecOps—so you can swap high costs and complexity for a more streamlined, efficient future.

We do more than just deploy Google SecOps—we optimize it to fit your environment, ensuring enhanced threat detection, streamlined operations, and a robust security posture, including:

Expert Implementation and Migration Engineering

- Provisioning and deployment of Google SecOps
- Integration with your identity provider for single sign-on (SSO).
- Migration, configuration, deployment, and/or custom creation of parsers, Yara-L detection rules, and SOAR playbooks.
- Configuration of UEBA for advanced threat detection, threat intelligence feeds, and integrations for security automation.
- Integration with Google Threat Intelligence (GTI), Gemini AI, Google Hunt, Mandiant breach analytics, and Mandiant incident response.
- Comprehensive data ingestion from identified log sources.
- Migration and enhancement of detection rules to achieve detection parity with your existing SIEM.
- Setup and optimization of dashboards and reports.

Comprehensive and Ongoing Engineering

With Netenrich SecOps Operate, you gain access to continuous security engineering support that enhances your Google SecOps environment, including:

- Ongoing engineering to enhance Google SecOps capabilities:
  - Data engineering: Development and maintenance of log ingestion standard and custom parsers with quality reviews.
  - Detection engineering: Continuous improvement of Yara-L detection rules (standard and custom) with quality assurance.
  - Response automation: Regular updates and optimizations for standard and customSOAR playbooks.
  - Dashboards and reporting: Ongoing enhancements to standard and custom dashboards.
- Regular security reviews to ensure Google SecOps adjusts to evolving security needs.
- Training sessions to keep teams updated on new features and best practices.

Continuous Data Engineering

We maintain, optimize, and ensure high-quality data ingestion and processing within Google SecOps.

- Regular parser updates for standard and custom log sources.
- Continuous data validation and normalization for accuracy.
- Custom API ingestion and enrichment for additional context.
- Ongoing monitoring of ingestion health and compliance reporting.

Enhanced Detection Engineering

Our expert engineering team ensures that detection rules evolve with emerging threats.

- Periodic reviews and updates of Yara-L detection rules for accuracy and relevance.
- Integration of new threat intelligence feeds for advanced threat detection.
- Validation of log source-to-detection coverage and MITRE mapping
- Review and enhancement of detection logic using UDM field analysis

Optimized Response Automation

We continuously refine response workflows to improve operational efficiency.

- Ongoing SOAR playbook development and updates.
- Refinement of automated response workflows based on attack trends.
- Continuous alignment with MITRE ATT&CK and other security frameworks.
- Enhancements to response orchestration for faster incident mitigation.

Regular Security Reviews and Training

We ensure your Google SecOps implementation remains efficient and aligned with best practices.

- Monthly reviews of detection, response, and log ingestion strategies.
- Performance and security audits to identify areas of improvement.
- Training programs to upskill security teams and improve operational efficiency.

The Netenrich Advantage

4+
years of Experience in Implementing Google SecOps

200+
Google SecOps Implementations across the globe

40+
playbooks consolidated in to 3 streamlined workflows

147%
improvement in detection coverage

92%
threat coverage mapped to MITRE ATT&CK framework

50%
reduction in response time

50%
reduction in manual triaging efforts

Your Team, Supercharged

We work alongside your internal teams or MSSPs, acting as an extension of your security operations center (SOC). With Netenrich, you don't just get a vendor — you get a partner who operationalizes Google SecOps for measurable outcomes.

> **Netenrich brought an unparalleled clarity and control to our once-complex security environment. By consolidating over 40 playbooks into just three streamlined workflows in Google Secops and boosting detection coverage by a remarkable 147%, they've enabled us to respond with better speed and precision.**

Andy Palaniappan | President and COO, Cloud Security Group

Solution Component	What We Deliver	Impact & Value
Implementation Support	One-time Google SecOps implementation engagement	Smooth onboarding and implementation that is foundation for long-term operational success
Data Engineering	Log ingestion parsers (standard & custom) with quality reviews	Maintains ingestion quality, addresses new log sources, and ensures long-term accuracy
Detection Engineering	Yara-L rules (curated and custom) with ongoing reviews	Evolves detections with threat landscape, reduces alert fatigue and blind spots
Response Automation	SOAR playbooks (standard and custom) with periodic updates	Ensures rapid, context-aware responses aligned with current threats
Dashboards & Reports	Regular optimization of security and compliance dashboards	Provides continuous visibility, regulatory alignment, and operational insights
Threat Intelligence	Integration and continuous tuning for improved detection	Enables proactive threat defense, enhances threat context and response precision
Security Reviews	Monthly analysis of security effectiveness and improvement	Delivers measurable improvements, maintains operational alignment and efficiency
Training	Ongoing knowledge transfer and best practice updates	Ensures in-house teams grow capabilities and stay aligned with SecOps evolution

A Smarter Way to Operate Google SecOps

Operationalizing Google SecOps requires more than just implementation—it demands ongoing refinement and engineering excellence. Netenrich SecOps Operate provides the expertise and support you need to sustain a powerful, adaptive, and efficient security operations environment.

Netenrich is a global leader in engineering and data-driven IT and cybersecurity operations. Our Adaptive Solutions, powered by Google Cloud Security, leverages AI and big data to deliver customized experiences and data-driven results for every customer. With a focus on agility and innovation, our solution evolves with changing needs and dynamic environments.