NETENRICH

Netenrich SecOps Implement

Google Cloud
SecOps Delivery Partner

Key Benefits

- Faster time-to-value: A rapid and seamless implementation and migration process that minimizes disruptions.
- Tailored implementation: A security deployment customized to your business, industry, and risk landscape.
- Future-ready security: A foundation for AI-driven analytics and automation.
- Optimized cost efficiency: Avoid common pitfalls such as over-provisioning and misconfigurations.
- Scalability and flexibility: An architecture designed to evolve with your business.
- Continuous security improvements: An implementation that strengthens your security posture over time.

Seamless Implementation and Migration for Google SecOps

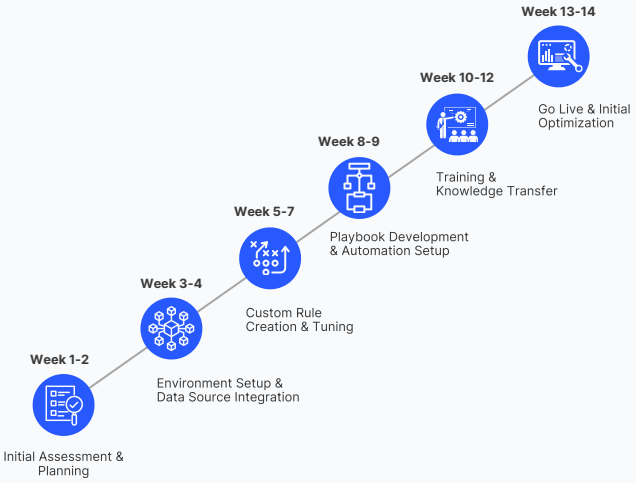
Migrating to Google Security Operations platform is a game changer for your organization's security team. But getting the platform up and running can be challenging. Netenrich SecOps Implement provides expert-led implementation and migration for Google SecOps, facilitating rapid adoption, strengthened security posture, and rapid time-to-value. Whether transitioning from a legacy SIEM like Splunk, QRadar, Exabeam, or initiating a new deployment, our tailored approach ensures your Google SecOps environment aligns with your specific security and compliance requirements.

Expert Implementation and Migration Engineering

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:

- 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 existing SIEM.
- Setup and optimization of dashboards and reports.

Typical Implementation Cadence



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)

Impact and Value of Netenrich SecOps Implement

Our solutions extend far beyond SIEM migration. Through our pioneering adaptive engineering, we create a dynamic security framework that evolves with your needs. Our integrated approach to data, detection, and response engineering ensures your protection and defenses remain robust against current and emerging threats, future-proofing your security investment.

> **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 CISO, Cloud Security Group**

Solution Component	What We Deliver	Impact and Value
Implementation	Google SecOps provisioning and deployment	Faster deployment and immediate operational readiness.
Identity & Access	SSO integration with identity provider	Seamless user access management with secure authentication.
Data Engineering	Log ingestion (standard and custom), data validation	High-quality, structured security data for reliable threat analysis.
Detection Engineering	Yara-L rules (curated and custom), UEBA, threat intelligence integration	Advanced threat detection with behavior-based analytics.
Response Engineering	SOAR playbooks (standard and custom)	Automated response workflows that accelerate mitigation.
Dashboards and Reports	OOTB and custom dashboards for security and compliance	Unified security visibility with actionable insights.
Compliance Support	Regulatory dashboards and reports	Pre-built compliance insights aligned with regulatory mandates.
Customized Enhancements	Tailored optimizations based on client requirements around best practices	Scalable, business-aligned security improvements.
Training and Support	Hands-on sessions, learning resources, and best practices for Google SecOps.	Empowers teams with proficiency, self-sufficiency and continuous improvements.

4+ Years of Experience in Implementing Google SecOps

200+ Google SecOps Implementations across the globe

Future-proof Your Security with Netenrich

Moving to Google SecOps is a strategic move towards a more adaptive and efficient security ecosystem. With Netenrich's expert implementation and migration, you can accelerate the transition, optimize your security operations, and maximize the value of Google SecOps.

Ready to enhance your security operations?

Contact us today to schedule a consultation and learn more about Netenrich SecOps Implement.

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.