NuSummit Cybersecurity | Google SecOps

SOLUTION BREIF

Empowering Security Operations with NuSummit Cybersecurity and Google SecOps

Experience Live Monitoring, Early Threat Detection, and Smooth Incident Management For Robust Security Response

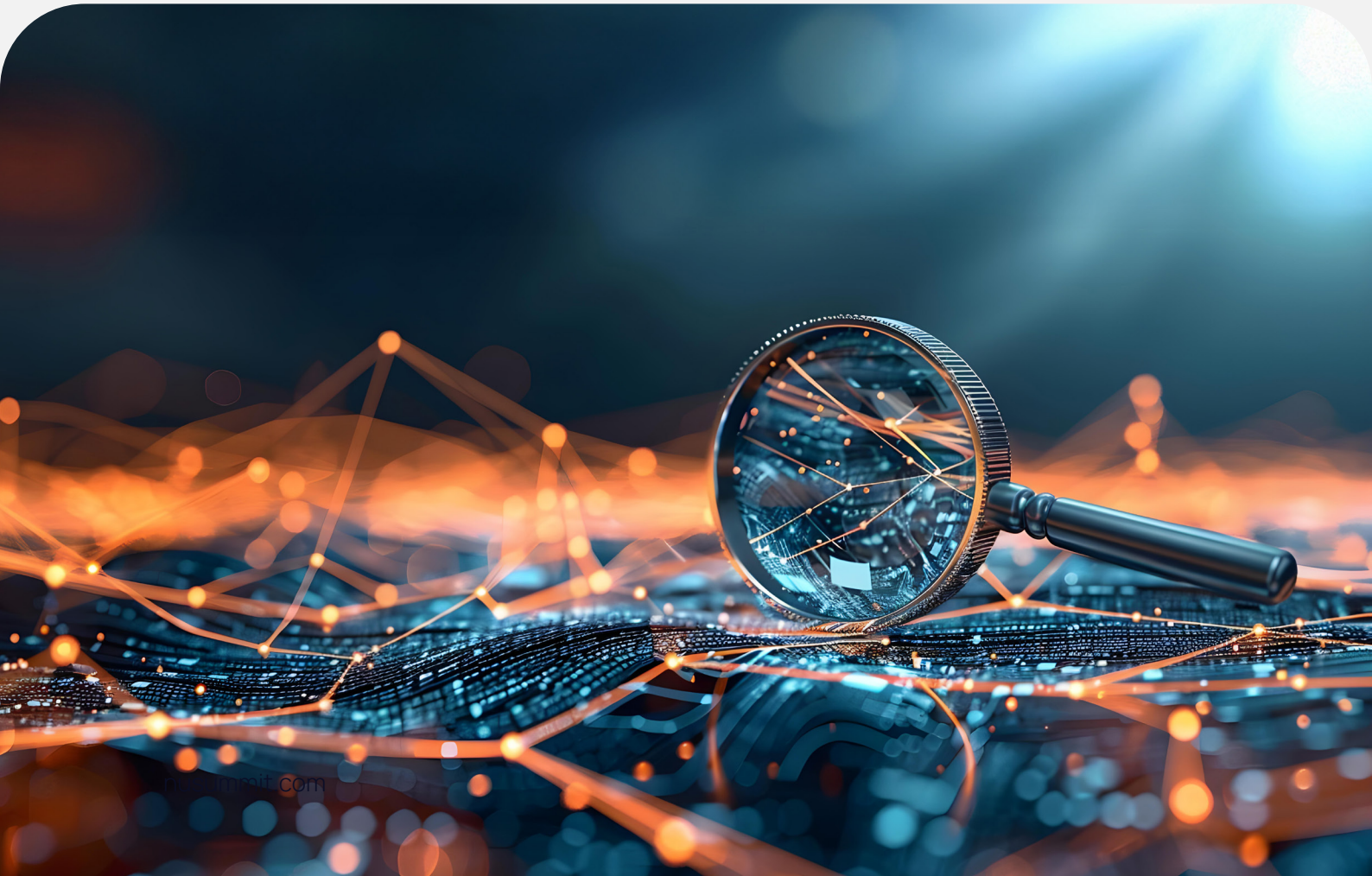


Table of Contents

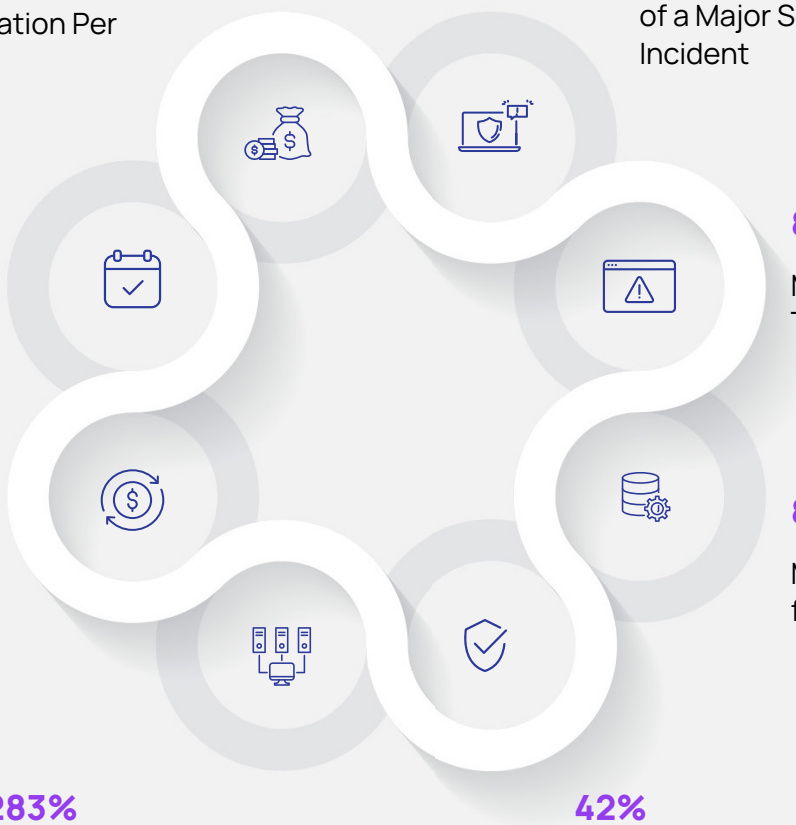
Security threat actors have started using sophisticated, specific, targeted threats against organizations. This is a critical indicator for organizations to accelerate their intent to modernize their IT security infrastructure for a heightened security posture. Google SecOps can help organizations transition from legacy security operations to advanced technologies and real-time analytics that detect, investigate, and respond to threats quickly and effectively. By consolidating security data and using machine learning, Google SecOps offers unparalleled visibility and proactive defense strategies.

According to the survey (companies using Google SecOps) conducted in Jan 2024, Google Security Operations enables organizations to analyze and correlate larger data sets. This leads to improved security outcomes and efficiencies for the team responsible for analyzing and engineering security data.

Business Value Highlights

$13.50 million
Higher Revenue Per Organization Per Year

407%
Reduced Likelihood of a Major Security Incident



7 months
To Payback

87%
More Potential Threats Identified

407%
Three-Year ROI

85%
More Capacity for Data Logs

283%
Higher Data Ingestion Volumes

42%
More Efficient Security Operations Teams

Source: IDC Business Value White Paper, sponsored by Google Cloud | January 2024

Why NuSummit Cybersecurity + Google SecOps?

Google Chronicle and NuSummit Cybersecurity provide comprehensive solutions to combat today's threats, including real-time monitoring and seamless incident management. Chronicle SIEM is a specialized cloud service built on top of Google infrastructure, designed for enterprises to securely retain, analyze, and search their extensive security and network telemetry volumes.

NuSummit Cybersecurity has been recognized as a top performer in the latest Gartner report for cloud-native SIEM despite not being in the Magic Quadrant since 2022.
Our integrated services help enterprises strengthen their online security strategies, ensure integrity, reduce fraud risk, maintain compliance, build trust, and safeguard online brand reputation effectively.

Tiered SOC Services

NuSummit Cybersecurity offers robust detection engineering services using Google Chronicle and related tools like SOAR and Applied Threat Intelligence. These services cater to small to medium-sized organizations, providing essential SOC capabilities, commercial-grade threat intelligence, and advanced cybersecurity solutions.

Our expert advisory services focus on analyzing and optimizing SIEM solutions, conducting risk assessments, and enhancing SOC operations. We specialize in integrating log sources, developing use cases and playbooks, and providing comprehensive SOC services for incident management, threat hunting, and detection engineering.

Applied Threat Intelligence Services

Google's SecOps platform integrates advanced threat intelligence for proactive threat detection and defense. It leverages Applied Threat Intelligence, combining feeds from Google, VirusTotal, and Mandiant Insights to enhance threat-hunting capabilities.

We offers Threat Intelligence services that can stand alone or be integrated into our next-generation SOC services. These services enrich alerts and incidents by integrating Mandiant and VirusTotal with SIEM/SOAR, delivering actionable intelligence. We configure Mandiant for automatic enrichment and prioritize events using machine learning.NuSummit Cybersecurity also provides industry-specific customized threat intelligence reports.

Cloud-Native Security Services

We specializes in designing and integrating native (such as VPC Firewalls, Cloud Armor, Cloud IAM, and Attack Surface Management) and third-party security controls. We utilize a cloud security reference architecture incorporating NIST, CSA CCM, Zero Trust, Data Security, and Continuous Compliance principles for robust GCP and multi-cloud security solutions.

Partnership Highlights

NuSummit Cybersecurity offers flexible delivery modes (MSSP, Captive, Hybrid) from our Bangalore and Mumbai centers in India. Our SOC services operate 24/7/365 from ISO27001-certified facilities. Our services include SLA and KPI reporting, analysis, dashboard visualization, continuous detection engineering, and end-to-end incident management. We regularly review SOC configurations and maintain a continuous improvement plan spanning 30-60-90 days.

Secure Design Advisory

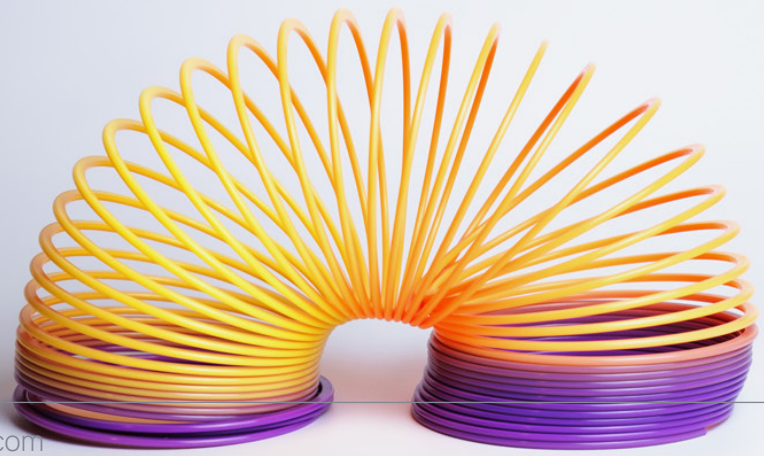
- Traditional vs cloud-native SIEM and SOAR Comaprative Study
- Risk assessment of existing setup and SIEM
- Design log sources and plan integration
- Design Chronicle workflows and alerts
- Design threat intel feeds

Secure Implementation

- Google Chronicle subscription
- Define and configure Chronicle alerts and playbooks
- Define and configure data connectors
- Define and customize Chronicle dashboard and reporting
- Define and configure ML and threat intel models

Managed Security Services

- Pre and post incidence security response SOP
- Continuous threat hunting and monitoring
- Continuous compliance reporting



Key Collaborative Strengths

Trained and Certified Professionals

- Over 200 trained and certified professionals ensure excellence in every deployment.

Industry Focus

- Tailored solutions for various sectors, addressing unique MDR challenges and regulatory landscapes.
- Demonstrated success stories in BFSI, Telecom, Manufacturing, Pharma, and beyond.

Continuous Monitoring and Threat Management

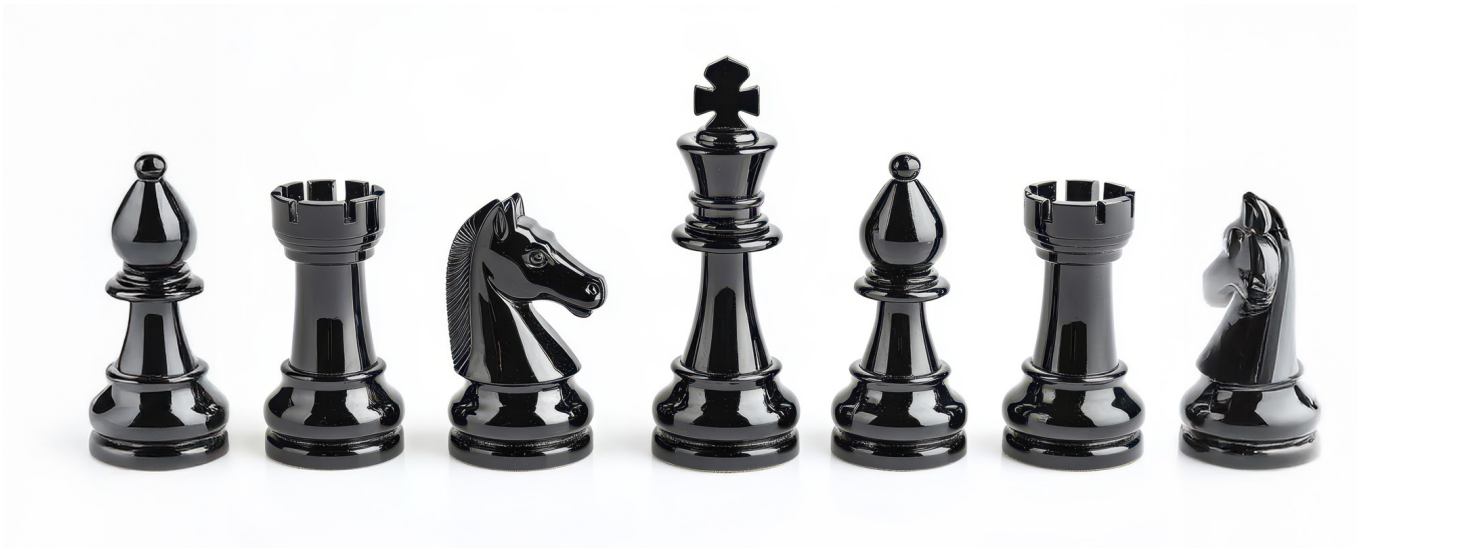
- 24x7x365 monitoring, baselining, anomaly detection and security incident response .
- Yearly, quarterly, and monthly threat-con reviews.
- Single pane visibility through in-depth dashboards.
- Industry-specific curated threat intelligence for anomaly detection and use-case enrichment.

Enhanced Threat Readiness

- Situational awareness through threat intelligence, threat modeling and threat hunting .
- Maintenance and operation of security monitoring infrastructure.

Regulatory and Compliance Assurances

- Incident response is aligned to the NIST Cybersecurity Framework's five pillars:
- Identify, Protect, Detect, Respond and Recover.



Licensing Tiers for Google Chronicle and NuSummit Cybersecurity

Feature	Standard Tier	Enterprise Tier	Enterprise Plus Tier
Base SIEM and SOAR Capabilities	Base capabilities for data ingestion, threat detection, investigation, and response.	Includes everything in Standard Tier.	Includes everything in the Enterprise Tier.
Data Ingestion	Core capabilities with 12 months of hot data retention.	Core capabilities with extended support to unlimited environments and remote agents.	Core capabilities with extended detection engine and BigQuery UDM storage.
Parsers	Full access to 700+ parsers.	Full access to 700+ parsers.	Full access to 700+ parsers.
SOAR Integrations	Full access to 300+ SOAR integrations.	Full access to 300+ SOAR integrations.	Full access to 300+ SOAR integrations.
Environments	One environment with a remote agent.	Unlimited environments with remote agents.	Unlimited environments with remote agents.
Detection Rules (Single-Event)	Supports up to 1,000 rules.	Supports up to 2,000 rules.	Supports up to 3,500 rules.
Detection Rules (Multi-Event)	Supports up to 75 rules.	Supports up to 125 rules.	Supports up to 200 rules.
UEBA (User and Entity Behavior Analytics)		Use YARA-L for custom UEBA rules, risk dashboard, and out-of-the-box UEBA detections.	Same as Enterprise Tier, plus advanced threat intelligence integration.

Feature	Standard Tier	Enterprise Tier	Enterprise Plus Tier
Threat Intelligence	Bring your own feeds.	Adds curated enriched open source intelligence (Google Safe Browsing, remote access, Benign, OSINT Threat Associations).	Adds full access to Google Threat Intelligence (Mandiant, VirusTotal, etc.).
Google Curated Detections		Access to out-of the-box detections maintained by Google experts.	Additional access to emerging threat detections based on Mandiant research.
Gemini in Security Operations		AI-driven productivity tools: natural language investigation assistant, contextualized summaries, recommended response actions, detection, and playbook creation.	Same as Enterprise Tier, with enhanced AI-driven productivity features.
BigQuery UDM Storage			Free storage for BigQuery exports for Google SecOps data up to the retention period (12 months by default).

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: