NETENRICH

RESOLUTION INTELLIGENCE CLOUD FOR SECURE OPERATIONS

TABLE OF CONTENTS

Introduction 3

Strengthen security with more data, more intelligence 3

Key benefits 3

Key scenarios 4

Have context you can act on, with ActOns™ 4

Speed Google SecOps time to value 5

How Resolution Intelligence Cloud Works 5

Top security features 6

Resolution Intelligence Cloud™ is a cloud-native data analytics platform for managing security and digital operations, with the scale and speed of Google Chronicle built in.

It goes beyond the capabilities of SIEM, SOAR, UEBA, and XDR by maximizing effectiveness with big data, real-time data analytics, machine learning, and automation.

Strengthen security with more data, more intelligence

Resolution Intelligence Cloud puts data and data analytics to work, correlating events from all detection sources across security and digital ops. The platform ingests and analyzes data from all detection sources across security and digital operations and then correlates alerts to reduce noise, identifies incidents and pre-incident situations, prioritizes them based on business risk, and provides extensive context for proactive and rapid resolution.

- **Observe everything** from a common operational view of security and digital operations data.
- **Determine what matters** without the distracting noise of irrelevant data.
- **Understand what's happening** with powerful analytics and visualizations.
- **Act quickly and proactively with rich context**, and automate processes as much as possible.

Key benefits

- **Strengthen cybersecurity and stop firefighting**. Ingest all data and proactively leverage it with advanced intelligence, machine learning, and automation. Identify and fix vulnerabilities, detect anomalies early, and avoid the flood of alerts and constant firefighting.
- **Boost productivity and effectiveness by up to 80%**. Up-level your team and save time with automation of low-level tasks, alert correlation, prioritization, and context. Working from a common operating picture, teams can resolve the most critical confirmed issues quickly and efficiently by having the information they need at their fingertips.

- **Streamline your tech stacks**. Reduce total cost of ownership (TCO) by streamlining your security and digital ops tech stacks. Using an open mesh architecture (aka **cybersecurity mesh architecture** or CSMA), Resolution Intelligence Cloud works with your tech stack now and later, so you can continuously improve without disruption.

Key scenarios

- **Detect unknowns and anomalies with behavioral analytics**: Identify anomalous behavior based on any attribute, not just user and entity behavior. Run "what if" analyses to simulate situations and observe outcomes. Investigate using Conversational AI.

- **Respond fast to what matters most, aligned to the business**: Respond fast with enriched context, automation, and collaboration. Prioritize based on business-aligned risk scoring. Over time, machine learning improves detection and automated responses.

- **Proactively find and fix vulnerabilities**: Continuously monitor your dynamic attack surface. Automatically tag assets. Identify gaps in log coverage using the MITRE ATT&CK® framework and known threat actor tactics and techniques.

- **Get comprehensive visibility and insights across environments and multiple tenants**: Achieve situational awareness across hybrid infrastructures. Get actionable insights that drive improvement and opportunities with multitenant analytics across all assets, clouds, and data centers. Provide end customers with visibility into metrics and trends that demonstrate your value.

Have context you can act on, with ActOns™

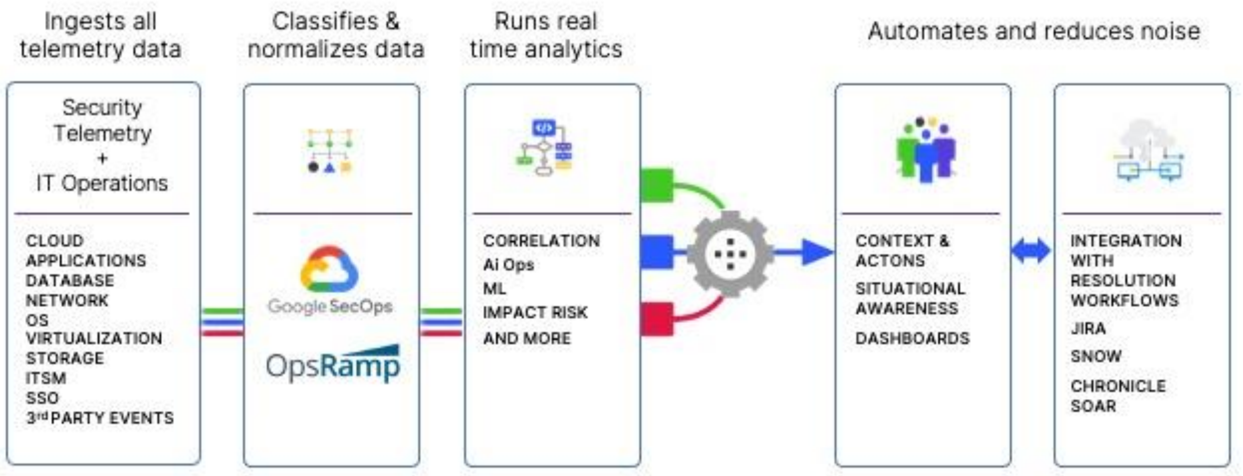
ActOns correlate the events, users, and assets that matter. They're prioritized by a business-aligned risk score based on likelihood, impact, and confidence. A single ActOn console shows correlated detections, user and asset data, evidence, MITRE ATT&CK mapping, and graphs, saving hours of research time. Instantly create a war room to securely collaborate on ActOns with colleagues and customers

Speed Google SecOps time to value

Google SecOps offers powerful, super-fast search of security telemetry at petabyte scale. Resolution Intelligence Cloud operationalizes Google SecOps, while Netenrich setup and support services ensure a smooth onboarding process — often completed in less than an hour, even with multiple Google SecOps tenants and diverse data sources. With Resolution Intelligence Cloud, you can unlock even greater Google SecOps capabilities.

For added value, consider **Netenrich Adaptive MDR**. This service seamlessly integrates with your existing security infrastructure and offers customized protection tailored to your business needs. Our team of security engineers provides 24/7 monitoring and analysis, leveraging advanced machine learning and automation to quickly detect, investigate, and respond to threats. Our adaptive MDR approach ensures proactive defense against evolving cyber threats and enhances your overall security posture without requiring significant in-house resources.

How Resolution Intelligence Cloud Works



- **Comprehensive visibility**
- **Faster resolution**
- **Lower workloads across all tenants**

Top security features

Observe: Common operational view across IT, cloud, and security

- Google SecOps built in as its infinitely scalable, fast security data lake, with hot data for a year
- Multi-level multitenancy with discretionary role-based access control (RBAC)
- Data ingestion from anywhere (cloud, hybrid, on-prem)

Detect: Monitor everywhere, detect anomalies, reduce noise

- Behavioral analytics based on any attribute, not just user behavior and entity behavior
- Attack surface management and automatic asset tagging
- Netenrich threat intel, threat models, import your own threat feeds

Understand: Get situational awareness and extensive context for analysis

- Alert correlation and prioritization based on business risk
- No-code dashboards with insights across tenants
- MITRE ATT&CK mapping

Act: Resolve faster, proactively

- Automation and AIOps: Reduce workloads
- Integration with existing resolution workflows: SOARs, ServiceNow, Jira, and more
- ActOns™: Fix issues faster with extensive context, correlated alerts, and collaboration war rooms. Observe: Common operational view across IT, Cloud, and Security