NETENRICH

carahsoft

NETENRICH

RESOLUTION INTELLIGENCE CLOUD FOR SECURE OPERATIONS

RESOLUTION INTELLIGENCE CLOUD FOR SECURE OPERATIONS

Thank you for downloading this Netenrich white paper. Carahsoft is the master government aggregator for Netenrich solutions available via GSA and other contract vehicles.

To learn how to take the next step toward acquiring Netenrich's solutions, please check out the following resources and information:

For additional resources:
carah.io/NetenrichResources

For upcoming events:
carah.io/NetenrichEvents

For additional Netenrich solutions:
carah.io/NetenrichSolutions

For additional cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Netenrich@carahsoft.com
571-591-6210

To purchase, check out the contract vehicles available for procurement:
carah.io/NetenrichContracts

For more information, contact Carahsoft or our reseller partners:
Netenrich@carahsoft.com | 571-591-6210

RESOLUTION INTELLIGENCE CLOUD FOR SECURE OPERATIONS

TABLE OF CONTENTS

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.

More than SIEM, SOAR, UEBA, and XDR, it maximizes 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 all data across security and operations, correlates alerts while minimizing noise, identifies incidents and pre-incident situations, prioritizes them by business risk, and provides extensive context for proactive, fast resolution.

- **Observe everything** from a common operational view of security and digital operations data.
- **Determine what matters** without the distracting noise of what doesn't.
- **Understand what's happening** with analytics and visualizations.
- **Act fast with context**, proactively, and automate as much as possible.

Key benefits

- **Strengthen cybersecurity and stop firefighting**. Ingest all of your data without penalty, then make use of it proactively with advanced intelligence, machine learning, and automation. Identify and fix areas of vulnerability, detect anomalies early, and avoid the flood of alerts and constant firefighting.
- **Boost productivity and effectiveness by up to 80%**. Up-level the team. Resolution Intelligence Cloud automates low-level tasks, correlates alerts, prioritizes, and provides context, saving substantial time. Working from a common operating picture, teams resolve the most critical confirmed issues first, with the information they need at their fingertips.

- **Streamline your tech stacks**. Resolution Intelligence Cloud slashes TCO by enabling you to streamline your security and digital ops tech stacks. Using an open mesh architecture (aka cybersecurity mesh architecture or CSMA), it works with your tech stack now and later, so you can continuously improve without disruption.

Key scenarios

- **Threat hunt**: Hunt for and find lurking supply chain attacks with one year of hot data and sub-second search on petabytes of data in Chronicle.

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

- **Find and fix vulnerabilities proactively**: Continuously monitor your dynamic attack surface. Automatically tag assets. Identify missing log coverage based on the MITRE ATT&CK framework and the tactics and techniques of known threat actors.

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

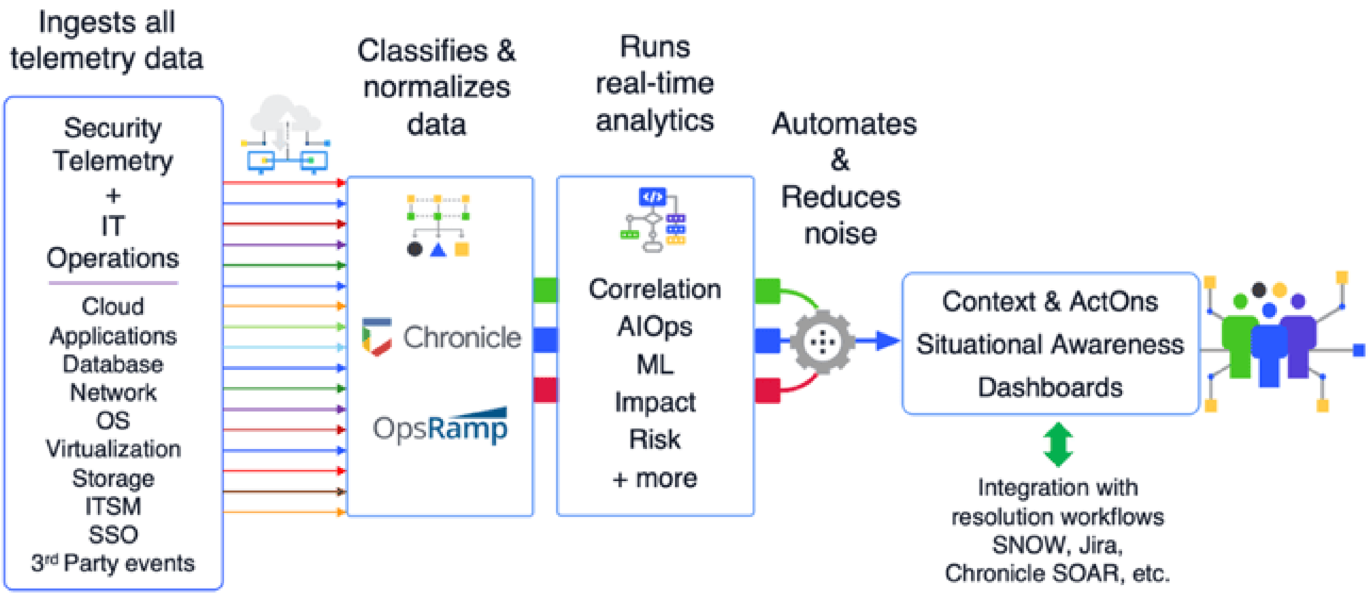
Speed Google Chronicle time to value

Chronicle is a powerful engine with super-fast search of security telemetry at petabyte scale. Resolution Intelligence Cloud operationalizes Chronicle, while Netenrich setup and support services ensure you're up to speed fast — in less than an hour with multiple Chronicle tenants and diverse data sources. With Resolution Intelligence Cloud, you can then do so much more.

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.

How Resolution Intelligence Cloud Works



Top security features

Observe: Common operational view across IT, Cloud, and Security

- Chronicle built in as its infinitely scalable, fast security data lake, with hot data for a year
- Multi-level multitenancy with discretionary RBAC (role-based access control)
- Data ingestion from anywhere (cloud, hybrid, on-prem), 1 year of hot data

Detect: Monitor everywhere, detect anomalies, reduce noise, threat hunt

- 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
- ActOns: Fix faster with extensive context, correlated alerts, collaboration war rooms
- Integration with existing resolution workflows: SOARs, ServiceNow, Jira, and more