

Resolution Intelligence[®] platform for secure operations at scale

Run with more **security**, **resilience**, **data**, and **visibility**

Unify security and digital operations

Resolution Intelligence is a native SaaS platform for unified cyber security and digital operations. With its holistic, risk-based approach to secure operations, Resolution Intelligence provides visibility and advanced insights you can act on, with ActOns™.

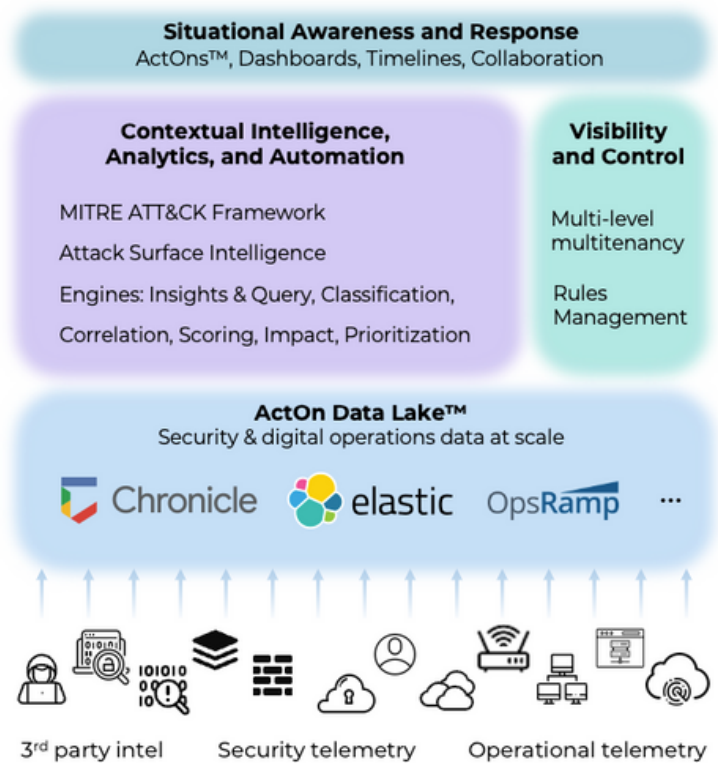
Win with Google speed and scale

Leveraging **Google Chronicle** as an infinitely scalable security data lake and other sources like Elastic, OpsRamp, and more, Resolution Intelligence enables levels of effectiveness and speed that weren't possible until now.

Grow your business

With Netenrich, you can align security and risk with business priorities, resolve issues faster, and focus on threats with the biggest impact. The result? Netenrich helps you run – and grow – your business with more confidence, not more people.

Resolution Intelligence's multi-level multitenancy gives you a single, intuitive interface for managing your clients (all, some, or any one).



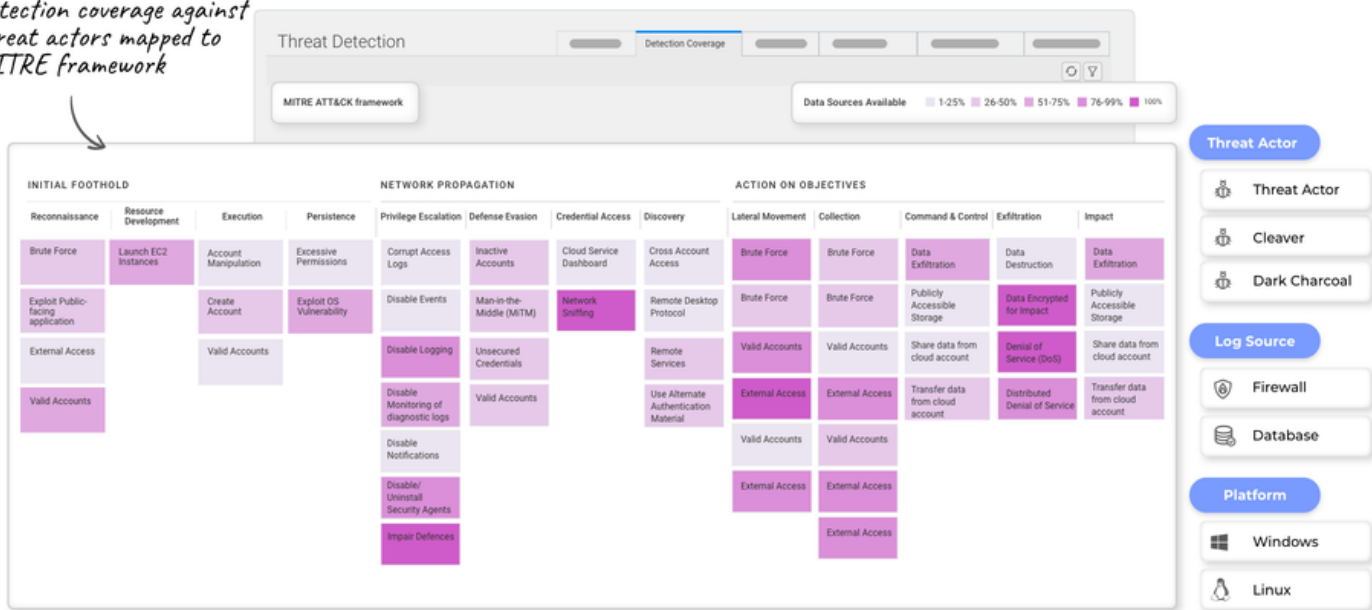
- ### Highlights
- Platform enables new services
 - Superior threat detection and response
 - Google Chronicle security data lake
 - Single interface to manage customers
 - Unlimited data, sub-second search



Put the power of unlimited security data to work

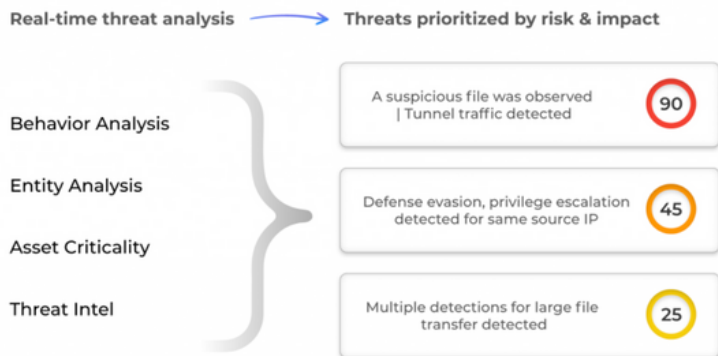
The Netenrich Resolution Intelligence platform operationalizes Google Chronicle to deliver insights and context that speed resolution, promote scale, and keep operations aligned to risk. Resolution Intelligence brings everything your IT, cloud, and security teams need to drive Google-scale insights and efficiencies across your entire environment and multiple tenants using a single interface.

Detection coverage against threat actors mapped to MITRE framework



Let your experts do more expert things

Resolution Intelligence boosts the power of Chronicle by correlating security, operational, and other data. It further streamlines incident response and speeds resolution, so your security teams waste fewer cycles chasing false positives and spend more time reducing your customers' risk exposure.



Act on curated, contextual intelligence

ActOns gather, prioritize, and present curated, contextual data – like related alerts, tickets, asset and user data – so you can focus on resolving what matters most, when it matters most. Based on advanced behavior analysis and identification of risky behaviors, ActOns are prioritized based on risk and business impact.

3. Know - prioritized by risk & impact

A suspicious file was observed | Tunnel Traffic Detected 90

Alert ID	Title	Priority	Category	Sub Category	Created Time
13196008	Epicor.Retail.Crm.CompactService Not Running	P4	Command and Control	Protocol Tunneling	21 Mar 21, 10:32
13140009	SRMain00 Not Running	P4	Discovery	Software Discovery	21 Mar 21, 10:32
13149812	Multiple alerts for device connectivity	P4	Defense Evasion	Masquerading	21 Mar 21, 10:32
13139775	Epicor.Retail.Crm.CompactService Not Running	P4	Defense Evasion	Windows Management	21 Mar 21, 10:32
13139771	Epicor Service Manager (8.3) Not Running	P4	Execution	User Execution	21 Mar 21, 10:32
13139774	Tunnel_Traffic_Detected	P4	Command and Control	Protocol Tunneling	21 Mar 21, 10:32
13139773	Discovery:Susp				10:32

Score Evidence

85 P0 High
Device down on Multiple devices
 35811537 - INC000013024205

Malware Detected
 Evaluation time: 22Mar 2022 16:40:00
 Malware: RevengeRAT. | Host: victorfranklin. | LogSource type: EDR | Product: Microsoft Defender ATP

Historically Linked To Threat Actors - 4 sighting(s)
 2 Related Threatactors: APT29 The Dukes, UNC2452.
 Most recent reference: ~18,000 organizations downloaded backdoor planted by Cozy Bear hackers

Historically Linked To Threat Actors - 4 sighting(s)
 2 Related Threatactors: APT29 The Dukes, UNC2452.
 Most recent reference: ~18,000 organizations downloaded backdoor planted by Cozy Bear hackers | Ars Technica
 Most recent link: <https://arstechnica.com/information-technology/2020/12/18000-organizations->
 Published on: 15 Dec, 2020

1. Analyze - connect event data with a what, where, and why intent

2. Detect threat, validate and enrich

Talk to a Neterich + Google Chronicle expert now

Schedule a demo at neterich.com/platform/request-demo/



Features	Benefits
Log coverage mapped to MITRE ATT&CK framework	See security blind spots. Manage detection coverage from automated mapping of log sources and detection rules to MITRE framework.
Threats mapped to MITRE ATT&CK framework	Get tactics, techniques, and mitigation suggestions of detected attacks from automated mapping of threats to MITRE framework.
Risk scoring of threats	Know what to focus on now: Get prioritized threats from a multi-dimensional analysis of detections by impact, threat, and confidence.
Detection rule packs	Gain immediate value with detection content packs covering multiple use cases.
Automated threat validation and diagnostics	Reduce response time and tedium with advanced automation that automates threat diagnostics otherwise performed by analysts.
Recommended actions	Accelerate response with recommended actions to contain threats.
Automated normalization of multi-vendor logs	Built-in custom parsers remove effort identifying and normalizing multi-vendor meta-data attributes to UDM.
Multi-level multitenancy	Define the scope of action across business units and customers from a central console
Content manager for rules, white/black filter lists, build-and-publish customer parsers	Create and manage custom content for all or any customers and business units from a single repository with role-based access control.
Collaboration and enrichment for case management + bi-directional sync with ITSM	Enhance incident response processes and protect your investments with curated context and intelligence that augments case management tools like SIEMPLIFY and ServiceNOW.
Reports and dashboards	In addition to using built-in reports and dashboards, you can easily create custom reports and dashboards without coding.

