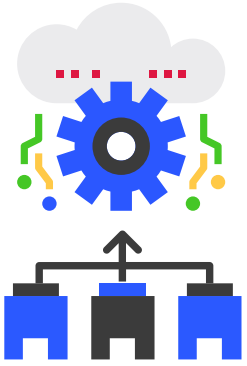
NETENRICH

Case Study



Large Global Manufacturer to Boost Security with Contextualized Data

When a large manufacturing company announced global growth plans that would triple their internal user base over the next few years, its director of IT found the news both daunting and exciting.

Daunting because her small team was already stretched thin, spending too much time responding to low-level security alerts and unsure critical issues were identified in a timely manner. Exciting because it was an opportunity to reimagine operations and demonstrate to executive leadership the value her team brings to the business.

Challenges:

Too many alerts, too few hours in the day

An increasing volume of security alerts — with too many false positives — would put the IT team at capacity. Without a formal security operations center (SOC), they took turns being "on call" after hours and addressed threats in a reactive mode. They simply lacked the resources to conduct thorough investigations into root cause, risky behaviors, and patterns — any activity that may have helped them get ahead of threats.

With the planned business growth, the director of IT knew that it was time for a change but did not want to make substantial staffing changes. Rather, she wanted to find a way to unify network and security operations, increase her team's effectiveness, and ultimately, enable them to focus more on proactive defense against threats targeting their industry.

To that end, she sought a solution that offered:

- Unlimited and affordable telemetry ingestion.
- Improved visibility across an expanding attack surface.
- Data-driven threat hunting capabilities.
- Security and operations analytics.
- Automation.

Solutions:

Resolution Intelligence Cloud™ + Google Chronicle offers the scale and speed to grow security with the business

Resolution Intelligence Cloud + Google Chronicle ticked all the boxes.

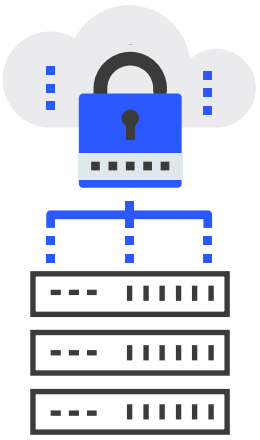
As a modern SOC and NOC workbench, Resolution Intelligence Cloud uses Chronicle as its security data lake. Chronicle ingests all security data without extra costs and maintains "hot" data for a year. On top of Chronicle, Resolution Intelligence Cloud adds multi-level multitenancy, parser and rule packs and management, real-time dashboards, and more, accelerating time to value. Critically, Resolution Intelligence also ingests operational data and applies analytics across both security and operational data, enabling it to provide extensive observability and context, find patterns over time and in real time, and enable faster incident resolution.

With more historical and contextualized data, the IT team will be able to gain better situational awareness over the full attack surface — all from a centralized console.

By automating L1 and L2 tasks, Resolution Intelligence Cloud will reduce noise and free up time for the team to focus on higher-priority issues. For example, detecting patterns of behavior and anomalies (following MITRE ATT&CK tactics), identifying critical security gaps and vulnerabilities, and resolving true incidents faster.

What's more, by mapping log sources to the MITRE ATT&CK framework, the platform will also allow the director of IT to easily show the C-suite the company's security posture. The platform's dashboard includes views into detection coverage, threat exposure, and the steps taken to secure the environment at every level — desktop, end user, and edge.

Expected outcomes and benefits:



A single pane of glass for communicating and collaborating

With Resolution Intelligence Cloud, the IT team will be better equipped to manage risk and optimize operations in support of the company's ambitious growth strategy. The platform's real-time data analytics and machine learning capabilities, which are designed to reveal risky behaviors and pre-incident situations, will help the IT team focus on the most important issues first.

With Resolution Intelligence Cloud + Google Chronicle, the company intends to increase scale and efficiency across all operations, benefiting from:

- A single pane of glass to unify NOC/SOC operations.
- High-fidelity context in ActOns to determine root cause.
- Proactive identification of blind spots and security gaps.
- AIOps to reduce alert fatigue through risk scoring and automation of L1/L2 tasks.
- Enhanced detection of availability, performance, and security issues on mission-critical assets.

