NETENRICH

LIFE SCIENCES LEADER & LARGE US COUNTY SET UP NEW SECURITY PLATFORM IN HOURS

TABLE OF CONTENTS

Introduction 1

Global life sciences leader ingests terabytes of data 4

Large US county sets up 15 Chronicle tenants 4

How does Netenrich do it? 5

Resolution Intelligence Cloud™ operationalizes security at service-provider scale. It's a cloud native, modern SaaS platform designed for ease of setup and self-provisioning in just days — even for multiple tenants, diverse data sources, and scale.

Resolution Intelligence Cloud is not a SIEM; it uses Chronicle as its security data lake. Technologies like SIEMs (Security Information and Event Management systems) can take many months to over a year to set up. But with Resolution Intelligence Cloud, you can be up and running in just days and start ingesting terabytes of data.

Customer	Time to set up	Usage
Global life sciences leader	1 day to provision and hand over	19 TB in 20 days, 32 log sources
Top-10 largest US county	1 day to provision	1.9 TB in 20 days

Customers and partners choose Resolution Intelligence Cloud to operationalize security at scale and maximize effectiveness. They want visibility into all their data without unpredictable, high costs for ingesting, storing, and searching it. They need scale and speed so they can hunt for and investigate threats, whether new and emerging or those with long dwell times. Resolution Intelligence Cloud does all that and more.

It starts with data: the more the better. Resolution Intelligence Cloud enables remarkably fast setup in less than an hour, with terabytes of data ingested in days. Setup for two recent customers, a global medical technology leader and a large US county, illustrates just how fast.

Global life sciences leader ingests terabytes of data

A global, Fortune 500 leader in patient-focused medical technology with over 14,000 employees had a managed service provider (MSSP) but wanted to bring security in house to gain visibility and control. Their in-house security team wanted access to all their data at scale and speed, to threat hunt and be more effective at managing risk and securing the business. The solution had to scale, and they needed to onboard quickly.

They selected Resolution Intelligence Cloud (Foundation and Analytics) and Google Chronicle so they could bring security functions in house, manage their security data at massive scale, threat hunt, and apply machine learning and automation to improve effectiveness and efficiency.

During the initial 45-minute kick-off meeting with the Netenrich Customer Success team, Netenrich set up the customer's Resolution Intelligence Cloud and Chronicle instance and an important log source. Netenrich showed the customer's security team how to add log sources. After the call, the customer was able to add additional log sources in hours with Resolution Intelligence Cloud's easy-to-use configuration interfaces and Chronicle's pre-built parsers.

After that initial setup meeting, the customer essentially onboarded themselves. Within days they had set up multiple log sources and ingested terabytes of data.

Large US county sets up 15 Chronicle tenants

One of the largest US counties (among the top 10) selected Chronicle and Resolution Intelligence Cloud to manage security for the agencies that they serve. The county was challenged to manage security for 17 agencies, each with its own tech stack. They needed enormous scale, access control, and ease of manageability — essentially a service-provider model at service-provider scale.

After consulting with Netenrich, they determined to follow a service-provider model, using Resolution Intelligence Cloud to manage 15 Chronicle tenants, ensuring not only role-based access control but also enabling each agency to continue to run its own tech stack, and easily manage data ingestion for all.

Setting up tenants was fast and easy, and they started ingesting data from their existing SIEM — with many diverse data sources — in 15 minutes (not a typo). Because Netenrich does not charge for additional tenants, there was no extra cost to implement this multitenant architecture.

How does Netenrich do it?

Our Resolution Intelligence Cloud platform is a cloud native, modern SaaS platform designed for ease of setup and use. The platform simplifies data ingestion by:

- Connecting directly to cloud data and populating Google Chronicle.
- Providing interfaces for configuring data feeds to Chronicle.
- Displaying real-time ingestion health and analytics, such as a dashboard showing ingestion by source over time, so you can quickly identify and correct issues.
- Providing a Content Management System for managing detection rules and parsers that run in your Chronicle instances. You can use and create rule packs, then apply rules, rule packs, and parsers to any, some, or one Chronicle tenant.

Netenrich provides quick turn-around if you need additional parsers or parser modification. If you need parsers that aren't among the over 800 pre-built parsers for Chronicle, we offer optional services to build them for you.

