NETENRICH

NETENRICH THREAT HUNTING SERVICES

TABLE OF CONTENTS

Netenrich offers subscription-based Threat Hunting Services (THS) to customers who use Resolution Intelligence Cloud™, our cloud-native platform for managing security and digital operations at scale.

> If you're stuck in low-value SOC work, you're always fighting fires. Netenrich Threat Hunting Services helps you transform security operations from firefighting to a data-driven, risk-aligned, and highly automated approach to managing threats using Netenrich's Resolution Intelligence Cloud and Google Chronicle.

Three levels of **Threat Hunting Services** subscriptions correspond to the three Resolution Intelligence Cloud plans:

THS subscription	Resolution Intelligence Cloud Platform subscription	Outcomes for security team
THS – Foundation	Foundation for Google Chronicle	Learn how to perform detection engineering like a pro. Ingest all your security data and tune detection rules.
THS - Analytics	Analytics	Learn how to threat hunt in Resolution Intelligence Cloud and Google Chronicle.

Netenrich security experts provide timely insights and guidance, rule tuning, attack surface reviews, and more while training your security team in advanced threat hunting, detection, and response techniques. In addition, Netenrich offers additional project-based services, described below.

You maintain control of your SOC: THS is not a managed "eyes on glass" service or SOC outsourcing. You maintain the relationships with your end-customers/end-users. You own your intellectual property: detection rules, parsers, and dashboards that Netenrich builds for you as part of your THS subscription are yours.

Threat Hunting Services subscription

THS for Resolution Intelligence Cloud – Foundation for Google Chronicle

Learn how to perform detection engineering like a pro with:

- Rule tuning in Chronicle
- **Threat feed** management / tuning
- Ongoing health checks
- Situational awareness reports based on Knowledge NOW (KNOW), Netenrich's free global threat intelligence service

THS for Resolution Intelligence Cloud – Analytics

Learn how to **threat hunt** in Resolution Intelligence Cloud and Google Chronicle with:

- Trend and activity reporting
- Identification of higher-value work to improve security posture
- Correlation/enrichment tuning
- Attack surface reviews

Project-Based Services

In addition to the THS subscriptions, Netenrich offers these non-recurring, project-based services:

- Custom YARA-L rules development
- Dashboard conversion/creation
- Parser building
- Splunk conversion

Threat Analytics Team: DEATH Labs

Led by John Bambenek, cybersecurity expert and Principal Threat Hunter at Netenrich, the Netenrich **Detection Engineering, Analytics, and Threat Hunting** (DEATH) Labs team uses data, data analytics, machine learning, external intelligence, Resolution Intelligence Cloud, and their deep experience to find and thwart threats. DEATH Labs delivers intelligence-driven threat awareness and analytics that improve the ability of Netenrich customers and partners to detect and respond to cyber threats targeting their high-value assets.