NETENRICH

NETENRICH ADAPTIVE MDR™ FOR GOOGLE SECOPS

....Because a One-Size-Fits-All MDR Fits No One

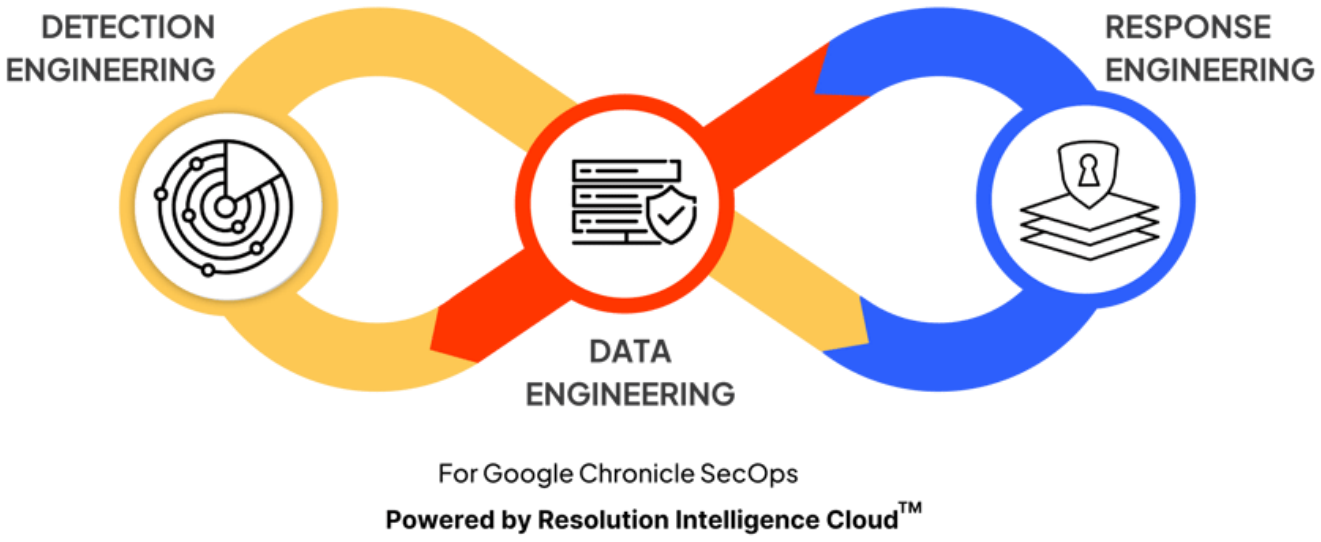
TABLE OF CONTENTS

Not all businesses operate the same way, which is why a one-size-fits-all or standardized MDR has proven inadequate for two main reasons: (a) a constantly changing threat landscape for customers, and (b) a constantly changing internal business environment for customers.

Consequently, many MDR vendors are unable to continuously customize services to address the unique threat environments and evolving needs of their customers. Worse, these MDR services become black boxes, inundating internal security teams at customers with non-contextualized alerts while restricting system access and modifications.

To address these issues, Netenrich has introduced Adaptive MDR for Google Chronicle SecOps, powered by Netenrich Resolution Intelligence Cloud technology. This solution seamlessly integrates our agile engineering-centric approach and MDR expertise with Google's best-in-class SecOps technologies (SIEM, SOAR, Mandiant, Duet AI, UEBA, and more) and sub-second search speed. It operates on a continuous, agile engineering loop of four key components — data engineering, detection engineering, response engineering, and threat hunting — to deliver continuous detection and continuous response for customers. Through this offering, we help ensure adaptive, customized, and comprehensive protection for our customers.

Making data the solution, not the problem



Data engineering

Data engineering has become increasingly important for modern organizations, especially in the cybersecurity realm, where it plays a critical role in distilling and deciphering security telemetry from diverse sources. Without agile and quality data engineering, the sheer volume of data generated daily will likely overwhelm internal teams and hinder business progress.

By proactively engineering for quality data at ingestion, our security engineers set up a data pipeline for more intelligent, customized analyses downstream, while helping organizations make faster, data-driven decisions with respect to threat response and mitigation.

Moreover, Adaptive MDR addresses the crucial aspect of parser engineering, which many customers prioritize but lack the skills to execute. Our security engineers are able to write customized parsers for each environment because they understand the unique context around new data sources at a localized level.

Detection engineering

Despite best-in-class detection rules provided by leading security vendors, adversaries are always evolving their tactics to bypass conventional detection measures and often fly under the radar by making seemingly legitimate moves within environments.

To address this issue and proactively respond to threats, it's important to observe and baseline legitimate movements or behaviors in environments and use advanced analytics to identify deviations and anomalies that may indicate suspicious or malicious activities.

With Adaptive MDR, customers don't need in-house data science expertise, as our agile detection engineering capabilities can effectively uncover the behaviors of sophisticated adversaries. Additionally, our solution is aligned with the MITRE ATT&CK framework and monitors both rules-based anomalies as well as behavioral deviations.

Response engineering

Our agile response engineering focuses on automating routine response tasks and orchestrating security technologies to streamline incident response and minimize the impact of security incidents. The process involves developing customized playbooks in Chronicle SOAR for each customer's environment and automating responses to manage and contain threats effectively. When a threat

is detected, our security engineers quickly intervene by executing these playbooks in Chronicle SOAR, which can be programmed to take predefined actions, such as shutting down ports or quarantining servers, among other things.

Continuous feedback loop: The sum is greater than the parts

Together, the three key components of Adaptive MDR operate as a continuous, agile feedback loop. When a response is executed, for example, quarantining a Linux server, it becomes a learning opportunity and prompts investigation into all other Linux servers. This agile approach emphasizes continual improvement and refinement based on ongoing insights and experiences. It also supports and optimizes hybrid SOC efficiencies and facilitates progress towards **Autonomic Security Operations** (ASO).

MDR fundamentals: Ensuring comprehensive coverage

At the same time, Netenrich delivers the essential components of an MDR service, including:

- **24/7 monitoring and response:** Bad actors don't rest, so neither do we. Around the clock, our security engineers monitor a customer's environment for potential risks and threats so that if incidents arise, they can quickly respond — and as necessary, send notifications and escalations — to effectively safeguard systems and assets.
- **SLAs for detection and response.** We outline and set clear expectations on levels of service, including commitments around threat detection and incident response.
- **MDR dashboards.** Netenrich creates customized dashboards and visualizations to facilitate security event monitoring, track key performance indicators, and gain actionable insights into overall security operations.
- **Status reports.** We provide regular reports to give customers a clear view of their security posture, including details on threats, vulnerabilities, and incident response activities. These reports can also help clients demonstrate compliance with regulatory requirements.
- **Customer success manager (CSM) and/or customer engineer (CE).** A dedicated CSM or CE helps you maximize the value and benefits of our Adaptive MDR by working with you to understand your unique requirements and ensure timely, ongoing tuning and maintenance.

- **Monthly or quarterly security review meetings.** Our security engineers deliver monthly or quarterly “security posture” assessments, reviewing areas such as threat detection and offering security recommendations.

Powered by Netenrich Resolution Intelligence Cloud

Adaptive MDR for Google SecOps leverages Resolution Intelligence Cloud, our secure data analytics platform designed to operate at Google speed and scale. Integrated with advanced technologies such as SIEM, SOAR, TIP, and UEBA, the platform helps our customers unlock the full potential of data and automate cybersecurity operations for improved incident response and cyber resilience.

Netenrich Adaptive MDR Entitlements

ENTITLEMENTS	
Data Engineering Integrate security data sources, including logs, alerts, threat intelligence feeds, and other relevant data into the Google SecOps platform.	✓
Detection Engineering Deploy detection rules and use Chronicle’s threat intelligence capabilities to identify security signals and threats effectively.	✓
Response Engineering Incident response automation and coordination to mitigate security incidents 24/7 via Chronicle SOAR.	✓
Mandiant Integration – on Managed Defense, Breach Analytics, and IR Integrate to Mandiant for hybrid SOC, advanced threat detection and analysis, breach analytics, and incident response.	✓
VirusTotal Threat Intel Feeds Integration Incorporate VirusTotal threat intelligence feeds for additional threat context and enrichment of security data.	✓
Automated Response Explore and test Google SecOps automation capabilities for responding to and mitigating security incidents, including OOTB playbook deployment.	✓

Delivery of Use Cases Deliver specific security use cases relevant to selected log sources, standard UEBA* and automated response. Use cases include insider threat detection and others.	✓
Reporting and Dashboards Create customized dashboards, reports, and visualizations to monitor security events, track key performance indicators, and gain actionable insights.	✓
Intelligent Routing Using machine learning to grasp incident context, severity, and business impact. Smart incident routing ensures timely escalation of pertinent information to appropriate individuals, leading to quicker incident resolution and reduced disruptions for organizations.	✓
24x7 Monitoring and Escalations	✓
Monthly Security Review Proactive assessment of an organization's security posture, delivered by a team of experts who monitor and respond to threats around the clock. The review covers key areas such as threat detections and security recommendations.	✓

* *For Google SecOps ENT & E+ SKUs*

Netenrich Adaptive MDR Outcomes At-a-Glance

Our engineering-driven approach provides 24/7 uninterrupted protection with tangible results, including increased visibility; enhanced data hygiene, quality, coverage, lineage, and integrity; improved detection and analysis correlation to eliminate false negatives; reduced mean time to detect (MTTD) and mean time to resolve (MTTR); and improved task prioritization and overall operational agility and efficiency.

Contact us

Learn more at **www.netenrich.com.**