NETENRICH

CSG TRANSFORMS SECURITY OPERATIONS WITH **NETENRICH ADAPTIVE MDR** FOR GOOGLE SECOPS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cloud Software Group (CSG), a $4.5 billion global software leader, embarked on a transformative security operations modernization journey. Faced with skyrocketing costs and operational challenges from its Splunk and XSOAR-based security architecture, the company sought a more scalable, cost-effective solution to align with its rapid growth and acquisition strategy.

Within an ambitious 12-week timeline, Netenrich successfully migrated CSG's entire security operations across all its subsidiaries to Google SecOps Enterprise with Mandiant Breach Analytics and UEBA, achieving remarkable results. Leveraging **Netenrich's Adaptive MDR™**, built on the **Resolution Intelligence Cloud™** platform, CSG achieved a more than a 50% reduction in security operational expenses, enhanced its visibility across its business units, and streamlined its security processes. The transformation delivered enhanced threat detection efficacy, faster response times, and a proactive security posture, positioning CSG for long-term scalability and operational excellence.

CUSTOMER PROFILE

Cloud Software Group (CSG) is a $4.5 billion holding company managing Citrix, TIBCO, NetScaler, JasperSoft, Spotfire, XenServer, and Information Builders. With a global footprint spanning over 100 countries and a workforce of 8,500+, CSG supports more than 100 million users in critical industries such as healthcare, finance, manufacturing, and retail.

As the company expanded through acquisitions, its legacy security operations struggled to keep pace, exposing limitations in cost, scalability, and performance. These underscored the need for a modernized and unified security solution. As a leader in business-critical software solutions, CSG's security infrastructure needed to maintain the highest standards of protection while supporting rapid business growth.

CHALLENGES

CSG's existing SOC Platform had become a costly and potentially detrimental bottleneck:

1. **Excessive Costs**
   CSG's annual security expenditures were considerable, with a significant portion allocated to Splunk licensing and infrastructure maintenance. As the company expanded through acquisitions, the need to scale the system placed additional pressure on the budget. Furthermore, the rising cost of talent became the largest expense, largely due to high turnover and the ongoing struggle to retain skilled personnel.

2. **Talent Retention Issues**
   Limited career growth opportunities for SOC team members led to frequent turnover, resulting in a constant need to onboard and train new hires.

3. **Scalability Roadblocks**
   Each new subsidiary required custom configurations for detection rules and log ingestion, resulting in inconsistent processes and longer onboarding times. This hindered CSG's ability to efficiently integrate acquisitions.

4. **Operational Complexity**
   The SOC team managed 40+ disparate playbooks, tailored for individual business units, leading to unnecessary complexity and duplication of effort. Each playbook demanded significant manual intervention, stretching resources thin.

5. **Limited Visibility and Efficacy**
   Siloed architecture and inconsistent data ingestion created blind spots, reducing situational awareness and delaying threat detection and response. The lack of standardized data formats further complicated integration with new tools.

Netenrich has transformed our security operations by delivering meaningful and measurable results. Their Adaptive MDR solution slashed our annual security costs by over 50% while reducing our response times to an impressive 15 minutes. With enhanced detection performance and a scalable framework, we are better equipped to safeguard our business and proactively adapt to future security demands.

Andy Nallappan, President and COO, Cloud Software Group

THE NETENRICH SOLUTION

To address this, Netenrich implemented its Adaptive MDR solution, powered by the **Resolution Intelligence Cloud™**, and expertly migrated CSG to the Google SecOps platform.

1. **Streamlined Playbook Management**
   Netenrich consolidated CSG's 40+ playbooks into three standardized workflows: incident triage, threat investigation, and response automation. These were aligned across all subsidiaries, ensuring consistency and streamlining operations.

2. **Enhanced Data Engineering**
   Netenrich implemented Google's Universal Data Model to unify data ingestion, normalize logs from disparate sources, and eliminate blind spots. The system expanded from 24 to 40 log sources, now ingesting and processing more than 2 TB of data daily, providing comprehensive visibility. Eight custom parsers were built to standardize data formats, complemented by the implementation of 194 out-of-the-box (OOTB) detection rules and 212 custom detection rules to ensure thorough coverage across all data sources.

3. **AI-Driven Threat Detection**
   Advanced machine learning models were deployed to replace 234 Splunk search queries with behavior-based detection coverage, consolidating into 26 behavior-based rules. This improved detection efficacy, achieving 99% coverage of critical alerts. The transition from traditional query-based detection to behavior-based analysis significantly enhanced the system's ability to identify and respond to emerging threats.

4. **Proactive Security Posture**
   The solution introduced continuous monitoring, signal analysis, and impact-based workflows, reducing mean time to detect and respond by 60–70%. This improvement allowed CSG to transition from reactive measures to a proactive security approach, enhancing threat anticipation and mitigation capabilities.

5. **Leverage Google SecOps Capabilities**
   Effectively used unlimited storage capabilities to address scalability concerns, enabling unrestricted data ingestion. Additionally, Mandiant's integrated threat intelligence provided enriched data insights, minimizing manual enrichment efforts and improving detection accuracy.

Netenrich brought unparalleled clarity and control to our once-complex security environment. By consolidating over 40 playbooks into just three streamlined workflows and boosting detection coverage by a remarkable 147%, they've enabled us to respond with better speed and precision. Their data-driven approach has ensured our operations align seamlessly with our growth strategy.

Kumar Palaniappan, CISO, Cloud Software Group

NETENRICH APPROACH

Netenrich executed the migration in three phases over 12 weeks, ensuring minimal disruption to CSG's ongoing operations:

1. **Data Engineering**
   Netenrich assessed CSG's existing log sources, built eight custom parsers, and aligned them with Google's Universal Data Model. This eliminated inconsistencies across subsidiaries.

2. **Detection Engineering**
   Threat models were redesigned to focus on behavior-based rules, ensuring comprehensive coverage with minimal noise. AI and machine learning capabilities were integrated for adaptive threat identification.

3. **Response Engineering**
   Playbooks were streamlined and automated using Google SOAR capabilities, reducing manual interventions and enabling rapid responses. Custom SOAR integrations further enhanced operational workflows.

Netenrich's Adaptive MDR was instrumental in overcoming CSG's legacy challenges. The solution emphasized:

- **Signal Analysis:** Comprehensive signal correlation and prioritization improved the SOC's ability to identify and address threats with precision.
- **Automation:** AI-driven workflows and impact-based routing reduced the dependency on manual intervention, increasing performance.
- **Integration Readiness:** Custom parsers and playbooks were designed to accommodate future acquisitions and scale dynamically with business growth.

***Netenrich's Adaptive MDR** has fundamentally improved our security performance, drastically reducing manual interventions from nearly 2,000 incidents per month to fewer than 10! Their advanced threat detection and automation capabilities allow us to scale securely while proactively addressing threats.*

Mohan Sekar, Sr. Director, Head of Product Security, Cloud Software Group

OUTCOMES AND IMPACT

The transformation delivered measurable results across several dimensions:

1. **Cost Savings**
   - Annual security expenses decreased by over 50%
   - Reduced SOC staffing requirements by 80% leading to smarter resource management and lower turnover-related costs.

2. **Data-Led Security Transformation**
   - Full correlation of data sources delivers contextual insights, reducing noise and prioritizing critical alerts.
   - Improved ability to detect trends, anomalies, and potential risks in real time.
   - Future-ready infrastructure supports continuous improvements and organization updates.

3. **Enhanced Threat Detection**
   - Detection coverage improved by 147%, supported by the ingestion of diverse data sources.
   - Mean time to detect and respond reduced from hours to 15 minutes, ensuring faster containment of threats.

4. **Operational Efficiency**
   - Monthly security incidents requiring manual intervention dropped from 1,920 to fewer than 10.
   - Playbook management became 90% more efficient, enabling the SOC team to focus on proactive threat hunting.

5. **Scalability and Flexibility**
   - Reduced the acquired subsidiaries onboarding time from 3 months to under 5 days.
   - The standardized workflows allowed seamless integration of new business units, enhancing operational workflow.

6. **Improved Visibility**
   - Real-time dashboards provided comprehensive insights into security posture, operational stability, and threat landscapes.

FUTURE VISION

Netenrich's Adaptive MDR positions CSG to embrace autonomic security operations—a future where systems self-manage, adapt, and respond to threats with minimal human intervention. With its scalable architecture and data-driven approach, CSG is now equipped to tackle tomorrow's evolving and enigmatic threat landscape.

NETENRICH

Netenrich is a global leader in engineering and data-driven IT and cybersecurity operations with a proactive, shift- left approach. Our Adaptive Solutions, powered by Resolution Intelligence Cloud, leverage artificial intelligence and big data to deliver customized experiences and data-driven results for every customer. With a focus on agility and innovation, our solution evolves with changing needs and dynamic environments and brings customers one step closer to achieving autonomic operations.

As a trusted Google partner, specializing in Google SecOps. Netenrich has transformed hundreds of companies across various sectors, including healthcare, finance, and technology. From our global hubs, we provide 24/7 proactive uninterrupted operations, peak performance, and peace of mind.

Netenrich.com

