Serving up security:

Delivering a streamlined security telemetry pipeline for largest restaurant group.

Customer Profile

Headquartered in California with 2,200 branches – is the largest restaurant chain in the United States.

Related Industries

- Hospitality

Business Demands

- Security posture improvement
- Regulatory compliance

Challenges

- Heterogeneous infrastructure (Windows, Linux, network devices)
- Diversity of log types
- Unified integration with Google SecOps

Solution

NXLog
Platform

Business Results

Delivered a unified log collection pipeline, built across the client's IT infrastructure, to streamline and optimize security analysis and regulatory compliance.

Background

A fast-casual restaurant group – the world leader in dining experiences – operating thousands of locations across the country. With its size and complexity, the Group faced mounting pressure to modernize its cybersecurity infrastructure. The organization's IT environment spanned 20,000 endpoints, including Windows, Linux, macOS, and various network appliances.

In the quick-service restaurant (QSR) industry, where customer data, web services, marketplace and payment systems are critical for business continuity, cybersecurity is not just a backend function; it's a frontline necessity. High transaction volumes, distributed operations, and third-party integrations (between suppliers and delivery services, for example) create a broad opportunity for malicious actors. Indeed, high-profile breaches in similar sectors highlighted the urgent need for real-time observability, telemetry management, proactive threat detection, and regulatory compliance.

The Restaurant Group needed a powerful, flexible, and scalable solution to collect, normalize, and securely forward logs from its hybrid infrastructure to its SIEM, Google SecOps (Google Chronicle). The challenge was multi-faceted: the Group had to aggregate logs from multiple operating systems and services – including Active Directory, DNS, DHCP, IIS, PowerShell, and Linux/macOS systems – while also capturing data from third-party firewalls and appliances via UDP.

The client's legacy log shipping tools were unable to scale effectively or support the current heterogeneous environment, and the organization wanted to streamline operations without introducing another overhead. So, enabling secure, high-performance log delivery to SIEM, combined with ready-to-go integrations, became the focus of Restaurant Group's business and technical requirements.

Solution

To address these challenges and create a robust telemetry pipeline, the team adopted the NXLog Platform, alongside NXLog Agent. With it, the client could establish a real-time logging infrastructure that could feed its security and observability systems. Integrated with Google SecOps, the platform allowed for seamless, structured log forwarding and centralized management – without the need for multiple disparate log shippers.

Being a true cross-platform solution, NXLog Agent provides complete log coverage across all major operating systems. It also offers a variety of different modules for collecting data. For instance, modules like im_msvistalog collect Windows Security, Application, System event logs, PowerShell, WinRM, RDP, SMB, and WMI logs. Meanwhile, logs from Linux endpoints are managed with im_file and im_systemd, capturing both flat files and journald logs.

NXLog Agent also natively supports macOS. And, since this was already installed in the client's IT ecosystem, log data collection and performance remained uncompromised. Finally, network devices, including firewalls and appliances, were integrated with im_udp, for capturing syslog messages sent over the network to the NXLog Agent – functioning as a collector.

Once collected, and before being passed to systems such as SIEM or observability platforms (APM) for analysis, the telemetry data requires proper processing (filtered, structured, formatted, etc.). The Group's team used NXLog Agent's targeted features to normalize logs, with built-in support for IETF (syslog) and JSON to enable structured outputs. The Agent was configured to enrich these logs on-the-fly, with hostnames, timestamps, and context-aware tags. It then routed them to the standard Google Forwarder, eventually feeding data into the Google SecOps platform.

Both security and automation were strategic goals of the deployment. The NXLog Agent provided TLS-secured management (via xm_admin module) with client certificates and access control lists, which enabled secure, whole-lifecycle handling. Deployments and updates were fully automated, minimizing operational friction. And centralized credential management, along with audit trail logging, supported compliance mandates.

From a performance standpoint, NXLog Agent provided a multi-threaded pipeline and orchestration, delivering high throughput and reliability. Features such as disk buffering, message queueing, and backpressure handling added resilience and guaranteed efficient log and telemetry delivery – even under network strain.

Lastly, native integration with Google SecOps allowed NXLog Agent to forward structured logs directly to Google's platform over TCP. Recommended by Google, NXLog helped the customer establish real-time analytics and long-term retention in Google SecOps and a chained security data lake with minimal effort.

Results

Since deploying NXLog Platform, the Restoraunt Group's team has optimized its security monitoring, balanced its SIEM performance and improved the quality of security alerts, achieving close to real-time threat detection. With its security team able to gain immediate access to comprehensive, centralized log data – accelerating investigation and remediation efforts – incident response has significantly improved.

Additionally, by providing a transparent audit trail and ensuring that all necessary logs are collected, stored, easily retrievable, and properly disposed of, NXLog Platform has enabled the client to meet its compliance requirements. With log pre-filtering reducing data noise, ten Group's team has been able to boost SIEM efficiency while retaining its current licensing tier, thereby avoiding additional costs.

Finally, the autonomous telemetry pipeline powered by NXLog Platform has streamlined the client's operations by centralizing log data and unifying reporting across different teams and departments.

Results:

- ✓ Full visibility: Unified logging across 20,000+ endpoints
- ✓ Efficient SIEM integration: Real-time security data ingested by Chronicle
- ✓ Compliance and security: Fully encrypted, audit-ready log trails
- ✓ Scalable and future-proof: Flexible architecture ready for new sources and formats

NXLog

For more information about NXLog products and services, visit our website, contact us via the web form, or schedule a meeting.

Start free with the NXLog Platform now!