NXLog

Streamlining Telemetry & Strengthening Security for a Global Energy Company

© Copyright 2025 NXLog FZE.

Customer Profile

A major North American energy company, which develops and operates critical energy infrastructure across Canada, the United States, and Mexico. Focused on three primary business areas: natural gas pipelines, liquid pipelines, and power generation.

Related Industries

- Energy
- Power generation

Business Demands

- Security posture improvement
- Regulatory compliance
- Reduction in SIEM costs

Challenges

- Heterogeneous infrastructure (Windows, Linux, network devices)
- Diversity of log types
- Unified integration with Palo Alto Cortex XSIAM

Solution

NXLog Platform

Business Results

Created a unified, real-time view of DNS communications

Optimized SIEM usage by filtering irrelevant data before ingestion

Improved compliance posture through auditable, encrypted logs

Enabled advanced threat detection using previously inaccessible DNS data

Background

A leading North American energy infrastructure company sought a vendor to help it strengthen its security posture and regulatory compliance while reducing SIEM costs. Responsible for critical global pipeline systems and power facilities, it faced a growing challenge. It needed to capture and analyze high-fidelity DNS telemetry across a wide network of Windows servers as efficiently as possible.

The company handles large volumes of Windows DNS Analytical logs generated via Event Tracing for Windows (ETW). So, it needed a scalable solution to extract meaningful security signals, filter out noise, and feed actionable data into Palo Alto Cortex XSIAM. All while maintaining compliance and operational integrity.

The organization's Windows-based DNS infrastructure was both expansive and essential, serving as a key telemetry source for identifying suspicious or anomalous network behavior. However, DNS Analytical logs are notoriously complex. And transmitting them unfiltered to a SIEM/XDR platform would have overwhelmed resources and driven up costs.

Beyond sheer volume, the logs also required extensive parsing and enrichment to become truly useful for detection and investigation. The company needed a way to isolate valuable signals from background noise, standardize data format, and deliver it securely from hundreds of globally distributed systems. And it needed to do so without compromising performance or compliance posture.

© Copyright 2025 NXLog FZE.

Solution

To meet these demands, the company turned to the NXLog Platform, deploying NXLog agents across its global DNS infrastructure. NXLog's native ETW support allowed the organization to capture DNS events at source. Custom filtering rules were implemented to exclude low-value queries and noise. This refocused efforts on high-relevance events, such as unusual query types, NXDOMAIN responses, or patterns known to be associated with attack techniques.

Each event could be parsed in depth, extracting key fields like query names, types, source IPs, and response codes. NXLog then normalized this data into structured JSON and enriched it with metadata, such as the server hostname and timestamp.

TLS-based encryption and certificate-based authentication ensured the secure delivery of data to Palo Alto Cortex XSIAM, while built-in buffering and smart queuing provided reliable transportation, even during network interruptions. Finally, all event data was captured in a compliant, tamper-evident format, supporting organization-wide audit and forensic readiness.

Results

With NXLog the organization gained real-time, global visibility into security-critical DNS communications — without flooding its SIEM solution. Filtering at the edge significantly reduced ingestion costs while preserving the signal needed for advanced threat detection. Analysts were able to detect DNS-based threats that were previously hidden in noise. And the organization's compliance posture improved through consistent, encrypted, and traceable log collection.

© Copyright 2025 NXLog FZE.

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!