NXLog

Building a Modern Telemetry Pipeline for Securing an Industrial Environment

Customer Profile

A multinational critical infrastructure operator responsible for real-time industrial process control across multiple facilities and geographic regions.

Related Industries

- Oil & Gas
- Utilities

Business Demands

- Achieve compliance (e.g., NIS2, IEC 62443, ISO 27001)
- Establish end-to-end security visibility across OT and IT
- Securely transfer logs from isolated networks
- Filter noise to reduce SIEM load and costs

Challenges

- Segmentation and restricted communications
- Legacy field devices with no logs
- High data volume and SIEM costs
- Heterogeneous infrastructure

Solution

NXLog Platform

Business Results

- Delivered end-to-end OT/IT visibility
- Ensured regulatory compliance
- Reduced SIEM load by up to 80%
- Enabled faster on-site threat detection
- Provided a scalable architecture for future expansion

Background

Our client, a multinational oil and gas operator, or critical infrastructure company, is responsible for real-time industrial process control across multiple global facilities. The organization needed to meet stringent regulatory standards, including the EU NIS2 directive and industry frameworks like IEC 62443 and ISO 27001, while maintaining robust, end-to-end visibility into both operational technology (OT) and IT activities.

Each of the production site's networks was highly segmented according to the Purdue Model, with firewalls isolating each layer and restricting cross-zone communication. This made transferring logs from protected OT zones very challenging.

The client also faced an influx of log and network data from heterogeneous sources, such as Windows and Linux systems, PLCs, SCADA/HMI stations, firewalls, and data historians. It also had many legacy field devices, producing either very little or non-standard log events, to contend with.

Securely collecting and centralizing these events without overwhelming the Security Information and Event Management (SIEM) or violating network isolation was critical to achieving both regulatory compliance and proactive cybersecurity monitoring.

Solution

To address these challenges, the operator deployed the NXLog Platform in a multi-tiered, agent-and-relay architecture across all OT and IT network layers. This involved industry-ready NXLog agents being installed in the OT field and control layers (Purdue Levels 0–2) to gather a wide range of log data.

These lightweight agents collected Windows Event Logs via the im_msvistalog module, and local application log files (im_file). They even captured industrial network traffic for protocols like Siemens S7, Modbus, and DNP3 using passive packet capture (im_pcap). Because many of the legacy controllers and PLC devices couldn't host an agent or generate logs themselves, this passive network monitoring ensured that important OT events weren't missed.

The agents also applied regex-based filtering and parsing at source to discard noise and irrelevant events. This significantly reduced log volumes and downstream SIEM ingestion costs before any data left the site.

All collected logs were then compressed and encrypted for transit using NXLog's batch-compression and secure transport features (im_batchcompress over TLS-encrypted TCP or HTTPS), and forwarded upward to an intermediate logging DMZ.

At the Industrial DMZ – sometimes referred to as "Layer 3.5" – the client set up NXLog relay servers to act as aggregation and control points. These relay nodes received incoming compressed log batches from the lower layers, then decompressed and inspected the data before re-transmitting it to the IT network.

The relays performed dual routing: one stream of logs was forwarded to a local ELK stack (Elasticsearch/Logstash/Kibana) within the DMZ for immediate on-site monitoring and analysis by the operations team. Simultaneously, the relays stored a copy of all logs on local storage as a forensic archive, ensuring that even if network connections were disrupted, log data would be retained to meet regulatory retention requirements.

This DMZ-layered approach provided an extra buffer and control stage, enabling reliable, traceable log transfer across the OT/IT boundary. For example, across the firewall demarcation between control networks and enterprise networks.

Finally, logs were relayed from the DMZ to the enterprise IT and cloud layer (Purdue Levels 4–5), where the company's central SIEM systems reside. The NXLog relay at this layer forwarded the consolidated logs to two primary SIEM platforms – the on-premise IBM QRadar and Microsoft Azure Sentinel in the cloud – over secure channels.

NXLog relay automatically transformed and normalized the data into structured formats (JSON, XML, CSV) using its built-in conversion modules (xm_json, xm_xml, xm_csv) and flexible processing engine. This ensured the logs could be readily ingested and correlated by the SIEMs.

Throughout the deployment, the NXLog Platform's centralized management capabilities pushed uniform configuration updates to all agents, monitored the health of each agent and relay, and maintained an audit trail of all log collection activities. This made the multi-layer setup easier to administer and audit, despite the network's geographically distributed and segmented nature.

"Implementing NXLog Platform fundamentally changed how we monitor and secure our industrial operations. For the first time, we have real-time visibility across every layer of our OT and IT environments, without overloading our SIEM or compromising network segmentation and operations. Having a unified telemetry pipeline not only helped us meet strict regulatory requirements but also empowered our teams to detect and respond to threats faster than ever before."

- Chief Information Security Officer, multinational Oil & Gas operator.

Results

With the NXLog Platform in place, our client achieved several key outcomes:

- **Full OT/IT observability:** The organisation achieved end-to-end visibility across all layers of its environment, including capturing telemetry from OT devices where no logging agent could be installed, by utilising NXLog's passive network capture module. This bridged a crucial visibility gap in monitoring industrial control systems.
- **Regulatory compliance:** By consistently collecting and securely storing logs from all critical systems, the operator can now demonstrate compliance with NIS2, IEC 62443, ISO 27001, and other mandates. Every log is gathered and retained in a tamper-evident, auditable manner, providing documentation for regulatory audits.
- **Reduced SIEM load:** Filtering out noise at the source and compressing data at the edge led to an 80% reduction in events per second (EPS) being forwarded to the SIEM platforms. This dramatic drop in log volume cut SIEM licensing costs and improved analysis efficiency by focusing only on relevant security events.
- **Faster on-site threat detection:** Integration with a local ELK stack allows the operations security team to rapidly detect and investigate threats within the industrial network, without waiting for data to be sent to central systems. Thanks to this, they now have immediate access to parsed OT log data for real-time threat hunting and forensic analysis.
- **Scalable architecture:** The relay-based, multi-layer log collection architecture is highly adaptable to the operator's evolving needs. New sites, devices, or data sources can be onboarded by deploying additional NXLog agents or relays at the appropriate layer, without redesigning the entire system. So, the client now has a future-proof logging infrastructure that can grow with its operations and easily incorporate new industrial protocols or IT/OT integrations as needed.

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!