NXLog

Strengthening a Global Mining Company's ICS/OT Security with NXLog Platform

Customer Profile

A global mining and commodities company focused on the safe, reliable, and compliant production of metals and minerals worldwide. It operates extensive industrial control systems (ICS) and operational technology (OT) across multiple mining sites.

Related Industries

- Mining
- Metals production

Business Demands

- Security visibility across OT networks
- Faster threat detection and better response time
- Compliance with ISA/IEC 62443
- Reduction of SIEM log volume and costs

Challenges

- Fragmented logging (PLCs, SCADA, and HMI)
- Limited detection of anomalous ICS traffic
- Time-consuming compliance audits
- Weak IT/OT collaboration

Solution

NXLog Platform

Business Results

- Centralized audit-ready OT logging
- Early detection of anomalous OT traffic
- Reduced SIEM costs
- Improved IT/OT convergence

Background

A global leader in mining and commodities, our client operates many mines and processing facilities worldwide. These sites rely on complex Industrial Control Systems (ICS) and Operational Technologies (OT) to automate heavy equipment, processing plants, and safety systems. This includes SCADA software and programmable logic controllers (PLCs), which run conveyors and ventilation systems.

The company's ICS/OT environment expanded over time, blending modern and legacy systems across multiple locations. As IT and OT convergence grew, securing the environment became more difficult. With compromised ICS posing risks like operational disruptions, financial losses, and safety hazards, the company prioritized strengthening its OT security.

One of the core issues was that the client's OT infrastructure lacked centralized logging capabilities. Each mine or processing plant had devices generating logs – alarms from SCADA software, Windows-based HMI event logs, PLC status messages, etc. – but these were siloed across local systems. The logs themselves were heterogeneous and non-standardized since different ICS components often produce logs in unique formats and locations. Some SCADA components logged to text files, others to proprietary databases, and many critical events were only visible on local operator stations.

While the company still managed to operate with these complexities, this patchwork approach made it difficult to aggregate and analyze OT security events centrally. This reduced the client's security visibility, so it couldn't get a clear view of what was happening on the plant floor. Without a unified logging solution, detecting threats or security-related malfunctions in real time was nearly impossible.

The company struggled with security compliance as standards like ISA/IEC 62443 demanded auditable OT event monitoring. Its setup couldn't generate system-wide, time-correlated logs, forcing manual collection — a slow, error-prone process. This lack of visibility hindered threat detection and left the company exposed to compliance risks.

Solution

To address these challenges, the company deployed the NXLog Platform – a unified logging and monitoring solution – across its mining operations. The Platform was rolled out in the heterogeneous OT environment with minimal disruption during planned maintenance.

Lightweight NXLog agents were installed on Windows-based SCADA and HMI servers to tap into native Windows Event Logs and capture events including PLC communications, operator actions, and system alerts. For systems that produced log files or proprietary text outputs, NXLog's file capturing modules were configured to tail, read and process those files in real time.

Crucially, NXLog could also collect telemetry from industrial devices and protocols that previously had no oversight. Using its passive network capture capabilities, NXLog was set up to listen to OT network traffic (via the im_pcap module) and decode common ICS protocols, such as Modbus, OPC, DNP3, BACnet, and Siemens S7. This meant that even PLC-to-PLC communications and sensor data sent over the network could be logged and analyzed. This gave the client a much deeper security insight into its process control communications.

The deployment was carefully tailored to the company's distributed and air-gapped environments. And having an on-premise solution meant that OT data stayed within each site's secure perimeter, ready to be accessed and analyzed.

With its vendor-agnostic design, NXLog Platform can work across hybrid and air-gapped networks. This meant that NXLog agents deployed at remote mines could operate without internet access or extra dependencies. Where network bandwidth was constrained, the platform enabled data compression and high-efficiency routing to ensure that the most pertinent OT events were forwarded and compressed to minimize impact on the network. This was useful, for example, in a mine site forwarding data to a central data center over GSM/LTE/LoRa links.

NXLog's built-in buffering and failover mechanisms provided resilience if a connection to the central repository or SIEM went down. So, logs would queue locally to be automatically forwarded when the link was restored, thereby guaranteeing that all critical audit data was captured.

The client leveraged NXLog's scalability and flexibility to integrate OT logs with its centralized security monitoring. And, while NXLog agents were rolled out across dozens of sites and hundreds of devices, management remained straightforward. The platform can support tens of thousands of endpoints per management server, which is far more than needed. This gave the company confidence that the solution could scale with future expansion.

With NXLog's out-of-the-box integration capabilities, the collected OT security logs were aggregated, processed (e.g. converting proprietary ICS events into JSON or syslog) and routed to Microsoft Sentinel alongside critical IT logs. This unified approach bridged the gap between IT and OT, allowing security analysts to see OT security events in the same dashboards as IT events. This enabled the client to correlate threats across its entire enterprise. Additionally, NXLog's support for industrial protocols and custom parsing allowed the company to define rules for OT-specific anomalies. For instance, detecting any rarely used control commands and communications that appeared on the network.

Despite the environment's complexity, NXLog's pre-built configurations and straightforward agent rollout meant the deployment was completed with minimal overhead. even where isolated OT networks were concerned.

> *"NXLog closed the visibility gap in our OT networks. Now, we detect threats faster, respond sooner, and meet compliance requirements with ease — all while lowering SIEM costs and streamlining operations. We transformed our OT security posture from fragmented and reactive into centralized, proactive, and audit-ready. This shift not only strengthens operational resilience and compliance but also reduces costs and improves collaboration between IT and OT teams across all our sites."*
>
> - Client's Chief Information Security Officer

Results

With NXLog Platform, our client enhanced visibility and security monitoring across its OT environment. Critical ICS/OT events, including logins, configuration changes, alarms, and network anomalies, are now sent to the SIEM and backed up in near real time, closing the IT/OT visibility gap. This allows the SOC to detect both malware and advanced persistent threats early (e.g. those leveraging unusual Modbus communications) and respond immediately, rather than hours or days later. As such, incident response times have dropped dramatically, and data from all sites is promptly correlated to enable faster detection with less noise.

The platform also improved compliance and audit processes, thanks to centralized, time-synced logs that meet ISA/IEC 62443 and similar standards. This provides a clear record of “who did what, when.” Where preparing for audits used to take weeks of manual work, it could now be done with quick queries, helping the client meet its requirements and maintain safety and reliability.

Operationally, the NXLog Platform telemetry pipeline reduced SIEM log volume and security costs by filtering noise, while giving OT engineers insight into equipment faults for proactive maintenance and fewer outages.

IT and OT teams now share a unified view of security and system health. The result is a cohesive, scalable logging solution offering full visibility, stronger defenses, faster response times, and assured compliance across the company’s entire industrial operation.

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!