ncc group

You can't stop what you can't see.

It's time OT security caught up.

splunk> a cisco company

Contents

Section 1
Introduction and problem statement..... 4

Section 2
The value of SIEM and why Splunk wins..... 5

Section 3
Strategic benefits for industrial organisations 6

Executive Summary

Industrial organisations are facing growing pressure from advanced cyber threats targeting their Operational Technology (OT) environments (NCC Group, 2025).

These environments are the backbone of critical sectors such as manufacturing, energy, and utilities. While many have invested in OT-specific sensors, such as NCC Group's Network Detection and Response (NDR) for OT or those provided by trusted partners, the data often remains siloed. Without integration into a central analytics platform, security teams lack the visibility, context, and responsiveness needed to navigate today's threat landscape.

This whitepaper examines how integrating OT telemetry with a mature Security Information and Event Management (SIEM) platform, using Splunk as an example, can help industrial organisations maximise the value of their existing investments.

This integration supports real-time, cross-domain visibility, improves threat detection, accelerates incident response, and helps meet both resilience and regulatory demands.

Section 1

Introduction and problem statement

Digital transformation is reshaping the industrial sector, driving gains in productivity, efficiency, and competitiveness. But as OT environments become more connected to IT networks, supply chains, and remote operations, they are also becoming more exposed. Where once OT systems relied on physical isolation for protection (Munz, 2024), they now face the same cyber threats that have long targeted IT infrastructures.

This convergence is creating new challenges. Ransomware, supply chain compromises, and state-linked threats are no longer confined to IT domains, industrial networks are now firmly in scope. In fact, in 2024, industrial sectors were the target of roughly 27% of all ransomware attacks, more than any other industry (NCC Group, 2025).

On top of that, evolving geopolitical tensions have shifted the threat landscape, leading to increased scrutiny and new regulations such as NIS2, IEC 62443, and the EU Cyber Resilience Act (CRA).

While many organisations have invested in OT monitoring tools, these sensors often operate in isolation. Without integration into centralised security platforms capable of correlating across diverse log sources, there is a critical visibility gap. Threats that originate in IT and pivot towards OT frequently go undetected until it's too late (Beiboer, 2023). A sensor-only approach leaves organisations blind to the full attack chain, resulting in delayed response, longer attacker dwell times, and heightened risk to safety, operations, and compliance.

Section 2

The value of SIEM and why Splunk wins

The role of a SIEM in OT Security

A SIEM platform serves as the foundation for modern security operations. It aggregates and normalises data from multiple sources, applies analytics to detect threats, and provides the context needed to investigate and respond.

For industrial environments, a SIEM helps bridge the gap between OT and IT by enabling security teams to:

- Correlate data across domains to identify threats that move between IT systems and OT networks
- Accelerate detection by analysing logs, telemetry, and alerts in real time
- Support incident response with a clear timeline of events and actionable insights
- Improve forensic capabilities to understand how attacks unfold and prevent recurrence.

Why Splunk is the best fit

Imagine a corporate account is compromised and used to access OT systems. In isolation, an OT sensor might register anomalous activity, while IT logs track credential misuse. Without a SIEM, these events seem unrelated.

By contrast, Splunk ingests both data streams, correlates them into one high-confidence incident, and triggers an automated response, isolating affected segments and notifying both security and operations teams, thus averting potential operational impact.

Splunk offers several important advantages as a SIEM for OT security:

Flexible data ingestion and normalisation.
Splunk is capable of ingesting data from a wide variety of OT sources, including protocol logs, device telemetry, and network sensor alerts. This enables organisations to break down silos and build a unified security picture.

Advanced analytics and machine learning.
Splunk's OT-specific modules and analytics tools can baseline normal behaviour and detect anomalies that may indicate emerging threats.

Real-time event correlation.
Splunk links OT and IT events as they occur. For example, it can connect an abnormal Modbus write command with a suspicious remote desktop login, highlighting the risk of lateral movement between domains.

Automated incident response.
Splunk integrates with security orchestration tools like Splunk SOAR, allowing organisations to automate actions such as isolating affected systems, triggering alerts, or initiating containment measures.

Scalability and extensibility.
Splunk can support both small and large industrial operations, from single sites to multi-national networks, while integrating with existing IT security operations centres.

Section 3

Strategic benefits for Industrial organisations

Integrating OT telemetry with Splunk provides a range of important benefits that directly support the security, resilience, and operational objectives of industrial organisations.

One of the most significant advantages is enhanced operational resilience. By bringing OT sensor data into a central analytics platform, organisations gain the ability to detect threats earlier and in a more comprehensive manner. This early detection capability helps prevent incidents from escalating into situations that could disrupt production or compromise safety. The ability to correlate and act on security data in real time reduces the risk of unplanned downtime, which in turn protects revenue, supply chain commitments, and customer trust.

Another key benefit is improved regulatory compliance. Industrial organisations face growing pressure to demonstrate adherence to security and resilience requirements set out in frameworks such as NIS2, IEC 62443, and sector-specific standards. A centralised SIEM solution like Splunk helps simplify compliance by consolidating monitoring, detection, and reporting activities.

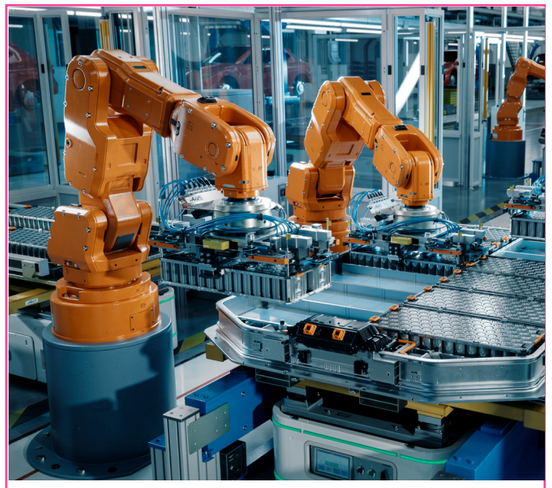
With Splunk, organisations can produce detailed, auditable records of security events and responses, making it easier to satisfy regulatory obligations and reduce the risk of penalties or reputational damage.

The integration of OT telemetry with Splunk also leads to stronger collaboration between IT and OT teams. Traditionally, these teams have worked with separate tools and data, which can make it difficult to coordinate during incidents or share insights. Splunk provides a shared view of security across both IT and OT environments, enabling teams to work together more effectively. This alignment enhances the organisation's ability to respond quickly and decisively when threats emerge, while also improving long-term security planning and risk management.

Finally, this integration helps organisations move toward a proactive security posture. Rather than reacting to incidents only after they have already had an impact, industrial organisations can use the insights generated by Splunk to identify patterns and indicators of emerging threats.

This shift from reactive to proactive security allows organisations to stay ahead of attackers, anticipate potential risks, and take action to mitigate them before they result in operational harm.

Together, these benefits help industrial organisations build a more secure, resilient, and future-ready security capability that keeps pace with the evolving threat landscape.



Case Study

Challenge: A UK manufacturing company encountered a coordinated threat across its IT and OT environments—suspicious account activity was flagged in IT systems, while OT sensors detected unauthorised commands targeting industrial controllers. Without unified visibility, these incidents would previously have been investigated in isolation, delaying threat detection and increasing risk to safety and operations.

Solution: The company integrated NCC Group's NDR for OT and Dragos sensors providing deep visibility into ICS/SCADA environments, with Splunk Enterprise Security for advanced threat detection and correlation, and Splunk SOAR to automate and accelerate incident response across IT and OT.

Result: By ingesting and correlating both IT and OT data in real time, Splunk generated a single, high-confidence alert that triggered an automated playbook. The affected OT network segment was swiftly isolated, and both security and plant operations teams were immediately notified. The threat was contained before it could impact production or compromise safety, reducing attacker dwell time and significantly enhancing the organisation's operational resilience.

Conclusion

As cyber threats grow in sophistication and increasingly target OT environments, industrial organisations must modernise their security operations to keep pace. OT sensors, like those from NCC Group and Dragos, offer essential visibility into industrial systems, but without integration into a centralised analytics and response platform, their value remains limited.

Splunk, combined with NCC Group's NDR for OT and Dragos sensors, delivers unified IT/OT visibility, advanced threat detection, and automated response capabilities. This integrated approach allows industrial organisations to detect and contain threats earlier, reduce operational and safety risks, and meet evolving regulatory requirements with confidence.

By correlating data across domains in real time and streamlining incident response, the combined solution strengthens resilience, supports proactive security, and most importantly, helps protect the safety of people and the continuity of essential operations.

Works Cited

Beiboer, R., 2023. OT Security Is Different, Isn't IT? Available at: https://www.splunk.com/en_us/blog/security/ot-security-is-different-isn-t-it.html

Munz, E., 2024. OT Security is the New Avenger in Manufacturing. Available at: https://www.splunk.com/en_us/blog/industries/ot-security-is-the-new-avenger-in-manufacturing.html

NCC Group, 2025. Cyber Threat Monitor Report 2024. Available at: https://www.nccgroup.com/uk/cyber-threat-monitor-report-2024/