

Powering Operational Resilience in the Energy Sector

With Sword and Splunk

Energy operations are becoming more connected, **and more exposed.**

Energy companies rely on complex operational technology (OT) systems to keep critical infrastructure running predictably and efficiently. But as these environments become increasingly connected to IT networks, many organisations are facing:

- **Expanded attack surface and operational risk**
- **Data overwhelm**
- **Evolving regulatory frameworks**

Together, Sword and Splunk help energy companies power operational resilience across converging IT and OT environments. By combining Sword's deep expertise in energy operations and OT cybersecurity with the Splunk unified platform, organisations can turn operational data into insights that strengthen security, empower confident decisions, and keep critical systems running.

10TB+

of data is generated every day by a typical drilling platform with 80,000 sensors

Source: ISG, The Latest Data and Cloud Trends for the Oil & Gas Industry

<1%

of oil and gas companies' vast amounts of data from sensors and logging tools is used to inform decision-making

Source: McKinsey, Digital and Advanced Analytics

Gain full visibility to reduce risk and support compliance

Bridging operational data with enterprise systems can extend visibility deep into industrial environments to better understand how physical processes and digital systems interact in real time. Splunk brings telemetry data together from across your IT and OT estate into a centralised platform. Organisations can discover, inventory, and track OT assets across facilities — from industrial control systems and sensors to network infrastructure and field devices. This includes the ability to ingest and analyse data from industrial protocols and systems such as SCADA, MQTT, Modbus, and OPC-UA.



A unified approach can help companies in the energy industry to:

Strengthen cybersecurity

Move away from disconnected tools and dashboards to proactive discovery and continuous monitoring that enables teams to detect threats earlier, prioritise incidents, and automate investigations.

Maintain compliance

Map controls and operational data to regulatory requirements such as the NCSC Cyber Assessment Framework, enabling teams to monitor compliance posture in real time and streamline reporting.

Turn data into insights

Combine OT telemetry with advanced analytics to identify patterns, detect early signs of equipment issues, and reduce the risk of costly downtime — driving reliable data-driven operations across the energy value chain.

Operational technology environments require specialised expertise. Sword brings over 20 years of experience in the energy sector to provide practical guidance and implementation tailored to its unique requirements and aligned with industry frameworks.

An in-house team of Splunk experts provide full end-to-end setup, implementation, and ongoing partnership to build unified visibility across IT and OT systems and operationalise security and resilience across critical infrastructure.

Backed by the industry-leading Splunk data and security platform, Sword helps organisations:

- **Establish OT monitoring strategies**
- **Integrate OT telemetry into Splunk**
- **Operationalise security monitoring**
- **Build scalable resilience programmes**

© 2026 Sword Group. All rights reserved.

Splunk, Splunk>, Data-to-Everything, and Turn Data Into Doing are trademarks or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2026 Splunk LLC. All rights reserved.