Operational Technology (OT) Security Add-on for Splunk

A complete view across the enterprise to improve safety, compliance and reliability

The energy sector is the fuel of the global economy, and the industry is rapidly changing. Consumers and investors are demanding clean, reliable and affordable sources of energy as companies contend with aging infrastructure, changing regulations and threats to traditional business models. Utilities are focusing on grid modernization and digitization to accommodate distributed energy resources (DER), the increased demand for renewable sources of energy like wind and solar, and to improve resiliency and drive new business models. Likewise, oil and gas companies are facing changing trends in supply and demand, and are turning to new digital technologies to optimize production and improve capital efficiency.

Additionally, manufacturing is facing increasing pressures stemming from the Covid-19 pandemic and the current geopolitical climate. These range from supply chain vulnerabilities, adapting to the rate of technological change and highly connected manufacturing environments (IoT); which are all contributing to substantially higher risk. These systems and processes have to be secure, vigilant and resilient with security built-in to all the processes in order to minimize risk and protect human life. Monitoring also has to be built-in to ensure the success of those controls while simultaneously being extended into the Operational Technology (OT) environment

This transformation is producing an exponential growth of data, as well as an increased cyberattack surface. Meanwhile, recruiting and retaining a new generation of talent with the necessary skill sets to secure and maintain IT and OT environments is a serious challenge. Splunk plays a pivotal role for IT, security and operations teams that need better visibility and insights to optimize performance, improve uptime, and ensure compliance and an enhanced security posture.

How can Splunk help?

Splunk is a data analytics platform that powers security, observability and IT Operations. Splunk provides the engine that helps in monitoring, searching, analyzing, and visualizing large amounts of energy and utility data at scale. Splunk has a vivid partner ecosystem with many apps that do not require any complicated databases, connectors, or controls. Splunk runs natively on premises or in the Splunk Cloud, shifting the burden of infrastructure and maintenance costs away from customers.

ATT&CK® for Industrial Control Systems

ATT&CK for Industrial Control Systems (ICS) is a collection of Tactics, Techniques and Procedures that an adversary may take against ICS with the goal of disrupting operations. Splunk uses these TTPs as annotations within our directions in order to add additional enrichment and characterization to the events we detect within your environment. With the Splunk for OT Security Add-on, organizations can expand coverage of both MITRE ATT&CK for ICS and NERC CIP compliance. This add-on includes detection rules supporting four additional MITRE ICS TTP's, as well as dashboards and reports for NERC CIP 006, 007, 008 and 009.

How Energy and Utility Organizations Use Splunk

IT and OT Cybersecurity

Strengthen cyber defenses across on-premises and multi-cloud environments with Splunk as your security nerve center. Bridge the gap between IT and OT to gain a holistic view of security and facilitate better collaboration between IT and operations teams to reduce security investigation from hours to minutes. Automate reporting for NERC CIP and other regulations and streamline compliance activities.

IT and OT Monitoring

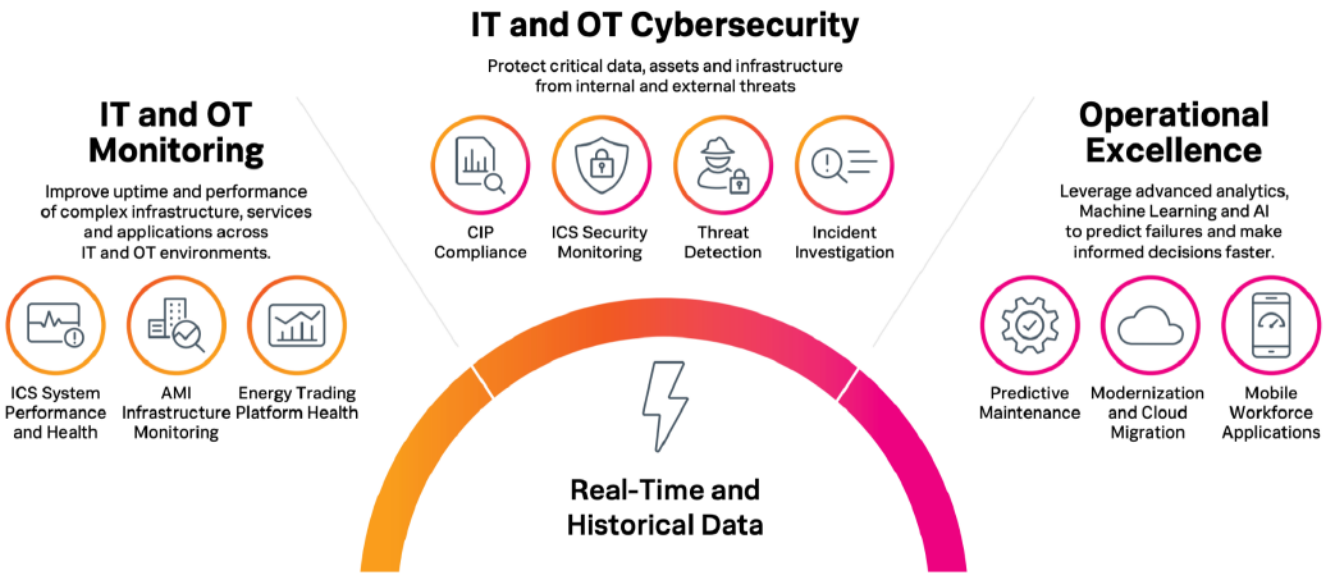
When critical systems like ERP, outage management, wired and wireless networks, energy trading platforms, ICS, IIoT endpoints, and safety instrumented systems fail it can cost you millions in downtime, environmental disaster and potential loss of human life. Splunk can help improve uptime, performance, and response time of business-critical applications and the infrastructure they run on, by monitoring and correlating issues to quickly determine root causes and remediate incidents.

Operational Excellence

Better manage complex, cloud-native and on-prem environments in order to deliver exceptional user experiences combined with technical agility, speed and deep insights. Splunk makes it easy to harness the power of machine learning for predictive maintenance, outage prevention, theft detection, demand forecasting and operational efficiency.

Security Orchestration, Automation and Response (SOAR)

Utilize automated response and case management within the context of OT to accelerate and augment the analyst experience. The included playbooks are aimed at providing a framework for conducting an OT investigation while simultaneously accelerating the pace of response. These playbooks are also tied into the MITRE ATT&CK for ICS framework in order to provide further enrichment for the analyst while working in one interface.



22-23857-Splunk-Operational Technology Add-on-DS-101