Splunk for Public Sector Utilities

At Splunk, we turn your critical infrastructure data into action. The sheer amount and breadth of data common to a modern utility can be overwhelming, especially when the data analysis is often across different tools or is a manual exercise. Splunk provides a centralized platform to correlate data, perform advanced analytics on various data sources, and apply built-in artificial intelligence (AI) to identify unusual behaviors or anomalies quickly. System outages and cyber investigations are collaborative efforts and everyone on the team plays an important role. Having a comprehensive view of the device data for all participants can reduce the time to determine if there is an attack from days or weeks to minutes. Splunk removes the barriers between data and action. We are here to support your missions.

"Already by 2018 nearly 60% of surveyed organizations had experienced a breach in their industrial control (ICS) or supervisory control and data-acquisition (SCADA) systems."

— McKinsey & Company, April 2019, "Critical infrastructure companies and the global cybersecurity threat"

54%

of global utilities surveyed expect an OT attack within 12 months

42%

rated their own readiness and response to cyberattacks as high

Source: World Economic Forum, Siemens

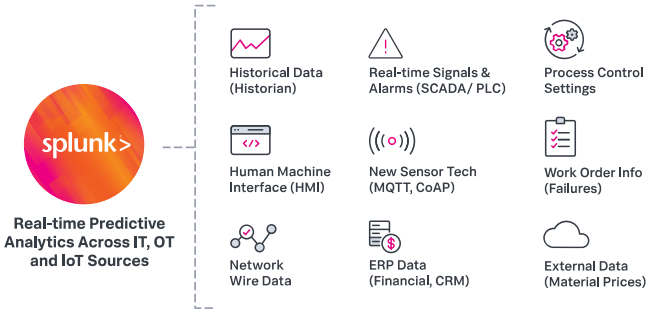
Why Splunk?

Splunk is a real-time analytics platform that monitors, searches, analyzes and visualizes large amounts of critical infrastructure, ICS, SCADA, sensor, and other operational technology (OT) data. Because Splunk can deal with any data structure, any data source, or any time scale it breaks down the barriers to analyzing data because there are no requirements for complicated databases, connectors or transformations. The platform helps security analysts detect an event across a vast amount of disparate data, which is typically what slows, or stop efforts to find and stop an attack.

Employing a risk-weighted approach to identify entities (e.g , privileged users, critical infrastructure) who are most likely to be threats allows Splunk's AI capabilities to prioritize and categorize alerts before it comes to an analyst. The Splunk platform can activate the rules, compute the risks, provide the alerts, and manage quick detection of potential threats and future performance issues or outages.

Focus Areas:

1. Expand ability to ingest, monitor OT Assets
2. Improve OT Vulnerability Management including supprt for Mitre ICS ATT&CK
3. Interfaces and reports to support NERC CIP audit and compliance



IT and OT monitoring

Leveraging Splunk to improve up-time and performance of complex infrastructures and applications across IT and OT environments:

- Industrial control systems performance and health
- Advanced metering infrastructure monitoring
- Energy trading platform health

IT and OT Cybersecurity

Protecting critical data, assets, and infrastructure from internal and external threats:

- NERC/CIP compliance
- ICS security monitoring
- Threat detections
- Incident investigation

Machine Learning and AI

Leveraging advanced analytics, machine learning, and AI to predict failures and make informed decisions faster.

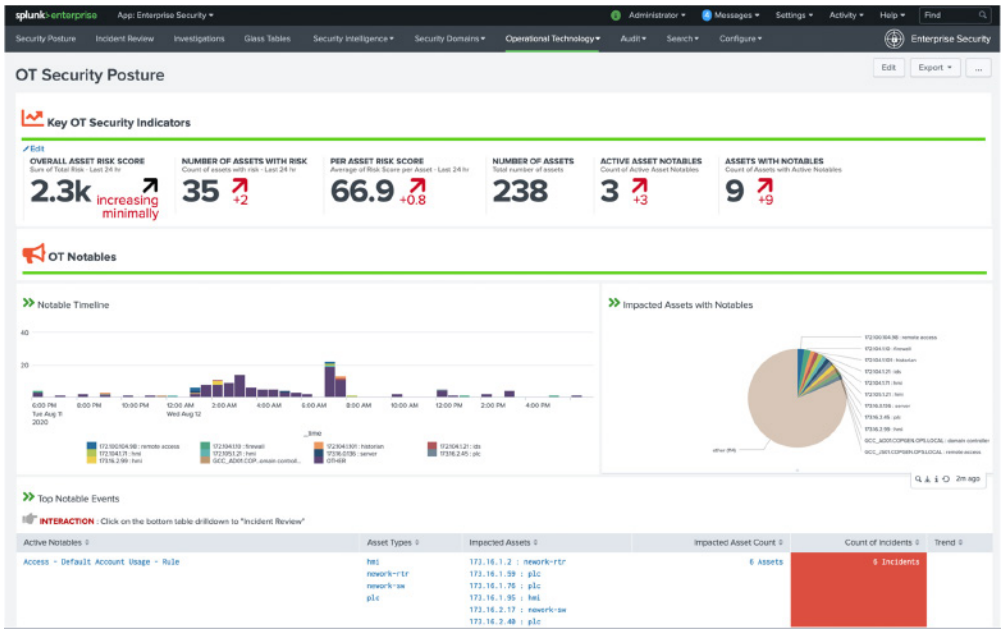
- Predictive asset maintenance
- Modernization and cloud migration
- Mobile workforce applications

"Splunk for Industrial IoT is important to us because it provides all the details about our site very quickly and we can make decisions on that data. We have to know how many customers are experiencing power outages."

— Chris Perez, Enterprise Technology Solutions Advisor, PSE

"If we have suspicious activity on an endpoint, we go to that specific dashboard in Enterprise Security and can see all of the movements, I just enter the hostname for a single machine, and I can see all of the endpoint response logs. Splunk lets you see everything going on in your environment to find the bad guys."

— Tibor Földesi, security automation analyst at Norlys



Contact Splunk at pbstutilities@splunk.com

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com