ACCENTURE'S OT SOC SOLUTION

VIDEO TRANSCRIPT

At Accenture Houston, we've created an Operation Technology Security Operations Center to identify and respond to threats against critical infrastructure.

A Security Operations Center enables you to build trust with your business by providing solutions to common problems, such as monitoring and tracking changes to control system infrastructure to secure your critical assets and reduce security response time by integrating tools onto a single platform with automation and reduce costly industrial outages by proactively solving issues.

We have security tools throughout our environment to detect and respond to attacks. Every tool generates logs which are sent to Splunk for analysis.

Splunk collects, displays, and correlates this data in dashboards, helping you act and respond to alerts.

In this dashboard, we see the overall security hygiene of our Center, including: Total Number of Assets, Total Number of Unique Protocols, and number of active internet connections coming from devices.

We also showcase various operational use cases that can help minimize and prevent significant financial losses to your business.

For instance, the number in this tile is typically very low. If the number increases drastically, it could indicate an impending network hardware failure—not a security event, but an issue that could cause a costly shutdown.

Maintaining stable operations and monitoring for security events are keys to success in an OT SOC while driving security as a business-enabler.

We've created an attack based on real-world scenarios that have been observed through OT Incident Response and Threat Hunting.

Here, an attack has caused an outage to one of our control systems. OT SOC Analysts can use this data, along with threat information from Accenture's Cyber Threat Intelligence to discover and respond to the attack. Having this information at your fingertips is critical when your most important assets are at risk.

Discover more about strengthening your OT security posture at the Houston OT Cyber-Fusion Center.