SIEM Integration

Siemens Energy is proud to offer a solution for Security Incident and Event Monitoring (SIEM) Integration that collects all the windows, network switch, and system logs with the T3000 system.

Problem	Cause	Solution	Benefit
• How to correlate information across all security relevant data and events. • Overloading of Information from alert emails • Lack of centralization for security alerts throughout the network	• Uncorrelated data that creates false positive alerts and noisy surroundings • Too many alerts makes it impossible for Operators to analyze every alert without centralization of events.	• SIEM helps identify unknown threats by providing context and centralizing alerts and providing a single point of context • Installed on the Disk space for the Elasticsearch database is limited to 15GByte • The core component of the SIEM is the ELK stack (Elasticsearch, Logstash, and Kibana) • The T3000 ASD can notify for critical security events	• User account login/logout activities are monitored, as well as failed login attempts • Alarms are reported for further follow-up action • SIEM is complementary to Omnivise T3000 security log module • The T3000 ASD can notify for critical security events • No additional equipment needed to install for SIEM

What We Deliver?

- Elasticsearch: Central Log database that indexes the messages and allows searching
- Logstash: Central Log Receiver. Parses and Structures messages
- Kibana: Web-based visualization and presentation
- Optional integration to existing customer SIEM

How We Deliver?

Data Collecting	Data Filtering	Data Presentation	Service
- Security events are collected from all systems and devices that are part of the T3000.	- Collected data are filtered, stored, and indexed to support analysis of alerts	- Kibana allows for the visualization of the data through a Web Interface - Visualizations can be arranged in one or more dashboards	- Log files and Logstash output files are deleted after 90 days - Hard disk space consumption is automatically checked during operation