PRODUCT OVERVIEW

LogRhythm and SEL: Cyber Security for Critical Infrastructure

LogRhythm

LogRhythm and Schweitzer Engineering Laboratories, Inc. have combined their complementary technologies to provide an enhanced solution for substation security auditing and monitoring. It delivers immediate awareness of potential cyber security threats and network breaches, such as unlawful attempted access to an Electronic Security Perimeter, and helps organizations comply with regulatory mandates, including the North American Energy Reliability Corporation's Critical Infrastructure Protection (NERC CIP) rules.

Electrical utilities and other critical infrastructure customers benefit from comprehensive security monitoring for SEL secure communication devices, with automated detection and alerting on suspicious activity, including inappropriate user access to Critical Cyber Assets (CCAs).

LogRhythm for Critical Infrastructure

- ☑ Out-of-the-box packages for NERC CIP/ NEI/NRC
- ☑ Specific support for SCADA devices
- ☑ Advanced correlation for protecting critical assets
- ☑ Secure, one-way communication for classified networks

LogRhythm's integration of devices such as the SEL-3620 Ethernet Security Gateway allows utilities to monitor and secure the entire range of relays, RTUs, PLCs, and communication processors across their organizations. It also delivers the tools they need to perform comprehensive forensic investigations of suspected breaches.

LogRhythm

LogRhythm is an enterprise-class Big Data Security Analytics platform that seamlessly combines Log Management & SIEM 2.0, File Integrity Monitoring, and Host Activity Monitoring into a single integrated solution. It is designed to address an ever-changing landscape of threats and challenges, with a full suite of high-performance tools for security, compliance, and operations. LogRhythm delivers comprehensive, useful and actionable insight into what is really going on in and around an enterprise IT environment. LogRhythm's SIEM 2.0 platform delivers:

- Fully Integrated Log & Event Management
- Automated Behavioral and Statistical Profiling
- Advanced Correlation and Pattern Recognition
- File Integrity/Host Activity Monitoring
- Powerful, Rapid Forensics and Search
- Intelligent, Process-Driven Smart**Response**™
- Ease-of-use and Simplified Management

SEL Security Solutions

SEL Security Solutions include a range devices and services that protect valuable data and provide secure access controls for critical infrastructure protection devices. Products such as the SEL ICON, the SEL-3025 Serial Shield, and SEL-3620 Ethernet Security Gateway provide data encryption and authentication for SONET, serial, and Ethernet communications. The SEL-3620 further provides secure access controls, enhanced authorization levels, and power auditing capabilities for local and remote interactive access to critical relays and RTUs. These capabilities result in easier compliance efforts, a stronger security posture, and easy centralized access to assets with automated password management.

LogRhythm and the SEL-3620 Ethernet Security Gateway in Action

LogRhythm and the SEL-3620 Ethernet Security Gateway allow utilities to bridge the gap between a requirement to implement secure network architectures for critical environments and the need for real-time situational awareness. The integration delivers the tools that utilities need to control access to critical devices and to respond appropriately when internal security policies are violated.

Controlling Access to the Electronic Security Perimeter (ESP)

Challenge NERC CIP requires strong access controls and logging for any interactive access attempt to the ESP. Many legacy devices, however, do not provide the necessary password strengths, centralized authentication, or logging necessary to securely meet this requirement.

Solution LogRhythm receives automatic notifications of multiple attempts to access protected critical devices directly from the SEL-3620. This data is immediately correlated against other relevant context surrounding the event to quickly identify the who, what, when, and where of a brute force attack.

Benefit Event data from SEL security products can be easily archived to aid compliance with NERC CIP requirements and provide relevant event data should forensic analysis be required in response to a security incident.

Auditing User Actions on Critical Devices

Challenge Global accounts on legacy devices limit the ability to correlate user activity to device settings because setting changes or access to shared accounts cannot be traced to specific users. This is particularly problematic when shared accounts require a common password.

Solution The SEL-3620 records all actions and commands sent to devices with global accounts and traces them back to a unique user. Wizard-driven investigation and reporting tools within LogRhythm then make it easy to correlate individual device access across an entire system infrastructure.

Additional Benefit ecurity administrators and auditors can quickly trace access and behavior to unique users. Such information is critical for quickly responding to incidents or conducting forensic analysis when a security event occurs.