OrionLX Integration into TRIPWIRE® NERC CIP Products

The NovaTech OrionLX integrates into three TRIPWIRE products to enable users to address all areas of NERC CIP compliance. These products are: Tripwire® Enterprise, Tripwire® IP 360 and Tripwire® Log Center®.

Tripwire® Enterprise

Orion is now defined as a "TRIPWIRE node" in Tripwire Enterprise, and TRIPWIRE has converted their standard Linux NERC CIP v5 compliance policy to work in an agentless fashion against the Orion. The monitoring of the Orion from Tripwire Enterprise has four main areas:

1) Monitoring policy compliance of the underlying operating system and patches against NERC CIP v5 standard
2) Detecting changes related to the operating system
3) Monitoring policy compliance of the OrionLX application and connected SEL® relays. For example, check to ensure all relays of a certain type have a certain setting, or do not have a certain setting
4) Detect changes related to the OrionLX application and connected SEL relays; also determine whether the change affect the security position.

The OrionLX makes configuration and settings data available to Tripwire Enterprise as follows: Using the Configuration Manager Agent (an OrionLX software product), the OrionLX periodically and automatically accesses all files and configuration data from itself and from the attached SEL® relays. These files and data are zipped into one file and either transferred to Tripwire Enterprise via SFTP, or filed inside Orion for access by Tripwire Enterprise.

For more on Tripwire Enterprise, please visit: http://www.tripwire.com/it-security-software/scm/tripwire-enterprise/

Tripwire® IP 360 Asset Discovery and Vulnerability

Tripwire IP360 provides visibility into the enterprise networks and substation networks including all networked devices and their associated operating systems, applications and vulnerabilities. IP 360 is engineered to look for specific vulnerabilities in the OrionLX, including:

1) Check for the presence of the factory-provided user account "novatech"
2) Check to make certain non-sure protocols are not being used: telnet, HTTP, FTP, etc.

For more on Tripwire IP360, please visit: http://www.tripwire.com/it-security-software/enterprise-vulnerability-management/tripwire-ip360/

Tripwire® Log Center®

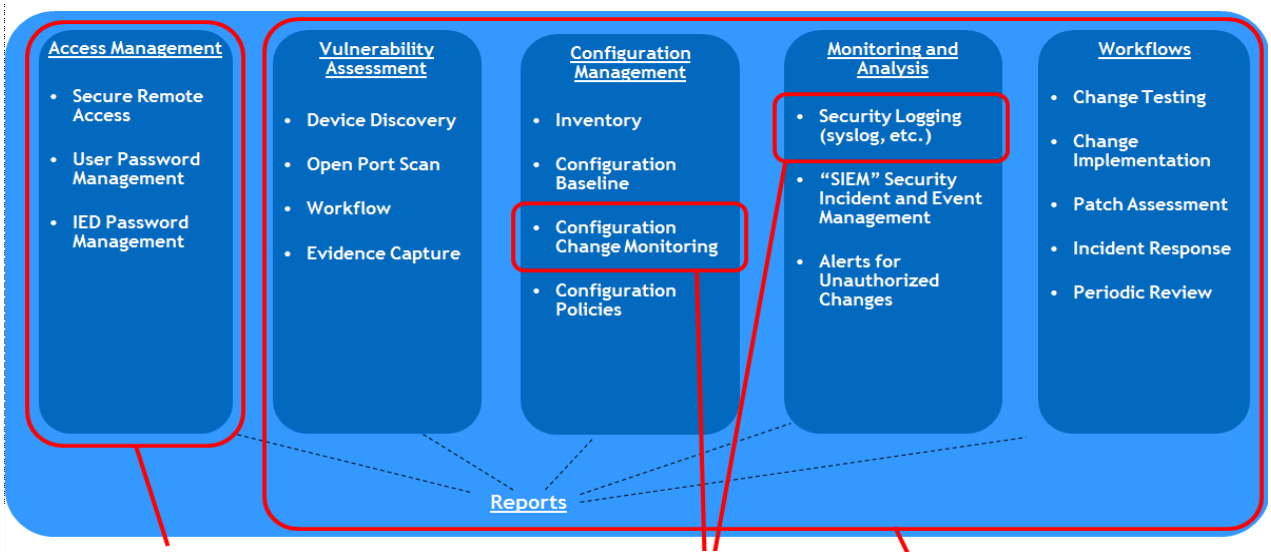
Tripwire Log Center applies automated real-time intelligence to machine data— with security analytics and forensics for rapid incident response. Log Center retrieves syslog data that is recorded inside the OrionLX. OrionLX syslog data includes user login data, access protocols, applications launched, and pages viewed, as well as any other real-time events added by the user with the "System Logger" software feature. Tripwire Log Center tools include:

1) Detection of correlated events; e.g. a high voltage breaker operation after a user login
2) Automatically-triggered remediation and alerting with scripts
3) "Threat and Security Solution Packs" including "Insider Threat", "Denial of Service Detection" and "Breach and Intrusion Detection"

For more on Tripwire Log Center, please visit http://www.tripwire.com/it-security-software/tripwire-log-center/

Complete NERC CIP Solution

The diagram below illustrates where the NovaTech and Tripwire products address the five major areas of NERC CIP compliance:



NovaTech Identity Manager (NIM) and Connection Manager (NCM) address requirements in Access Management

NovaTech also provides monitoring products in these areas

NovaTech integrates with TRIPWIRE (Portland, OR) to address other areas of NERC CIP compliance.

For more information on NovaTech NERC CIP products, please see the document "NovaTech Products for NERC CIP Compliance - May 2016.pdf".