Cyber Security Audit and Attack Detection Toolkit

Adding control system intelligence to widely deployed enterprise vulnerability scanners and security event managers

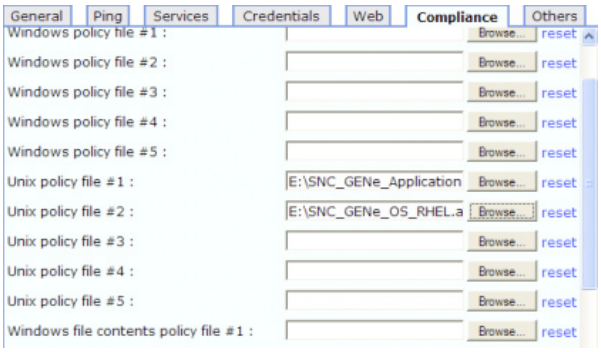
While many energy utilities employ vulnerability scanners and security event managers (SEM) on their enterprise systems, these tools often lack the intelligence necessary to be effective in control systems. This two-year project aims to integrate control system intelligence into widely deployed vulnerability scanners and SEM, and to integrate security incident detection intelligence into control system historians. These upgrades will be provided at no or a low cost to control system asset owners.

The popular Nessus Vulnerability Scanner supports an audit plug-in that gathers configuration information from systems and compares it to a template of good practice. The project team will create these templates, known as ".audit" files, for 20 control system devices and applications deployed in the facilities of utility project partners.

OSIsoft's PI System collects historical information from data sources throughout a control system network. The project team will leverage PI's advanced computing engine (ACE) to develop correlation rules that detect cyber attacks on control systems. By adding these ACE security incident detection modules, the team will effectively convert the PI System into a control system SEM, allowing many energy asset owners to deploy SEM at no extra cost.

The team will then bridge the newly developed control system SEM capability with existing enterprise SEM. Researchers will correlate control system security events detected in the PI system with other security events–such as firewall logs–in the enterprise SEM, and transform this information into meta events that the enterprise SEM can detect.

These solutions will be available as subscriber content on Digital Bond's website at a subscription cost of $100. Solutions will be specialized for products from partner vendors, but also generalized for use in systems from other vendors.



Screenshot from NESSUS Vulnerability Scanner

National SCADA Test Bed

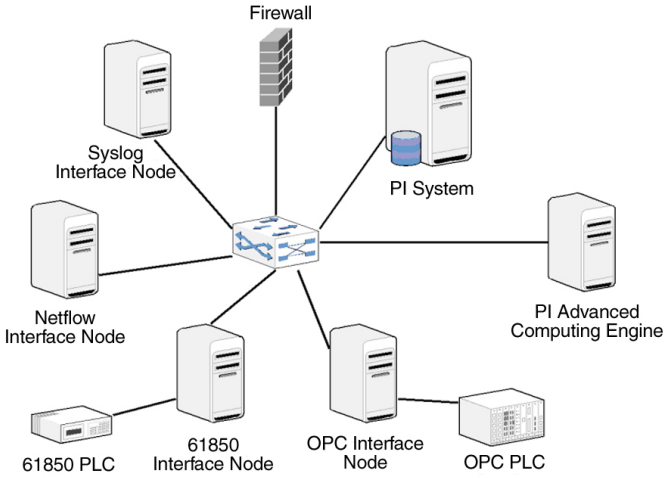
Benefits

- Integrates vulnerability detection and security event management capabilities into systems currently deployed by a majority of the energy community
- Creates these capabilities for systems from other vendors along with documentation on how to implement them
- Offers a low- or no-cost security solution to asset owners
- Operates with existing and new control systems
- Provides immediate capability to existing systems without requiring investment in new systems

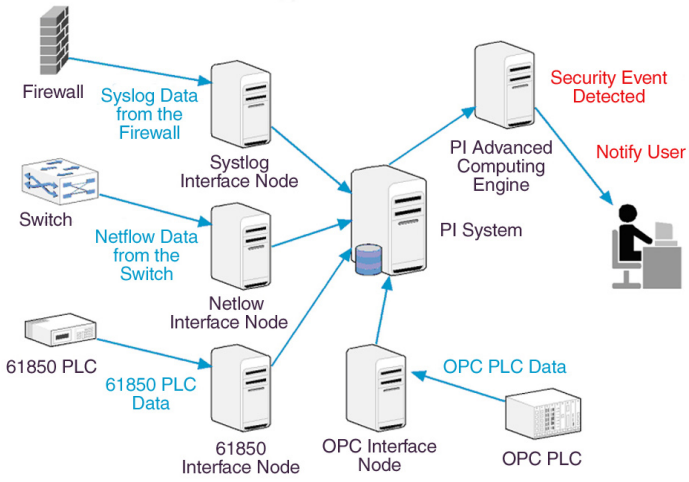
Partners

- Digital Bond Inc.
- OSIsoft
- Tenable Network Security
- Constellation Energy
- PacifiCorp
- Tennessee Valley Authority

Physical Layout



Data Flow



Technical Objectives

The security components will be designed and tested through the following tasks over three phases.

Phase 1: Vulnerability Scanner

- Select 20 control system applications (e.g. real-time servers, historians, etc.) from owner participants
- Collect system data from asset owners and vendors
- Create ".audit" good practice configuration files
- Test files on asset owners' systems
- Update files and documentation
- Create similar files in the industry standard file format (OVAL/XCCDF)
- Develop a ".audit" template, available to asset owners with similar product classes from other vendors, and documentation on how to customize the ".audit" file

Phase 2: Lab and Field Testing

- Collect security data from asset owners' PI Systems
- Identify security events from data and develop meta events that will be detected as cyber attacks
- Write these events into ACE incident detection modules
- Test modules in asset owners' PI Systems for two months
- Create guidelines for using incident detection modules in other historians, and test them in a custom historian

Phase 3: Enterprise SEM

- Integrate ".audit" files and ACE incident detection modules into Tenable Security Center SEM
- Identify enterprise SEM meta events from control and enterprise information
- Test at asset owner facilities
- Test with a custom SEM

End Results

All deliverables will be released as subscriber content on the Digital Bond website. Deliverables will include:

- The ".audit" files for the Nessus Vulnerability Scanner; standard OVAL/XCCDF files; and ".audit" template files for future customization to other vendor products
- ACE incident detection modules for the OSIsoft PI System and other custom historians
- Enterprise SEM integration tools for use with OSIsoft PI System or other SEM

All deliverables will be tested at asset owner facilities before being released with all documentation.

Subscription to the Digital Bond website currently costs $100 per year, making these security upgrades an affordable and immediate solution for all energy asset owners.

May 2008

DOE National SCADA Test Bed (NSTB)

NSTB is a multi-laboratory resource that partners with industry and other government programs to test, research, and help design cyber security solutions to enhance control systems security in the energy sector and reduce the risk of energy disruption due to cyber attack.

For More Information:

Hank Kenchington
Program Manager
DOE NSTB
202-586-1878
henry.kenchington@hq.doe.gov

Dale Peterson
Digital Bond, Inc.
954-315-4633
peterson@digitalbond.com

Visit Our Website:

www.oe.energy.gov/control security.htm