Cyber Security Audit and Attack Detection Toolkit

Bandolier Audit Files for optimizing security configurations and the Portaledge event detection capability for energy control systems

A cost-shared effort between industry and

U.S. DEPARTMENT OF ENERGY | Cybersecurity, Energy Security, and Emergency Response

Cyber Security for Energy Delivery Systems

Bandolier and Portaledge

Project Lead:
Digital Bond

Partners:
OSIsoft
Tenable Network Security
PacifiCorp
Tennessee Valley Authority

Other Participating Vendors:
ABB
AREVA
Emerson
Matrikon
SNC
Telvent

The Concept

By building configuration audit and attack detection capabilities into tools already used by the energy sector, Bandolier and Portaledge offer energy asset owners low-cost and easily integrable control systems security solutions. Energy system operators can optimize the security of their control system configuration using Bandolier Security Audit Files, which assess the current configuration against an optimal security configuration. Portaledge is a software tool that uses OSIsoft's PI Server to gather, analyze, correlate, and alert operators to control system security events. Both of these customizable tools are available to Digital Bond site subscribers and from participating control system vendors.

Bandolier—The Approach

To reach the greatest number of asset owners and enable rapid development, the Bandolier team built upon the capabilities of the widely used Nessus Vulnerability Scanner. The team developed custom security audit files that work with the scanner's compliance plugins to check for flaws with the same low impact as an administrator remotely examining the configuration. This approach is both more accurate and less disruptive than typical scanning techniques.

Digital Bond drew on its strong relationships with energy companies and control system application vendors to select widely deployed control systems and develop an optimal security configuration for each—using vendor-recommended settings, industrial consensus documents (including the North American Electric Reliability Corporation Critical Infrastructure Protection [NERC CIP] standards), and research from Digital Bond's team. After gathering configuration data at client sites, the team used that data to create prototype audit files and return to the system sites to test them. Digital Bond worked with vendors to further refine the system-specific audit files and trained clients to use the files and analyze audit results. The team introduced the first set of files at the 2008 International Society of Automation Expo to raise awareness and encourage adoption.

Bandolier—The Commercialized Solution

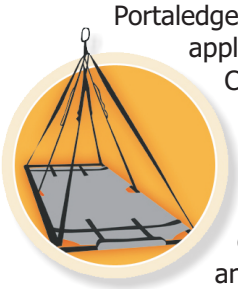
Bandolier Security Audit Files allow energy asset owners to verify and maintain a secure configuration for more than 20 control systems applications.

Features:
Bandolier Security Audit Files run hundreds of security checks to assess the configuration strength of each system component and audit thousands of security parameters in a SCADA or distributed control system. The resulting report identifies those security settings that vary from the recommended optimal security configuration the team developed.

Available Now:
Bandolier Audit Files are available to www.digitalbond.com subscribers for Siemens, Telvent, ABB, Matrikon, Emerson, AREVA, OSIsoft, Invensys, and SNC systems. For more information, visit www.digitalbond.com/wiki/index.php/List_of_Bandolier_Audit_Files.

Portaledge—The Approach

Portaledge builds upon OSIsoft's widely deployed PI server, an enterprise historian used to aggregate, analyze, and display process system data. With the Portaledge package, the PI Server interfaces with control system devices and applications and uses its advanced correlation capability, the Advanced Computing Engine (ACE), to analyze and report control system data that potentially signify an attack.



Digital Bond identified, documented, and integrated security events to enable the PI Server to collect and store control systems security event data. The team developed ACE modules by event class to analyze and aggregate control systems security data, creating a hierarchical structure (taxonomy) based on the source and type of event that occurs. The event classes categorize chains of events that potentially indicate an attack. For example, numerous events revealing a single system probing multiple systems in a control center could indicate a port scan from an attacker trying to enumerate the network.

Benefits

- Enables expert identification of optimal security settings and event detection for control system components
- Integrates affordable security solutions into systems deployed by a majority of energy companies
- Delivers customizable solutions for site-specific policies
- Operates with existing and new control systems
- Requires minimal effort to customize and implement

Portaledge—The Commercialized Solution

Portaledge is a package of user-customized data inputs and modules that enable OSIsoft's PI server to function as a security event manager (SEM) for aggregating and correlating energy control system security events to detect cyber attacks. This event detection capability can provide the security monitoring required in the NERC CIP standards. Portaledge includes a template for creating security PI tags, a spreadsheet to create the module database Portaledge uses to convert asset owner tag names to aliases that are used in the ACE modules, ACE modules by event class, an administrator-customized datalink display, and installation and customization instructions for each component.

Features:
The user can customize when a particular combination or sequence of events in an event class chain requires operator notification, as well as the appropriate type of notification. Portaledge output includes the correlated security events and the chain of individual log entries or data points that triggered the correlated security event. These chains are useful in preparing a response to an attack and for after incident analysis.

Available Now:
The Portaledge Release Package is available to www.digitalbond.com subscribers. For more information, visit www.digitalbond.com/wiki/index.php/Portaledge_Release_Package.

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Dale Peterson
Digital Bond
954-315-4633
info@digitalbond.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov