DOE Award Number: DE-FC26-07NT43312

Recipient: Digital Bond, Inc.

Project Title: Cyber Security Audit and Attack Detection Toolkit

Principal Investigator: Dale Peterson

Team Members: Tenable Network Security, OSIsoft

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Final Technical Report for NT43312

Cyber Security Audit and Attack Detection Toolkit

1. Executive Summary

Digital Bond performed a research project for the Department of Energy that ran from 1 October 2007 to 31 May 2012. This goal of this project was to develop cyber security audit and attack detection tools for industrial control systems (ICS). This is the Final Technical Report for the project. There are four sections in this report:

- Executive Summary
- Bandolier – Cyber Security Audit Tool
- Portaledge – Cyber Attack Detection Tool
- Contract Tasks and Deliverables

Digital Bond was able to complete all contract tasks and deliverables, and we were able to accomplish this for $313,726 less than awarded for these tasks and deliverables.

Cyber Security Audit

Digital Bond developed and released a tool named Bandolier that audits ICS components commonly used in the energy sector against an optimal security configuration. You can think of Bandolier as a SCAP for ICS.

We worked closely with the vendors that make the energy sector ICS, such as ABB, Alstom Grid, Emerson, OSIsoft, Siemens, Telvent and others, to determine the optimal security configuration for components. This included both operating system security settings and ICS application security settings. A typical component would have about 200 security settings.

Once the optimal security configuration was agreed on, Digital Bond then developed a .audit file that worked with the industry leading Nessus Security Scanner. The result was a low impact audit of the ICS components that identifies all variances with the optimal security configuration. All Bandolier Security Audit Files developed with Dept. of Energy funding are available free of charge.

Bandolier has been highly successful measured by its impact and use in the industry. For example, Telvent's Board of Directors made Bandolier one of their four strategic initiatives one year. Telvent uses Bandolier to verify new systems are deployed in the optimal security configuration. Telvent is also an example the program will not end with the completion of Dept. of Energy. Telvent has updated the Bandolier file to audit new versions of their product, developed training videos, and even enhanced the Bandolier GUI.

Alstom Grid is another example of a company that is using Bandolier during Factory and Site Acceptance Testing to verify the system is in the optimal secure configuration. Digital Bond has participated in acceptance tests with other vendor systems where Bandolier was used as well.

The result is new critical infrastructure control systems deployed in their optimal security configuration.

Owner/operators are downloading and using Bandolier to verify initial deployments, harden existing deployments and periodically audit securely deployed systems.

Another indicator that the Bandolier program has been a success is vendors have engaged Digital Bond after the end of the Dept. of Energy project to develop Bandolier Security Audit Files.

In addition to the Bandolier Security Audit Files for ICS components, the project also developed Bandolier Baselines for Windows 7 and Windows 2008 Server and NERC CIP-007 scan policies. The Bandolier Baselines can be used by any vendor to audit their operating system deployment. The NERC CIP-007 scan policy collects information required for compliance.

Cyber Attack Detection

The Portaledge Project developed a capability for the PI Historian, the most widely used Historian in the energy sector, to aggregate security events and detect cyber attacks. The program met all the technical objectives, but it was not adopted by the energy sector.

The Portaledge Project releases would detect an attacker performing reconnaissance, affecting system availability, changes to the firewall configuration, and changes to open ports or listening services on workstations or servers. It could then display these alerts in the control center or forward the alerts to an enterprise security information and event management system.

The primary reason the resulting capability was not adopted was it required the owner/operator understand and modify some complex technology in the PI Server. Given the needed effort to achieve basic security controls, and how little progress was made on these basic controls, it is unrealistic to expect this complex and advanced technology be deployed.

It may be of interest in the future, but even this is doubtful. In recent years, IT Security tools have begun to penetrate the ICS networks. There are more full featured and off the shelf tools that could do the job of Portaledge and fit better with an enterprise strategy. Digital Bond does not recommend further work on Portaledge and will not be pursuing it ourselves.

We would like to thank the Department of Energy for funding this research and their support throughout this project.

2. Bandolier – Cyber Security Audit Tool

The Bandolier Security Audit Tool helps asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. Digital Bond partners with leading ICS vendors to identify the optimal security configuration that still allows the vendor's product to operate properly. This requires access to the vendor's security experts, lead engineers and a test lab. Digital Bond then creates Bandolier Security Audit Files that work with the compliance plugin in the Nessus vulnerability scanner.

For asset owners and operators, the Bandolier Security Audit Files provide a way to verify that their systems are in an optimal, vendor-supported security configuration – both at the time of delivery to hold the vendors accountable and for ongoing, routine security auditing. In addition, the Bandolier reports provide valuable evidence for NERC CIP and other regulatory compliance requirements. Vendors like Telvent, Alstom Grid, and OSIsoft are using Bandolier to help deliver hardened systems. They use Bandolier for acceptance testing and for routine security validation testing in the patch and update process.

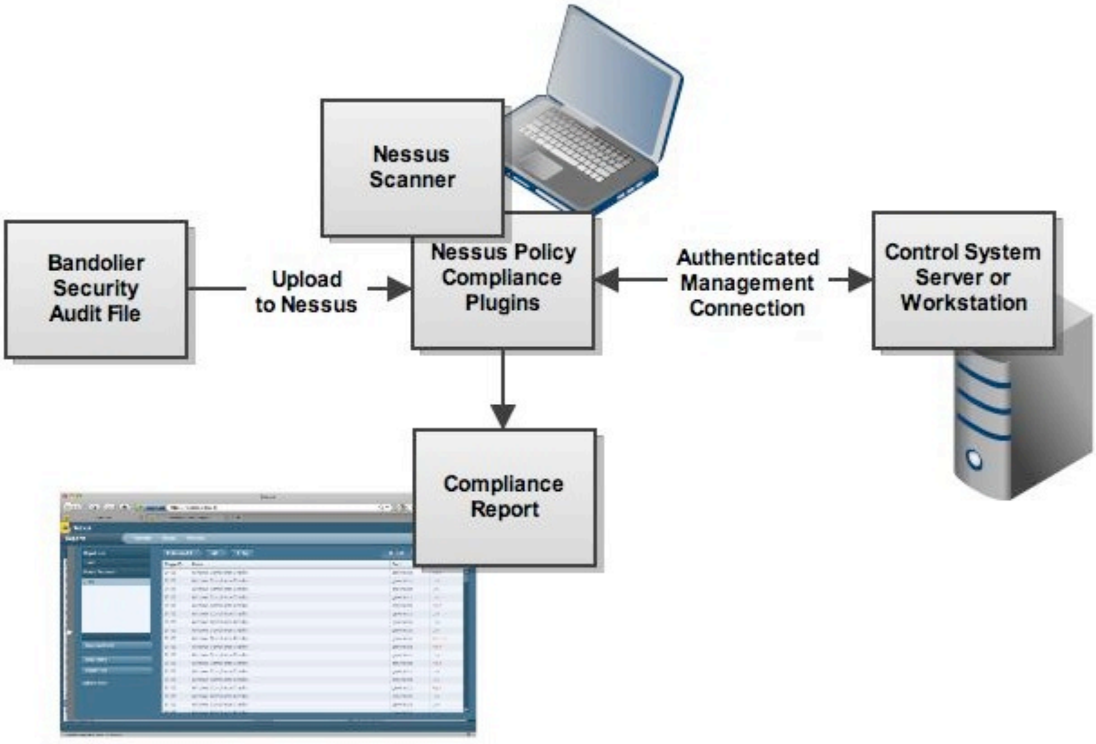
The Bandolier program lives on after DoE funding has ended. Some vendors, such as Alstom Grid and Telvent, have updated the files as new versions of their products have come out. Other vendors have engaged Digital Bond to develop new Bandolier security audit files.

Overview

- Defines optimal security configuration for SCADA and DCS servers and workstations
- Provides vendor-supported, customized security audit files for control system applications
- Provides a safe and effective way to audit the security of control system components

How it Works

- No client software, services, or agents are required on the control system server or workstation
- User uploads Bandolier Security Audit Files to the Nessus vulnerability scanner
- Nessus policy compliance plugins make a low impact connection to the ICS server or workstation
- Nessus uses built-in operating system functionality to compare the settings on the control system server to those defined in the Bandolier Security Audit File
- Nessus provides a report that shows whether each setting matched what is in the Bandolier Security Audit File


Nessus Scanner
Bandolier Security Audit File
Upload to Nessus
Nessus Policy Compliance Plugins
Authenticated Management Connection
Control System Server or Workstation
Compliance Report

Phase I

The main task in Phase I was to develop Bandolier Security Audit Files for at least 20 different ICS devices or components. A total of 23 different Bandolier Security Audit Files were developed for ICS from leading energy sector systems such as ABB's Ranger, Alstom Grid's eterra, Emerson Ovation, Matrikon's Secure Tunneler, OSIsoft's PI Server, SNC's GENe, Siemens Telegyr and Telvent OASyS DNA. A complete list of the Bandolier Security Audit Files created in Phase I is available in Section 4.

The were two other Bandolier tasks in Phase I. First, to attempt to make the ICS security application specific audit tests available in other scanners, Digital Bond converted all the Bandolier Application Security Audit Files to the OVAL format. OVAL was selected because the testing envisioned by OVAL's developers is similar to the Nessus audit capability. The Bandolier OVAL files were tested using MITRE's OVAL interpreter.

Digital Bond discovered that most security tools, even those that explicitly support OVAL, require some level of conversion to the tool's native format. This combined with a lack of interest in the scanner vendors led Digital Bond to recommend this effort not be continued in Phase II.

The second additional task was to develop a guide to help vendors develop something similar to Bandolier. Digital Bond released the Security Configuration Audit Development Guide.

There is a significant amount of additional documentation on digitalbond.com including:

- A Bandolier FAQ - http://www.digitalbond.com/tools/bandolier/bandolier-faq/
- A Bandolier Demonstration Video - https://www.digitalbond.com/tools/bandolier/bandolier-demonstration-video/

- A Bandolier User Guide for Nessus - https://www.digitalbond.com/tools/bandolier/bandolier-user-guide-for-nessus/
- Bandolier and NERC CIP - http://www.digitalbond.com/tools/bandolier/bandolier-and-nerc-cip/

The Bandolier Security Audit Files are available for free download at https://www.digitalbond.com/tools/bandolier/downloads/

Phase II

With the success of Bandolier in Phase I, Phase II included the decision to generate additional Bandolier Security Audit Files for ICS that are important in the energy sector. Bandolier Security Audit Files were developed for ABB 800xA, CSI UCOS, OSIsoft PI Server on Windows 2008 Server and the SISCO AX-4 ICCP Server. The ABB 800xA and CSI UCOS actually consist of many different components, and a Bandolier Security Audit File was developed for each component.

As part of this development, there were not existing quality audit files for Windows 7 and Windows 2008 Server R2. So Digital Bond developed these files that we call the Bandolier Baselines. They are based on Microsoft security configuration recommendations and then slightly modified for ICS concerns. For example, Microsoft recommends stopping operation if logs are full. This would be unwise and unacceptable in an ICS. The Bandolier Baselines are described at: https://www.digitalbond.com/tools/bandolier/bandolier-baselines/ and can be downloaded on the Bandolier download page.

The final Bandolier task in Phase II was to develop scan policies for NERC CIP-007. Policies were developed that gather listening ports, running services, default account and other miscellaneous information that is accessible by a security scanner and useful for CIP-007 compliance. Information on the NERC CIP-007 scan policies is available at https://www.digitalbond.com/tools/bandolier/nerc-cip-scan-policies/.

3. Portaledge – Cyber Attack Detection

The initial thinking behind the Portaledge Project was as follows:

1. ICS components generate a significant number of security events that would be useful in attack detection and after incident analysis.
2. These ICS security events should be included in enterprise wide security event analysis.
3. The Operations Organizations that run SCADA and DCS would not allow an IT Department to put an IT Security product, a Security Information and Event Management (SIEM), on the ICS network. Nor would the Operations Organizations allow the IT Department to deploy, manage and monitor a device on their ICS networks.
4. ICS typically have one or more Historians. Full featured Historians aggregate events and correlate them to identify operational incidents and calculate key performance indicators.
5. A full featured Historian could aggregate ICS security events and analyze these security events to detect cyber attacks.
6. After collecting and analyzing ICS security events, the Historian could forward appropriate security information to the Enterprise SIEM.

While the technical objectives of the Portaledge Project were met, the future of this type of adaption of an ICS Historian to an ICS SIEM is unlikely to have a significant market. The primary reason is traditional Enterprise SIEMs have made progress in penetrating the ICS networks amongst early adopters. The IT / Operations turf wars still remain, but they are receding in early adopter organizations as the Operations Department realizes they need IT assistance and the IT Department becomes more educated on ICS culture and requirements.

A secondary reason is resource related. Organizations have struggled to make progress securing ICS since the project started in October of 2007. It will take a major investment in time and money to deploy and maintain basic security controls in critical infrastructure ICS over the next 3 – 5 years. The effort to customize a Historian at each facility to work as an ICS SIEM is a low priority, particularly if the IT Department has an existing SIEM solution in the Enterprise that can be extended to the ICS network.

The only way the Portaledge concept is likely to progress in the ICS space is if a major ICS vendor determined to add and support this capability to their Historian. The business case for this seems highly unlikely.

In summary, Portaledge was a technical success, in that all of the objectives and deliverables were achieved, but a market failure. Digital Bond does not recommend future investment in the ICS SIEM approach of Portaledge.

Basic Technical Approach

Portaledge is a Digital Bond research project that aggregates security events from a variety of data sources on the control system network and then correlates the security events to identify cyber attacks. Portaledge leverages the aggregation and correlation capability of OSIsoft’s PI server, and its large installed base in the energy sector to provide this cyber detection capability in a system many industrial control system (ICS) owner / operators already have deployed.

The security events are sent from the event source to a PI Interface and loaded as tags. The tag data is then sent from the PI Interface to a PI Server. The ICS security data is now aggregated at a central site.

Digital Bond then developed PI Advanced Computing Engine (ACE) modules to analyze the data in the security event tags and detect events. A Portaledge release package consists of:

Tag Creator

PI tags must be created for each security event sent to the PI server for aggregation and correlation.

Alias Creator

The Alias Creator provides the method to aggregate security event information in the form of asset owner tags into the normalized tags that Portaledge will use to correlate data and detect attacks. This is the part of the project that will require the most work by the asset owner, but creating tags is something PI users are very used to doing.

The Alias Creator is provided as an Excel spreadsheet. The Alias Name is in one column and the Asset Owner Tag Name is in an adjacent column. Each row will include a description of the Asset Owner Tag that should be paired with the Alias Name. For example, an Alias Name could be CPU Utilization from the Windows performance monitor or Firewall Syslog from the firewall.

The completed spreadsheet is imported into the PI server and then the PI server has the data that it will run event, event class event and meta event correlation rules on in the proper Alias Name format.

ACE Modules

Correlation takes place in the Advanced Computing Engine (ACE) modules. Each Event has at least one ACE module and may have multiple ACE modules if there are multiple Event Triggers; each Event Class Event has an ACE module; and there is an ACE module for Meta Events. Each Event Class will have a zip archive that will include all Event ACE modules in that Event Class and an Event Class Event ACE module.

Event Modules are imported into the PI server using the PI ACE Scheduler.

Datalink Displays

Once the Event, Event Class Events and Meta Events are identified by an ACE module, the name and chain are available in the PI Server. There are a tremendous amount of ways to present this information. Creating displays, sending pages, and other methods of visualization and notification are regular control system activities by PI users.

One method of visualizing Portaledge Events, Event Class Events and Meta Events is populating a display page using OSIsoft’s Datalink display. Digital Bond may develop a number of Datalink display pages and other methods of tracking the security status of a control system as part of Portaledge and other projects. This is an interesting area of research. However, in the first release a simple Datalink display page will be included that will list the Events and Event Class Events in scrolling windows, and may include some general security status indicators or trends.

Detailed installation information is available at https://www.digitalbond.com/tools/portaledge/portaledge-event-installation/

Phase I

In Phase I Digital Bond developed modules to:

- Detect Availability Events
- Detect Enumeration Attacks
- Correlate Availability and Enumeration Attacks, called Meta Events in Portaledge

Availability Events

This section provides a summary of the Portaledge Availability Events. There are individual documentation pages for each Event that include significantly more detail and installation instructions.

Computer System Availability Event

The Computer System Availability Event will generate an alert when one of the triggers reaches a threshold. The thresholds can be modified by an administrator in the AliasCreator_ComputerSystemAvailability.xls spreadsheet.

Triggers

- CPU Utilization: This trigger will raise an alarm if the average CPU usage over the past 5 minutes has reached the threshold (default is 85%).
- Memory Utilization: This trigger will raise an alarm if the average memory usage over the past 5 minutes has reached the threshold (default is 85%).
- Hard Disk Space: This trigger will raise an alarm if the percentage of free hard disk space has reached the threshold (default is 10%).
- Network Bandwidth: This trigger will raise an alarm if the average number of packets over the past 5 minutes has reached the threshold (default is 85%).
- Network Latency: This trigger will raise an alarm if the average network latency over the past 5 minutes has reached the threshold (default is 30 ms).

Interfaces

- Ping Interface: Used to determine network latency.
- TCP Response Interface: Used to determine network latency.
- Performance Monitor Interface: Used on Windows systems to determine CPU utilization, memory utilization, hard disk space, network bandwidth.
- SNMP Interface: Used on Linux systems to determine CPU utilization, memory utilization, hard disk space, network bandwidth.

Network Device Availability Event

The Network Device Availability Event will generate an alert when one of the triggers reaches a threshold. The thresholds can be modified by an administrator in the AliasCreator_NetworkDeviceAvailability.xls spreadsheet.

Triggers

- CPU Utilization: This trigger will raise an alarm if the average CPU usage over the past 5 minutes has reached the threshold (default is 85%).
- Memory Utilization: This trigger will raise an alarm if the average memory usage over the past 5 minutes has reached the threshold (default is 85%)..
- Network Bandwidth: This trigger will raise an alarm if the average number of packets over the past 5 minutes has reached the threshold (default is 85%).
- Network Latency: This trigger will raise an alarm if the average network latency over the past 5 minutes has reached the threshold (default is 30 ms).

Interfaces

- Ping Interface: Used to determine network latency.
- TCP Response Interface: Used to determine network latency.
- SNMP Interface: Used to determine CPU utilization, memory utilization, hard disk space, network bandwidth.

Field Device Availability Event

The Field Device Availability Eventwill generate an alert when one of the triggers reaches a threshold. The thresholds can be modified by an administrator in the AliasCreator_FieldDeviceAvailability.xls spreadsheet.

Triggers

- CPU Utilization: This trigger will raise an alarm if the average CPU usage over the past 5 minutes has reached the threshold (default is 85%).
- Memory Utilization: This trigger will raise an alarm if the average memory usage over the past 5 minutes has reached the threshold (default is 85%).
- Network Bandwidth: This trigger will raise an alarm if the average number of packets over the past 5 minutes has reached the threshold (default is 85%).
- Network Latency: This trigger will raise an alarm if the average network latency over the past 5 minutes has reached the threshold (default is 30 ms).

Interfaces

- Ping Interface: Used to determine network latency.
- TCP Response Interface: Used to determine network latency.
- SNMP Interface: Used to determine CPU utilization, memory utilization, hard disk space, network bandwidth.

Performance Degradation Events

The Performance Degradation Events will trigger an alert when the load on one of the triggers is significantly greater than the previous days load at the same time.

Triggers

- CPU Utilization: This trigger will raise an alarm if the average CPU usage over the past 5 minutes is significantly greater than the CPU usage 24 hours earlier (default is 200%).
- Memory Utilization: This trigger will raise an alarm if the average memory usage over the past 5 minutes is significantly greater than the memory usage 24 hours earlier (default is 200%).
- Hard Disk Space: This trigger will raise an alarm if the percentage of free hard disk space is significantly less than the percentage of free disk space 24 hours earlier (default is 200%).
- Network Bandwidth: This trigger will raise an alarm if the average number of packets over the past 5 minutes is significantly greater than the number of packets 24 hours earlier (default is 200%).
- Network Latency: This trigger will raise an alarm if the average network latency over the past 5 minutes is significantly greater than the network latency 24 hours earlier (default is 200%).

Interfaces

- Ping Interface: Used to determine network latency.
- TCP Response Interface: Used to determine network latency.
- Performance Monitor Interface: Used on Windows systems to determine CPU utilization, memory utilization, hard disk space, network bandwidth.
- SNMP Interface: Used on Linux systems to determine CPU utilization, memory utilization, hard disk space, network bandwidth.

There are three Performance Degradation Events:

- Field Device Performance Degradation Event
- Computer System Performance Degradation Event
- Network Device Performance Degradation Event

Simple Network Availability Event

The Simple Network Availability Event will generate an alert when one of the monitored devices is non-responsive to network requests. The thresholds can be modified by an administrator in the AliasCreator_SimpleNetworkAvailability.xls spreadsheet.

Triggers

- Network Availability – This trigger will raise an alarm if the system no longer responds to network requests or if the ping reply latency exceed a user defined threshold (default is 20 ms).

Interfaces

- Ping Interface: Used to determine whether a system is available on the network.
- TCP Response Interface: Used to determine whether a system is available on the network.

Enumeration Events

The Enumeration Event Class in Portaledge is comprised of Events that are triggered when enumeration efforts occur, e.g. a device or network is scanned, has a service attached to, or is otherwise communicated in a manner the is indicative of at attacker determining information about the device or network.

Enumeration Events rely on the PI IP Flow Interface, Snort IDS, or other sensors that detect traffic indicative of someone or something probing for information about the control system and its components. Sensors on the network can also monitor for stealth enumeration techniques such as an ArpScan. Monitoring enumeration techniques is critical as enumeration is a typical first step in a penetration attempt. If an attack can be identified during the enumeration stage the asset owner is better able to stop the attack or at a minimum limit its impact.

Enumeration Session Info Module

Most of the Events in the Enumeration Event class require information about TCP sessions be analyzed to determine if activity exceeds a trigger threshold and is indicative of an enumeration attempt. Rather than gather, store and analyze this data in each Event ACE module, Digital Bond has created an Enumeration Session Info Module that serves this purpose for all Events. This improves performance significantly and reduces the resource requirements on the PI server for this Event Class.

Detecting Port Scans and Port Sweeps

Many of the Enumeration Events detect port scans use two different criteria for triggering an alert and have different names for the alarm.

Port Scans A Port Scan Event is generated if a single system, represented by an IP address, is scanned on multiple ports with a time period. The defaults are scanned on three ports in five minutes. This will detect an attacker doing a detailed scan on a single workstation, server or other device. The thresholds can be modified to reduce false positives or catch more attackers who are scanning slowly to avoid detection. Source and destination IP addresses can be excluded from detection to prevent false positives from repeated, authorized scans.

When detected an Event will be generated such as “TCP Port Scan” or “FIN Port Scan”.

Port Sweeps A Port Sweep Event is generated when multiple systems are scanned on the same port within a time period. The defaults are three systems scanned on the same port in five minutes. This will detect an attacker who is searching a subnet for a certain service or application, like a web server or DNP3 server. The thresholds can be modified and systems can be excluded from analysis.

When detected an Event will be generated such as “TCP Port Sweep” or “FIN Port Sweep”.

FIN Port Scan Enumeration Event

Definition: The FIN Port Scan Enumeration Event will trigger an Event when TCP FIN packets are sent to multiple ports on one or more hosts.

Description: FIN port scans are used by attackers to bypass firewalls and work by sending TCP FIN packets to targeted ports. Closed ports reply with an RST packets, active ports do not reply.

Triggers

- FIN Port Scan: This trigger will generate an Event if TCP FIN packets are detected that are directed at multiple ports on a single host [default is 3 ports].
- FIN Port Sweep: This trigger will raise an Event if TCP FIN packets are detected that are directed at the same port on multiple hosts [default is 3 hosts].

Interfaces

- IP Flow: Used to detect TCP FIN communications.
- Snort or other IDS into Syslog> or Windows Event Log: As an IDS may not necessarily be deployed on a network, it is considered a secondary interface.

Finger User Enumeration Event

Definition: The Finger User Enumeration Event will trigger on any session to port 79, the standard Ringer port.

Description: Through querying the Finger service (if enabled) an attacker can enumerate the user accounts on a system.

Triggers

- Finger – This trigger will raise an alarm if any session is established on port 79.

Interfaces

- IP Flow: Used to detect the creation of a session with the Finger service.

ICMP Scan Host Enumeration Event

Definition: The ICMP Scan Enumeration Event will trigger an alert when gratuitous non ECHO ICMP packets are detected across multiple hosts.

Description: ICMP Information Request, Timestamp Request, CMP Address Mask Request, ICMP error message packets (and others) can be used to enumerate hosts utilizing methodologies not as commonly employed as ping sweeping. These methodologies rely on the replies to the various ICMP packets to detect if a host is alive.

Triggers

- ICMP Scan: This trigger will raise an alarm if any type of gratuitous non ECHO ICMP packets are detected across multiple hosts.

Interfaces

- IP Flow: Used to detect portscans.
- Sort IDS into Syslog or Windows Event Log: As Snort may not necessarily be deployed on a network, snort detection is a secondary interface path.

Syn Portscan Enumeration Event

Definition: The Syn Portscan Enumeration Event will trigger an alert when incomplete (Syn to Syn-Ack) TCP sessions are created across multiple ports on one or more hosts.

Description: A Syn Portscan sends a Syn packet to a target port and awaits the Syn-Ack reply, without ever fully establishing a full TCP session.

Triggers

- Syn Portscan: This trigger will raise an alarm if incomplete TCP sessions are tried against multiple ports on one or more hosts.

Interfaces

- IP Flow Interface: Used to detect incomplete TCP connection.
- Snort IDS into Syslog or Windows Event Log Interface: As Snort may not necessarily be deployed on a network, snort detection is a secondary interface path.

TCP Portscan Enumeration Event

Definition: The TCP Portscan Enumeration Event will trigger an alert when complete TCP sessions that immediately terminate are created across multiple ports on one or more hosts.

Description: A TCP Portscan completes the 3 way TCP connection establishment and then immediately terminates the session.

Triggers

- TCP Portscan: This trigger will raise an alarm if complete TCP to quick terminating session are tried against multiple ports on one or more hosts.

Interfaces

- IP Flow Interface: Used to detect TCP connections.
- Snort IDS into Syslog or Windows Event Log Interface: As Snort may not necessarily be deployed on a network, snort detection is a secondary interface path.

Traffic Monitor Enumeration Event

Definition: The Traffic Monitor Enumeration Event event will trigger when "out of bounds" communications occur.

Description: The Traffic Monitor Enumeration Event allows a system administrator to profile network communications on their systems. Communications that are allowed can be added on a per system basis, specifying IP addresses and ports of the allowed communications. When a communication occurs to a system that participates in the Traffic Monitoring that is not in the allowed list of communications an "out of bounds" communication is detected and an alert is created.

Triggers

- Traffic Monitor – This trigger will raise an alarm if "out of bounds" communications are detected.

Interfaces

- IP Flow Interface: Used to monitor communications.

UDP Portscan Enumeration Event

Definition: The UDP Portscan Enumeration Event will trigger an alert when UDP packets are detected as having been sent to multiple ports on one or more hosts.

Description: As UDP is a connectionless protocol, UDP scanner sends a UDP packet at a port and wait for the ICMP port not available reply. If the reply is not received the port is assumed to be active.

Triggers

- UDP Portscan: This trigger will raise an alarm if UDP packets are detected that are directed at multiple ports across one or more hosts.

Interfaces

- IP Flow Interface: Used to detect UDP communications.
- Snort IDS into Syslog or Windows Event Log Interface: As Snort may not necessarily be deployed on a network, snort detection is a secondary interface path.

Enumeration Events

- FIN Port Scan Enumeration Event
- Finger User Enumeration Event
- ICMP Scan Enumeration Event
- Syn Portscan Enumeration Event
- TCP Portscan Enumeration Event
- Traffic Monitor Enumeration Event
- UDP Portscan Enumeration Event

Integration with Enterprise SIEM

Another task in Phase I was to send the Events generated by Portaledge to an Enterprise SIEM. This was proven with Tenable Security's Security Manager and generalized for any SIEM. The integration was straightforward and took the team less than two days.

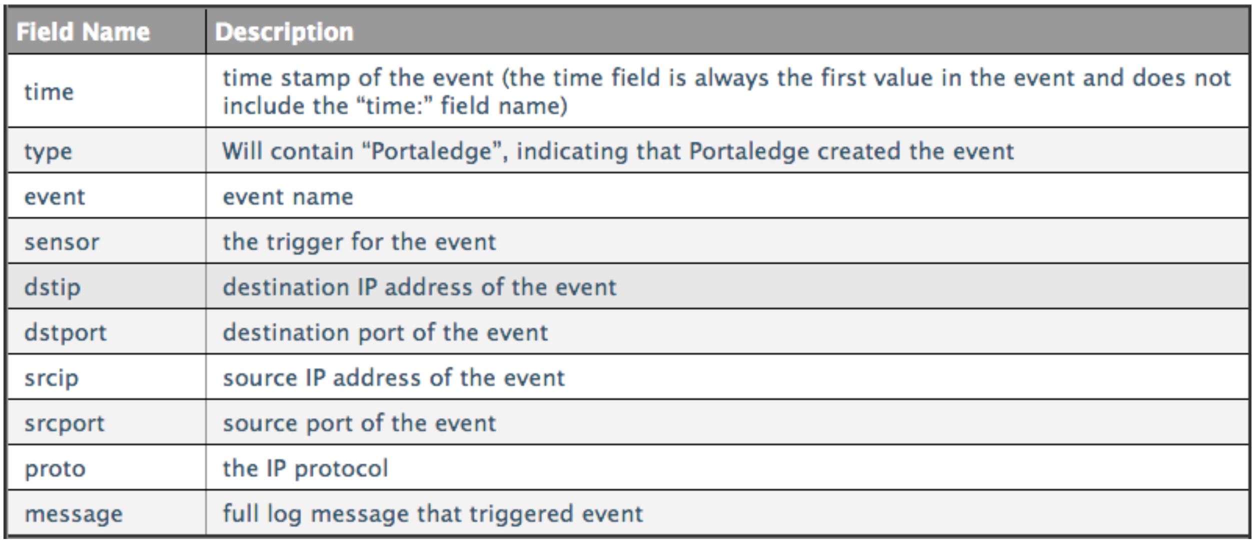
The Portaledge Events, Event Class Events and Meta Events store information not only on the event, but also on what triggered an event and the related event chain. This information is useful for eliminating false positives and better characterizing potential attacks, but it makes integration into an enterprise SIEM very difficult because the data varies in length and field structure. While SIEM's can import and decode a variety of log and event formats, the format must be consistent to use the SEM import tools.

Therefore the Portaledge team developed and integrated a semOutput functions to normalize the various event fields for transfer and import into a SEM. This function resides internal to the Portaledge software package, thereby eliminating the need for secondary scripts to translate Portaledge output into the normalized output.

The semOutput function creates a normalized event in the following format:

Field Name: Value | Field Name: Value | … Field Name: Value <eol>

The fields are listed in described in the table below. The fields are listed in the table in the order they are placed in the semOutput normalized output, and all fields are included in all semOutput normalized events. A value of 0 is used when the field is not applicable for a normalized event.



Field Name	Description
time	time stamp of the event (the time field is always the first value in the event and does not include the "time:" field name)
type	Will contain "Portaledge", indicating that Portaledge created the event
event	event name
sensor	the trigger for the event
dstip	destination IP address of the event
dstport	destination port of the event
srcip	source IP address of the event
srcport	source port of the event
proto	the IP protocol
message	full log message that triggered event

Documentation to support the integration and a detailed example is available at https://www.digitalbond.com/tools/portaledge/portaledge-sem-integration/ . This includes white papers that describe integration with Tenable Security's SIEM and a generic SIEM.

Phase II

The purpose of Phase II was to develop Portaledge modules to monitor and detect security events related to NERC CIP-005 and NERC CIP-007. The NERC CIP focus was chosen because security spending and interest in the electric security was and is almost entirely based on its impact on helping organizations be NERC CIP compliant.

NERC CIP-005 Monitoring - AKA Firewall Monitoring Modules

NERC CIP-005 covers the security requirements for the electronic security perimeter (ESP). The electronic access devices that control access to the ESP are typically firewalls. There are security requirements that involve monitoring the ESP access device. Specific requirements for IP-based access devices from CIP-005-4 are:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
>
> R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

Firewall Security Events

The Portaledge team reviewed all of the events logged by the supported firewalls and selected the events that were related either to a potential attack that required alerting or successful login attempts that needed to be recorded and saved for at least 90 days. The events are placed in one of the following categories:

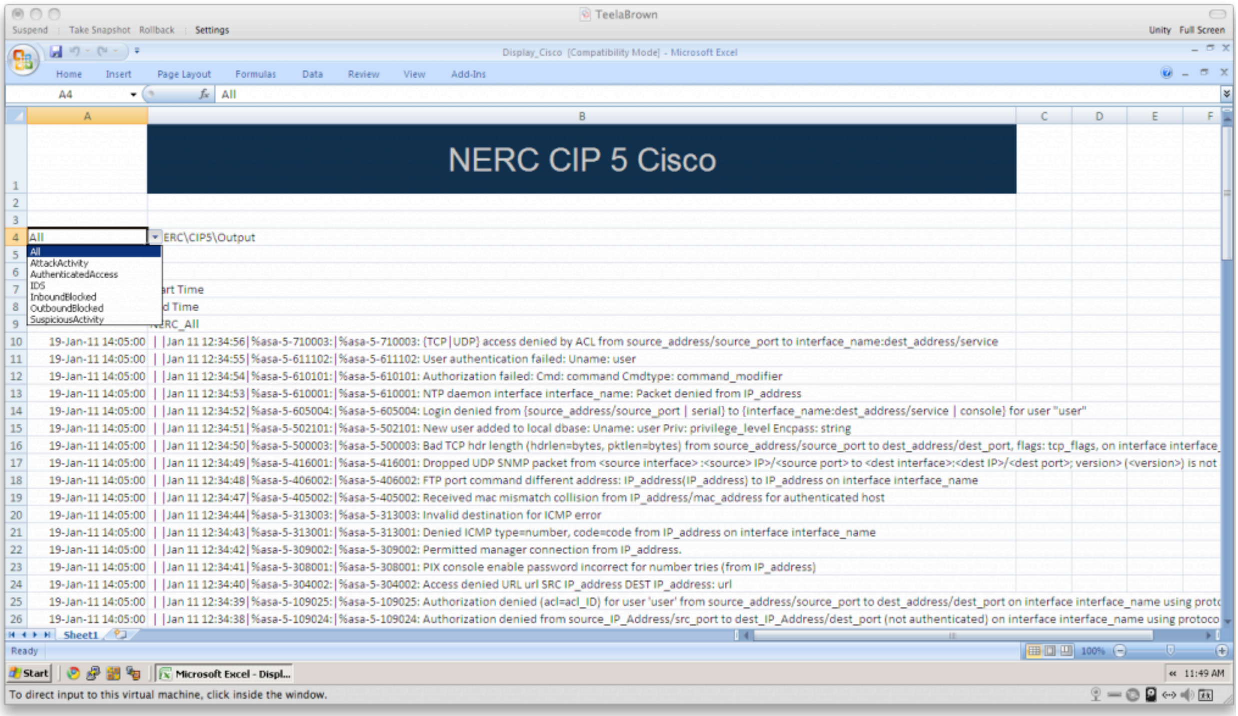
- Inbound Blocked
- Suspicious Activity
- Attack Activity
- Outbound Blocked
- Authenticated Access

The CIP-5 modules are currently available for CISCO PIX/ASA firewalls and the Juniper firewalls. You can view the list and categorization of all the security events that are monitored by the CIP-5 modules.

- Cisco PIX/ASA Firewall Monitored Security Events
- Juniper Firewall Monitored Security Events

The CIP-5 Module Approach is very simple. The firewall is configured to send the syslog events to a PI Syslog Interface. The PI Syslog Interface forwards the events to a PI Server where the module is deployed.

The defined security events have corresponding tags in the PI server. The data is stored in these tags. The module database and PI server then take the data in tags and output it in an event window. Currently the Portaledge CIP-5 output is a window of scrolling events, see below.



```
All  ERC\CIP5\Output
     rt Time
     d Time
     ERC_All
19-Jan-11 14:05:00 | |Jan 11 12:34:56|%asa-5-710003:|%asa-5-710003: {TCP|UDP} access denied by ACL from source_address/source_port to interface_name:dest_address/service
19-Jan-11 14:05:00 | |Jan 11 12:34:55|%asa-5-611102:|%asa-5-611102: User authentication failed: Uname: user
19-Jan-11 14:05:00 | |Jan 11 12:34:54|%asa-5-610101:|%asa-5-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
19-Jan-11 14:05:00 | |Jan 11 12:34:53|%asa-5-610001:|%asa-5-610001: NTP daemon interface interface_name: Packet denied from IP_address
19-Jan-11 14:05:00 | |Jan 11 12:34:52|%asa-5-605004:|%asa-5-605004: Login denied from {source_address/source_port | serial} to {interface_name:dest_address/service | console} for user "user"
19-Jan-11 14:05:00 | |Jan 11 12:34:51|%asa-5-502101:|%asa-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
19-Jan-11 14:05:00 | |Jan 11 12:34:50|%asa-5-500003:|%asa-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address/source_port to dest_address/dest_port, flags: tcp_flags, on interface interface_
19-Jan-11 14:05:00 | |Jan 11 12:34:49|%asa-5-416001:|%asa-5-416001: Dropped UDP SNMP packet from <source interface> :<source> IP>/<source port> to <dest interface>:<dest IP>/<dest port>; version> (<version>) is not
19-Jan-11 14:05:00 | |Jan 11 12:34:48|%asa-5-406002:|%asa-5-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
19-Jan-11 14:05:00 | |Jan 11 12:34:47|%asa-5-405002:|%asa-5-405002: Received mac mismatch collision from IP_address/mac_address for authenticated host
19-Jan-11 14:05:00 | |Jan 11 12:34:44|%asa-5-313003:|%asa-5-313003: Invalid destination for ICMP error
19-Jan-11 14:05:00 | |Jan 11 12:34:43|%asa-5-313001:|%asa-5-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
19-Jan-11 14:05:00 | |Jan 11 12:34:42|%asa-5-309002:|%asa-5-309002: Permitted manager connection from IP_address.
19-Jan-11 14:05:00 | |Jan 11 12:34:41|%asa-5-308001:|%asa-5-308001: PIX console enable password incorrect for number tries (from IP_address)
19-Jan-11 14:05:00 | |Jan 11 12:34:40|%asa-5-304002:|%asa-5-304002: Access denied URL url SRC IP_address DEST IP_address: url
19-Jan-11 14:05:00 | |Jan 11 12:34:39|%asa-5-109025:|%asa-5-109025: Authorization denied (acl=acl_ID) for user 'user' from source_address/source_port to dest_address/dest_port on interface interface_name using prot
19-Jan-11 14:05:00 | |Jan 11 12:34:38|%asa-5-109024:|%asa-5-109024: Authorization denied from source_IP_Address/src_port to dest_IP_Address/dest_port (not authenticated) on interface interface_name using protoco
```

The monitored data is available as tags and in the module database, so an owner/operator familiar with PI could build displays to show the data in any way they wanted. This could include graphs, pie charts, trends, etc.

Installation

Installing the CIP-5 module does require some PI skills such as configuring a PI interface, adding tags from a spreadsheet, and configuring the module database from a spreadsheet. A user skilled with the PI ACE will understand how to do this quite easily, but those that are not may have difficulty.

Detailed documentation on the installation is available in the download of the CIP-5 monitoring release package. The release package is an executable, .exe, file that you run on the PI Server.

General information on installing Portaledge, including a list of the PI Server license requirements, is available on the Event Installation page.

Non-CIP Use By Other Industries

While these modules were developed to help electric sector companies meet the NERC CIP-5 security monitoring requirements, they are useful for any organization that has:

- A Cisco ASA/PIX or Juniper firewall at a security perimeter

- A PI Server

Monitoring the security perimeter is a good security practice even when the firewall is effective. If you see someone from the Enterprise Network trying to break through the firewall to the control center you can potentially stop the attacker before he is successful. If outbound, control center originated traffic is stopped at the firewall it is likely a person or automated program trying to reach something it shouldn't and can indicate the control center has been compromised. For example, a Stuxnet infected system in the control center would have been detected trying to contact the command and control servers in Malaysia.

NERC CIP-007 Monitoring - AKA Ports and Services Monitoring Modules

NERC CIP-007 regulates the security of cyber assets, particularly workstations and servers inside the electronic security perimeter. An important element is that each cyber asset should only have open ports and running services that are required for operation. The Portaledge NERC CIP-007 Monitoring identify when new listening ports are opened or new services are running.

This is an agent based approach that requires the Windows computers to send the information to a PI interface. There are a couple of different methods to achieve this including WMI and Event Logs.

For port monitoring the design writes to 3 output tag aliases (sy_TCPestablished, sy_TCPlisteners, sy_UDPlisteners) Results are a sorted comma separated string (eg. Established: 135,445, 49152, 49153, 49154)

Monitoring services is similar and the two outputs are (sy_Services_All, sy_Services_Started) In this case tag values represent a count. On changes in services the value is annotated with a csv string of service names.

4. Contract Tasks and Deliverables

The contract was awarded in two Phases: Phase I and Phase II. This section details the contract deliverable requirements and deliverable results by Phase.

Phase I Deliverables

Deliverable 1: Task 5.0: Demonstrate each of the .audit files and the anonymized results from demonstration.

Digital Bond, working with the vendor, ran the .audit file on a system in the lab and delivered a complete set of demonstration results. One results file for each Bandolier Security Audit File developed in Phase I. These are available for government inspection or use.

Deliverable 2: Task 6.0: Prepare Nessus .audit files and associated documentation for at least 20 control system devices or applications will be available to project participants, from Tenable Network Security's direct feed, and the Recipient's website through subscriber content.

The following 23 Nessus .audit files were developed and released to meet this requirement:

1. ABB Ranger NM2003 DAS for TRU64
2. ABB Ranger NM2003 RDAS for TRU64
3. ABB Ranger NM2003 WEB for TRU64
4. ABB Ranger NM2003 Workstation for Windows XP
5. Altsom Grid e-terrabrowser Client for Windows XP
6. Alstom Grid e-terrabrowser Web Server for Redhat Linux
7. Alstom Grid e-terrabrowser Web Server for Windows 2003 Server
8. Alstom Grid e-terraplatform App Server for Redhat Linux
9. Alstom Grid e-terraplatform App Server for Windows 2003 Server
10. Emerson Ovation Domain Controller for Windows 2003 Server
11. Emerson Ovation Engineering Workstation for Windows 2003 Server
12. Emerson Ovation Operator Workstation for Windows XP
13. Emerson Ovation SCADA Server for Windows 2003 Server
14. Matrikon Security Gateway Tunneller on Windows 2003 Server
15. OSIsoft PI Server on Windows 2003 Server
16. Siemens Spectrum Power TG SCADA Host Server on Linux
17. Siemens Spectrum Power TG SCADA Workstation on Windows XP
18. Siemens Spectrum Power TG Web Host on Windows Server 2003
19. SNC GENe on Linux
20. Telvent OASyS DNA Engineering Station on Windows 2003 Server

21. Telvent OASyS DNA Historical Server on Windows 2003 Server
22. Telvent OASyS DNA RealTime Server on Windows 2003 Server
23. Telvent OASyS DNA XOS Workstation on Windows XP

The Bandolier Security Audit Files can be downloaded from:

http://www.digitalbond.com/tools/bandolier/downloads/

Deliverable 3: Task 7.0: Prepare an XCCDF / OVAL file for each of the .audit files in deliverable 2 that will be available on the Recipient's website through subscriber content. This file will allow the .audit files to be used on most vulnerability scanners other than Nessus. These files will be available on the Recipient's website through subscriber content.

Digital Bond converted the Bandolier Security Audit Files listed in Task 6.0 above into the OVAL format. They are available to the US Government and any interested party free of charge. For example in March 2013, they were provided to Farnam Hall Ventures for an ERCOT project.

Deliverable 4: Task 8.0: Prepare Nessus .audit templates for each class of device in item 2 to ease asset owners modifying the .audit files for the brand of system they use. These files will be available on the Recipient's website through subscriber content.

Digital Bond prepared a document titled Bandolier Audit Development Guide to meet this task. It includes both a process and checklist for developing .audit files.

Deliverable 5: Task 13.0: Demonstrate of each of the ACE incident detection modules and the anonymized results from demonstration.

Digital Bond provided a sample text file for each time of alert. This was done in a lab environment so no owner/operator data was revealed. This files are available upon request.

Deliverable 6: Tasks 14.0 and 15.0: Prepare a documented set of ACE incident detection modules for the PI System that can be used by any asset owner with a PI System. The ACE incident detection modules and associated documentation will be available to project participants, from OSIsoft support website, and the Recipient's website through subscriber content.

Digital Bond developed and released a set of ACE Incident Detection Modules including an Availability Event Class, Enumeration Event Class and Meta Event Class. The modules, documentation and other information is available for download at:

http://www.digitalbond.com/tools/portaledge/

Deliverable 7: Tasks 16.0 and 17.0: Prepare an ACE incident detection module conversion document to allow third party historians to use the data dictionaries and meta security event language.

Digital Bond developed pseudo code detailing the logic behind each of the existing Portaledge models. This is available free of charge upon request

Deliverable 8: Task 24: Deliver OSisoft PI / Tenable Security Center integration package.

Digital Bond has posted a web page with this information and created a document that explains the process in more detail. These can be seen and downloaded at:

http://www.digitalbond.com/tools/portaledge/portaledge-sem-integration/

Deliverable 9: Task 26: Deliver OSIsoft PI / Generic enterprise SEM integration package.

Digital Bond has posted a web page with this information and created a document that explains the process in more detail. These can be seen and downloaded at:

http://www.digitalbond.com/tools/portaledge/portaledge-sem-integration/

Phase II Deliverables

Task 1.0: Revised Project Management Plan

Digital Bond completed the revision shortly after Phase II award.

Task 2.0 : Identify and select 4 SCADA or DCS widely used in the energy sector.systems and applications at asset owner participants

> Task 2.0: Create and test .audit files for system 1
>
> Task 2.0: Create and test .audit files for system 2
>
> Task 2.0: Create and test .audit files for system 3
>
> Task 2.0: Create and test .audit files for system 4
>
> Task 2.0: Update/Document .audit Files and Release for systems 1 through 4

Task 2.0 was essentially creating and releasing .audit files for four new systems. Note that Phase II count of Bandolier Security Audit Files is by system, while the Phase I was by component.

1. SISCO ICCP AX-S4 ICCP Server, Version 4.0059.2 on Windows Server 2003
2. ABB 800xA DCS with the following components
    a. Connectivity Server 5.x on Windows Server 2003
    b. Aspect Server 5.x on Windows Server 2003
    c. Historian 5.x on Windows Server 2003
    d. Domain Controller on Windows Server 2003
    e. Engineer / Operator Workplace 5.x on Windows XP
3. Control Systems International (CSI) UCOS SCADA with the following components
    a. PHA – Historian 5.2 on Windows Server 2008 R2
    b. FCU App Server 1.0 on CENTOS
    c. Operator Work Station 5.2 on Windows 7
4. OSIsoft PI Server 3.4.x on Windows Server 2008 R2

These Bandolier Security Audit Files can be downloaded from Digital Bond's website at: http://www.digitalbond.com/tools/bandolier/downloads/

Task 3.0: Create NERC CIP subset .audit files for the twenty Bandolier Security Audit Files developed in Phases 1 and 2

Digital Bond created and released a NERC CIP-007 R8 Scan Policy Package. CIP-007 R8 is the vulnerability assessment portion that applies to the cyber assets (the systems that Bandolier audits). It collects the information required for that CIP requirement using a low impact credentialed scan. The package includes the capability to audit both Windows and Unix systems.

This package can be downloaded from Digital Bond's website at: http://www.digitalbond.com/tools/bandolier/downloads/

Task 4.0: Develop and release a Portaledge Module to collect, retain and analyze to detect attacks in real time for the electronic security perimeter access devices as required in NERC CIP-005

Digital Bond released NERC CIP-005 Portaledge Modules for the Juniper firewall and CISCO ASA/PIX firewalls. The modules are available for download from http://www.digitalbond.com/tools/portaledge/portaledge-release-packages/

Task 4.0: Develop and release a Portaledge Module to collect, retain and analyze to detect attacks in real time for the cyber assets as required in NERC CIP-007.

Two ACE modules were completed and released. One for port monitoring, Portaledge_NERC_CIP_Seven_Portinfo.exe, and a second for monitoring services, Portaledge_NERC_CIP_Seven_Serviceinfo.exe. These are two important CIP-007 security configuration settings that must be documented and periodically audited. They have been released to interested users and are available to any government user upon request.