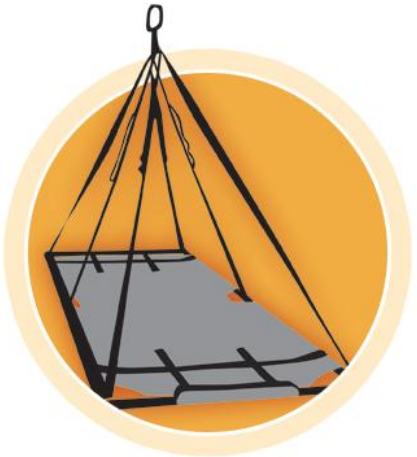

Turning **insight** into **action**.

OSIsoft. USERS CONFERENCE 2011

# Portaledge: Using the PI System for CIP-5 / CIP-7 Monitoring

Presented by **Dale Peterson, Digital Bond, Inc.**

# Portaledge Research Project



- Funded by US Dept of Energy
  - More than $500K in funding
- OSIsoft is a contributor
  - Donated software and support services
- Available free of charge at digitalbond.com
  - Still requires appropriate OSIsoft licenses

# Concept

- PI Server aggregates and correlates data
- Use PI Server to aggregate and correlate security data to detect cyber attacks
  - Requires PI IT Monitor Interfaces and PI ACE
- BIG & SIMPLE IDEA – This can meet CIP-5 and CIP-7 automated monitoring requirements

# CIP-005 R3.2

Where technically feasible, the security monitoring processes shall detect and alert for attempts at or actual unauthorized access.

# Simple Solution

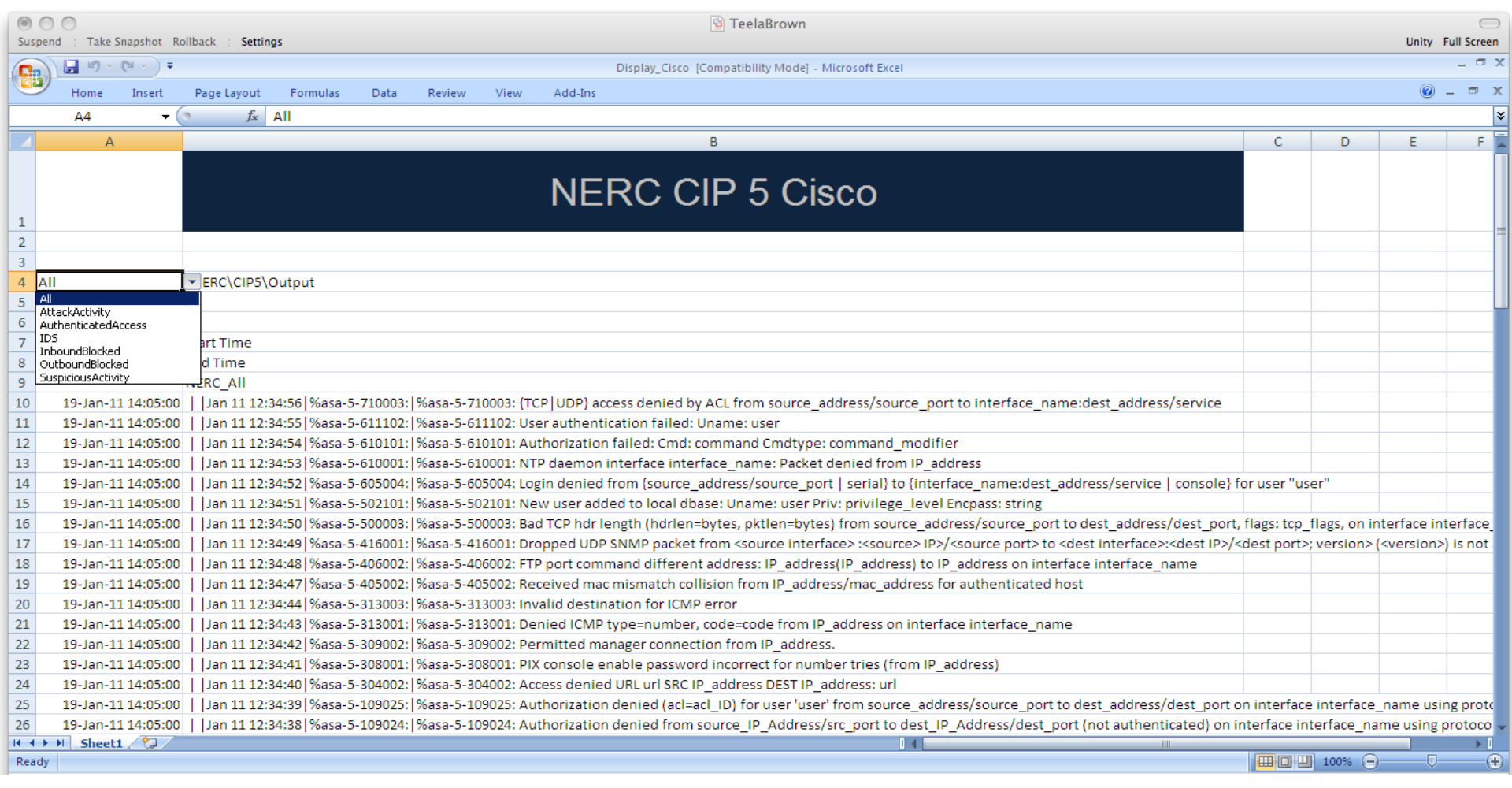
- CIP-5 covers perimeter security / firewalls
- Monitor firewall logs
  - Syslog PI Server interface
  - Identify security events in list of all log events
  - Currently available for Cisco and Juniper

# Security Monitoring Categories

- Inbound Blocked
- Suspicious Activity
- Attack Activity
  - No IDS/IPS monitoring at perimeter, yet - simplicity
- Outbound Blocked
- Authenticated Access
  - Retain electronic access logs for 90 days

# Output / Alerting

- Currently very simple
  - A window with the scrolling list of security events including category
- You're all PI System experts, display what you want!
  - The events and categories are in the database
  - We are considering adding some logic


TeelaBrown
Suspend
Take Snapshot
Rollback
Settings
Unity
Full Screen
Display_Cisco [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Add-Ins
A4
All
NERC CIP 5 Cisco
All
AttackActivity
AuthenticatedAccess
IDS
InboundBlocked
OutboundBlocked
SuspiciousActivity
ERC\CIP5\Output
art 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 proto
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
Sheet1
Ready
100%

# Useful for Any Sector

- Focus and name relates to NERC CIP / Bulk Electric Sector
- But . . . will detect attacks and save forensic evidence for any SCADA or DCS perimeter firewall

# CIP-007 R6

The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

# First Module – Windows Systems

- Same approach as firewalls
  - Identify security events
  - http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx
  - Create PI System events and categories via PI ACE
  - Display as a console window

# Timeframe

- CIP-7 Windows Module in June
- CIP-7 Unix Module in July
- Unknown: Printers, Field Devices with Ethernet Card, etc.

# Bonus: Bandolier Security Audit Files

- Another DoE funded project
  - Free at digitalbond.com
- Audit PI Server security settings
  - Operating System Settings, 196
  - PI Server security settings, 26
  - Works with Nessus Compliance Plugins
  - Reduced / CIP only version coming this summer

# OS Settings Audit

- Based on Microsoft recommendations
- Tested by OSIsoft with the PI Server
  - Verify the setting will not break the app
  - Not much of an issue with PI Server, but can be a big issue with SCADA and DCS apps

# PI Server Security Audit Tests

- Run a batch file to extract info from database
  - PI Config dumps settings to a file that is audited
- Application Check Examples
  - Has default user read access been disabled?
  - Are any PI Server trusts using the PI Admin account?
  - Most derived from the OSIsoft white paper

# Reference Links

OSIsoft Whitepapers:
techsupport.osisoft.com/Knowledge+Center/System+Manager+Resources

OSIsoft Webcasts:
www.osisoft.com/resources/webinars/Webinars_On_Demand.aspx

Portaledge: www.digitalbond.com/tools/portaledge

Bandolier: www.digitalbond.com/tools/bandolier

# Thank you

Turning **insight** into **action**.