Department of Energy
PI for Security and Securing PI

Dale Peterson

Digital Bond, Inc.

peterson@digitalbond.com

Digital Bond

- Control System Security Practice
  - Research and Consulting
- Available on Digital Bond Site
  - IDS Signatures for Control System Protocols
  - Nessus SCADA Plugins
  - SCADA PLC Honeynet
  - Blog, SCADApedia, White Papers, Podcasts
  - SCADA Security Scientific Symposium (S4)

Digital Bond Research Approach

- Add control system intelligence to existing security solutions
  - Control system IDS signatures
  - SCADA plugins for Nessus scanner
- Add security intelligence to deployed control system products
- Make resulting tools available to Digital Bond site subscribers
  - Almost free, $100 / year

Department of Energy Contract

- Digital Bond is one of the recipients
- OSIsoft was a partner in the submission
  - Generous contribution of PI software
  - Training and technical support
  - Access to top OSIsoft technical talent
- Two-year research program
  - Results will begin to be available Summer, ‘08

Part 1 - Bandolier

- Concept: How do we verify that our control system workstations and servers are in a secure / best practice configuration.
  - Identify best practice [gold standard]
  - Create an audit template that can be used in Nessus and other scanners
  - Asset owners audit systems at install and periodically
    - Audits are much less risky than typical scanning

Bandolier

- Tests for ‘goodness’ rather than ‘badness’
- Operating system tests
- Application tests [web server, database]
- Control system application tests
  - Work closely with vendor to understand configuration settings and gold standard
- Result identifies variations from Gold Standard

Bandolier Candidates

- OSIsoft PI Server
  - Possibly OPC interface
- OPC UA Server
- Telvent OASyS DNA
- ABB Ranger
- SNC GENe
- Matrikon OPC server
- Siemens Telegyr
- Emerson Ovation
- More to come
  - At least twenty

Part 2 - Portaledge

- Concept: How do we aggregate and correlate security events on control system networks to identify attacks?
  - – PI server aggregates and correlates data
  - – PI server exists on a huge percentage of control system networks
  - – Add security event management intelligence to PI server

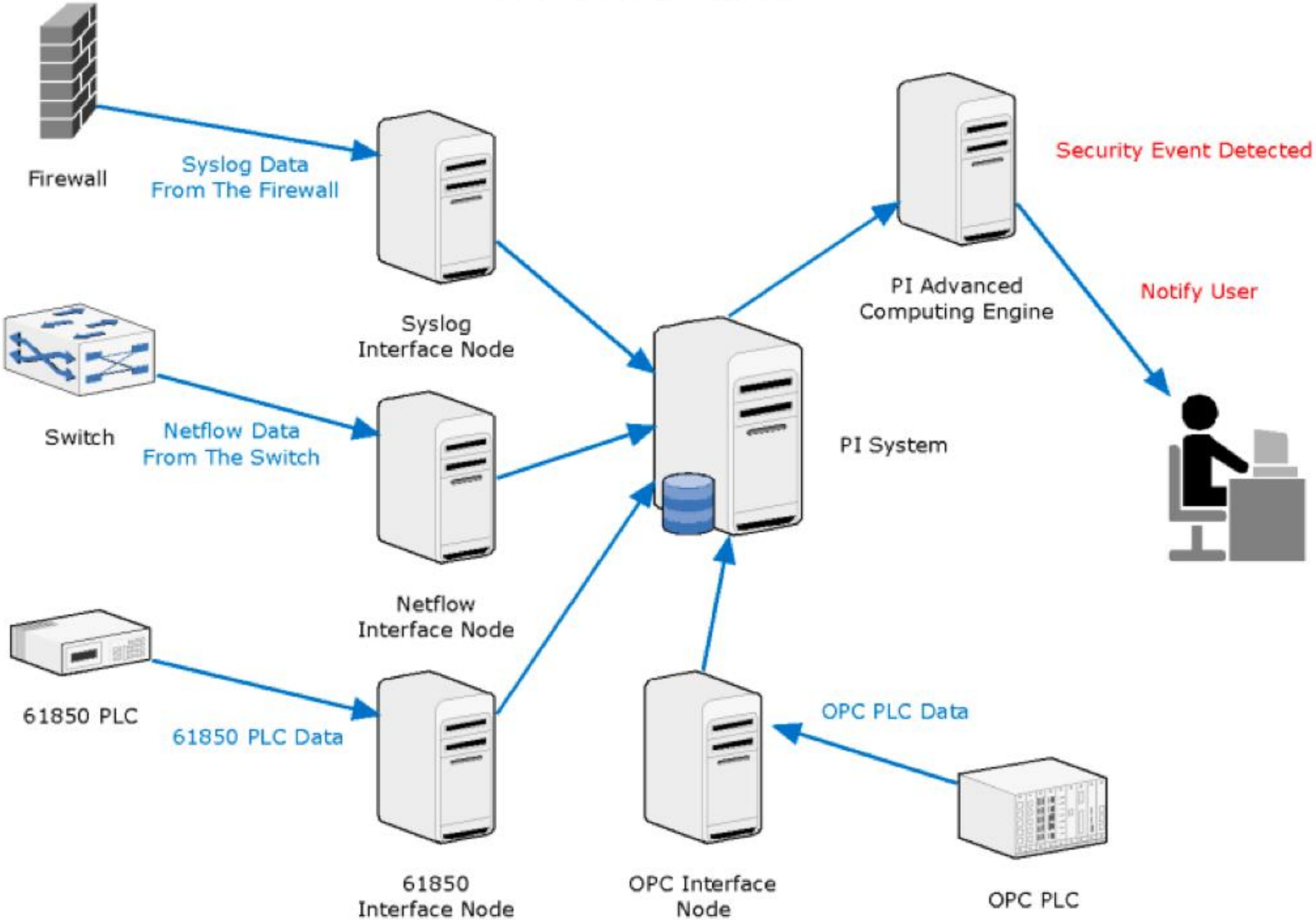
Step 1: Identify Security Events

- Security events are everywhere
- Network and security systems
  - Firewall and IDS logs
  - Router netflow data
- Workstation and server logs
- Control system application logs
- Field device logs
- …

Step 2: Get the Data Into PI

- PI interfaces offer tremendous flexibility
  - IT Monitor interfaces [syslog, snmp, netflow]
  - Protocol interfaces
  - Application interfaces
  - Exceeded our expectations
  - You all know this
  - Only challenge to date is IEC 61850 interface

DATA FLOW


Firewall
Syslog Data From The Firewall
Syslog Interface Node
Switch
Netflow Data From The Switch
Netflow Interface Node
61850 PLC
61850 PLC Data
61850 Interface Node
OPC Interface Node
OPC PLC Data
OPC PLC
PI System
PI Advanced Computing Engine
Security Event Detected
Notify User

Step 3: Identify Meta Events

- What is a meta event
  - A sequence of security events that indicate a specific attack goal or achievement
    - Firewall log rejection, followed by scanning, followed by exploit attempt, followed by new user added to control system application
    - New workstation on control system network, followed by function code scan of PLC, followed by reboot or write commands

How to Identify Meta Events

- Digital Bond has an offensive team
  - Attack and build exploits
  - Used for application assessments
- Run application assessment and exploit building in our lab
- Follow respected attack taxonomies
- Defensive team identifies created evidence

Step 4: Write ACE Modules

- Correlation is what PI ACE does today
  - Now using it for security incident detection
- ACE modules and documentation on meta events will be available on Digital Bond site
  - Will require appropriate ACE and interface licenses from OSIsoft

How Can You Help?

- Fill out anonymous survey on what interfaces you currently use and what interfaces you own
- If you are highly interested in this we could use a couple more test sites

Questions?

Dale Peterson
Digital Bond, Inc.

954-384-7049
peterson@digitalbond.com