U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Dale Peterson

Digital Bond, Inc.

Bandolier and Portaledge

Summary Slide: Bandolier

- **Outcomes:** Insure new and upgraded SCADA and DCS are deployed in the best possible security configuration
- **Roadmap Challenge:** Consistent metrics are not available to measure and assess security posture; there is a lack of tested and validated security tools
- **Major Successes:** Over twenty Bandolier Security Audit Files, major vendor participation, used in FAT/SAT, more vendors want in

- **Schedule:** Over twenty files to date. NERC CIP files and more Bandolier files planned.
- **Level of Effort: $**1.2M to date
- **Funds Remaining:** $575K pending
- **Performers:** Digital Bond, Inc.
- **Partners:** ABB, AREVA, Emerson, Matrikon, OSIsoft, SNC, Tenable, Telvent and more

Technical Approach and Feasibility

- **Approach**
  - – Work with vendor to identify all security parameters and each parameter’s optimal setting
    - 100’s of settings, previously defaults were often weak
  - – Develop Bandolier Security Audit File
  - – Nessus scanner & Bandolier File can audit a component and identify settings that are weak
    - Cost of only $100 + Nessus or free from vendor
- **Metrics for Success**
  - – % of Energy Sector systems covered
  - – % of new systems being deployed securely

Technical Approach and Feasibility

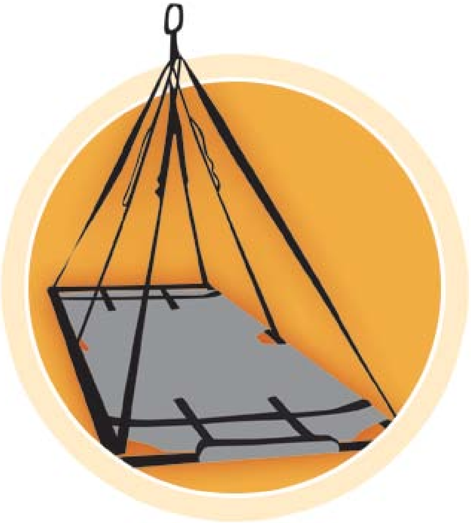
- **Challenges to Success**
  - Getting SCADA/DCS Vendors to Participate
    - Focused first on vendors with active security programs
    - Get customers to ask vendors for Bandolier
  - Sustainability of Bandolier post DoE funding
    - Initial Bandolier file shows the value in addressing security at deployment, QA help, customer demand, …
- **Technical Achievements to Date**
  - ABB, AREVA, Emerson, Matrikon, OSIsoft, SNC, Telvent
  - Being used in Factory and Site Acceptance Testing
  - Vendors are paying for next version and new components

Next Steps

- **Approach For the Next Year**
  - Get remaining vendors with significant market share into the program
    - Honeywell, SISCO, Siemens & Yokogawa are already in
  - Help vendors maximize Bandolier benefit
    - Integrate into QA, engineering services
  - Move more vendors to payment model for future
  - Reduced and enhanced NERC CIP versions
    - CIP is driving electric asset owner programs
    - Get more asset owners used to security auditing tool

Summary Slide: Portaledge

- **Outcomes:** Use existing historian, PI Server, to aggregate security events and detect cyber attacks
- **Roadmap Challenge:** Detect intrusions
- **Major Successes:** Proven attack detection capability, released versions of Portaledge, proven sending of detected cyber events to a SEM



- **Schedule:** Released versions to date. Planned are CIP detection modules in 3/2011
- **Level of Effort:** 1.2M to date
- **Funds Remaining:** $575K
- **Performers:** Digital Bond, Inc.
- **Partners:** OSIsoft

Technical Approach and Feasibility

- **Approach**
  - Deploying complex security systems on SCADA/DCS is difficult
  - Historians have the capability to aggregate and correlate events, why not do this with security
  - Cyber attack detection in most popular historian
- **Metrics for Success**
  - % of Energy Sector systems deploying Portaledge
  - Ease of deployment based on time and skill level

Technical Approach and Feasibility

- **Challenges to Success**
  - Deploying Portaledge requires PI Server skills
    - Templates and documentation to ease process
    - Active with more skilled PI clients
    - Get PI Integrators to offer Portaledge services
  - Owner/operator attack detection demand is low
    - Focusing on helping meet CIP monitoring requirements
- **Technical Achievements to Date**
  - Detecting cyber attacks such as scans and outages
  - Integrated in a few owner/operator sites, demo at PNNL
  - Exporting events to 3rd party Security Event Managers

Next Steps

- **Approach For the Next Year**
  - Develop NERC CIP-005 R3 module to monitor firewalls
  - Develop NERC CIP-007 module to monitor cyber assets
  - Owner/operators are clamoring for CIP solutions
- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - Portaledge can feed raw and correlated security events to visualization projects and SEM's
  - Already demonstrated at PNNL and with SEM