Challenges to Vendors

DOE-OE National SCADA Test Bed - based on Lessons Learned from Idaho National Laboratory's NSTB Activities

www.inl.gov

Idaho National Laboratory

Challenges to Vendors – Code and Features

- Proof of Secure Coding Practices
  - Code Reviews vs Code Certification
  - Management of memory and String processing
  - Debug and compile features disabled at installation
  - Critical Partners Coding Practices
- Security Features
  - Authentication, Least Privileged, Filtered, Monitored and Logged of all Resources
    - Hosts, Memory, Networks
  - Secure Update Capabilities

Challenges to Vendors – Vulnerability Results

- Availability of Independent Vulnerability Assessment Results
  - Open Configurations to Researchers
  - Appropriate Information Sharing of Results
- Response to Vulnerability/Exploit Release or Incident
  - Partnerships with other incident response entities
    - Government CERTS, Sector Specific ISACs, Research Communities and Regulatory

Challenges to Vulnerabilities

- Response to Vulnerability/Exploit Release or Incident (continued)
  - Notification to Users
  - Notification to Stakeholders
  - Decision Points and Makers Identified
    - Roles and Responsibilities
  - Management of Message
- Response to Vulnerability/Exploit Release
  - Response plan established
    - Corrective Action to Users
  - Relationships with OS and Integration providers

Challenges to Vendors - Incidents

- Response to Incident
  - Forensics data analysis
  - Consequence Analysis
  - Threat Analysis Requires associations with other entities
  - Decision points to involve regulatory entities and law enforcement

Challenges to Vendors - Support

- Creating a Security Support Model that fits the Business Model
- Integration with Others
  - Managed Security Service Providers
  - Third Party Integrators
  - On-Site Integrators
- Revision Control of Code
- Version Control of Installation
- Remote Access Roles and Responsibilities
  - Roles, Authentication
  - Revocation
  - Logging of Actions