Bandolier
Auditing Control System Security with Vulnerability Scanners

Dale Peterson
Digital Bond, Inc.
peterson@digitalbond.com

© 2009 Digital Bond, Inc.
Identifying the Problem

• How do we establish an optimal / best possible secure configuration for our control system servers and workstations?
• How do we verify that this configuration has not changed over time?
• Can we do this using existing security tools at a low or no additional cost?
The Solution: Bandolier

- Collaborate with vendor and asset owner partners to identify the optimal security configuration
- Assess and extract security configuration data
- Create audit files that can be used in Nessus and other scanners
- Deliver through subscriber content and vendor support channels
Multiple Levels of Testing

**Operating System Settings**
- Policies
- Account Management
- Logging
- Ownership and Permissions
- Services
- Processes
- Windows Registry
- Configuration Files

**Supporting Application Settings**
- Web Servers
- Application Servers
- Database Servers
- SSH Servers
- LDAP Servers
- Authentication Libraries

**Control System Application Settings**
- Authentication and Authorization
- Configuration Files
- Default Accounts
- Logging
- Application File Ownership and Permissions
- Services
Example: Telvent OASyS DNA

Over 1,100 Security Audit Checks!

Realtime Server, Historian, HMI, Engineering Station
Nessus Compliance Check Plugin

- Only use one Nessus plugin
- Safer than traditional scanning
  - Secure management connection, not a scan
- Evaluates the “known good” rather than the “known bad”
- Customizable for local security policy
- Exporting to OVAL/XCCDF for use in other vulnerability scanners and security tools
Using Bandolier with Nessus

• Prerequisites
  - Digital Bond Site Subscription [$100] or
  - Get file from your control system vendor
  - Nessus Professional Feed Subscription
    • Many organizations already have a Nessus subscription
Bandolier Status

• Available
  - ABB Ranger
  - Siemens Power TG
  - SNC GENe
  - Telvent OASyS DNA

• In-Process
  - AREVA e-terra
  - Emerson Ovation
  - Matrikon OPC
  - OSIsoft PI
  - Wonderware InTouch
More Information

• **Funded by Department of Energy**
• SCADApedia Articles
  – www.scadapedia.com
• Digital Bond Website and Blog
  – www.digitalbond.com
• Your Control System Vendor
• Contact Us
  – info@digitalbond.com