Industrial Defender
Global Leader in Automation Systems Management:

Addressing the convergence of security, compliance and change management in automation systems environments

January, 2013
Goals and Objectives for the session

- Control System security threat trends

- Is your control system secure?

- How would you know if your system integrity was compromised?

- Review Control System Security challenges

- Discuss solutions to automate security, compliance and change management
Security

Question:
Do you believe your automation environment is MORE or LESS vulnerable to service disruptions, whether from malicious attackers or well intentioned insiders who do something they shouldn’t?

Vulnerabilities are on the rise: In 2011, NEW public SCADA vulnerabilities increased 8x according to Symantec’s 2012 Threat Report

“Major cyber attack aimed at natural gas pipeline companies”
May 7, 2012

“Oil Companies Spring a Leak”
July 17, 2012

“Hackers Lay Claim to Saudi Aramco Cyberattack”
August 24, 2012

Security is now a part of doing business
Threat trends for control systems


Era of Legacy Control System Technology

- Code Injection
- Password Cracking
- Self-Replicating Malicious Code
- Password Guessing

Era of Information Technology

- Advanced Persistent Threat
- ICS Application Specific Malicious Code (STUXNET)
- SHODAN/OSINT
- Rogue VPN Tunnel Attack
- ICS Attack Proof-of-Concept
- Command and Control Distributed Attack Tools
- Enumeration Scripts
- Specific Malicious Code
- Automated Probes and Scans

Control System Zone of Defense

- C-Day Vulnerabilities
- Denial of Service
- Packet Spoofing
- Exploiting Known Vulnerabilities
- Brute Force Attacks
- HTTP Proxy Servers
- Log Flossing
- Accessing and Controlling Sessions
- "Compromise" Sessions
- Device Hijacking
- Root Access
- Hardware Hijacking
- Code Injection
- Password Cracking
- Self-Replicating Malicious Code
- Password Guessing

Derived from 

Growing Malware Threats 17x over the past 2 years!

According to F-Secure, “As much malware [was] produced in 2007 as in the previous 20 years altogether.”

The 14 zero-day vulnerabilities in 2010 were found in widely used applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player. Industrial Control System software was also exploited. In a sign of its sophistication, Stuxnet alone used four different zero-days.

Source: Symantec ITR

The Year in Numbers
Some of the more noteworthy statistics that represent the security landscape in 2010

286M+ Threats
Polymorphism and new delivery mechanisms such as Web-attack toolkits continued to drive up the number of malware variants in common circulation. In 2010, Symantec encountered more than 286 million unique variants of malware.

Source: Symantec ITR
Compliance & Auditability

Question:
Is corporate auditing the OT for compliance with corporate standards? Must you adhere to external compliance requirements, such as NERC CIP, CFATS, NIST, ISA-99, IEC-ISO, WIB etc.?
Compliance with international standards?

- ISA-99, NERC CIP, ISO 27000, NIST 800-82
  ChemITC, IEC 62443-3…

- Catalog of Control System Security


- Security should be a program and not a project
Change Management

Question:
Will you add new hardware or make software upgrades to your automation environment over the next 3-5 years?

More than 50% of ICS professionals expect industrial intelligent endpoints to double over this period, according to a 2011 survey.

How will you manage change across a growing, heterogeneous complex automation environment
I have a firewall so my control system is secure right?

- Firewalls don’t provide protection against:
  - Engineers using USB drives for projects
  - Websites that have been compromised
  - Modem ports and wireless access points
  - Unpatched operating systems
  - Social engineering attacks

![Diagram showing firewall configuration and internet security](image-url)
How would you know if your system was infected?
Do you have more than one control system to worry about?

*Some vendors may supply security solutions for only their system*
Are you keeping up with security technology?

Where is your company?

Technology Sophistication

Firewalls
- Business connectivity
- Network-based
- Host-based
- Known bad
- Industrial Protocols

Locks on the Door

Intrusion Detection
- Network-based
- Host-based
- Known bad
- Industrial Protocols
- Monitor and respond
- Alert on events of interest
- Log everything and apply forensics
- Incident Management

Alarm Sensors

Event Monitoring
- Central Logging
- Monitor and respond
- Alert on events of interest
- Log everything and apply forensics
- Incident Management

Flight recorder

Intrusion Prevention
- Network-based
- Host-based
- Deep packet inspection
- Known bad signatures
- Known Good Signatures
- Whitelisting
- System hardening

System locked down

Automation Systems Management
- Automates manual processes
- Enforces policy, process & procedures
- Leverages system baselines
- Manages changes
- Audit reporting
- Continuous assessments
- Attestation data

Doing it and proving you are doing it

2003
2005
2007
2010
2012
How many tools are you using today?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Ticketing</td>
<td>Patch Monitoring</td>
<td>GIS</td>
<td>Documentation</td>
<td>Email/Web Events</td>
<td>User Base Lines</td>
<td>Network Visualization</td>
<td>Operational Algorithms</td>
</tr>
<tr>
<td>Source Code</td>
<td>Patch Base line</td>
<td>Maintenance</td>
<td>Tasks</td>
<td>DPI</td>
<td>User Activity</td>
<td>Config Backups</td>
<td>Configuration Backups</td>
</tr>
<tr>
<td>Development</td>
<td>Patch Exception</td>
<td>Work Orders</td>
<td></td>
<td>Root Cause Analysis</td>
<td>Reporting</td>
<td>Event Correlation</td>
<td>Security logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Change monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Configuration Backups</td>
</tr>
</tbody>
</table>

**Functions address by Industrial Defender - ASM**

- Change Management: Change Initiation, Pre-Post change, Config/Policy Exceptions, Change Documentation
- Patch Management: Patch Monitoring, Patch Base line, Patch Exception
- Asset Management: Device inventory, Logic Rules, Event Correlation
- Ticketing Management: Documentation, Tasks, Ticketing workflows, Ticketing approvals
- Event Management: ICS Collectors, Logic Rules, Event Correlation
- User Management: User Base Lines, User Activity, Reporting
- Network Management: Config Backups, Event Correlation
- PCS Configuration Management: Security logging, Change monitoring, Configuration Backups

**Tools and Logos**

- BMC Software
- IBM
- Lumension
- Oracle
- Crossbow
- ABB
- SolarWinds
- IBM Maximo
- ArcSight
- NitroSecurity

**Date:** 1/16/2013
Why “IT” enterprise security tools can be dangerous...

Maybe you have “Defense-in-Depth”…

- Firewall (UTM)
- NIDS
- HIDS
- HIPS
- Patch Mgmt
- Reporting
- Monitoring

Network Intrusion Detection

Host Intrusion Detection
Host Intrusion Prevention
Active Patch Management

Business Network

24x7 Monitoring

Security Event Manager
Top challenges for automation system owners

- **Reviewing patch information and patching systems/devices**
  - Many vendors, devices and formats – manual effort
- **Change Management**
  - Configuration tracking & asset inventory at device level (IED, RTU, PLC)
- **Collection of information like “ports and services”**
  - Manual effort, very time consuming
- **Disaster Recovery**
  - Backup and archiving system images, firmware, configurations
- **User access and accounts across all system assets**
  - Who has access to what, proof of decommissioning, substation assets
- **Managing multiple security technologies**
  - Firewalls, IPS/IDS, SIEM, AV, Whitelisting
- **Generating evidence for corporate & government auditors**
  - Documentation and reporting are time consuming
Who is Industrial Defender?
Exclusively focused on Operations Technology

- Security & Compliance since 2002
- Leadership team with extensive industry experience
- FORTUNE 100 endorsed
- Pioneering solutions for automation systems management in 2012 and beyond

Pike Research ranks Industrial Defender #1
Addressing the Challenges in Automation Systems Management

- Automation Systems becoming more complex
  - Mix of legacy and next generation architectures
  - Heterogeneous Systems
  - Exponential Increase in intelligent devices
  - Unclear responsibility/ownership

- Need for increased security

- Increasing compliance requirements

- Managing change introduces additional business process requirements and labor allocation

- Fewer Resources / increasing skill set gaps

- Downward Budgetary Pressure

Managing Diverse Requirements of Automation Systems Environments

The convergence of:

- Security
- Compliance
- Change Management

Balancing Operational Requirements with Security, Compliance, Change Management requirements
Automation Systems Management Architecture

Applications Software

Infrastructure

Automation Systems Manager

Software Applications

Asset Mgmt.  Event Mgmt.  Configuration Change Mgmt.  Policy Mgmt.  Reporting  End Point Security

ASM Hardware

Advanced Services Appliances

Automatic Systems End-Points

Optional Agent

Industrial Defender®
Advanced Services Appliance (ASA)

- Data collection appliance
  - Security / Operational events
  - Device configuration data
- Store-and-forward capabilities
- Data encryption
- Noise filtering capabilities
- Powerful event correlation capabilities
- Custom alert generation
- Signature distribution point (NIDS)
Agents - Data Collection

<table>
<thead>
<tr>
<th>System Logging</th>
<th>Application Logging</th>
<th>Health / Performance monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>System log entries</td>
<td>Application Log messages</td>
<td>Agent status</td>
</tr>
<tr>
<td>System errors /warnings</td>
<td></td>
<td>System uptime</td>
</tr>
<tr>
<td>Valid/invalid System logins</td>
<td></td>
<td>Usage: CPU, disk, memory</td>
</tr>
<tr>
<td>Firewall log entries</td>
<td></td>
<td>Traffic: Incoming/outgoing</td>
</tr>
<tr>
<td>Valid/invalid Perimeter logins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall exception packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS packet anomalies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS traffic flow anomalies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General syslog / traps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| System Configuration                                |                      |                              |
| Hardware                                            |                      |                              |
| Interfaces                                          |                      |                              |
| System events monitor                               |                      |                              |
| Processes: unexpected starts/stops                  |                      |                              |
| Sockets: unexpected connect/disconnections           |                      |                              |
| Registry: Unexpected modifications                  |                      |                              |
| Files/programs: Unexpected modifications            |                      |                              |

| System Settings                                     | Whitelist Monitoring | Whitelist Management         |
| System Logging policies                             | Unauthorized executable attempt | Whitelist inventory |
| System Password policies                            | Whitelist change activity    | Trusted change policy settings|
| Firewall rules                                      |                          |                              |
| Ports & Services allowed/used                       |                          |                              |

| Software / Patches                                  | Local accounts          |                              |
| Software inventory /dates                           | Account ID              |                              |
| Patches installed /dates                             | Account type, age        |                              |
“Control system security is a critically important issue for our customers; this additional capability enhances 800xA’s strong system security foundation. Industrial Defender’s ASM Monitor solution provides expanded situational awareness with security event monitoring centrally across all plant systems and assets that will give our customers even more security protection for their system.”

Tobias Becker, head of ABB’s Control Technologies business
800xA Architecture
## Automation System Manager Functions

- Event logging, correlation, and archiving
- Single unified view across disparate endpoint base
- Customizable User Interface Dashboards
- Scalable Architecture
- File Integrity
- Network traffic monitoring
- Critical process & service monitoring
- Report subscriptions
- User account change identification
- Device configuration file archiving
- Network & system health and performance
- Maintain central configuration policy
- Collect & report on settings, accounts, configurations
- Analyze changes across asset base & environment
- Manage hardened electronic security perimeter
- Configuration change management
- Enforce host level application policies
- Prevent rogue applications/malware
- Block unauthorized applications
- Enforce trusted change policies

### Monitor
- ▲
- ▲
- ▲

### Manage
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲

### Protect
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
- ▲
Application Whitelisting

- **Control**: Lockdown control system to stop unapproved applications from executing
  - While some applications may not be malicious, they impact productivity and may not be approved for use (i.e. Solitaire, Pinball, Chat Utilities, etc.)

- **Flexibility**: Flexible deployment options available
  - Ability to deploy using existing AD infrastructure
  - Ability to deploy in ‘learning’ mode

- **Protection**: Systems can finally be hardened against viruses and malware, both known and unknown
  - Malware can compromise system availability and performance
  - Prevents zero-day threats such as Stuxnet and Duqu from executing
  - Likely going to see an increase in zero-day malware targeting critical control systems; Stuxnet was just the beginning
Situational Awareness
Automation Systems Management: Turnkey Solution

**SUSTAIN SERVICES**
- Firmware/Patch Updates
- Performance/Alert Tuning
- Rebaselining Software, Patches, Ports & Services

**SUPERVISE SERVICES**
- Event Monitoring
- Configuration Baseline Monitoring
- Whitelisting
- Move, Add, Change Management

**SURVIVE SERVICES**
- Backup
- Restoration
- Disaster Recovery

---

**Automation Systems Manager (ASM)**

**Application Capabilities**

- Asset Mgmt.
- Event Mgmt.
- Configuration Change Mgmt.
- Policy Management
- Reporting
- End Point Security

---

**Automation Systems End-Points**

- Server
- HMI Station
- Work Station
- Client
- Firewall
- PLC
- Device
- IED
- Sensors
- Controllers
- Optional Agent

---

**Industrials Defender**

1/16/2013 27
Experience across many automation environments

- **Security performance monitoring**
  - ABB 800xA, Symphony/Harmony, Infi90, Network Manager, FACTS, SYS600C and MicroSCADA
  - Automsoft RAPID Historian
  - Emerson DeltaV and Emerson Ovation
  - Emerson/Westinghouse WDPF
  - GE XA/21
  - GE PowerOn Fusion
  - Foxboro I/A Series
  - Honeywell Experion
  - Itron OpenWay System
  - Rockwell RSView
  - Schneider/Telvent Oasys, Citect Momentum, Quantum
  - Siemens PCS7
  - Yokogawa Centrum CS 3000

- **Operating systems**
  - Windows 7
  - Win 2k, 2k3, 2k8 R2, XP, WinNT
  - HP-UX PA-RISC & Itanium
  - Linux
  - DEC Tru-64
  - Sun Solaris
  - IBM AIX

- **Industrial rules**
  - DNP3
  - Modbus
  - ICCP
  - IEC 61850
  - TCP/IP
Summary

- **Sustainability** of your automation environment: It’s a program, not a project!
- **Increasing challenges** in Security, Compliance and Change Management will further tax resources
- Enabling IT and OT to work together
- Unified approach to challenges will **reduce overall TCO**
- **Turnkey solutions** that evolves with your needs, providing scalability and flexibility as your business needs evolve and technology changes
- Consider service partners that allow you to **focus** on your primary objectives

**Industrial Defender:**
*Your Solution for Automation Systems Management*