January 2017 David Macy

Sensible Cyber Security

Deploying Baseline Controls

Sensible Cyber Security

Speaker name:	David Macy
Speaker title:	Cyber Security Manager BU Service

The Threat Landscape

- We have always seen the biggest cyber threat to be accidental infection through removable media.

- That may still be true, but the world continues to get more dangerous.

- That doesn’t mean, we can’t make ourselves very difficult targets.

The New Threat Landscape

- On December 23, 2015, around half the homes in the Ivano-Frankivsk region of Ukraine were left without electricity for a few hours due to a targeted attack using BlackEnergy malware
- The malware was deployed using spear-phishing with a spoofed sender address and Microsoft Office docs with macro code.
- This attack is likely state sponsored.

The New Threat Landscape

- In 2014 a malicious actor infiltrated a German steel facility.
- The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network.
- The adversary showed knowledge in ICS and was able to cause multiple components of the system to fail.
- This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.

The New Threat Landscape

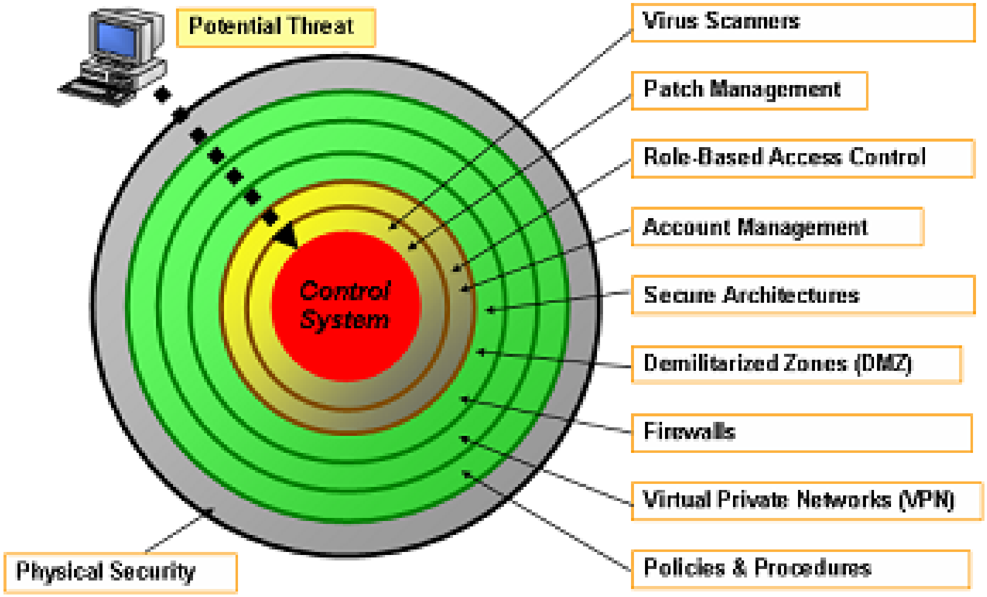
- A municipal water utility in the US had their control system on the corporate network against the vendor's advice.
- They were hit with ransomware and had to pay to regain access to their system.
- They have since revised their architecture as well as other practices.

Common factors with these three events

- Path to control system started from the internet through the corporate network
- Did not compromise a remote access mechanism
- Originated with human engineering – spear phishing
- Involved complex sequence of network exploration, vulnerability identification, privilege escalation, and further movement in the system which takes a lot of time
- Involved sophisticated ICS knowledge in two out of the three attacks

What can you do with your systems to fight the threat?
The Baseline Controls:

- Inventory of all assets
- Zone based architecture
- Perimeter Defense
- Hardening
- Patch Management / Antivirus / Whitelisting
- Software Backups
- Monitoring
  - Events
  - Changes to hardening profiles
- Training of system users



Regulatory and Standards for Guidance

- ABB bases our recommendations and service offerings on internationally recognized principles and best practices.
- Regulations are the key element driving some market segments and help define our programs. Examples:
  - NERC CIP
  - CFAT
  - OLF Guideline 104
- Existing and emerging standards help define what steps are taken. Examples:
  - IEC62443 / ISA99
  - ISO 27002
  - NIST 800-53

ISA-62443-2-1-2009 – 126 Req.

Cybersecurity Framework – 99 Categories
SP800-53r4 – 256 Req., 666 Req. Enhancements

ISO/IEC 27001 – 140 Req.
ISO/IEC 27002 – 114 Req.

(Example references are shown in many slides in this presentation.)

Two Important Principles Common to Most Standards

- Principle of Least Privilege
  - No user should have more rights and permissions than needed to perform his function in the system

  References: NIST 800-53 AC-6, NERC CIP 7, IEC62443-3-3 Paragraph 4.4

- Principle of Least Function
  - Only the functions needed for the system to accomplish its purpose should be present or enabled in the system

  References: NIST 800-53 CM-6, NERC CIP 7 R2, IEC62443-3-3 SR 7.7

Security Policies to Document What You Do

- Policies define the Cyber Security program
- Some policies may cover details of security implementation such as password complexity and length
- Some policies are administrative such as who can make changes to the user database or what to do if an administrator leaves the company
- If there are no policies, security implementation will lack strategic focus and will be ineffective
- Policy primer, templates, and many other resources can be found at the SANS Policy Project:

http://www.sans.org/security-resources/policies/

Reference: NIST 800-53 MA-1

Inventory All Assets

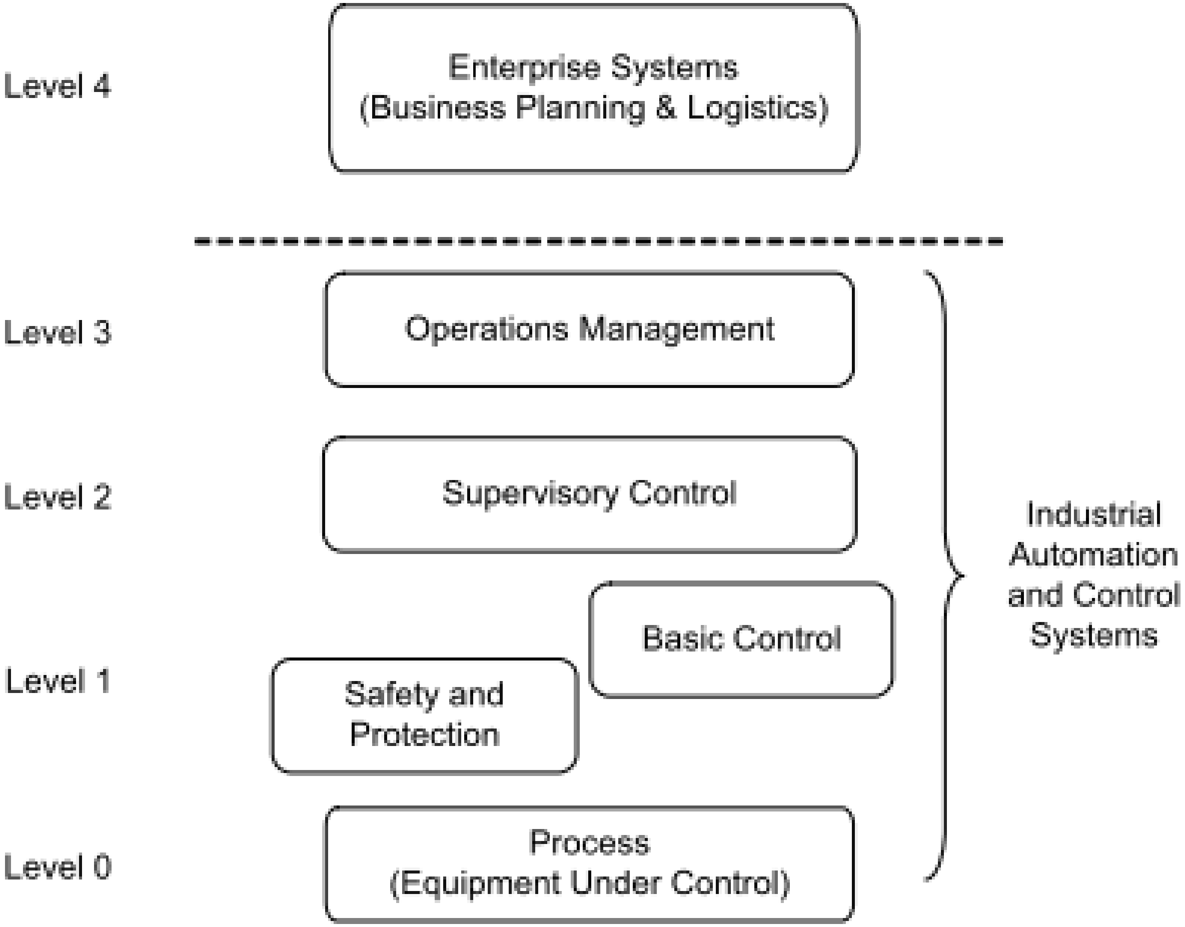
This is critical to be sure you know what nodes to manage with hardening and patch management, etc. and to make sure there are no rogue nodes.

- Physical inventory
- Ping, NetBIOS, and other sweeps (NMAP or other tools)
- Wireless sweeps
- For monitoring long term, NIDS
- Lock down ports on switches
- Secure any wireless with access restrictions and encryption

References: NIST 800-53 CM-8, NERC CIP 2 R2/3, IEC62443-3-3 SR 7.8

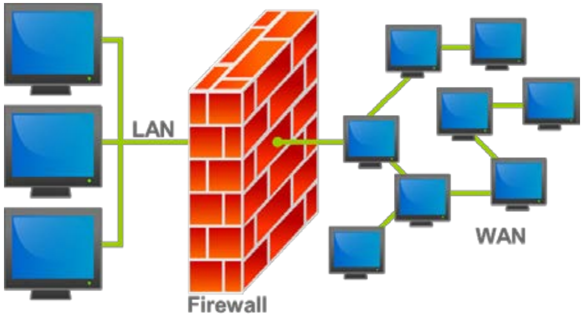
Zone Model in ICS Networks

ISA-99.03.02



Perimeter Defense

- Make sure perimeters are really perimeters:
  - Someone plugging in phone to USB
  - A direct control system connection bypassing the firewall for a historian
  - An inadvertent connection between networks
- No default settings left in place such as admin password, non secure shell, etc.
- Default deny rule
- Secure outgoing as well as incoming connections
- The more granular the rules, the better: IP address, port, protocol
- No DCOM through firewalls
- Best using DMZ with different vendor firewalls on each side
- No traffic between non adjacent zones



Hardening of Assets

Least Function:

- Ports and Services
- Removable Media
- BIOS password and restricted boot order
- Scanning methodology for removable media if used

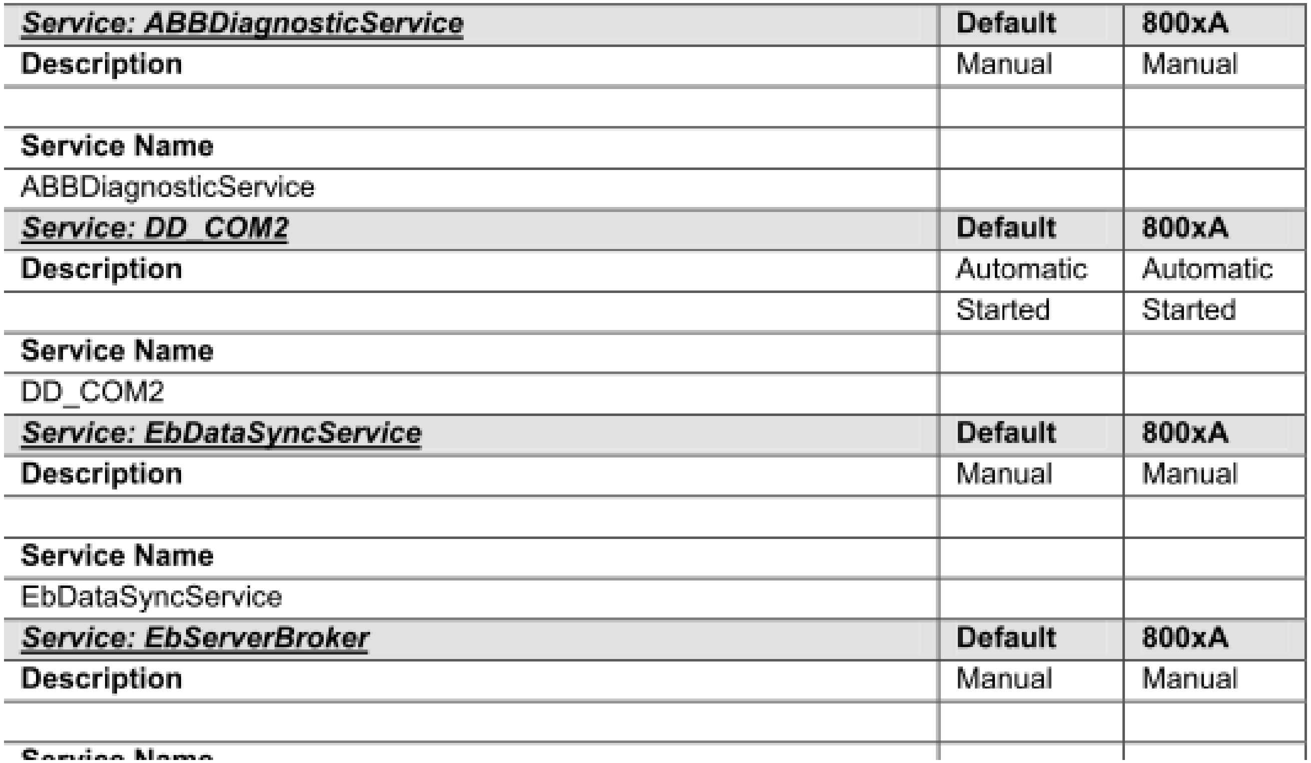
Least Privilege:

- Account Management
- Group Policies for desktop lockdown and other restrictions
- Physical restriction of access to computers

References: NIST 800-53 CM-7, NERC CIP 7 R2, IEC62443-3-3 SR 7.7

Hardening Services and Ports

- A very important step for securing computers is to eliminate unneeded services and network ports
- Services and ports are audited to record their current state and are compared to the ABB required services documentation
- Any required third party services are reviewed
- All others are disabled or uninstalled



Service: ABBDiagnosticService	**Default**	**800xA**
Description	Manual	Manual
Service Name		
ABBDiagnosticService		
Service: DD_COM2	**Default**	**800xA**
Description	Automatic	Automatic
	Started	Started
Service Name		
DD_COM2		
Service: EbDataSyncService	**Default**	**800xA**
Description	Manual	Manual
Service Name		
EbDataSyncService		
Service: EbServerBroker	**Default**	**800xA**
Description	Manual	Manual
Service Name		

Account Management and Policy Implementation

User Roles, Access Control and Workstation Hardening

- Establish hierarchy of User Accounts (operator, tech, admin, etc) with least privileges needed for job
- Policy to restrict use of administrative accounts to administrative tasks
- Domain wide policy to enforce:
  - Password Requirements and Role Association
  - Define Remote Access Security
- Operator Group Policy that restricts access to Desktop and Applications

References: NIST 800-53 CM-6, NERC CIP 7 R5, IEC62443-3-3 FR 2

Removable Media Protection

- Group policies in Windows can restrict use while computer is booted into Windows
- Must be coupled with boot restrictions and BIOS restrictions
- Must also be coupled with appliances and practices and policies regarding scanning of media, preferably with multiple anti-malware scanners
- Third party products provide additional options such as signatures limiting which removable media can be used
- Many companies are abandoning the use altogether and using file sanitizers in the DMZ with network access for transfer to and from control network

References: NIST 800-53 CM-6

NERC CIP 7 R1,

IEC62443-3-3 SR 2.3

Patch Management and Anti-Virus

Rated by DHS and SANS as the most effective of all controls

- Once inside a network, all further exploits and privilege escalation rely on unpatched vulnerabilities
- Malware relies on unpatched vulnerabilities to spread

Management is the key word

- This needs to be done very regularly
- Without a defined process, it is impossible to keep up
- Even with a process, it is difficult and time consuming without automation tools
- The good news is that automation tools exist that allow for easy management and documentation

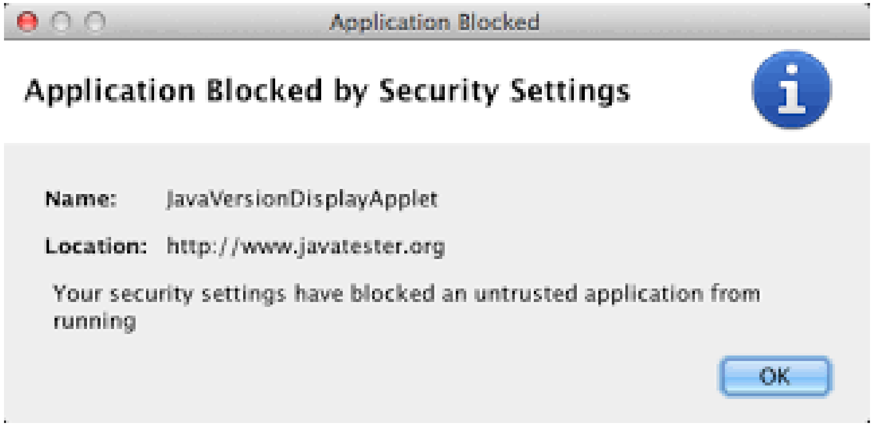
References: NIST 800-53 CM-6, NERC CIP 7 R2, IEC62443-3-3 SR 7.7

Windows Server Update Services

McAfee An Intel Company

Application Whitelisting

- Configures what is allowed to run versus what is not allowed to run
- Good supplement to patch management and anti-virus. Allows for more relaxed schedule of applying updates
- Not foolproof, there are exploits to bypass it
- There are products approved for 800xA and Symphony Plus



Application Blocked by Security Settings

Name: JavaVersionDisplayApplet

Location: http://www.javatester.org

Your security settings have blocked an untrusted application from running

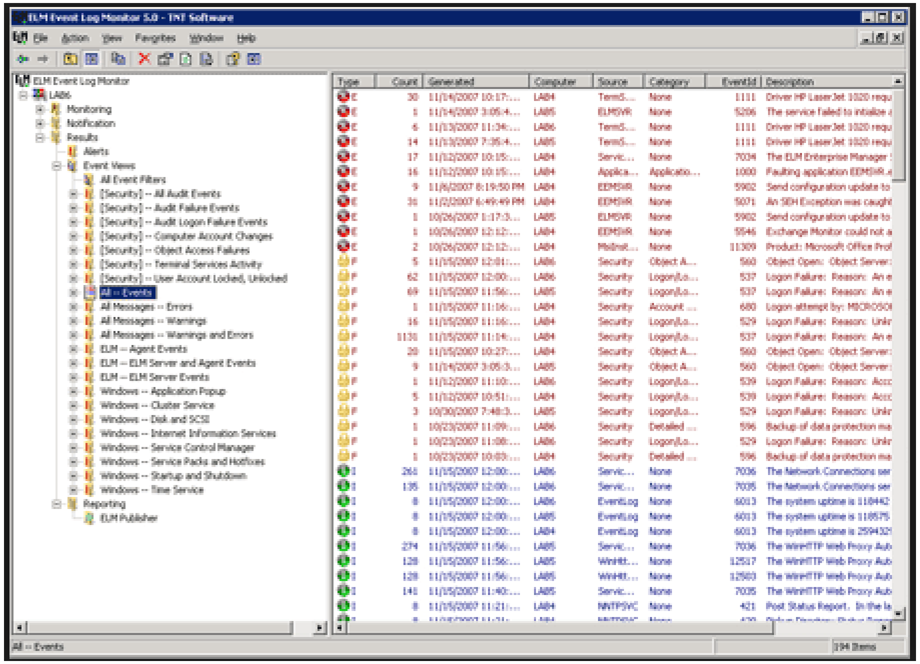
Software Backup System Purposes

- Safeguard the data and configuration of the system against loss
  - Hardware failure
  - Mistake by operation or engineering personnel
  - Corruption due to malware
- Enable rapid recovery from a computer device failure
- Maintain the data needed in the process of an upgrade of the applications
- Verify system recovery data is valid
- Meet regulatory requirements such as NERC CIP regulations regarding disaster recovery

References: NIST 800-53 CP-9/10, NERC CIP 9, IEC62443-3-3 SR 7.3

Configuration Change Management and Security Event Logging

- 800xA or Symphony Plus audit trail logs specified events and includes time stamp when changes were made, which changes were made, on which node the changes were made and who made the changes.
- Windows Security Event Log Configuration
- Installation of a central security event log server for automating collection, analysis, and reporting makes for easier management
- Some products can provide integration with NIDS, HIDS, Whitelisting, and network devices using syslogs and can provide alarm and analysis functions
- Some products can monitor for changes such as a TCP port state changing on a computer or patches out of date



- ELM Event Log Monitor
  - LAB6
    - Monitoring
    - Notification
    - Results
      - Alerts
      - Event Views
        - All Event Filters
        - [Security] -- All Audit Events
        - [Security] -- Audit Failure Events
        - [Security] -- Audit Logon Failure Events
        - [Security] -- Computer Account Changes
        - [Security] -- Object Access Failures
        - [Security] -- Terminal Services Activity
        - [Security] -- User Account Locked, Unlocked
        - All -- Events
        - All Messages -- Errors
        - All Messages -- Warnings
        - All Messages -- Warnings and Errors
        - ELM -- Agent Events
        - ELM -- ELM Server and Agent Events
        - ELM -- ELM Server Events
        - Windows -- Application Popup
        - Windows -- Cluster Service
        - Windows -- Disk and SCSI
        - Windows -- Internet Information Services
        - Windows -- Service Control Manager
        - Windows -- Service Packs and Hotfixes
        - Windows -- Startup and Shutdown
        - Windows -- Time Service
    - Reporting
      - ELM Publisher

Type	Count	Generated	Computer	Source	Category	EventId	Description
E	30	11/14/2007 10:17:...	LAB4	TermS...	None	1111	Driver HP LaserJet 1020 requ
E	1	11/14/2007 3:05:4...	LAB5	ELMSVR	None	5206	The service failed to intialize a
E	6	11/13/2007 11:34:...	LAB6	TermS...	None	1111	Driver HP LaserJet 1020 requ
E	14	11/13/2007 7:35:4...	LAB5	TermS...	None	1111	Driver HP LaserJet 1020 requ
E	17	11/12/2007 10:15:...	LAB4	Servic...	None	7034	The ELM Enterprise Manager :
E	16	11/12/2007 10:15:...	LAB4	Applica...	Applicatio...	1000	Faulting application EEMSVR.e
E	9	11/6/2007 8:19:50 PM	LAB4	EEMSVR	None	5902	Send configuration update to
E	31	11/2/2007 6:49:49 PM	LAB4	EEMSVR	None	5071	An SEH Exception was caught
E	1	10/26/2007 1:17:3...	LAB5	ELMSVR	None	5902	Send configuration update to
E	1	10/26/2007 12:12:...	LAB4	EEMSVR	None	5546	Exchange Monitor could not a
E	2	10/26/2007 12:12:...	LAB4	MsiInst...	None	11309	Product: Microsoft Office Prof
F	5	11/15/2007 12:01:...	LAB6	Security	Object A...	560	Object Open: Object Server:
F	62	11/15/2007 12:00:...	LAB6	Security	Logon/Lo...	537	Logon Failure: Reason: An e
F	69	11/15/2007 11:56:...	LAB5	Security	Logon/Lo...	537	Logon Failure: Reason: An e
F	1	11/15/2007 11:16:...	LAB4	Security	Account ...	680	Logon attempt by: MICROSOI
F	16	11/15/2007 11:16:...	LAB4	Security	Logon/Lo...	529	Logon Failure: Reason: Unk
F	1131	11/15/2007 11:14:...	LAB4	Security	Logon/Lo...	537	Logon Failure: Reason: An e
F	20	11/15/2007 10:27:...	LAB4	Security	Object A...	560	Object Open: Object Server:
F	9	11/14/2007 3:05:3...	LAB5	Security	Object A...	560	Object Open: Object Server:
F	1	11/12/2007 11:10:...	LAB6	Security	Logon/Lo...	539	Logon Failure: Reason: Acc
F	5	11/12/2007 10:51:...	LAB4	Security	Logon/Lo...	539	Logon Failure: Reason: Acc
F	3	10/30/2007 7:48:3...	LAB5	Security	Logon/Lo...	529	Logon Failure: Reason: Unk
F	1	10/23/2007 11:09:...	LAB6	Security	Detailed ...	596	Backup of data protection ma
F	1	10/23/2007 11:08:...	LAB6	Security	Logon/Lo...	529	Logon Failure: Reason: Unk
F	1	10/23/2007 10:03:...	LAB4	Security	Detailed ...	596	Backup of data protection ma
I	261	11/15/2007 12:00:...	LAB6	Servic...	None	7036	The Network Connections ser
I	135	11/15/2007 12:00:...	LAB6	Servic...	None	7035	The Network Connections ser
I	8	11/15/2007 12:00:...	LAB6	EventLog	None	6013	The system uptime is 118442
I	8	11/15/2007 12:00:...	LAB5	EventLog	None	6013	The system uptime is 118575
I	8	11/15/2007 12:00:...	LAB4	EventLog	None	6013	The system uptime is 2594321
I	274	11/15/2007 11:56:...	LAB5	Servic...	None	7036	The WinHTTP Web Proxy Aut
I	128	11/15/2007 11:56:...	LAB5	WinHtt...	None	12517	The WinHTTP Web Proxy Aut
I	128	11/15/2007 11:56:...	LAB5	WinHtt...	None	12503	The WinHTTP Web Proxy Aut
I	141	11/15/2007 11:40:...	LAB5	Servic...	None	7035	The WinHTTP Web Proxy Aut
I	8	11/15/2007 11:21:...	LAB4	NNTPSVC	None	421	Post Status Report. In the la

All -- Events

194 Items

References: NIST 800-53 AU-1-16, NERC CIP 7 R4, IEC62443-3-3 FR 6

Training

- Awareness training for all – this is needed for purposes of reducing human engineering issues such as phishing
- Training for all regarding the company's security policies such as removable media handling
- Technical training for those performing cyber tasks such as hardening, patch management, and software backups
- Training for responding to event or condition monitoring
- Much of this is required by inspectors for regulatory agencies such as NERC

References:
NIST 800-53 AT-1 through AT-5
NERC CIP 4

On-going compliance measures required

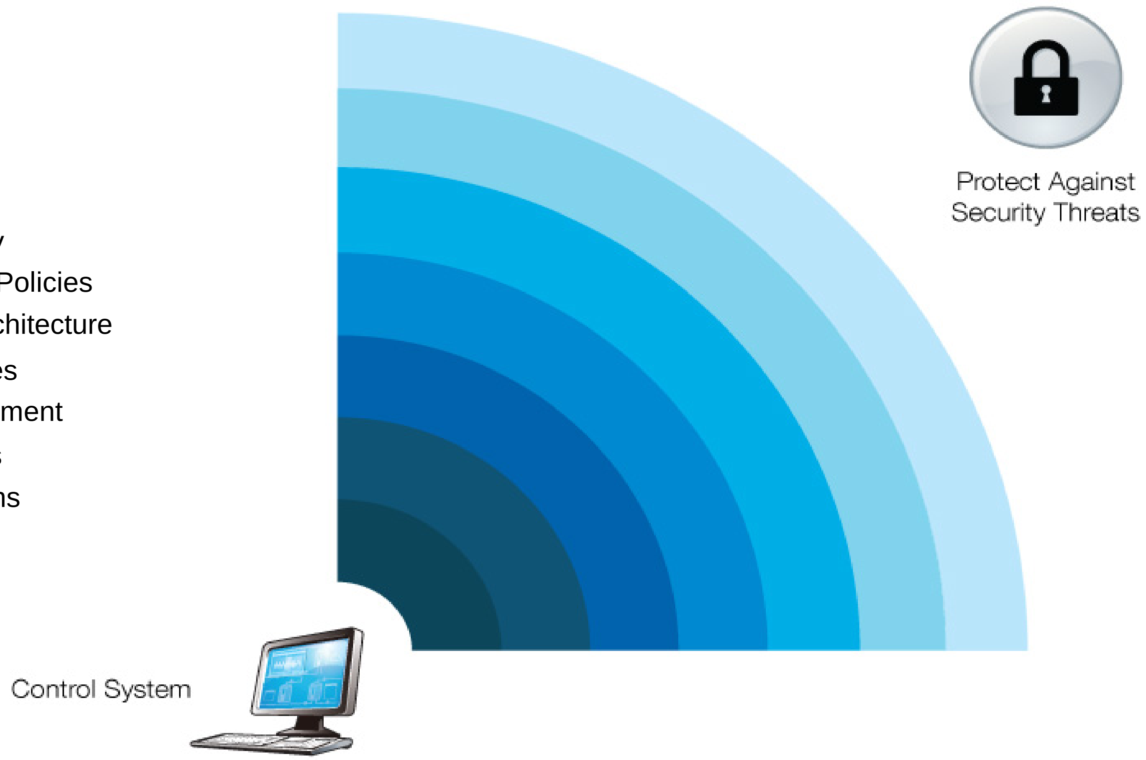
- The system is likely to fall out of compliance over time, as a result of:
  - Intentional or unintentional changes
  - Replacements of PCs
  - Software reloads, upgrades, etc.
  - New threats
- Periodic audits or continuous monitoring to ensure correct settings
- Training of new or periodic retraining of existing personnel
- Discussions with the plant personnel responsible for the system to make sure the security steps are compatible with their use of the system

How ABB Can Help with Security Management

- Cyber Security Fingerprint and remediation of deficiencies
- Software Update Services
- Software Backup services
- Service Port Cyber Channel
- Security Workplace
- Secure Remote Access
- Training

Cyber Security Fingerprint
Security in depth

- 🟦 Physical Security
- 🟦 Procedures and Policies
- 🟦 Firewalls and Architecture
- 🟦 Computer Policies
- 🟦 Account Management
- 🟦 Security Updates
- 🟦 Antivirus Solutions



Security Update Service

Automated and Controlled

1. Microsoft Patch monthly deployment

Windows Server Update Services

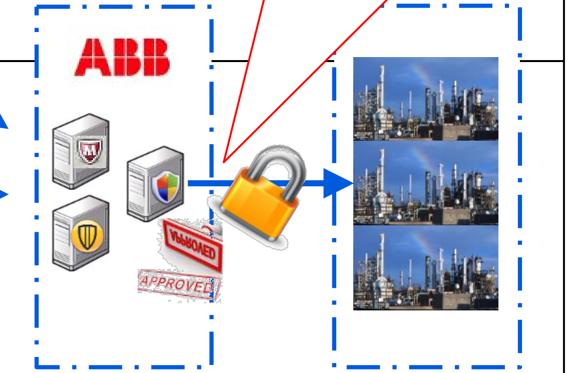
WSUS (Server)

2. Antivirus McAfee daily pattern updates

McAfee An Intel Company

ePo (ePolicy Orchestrator) Server

Security Update Service for the automated distribution and deployment of ABB validated Cyber Security updates using highly secured methodology



Software Backup Services Essential Features

- Hard drive imaging to a central server for rapid recovery
- Configuration backups in addition to imaging
- Scheduling and scripting to automate the update of images
- Tested bandwidth and CPU utilization to avoid performance problems
- Full domain integration
- Backup image testing
- Restoration training for technicians who will have to recover in the middle of the night

Cyber Security Monitoring Service

- **Application**
- ABB or third-party control systems
- **Scope (**provided through ServicePort**)**
- On-site installation, commissioning, and customer training (first year only)
- Automatic data collection and KPI generation for
  - Procedures and Protocols
  - Security Policies
  - Computer Settings
- Twice-a-year assessment by ABB experts
- Presentation and evaluation of report
- Available 24/7 for customer use in daily operations
- Optional: remote on-demand support

Security Workplace
Package overview

Security Workplace

MAINTAIN

- **Centralized Microsoft Patching***
- Centralized Antivirus Management
- Centralized, Automated Backup and Recovery

COMPLY

- Security Event Monitoring
- Configuration Change Management
- ICS Asset Management
- Automated Compliance Reporting
- Policy Management
- Workflow Automation Suite

DEFEND OPTIONS

- **File Sanitizer (ODI-X)***
- Intelligent Whitelisting
- Network Segmentation and DMZ Implementation

* Indicates product is in managed release

Training Available from ABB University

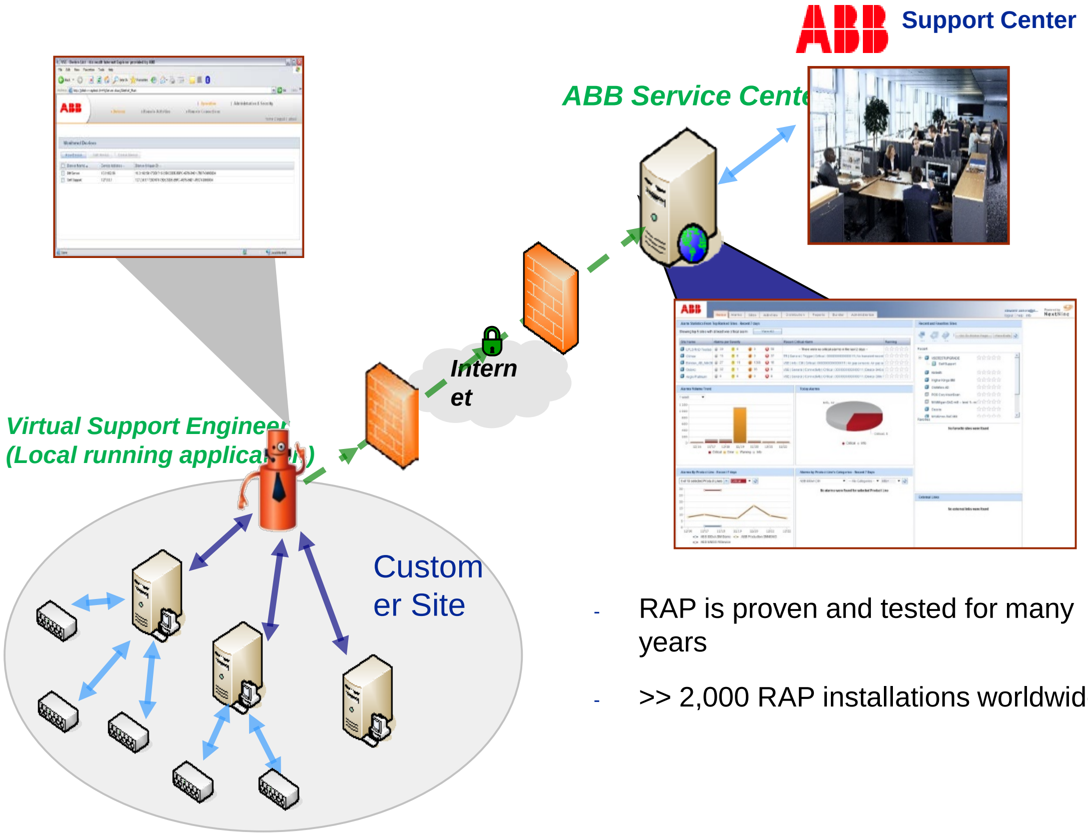
US925 course covers:

  - Patch Management
  - Antivirus
  - Software Backup Systems

- US926 course covers:
  - Standards, policies, basic principles, and best practices
  - Network architecture
  - Hacking / penetration testing tools
  - Audits and assessments
  - Hardening
  - IPSec and whitelisting
  - Event monitoring

Secure Remote Access

- Connection to Corporate Network via Router w/ Firewall or DMZ.
- Allows for Remote Diagnostics for Control System support
- Can Support WSUS (Windows Update) and Anti Virus Updates
- Allows for Remote Operator and Engineering Clients
    - Secured as Read-Only
    - Configured for off-site Operation and Maintenance



- RAP is proven and tested for many years
- >> 2,000 RAP installations worldwide

Power and productivity
for a better world™

ABB