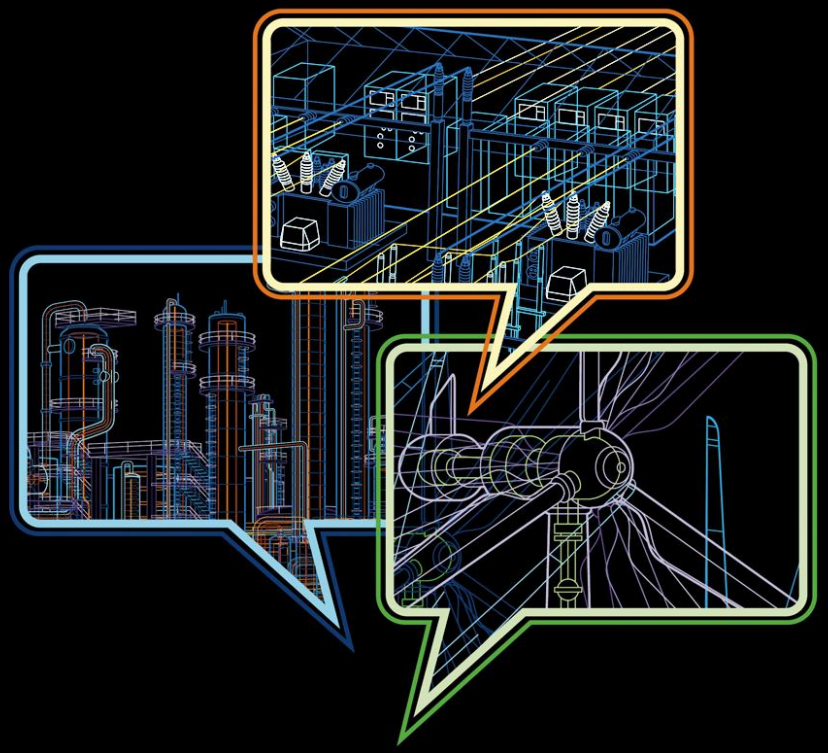


ABB Automation & Power World: April 18-21, 2011

CSE-101-1 Leveraging the Industrial Defender ABB Partnership to Secure your Control System – Case Studies

WCS-120-1 Leveraging the Industrial Defender ABB Partnership to secure your control system

- **Speaker** Jim Crowley
- Speaker title: Director NA Sales, Energy Mgmt
- Company name: Industrial Defender
- Location: Foxborough, MA

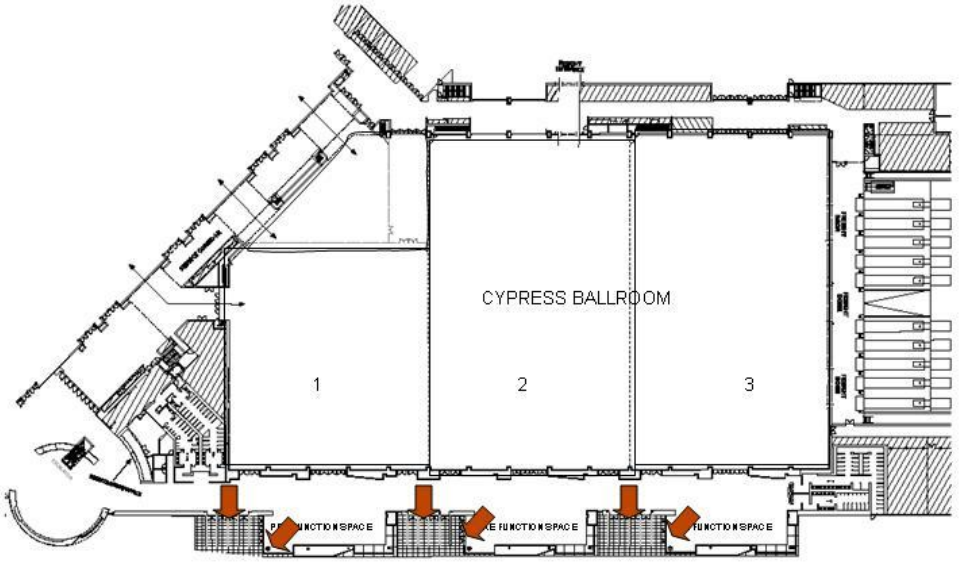
Co-presenter

- Speaker name: John Fridye
- Speaker title: Cyber Security Engineer
- Company name: ABB - Ventyx
- Location: Sugarland, TX

Your safety is important to us
Please be aware of these emergency procedures

- In the event of an emergency please dial ext. 55555 from any house phone. Do not dial 9-1-1.
- In the event of an alarm, please proceed carefully to the nearest exit. Emergency exits are clearly marked throughout the hotel and convention center.
- Use the stairwells to evacuate the building and do not attempt to use the elevators.
- Hotel associates will be located throughout the public space to assist in directing guests toward the closest exit.
- Any guest requiring assistance during an evacuation should dial “0” from any house phone and notify the operator of their location.
- Do not re-enter the building until advised by hotel personnel or an “all clear” announcement is made.

Your safety is important to us
Convention Center exits in case of an emergency



Know your surroundings:

- Identify the meeting room your workshop is being held in
- Locate the nearest exit

AGENDA

- About Industrial Defender
- Profile of our customers using ABB technology
- Case Study – East Coast EMS and Power Generation Compliance Deployment
- Case Study – Western State EMS and Power Generation Security Deployment
- ABB System Security complemented with Industrial Defender Security and Automation

About Industrial Defender

- Exclusive focus on providing an integrated set of products and services for Automation Systems Security & Compliance Management
- Unify three challenging domains:
  - Automation Systems
  - Cyber security
  - Compliance
- Privately held company headquartered in Foxborough, MA
- 8 year focus on Automation Systems Security & Compliance Management
- 350 customers worldwide, 10,000 product deployments, 21 countries

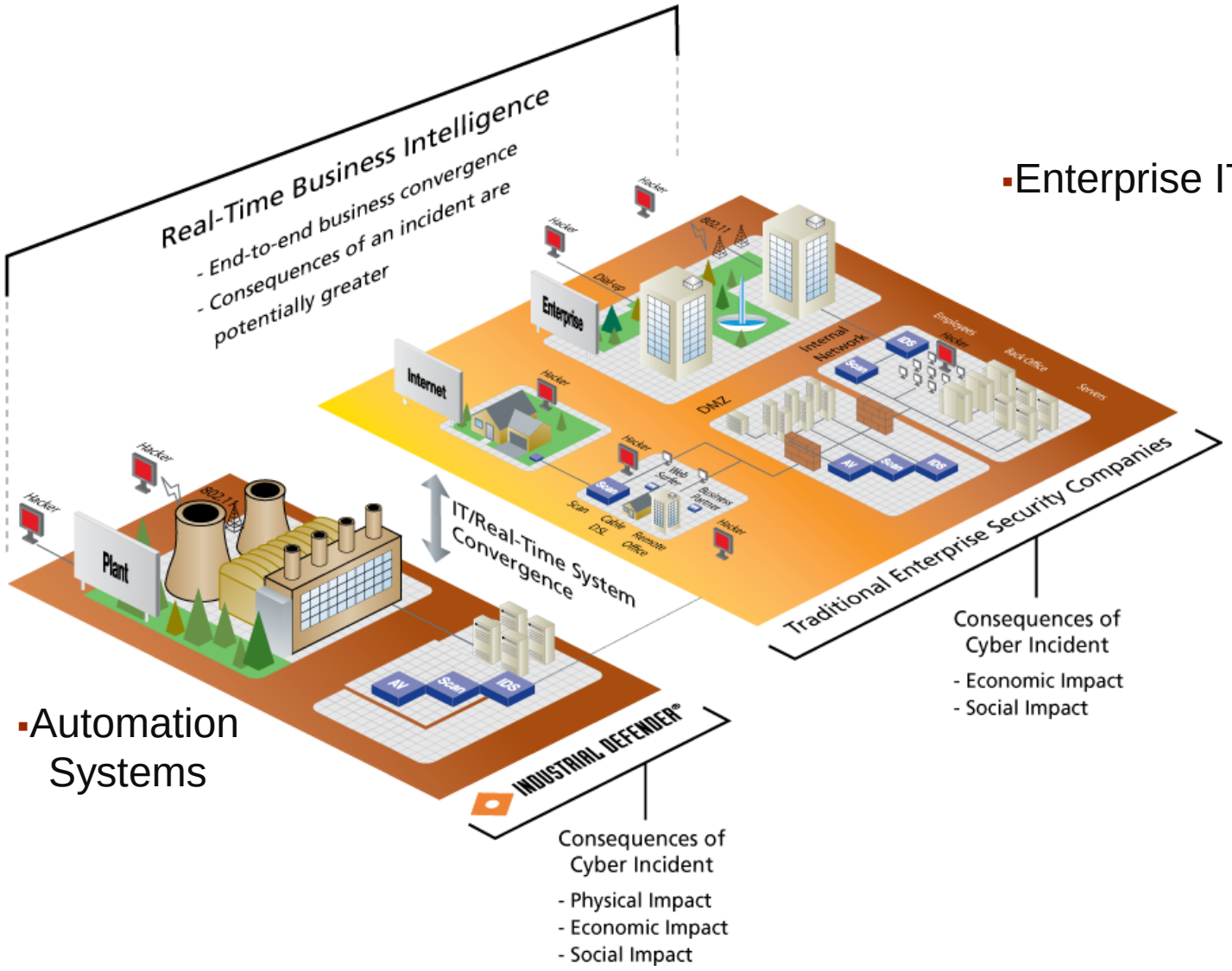
Representative Customer Roster

ABB

Reality of the Automation System Environment…

- "Always on" mentality; system reboots are not a way of life
- Legacy infrastructure (low bandwidth, slower processors)
- Unique Industrial endpoint infrastructure (more than just clients, servers and networking devices)
- Applications often lag most recent OS versions and patches
- Industrial protocols (DNP3, Modbus, ICCP, IEC61850, etc.)
- Application anomaly monitoring in addition to OS anomaly monitoring

Assuring Security, Availability & Compliance of Automation Systems



- Enterprise IT
- Automation Systems

East Coast Utility EMS and Plant System Case Study

- Transmission and Generation Assets
- 2 ABB EMS Systems plus backup 4 locations
- 1 ABB Plant Control System
- Security Concerns
- NERC–CIP audit requirements
- Centralized SOC for alerting

Unique Customer Requirements

▪Automation Systems Security

- Network and event management
- Break / Fix (Incident response)
- Change management
- Software / patch management
- Auditing and compliance

▪Device Interfaces and Communications

- Event / log collection
- IDS / IPS
- Configuration and patch data collection
- Remote access controls

▪*Automation Systems Devices*

▪Servers: PCS, SCADA, …

▪Work stations

▪Firewalls

▪HMI Stations

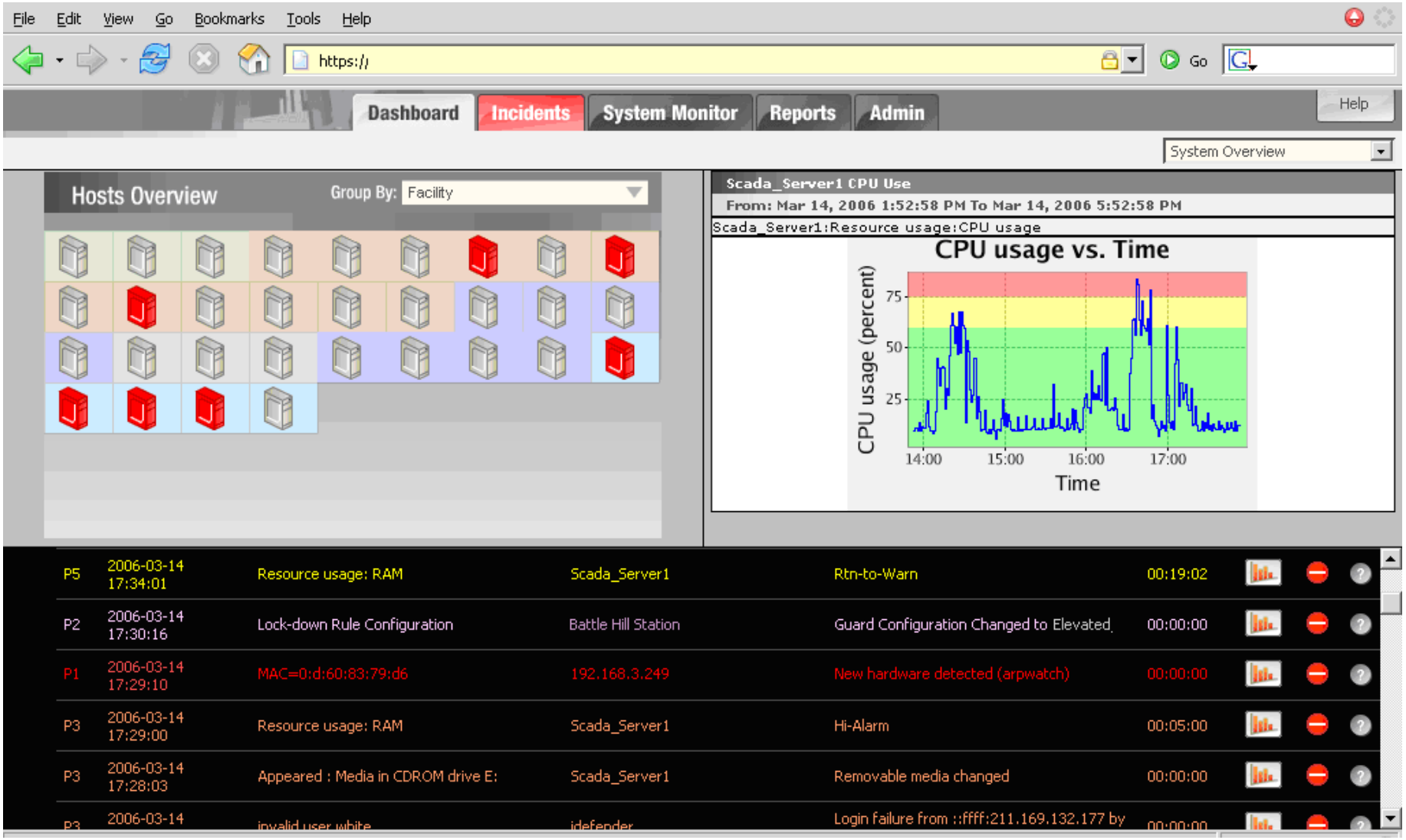
▪Hardened networking devices

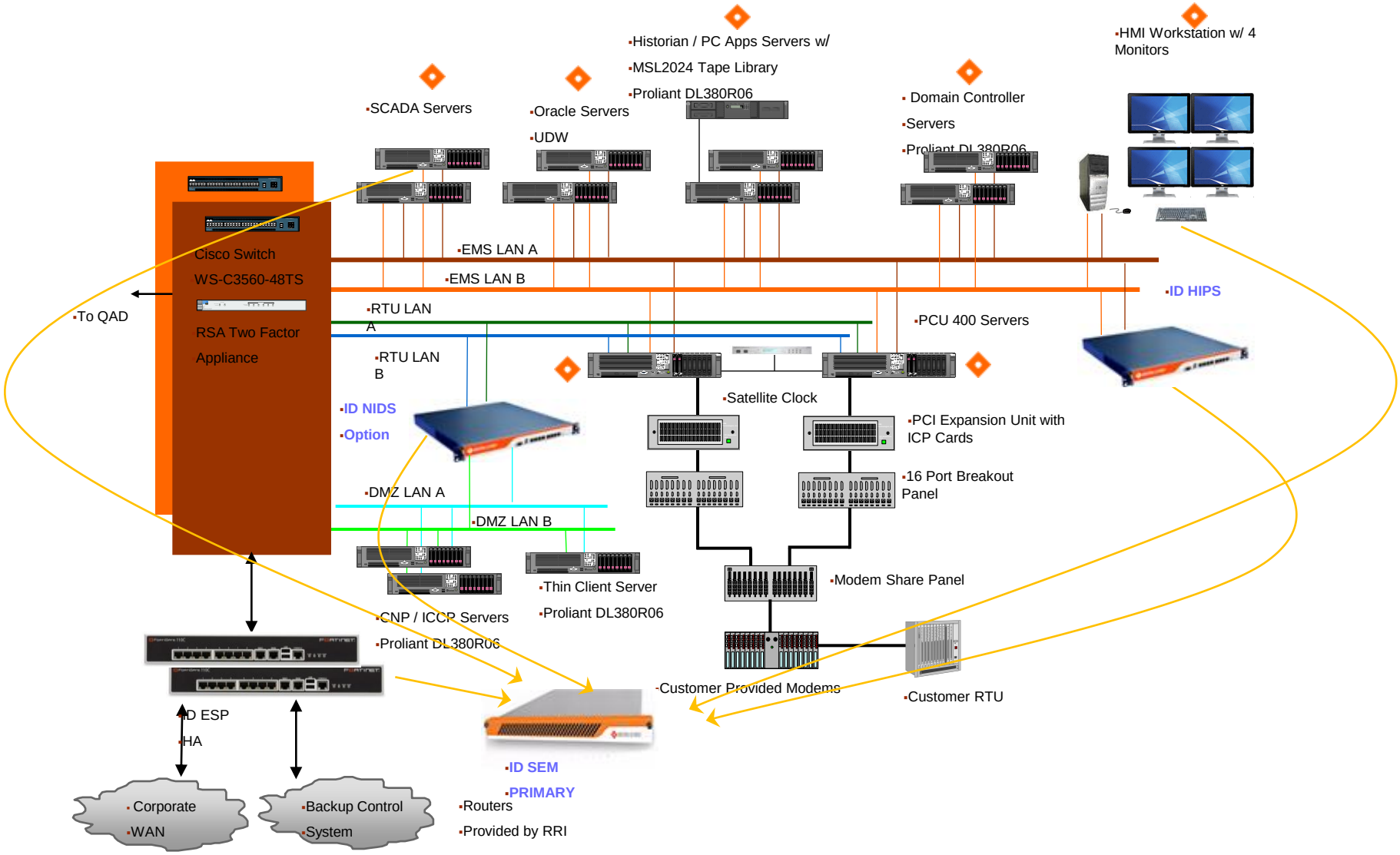
▪IEDs, ▪Sensors, Controllers

Deployed Defense in Depth Security

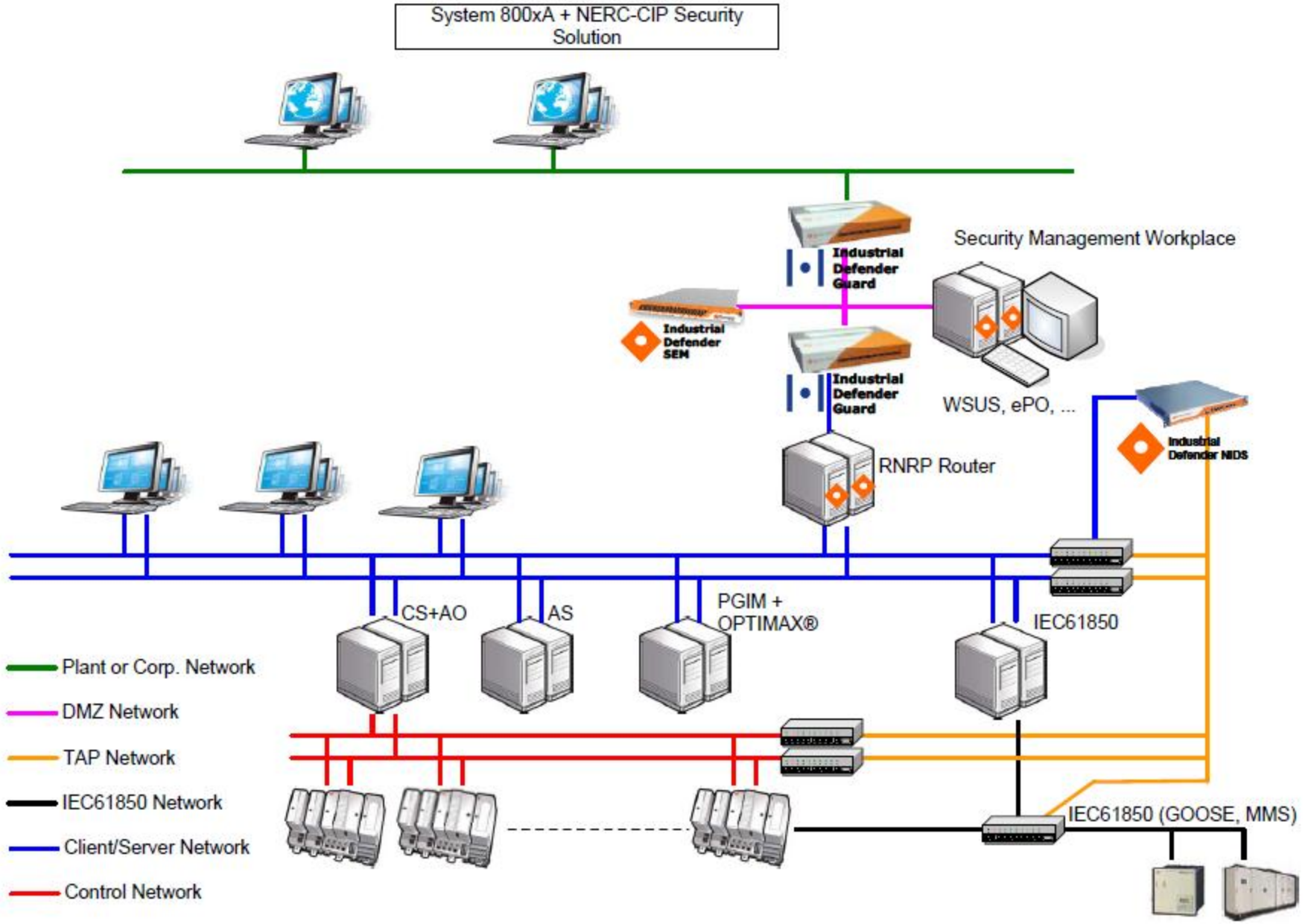
- Monitoring of ABB EMS servers
- Monitoring of Network Segments at Plant and EMS Control Center including industrial protocols such as modbus
- Security Event Manager Technology
- Events forwarded to centralize monitoring system at corporate from all locations
- Syslog reporting on all events within the Electronic Security Perimeter
- Additional Security Layer in addition to built in security for EMS provided by ABB

Security and System Health Alerting





▪Example Energy Management System

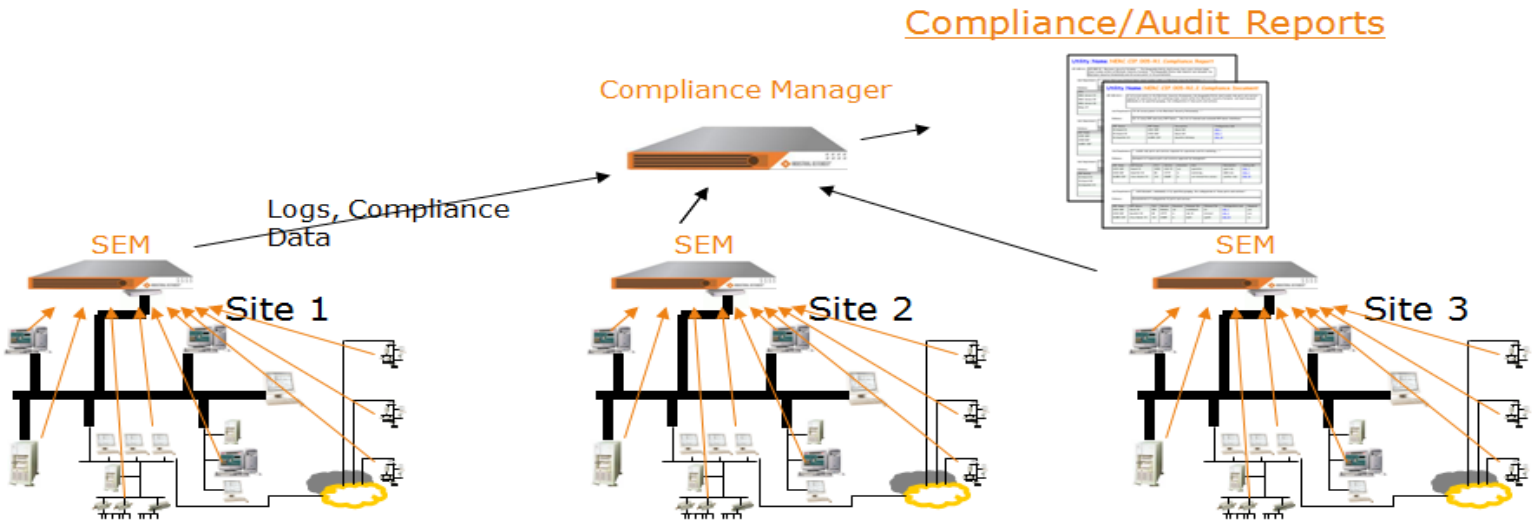

System 800xA + NERC-CIP Security Solution
Industrial Defender Guard
Security Management Workplace
Industrial Defender SEM
Industrial Defender Guard
WSUS, ePO, ...
Industrial Defender NIDS
RNRP Router
CS+AO
AS
PGIM + OPTIMAX®
IEC61850
IEC61850 (GOOSE, MMS)
Plant or Corp. Network
DMZ Network
TAP Network
IEC61850 Network
Client/Server Network
Control Network

Case Study – Security and Compliance Automation

- Western States Power Generation and Transmission Company
- ABB Network Manager EMS
- Generation units with various control systems
- NERC-CIP compliance requirements
- Manual Process for Collection of Data
- Installed monitoring/logging technology on Network Manager servers and workstations
- Used sensors to pick up data from Non-ABB systems in place

Deployment

- Deployed Compliance Manager Technology on top of control room environments
- Automatically collect log data from Servers, Workstations, Firewalls, IED's, PLC's, Routers
- Automatically Generate NERC-CIP Reports
- 10,000,000 records per month



Complimenting ABB System Security
Industrial Defender Security and Automation

- Cyber Security in ABB Control Systems
  - System security components necessary to support customer's processes to comply with NERC CIP, CFATS
  - System security components listed in DHS's Cyber Security Procurement Language for Control Systems

- Testing Industrial Defender with ABB Control Systems
  - Industrial Defender has been tested at all ABB Control Systems Centers of Excellence – EMS, 800xA, Process Portal B, Mach 2

- Case Study – How Industrial Defender integrates with and compliments ABB Network Manager EMS

- Follow-up – How Industrial Defender Compliance Automation Solution can support your compliance program

ABB Control System Cyber Security

- Control System Cyber
  - Network Partitioning – Security Zones
  - Hardening of Hosts
  - Kerberos Authentication
  - Protected Communication
  - Security Audit Trails
  - Intrusion Detection
  - Secure coding guidelines – review code for security

Network Partitioning

Partitioning allows for separation of critical cyber assets with varied security mechanisms between network zones. Goal is to achieve an overall heightened level of security for the control network.

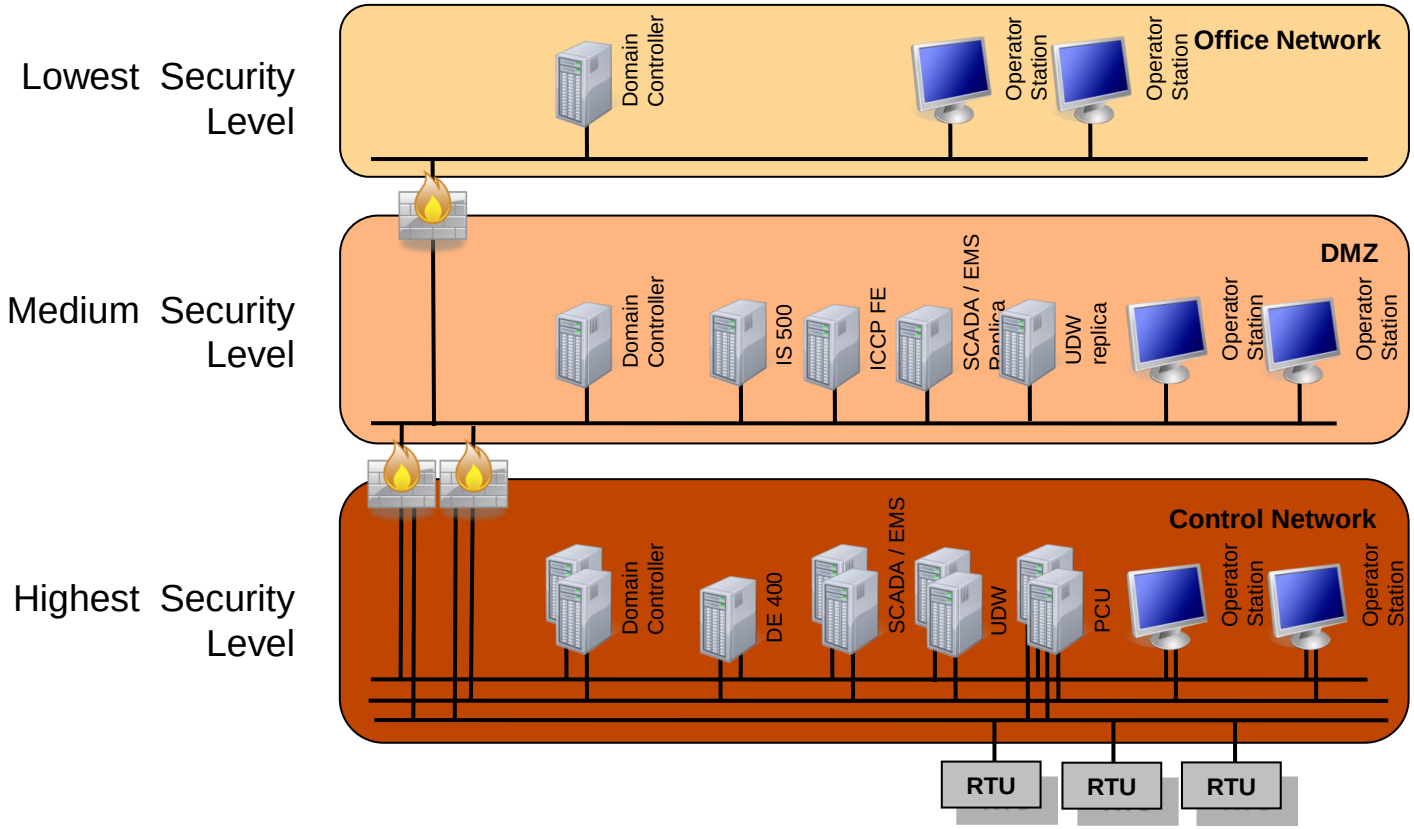


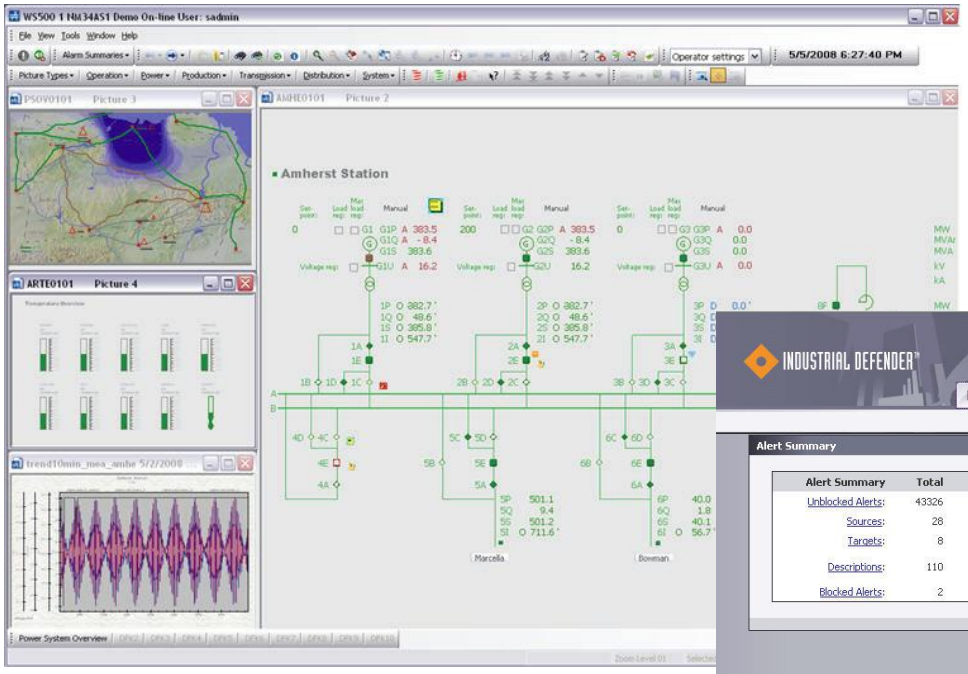
ABB EMS Security

- Closing or disabling all non-vital ports and services
- Static host/ARP tables
- Security Audit Trails – all security related events logged
- Intrusion Detection Systems (NIDS/HIDS) – logs, SNMP traps, and suspicious event monitoring and analysis
- Test and implementation of latest security patches
- Malware Prevention
- Secure Coding Practices
  - Instruct developers secure coding practices
  - Secure code is already part of our code review guidelines
- Protected Communications - proprietary communication libraries use the Kerberos to protect the data flows
  - Default settings include authentication, integrity and encryption.

Strong Authentication

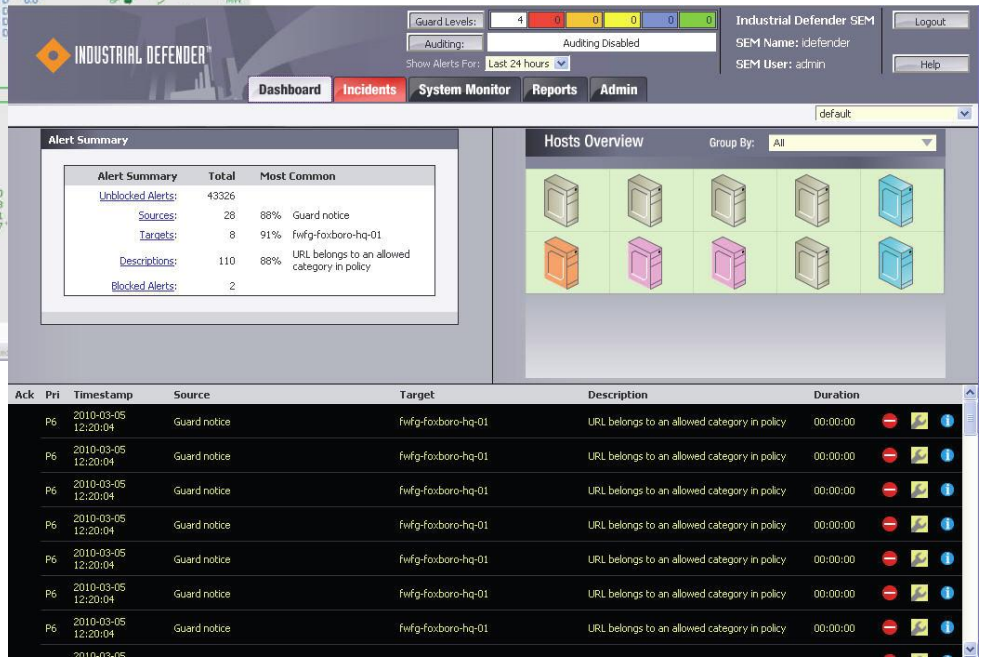
- All normal user and service accounts require Kerberos authentication in all non-bastion Network Manager hosts (including non-Windows hosts)
- Kerberos provides for Single-Sign-On and Session Control and interacts with Active Directory for centralized and uniform management of users and security policy
- Kerberos provision Single-Sign On and Session Control (expiration times) features through a cacheable ticketing mechanism
- User 2-Factor Authentication for Operator Workstations
- Linux hosts access user and service account information in Active Directory through secure LDAP

Integration of Industrial Defender Security and Automation in Network Manager EMS



Network Manager
Operator Console

Industrial Defender
SEM GUI



Industrial Defender ABB Network Manager Solution

- Industrial Defender adds
  - Best in class security
  - Defense in depth
  - Security and Compliance Automation
- Integration and Testing
  - Implement in the factory
  - Do it in phases – implement what you need
  - Implement after system delivery
- Network Manager Extensions

Industrial Defender Best in Class Solution

- Security Event Management (SEM) Console
- Unified Threat Management (UTM) enabled Firewall
- Network Intrusion Detection System (NIDS)
- Host Intrusion Detection Software (HIDS)
- Host Intrusion Protection (HIPS)

ABB Network Manager Extensions

- Special HIDS rules for ABB Network Management node types, including SCADA and Application servers, Data Engineering Servers, and PCU400 servers. Each of these nodes have specific rules for files, process, sockets and registry.
- HIDS agent that monitors the heartbeat of critical applications and generates an alert when heartbeat is no longer heard.
- The Network Intrusion Detection Sensor (NIDS) is configured with ABB specific rules for known traffic between node types.
- The SEM supports redundant networks via a NIC teaming/bonded interface.

Security and Compliance Automation

- Industrial Defender's Compliance Solution for Network Manager facilitates:
  - Automates data collection, analysis and archiving
  - Consolidates event, log and configuration information into a centralized permanent data repository
  - Provides historical reports needed for compliance audits
  - Provides tools for risk analysis and compliance assessment
  - Automatically generates NERC CIP specific compliance audit reports
  - Automate security validation checklist

Q&A

Reminders
Automation & Power World 2011

- Please be sure to complete the workshop evaluation
- Professional Development Hours (PDHs) and Continuing Education Credits (CEUs):
  - You will receive a link via e-mail to print certificates for all the workshops you have attended during Automation & Power World 2011.
  - BE SURE YOU HAVE YOUR BADGE SCANNED for each workshop you attend. If you do not have your badge scanned you will not be able to obtain PDHs or CEUs.

Power and productivity
for a better world™