

DHS ICSJWG Fall Conference 2011



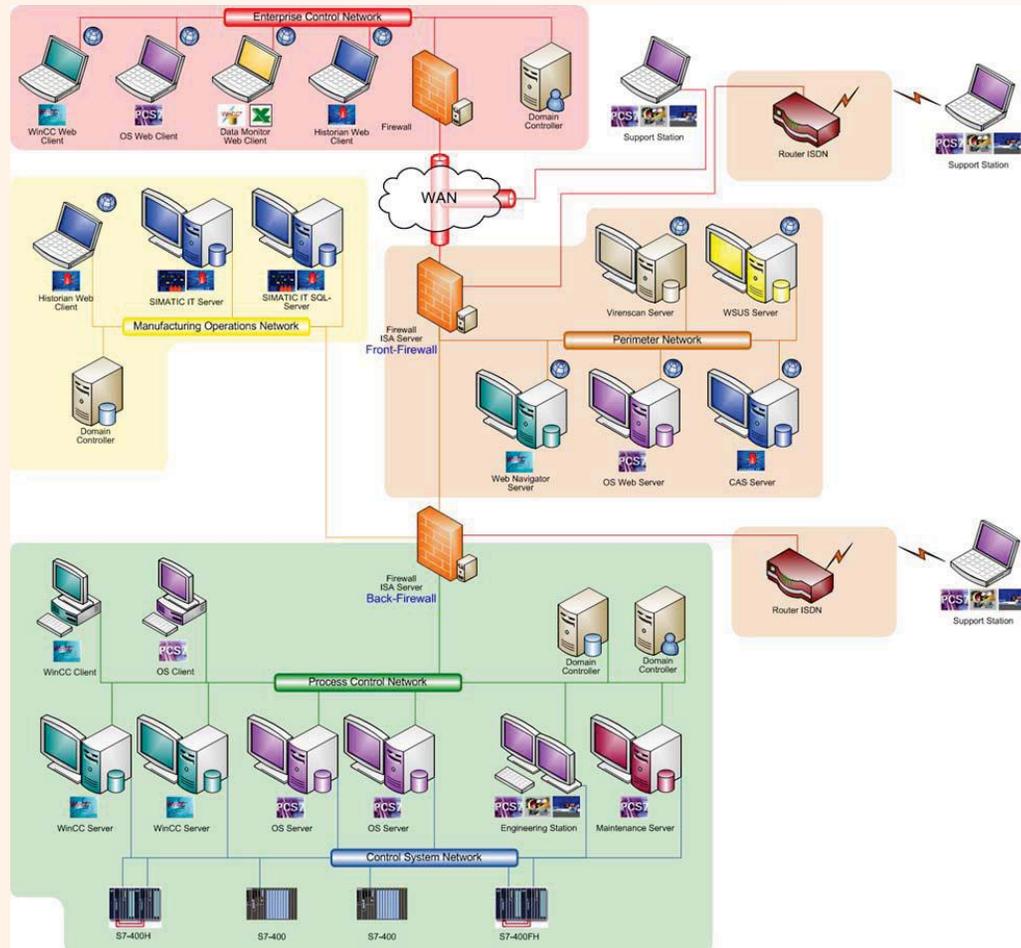
Maintaining Necessary Information Paths Over Unidirectional Gateways

Mohan Ramanathan
Solutions Architect for Critical Infrastructure
NitroSecurity

Andrew Ginter
Director of Industrial Security
Waterfall Security Solutions

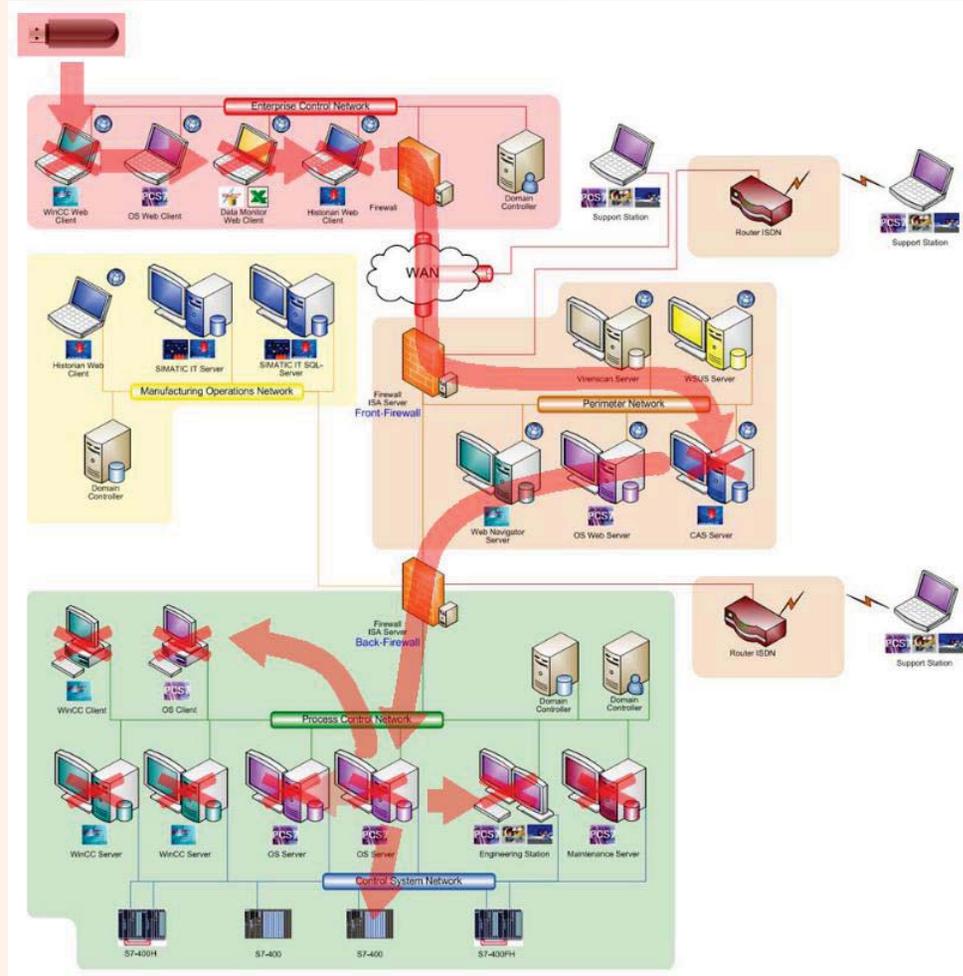
Security "Best Practices"

- Firewalls
- Patching
- Anti-virus
- Host hardening



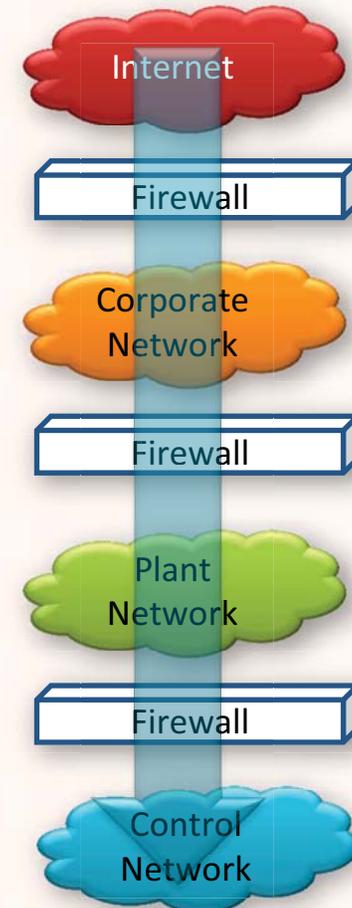
Stuxnet Defeated "Best Practices"

- Firewalls: pass through on "essential" connections
- Zero-days compromise fully-patched equipment
- Encrypted to defeat existing anti-virus signatures, behavior evades specific AV engines
- Open ports: pass through on "essential" connections, escalation of privilege defeats "least privilege"



Night Dragon (APT) Defeated “Best Practices”

- Corporate firewalls: “spear phishing” usually, occasionally SQL injection, conventional attacks
- Remote control (RAT) data gathering, “pass the hash,” domain controller compromise, and others.
- Plant firewalls: pass through on “essential” connections. Exploit vulnerabilities on servers behind the firewall. Or just find the password.
- Zero days: gap between publication of security update and installation.
- RAT tools recompiled and encrypted to defeat anti-virus
- Host hardening: escalation of privilege defeats least privilege, stolen passwords defeat long passwords, “essential” services still leave most services running

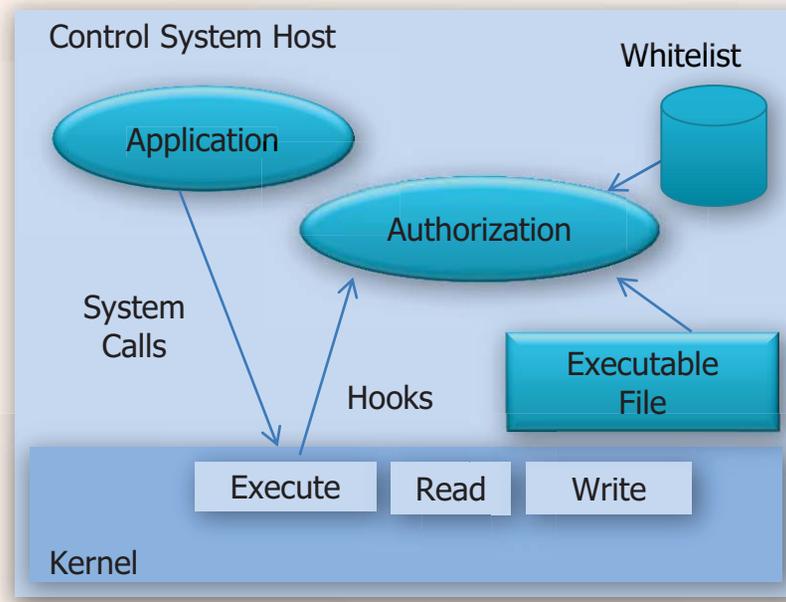




D'oh

Application Control / Whitelisting

- Keep a list of crypto signatures for all authorized executables and libraries
- Hook operating system calls - when loading a library or executable, check the signature -- only recognized files are executed
- Zero days: detects new viruses before signatures are issued
- Protection against in-memory changes of running programs
- Good fit for ICS:
 - No signatures to update
 - Very predictable execution costs
 - ICS networks change control discipline is good fit for approved executable list control



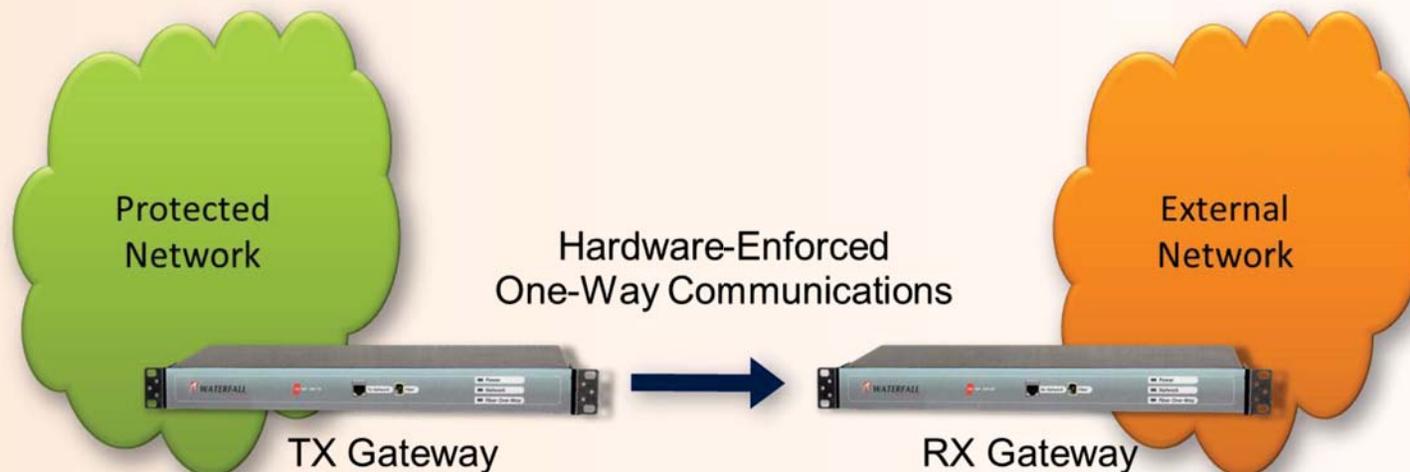
Advanced / Device Firewalls

- Specialized – fewer features, fewer possible connections, *fewer mistakes*
- Device and protocol auto-discovery, auto-configuration
- Deep understanding of industrial protocols
- Allows only certain protocol commands through from certain machines
 - Eg: Only certain hosts can change PLC programs, or change firmware, or write certain values
- Denial-of-Service protection



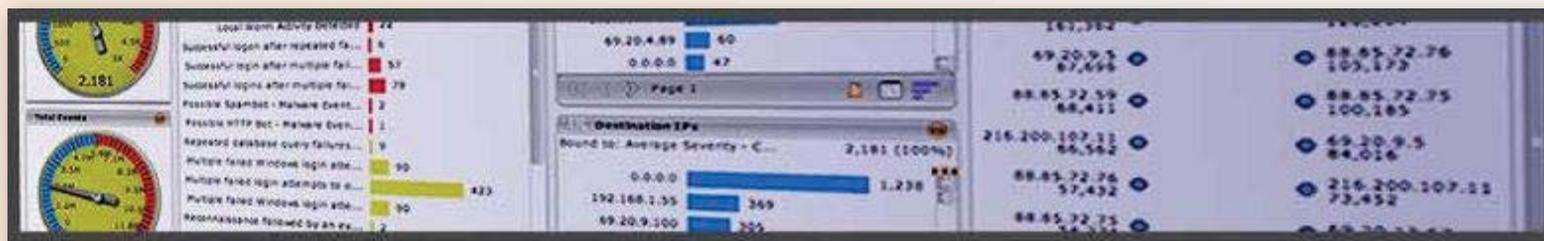
Unidirectional Security Gateways

- Laser in TX, photocell in RX, fibre-optic cable – you can send data out, but *nothing* can get back in to protected network
- TX uses 2-way protocols to gather data from protected network
- RX uses 2-way protocols to publish data to external network
- Server replication, not protocol emulation
- Non-routable one-way communications protocol



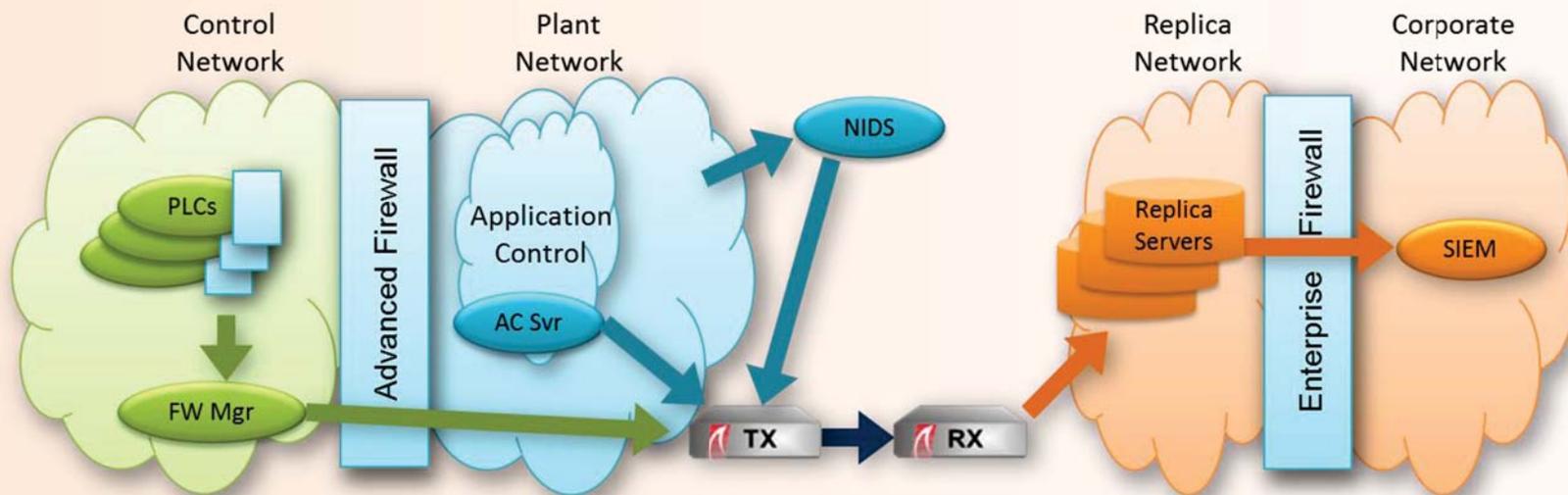
SIEM and Anomaly-Based Intrusion Detection

- Security Information and Event Management
 - Gathers security logs, security events, and compliance information into one pane of glass
 - Gathers information from industrial systems, networks and devices
- Comparatively small, uniform industrial networks support anomaly-based intrusion detection without floods of false-positive alerts
- Anomaly-based host intrusion detection
 - Learns what is "normal" – alerts on everything else
 - Passive – mirror port on managed switch sends a copy of every message



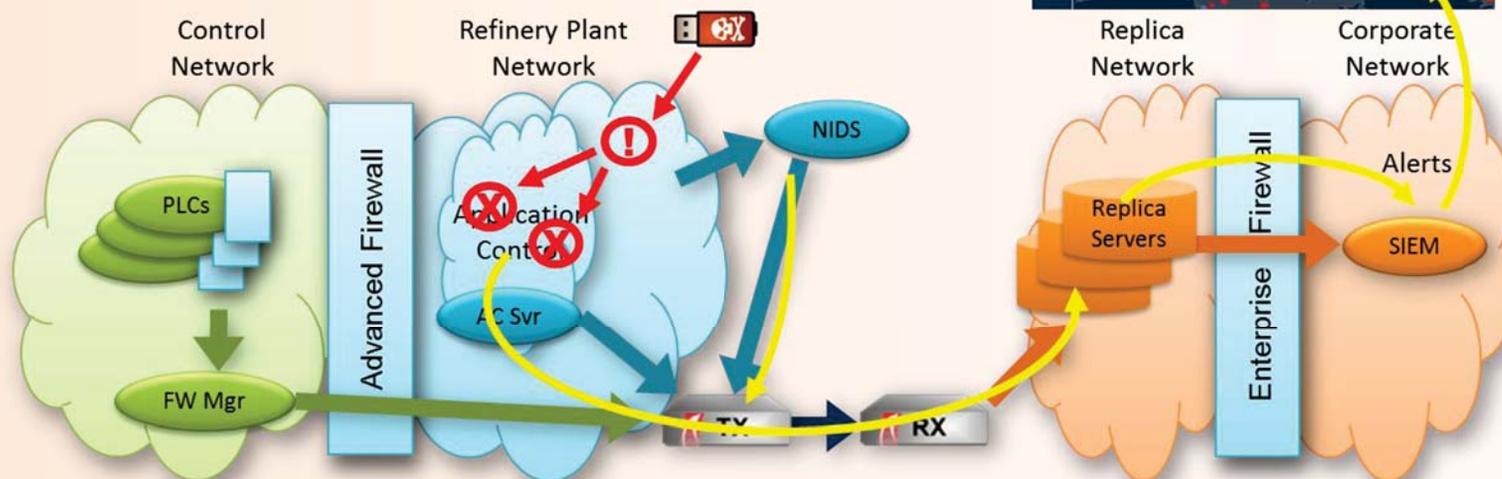
Pulling It All Together

- These technologies *do* all work together
- Syslog, SNMP traps, log files and SMTP messages blocks all are transferred to the SIEM
- SIEM provides advanced correlation with data from entire network, and visibility into the entire network



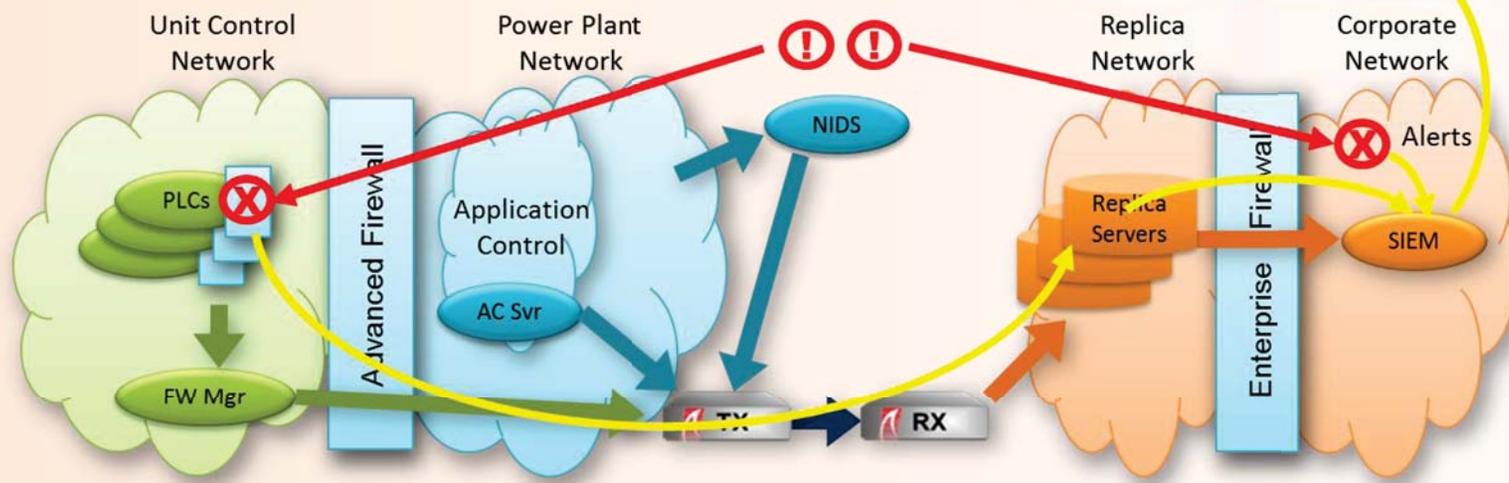
Scenario: Common Virus on Refinery PCN

- USB key infects unprotected host on refinery PCN and host attacks protected equipment
- NIDS identifies attacker, application control prevents infection
- Alerts propagate to SIEM for global visualization, correlation and triage



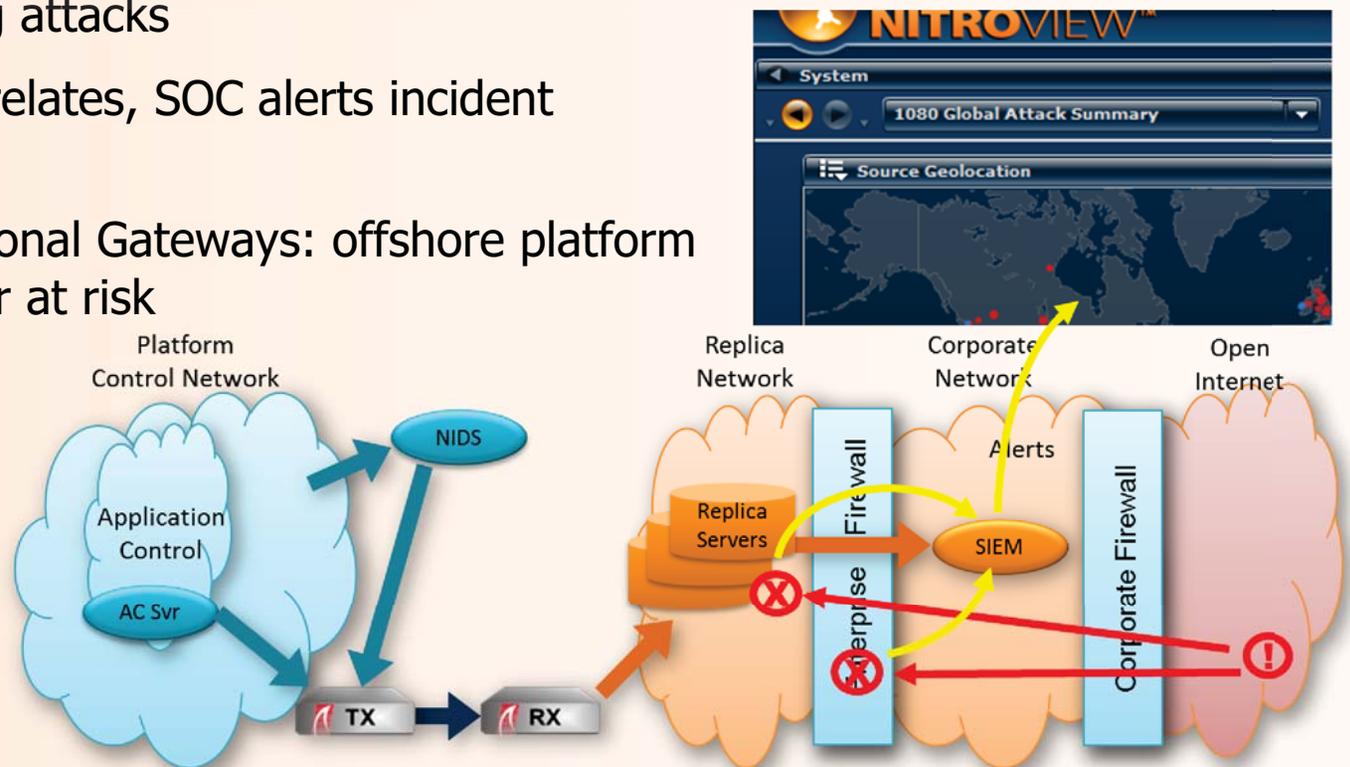
Scenario: Insider Attack at Power Plant

- Insider within PCN network physical perimeter has two desktops: access both to PCN and to corporate network
- PLC firewall blocks attempt to reprogram PLC from unauthorized engineering station
- Corporate network alerts re: password attempts on critical databases
- SIEM correlates attacks to one individual



Scenario: Targeted Attack on Offshore Platform

- Advanced adversary penetrates corporate defenses
- Replica network firewall defeats and logs most attacks
- Application control on replica servers defeats remaining attacks
- SIEM correlates, SOC alerts incident response
- Unidirectional Gateways: offshore platform was never at risk



Industrial Security Vendor Coalition (I-SVC)

- Best-of-breed industrial security solutions
 - Committed to industrial security
- All solutions interoperate, all support integrated deployment
 - Documentation to support integrated deployments
 - Services personnel trained on integrated deployments
- Mutual support relationships – escalation paths into each other's support organizations
 - No finger-pointing in complex deployments



Interoperability is no accident

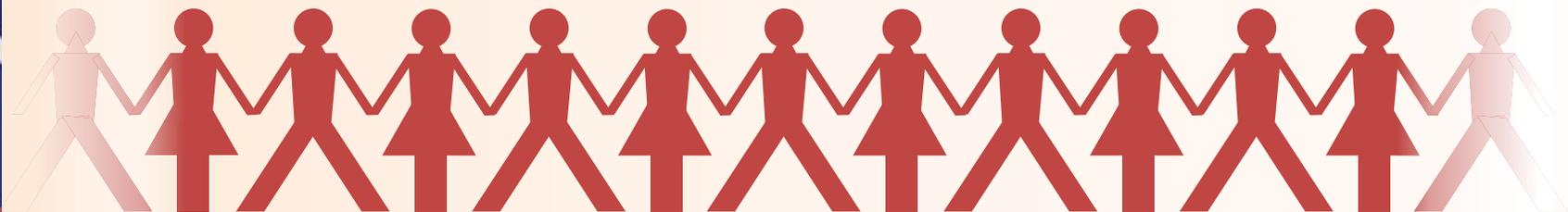
Associates Program

- All control system product vendors are eligible
- Vendors officially support interoperability with I-SVC integrated security solution
- Simplified support, mutual escalation paths for support personnel
- Recognized as supporting strong industrial security
- Opportunities to participate in joint security awareness-building and other programs



Validated Partners Program

- All control system product vendors are eligible
- Vendors support interoperability with I-SVC integrated security solution, and have tested and validated that interoperability
- Simplified support, mutual escalation paths for support personnel
- Recognized as supporting strong industrial security
- Opportunities to participate in joint security awareness-building and other programs



Industrial Security Vendors Coalition

- Security interoperability delivers robust, reliable control system networks
- Firewall / AV / Patching / Hardening “Best Practices” are not enough
- Best practices are evolving: security leaders invest in:
 - Security Information and Event Managers
 - Unidirectional Gateways
 - Application Control
 - Intrusion Detection
 - Advanced Firewalls
- Coalition makes deploying best-of-breed, integrated security systems straightforward



Strong security, simpler