Verifying Operational Effectiveness For Physical Protection Systems

Charlie Nickerson
Nuclear Cyber Programs
Idaho National Laboratory

Janice Leach
Physical Security Analysis
Sandia National Laboratories

November 2017
Let’s Set The Stage: What Are We Facing?
Managing Expectations & Security Concerns

"I'll let the developer have access"
"You're a senior executive, of course you can."
"We'll patch that later."
"We'll allow contractors thru the air gap."
"No means no…right?"
Understanding Systemic Vulnerabilities

1. Errors
2. Vulnerabilities
3. Discovered Vulnerabilities
4. Disclosed Vulnerabilities
5. Patched Vulnerabilities
Analyzing The Vulnerability Life Cycle

- **Design Errors**
  - Systems level errors and weaknesses (architecture)

- **Coding Errors**
  - Application level errors and weaknesses (routines)

- **Discovery Of Error**
  - Error is discovered by white, black, or grey hat

- **Patch / Fix**
- **Release / Disclosure**
- **Weaponize**
  - Vulnerability is known
Applying Cyber Security Principles To PPS

EXTERNAL FACING NETWORK
Level 5

CORPORATE WAN
Level 4

SITE LAN
Level 3

PLANT PROCESSES & CONTROL
Level 2

FIELD DEVICES
Level 1

Infrastructure

Field Distribution Box

Head End System (AC&D)

Edge Devices

Lighting

Interior Sensors

Exterior Sensors

Access Control

Cameras

FDB

Servers

Client Workstations

Power
Process Oriented Risk Reduction

Analytic

Computer Security Policies: PPS Life Cycle

Assets & Consequences

Thickness

Threat

Vulnerabilities

Mitigated Risk

Design Analysis

Supply Chain Management

FAT Performance

SAT Performance

Deployment & Configuration
Process Oriented Risk Reduction

Requirements Document
• Cybersecurity and operational performance requirements should be integrated and clearly stated
• This document can be used to define vendor expectations
• This includes clearly defined METRICS!!!!
• These requirements become FAT Metrics

Factory Acceptance Testing
• Verify that product meets contract defined security requirements
  • Functionality & Resiliency
• Verify functionality of human-machine interactions & external interfaces

Functional/Pre-Testing At Site
• Random sample of delivered equipment and repeat of FAT
• Quality Assurance
• Not integrated into the overall network

Site Acceptance Testing
• Systems level testing of the new components/sub-system(s) within the overall existing network
• This also includes user acceptance testing to ensure the personnel operating the systems agree with performance and that it meets the delivered system meets the design requirements
  • Visual checks on installation
  • Software integration with other systems, etc.

Black Box Testing
• Test simple actions a cyber threat would do to impact digital devices along the critical path
• Focuses on functional security specifications of the specific device and/or subsystem
• Create a set of exercises that encompasses inputs and outputs based on potential adversary actions
Applying Security Controls

1. Treat cybersecurity as a human issue, not a technology problem
2. Share as much information about lessons learned as permitted
3. Deliberate security: Not security by accident and/or DIY Security
4. Make security references easier to understand
5. Create regulations that support implementation of cybersecurity; not just compliance