Setting the Standard for Automation™

SCADA Attack Vectors Protection & Defense

Pat Warton, CMNA

Control Engineering, Inc.

www.controlengineering.com

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Scope

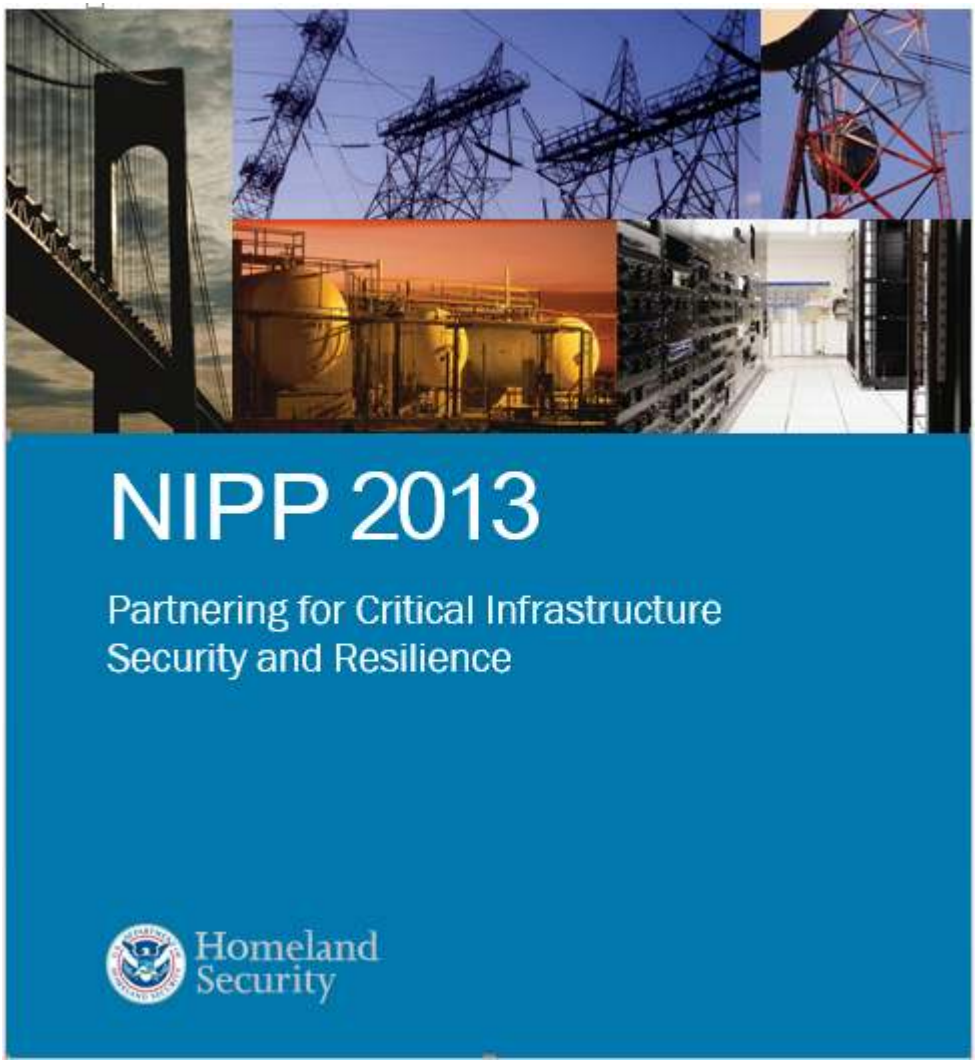
- Background Specifications & Regulations
  - PPD-21
  - NIPP
  - DHS C-3 Program
  - U.S. Air Force DC-3 DoD Cyber Crime Center
- DOCUMENTED Attack
  - STUXNET
- SHODAN (You really are not as hidden as you think)
  - Internet SNIFFER for Control Systems
- CIA Wikileaks - TBD
- Exploits
- Network Attack Surfaces
- Prevention

Presidential Policy Directive 21
2/12/2013

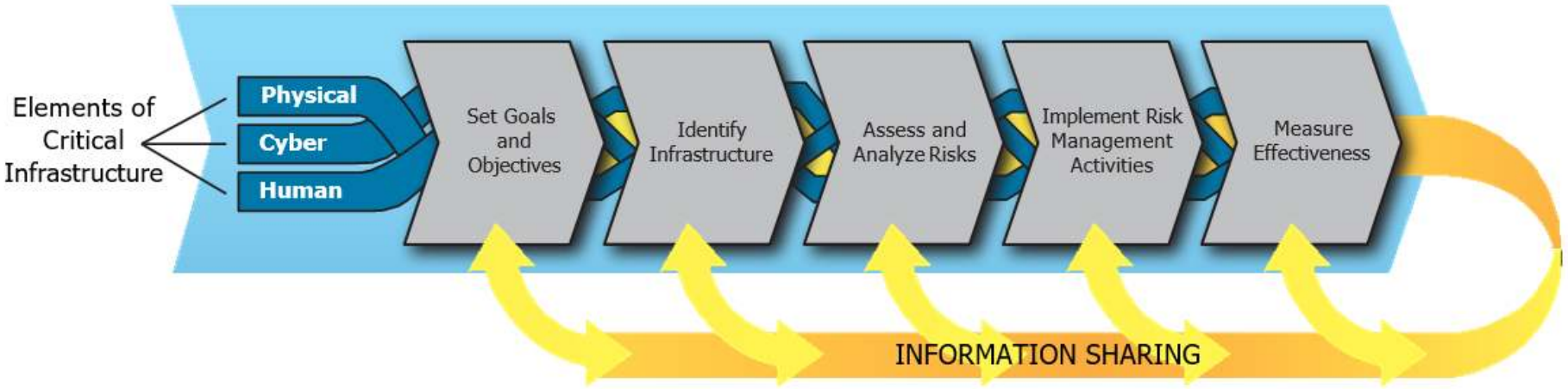
- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

PPD-21 assigns a federal agency, known as a Sector-Specific Agency (SSA), to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the NIPP concepts to the unique characteristics and conditions of their sector. Sector-Specific Plans are being updated to align with the NIPP 2013.


NIPP 2013
Partnering for Critical Infrastructure
Security and Resilience
Homeland
Security

NIPP 2013



This requires a continuous cycle of analysis, implementation and testing

C³ Voluntary Program Activities

Use

Assist stakeholders with understanding use of the Cybersecurity Framework (the Framework) and other risk management efforts, and support development of general and sector-specific use guidance.

Outreach and Communications

Serve as a point of contact and customer relationship manager to assist organizations with Framework use, and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Framework.

Feedback

Work with organizations using the Framework to understand how they are using the Framework, and receive feedback on how the Framework and C^3 Voluntary Program resources can be improved to better serve organizations.

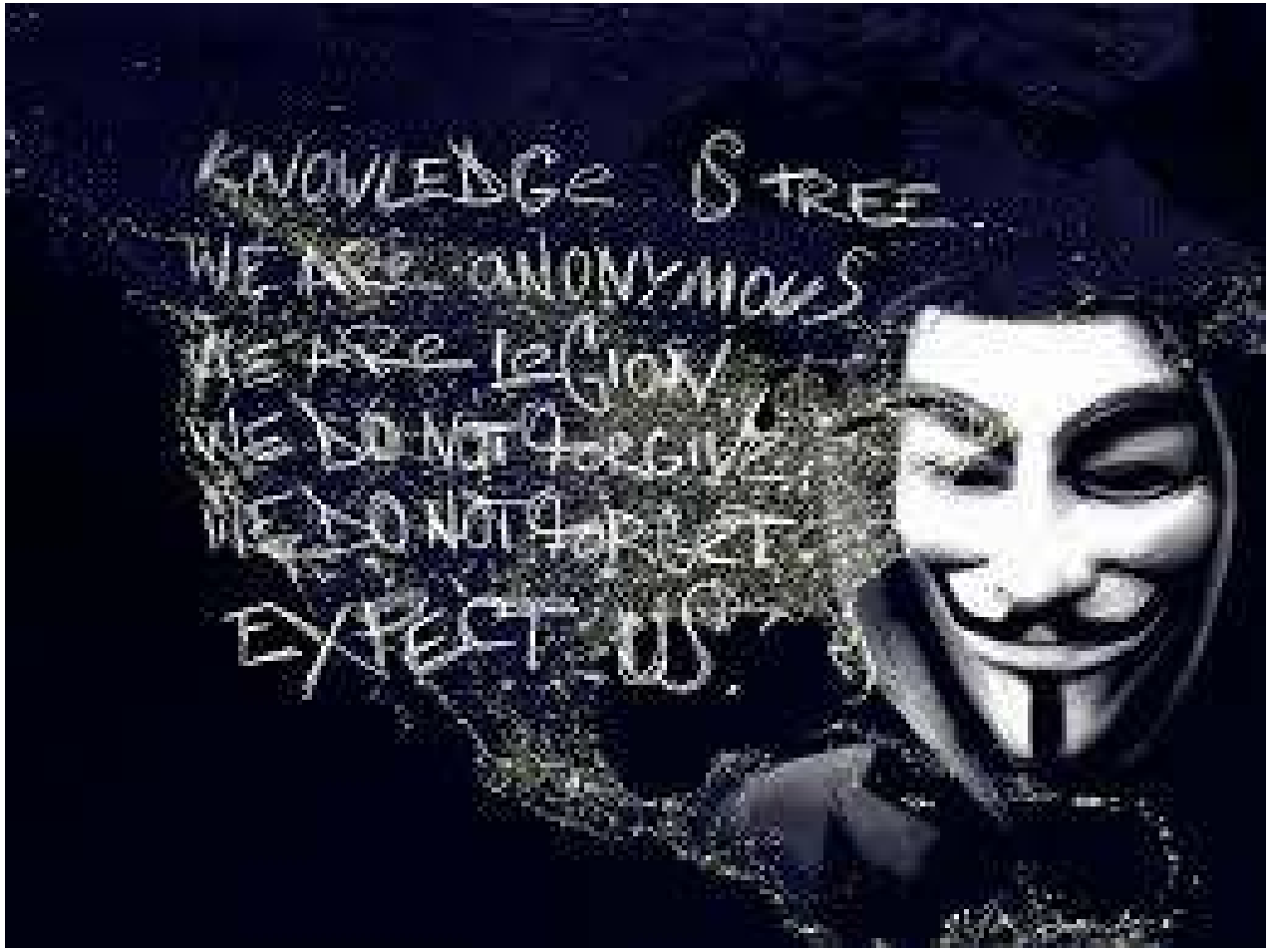
DC3

DoD Cyber Crime Center

Air Force Office of Special Investigations

TECHNICAL SOLUTIONS

Provides a series of tools to test systems and subsystems


KNOWLEDGE IS FREE
WE ARE ANONYMOUS
WE ARE LEGION
WE DO NOT FORGIVE
WE DO NOT FORGET
EXPECT US

Stuxnet: The World's First True Cyber Weapon

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a rootkit component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet.[1]

[1] "STUXNET Malware Targets SCADA Systems". Trend Micro. January 2012

For its targets, Stuxnet contains, among other things, code for a man-in-the-middle attack that fakes industrial process control sensor signals so an infected system does not shut down due to detected abnormal behavior.[2] Such complexity is very unusual for malware. The worm consists of a layered attack against three different systems:

1.The Windows operating system,

2.Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows and

3.One or more Siemens S7 PLCs.

[2] Steven Cherry; with Larry Constantine (14 December 2011). "Sons of Stuxnet". IEEE Spectrum.

Shodan

Originally developed by John Matherly

When he was 18

Exposes Industrial Control Systems On the Internet

As the dimensions of the challenge posed by Shodan became clear, the DHS Industrial Control Systems Cyber Emergency Response Team issued a stark warning in October 2010, noting "the increased risk" of brute-force attacks on "systems available on the Internet."

Wikileaks Vault7

ExitBootServices hooking

```
    /* Get the memory map */
    UINTN MemoryMapSize;
    EFI_MEMORY_DESCRIPTOR *MemoryMap;
    UINTN LocalMapKey;
    UINTN DescriptorSize;
    UINT32 DescriptorVersion;
    MemoryMap = NULL;
    MemoryMapSize = 0;


    do {
        Status = gBS->GetMemoryMap(&MemoryMapSize, MemoryMap, &LocalMapKey, &DescriptorSize,&DescriptorVersion);
        if (Status == EFI_BUFFER_TOO_SMALL){
            MemoryMap = AllocatePool(MemoryMapSize + 1);
            Status = gBS->GetMemoryMap(&MemoryMapSize, MemoryMap, &LocalMapKey, &DescriptorSize,&DescriptorVersion);
        } else {
            /* Status is likely success - let the while() statement check success */
        }
        DbgPrint(L"This time through the memory map loop, status = %r\n",Status);

    } while (Status != EFI_SUCCESS);

    return gOrigExitBootServices(ImageHandle,LocalMapKey);

}
EFI_STATUS
EFIAPI
HookDriverMain(IN EFI_HANDLE ImageHandle, IN EFI_SYSTEM_TABLE *SystemTable){

    /* Store off the original pointer and replace it with your own */
    gOrigExitBootServices = gBS->ExitBootServices;
    gBS->ExitBootServices = ExitBootServicesHook;

        /* It's hooked! Return EFI_SUCCESS so your driver stays in memory */
    return EFI_SUCCESS;
}
```

Current Exploits of Routine Devices

- Siemens Step 7 Switch Zero Day (Patched but Field Updates Missing)
- Omron Clear Text transmission of Encrypted Passwords (Patched)
- Rockwell Automation -
- GE LogicLinx -
- Schneider - Ethernet/IP CIP protocol Hack
- Wago -
- Koyo -

These requests can all be performed without authentication:

The PLC CPU can be placed into STOP mode, meaning that it won't execute ladder logic any longer.

The PLC CPU can be crashed using a malformed request.

The Ethernet card can have a new firmware uploaded.

The Ethernet card can be crashed using a malformed request.

The IP address of the Ethernet card can be changed.

HART Device Configuration Goes Really Mobile

HART communication technology combined with digital valve controllers, flowmeters and other analytical transmitters can make control-valve maintenance and configuration much easier. Now, HART device management has gotten even easier with a HART communicator app for Android smart phones.

Renee Bassett , Managing Editor, on November 14, 2014

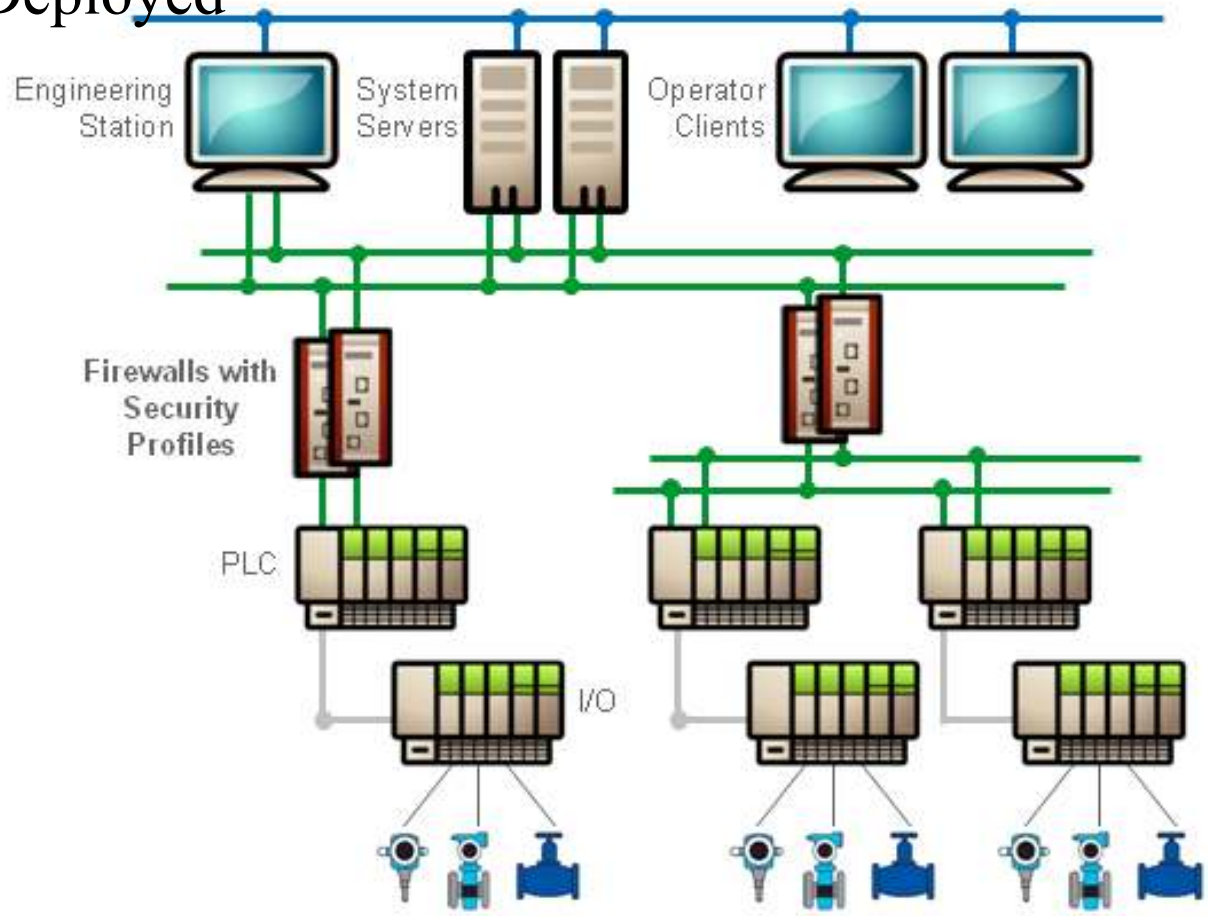
Wireless HART industrial control kit is riddled with security holes

1 Feb 2016 at 18:01, John Leyden, Applied Risk

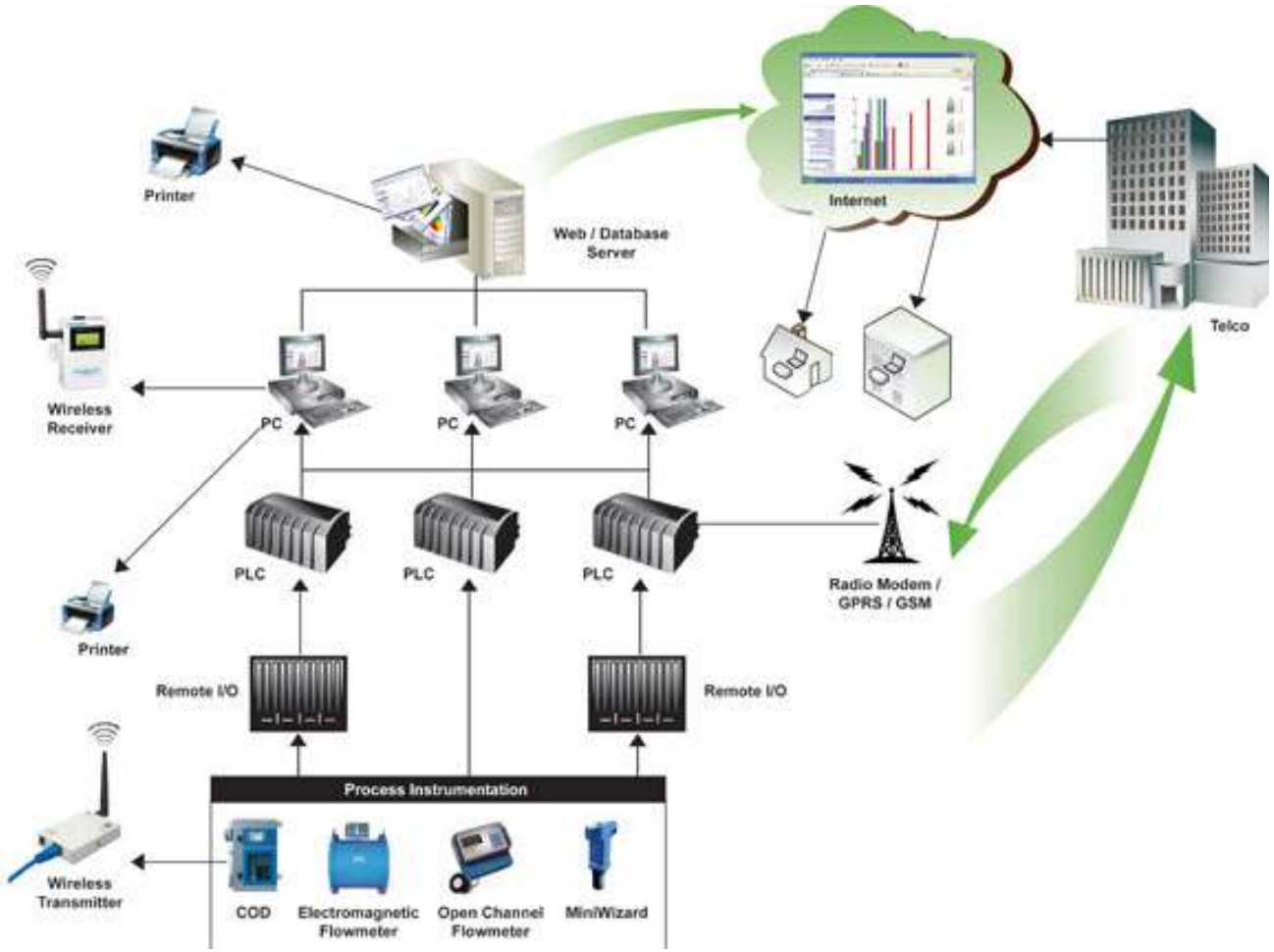
Jalal Bouhdada, founder and principal security consultant for Applied Risk, stated:

“Our research team was concerned to find a number of vulnerabilities in various Wireless HART components used across the globe. The majority of plants are unaware of the risks as security assessments at this level have often been overlooked.”

SCADA Systems as Originally Developed & Deployed



New SCADA Deployments



Recent Attack Surfaces for Exploits

- 900 MHz Radio Traffic
  - 802.11 Ethernet framing on 900 MHz
  - Modbus Over 900 MHz
- 2.4 & 5.2 GHz Radio Traffic
- Bluetooth Radio Traffic
- Zigbee Mesh
- Man in the Middle Attack Vectors
- Internet Exposure / Off Network Attack Vectors

Prevention

AUDIT

Create the Logical Layout Identifying Exposures

ANALYZE

Look at ALL SECURITY

UPDATE

Install ALL Software and Hardware Patches

PENTEST

End to End Functionality Test of Security for Known Attacks Vectors / Ports

UPDATE

If Updates are not Available, Notify the Manufacturer

RETEST

PITFALLS

Far to often, Facilities and Information Technology groups are pitting themselves against one another.

This is not an US vs. THEM

CISCO ISE – Identity Service Engine
RADIUS
802.1x
White Listing Devices