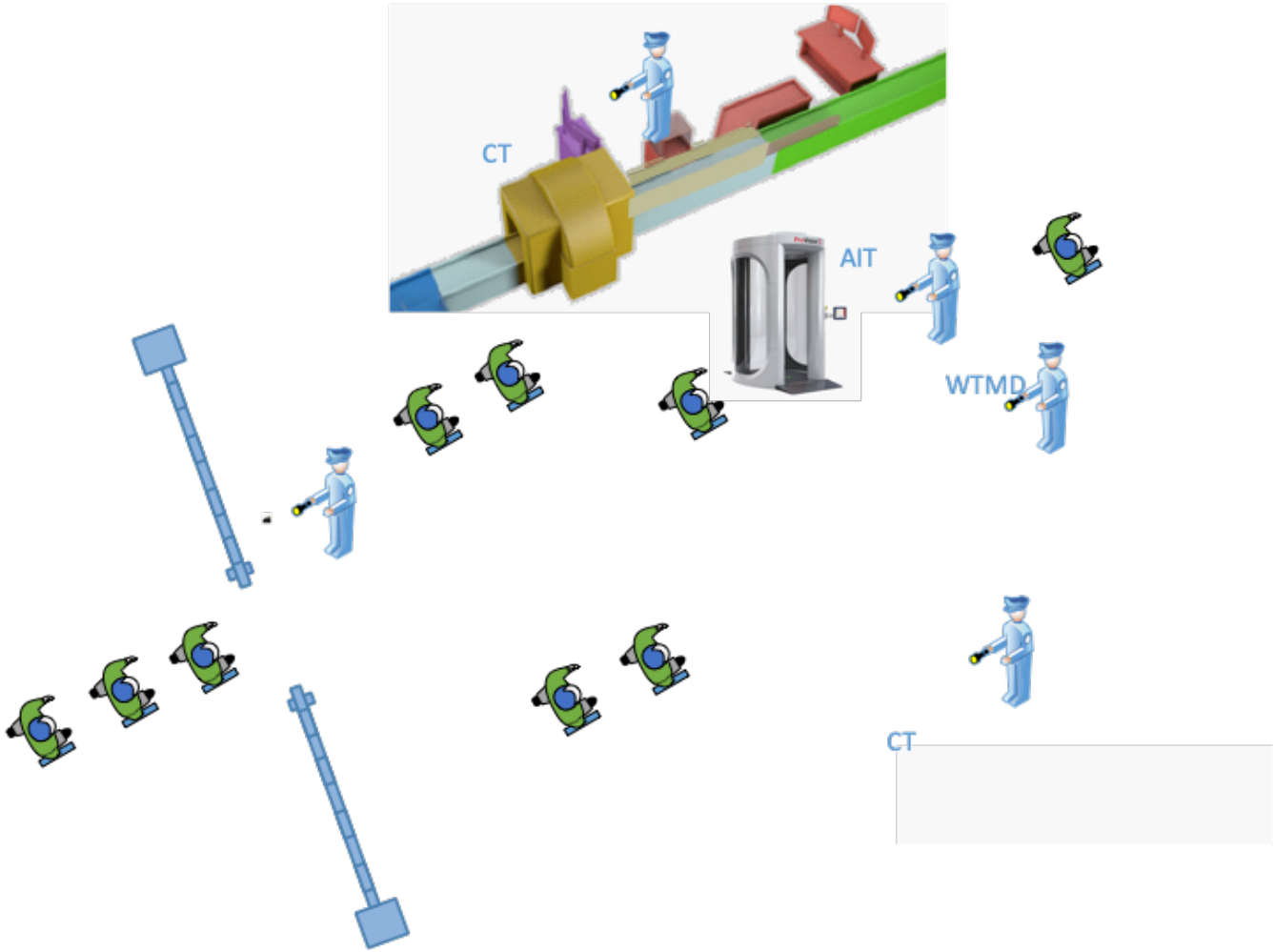
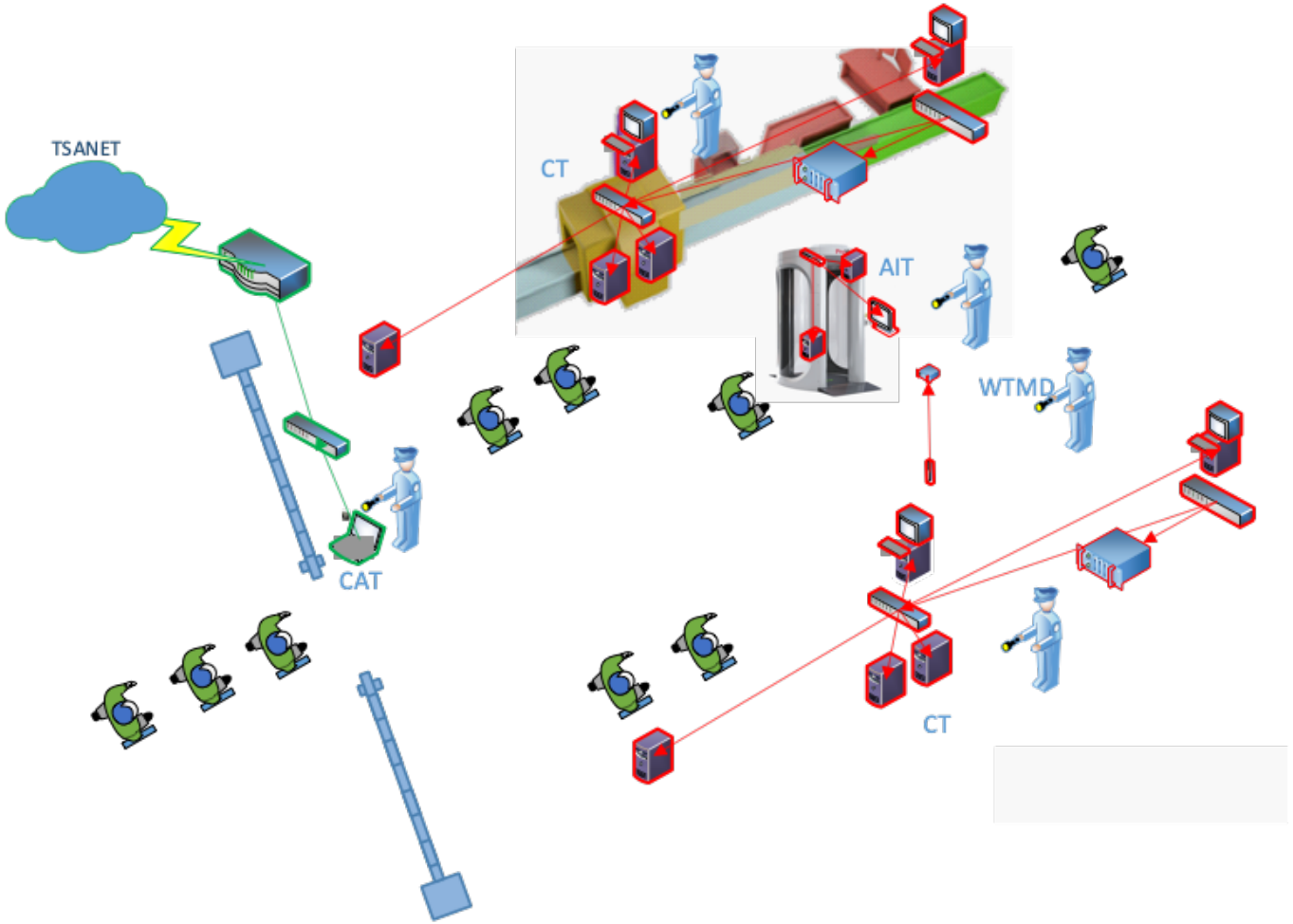
Transportation Screening Equipment (TSE) Cybersecurity Briefing

Edam Colón
Cybersecurity Specialist

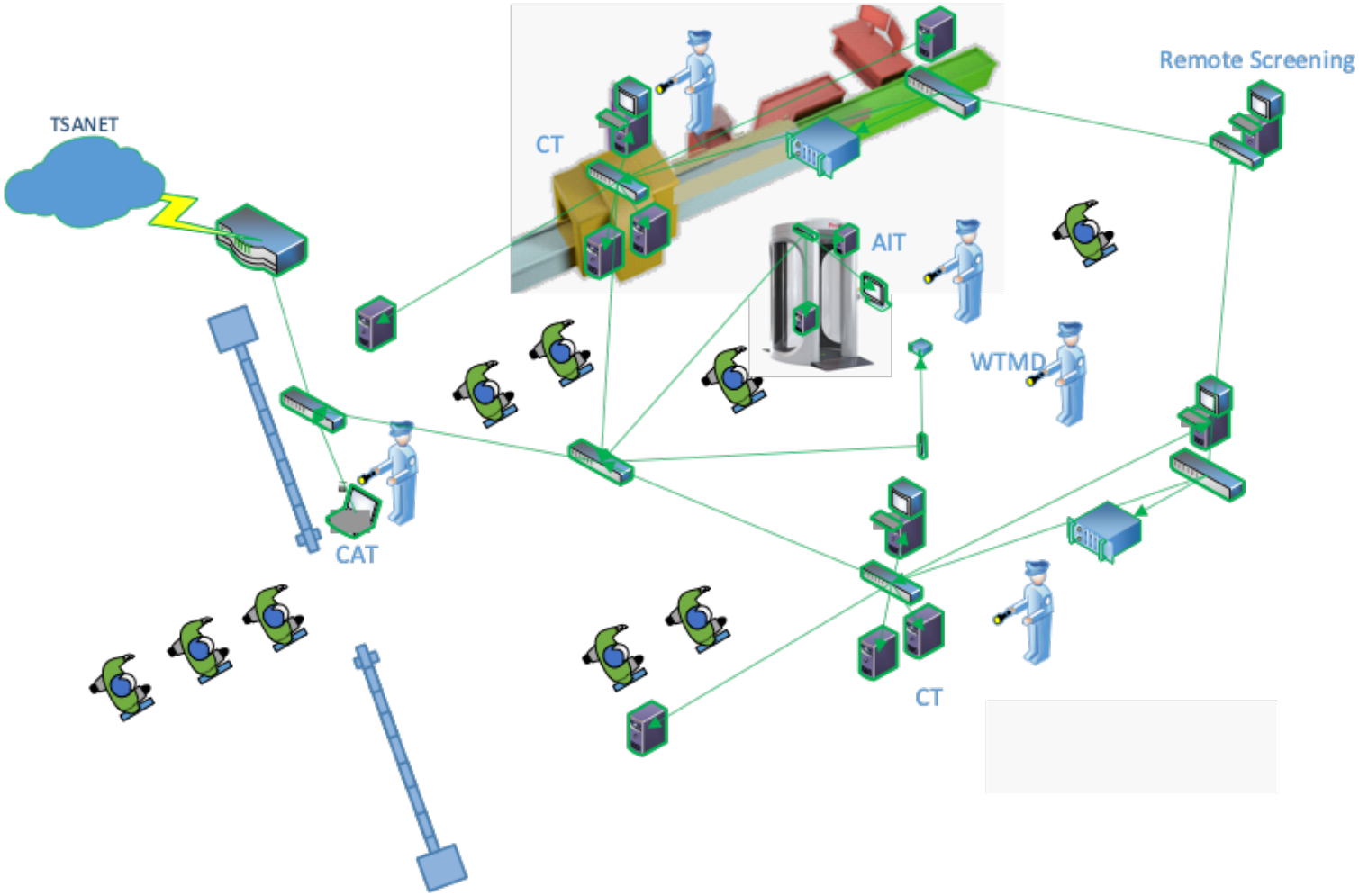
What Most People See at a Checkpoint



What is Actually at a Checkpoint



Checkpoint Connectivity Goals



Transportation Screening Equipment (TSE)

- **Computed Tomography (CT)**
  - Enables 3D imagine platform for enhanced visual interpretation and image manipulating versus 2D X-ray image.
  - Allows upgrades to automatically detect a broader range of threats.

- **Advanced Technology (AT) X-ray**
  - X-ray systems that screen carry-on baggage providing threat detection capabilities for a wide range of threats by displaying dual views.

- **Automated Screening Lanes (ASL)**
  - Uses automated conveyor belts to draw bins through screening and return the bins back to the front of the queue.
  - Automatically pushes carry-on bags that trigger an alarm warning of a potential threat to a separate area.

- **Credential Authentication Technology (CAT)**
  - Verifies passenger IDs at airports security screening checkpoints and detects and alerts the Transportation Screening Officer (TSO) of any ID that appears to be fraudulent and/or expired.

- **Boarding Pass Scanner**
  - Reads a passenger's boarding pass and displays the passenger's name, flight information, and risk status to the Travel Document Checker (TDC).

Transportation Screening Equipment (TSE)

- **Advanced Image Technology (AIT)**
  - Detects a wide range of metallic and non-metallic threats in a matter of seconds using millimeter wave to safely screen passengers for threats (that may be concealed under clothing) without physical contact.

- **Enhanced Metal Detector (EMD)**
  - Detects potentially dangerous metallic threats to aviation security without physical contact.

- **Explosive Trace Detection (ETD)**
  - Detects explosive threats on passengers and/or concealed in carry-on baggage. ETD provides a means for operators to examine articles for explosive residue on passengers and bags.

- **Bottled Liquid Scanner (BLS)**
  - Differentiates dangerous liquids and compounds from common, benign substances carried by passengers.

- **Chemical Analysis Device**
  - Screens and identifies unknown liquid and solids (including powder) materials for harmful substances.

OT vs IT - Two Sides of the Same Coin

Today's interconnected world can no longer consider the security of Information Technology (IT) and Operational Technology (OT) separately.

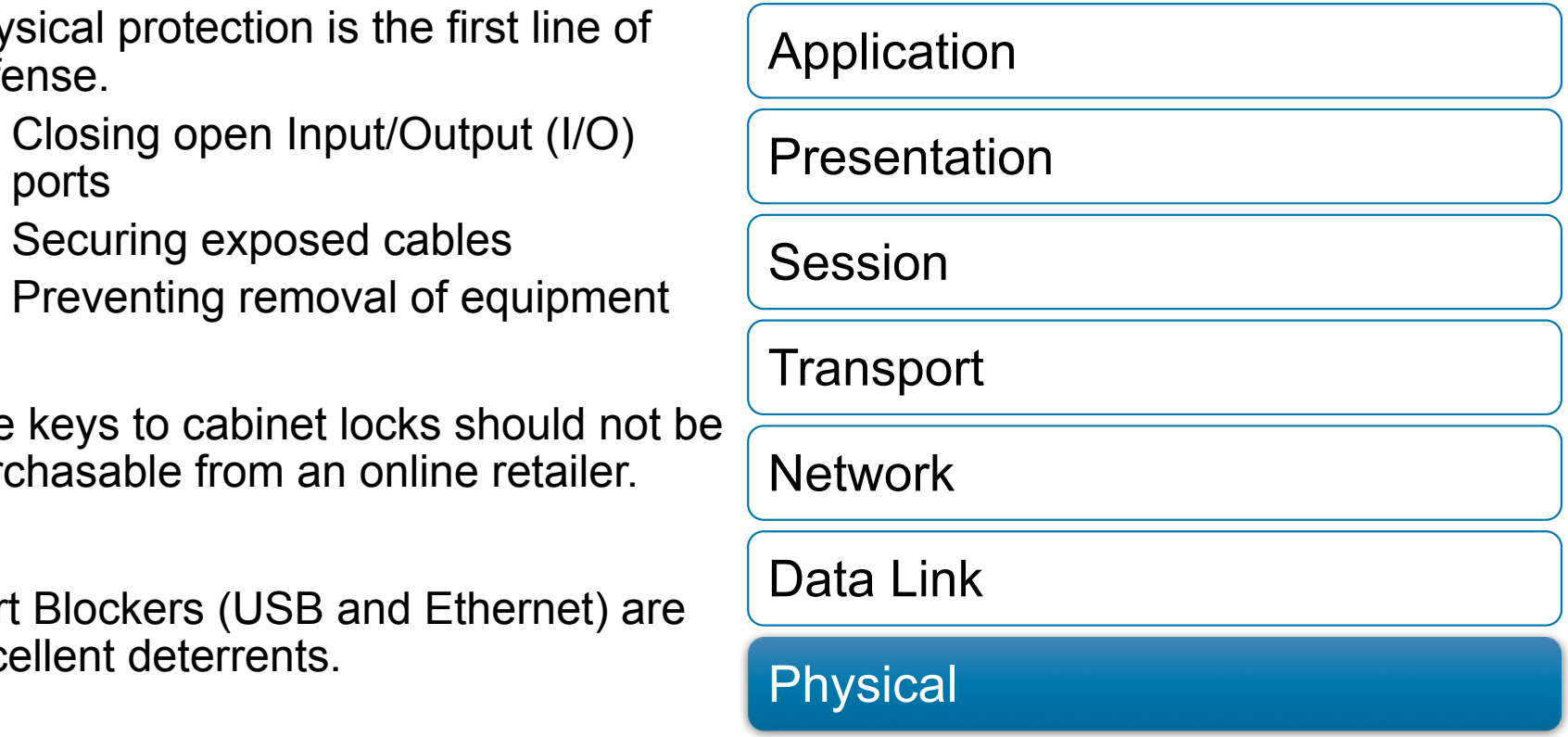
Both use hardware, software, and communication technologies in order to perform their function and process the data.

The security by design of OT systems is integral to protecting the IT infrastructure, as leaving them disconnected is no longer viable.

NIST 800-82r3 will be the US government standard for how to secure OT systems using the NIST 800-53 Risk Management Framework.

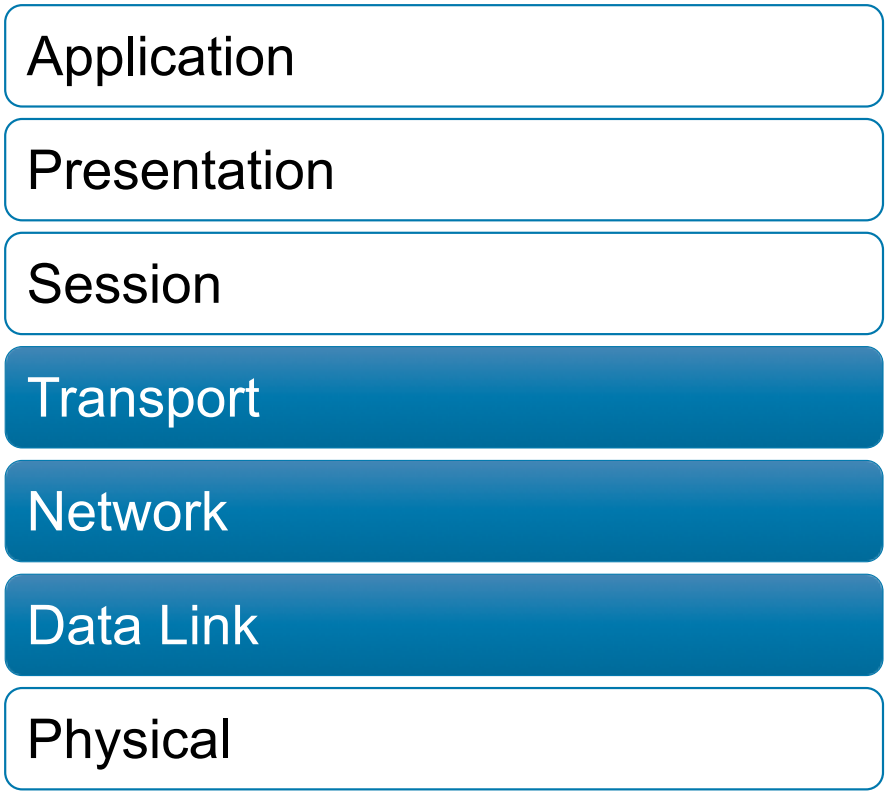
Where do we start?

- Physical protection is the first line of defense.
  - Closing open Input/Output (I/O) ports
  - Securing exposed cables
  - Preventing removal of equipment
- The keys to cabinet locks should not be purchasable from an online retailer.
- Port Blockers (USB and Ethernet) are excellent deterrents.



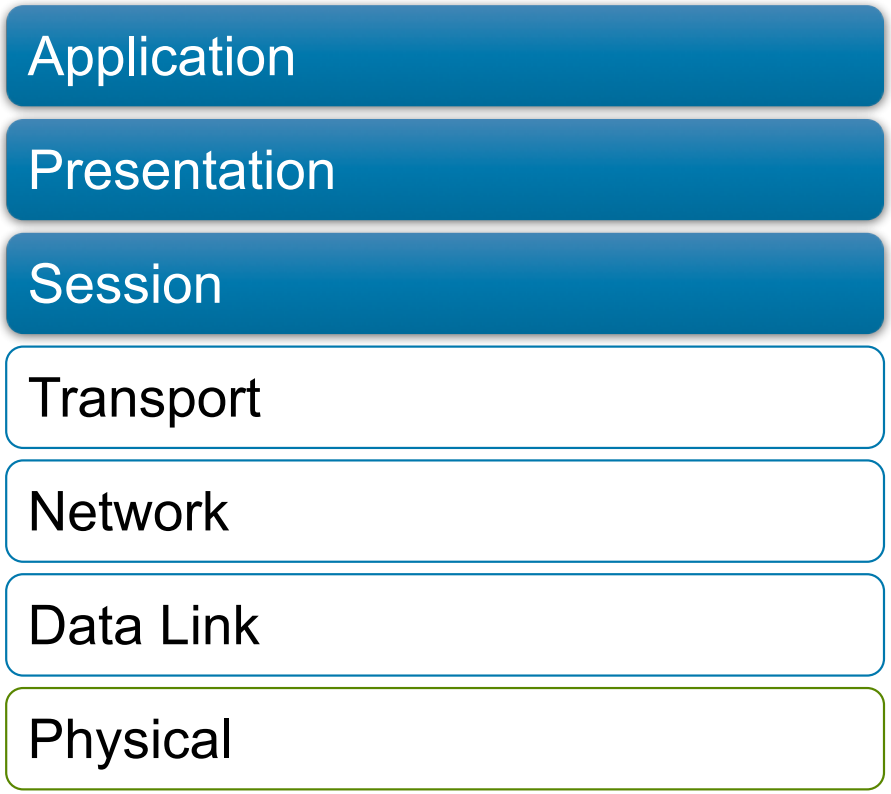
Are the Communications Secure?

- Every TSE has network devices that must be secured.
- Are the routers and switches configured to be secure or are they out of the box installed?
  - Port Security
  - Access Control Lists
- Does the technology use Secure Socket Shell (SSH) or Telnet?
  - If Telnet, it's an automatic failure!
- Need to use trusted PKI certificates to secure communication.
  - Avoid using self-signed certificates.



The Operating System Matters!

- Most Original Equipment Manufactures (OEM) focus on the application that is used for their system.
- The operating system (OS) must be seen as a part of the whole system and secured using security best practices.
  - Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs) are TSAs current standard for OS security configurations.
- A secure application being used on an insecure operating system isn't secure!



Can I Use Any Operating System?

•OS that currently meet those requirements are:

- Red Hat Enterprise Linux
- Ubuntu (Long Term Support (LTS) OS only)
- Microsoft Windows 10 (LTS Only)
- •Microsoft Windows Server (Long-Term Servicing Channel (LTSC) Only)

Not every OS is built the same.

A TSE must have its OS last longer due to the time it takes to make modifications.

The OS must be supported by the OS company with security updates for prior point release versions of the OS releases.

The OS must have at least five years of extended security updates beyond the standard support.

But Wait, There's More!

- Most TSEs are complex pieces of Operational Technology with numerous components IT typically doesn't consider.
  - HMI – Human Machine Interface
  - PLC – Programmable Logic Code
  - RFID – Radio Frequency Identification
  - ASI – Actuator Sensor Interface
  - Etc.
- These are generally firmware, not operating systems!
- These typically contain a web interface, which is browsable by IP address in order to manage it.
- They are most likely to contain default admin credentials or no credentials at all because they are easily overlooked during the hardening process.

Firmware Vs Operating Systems

Features	Firmware	Operating System
Definition	Programing code embedded in specific hardware	It serves as a bridge between the system and the user. It is responsible for all system functions.
Storage	It is stored in non-volatile memory.	It is stored on a hard disk.
Purpose	Its purpose is to manage specific hardware components. As a result, these are single-purpose codes designed to control a single device.	It is a multi-purpose that is used to control several parts of the system. It mainly controls all hardware components. As a result, it is a multi-purpose application because it may run various tasks simultaneously.
Portability	It is embedded in the hardware and may not be changed.	It is a software system that the user may install and change.
Program	It is a small program.	It is a big program.
Updates	It is usually fixed and rarely updated	Often updated on a regular basis
Examples	It resides in keyboards, video cards, routers, webcams, motherboards, mice, microwave ovens, refrigerators, washing machines, etc.	It is Apple macOS, Microsoft Windows, Googles Android, Linux Operating System, and Apple iOS, etc.

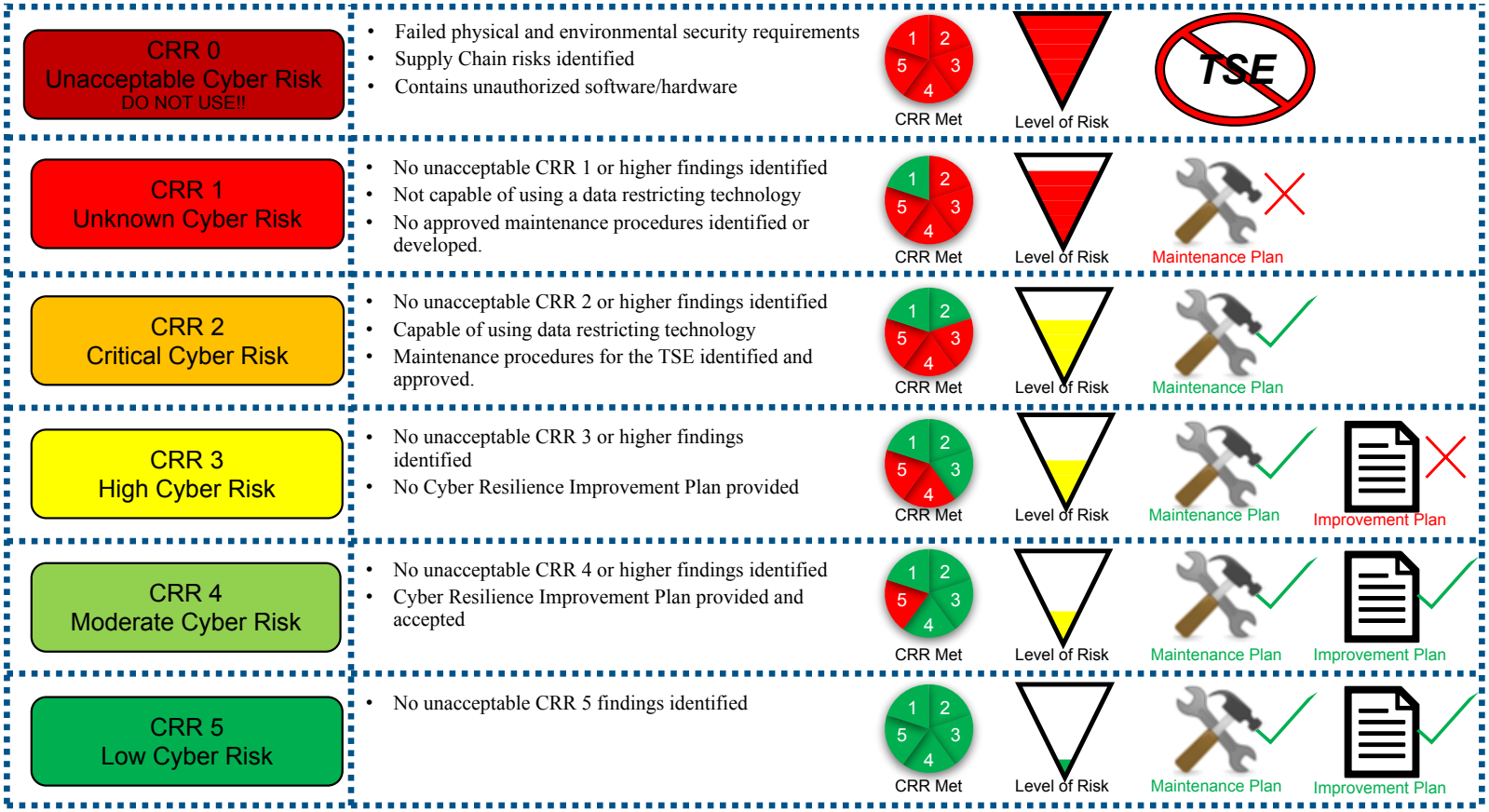
Types of Testing We Conduct

The Security Controls Assessment (SCA) is an evaluation of the NIST 800-53 Controls applicable to the Federal Information Security Management Act (FISMA) system that will be used to determine whether the system is granted an Authority to Operate (ATO)

The Cooperative Vulnerability & Penetration Assessment (CVPA) is the technical security evaluation against the TSE that consists of automated tools and manual assessments designed to identify vulnerabilities and risks with the TSEs Cyber Resilience.

The Adversarial Assessment (AA) is designed to evaluate the TSEs Cyber Resilience under a specific set of scenarios to test whether the TSE is capable of maintaining its screening operations while under a cyber attack.

Cyber Resilience Rating (CRR) Progression Concept



So, What Can We Do?

Develop a Continuous Monitoring Strategy.

Scan for vulnerabilities and patch on a regular basis.
Build in functional testing of security patches at a test facility.

Leave no IP address behind!

If it has an IP address, then it should be part of the network documentation and evaluated for security risk.

Harden with security best practices from the beginning.

CIS (Center for Internet Security) Benchmarks.
DISA STIGs – Security Technical Implementation Guide.
OWASP - Open Worldwide Application Security Project.

Establish better Account Management practices.

Stop the use of Shared or Group Accounts.
Secure both OS and application accounts.
Use service accounts for anything that has Auto-Logon.

Challenges We Need to Overcome

Designing checkpoints for future technologies, not just what is there today.

Finding the balance between Operations and Security.

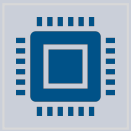
Identifying what changes impacts certification and what changes don't require re-certification.

Treating the technology as if it is exempt from cybersecurity because it perform an operational function.

Applying security best practices during development and not trying to fix it post-deployment.

Every OEM wants to be unique, which means different architectures and solutions for the same problem.

How We Can Help Reach Those Goals



Understanding that a screening technology is more than just the algorithm, hardware, and application.

Securing the ENTIRE system to include the physical checkpoint it is kept at, the operating system, services, accounts, default applications, etc., are critical to the overall security of the TSE.

Stop using outdated, end of life technology or technology that will be end of life within three years.

The five years until end of life prevents the risks of using technology that is no longer supported before the next procurement cycle.

Develop processes to continuously patch, monitor, and update existing TSEs.

All the testing and verification is a snapshot in time and is typically obsolete within a few months, if not weeks.

Questions?