CYBERSECURITY FOR FMCS

Kingston Ng | Taiwan | 19 Sept 2019

Agenda

Opening	Cybersecurity Message
	Defense-in-Depth Strategy
	IT vs OT Challenges & Dilemma
	Case Study Architecture & Recommendation for ICS
	Solutions to Defend from Cyber Attacks
	Cybersecurity Assessment & Tier Studies
Closing	Summary (Q&A)

WannaCry RansomWare

Impact – May 2017

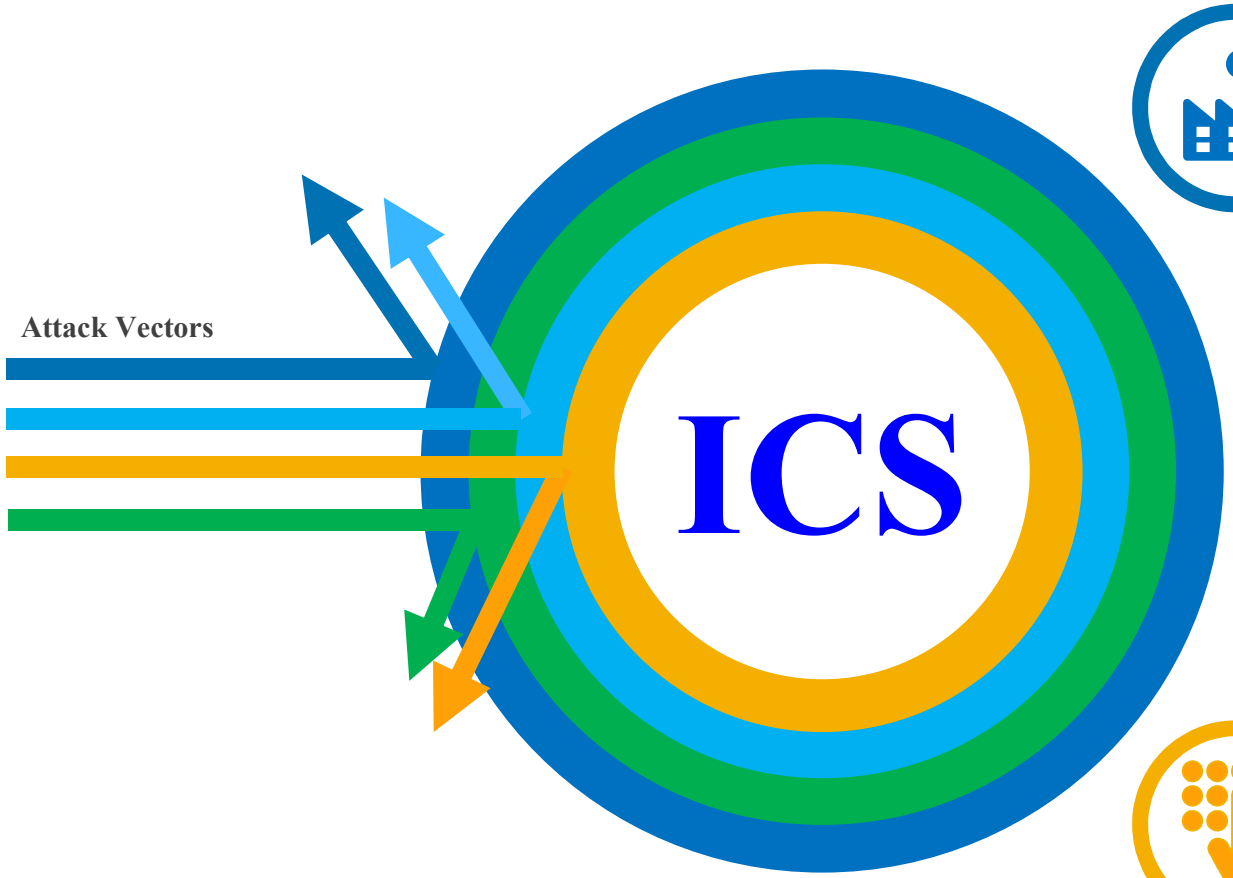
- 4 Billions (USD)
- 150 Countries
- 200,000+ Computers
- Affected many industries, hospitals, Automotive, include Semicon industries
- Microsoft Security Update April2017

Cybersecurity Moment – Middle East – Saudi & Iran

- "30,000 Windows based systems overwritten, master boot record and data wiping" – Wikipedia
- "world's biggest cyberattack. Business was in turmoil" - CNN
- "…stopped selling oil to domestic gas tank trucks" – CNN
- "flew representatives directly to Southeast Asia factories to purchase every computer hard drive currently on the manufacturing line. In one fell swoop, it bought 50,000 hard drives." - CNN
- "Five months later, with a newly secured computer network and an expanded cybersecurity team, **Saudi Arab-company** brought its system back online. An attack of that size would have easily bankrupted a smaller corporation, Kubecka said." - CNN
- "The hackers were never identified or caught -- at least not that we know of. " - CNN

Defense-in-Depth Strategy

ISA/IEC 62443



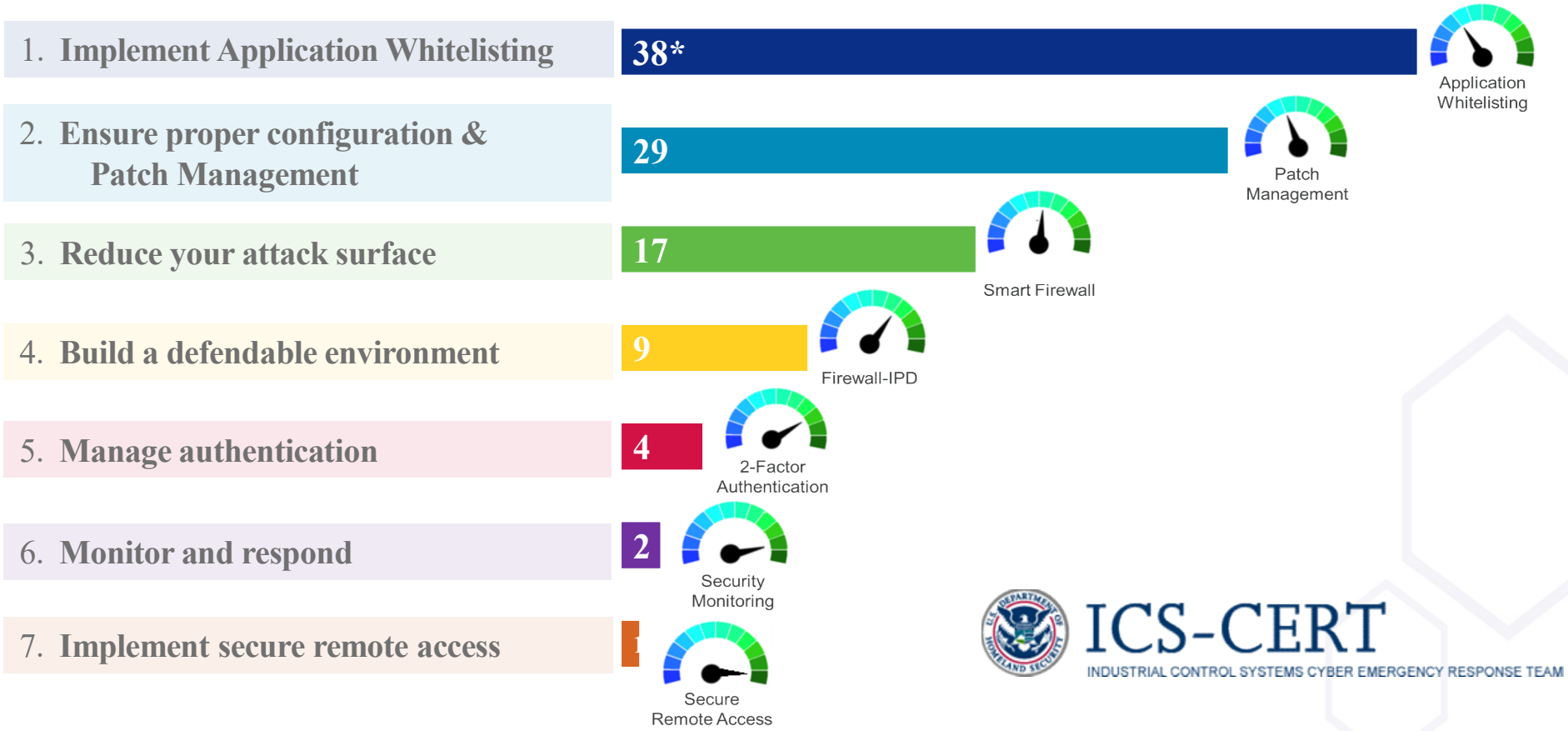
Plant Security
Policies & Procedures ◆ Personnel Trainings ◆ Physical Security

Security Products
Smart Firewalls ◆ Firewall-IPDs ◆ Smart Switches ◆ Layered Network Architecture

Services & Support
Endpoint Security ◆ Whitelisting ◆ SIEM ◆ NSM ◆ Patch Management

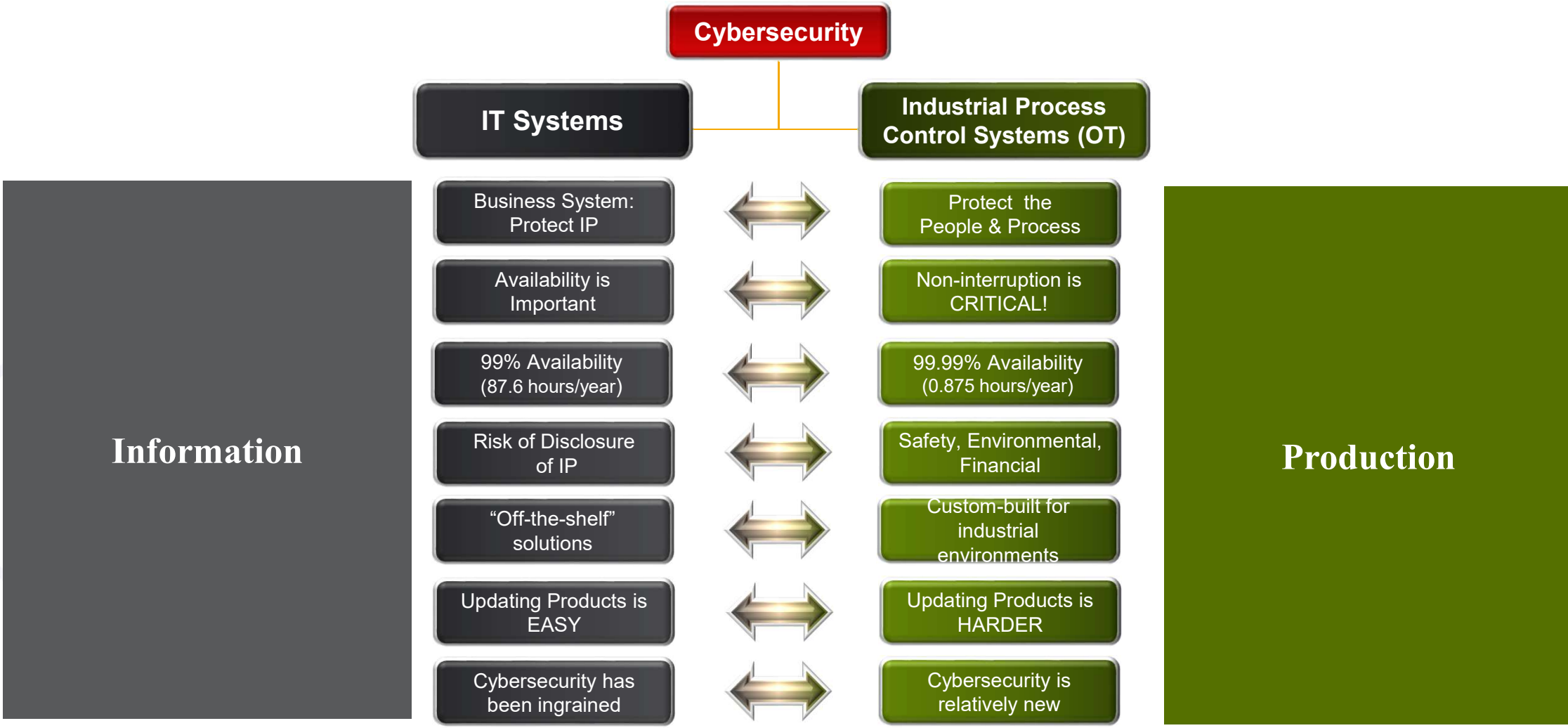
Features & Setup
System Hardening ◆ Digital File Signing ◆ Windows GPOs ◆ Network Device Command Center

Defense-in-Depth Strategy



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IT vs. OT - Process Control : Challenges / Differences



Reference Architecture

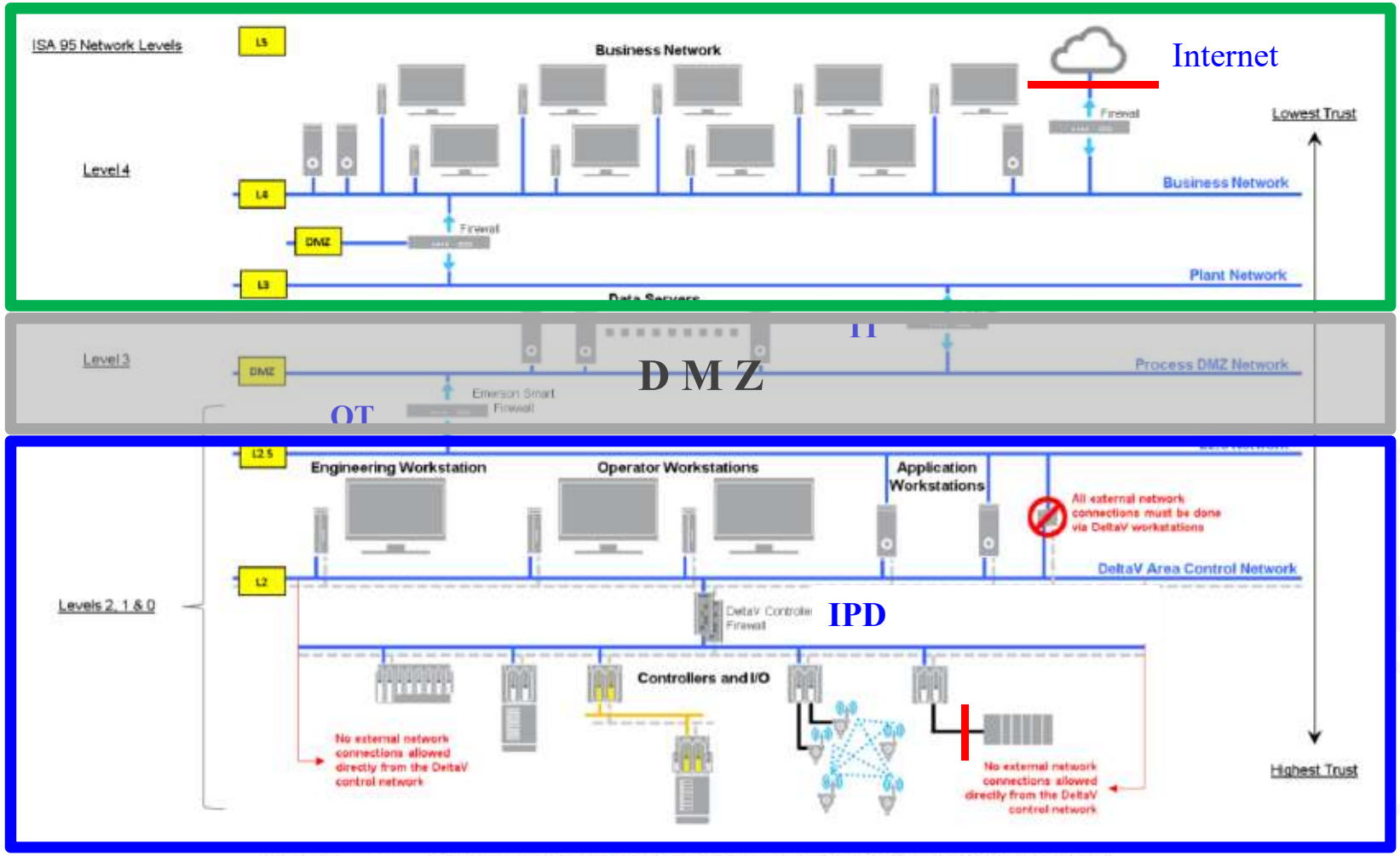
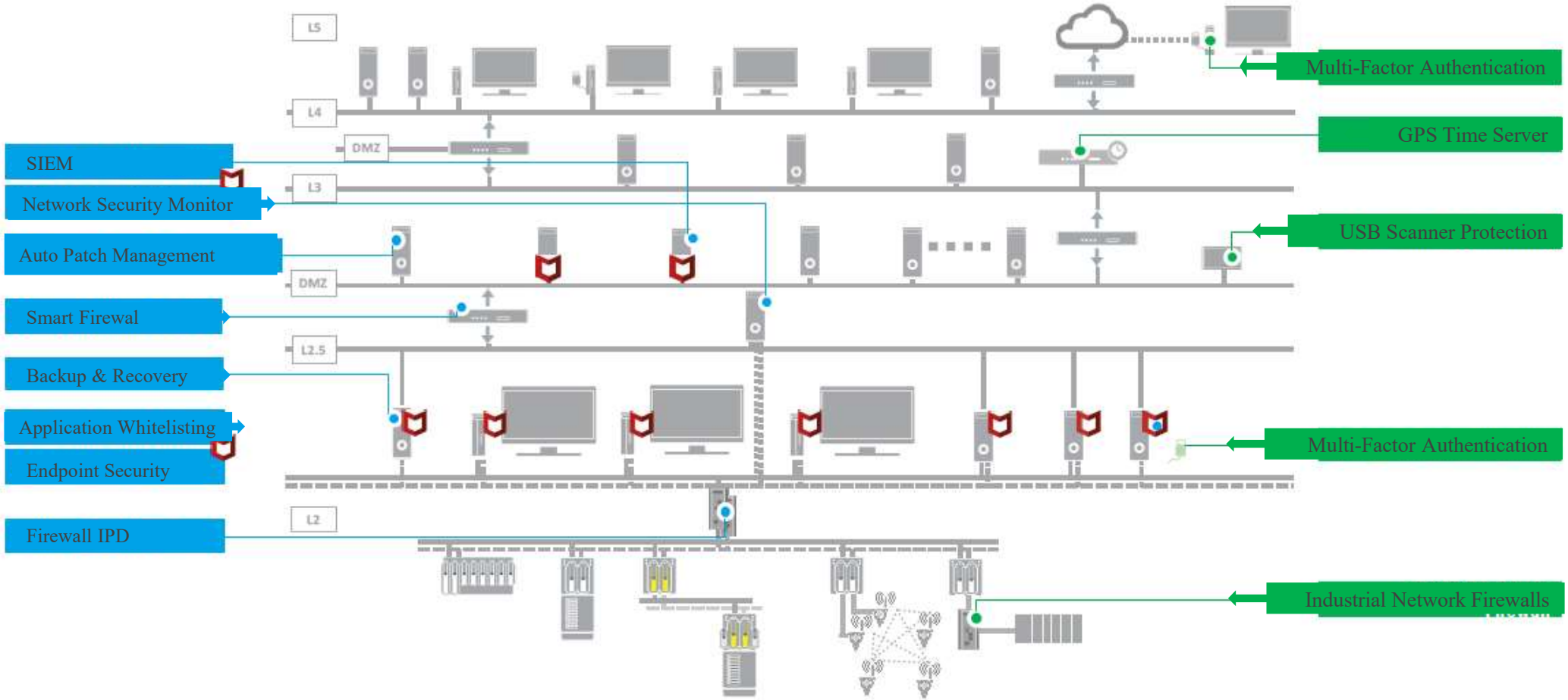


Figure 3 – Reference Architecture with references to the ISA95 / Purdue Reference Model

Reference Architecture with OT Cybersecurity Recommended Solutions



ENDPOINT SECURITY / ANTIVIRUS

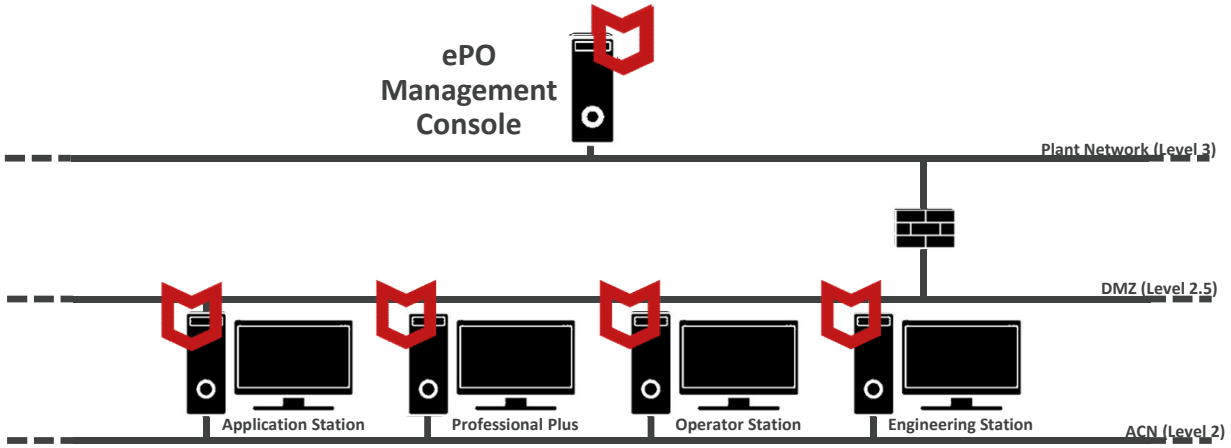
COMMON CHALLENGES

- Lack of malware protection
- Compliance with new cyber policies
- Proactively securing your system against millions of known threats

KEY PROTECTION

- **Known threat** scanning and detection
- **Centralized management** from ePO console (unmanaged mode available)
- Detected malware **auto-quarantined**

Antivirus with Managed Architecture Design



Known threats:
- ✓ WannaCry
- ✓ NotPetya
- ✓ Shamoon
- ✓ Stuxnet
- ✓ Cryptolocker
- ✓ Slammer
- ✓ etc

Blacklisting protects against KNOWN threats

Requires regular patching!

Antivirus Protection

APPLICATION WHITELISTING

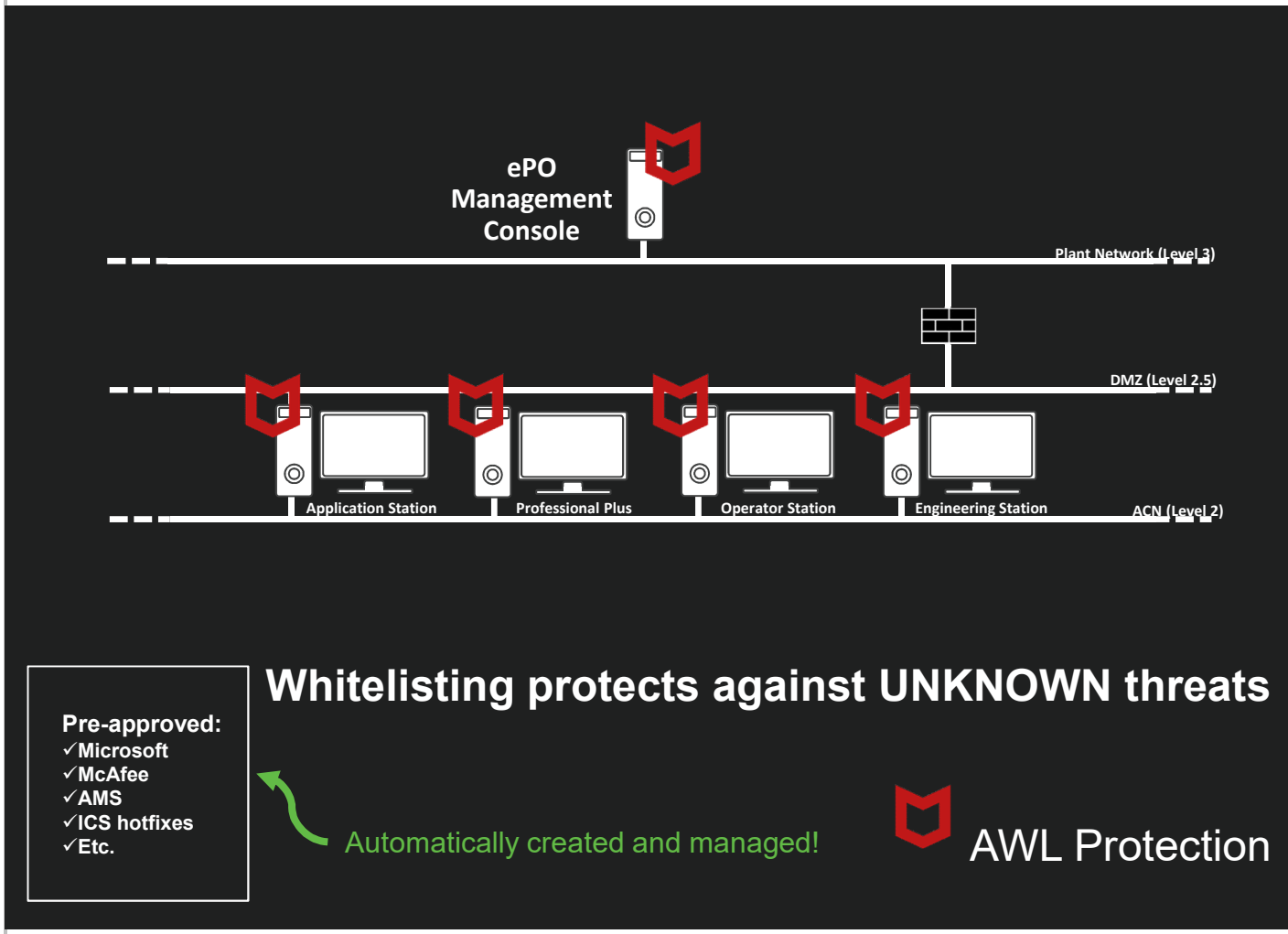
COMMON CHALLENGES

- Signature file update management
- Lag between malware release and signature detection
- Unknown USB contents / applications

KEY PROTECTION

- Protect against **UNKOWN threats** **Automatically whitelist** files from trusted sources
- **Centralized management** from ePO

Application Whitelisting Architecture Design



Block threats without signature updates and stop unwanted applications before they start

AUTOMATED PATCH MANAGEMENT

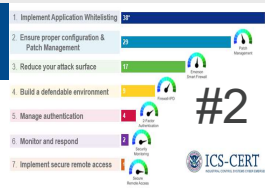
COMMON CHALLENGES

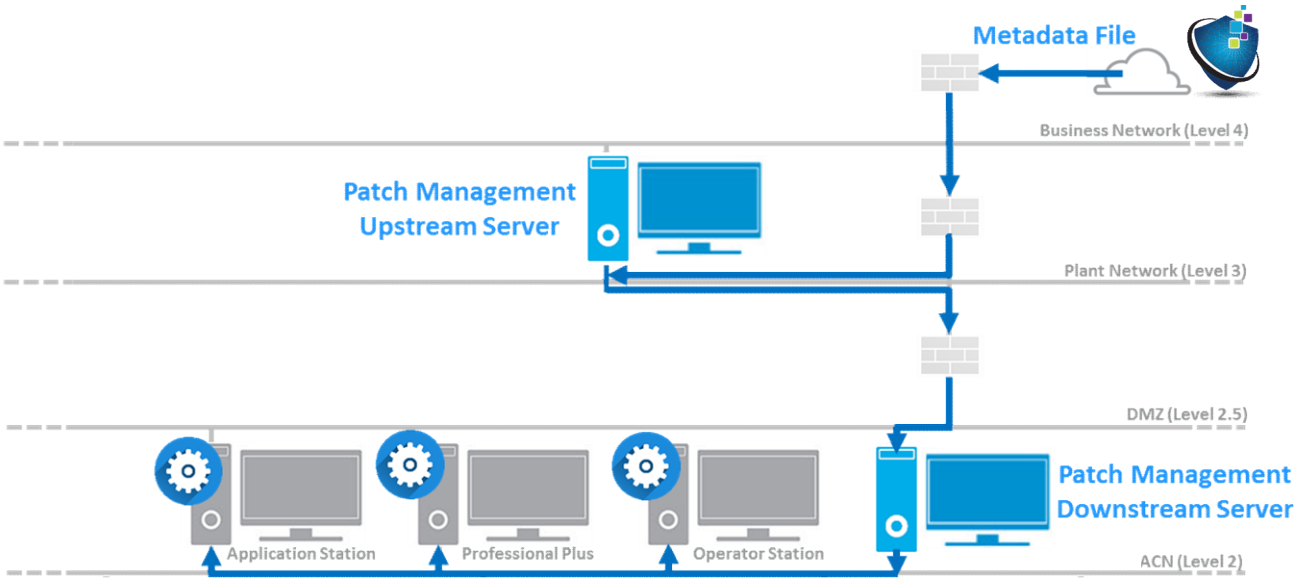
- Time required to manually identify, transfer, and install system patches
- Compliance with new cyber policies
- Proactively securing your system against millions of known threats

KEY PROTECTION

- **Automated** patch matching & delivery
- Significantly **reduced manual effort**
- Patch status auto-updated

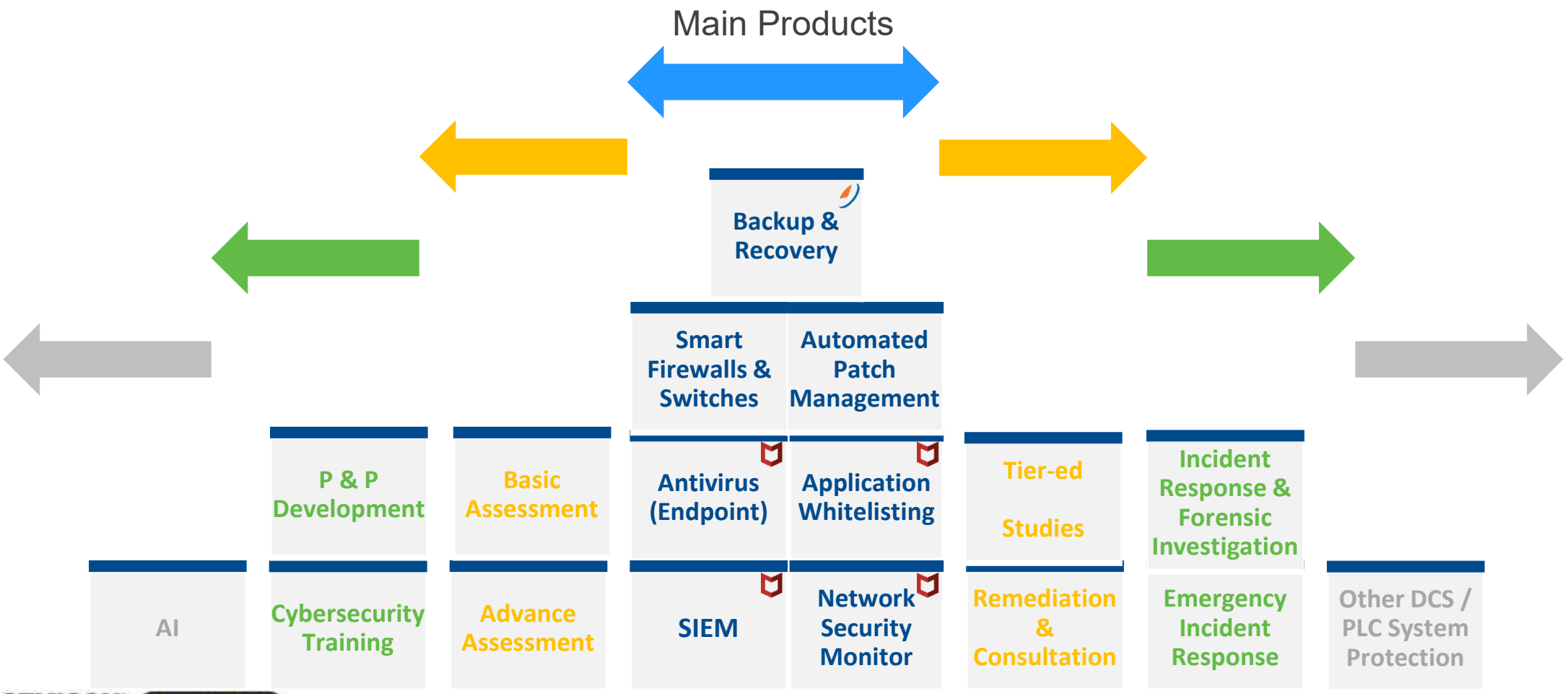
Automated Patchment Architecture Design





Patch Type	System / KBA Matching?	Automated L2 File Delivery?	Automated Install?
FMCS	Yes	Yes	Optional
Windows	Yes	Yes	Yes
Endpoint Security	Yes	Yes	Yes

Horizontal Wide Array – Products | Consultancy | Services | Future

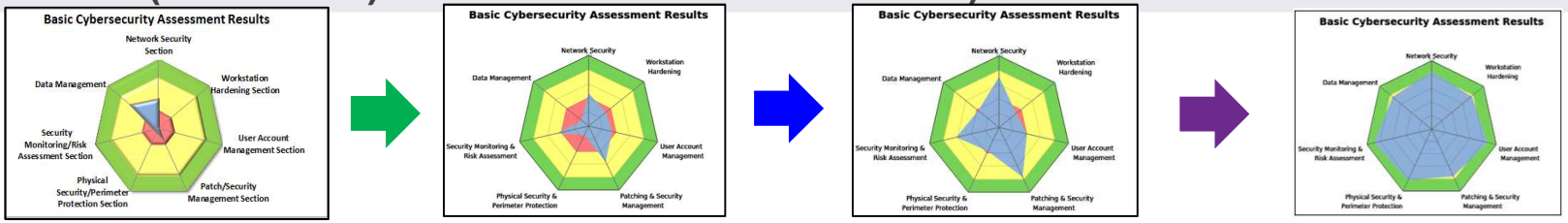


SEMICON TAIWAN HTFC

Ala Carte Options → Start Small → Phase by Phase

Solution	Baseline Assessment	Phase 1 (Must Have)	Phase 2 (Improved)	Phase 3 (Monitoring)
Endpoint, Patch Mgnt		+		
Whitelisting		+		
Firewall*		+		
Auto Patch Mgnt			+	
Backup & Recovery			+	
SIEM				+
NSM				+
Others (Consultation / ICSP (Blue Coat) / Two Factor Authentication)				

Cybersecurity Journey



Step-by-Step
ASSESS → SOLUTION(S) → IMPROVE

Basic Cybersecurity Assessment

Executive Summary:

Cybersecurity risk assessments are conducted to ensure that proper security safeguards are present in the DeltaV system. The following radar chart graphically shows an overview of the cybersecurity readiness results for this system/site. The closer the blue plot area is to the outside edge of each of the 7 key element vectors, the better the results were for that assessment section. From this chart, it should be clear which of the report elements any initial remediation focus should be on.

Round Rock Refining

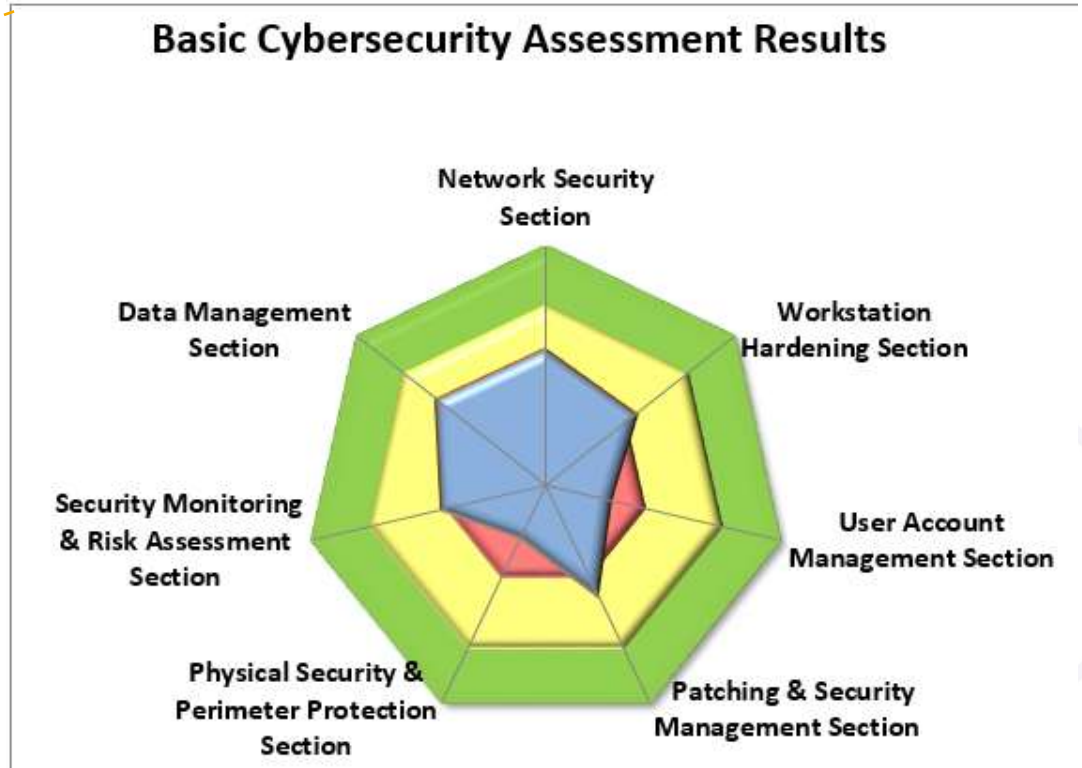
System ID: (0001-000x-xxxx)

February 21, 2017

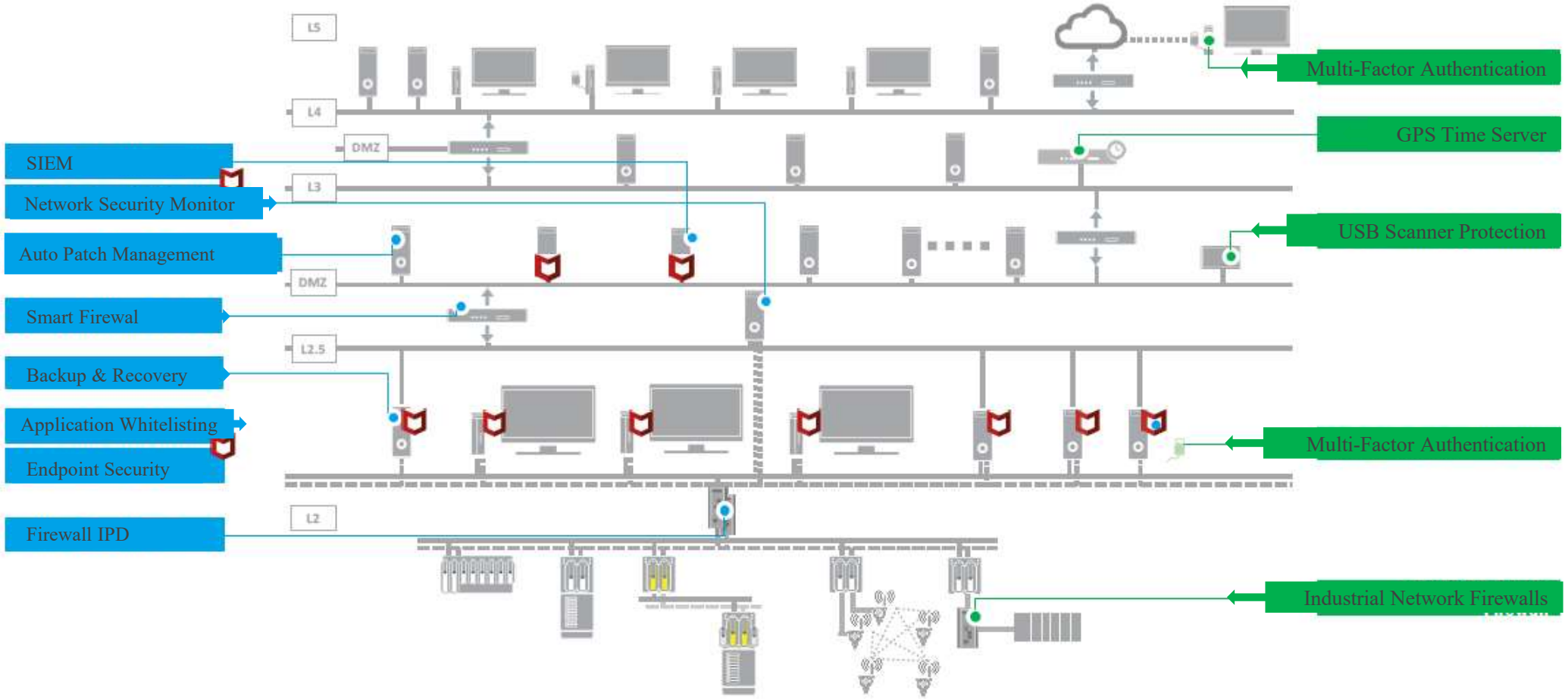
Overall Evaluation:

- **Positive:** *Good results evaluation. Continue to monitor.*
  - N/A
- **Neutral:** *Results are marginal. We suggest Round Rock Refining evaluate each recommendation and implement accordingly.*
  - Network Security
  - User Account Management
  - Patching & Security Management
  - Physical Security & Perimeter Protection
- **Concerning:** *Results are of concern. We suggest Round Rock Refining evaluate each recommendation as a Priority and implement accordingly.*
  - Security Monitoring & Risk Assessment
  - Workstation Hardening
  - Data Management

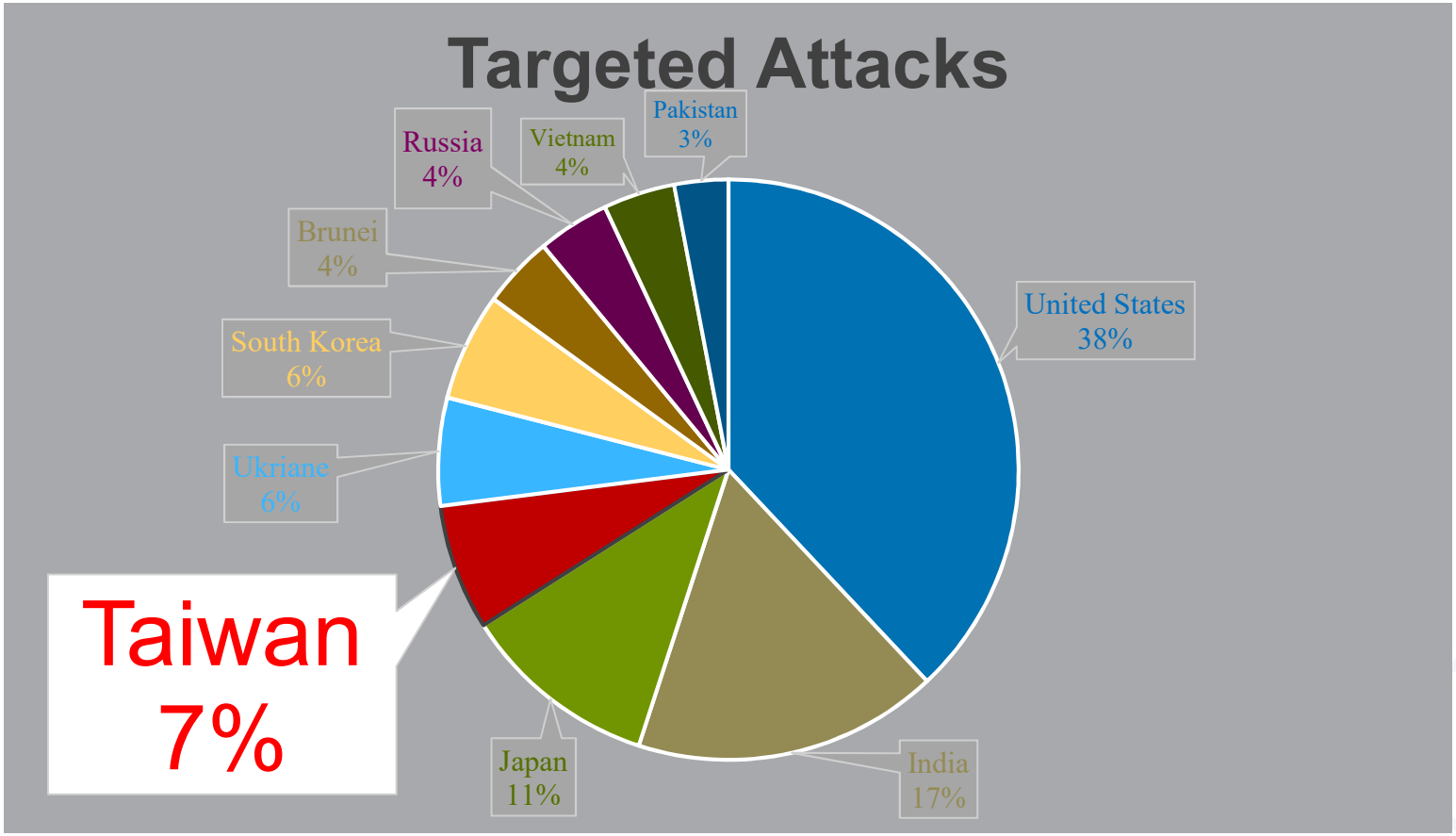
Page 3 of 23



Reference Architecture with OT Cybersecurity Recommended Solutions



CYBER WAR



CYBER Secure