The PMC Group LLC

Engineering a better tomorrow today

ISSA
Information Systems Security Association
National Capital Chapter

DoD Cybersecuring Facility-Related Control Systems

Michael Chipley, PhD GICSP PMP
President

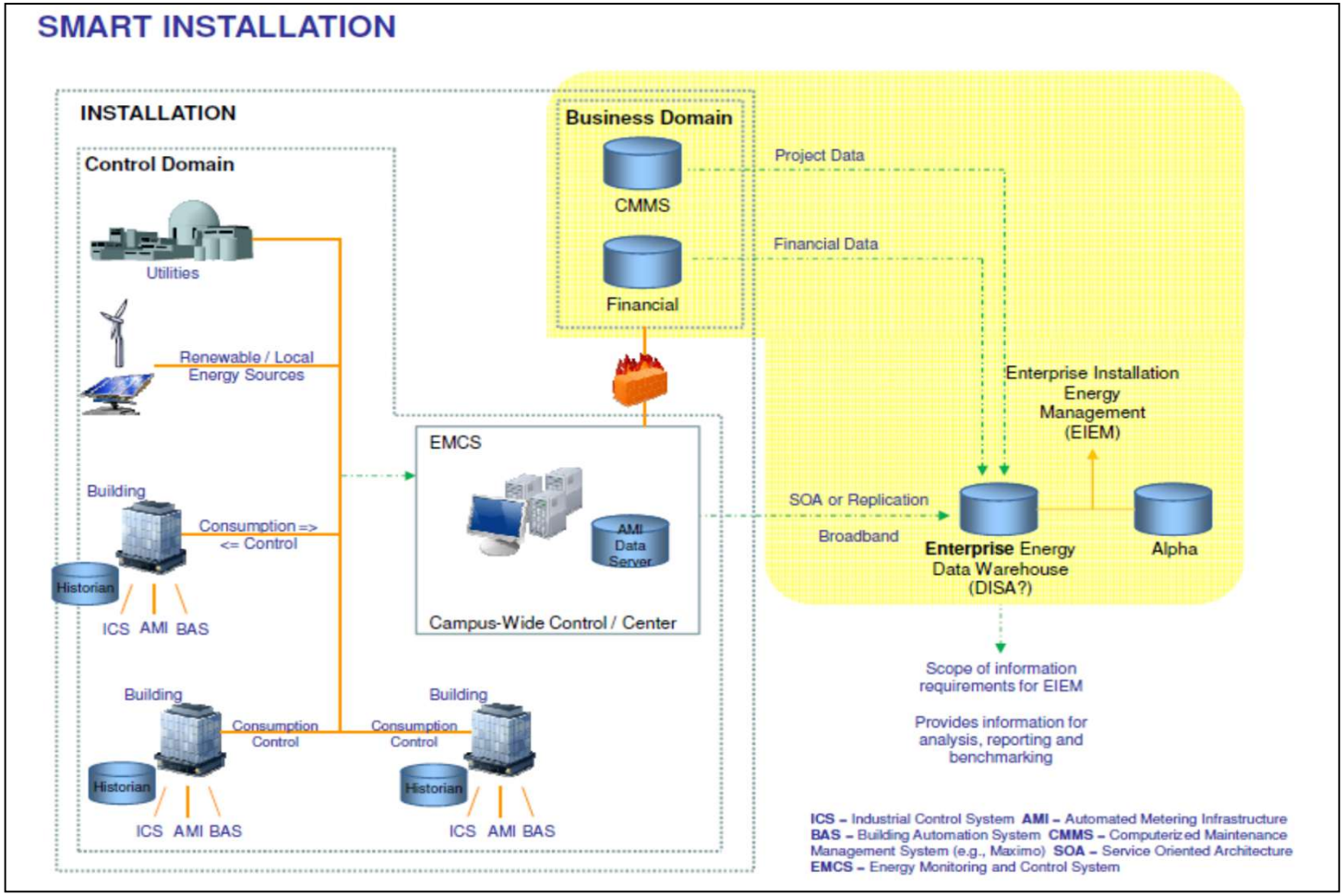
mchipley@outlook.com

February 20, 2025

Abstract

Over the past decade, the DoD has implemented Cybersecuring Facility-Related Control Systems to protect these Critical Infrastructure systems from adversaries and malicious actors. This presentation will review the history of how the program came to be and some key milestones such as the release of the first Cybersecurity Design Unified Facility Criteria, the first Construction Unified Facility Guide Specification, and the need for qualified Cybersecurity Subject Matter Experts and Specialists. **The session will provide hands on examples of the types of control systems, how the design criteria and construction specifications are used, and what the Cyber Team does to include provisioning and hardening the components and devices, capturing the Configuration Baseline Audit Report and Artifacts, and preparing the Cyber Submittals to obtain an Authority To Operate.** Similar to many of the ISSA activities for IT systems, the Control Systems now use traditional IT components and devices and the NIST SP 800-53, but now use NIST SP 800-82 to address the unique challenges of securing Operational Technologies such as Combined Heat Power Plants, Microgrids, HVAC, Fire, Lighting and Electronic Security Systems. ISSA members looking to expand their skill sets and become an OT Cyber Specialist will find a number of opportunities awaiting, this session is the introduction to get you started on the path to becoming a Cyber Warrior.

In the Beginning – Smart Installations



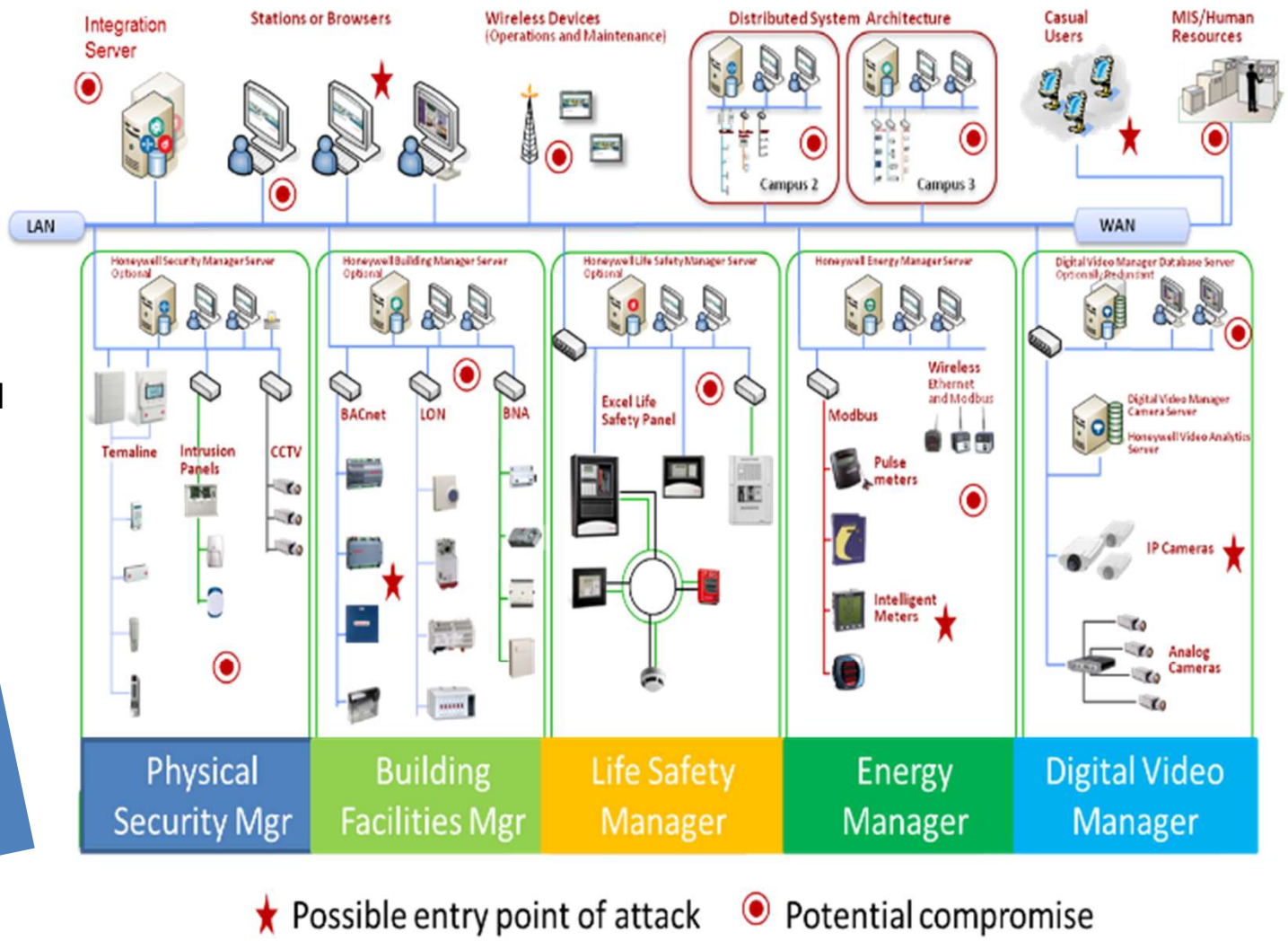
A great idea rudely interrupted by reality…CIO AMI ATO denial,… Stuxnet attack on Iranian Centrifuges, Flame, Duqu, Shamoon….

DoD Building FRCS

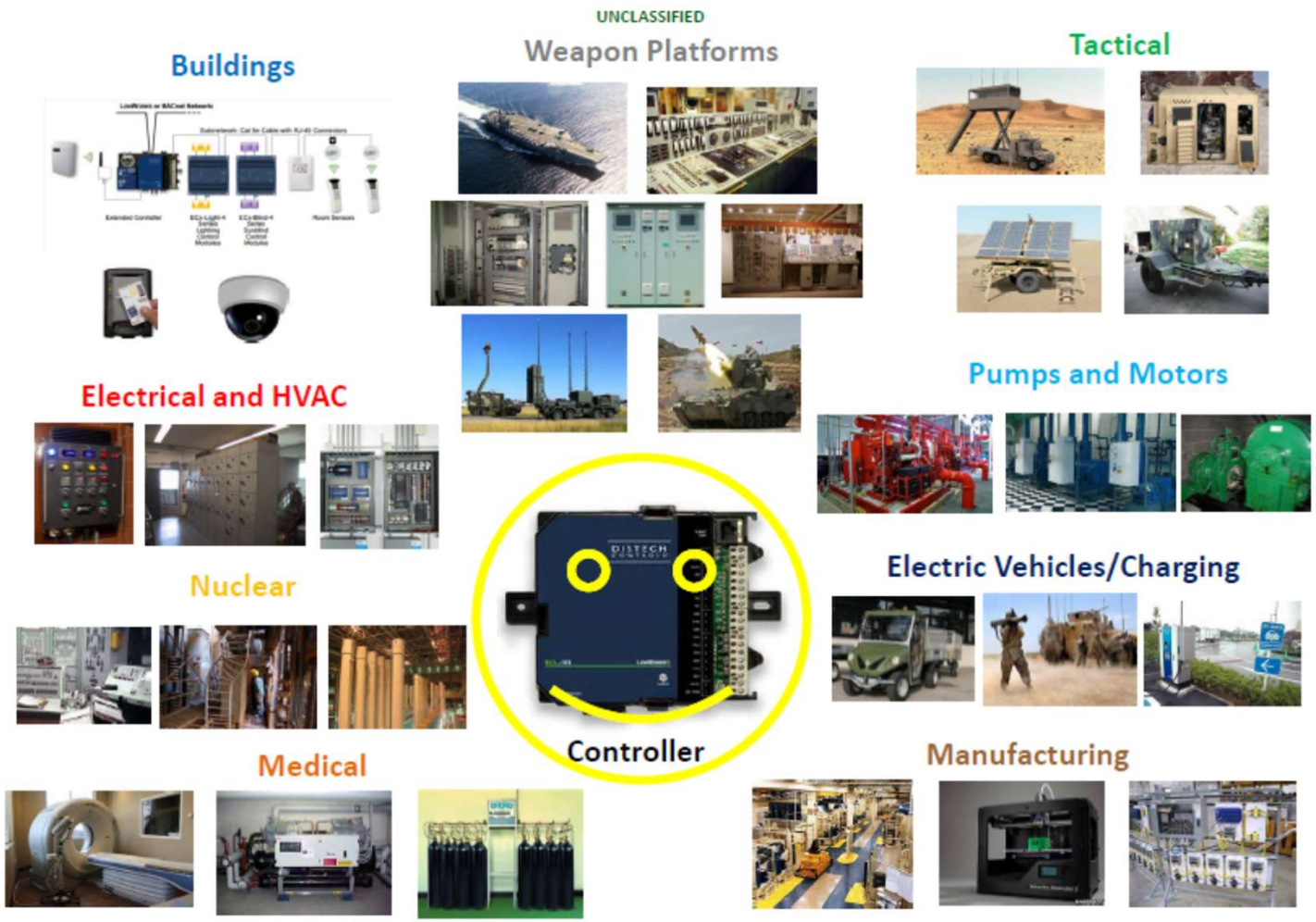
DoD
Real Property
Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- $847 B value

What's in Your Building?

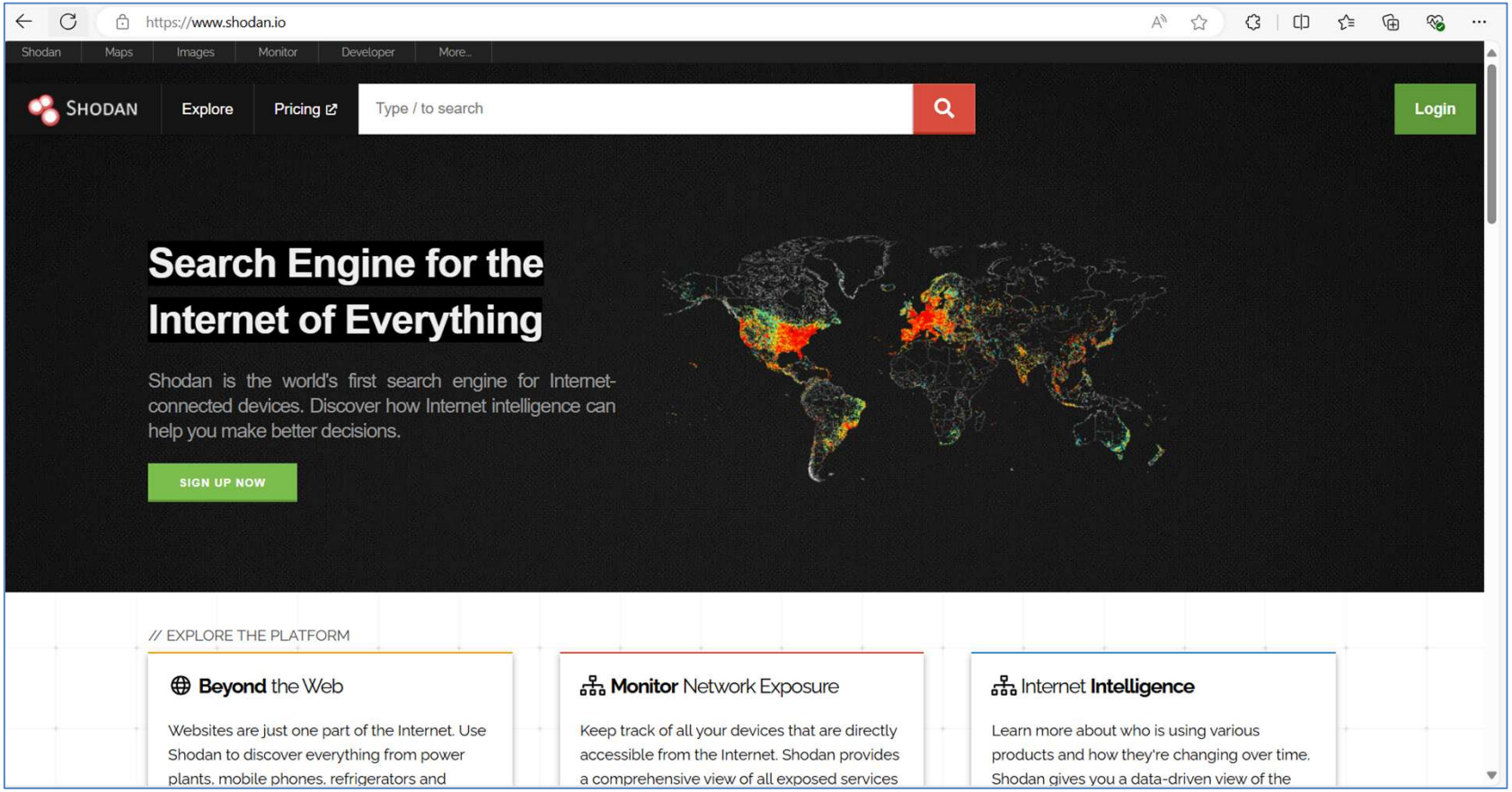


OT IP Based Controllers Are in Everything



Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

Shodan



Our joint job is to make sure no DoD Systems show up on Shodan

[Shodan Search Engine]

Shodan Rockwell Bradley

https://www.shodan.io/search?query=rockwell+bradley

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | rockwell bradley | Login

TOTAL RESULTS

6,466

TOP COUNTRIES

United States	4,378
Canada	575
Spain	239
Italy	170
Australia	146

More...

TOP PORTS

44818	6,433
2003	4
2004	3
502	2

View Report | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

107.84.240.246 2024-09-05T20:28:44.885487

AT&T Mobility LLC

United States, Lincoln

ICS

```
Product name: 1769-L24ER-QBFC1B/A LOGIX5324ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0xc01b8175
Device type: Programmable Logic Controller
Device IP: 192.168.1.10
```

166.136.164.19 2024-09-05T12:47:42.346602

mobile-166-136-164-019.mycingular.net

Wireless Data Service Provider Corporation

United States, Glendale

ICS

```
Product name: 1766-L32AWA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0xd050d191
Device type: Programmable Logic Controller
Device IP: 192.168.100.2
```

63.46.1.66 2024-09-05T12:19:42.745040

host66.sub-63-46-1.myvzw.com

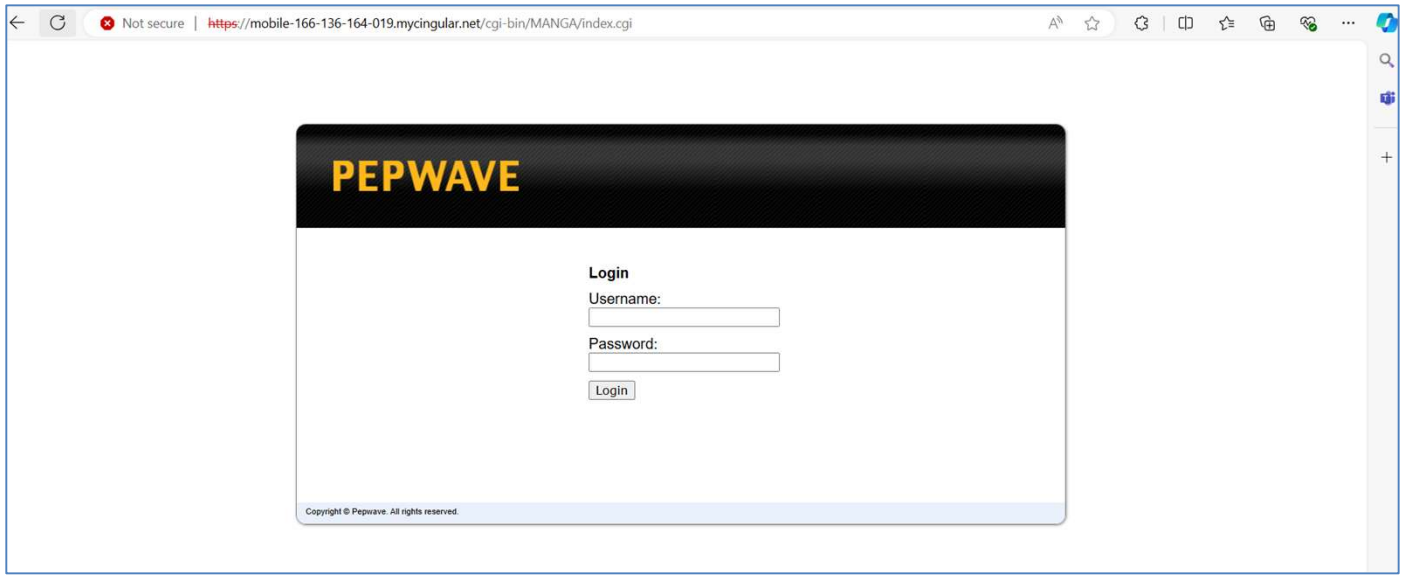
Verizon Business

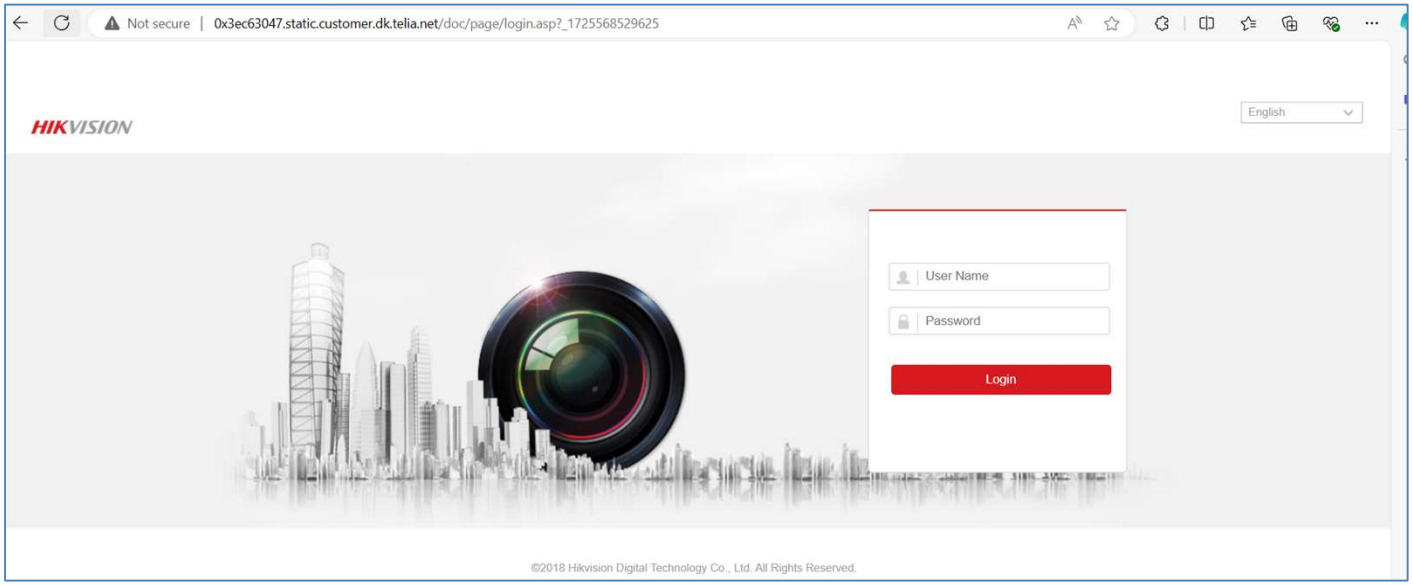
United States, Baldwin

ICS

```
Product name: 1766-L32BXBA C/21.07
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60f099c9
Device type: Programmable Logic Controller
Device IP: 192.168.13.100
```

Shodan HMI Logins





Shodan DoD

192.63.80.11

syn-192-063-080-011.res.spectrum.com

Charter Communications

United States, Killeen

eol-os self-signed

SSL Certificate

Issued By:

|- Common Name:

HOODRRMWRSPR04

Issued To:

|- Common Name:

HOODRRMWRSPR04

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:

RFC2409/Oakley Group 2

Vulnerabilities

BlueKeep

2024-09-05T17:23:36.596250

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\t\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: HOODRRMWRSPR04
  NetBIOS Domain Name: HOODRRMWRSPR04
  NetBIOS Computer Name: HOODRRMWRSPR0...
```

152.179.117.114

Internet-gw.customer.alter.net

Verizon Business

United States, Jessup

2024-08-29T23:49:50.286343

```
CC
#######################################################################
THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM. ALL DOD
INTEREST COMPUTER SYSTEMS AND RELATED EQUIPMENT ARE INTENDED FOR
COMMUNICATION, TRANSMISSION, PROCESSING, AND STORAGE OF OFFICIAL U.S. GOVERNMENT
...
```

65.199.61.70

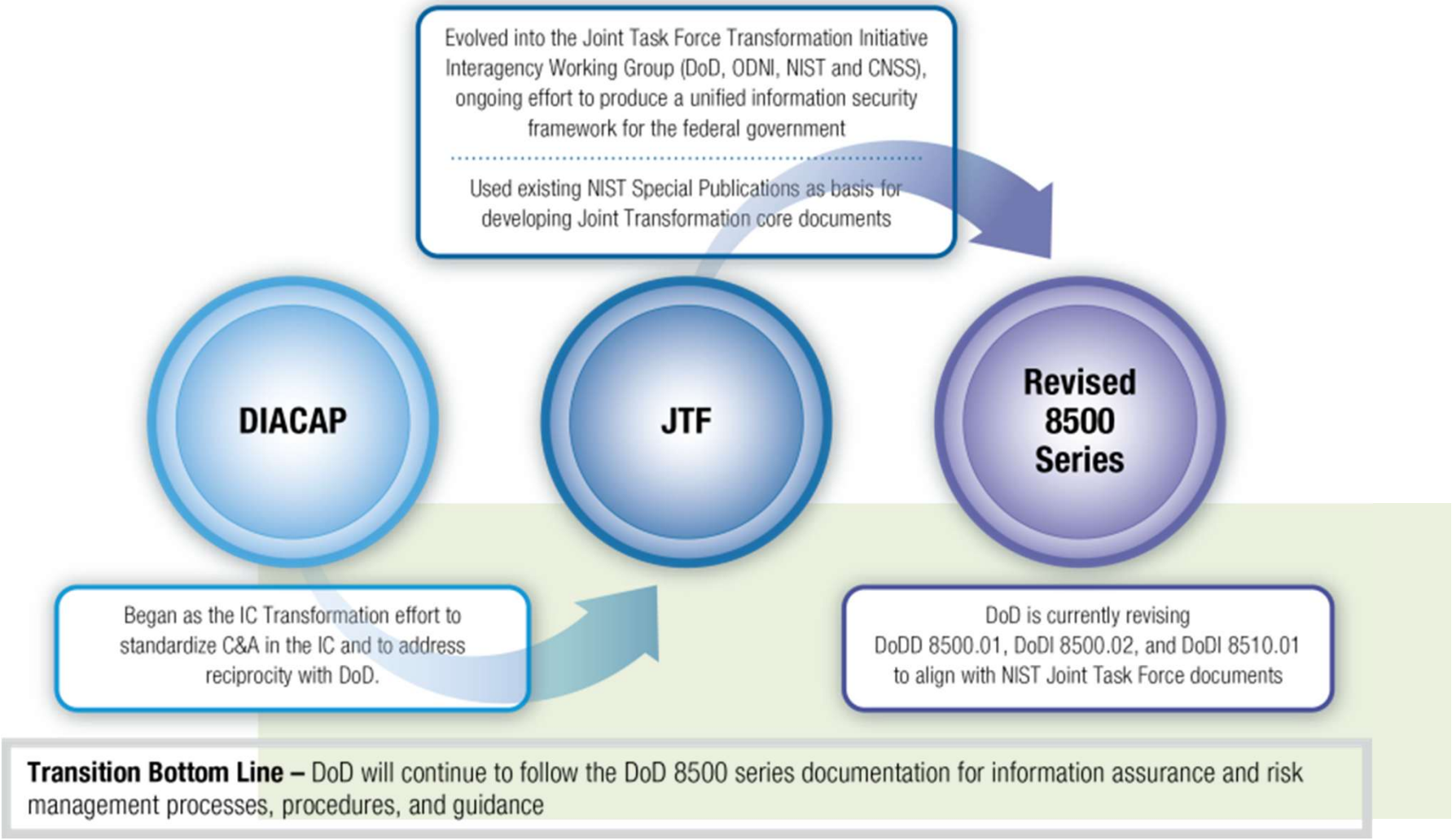
Verizon Business

United States, Washington

2024-08-29T15:03:16.956223

```
CC
#######################################################################
THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM. ALL DOD
INTEREST COMPUTER SYSTEMS AND RELATED EQUIPMENT ARE INTENDED FOR
COMMUNICATION, TRANSMISSION, PROCESSING, AND STORAGE OF OFFICIAL U.S. GOVERNMENT
...
```

DoDI 8500.01 and 8510.01 Update



8500 PIT Cybersecurity Considerations

(2) PIT

(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (ah) for PIT cybersecurity requirements.

(b) Examples of platforms that may include PIT are: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), **buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering,** including associated data transport mechanisms (e.g., data links, dedicated networks).

8500 PIT Systems

(d) PIT Systems

1. Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a **collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support.** PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

DoD Facility-Related Control Systems (FRCS)

Categories

- Airfield Systems
- Building Control System
- Dam, Lock and Levee Systems
- Electronic Security Systems
- Environmental Monitoring
- Fire & Life Safety
- Pier Systems
- Traffic Control Systems
- Transportation & Fueling Systems
- Utility Control Systems
- Utility Monitoring & Control Systems
- Control System Platform Enclave

Systems

- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More…*

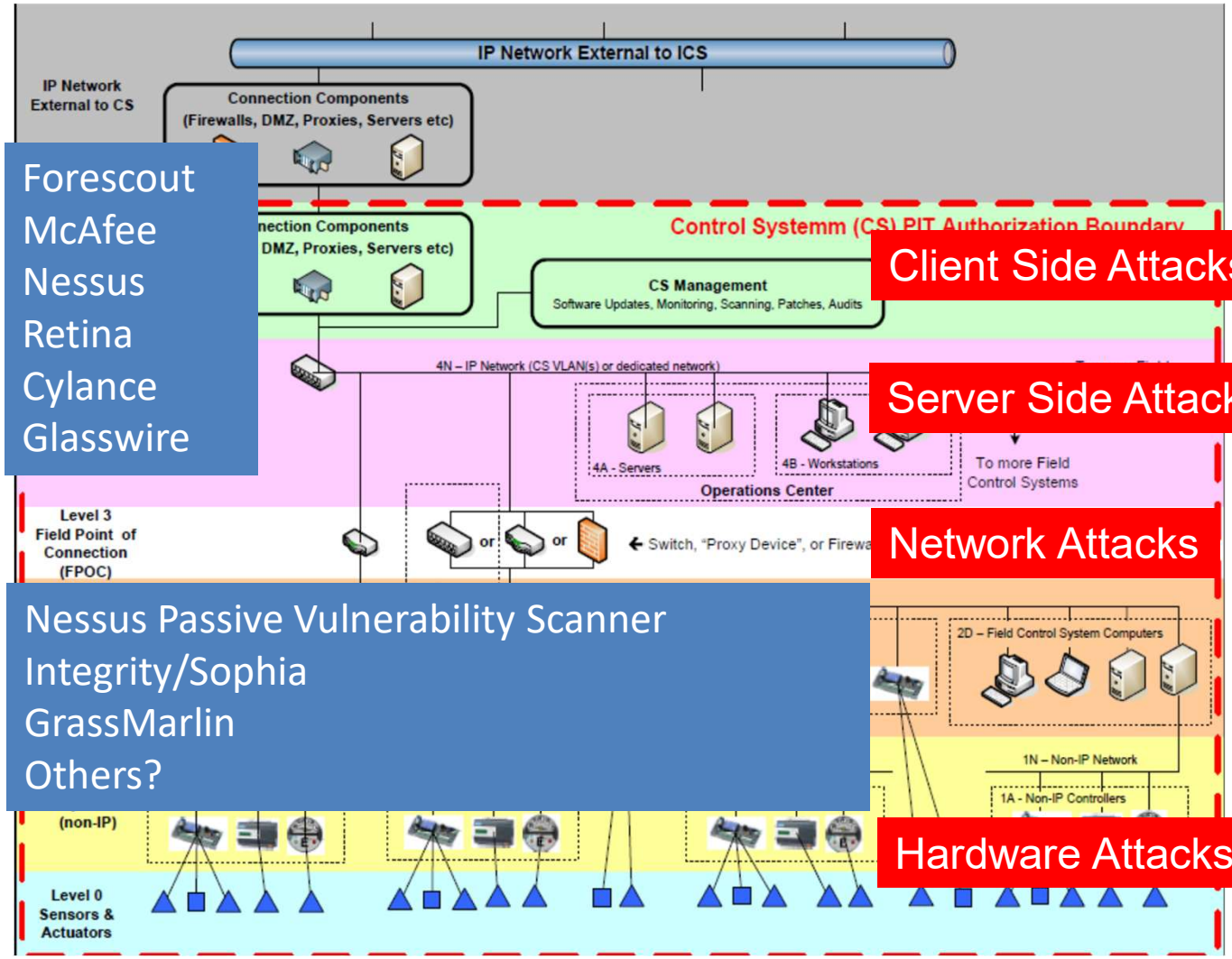
DoD Control Systems are just as vulnerable as industry, how do we protect them?

Continuous Monitoring and Attack Surfaces

Host Based
Security Systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

Intrusion Detection
Systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk,
BACnet, DNP3



Forescout
McAfee
Nessus
Retina
Cylance
Glasswire

Client Side Attacks

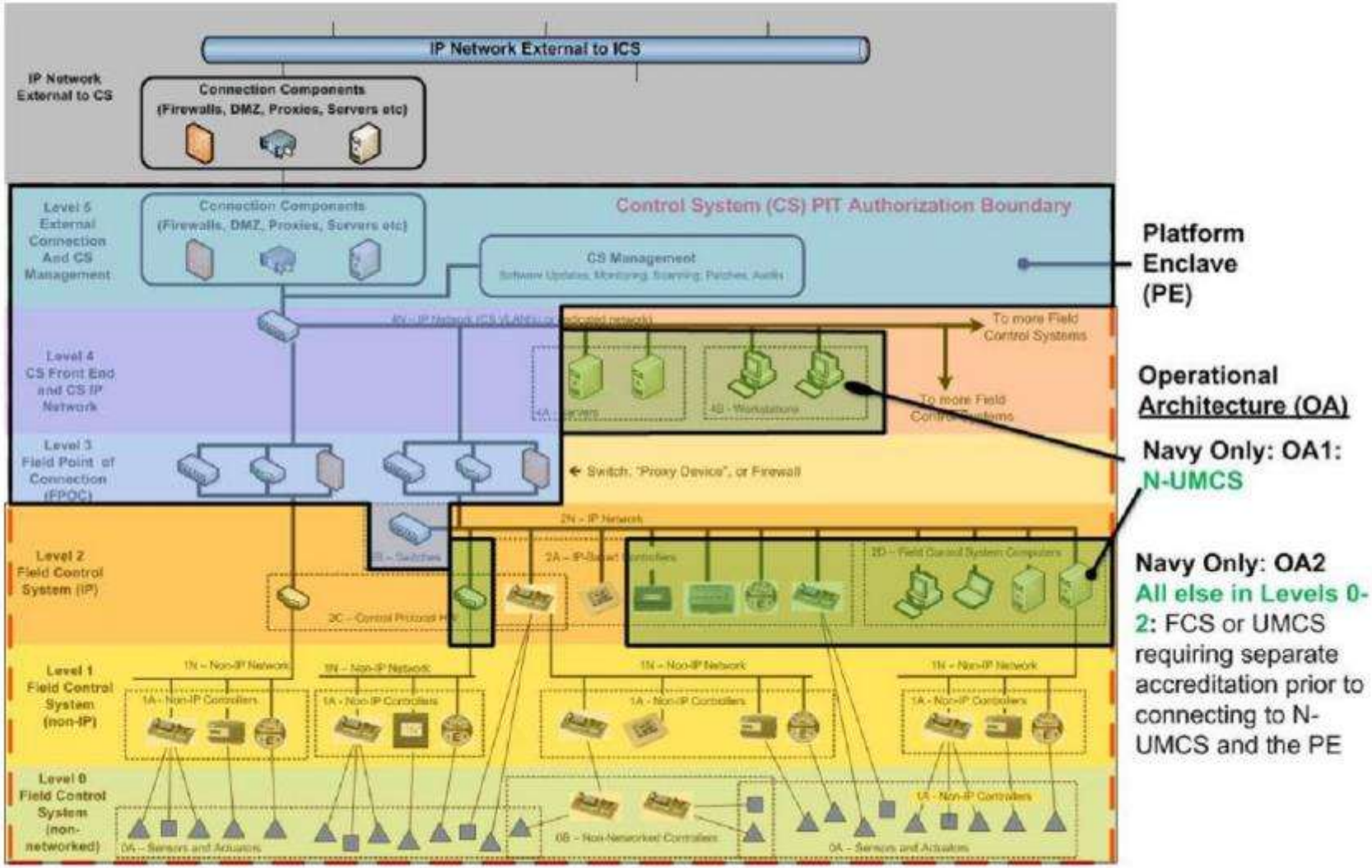
Server Side Attacks

Network Attacks

Nessus Passive Vulnerability Scanner
Integrity/Sophia
GrassMarlin
Others?

Hardware Attacks

DoD UFC 4-010-06 Appendix D



All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the FRCS-PE and NUMCS.

Personnel IAT II Qualifications

DoDM 8570 – Approved IA Baseline Certifications

https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

As an extension of Appendix 3 to the DoD 8570.01-Manual, the following certifications have be approved as IA baseline certifications for the IA Workforce. Personnel performing IA functio must obtain one of the certifications required for their position category or specialty and level

Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
	CCNA Security	CASP+ CE
A+ CE	CySA+ **	CCNP Security
CCNA-Security	GICSP	CISA
CND	GSEC	CISSP (or Associate)
Network+ CE	Security+ CE	GCED
SSCP	CND	GCIH
	SSCP	CCSP

Cybersecurity Kickoff Meeting

Agenda

- Stakeholder Introductions (AO, AODR, ISSM, ISSO, ISSE, SO)
- Schedule
- BOQ-A Project Overview
- NAVFAC BOQ-A RFP Cyber Requirements
- Six steps of the RMF – UFGS 25-08-11 Navy RMF
- Define platform enclave /authorization boundary (CRN)
- Initiate eMASS registration – Navy Echelon II Business Rules
- Preliminary Categorization (Navy RMF Steps 1&2)
- Select NIST SP 800-82 security controls
- Create the Authorization Strategy Plan (ASP)
- Develop initial System Security Plan (Excel version)
- Develop ISCP, EICP, EIRP, SAP (artifacts)
- Design construction, Test & Development Environment, FAT & SAT / Commissioning, ISSE Checklist, SCAP Scans, Patch Reports, AV/MW Report, SW Keys and Licenses

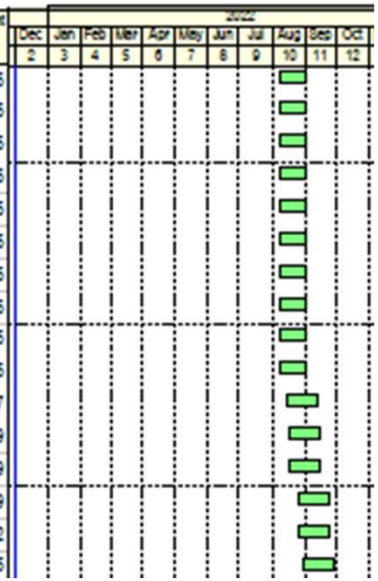
UFGS Div 25 Submittals

- UFGS 25 05 11
  - SD-01 Pre-Construction
  - SD-02 Shop Drawings
  - SD-03 Product Data
  - SD-06 Test Reports
  - SD-07 Certificates
  - SD-11 Closeout
- UFGS 25 08 11.00 20
  - 3.1.1 RMF Step 1 Control System Categorization
  - 3.1.2 RMF Step 2 Security Control Selection
  - 3.1.3 RMF Step 3 Implement Controls
  - 3.1.4 RMF Step 4 Validate Controls
  - SD-01 Pre-Construction
  - SD-05 Design Data
  - SD-06 Test Reports
  - SD-07 Certificates

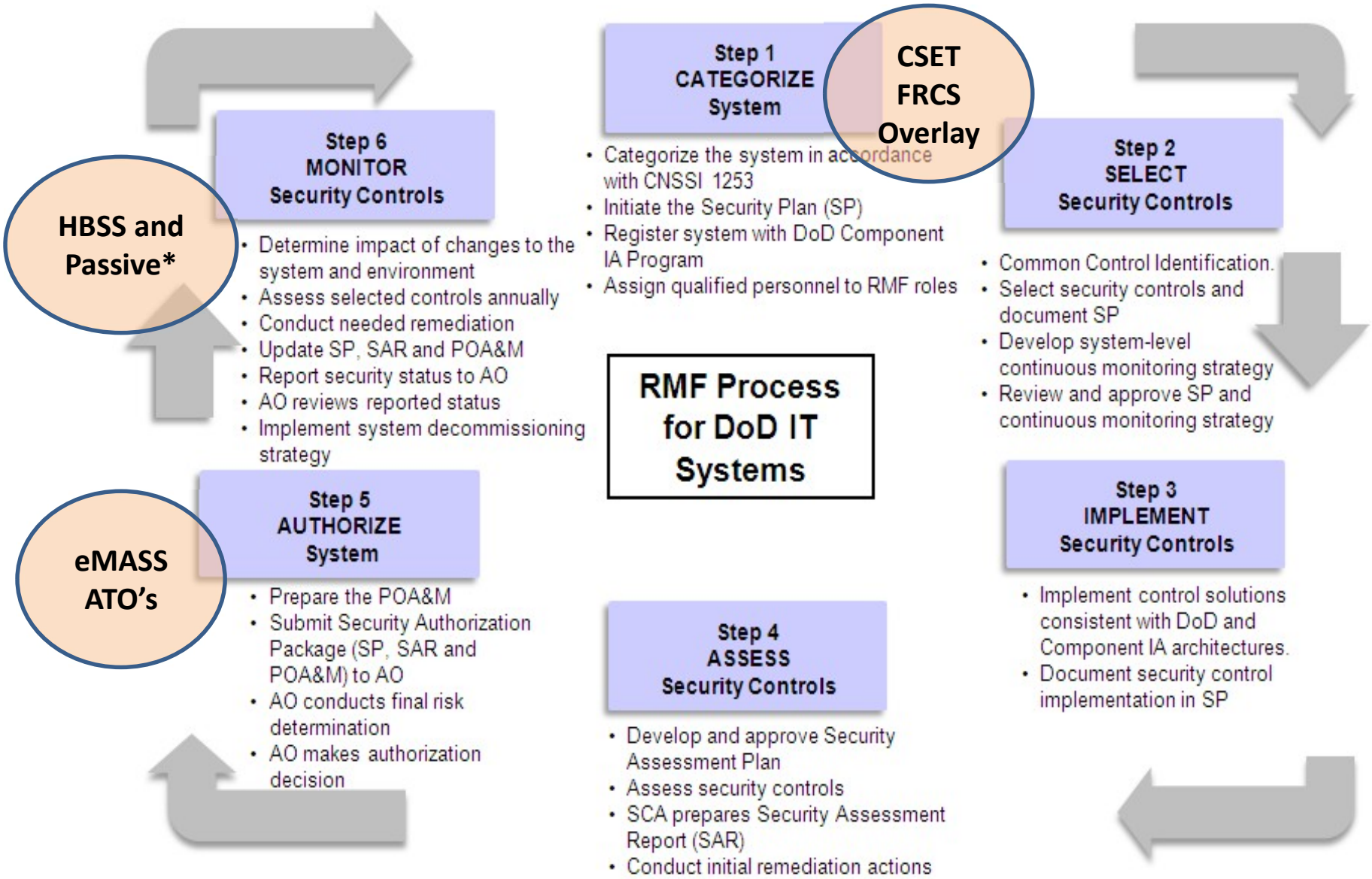
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION	GOVT OR A/E REVWR	CONTRACTOR: SCHEDULE DATES			CONTRACTOR ACTION			
							SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/ DATE RCD FROM CONTR	DATE
(a)	(b)	(c)	(d)	(e)	(f)		(g)	(h)	(i)	(j)	(k)	(l)	
		01 35 13.02	INDUSTRIAL CONTROL SYSTEMS PROCUREMENT										
			SD-03 Product Data										
PCP.SADM-195	0995	1	Network Switches				03/22/22	04/19/22		A	11/06/24	11/06/24	
PCP.SADM-200	0995	2	Media Converters				03/10/22	04/07/22		A	11/06/24	11/06/24	
PCP.SADM-205	0995	3	Uninterruptible Power Supply (UPS)				03/10/22	04/07/22		A	11/06/24	11/06/24	
PCP.SADM-210	0995	4	Remote Terminal Unit (RTU)				03/10/22	04/07/22		A	11/06/24	11/06/24	
PCP.SADM-215	0995	5	Intermediary Network Devices				03/10/22	04/07/22		A	11/06/24	11/06/24	
			SD-10 Operation and Maintenance Data										
		6	Operator Manual	3.5.1	G		09/07/23	10/04/23					
		7	Sustainment Materials	3.5.2	G		09/07/23	10/04/23					
		8	Security Controls Documents	3.5.3	G		09/07/23	10/04/23					
		9	System Authorization Documents	3.5.3.1	G		09/07/23	10/04/23					
		10	Access Controls Summary	3.5.3.2	G		09/07/23	10/04/23					
		11	Auditing Controls Summary	3.5.3.3	G		09/07/23	10/04/23					
		12	Configuration Management Plan	3.5.3.4	G		09/07/23	10/04/23					
		13	Contingency Plan	3.5.3.5	G		09/07/23	10/04/23					
		14	Security Features Guide	3.5.3.6	G		09/07/23	10/04/23					
		15	Vulnerability Management Plan	3.5.3.7	G		09/07/23	10/04/23					
		16	Maintenance Plan	3.5.3.8	G		09/07/23	10/04/23					
		17	Documented Statements	3.5.3.9	G		09/07/23	10/04/23					
		18	Test Results	3.5.3.10	G		09/07/23	10/04/23					
			SD-11 Closeout Submittals										
		21	Technical Narrative	3.7	G		09/07/23	10/04/23					
		22	Completed Navfac Marianas Ics Checklist	3.6	G		09/07/23	10/04/23					
								DIVISION 25 - INTEGRATED AUTOMATION					
		25 05 11	CYBERSECURITY FOR FACILITY - RELATED CONTROL SYSTEMS										
			SD-01 Preconstruction Submittals										
	0072	1	Wireless Communication Request	3.1.6.1	G		07/29/22	08/26/22		A	03/26/22	03/29/22	
	0072	2	Device Account Lock Exception Request	3.1.3.2	G		07/29/22	08/26/22		A	03/26/22	03/29/22	
	0072	3	Multiple IP Connection Device Request	3.9	G		07/29/22	08/26/22		A	03/26/22	03/29/22	
	0072	4	Contractor Computer Cybersecurity Compliance Statements	3.9.1.4	G		07/29/22	08/26/22		A	03/26/22	03/29/22	

Project Schedule

Activity ID	Activity Name	Original Duration	Remaining Duration	Physical % Complete	Start	Finish	Total Float
PCP.RAMT-440	Review and Approve - Electricity Metering	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-445	Review and Approve - Coordinated Power System Protection	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-465	Review and Approve - Lightning Protection System	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-470	Review and Approve - Interior Lighting	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-480	Review and Approve - Television Distribution System	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-490	Review and Approve - Interior Fire Alarm And Mass Notification System	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-590	Review and Approve - Water Utility Distribution Piping	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-302	Review and Approve - Cybersecurity For Facility-Related Control Systems	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-380	Review and Approve - Hydronic Pumps	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-325	Review and Approve - Plumbing, General Purpose	20	20	0%	08-Aug-22	02-Sep-22	56
PCP.RAMT-600	Review and Approve - Sanitary Sewerage	20	20	0%	15-Aug-22	12-Sep-22	47
PCP.RAMT-745	Review and Approve - Building Air Barrier System	20	20	0%	18-Aug-22	15-Sep-22	189
PCP.RAMT-750	Review and Approve - Spray Foam Air Barriers	20	20	0%	18-Aug-22	15-Sep-22	189
PCP.RAMT-245	Review and Approve - Storm Shutters	20	20	0%	26-Aug-22	23-Sep-22	79
PCP.RAMT-695	Review and Approve - Metal Railings	20	20	0%	26-Aug-22	23-Sep-22	52
PCP.RAMT-620	Review and Approve - Exterior Buried Preinsulated Water Piping	20	20	0%	30-Aug-22	27-Sep-22	45



FRCS Overlay & RMF Implementation



Step 1 Categorize the System

USN RMF Information System Categorization Form v1.6				
System Name				
System Acronym				
Version Number				
eMASS Number	Write "N/A" if not registered. For systems registered on SIPR eMASS, write "S-"#			
DITPR ID	Write "N/A" if not registered			
Table 1 - List of RMF Team Members			Table 2 - Additional Considerations	
The personnel listed in the table below are the RMF team members associated with the system being categorized. Additional personnel can be added as required, including Information Owner (IO), joint AO, or others.			In the table below, select the answer from each drop-down list that applies to your system for each question.	
Role	Name	Organization	Classification of System	
PM			Classification of Information	
ISO (if different)			Releasability of Information	
ISSM			Applicable Required Overlays	
User Representative			Any Interconnected Systems/External Services which could elevate impact level?	

Step 2 Select Controls (eMASS)

Exported on 25-Sep-2023 by MICHAEL CHIPLEY

Control / AP Information (read-only)									Latest Test Results (read-only)
Implemented	Hybrid	-	CP-2.1	000443	000443: The organization develops a contingency plan for the information system that identifies essential missions.	The organization being inspected/assessed must clearly and accurately document essential missions for its information system(s). Impact of loss of essential mission functions must be defined using CNSSI 1253. Recommended Compelling Evidence: 1.) Signed and dated contingency plan, referencing essential missions section	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s).	Local	Reference the NLON BCS Contingency Plan with the essential missions section. Compelling Evidence: 1.) Signed and dated contingency plan, referencing essential missions section

Step 3 Implement Controls

TABLE OF CONTENTS

Step 3 Implement Controls

ORG

CORPORATE RISK MANAGEMENT PLAN

SECURITY MONTHLY AUDIT REPORT (SMAR)

CONFIGURATION BASELINE

December 30, 2020

CLIENT

Controlled Unclassified Information (CUI)

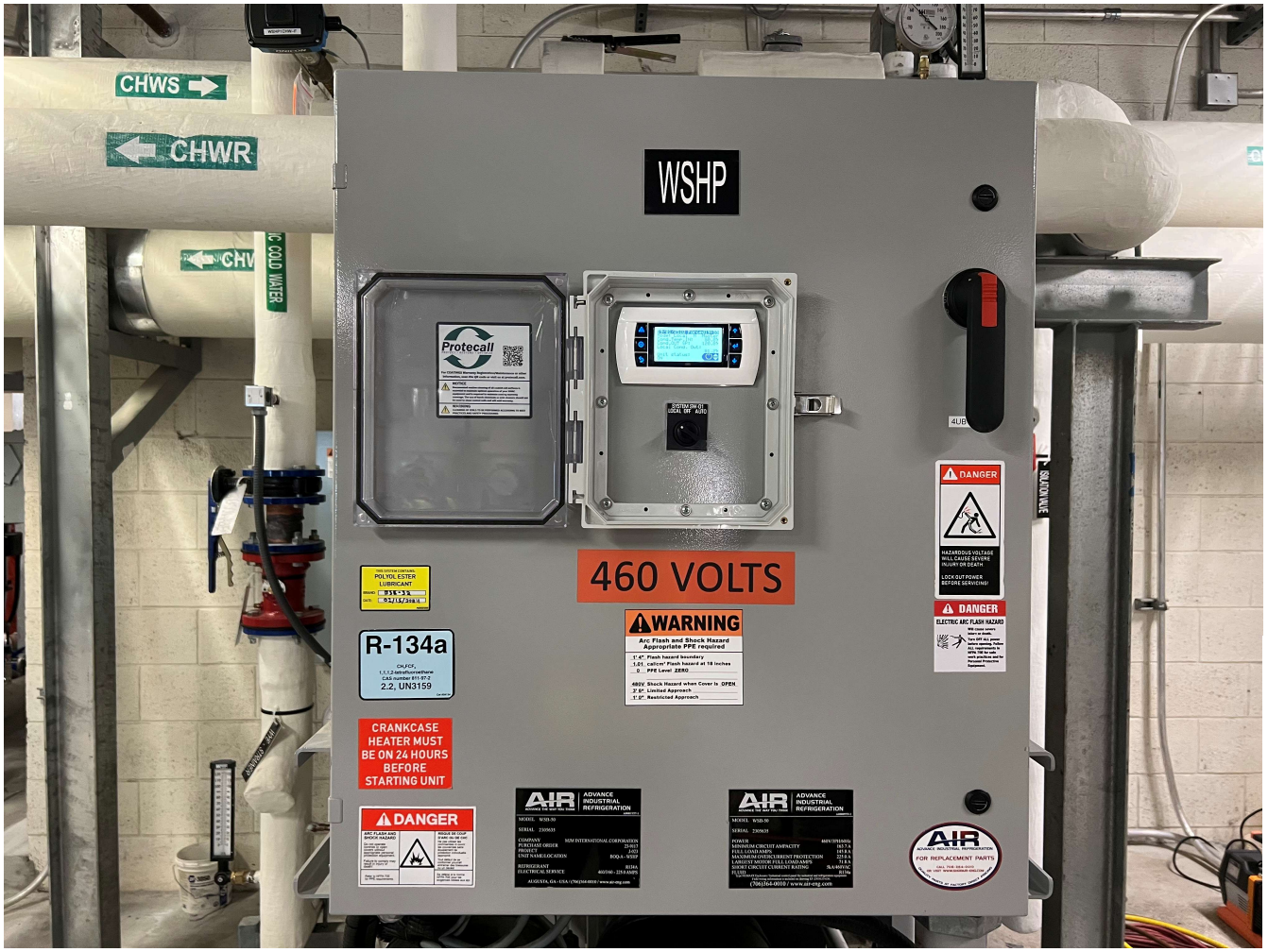
TABLE OF CONTENTS

Configuration Baseline Audit Report

Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS



Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

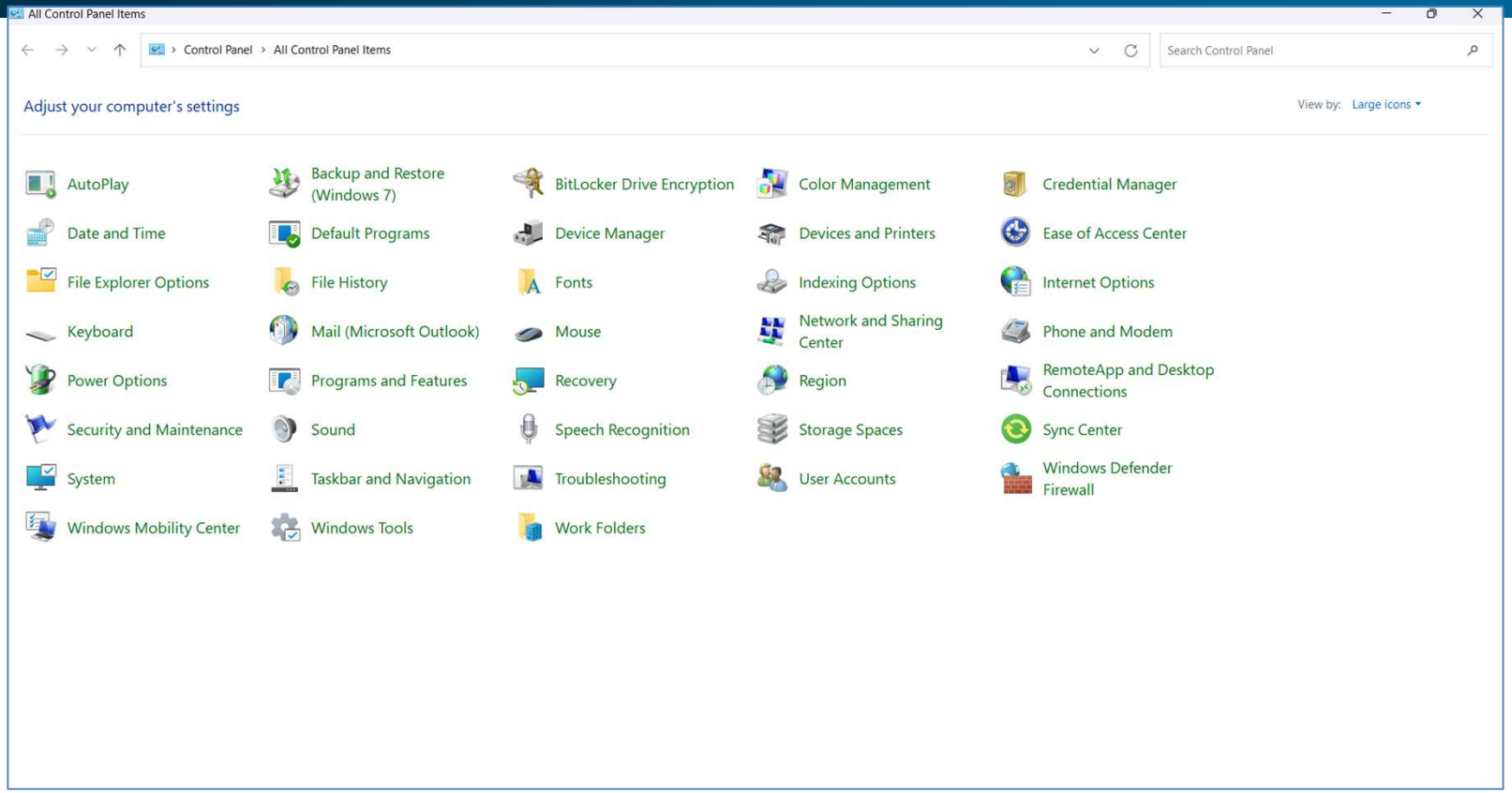
Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

Typical Site Photos of FRCS

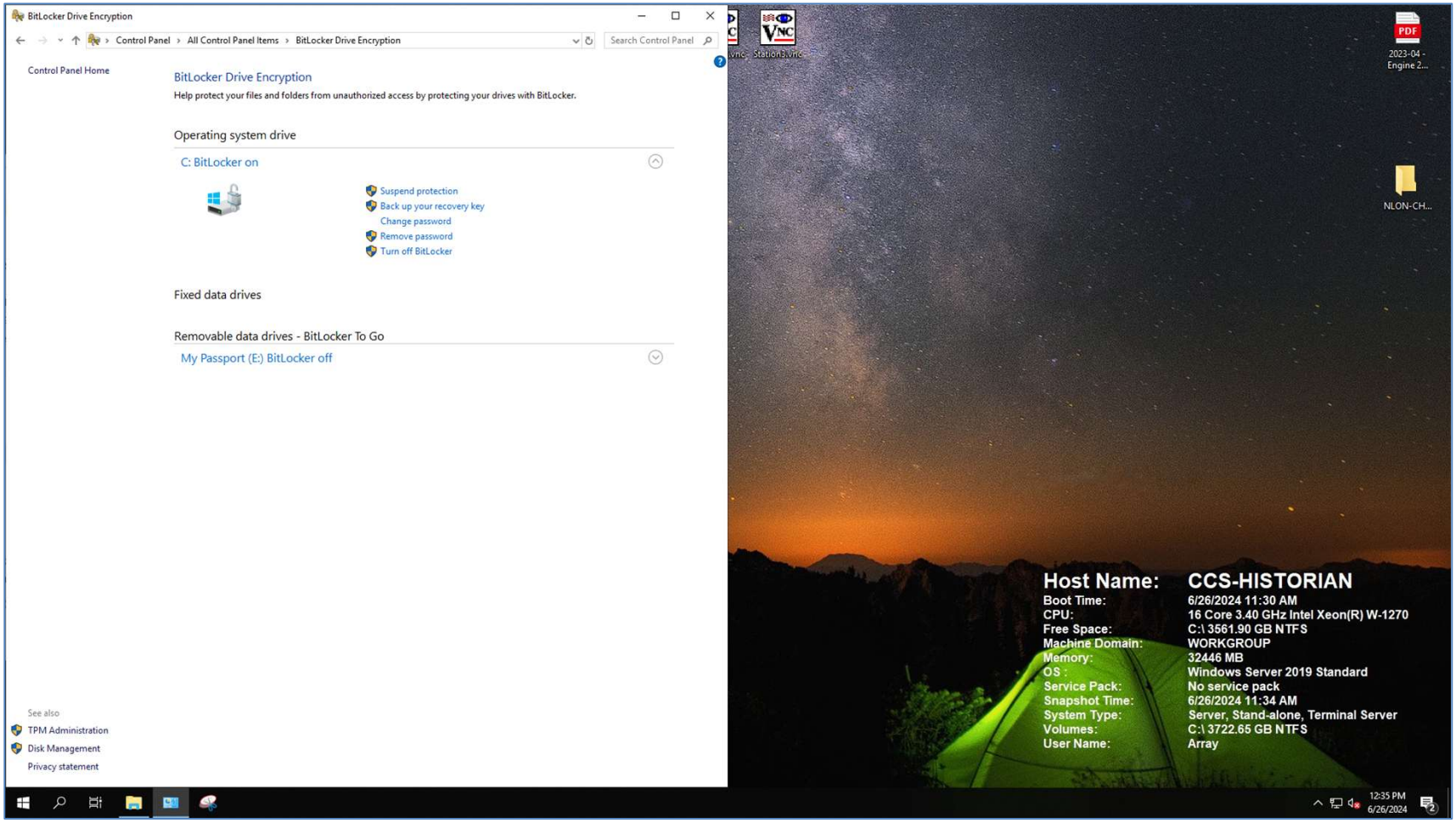
Control Panel



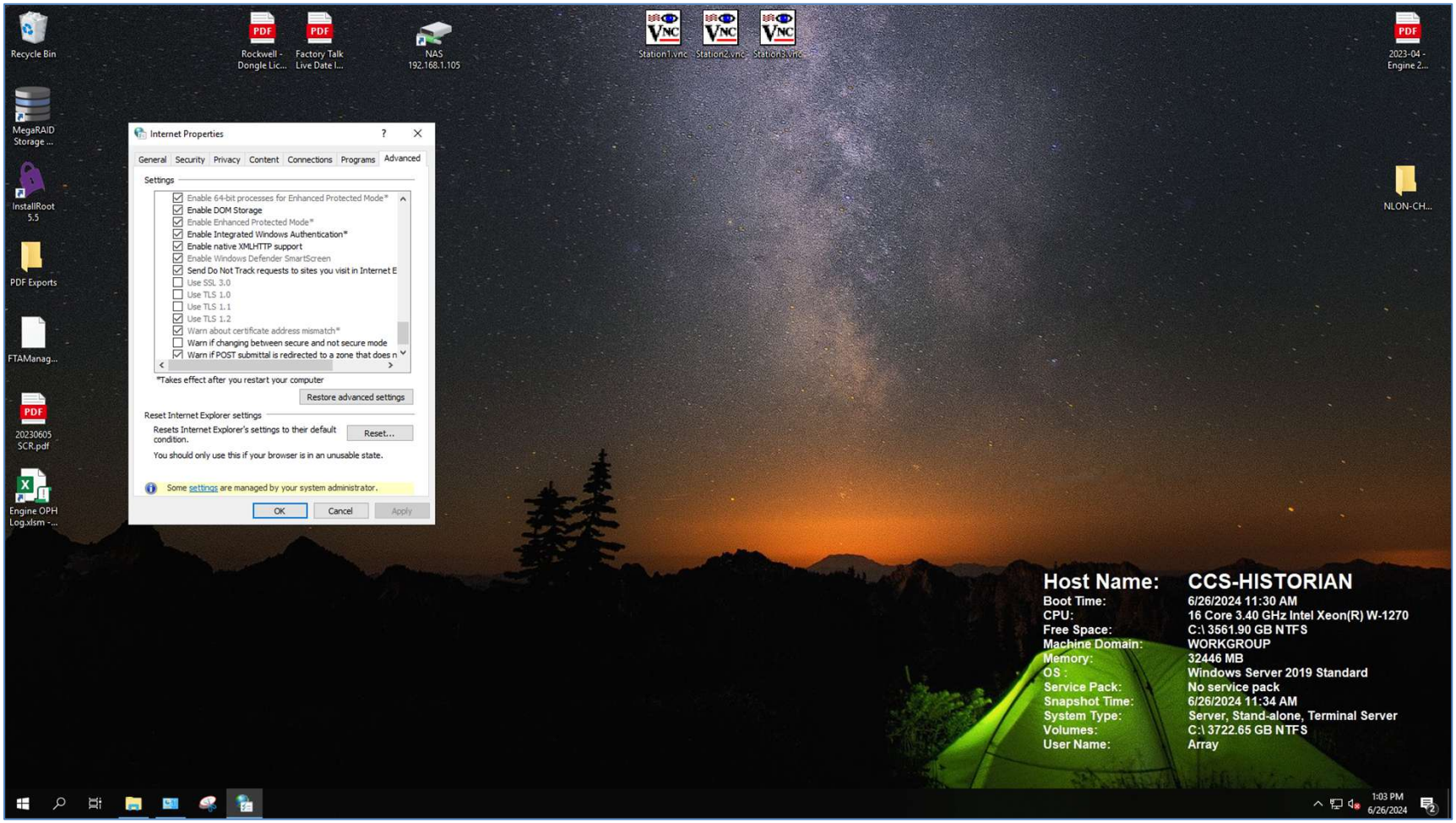
The Control Panel can access 90% of key settings and operations:

- BitLocker Full Disk Encryption Data at Rest
- Transport Layer Settings 1.2 and 1.3 Data Encryption in Transit (web pages)
- Windows Defender Firewall
- Security and Maintenance
- Backup and Retore
- User Accounts

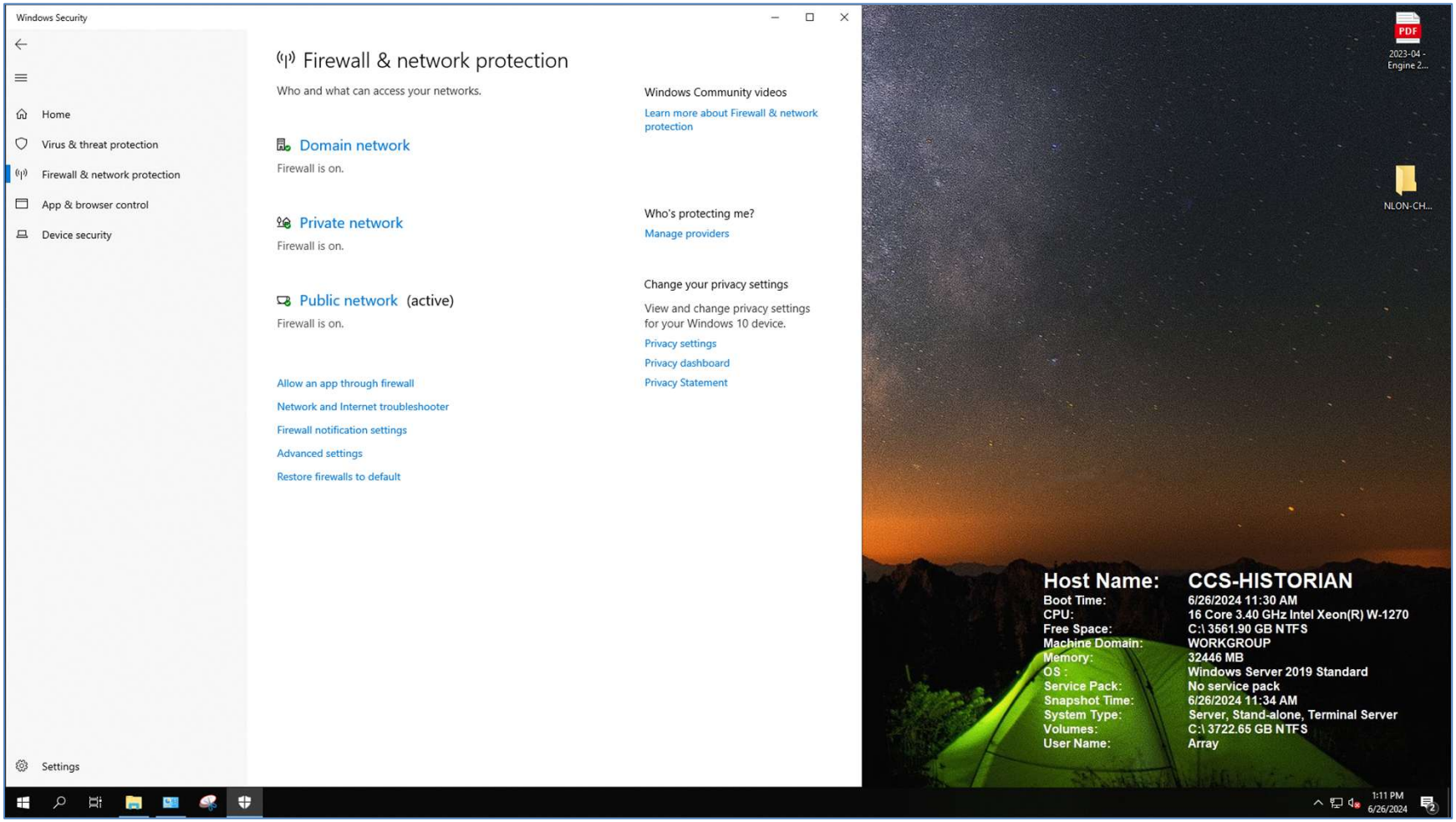
BitLocker On



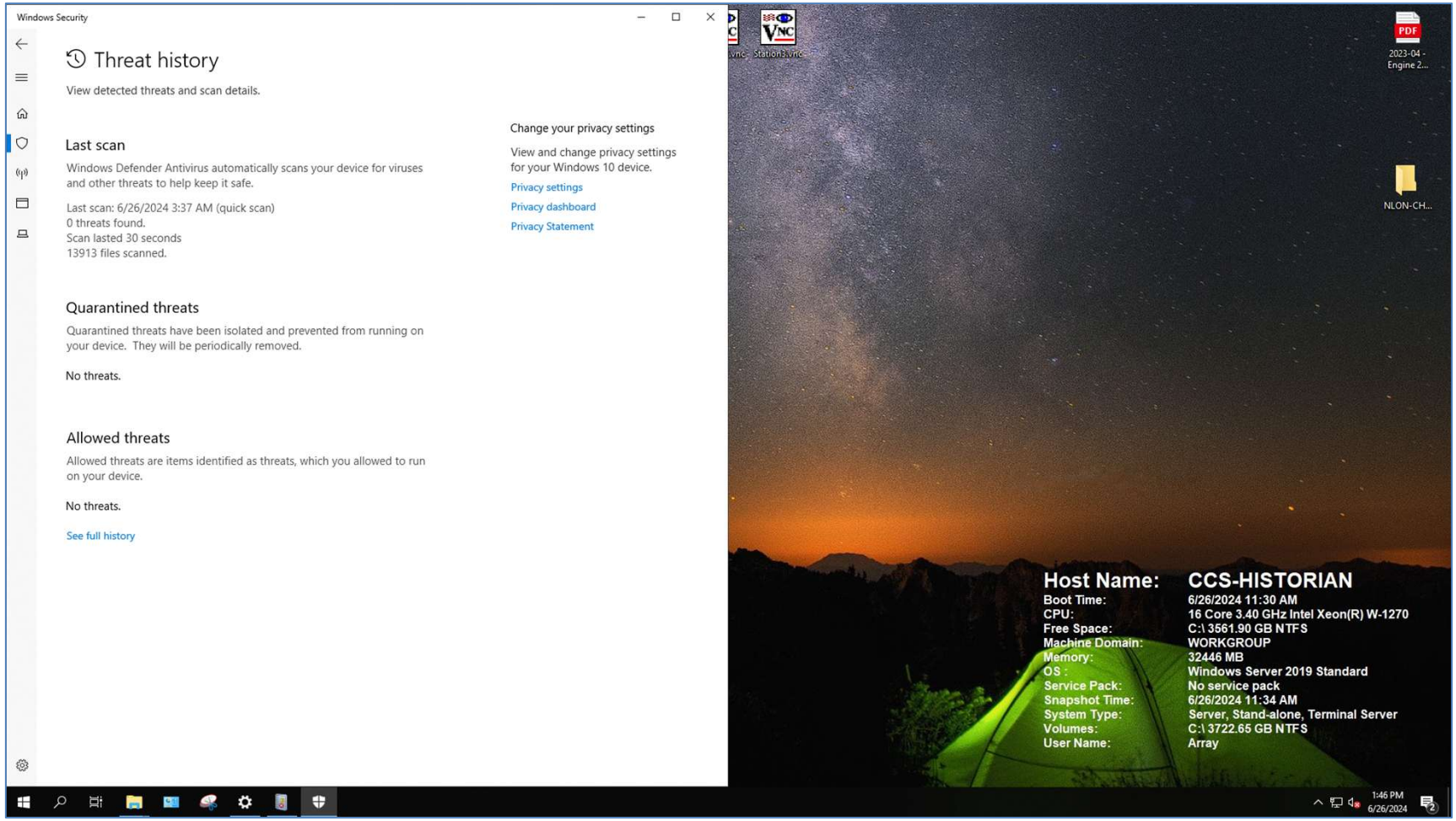
Internet Options Advanced - TLS 1.2 Enabled



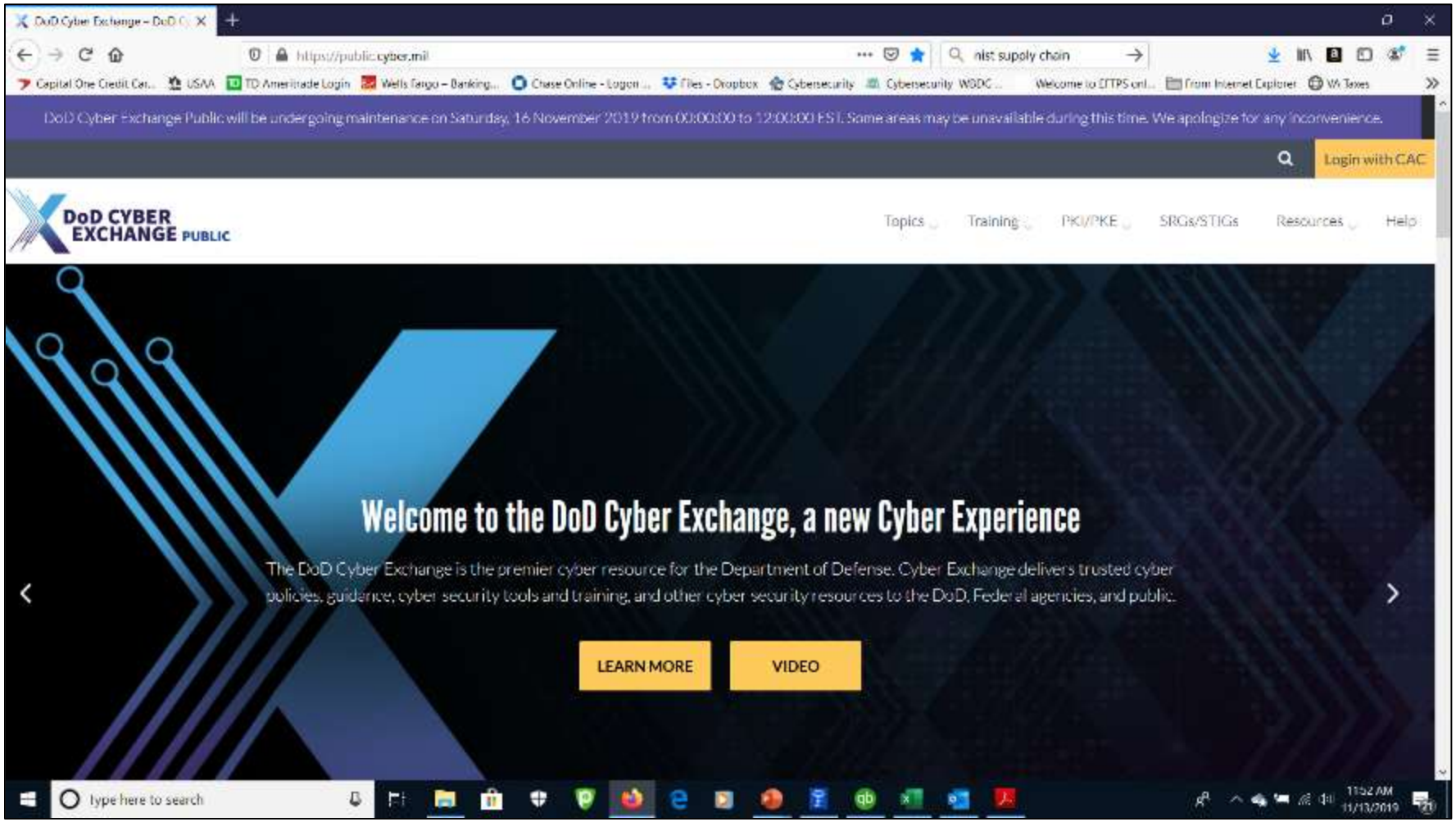
Windows Firewall - On



Windows Security AV Scan – No Threats



DISA STIGs



https://public.cyber.mil/

DISA STIGs

Sessions: 10 Files: 361 Total Size (MB): 111.34

Filter by session, hostname or content...

Sessions

Scan Session	Status	Directory	Files	Size (MB)	Hosts	Content	Errors	Warnings	Ave %	Max %	Min %
2022-02-22_234521		C:/Users/Administrator/SCC/Sessions/2022-02-22_234521/	36	10.36	1	6	0	0	98.4	95.26	100
2022-02-22_234120		C:/Users/Administrator/SCC/Sessions/2022-02-22_234120/	36	10.36	1	6	0	0	95.06	95.26	100
2022-02-22_233531		C:/Users/Administrator/SCC/Sessions/2022-02-22_233531/	36	10.36	1	6	0	0	95.06	95.26	100
2022-02-22_230734		C:/Users/Administrator/SCC/Sessions/2022-02-22_230734/	36	10.54	1	6	0	0	78.48	95.73	0
2022-02-22_225943		C:/Users/Administrator/SCC/Sessions/2022-02-22_225943/	36	10.74	1	6	0	0	76.5	95.12	0
2022-02-22_163034		C:/Users/Administrator/SCC/Sessions/2022-02-22_163034/	37	11.49	1	6	63	0	52.6	84.36	0
2022-02-22_162436	* new *	C:/Users/Administrator/SCC/Sessions/2022-02-22_162436/	36	11.69	1	6	0	0	49.32	80	0
2022-02-22_161414	* new *	C:/Users/Administrator/SCC/Sessions/2022-02-22_161414/	36	11.69	1	6	0	0	49.4	80	0
2022-02-22_160626	* new *	C:/Users/Administrator/SCC/Sessions/2022-02-22_160626/	36	11.94	1	6	0	0	39.38	80	0
2022-02-21_234247	* new *	C:/Users/Administrator/SCC/Sessions/2022-02-21_234247/	36	12.17	1	6	0	0	31.22	80	0

Results

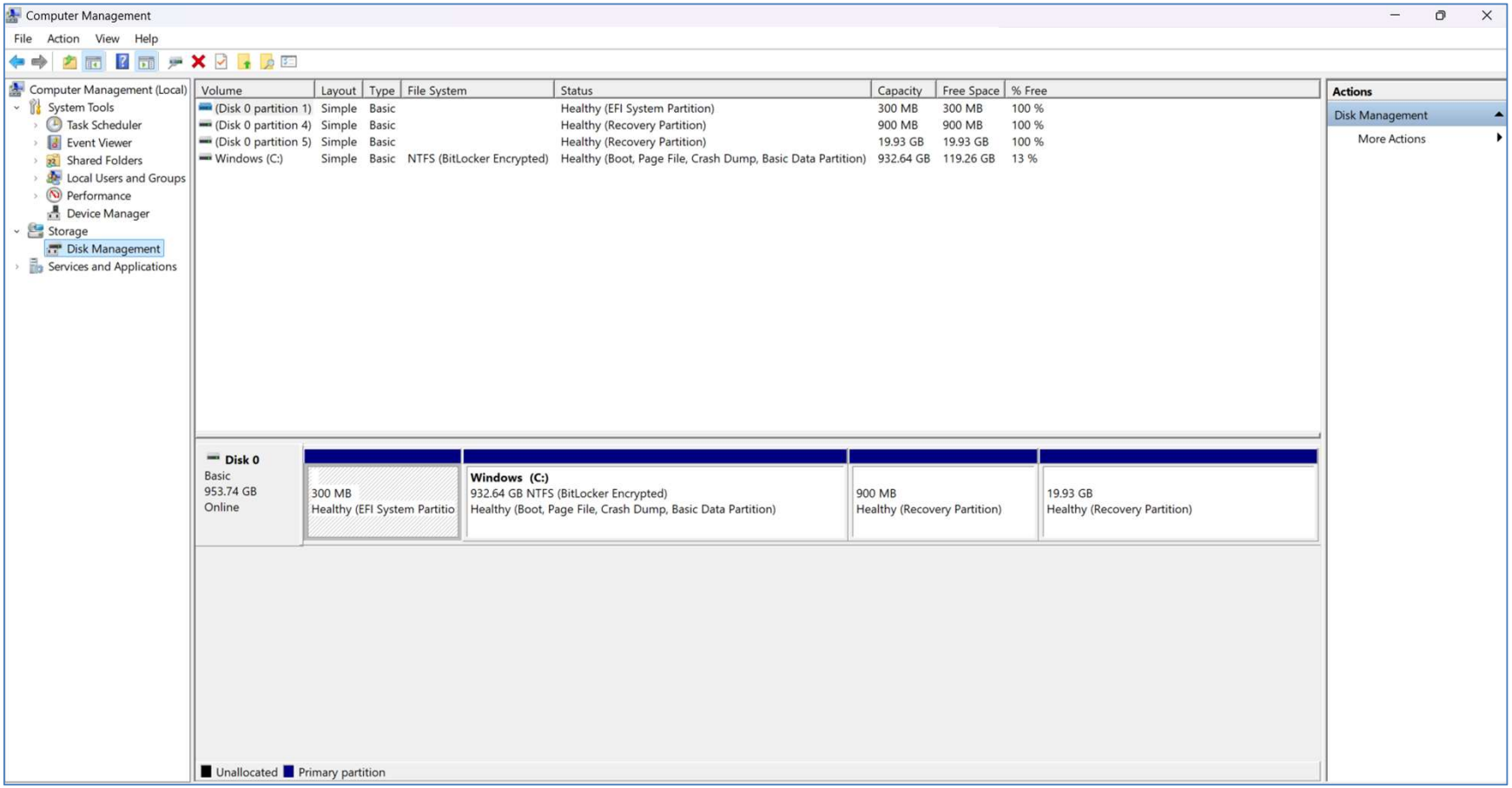
Host Name	Content	Score	Errors	Warnings
CCS-STATION1	Windows_Firewall...Advanced_Security	100	0	0
CCS-STATION1	Windows_Defender_Antivirus	95.12	0	0
CCS-STATION1	Windows_10_STIG	95.26	0	0
CCS-STATION1	MS_Edge_STIG	100	0	0
CCS-STATION1	MS_Dot_Net_Framework	100	0	0
CCS-STATION1	IE_11_STIG	100	0	0

Reports XML

Report Type	Format	Filename	Size (MB)
All Settings	HTML	Results/SCAP/CCS-STATION1_SCC-5.4.2_2022-02-22...ws_Firewall_with_Advanced_Security-002.001.html	0.31
Non-Compliance	HTML	Results/SCAP/CCS-STATION1_SCC-5.4.2_2022-02-22...ws_Firewall_with_Advanced_Security-002.001.html	0.01

The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
We want scores of 90 or better.

Computer Management Disk



Disk Healthy and Plenty of Disk Space

Computer Management Event Logs

Computer Management

File Action View Help

Computer Management (Local)
- System Tools
  - Task Scheduler
  - Event Viewer
    - Custom Views
    - Windows Logs
      - Application
      - Security
      - Setup
      - System
      - Forwarded Event
    - Applications and Ser
    - Saved Logs
    - Subscriptions
  - Shared Folders
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Disk Management
- Services and Applications

Filtered: Log: Application; Levels: Critical, Error, Warning; Source: . Number of events: 5,212

Level	Date and Time	Source	Event ID	Task Category
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:17 PM	RestartManager	10010	None
Warning	8/27/2024 1:25:51 PM	Search	10024	Gatherer
Warning	8/27/2024 1:25:51 PM	Search	10024	Gatherer
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	7/24/2024 4:21:00 PM	WMI	63	None
Warning	7/24/2024 1:29:48 AM	Search	10024	Gatherer
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None

Event 10010, RestartManager

General Details

Application 'C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe' (pid 22560) cannot be restarted - Application SID does not match Conductor SID..

Log Name:	Application		
Source:	RestartManager	Logged:	8/27/2024 12:29:18 PM
Event ID:	10010	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	LT13-Mike

Actions

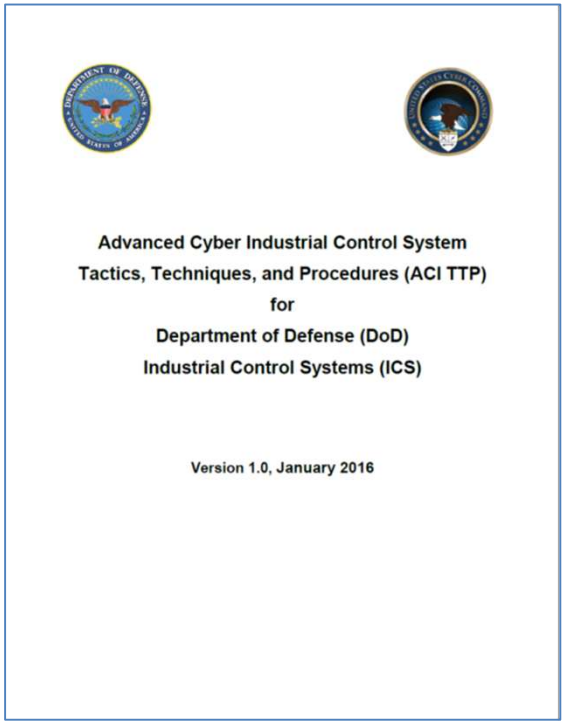
Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Clear Filter
- Properties
- Find...
- Save Filtered Log File As...
- Attach a Task To this Log...
- Save Filter to Custom Vi...
- View
- Refresh
- Help

Event 10010, RestartManager
- Event Properties
- Attach Task To This Eve...
- Copy
- Save Selected Events...
- Refresh
- Help

Check for Critical, Warning and Error, research the Event ID’s to resolve

ACI TTP for DoD ICS

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include **supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS),** and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. **ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation.**


Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Version 1.0, January 2016

3. How to Use These TTP

This ACI TTP is divided into essentially four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures** (**Detection, Mitigation, Recovery**) (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

TTP 's Apply to IT and OT

The Tactics, Techniques and Procedures can be used by any organization and apply to:

Information Technology (IT) Systems – Business and Home
Operational Technologies (OT) Systems – Any Kind (Utility, Building, Environmental, Medical, Logistics, Transportation, Weapons, etc.)

The tools that will be used are almost all open source and free to use (premium or business versions are modestly priced)

- ***Segment and VLAN IT and OT networks; DMZ's with gateways and/or firewalls***
- ***Separate the OS and OT data (C: OS and D: OT data), enable BitLocker on both drives***

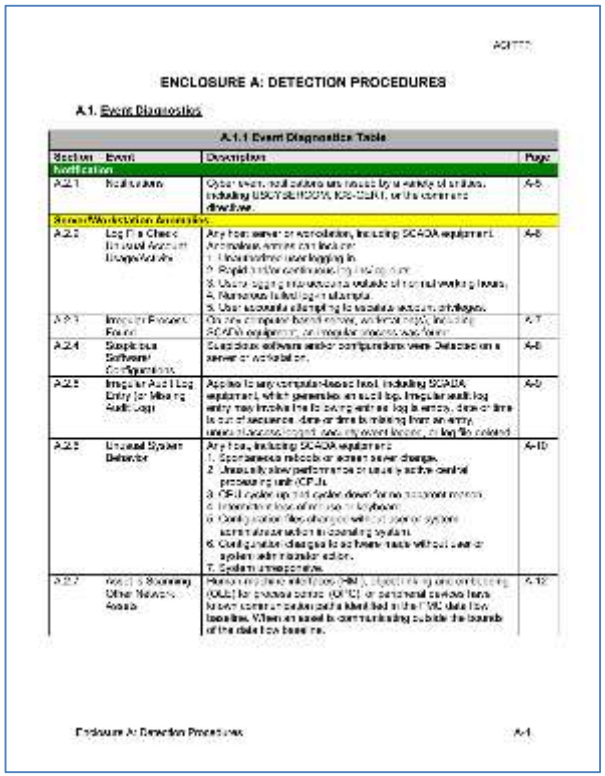
Key Roles
AO-Authorizing Official NAVFAV HQ
SO-System Owner NAVFAV Public Works Directorate
ISSM-Information System Security Manager CIO2 and 4
ISSO-Information System Security Officer CIO2 and 4
ISSE-Information System Security Engineer CIO 2 and 4 and NORESCO Cyber Team
Operators-Construction and O&M
CPT-Computer Protection Team-Services, CYBERCOM, NSA

Threat-Response Procedures

b. Threat-Response Procedures (Detection, Mitigation, and Recovery).

Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general each section is designed for execution by the individuals responsible for the operations of the equipment, regardless of formal designations. **Successful Detection of cyber anomalies is best achieved when IT and ICS managers remain in close coordination.** The *Integrity Checks Table* (enclosure A, section A.3, table A.3.1) lists the procedures to use when identifying malicious cyber activity.

ENCLOSURE A: DETECTION PROCEDURES



ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostics Table

Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including US-CERT, ICS-CERT, or the company directive.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host, server or workstation, including SCADA equipment. An intrusion event can include: 1. Unauthorized user logging in. 2. Rapid or continuous logins/logouts. 3. User logging in at unusual or outside of normal working hours. 4. Numerous failed login attempts. 5. User accounts changing to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer based device, including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following: entries, log in entry, date or time is out of sequence, date or time is missing from an entry, [illegible] or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver changes. 2. Unusually slow performance or unusually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Data or other files which are written to or deleted from system without operation in operating system. 6. Configuration changes to scheduled tasks without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset Is Scanning Other Network Assets	Human machine interfaces (HMI), operational technology communications (OPC) or personnel devices have known communications and identified in the IT/OT data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

Enclosure A: Detection Procedures A-1

Notification

A.2.1 Notifications

Server/Workstation Anomalies

A.2. Event Diagnostic Procedures

A.2.2 Server/Workstation: Log File Check: Unusual Account Usage/Activity

A.2.3 Server/Workstation: Irregular Process Found

A.2.4 Server/Workstation: Suspicious Software/Configurations

A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)

A.2.6 Server/Workstation: Unusual System Behavior

A.2.7 Server/Workstation: Asset Is Scanning Other Network Assets

A.2.8 Server/Workstation: Unexpected Behavior: HMI, OPC, and Control Server

DETECTION PROCEDURES SERVER EXAMPLE 1

A.1.1 Event Diagnostics Table			
Section	**Event**	**Description**	**Page**
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log-ins/log-outs. 3. Users logging into accounts outside of normal working hours. 4. Numerous failed log-in attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver change. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

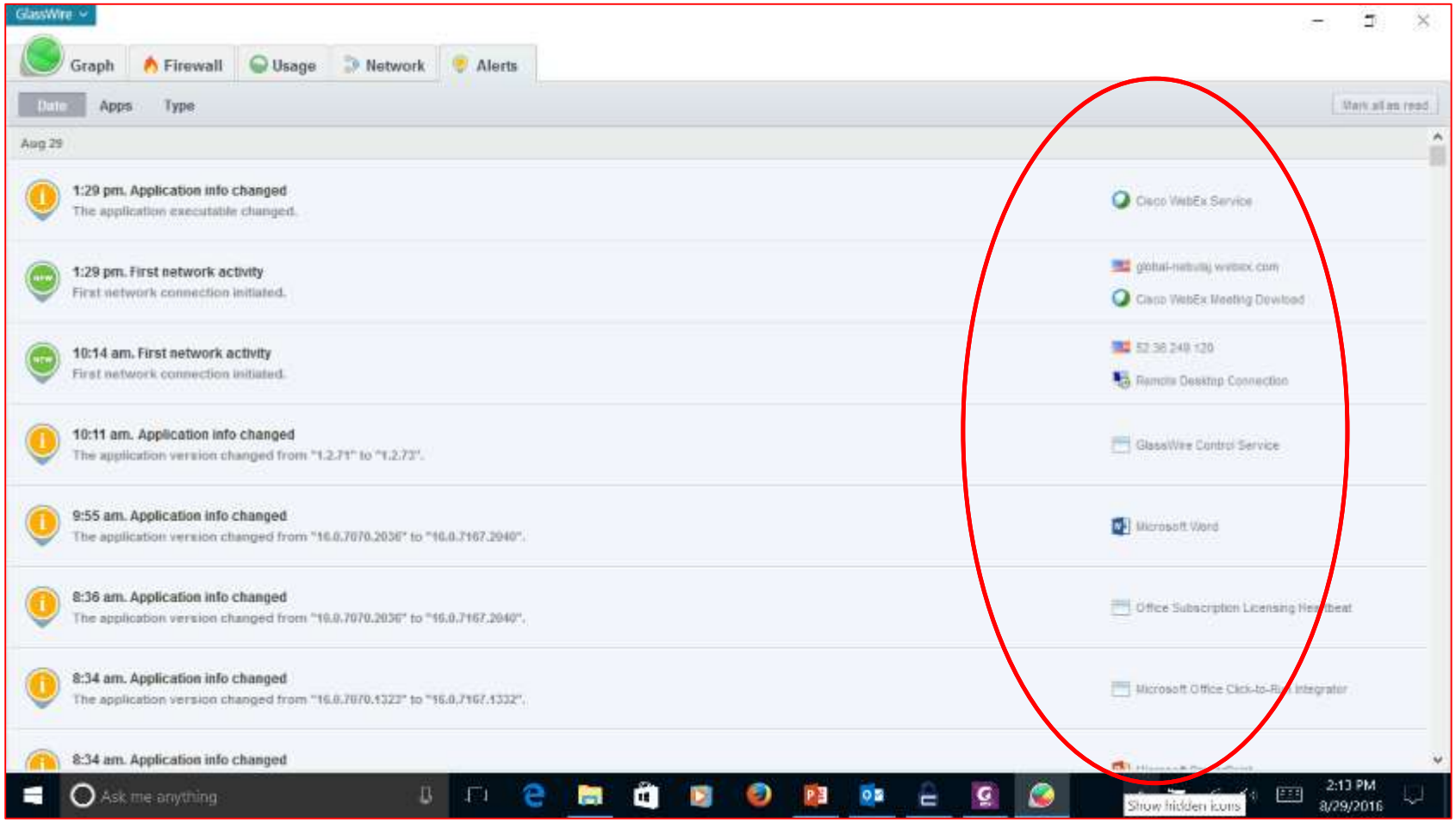
DETECTION PROCEDURES SERVER EXAMPLE 1

A.2.3 Server/Workstation: Irregular Process Found

- **Functional Area:** IT or ICS
- **Description:** On any computer-based server, workstation, including SCADA equipment, an irregular process was found

Step	Procedures
Investigation	1. **DETERMINE** if the new process belongs to an authorized installation: a. New software was installed on to the system? b. Was maintenance performed on the system, and if the new process was installed during that maintenance? c. Is the new process a result of a patch update?
No Action Required	2. If the new process belongs to an authorized installation: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the new process **does not** belong to an authorized installation: a. **DOCUMENT** in Security Log. b. **GO TO** Section *A.3, A.3.1 Integrity Checks Table.* (See recommended checks below.) **LOCATE** the integrity check associated with server or workstation you are investigating and **EXECUTE** the Integrity checks. **Recommended Checks:** A.3.2.1 Server/Workstation Process Check A.3.2.2 Server/Workstation Log Review A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

DETECTION PROCEDURES SERVER EXAMPLE 1



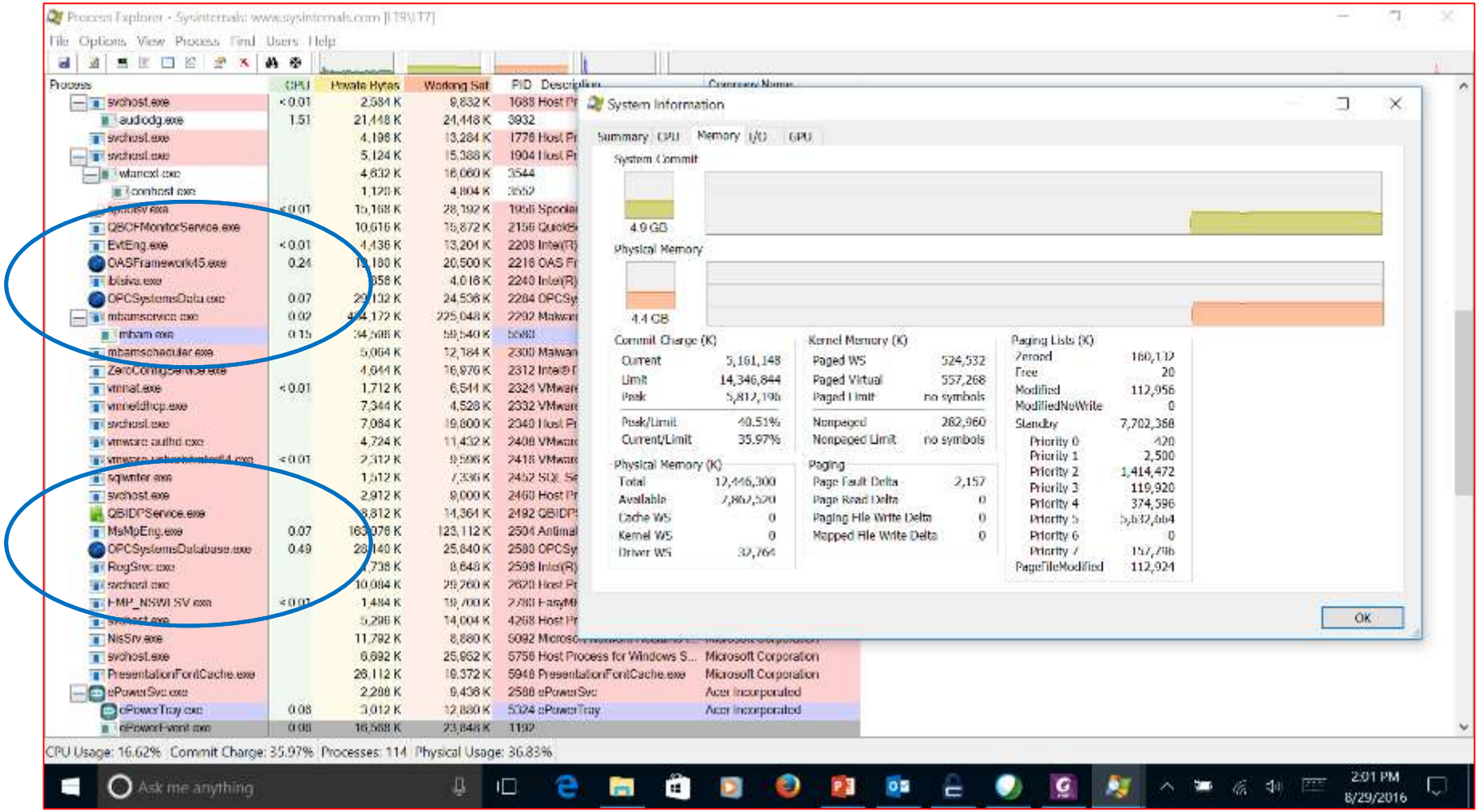
DETECTION PROCEDURES SERVER EXAMPLE 1

A.3.2.1 Server/Workstation Process Check

- **Who should do this check:**
  The organization or individual responsible for the server or workstation
- **What is needed for this check:**
  1. FMC data flow chart
  2. FMC baseline topology
  3. FMC baseline authorized process and tasks
  4. FMC baseline software list
  5. FMC baseline system information

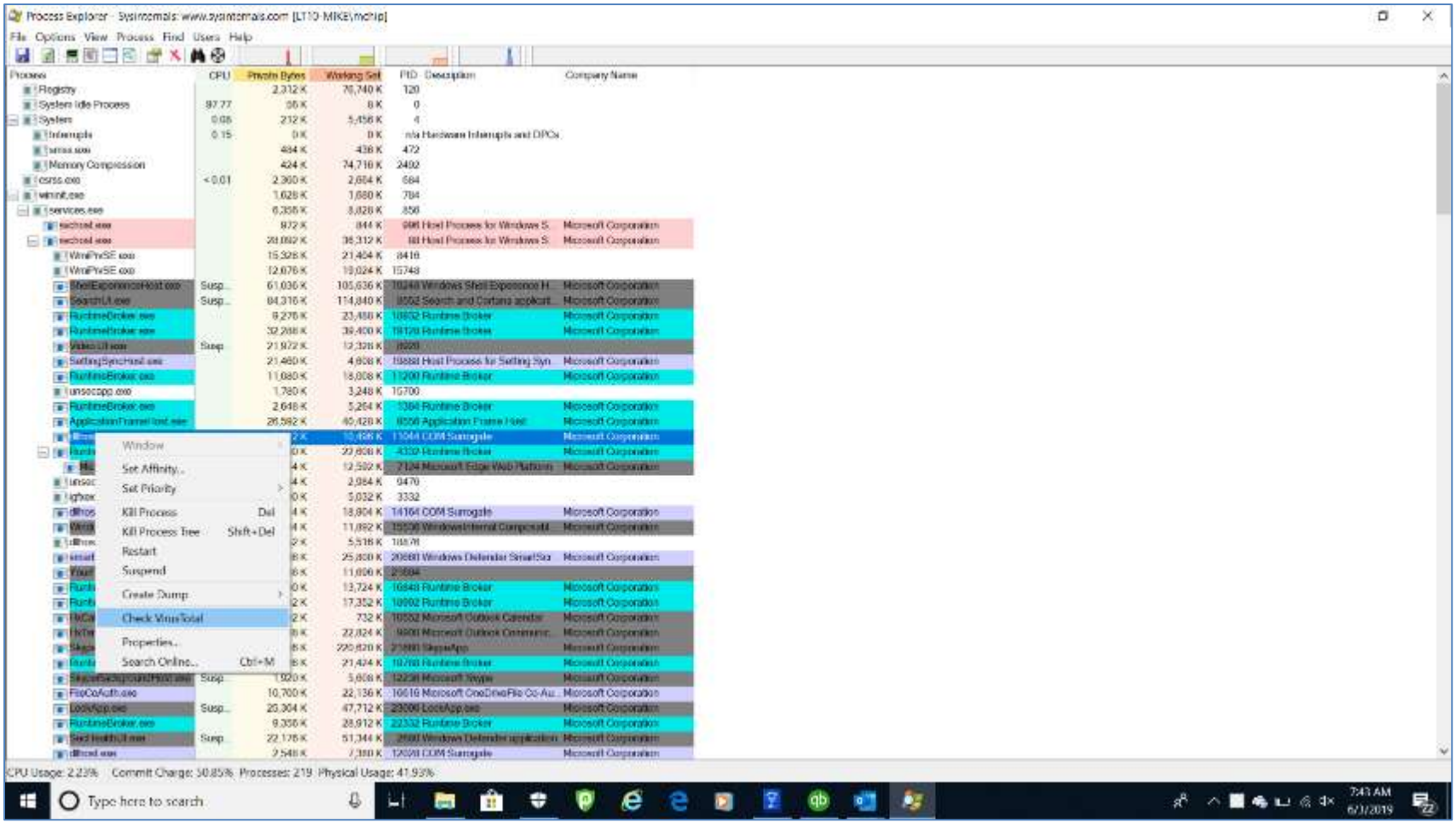
Step	Procedures
1.	If the machine is **responsive**, **EXECUTE** steps a and b below. Once completed, **RETURN** to this section, and resume with Step 2. a. Section: A.3.2.2 Server/Workstation Log Review. b. Section: A.3.2.3 Unauthorized User Account Activity. If the machine is **not responsive**, **GO TO** Section *A.3.2.5 Server/Workstation Unresponsive Check*.
2.	If Procedures A.3.2.2 or A.3.2.3 do **not** result in a **Severity Level of High (3)**, **CONTINUE** to step 3.
3.	**Process Check: LAUNCH** SysInternals: **CHECK** for processes that do not appear legitimate. This can include (but is not limited to) processes that: a. Have no icon or name. b. Have no descriptive or company name. c. Are unsigned Microsoft images. d. Reside in the Windows directory. e. Include strange uniform resource locators (URLs) in their strings. f. Communicating with unknown IP address (use FMC data flow diagram to compare). g. Host suspicious dynamic link library (DLL) or services (hiding as a DLL instead of a process). h. **LOOK** for "packed" processes which are highlighted in purple.
4.	If an anomalous process was found: a. **DOCUMENT** details of the event in Security Log. b. **CONTACT** system administrator responsible for the machine or the command ISSM. (1) **REPORT** suspicious process. (2) **REQUEST** assistance in determining if the process is malicious (process may be undocumented but normal). (3) If the process is not malicious, **DOCUMENT** in Security Log, and **EXECUTE** A.3.2.4 Server/Workstation Communications Check. (4) If the process is malicious, **DOCUMENT** the **Severity Level of High (3)** in the Security log. c. **GO TO** section ***A.2.29 Action Step***.
5.	If an anomalous process was not found: a. **DOCUMENT** the **Severity Level as None (0)**. b. **RETURN** to the previous diagnostic procedure and continue with *Recommended Checks*.

DETECTION PROCEDURES SERVER EXAMPLE 1



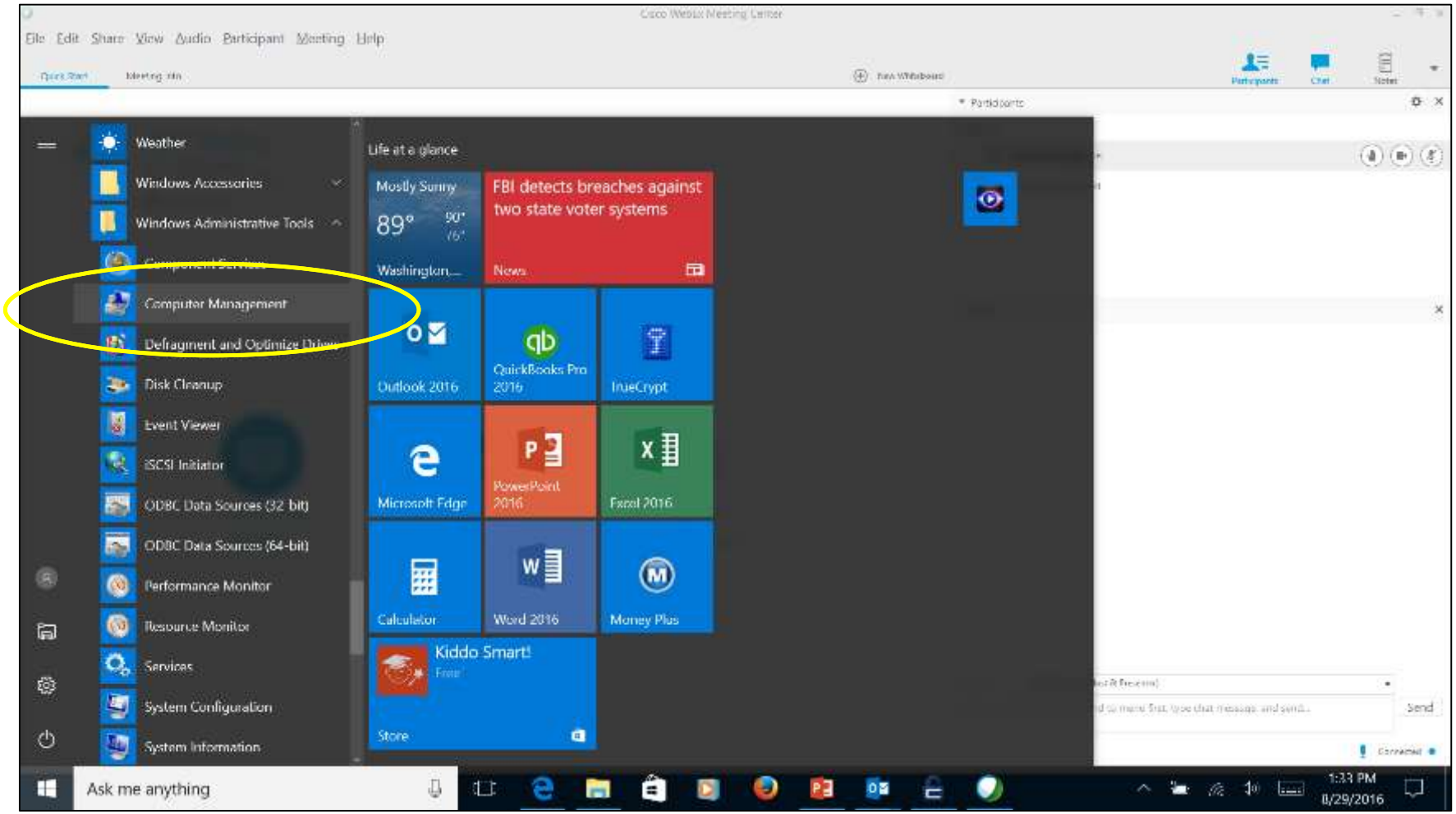
MS Process Explorer

Virus Total – Use with Extreme Caution



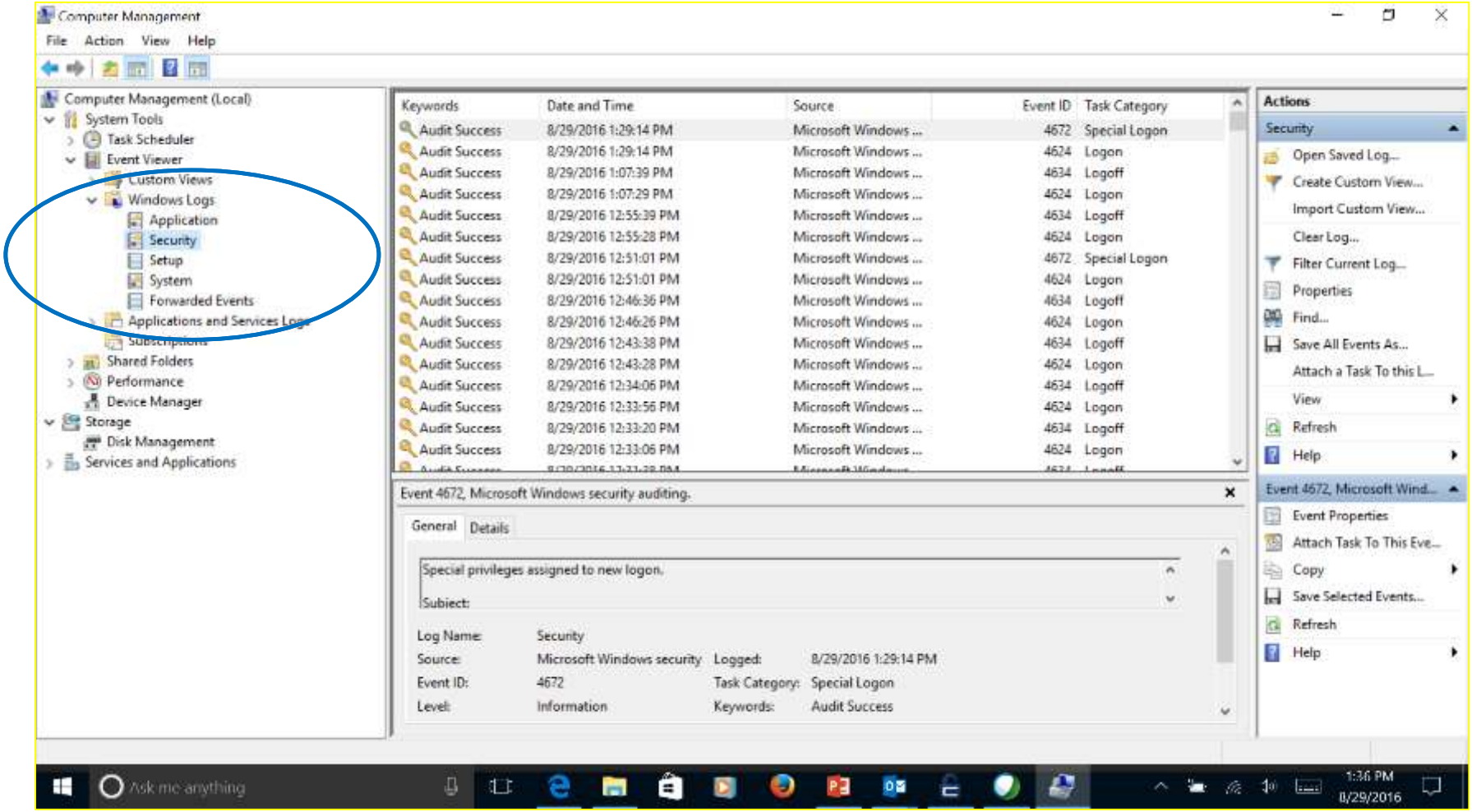
DO NOT submit a file to Virus Total unless you want it to be seen by the world forever
But we will use it to check suspicious files…..

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management Windows Logs

Detect Privilege Escalation

EE.16 Detect Privilege escalation

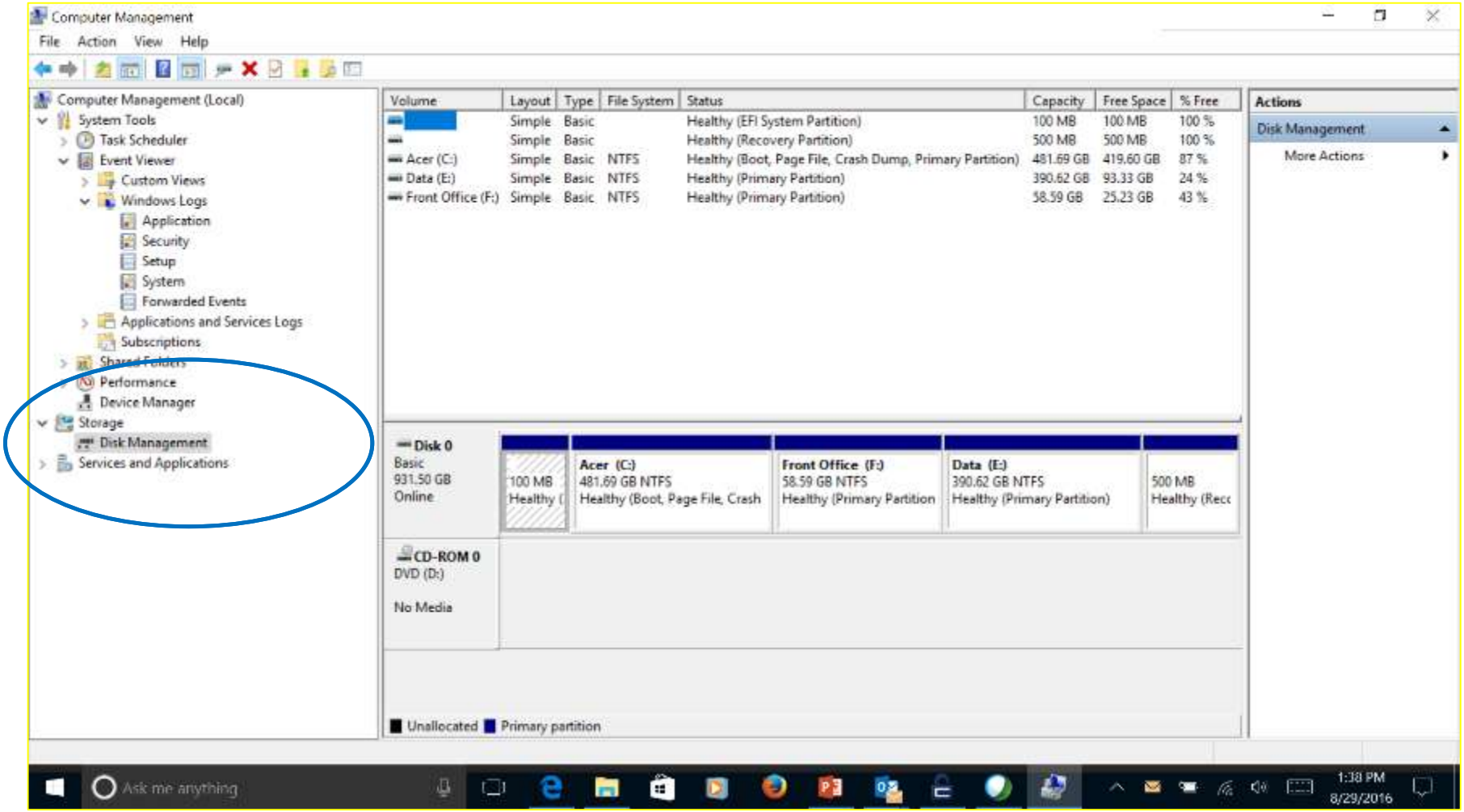
Malware may attempt to gain privileges on an OS (i.e. from a standard user to administrator) in order to execute tasks that require administrative privileges.

A. Detect Windows Scheduler based or similar attacks (on AT, WinAT), as well as attacks on permissions:

Review Windows Event Log for the following eventIDs and determine if the event(s) were authorized.

- 4648 (security) A logon was attempted using explicit credentials (often used in scripts, scheduled tasks, or with RUNAS command, or to authenticate to a remote host as a different user)
- 4697 (security) A service was installed on the system
- 4698 (security) A scheduled task was created
- 4720 (security) A user account was created
- 4724 (security) An attempt was made to reset an accounts password
- 4728 (security) A member was added to a security-enabled global group
- 4732 (security) A member was added to a security-enabled local group
- 4735 (security) A security-enabled local group was changed

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management Data Management

Protecting FRCS

- Turn on BitLocker (Full Disk Encryption Data at Rest)
- Ensure Internet Options Transport Layer Security 1.2 and/or 1.3 on (Data encrypted in Transit)
- Update Operating System and Applications (patching)
- Applying the Security Technical Implementation Guides with the SCAP Tool (Hardening)
- Daily Anti-Virus Malware Scan (Windows Security or HBSS/ACAS/ESS)
- Regular Vulnerability Scans (HBSS/ACAS/ESS)
- Regular Password Changes (enforced by the STIGS)
- Regular System Checks by Operators (Computer Management, Disk Health, Event Logs)
- Maintain the Configuration Baseline Audit Reports (Quarterly per contract)
- Practice using the DoD Advanced Industrial Control Systems Tactics, Techniques and Procedures (Hunt and Defend 101)

Protecting FRCS Resources

CompTIA Security +
Cisco CNNA
DHS CISA
DoD ESTCP Cybersecuring FRCS Website
SANS
GIAC GICSP
Whole Building Design Guide Cybersecurity Website
DOE Energy Exchange Conference Cyber Tracks
SAME Cyber Resilience IGE
SAME JETC Conference
Vendor Newsletters

The need for Cyber Warriors in the OT/FRCS space will continue to increase; understanding what the Components and Devices are, how they function, how they are connected, how to harden them, how to establish the Configuration Baseline and Normal Behavior and then Identify and Mitigate Abnormal Behavior are challenging.

Next Phase Coming – Quantum Computing and AI – SkyNet is not far away....

QUESTIONS

Michael Chipley
President, The PMC Group LLC
Cell: 571-232-3890
E-mail: mchipley@pmcgroup.biz