Security and Hardening of Your PI System

Lubos MIcoch, Cyber Security Advisor

OSIsoft®

Agenda

1. Prologue
2. Sliding Scale of Security
3. The Big 4 of Cyber Security
4. Cyber Security Data Sheets
5. Call to Action

But my mission is just…

Small electricity generator

IoT manufacturer

Non critical process plant

ICS systems integrator

Attacker viewpoint

Pathway to bulk electric system

Platform for botnet

Exploit development system

Malware distribution channel

Three Laws of SCADA Security

1. Nothing is secure

2. All software can be hacked

3. Every piece of information can be an attack

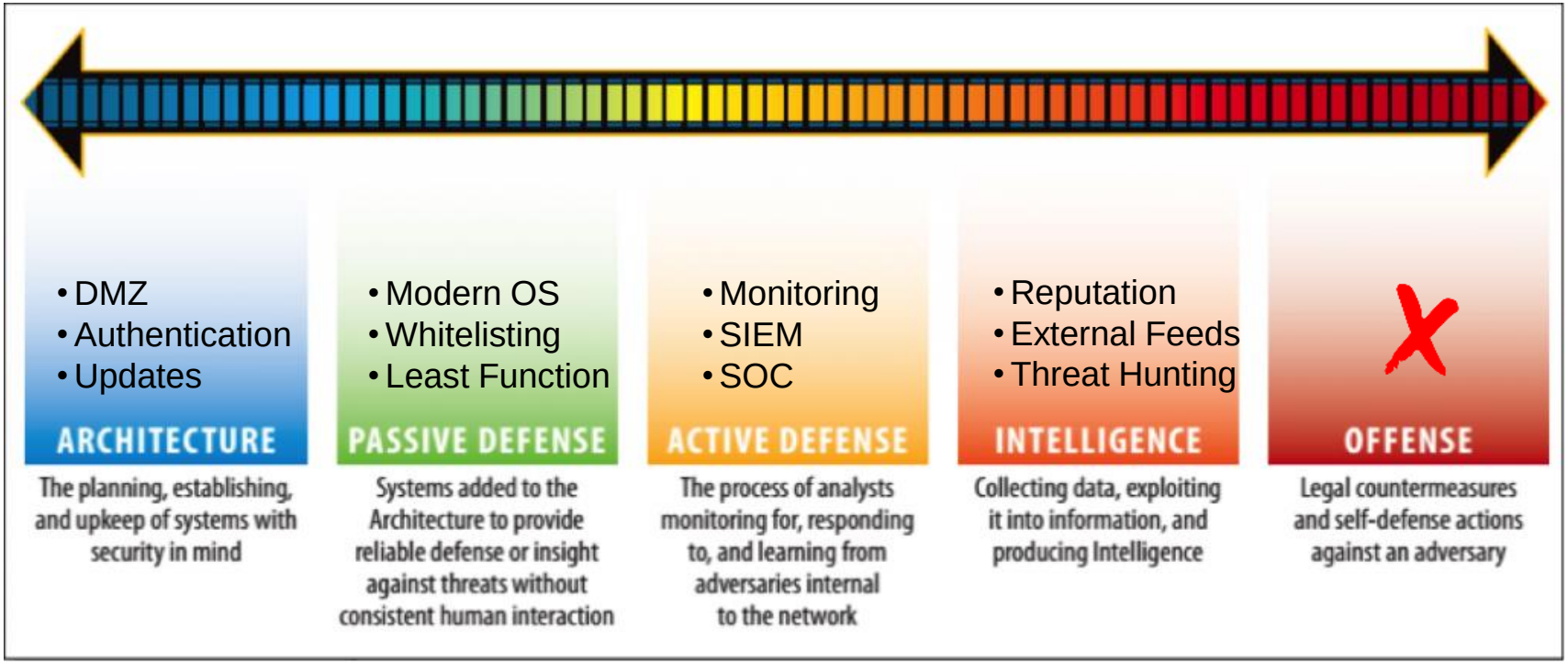
Ginter, Andrew (2016) SCADA Security: What's broken and how to fix it.

Threat Spectrum

Threat	Resources	Attacks
Nation States Military Grade	Nearly Unlimited	Autonomous Targeted Malware
Intelligence Agencies	Professional	Remote Control 0-Day Vulnerabilities
Hacktivists	Skilled Amateur	Remote Control Exploit Permissions
SCADA Insiders	Amateur	Exploit Permissions
Organized Crime	Professional	Malware Known vulnerabilities
Corporate Insiders	Amateur	Exploit Permissions

Ginter, Andrew (2016) SCADA Security: What's broken and how to fix it.

Sliding Scale of Security



The Sliding Scale of Cyber Security - Robert M. Lee
https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

Fundamental PI System Security Advantage

Critical Systems

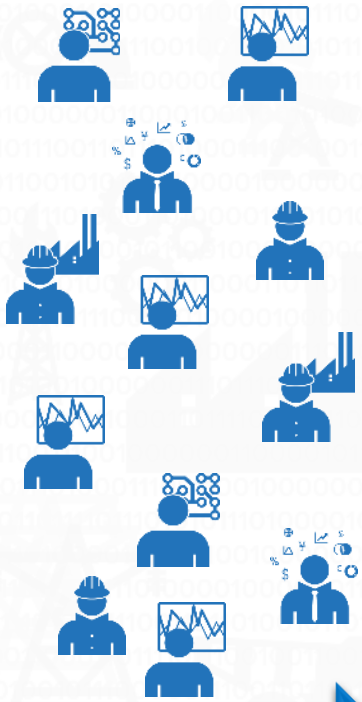
Transmission & Distribution SCADA

Plant DCS

PLCs

Environmental Systems

Other critical operations systems



Reduce the risks on critical systems

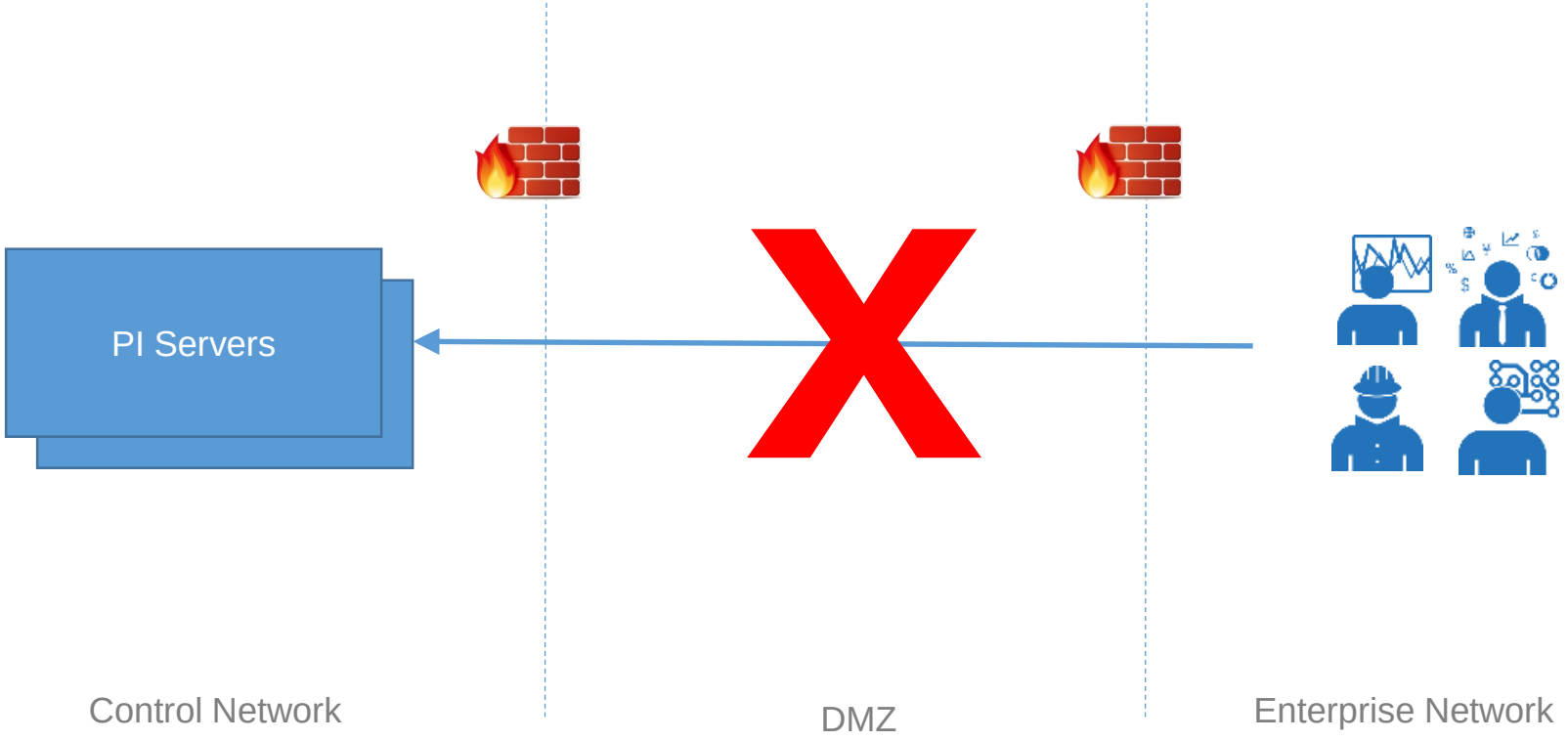
Limits direct access to critical systems while expanding the use of information.

OSIsoft.

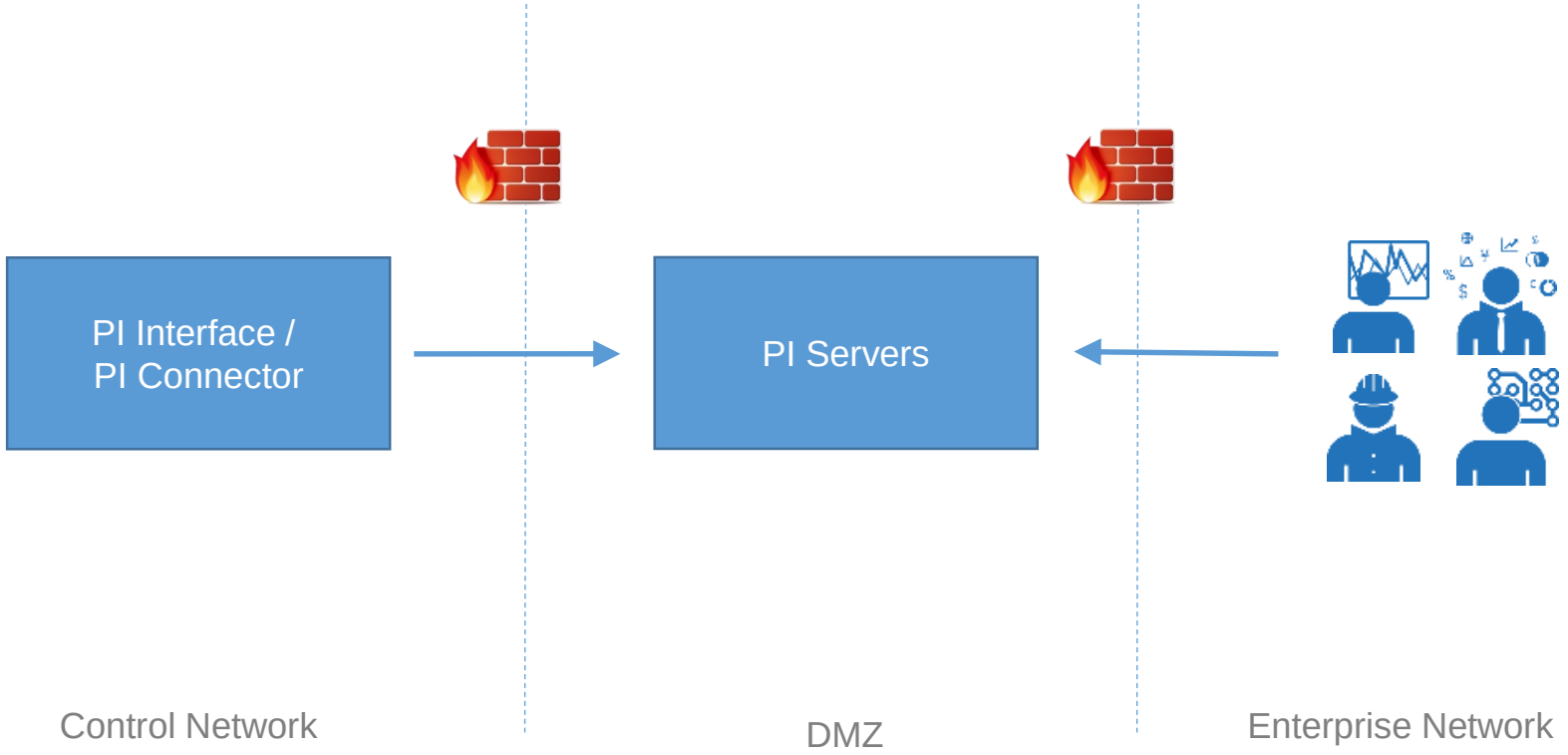
Infrastructure

Security Perimeter

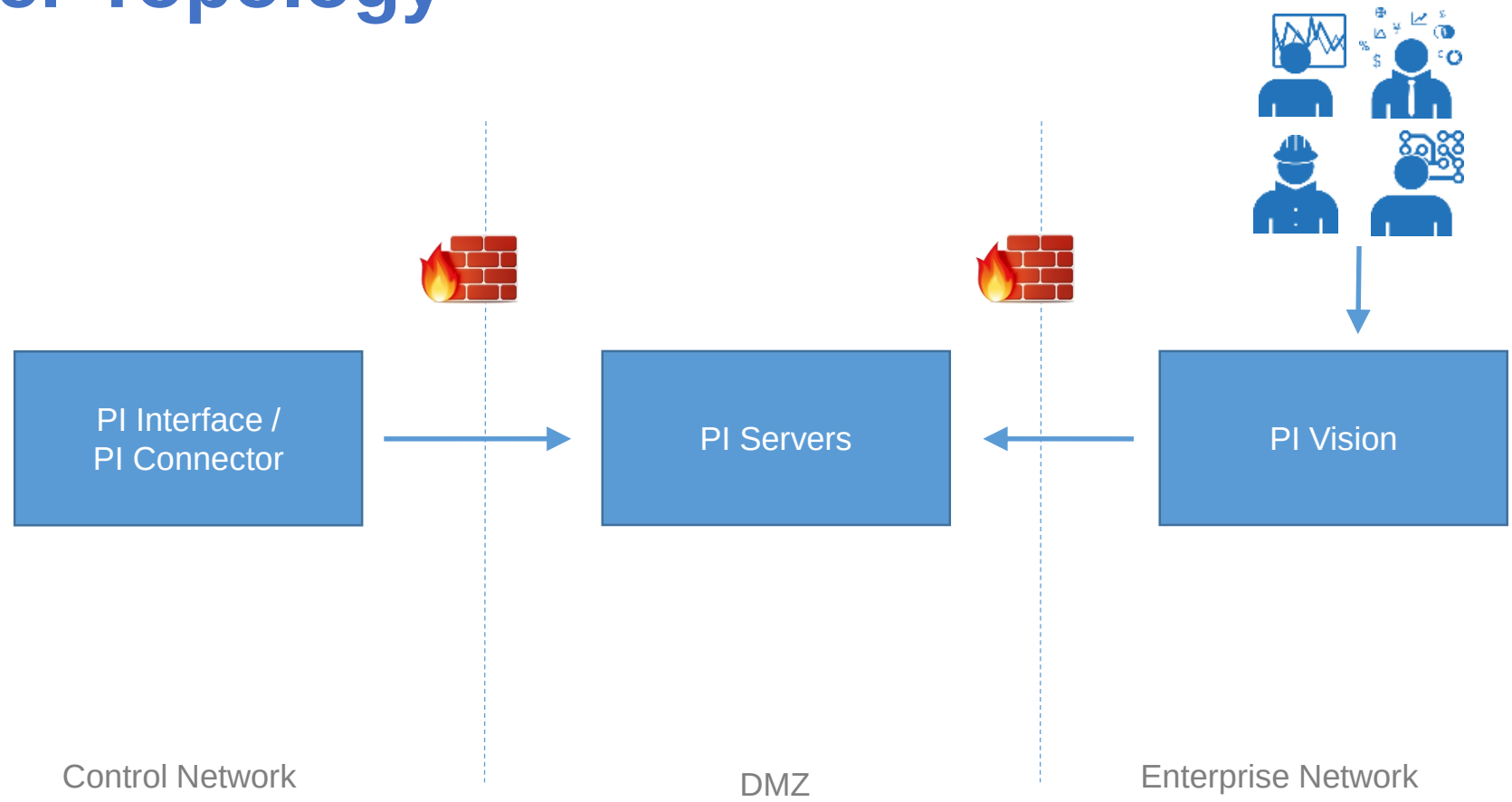
Undesirable Topology



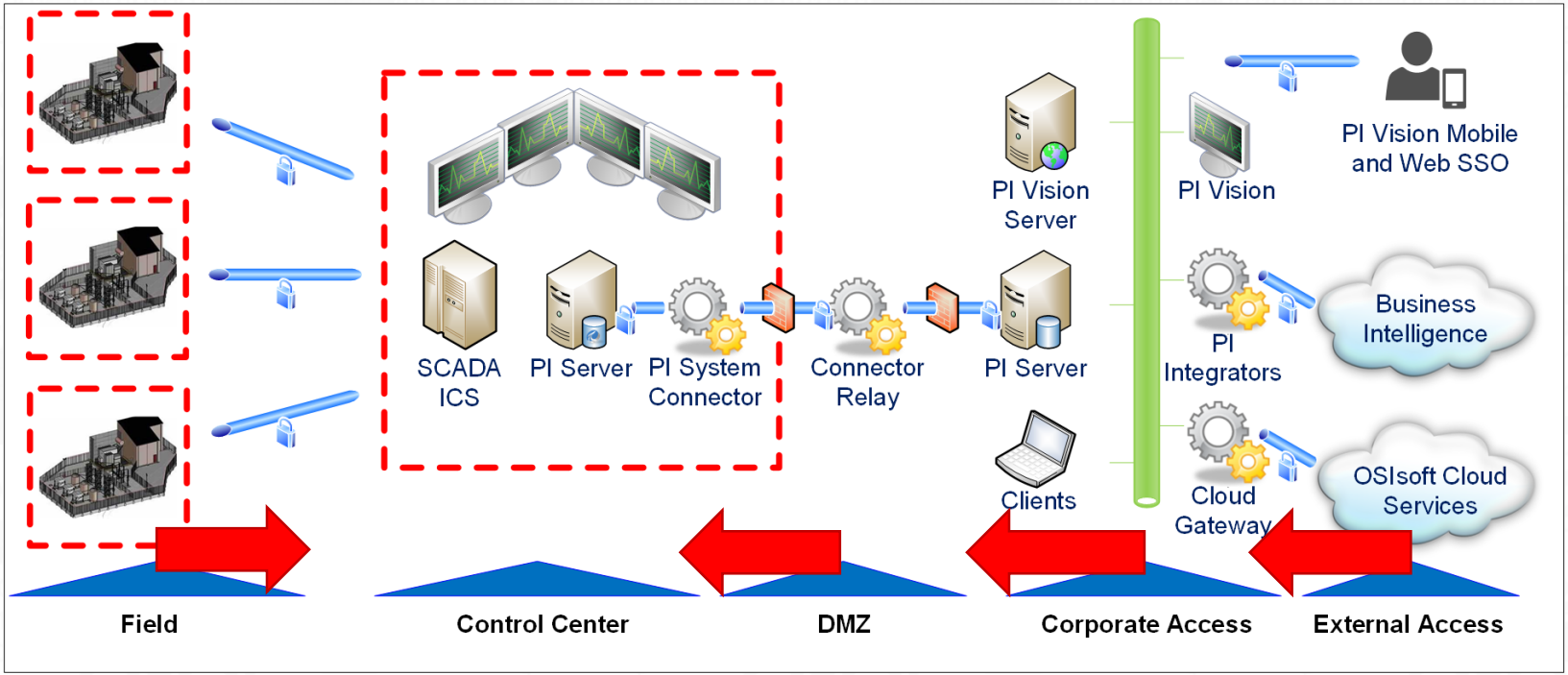
Good Topology



Better Topology



PI System 2019 Reference Architecture



NERC CIP, NIST 800-53, and NIST 800-82

Reduce Surface Area of the Platform

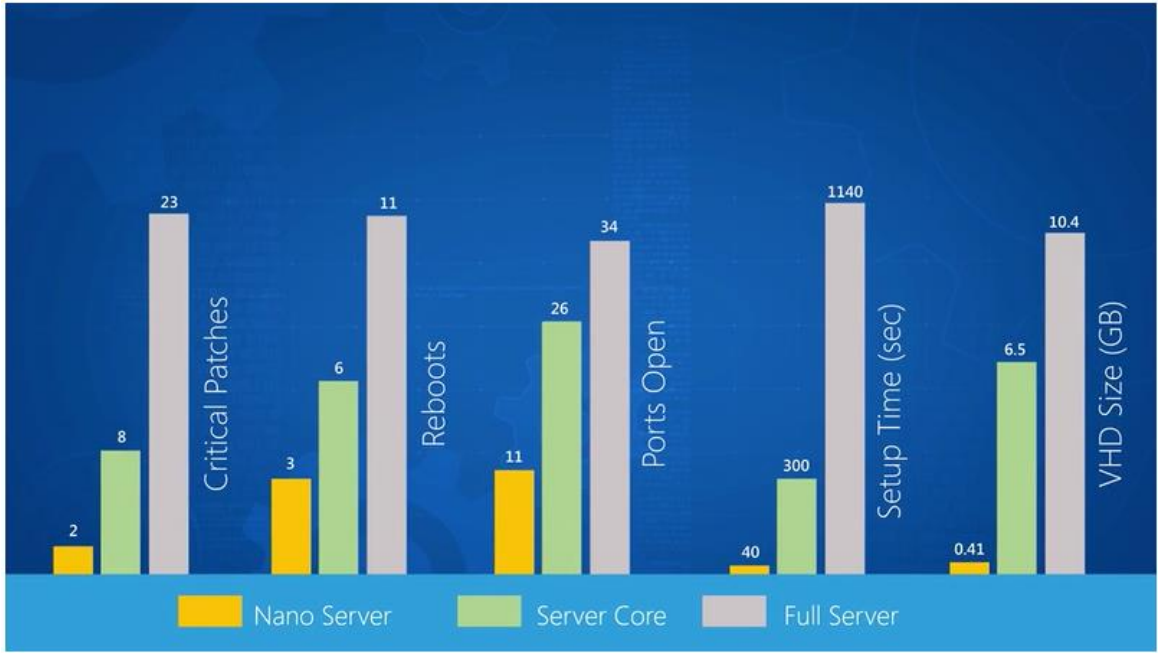
Windows Server Core

- Less installed, less running (No GUI applications)
- Fewer open ports
- Less patching
- Less Maintenance
- Lower TCO

…. More secure

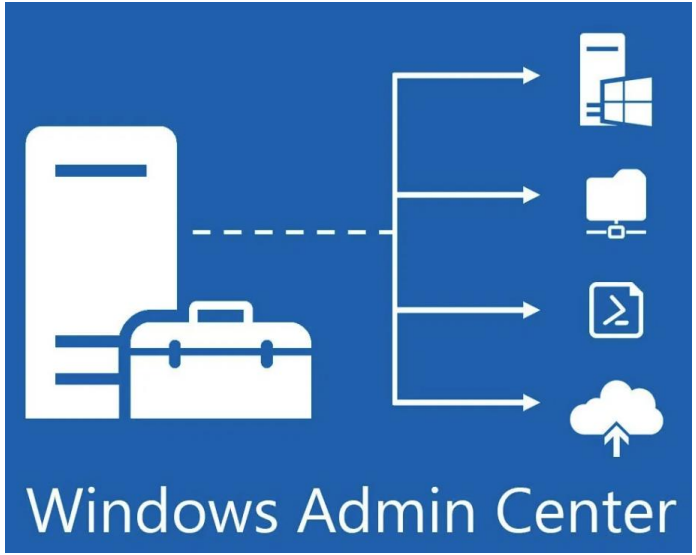
Supported OSIsoft products:

PI Data Archive
PI AF Server
PI Vision
PI Web API
PI Connectors

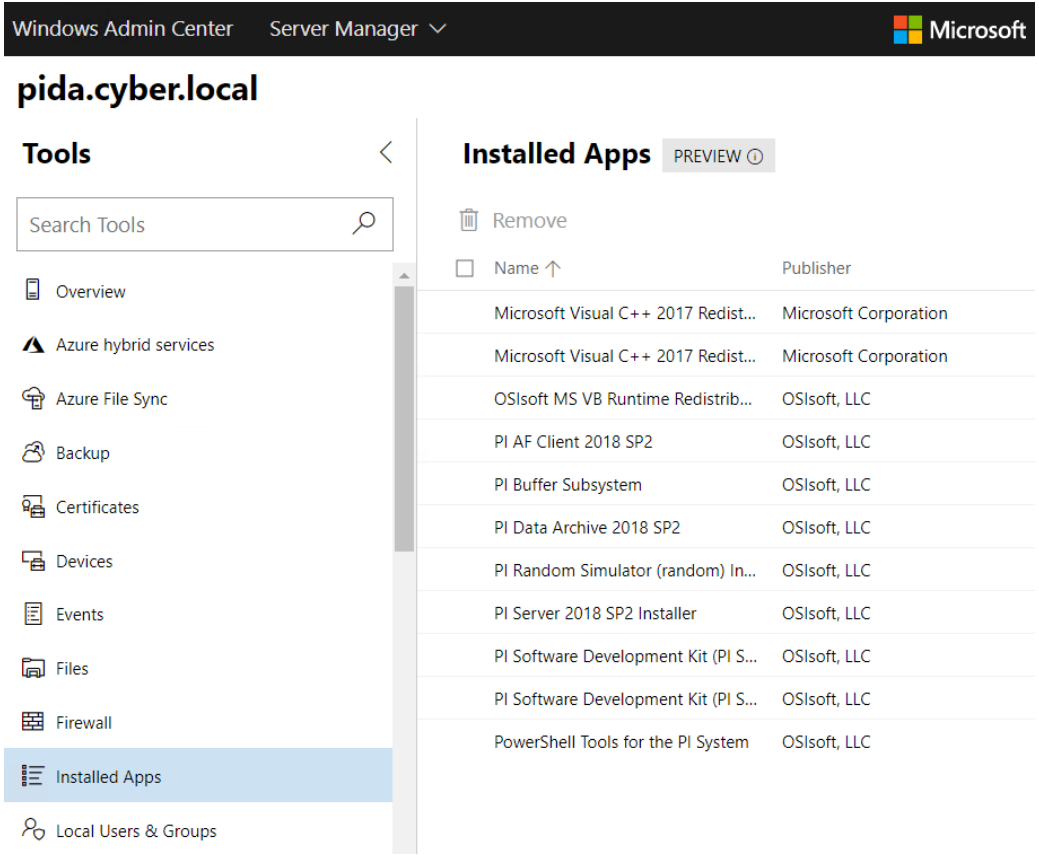


Microsoft Mechanics. "Exploring Nano Server for Windows Server 2016 with Jeffrey Snover." Online video clip. YouTube, 10 Feb. 2016

Reduce Surface Area of the Platform



Free, browser-based app for managing Windows Servers (**including Server Core**)



Whitelisting

All Applications: A, B, C

Blacklist: Allow All, Deny A, C

Whitelist: Deny All, Allow B

All Applications: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, ...

Blacklist: Allow All, Deny A, C, E, F, G, H, I, J, K, L, M, N, O, P, ...

Whitelist: Deny All, Allow B, D

Blacklisting

Whitelisting

Whitelisting – using built-in Windows features

Whitelisting with Windows Defender Application Control
- Used to be called Device Guard
- Available since Windows 10 / Server 2016 (incl. Core)

Whitelisting with AppLocker
- Can be used in tandem with WDAC
- Available on older OS version, but doesn't work in Server Core

Whitelisting PI applications based on catalog files
- OSIsoft provides a Catalog file for products that use unsigned third-party files

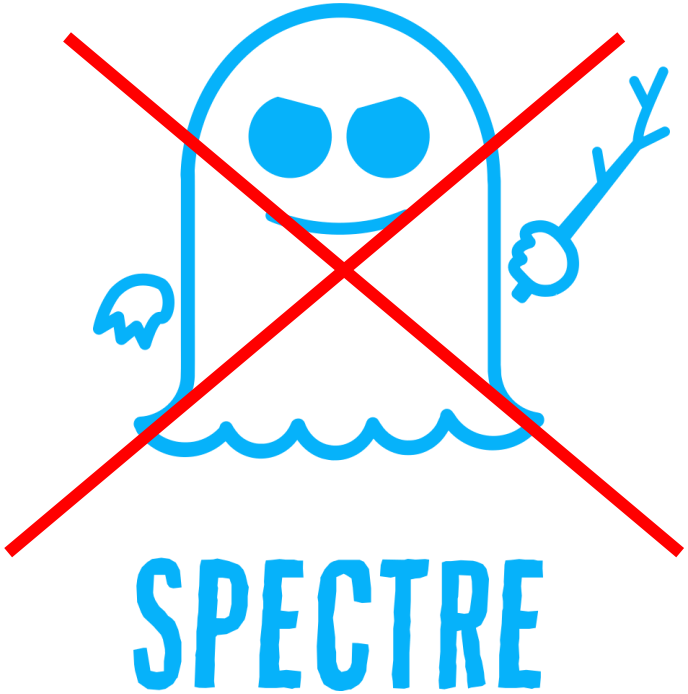
Upgrade your software

OSIsoft is consistently:

Implementing compiler flags as they become available

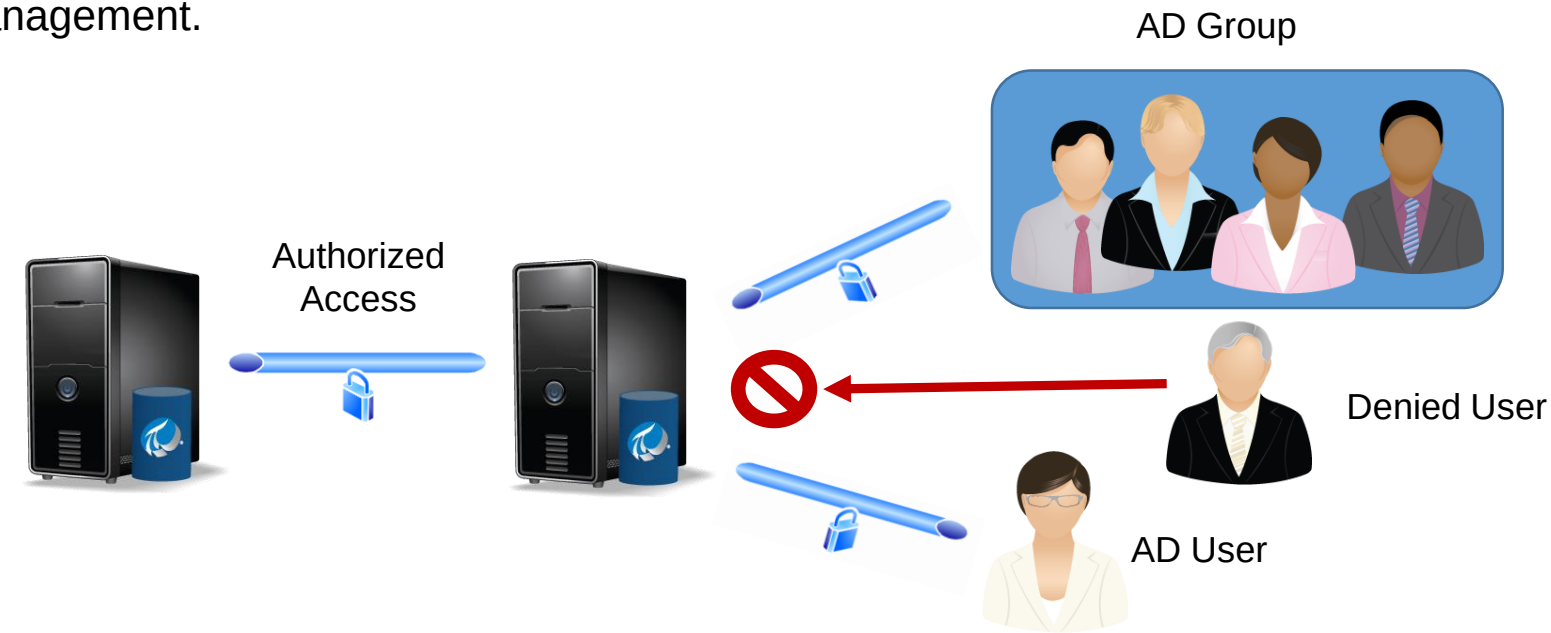
Applying least privileges to services

Adding support for Windows Core systems



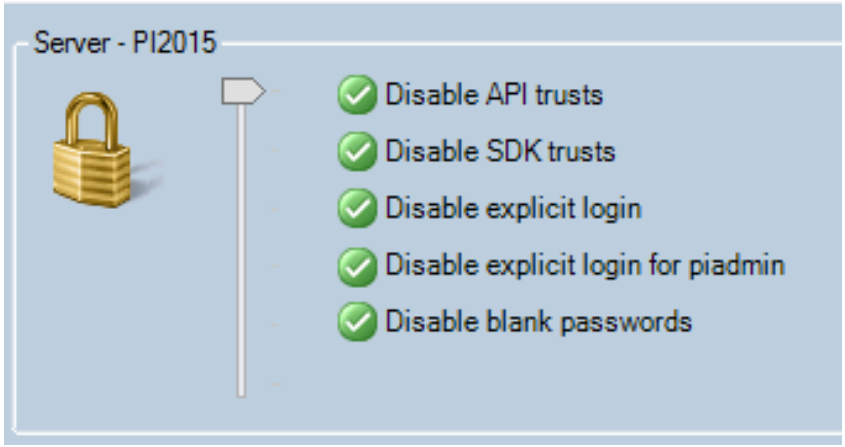
Role Based Access:
Leverage Windows Integrated Security

Less work for administrators: Active Directory provides SSO and Identity and Access Management.



Authentication Management

Enforce the strongest authentication method server-side.



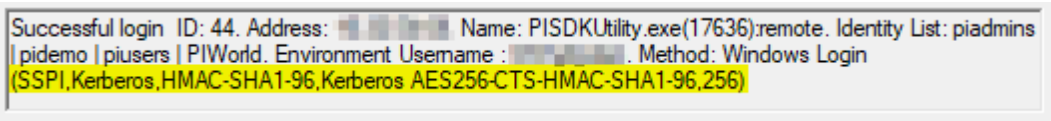
PI API trusts can be disabled with the installation and configuration of the PI API 2016 for WIS and later

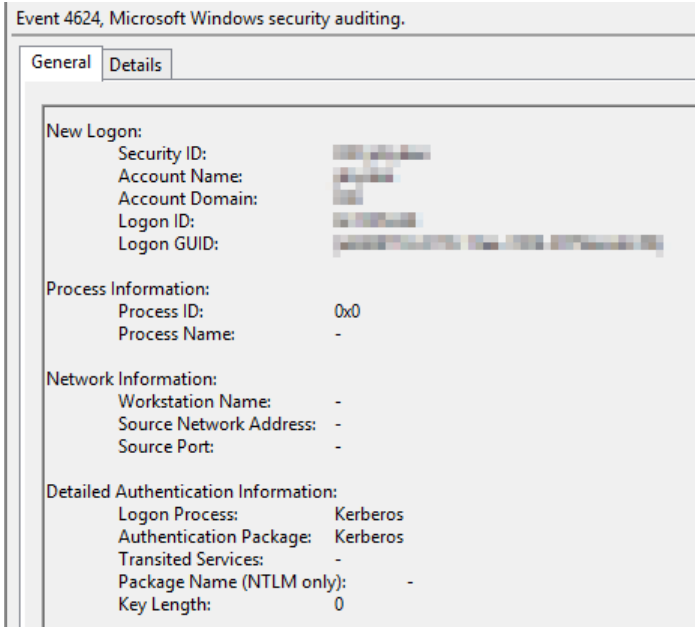
Audit Connections

WIS provides connection auditing through Security event logs

PI Message Logs provide connection auditing (Message ID: 7082)

PI Data Archive connection history



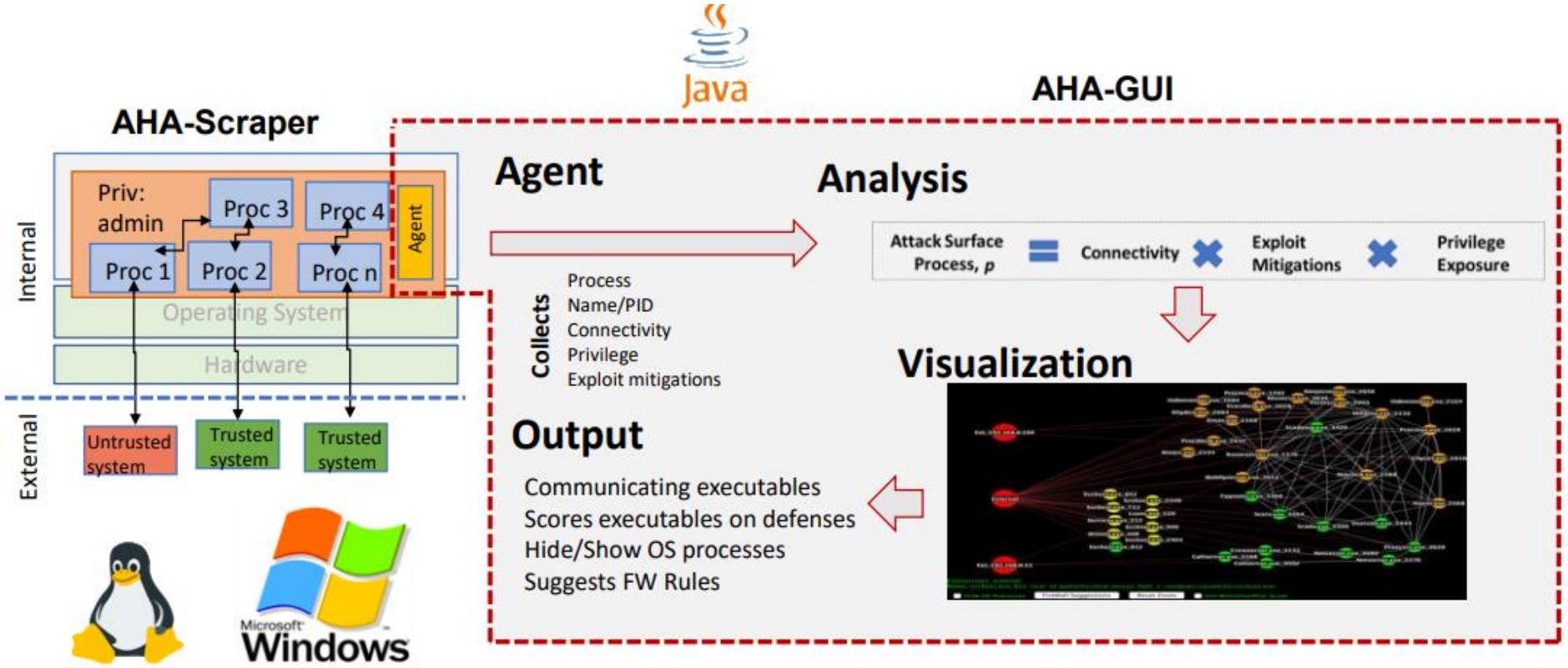


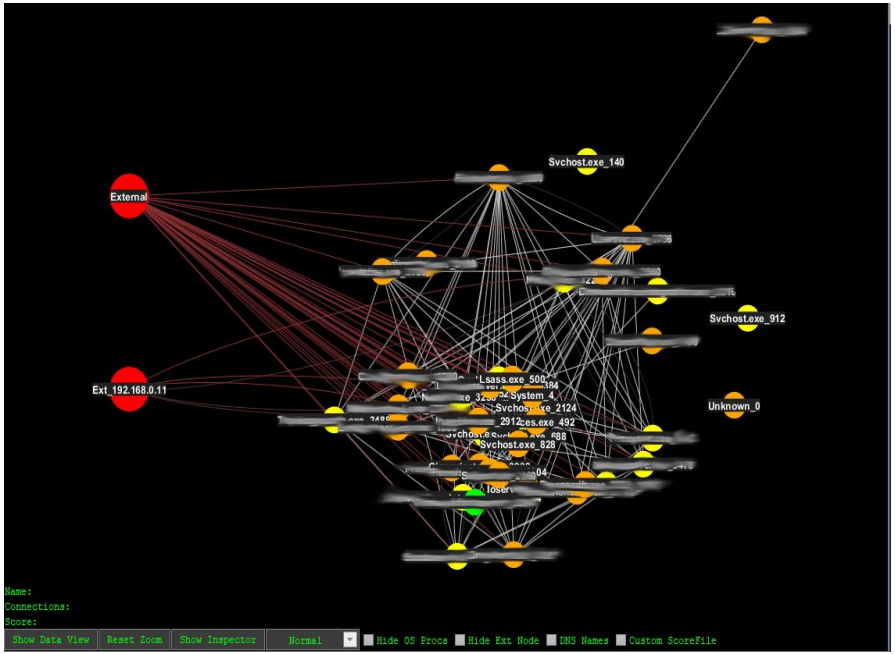
Analyzing Attack Surface #1

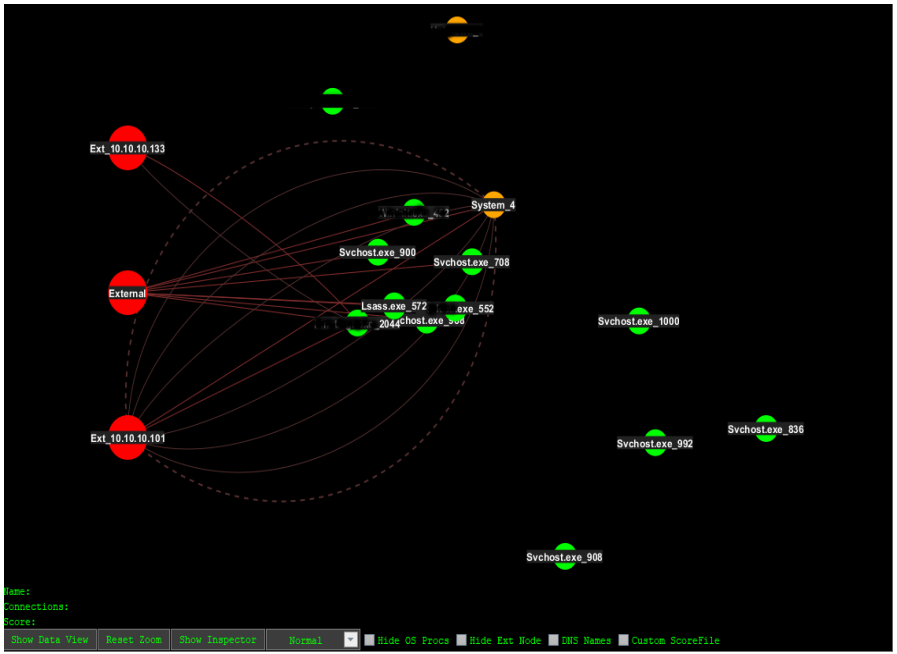
AHA - AttackSurface Host Analyzer

site: https://aha-project.github.io/

code: https://github.com/AHA-Project/AHA-Scraper-Win
https://github.com/AHA-Project/AHA-Scraper-Lin
https://github.com/AHA-Project/AHA-GUI



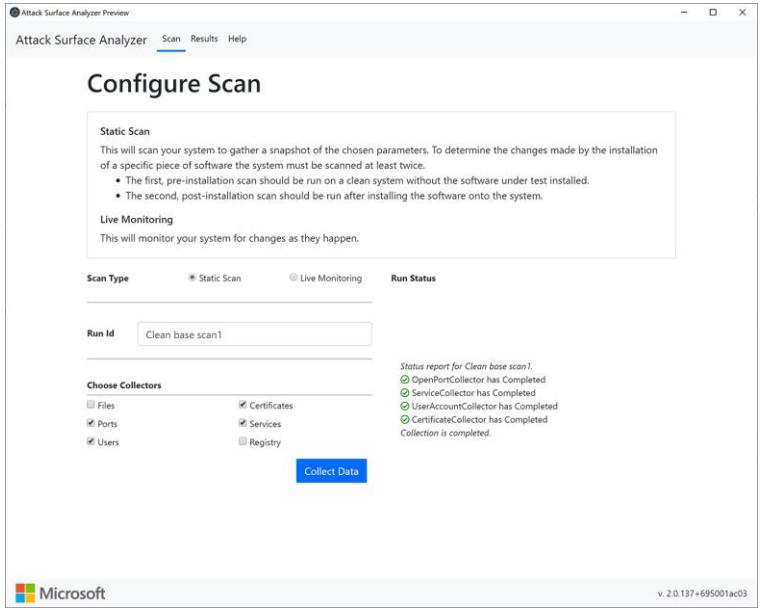




Windows Server 2008 R2	Mean Score
External Attack Surface	9.5%
Internal Attack Surface	8.2%

Windows Server 2016 Core	Mean Score
External Attack Surface	80%
Internal Attack Surface	80%

Analyzing Attack Surface #2



Microsoft Attack Surface Analyzer 2.0

Site & code: https://github.com/Microsoft/AttackSurfaceAnalyzer

Attack Surface Analyzer Scan Results Help

Analyze Results

Scan Type Static Scan Live Monitoring

Base Run Id Clean scan1 Product Run Id After Install Run Analysis

Started Analysis
CertificateCompare is No Results
OpenPortCompare is No Results
ServiceCompare is Completed
UserAccountCompare is No Results

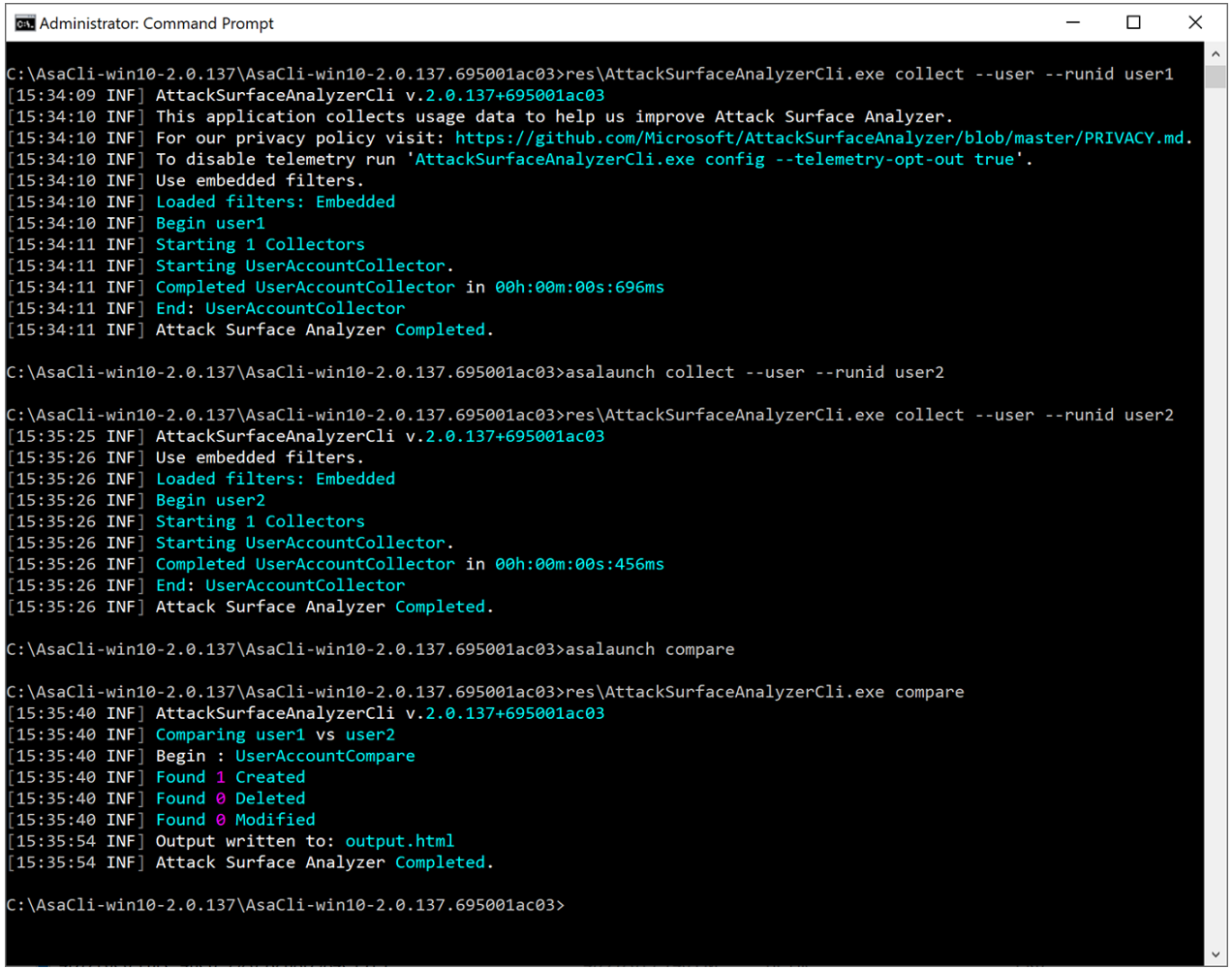
Select a type of result to view.
Files
Ports
Services
Certificates
Registry
Users

More Results

Export Options

Showing 1 - 10 Results. 10 total records.

Change Type				
Modified	PimIndexMaintenanceSvc_1899061	Manual	Contact Data_1899061	Stopped
Modified	AppXSvc	Manual	AppX Deployment Service (AppXSVC)	Running
Modified	wlidsvc	Manual	Microsoft Account Sign-in	Running



Material Safety Data Sheets

MATERIAL SAFETY DATA SHEET

Trade Name: **ACETONE**

Chemical Family: Acetone

Formula: C3 H6 O

FIRE AND EXPLOSION DATA

Flashpoint & Method:0% F (TCC)
Flammable Limits: LFL 2.0 , UFL 13.0
Extinguishing Media: water spray, dry chemical, CO_2, alcohol foam
Special equip. & procedures: Self contained breathing apparatus & complete protective clothing. Acetone is extremely flammable, any source of ignition will ignite it. Vapor is extremely explosive.

REACTIVITY DATA

Conditions Contributing to Instability: Heat, Sparks & Open Flame
Incompatible Substances: Acids, Oxidizing materials, Alkalis, Amines, Potassium T-Butoxide, Alkanolamines, Ammonia, Aldehydes, Chlorinated compounds.
Hazardous Decomposition Products: Carbon Monoxide, Carbon Dioxide
Hazardous Polymerization: will not occur.

PREVENTATIVE MEASURES

Skin: Wear impervious gloves (butyl rubber), coveralls and safety footwear.
Eyes: Chemical proof goggles or full face respirator if vapors cause eye discomfort.
Ingestion: Wash thoroughly before consuming food stuffs.
Inhalation: Use only in well ventilated areas or use NIOSH approved respiratory protection with organic vapor cartridges.

CONTROL MEASURES AND PRECAUTIONS

Keep container tightly closed. **DO NOT** consume food, drink or tobacco in work or material storage areas. **Flame or any source of ignition is to be kept away from this product.** Use caution and personal cleanliness to avoid skin and eye contact. Avoid breathing vapors.

Cyber Security Data Sheets

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

Cyber Security Technical Assessment Methodology

Risk Informed Exploit Sequence Identification and Mitigation, Revision 1

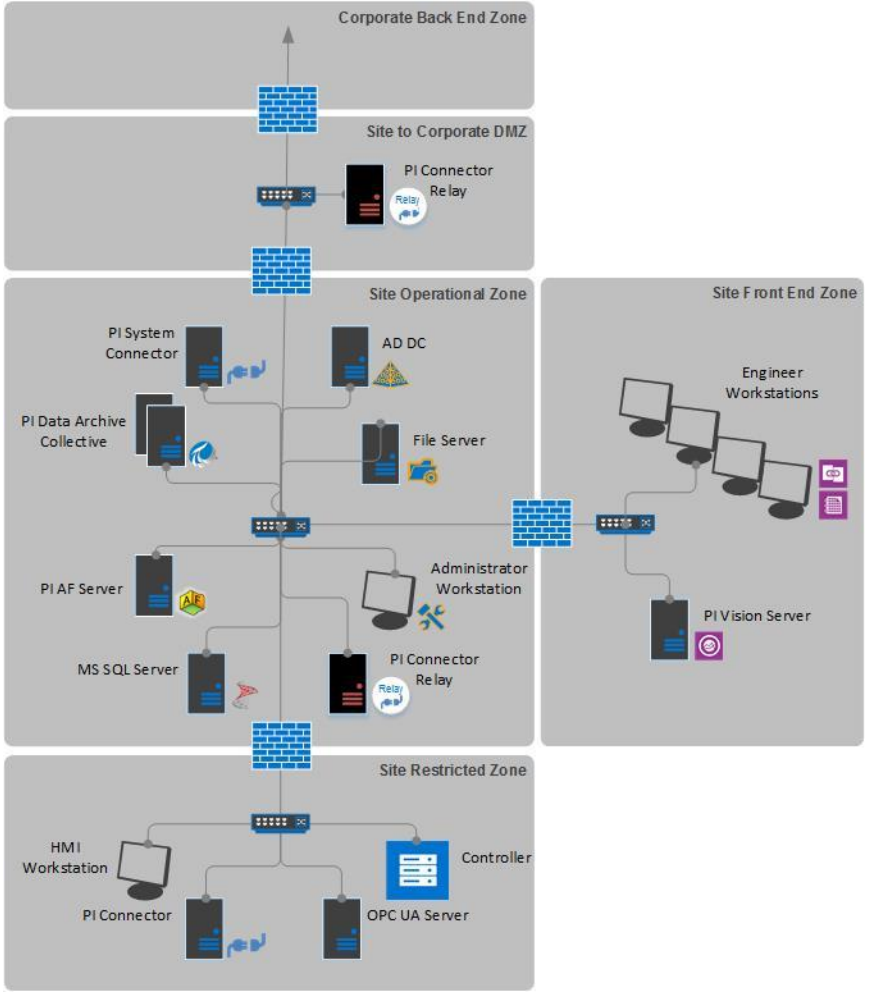
>>> Get the full TAM report

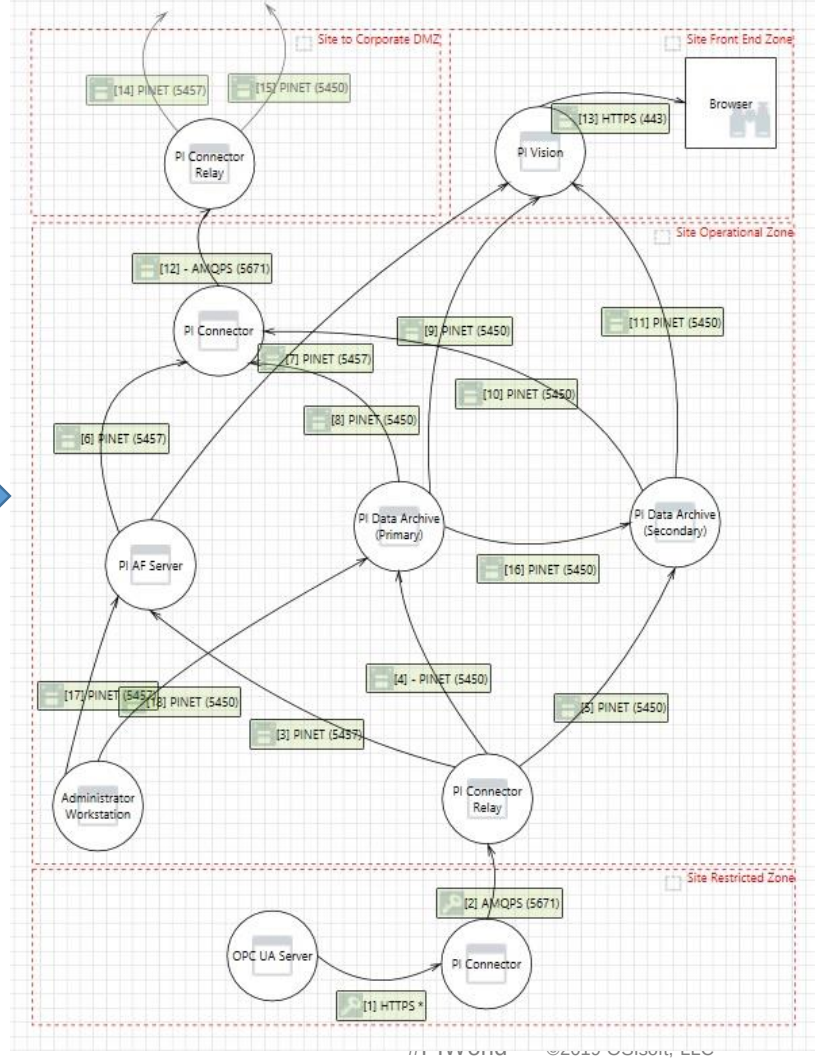
Michael Thow mthow@epri.com

Matt Gibson mgibson@epri.com

CSDS part 1

- Characterize Attack Surface and identify Exploit Sequences


Corporate Back End Zone
Site to Corporate DMZ
PI Connector Relay
Site Operational Zone
Site Front End Zone
PI System Connector
AD DC
Engineer Workstations
PI Data Archive Collective
File Server
PI AF Server
Administrator Workstation
PI Vision Server
MS SQL Server
PI Connector Relay
Site Restricted Zone
HMI Workstation
Controller
PI Connector
OPC UA Server


Site to Corporate DMZ
Site Front End Zone
Site Operational Zone
Site Restricted Zone
[14] PINET (5457)
[15] PINET (5450)
PI Connector Relay
[13] HTTPS (443)
Browser
PI Vision
[12] - AMQPS (5671)
PI Connector
[9] PINET (5450)
[11] PINET (5450)
[7] PINET (5457)
[10] PINET (5450)
[8] PINET (5450)
[6] PINET (5457)
PI Data Archive (Primary)
PI Data Archive (Secondary)
PI AF Server
[16] PINET (5450)
[4] - PINET (5450)
[17] PINET (5457)
[18] PINET (5450)
[5] PINET (5450)
[3] PINET (5457)
Administrator Workstation
PI Connector Relay
[2] AMQPS (5671)
OPC UA Server
PI Connector
[1] HTTPS *

CSDS part 1 – Attack Pathways

	CSDS Part 1c Attack Pathways		
	Refer to the separate instruction sheets for how to complete the workbook.		
Manufacturer		**Device Name**	**CSDS ID**
OSIsoft		PI Data Archive	CSDS1

Attack Pathway Number	Attack Vector	Physical Interface	Communications Protocol	Available Logical Port Numbers	Interface ID	Interfacing Connections	Attack Pathway Description
A01	Direct Network Access	RJ-45	TCP/IP		CSDS1-RJ-45-1		Windows Update patch data
A02	Direct Network Access	RJ-45	TCP/IP		CSDS1-RJ-45-2		PI Backup data
A03	Direct Network Access	RJ-45	TCP/IP		CSDS1-RJ-45-3		PowerShell remoting traffic
A04	Direct Network Access	RJ-45	TCP/IP		CSDS1-RJ-45-4		PINet requests
A05	Direct Network Access	RJ-45	Ethernet/IP		CSDS1-RJ-45-5		General network traffic
A06	Direct Network Access	Hard Drive	Operating System		CSDS1-Hard Drive-1		Windows backup image restoration
A07	Direct Network Access	Hard Drive	Operating System		CSDS1-Hard Drive-2		Windows audit events
A08	Direct Network Access	Hard Drive	Operating System		CSDS1-Hard Drive-3		System boot image
A09	Direct Network Access	Hard Drive	Operating System		CSDS1-Hard Drive-4		OS and application files stored on disk
A10	Portable Media & Equipment	USB	USB		CSDS1-USB-1		Removable media
A11	Direct Network Access	RJ-45	UDP		CSDS1-RJ-45-6		Upstream time data
A12	Direct Physical Access	Faceplate Knob or Button	Operating System		CSDS1-Faceplate Knob or Button-1		Physical access to host server
A13	Direct Network Access	RJ-45	TCP/IP		CSDS1-RJ-45-7		Windows Integrated Security (NTLM, Kerberos) data

EPRI TAM – Attack Surface Characterization

Objective Criteria that Bounds and Groups Exploit Objectives

- 28 Classes of Exploit Objectives
- Based On:
  - Direct Action
  - Critical Data
- Bounding
- Complete

- 5 Attack Vectors
  - Wired Network
  - Wireless Network
  - Portable Interfaces
  - Physical Access
  - Supply Chain
- Determine Specific Attack Pathways
- Determine Specific Exploit Mechanisms

Exploit Sequence = Exploit Objective + Attack Pathway + Exploit Mechanism

An exploit sequence is an attack pathway and exploit mechanism that allows an attacker to achieve an exploit objective.

Exploit Sequence Example

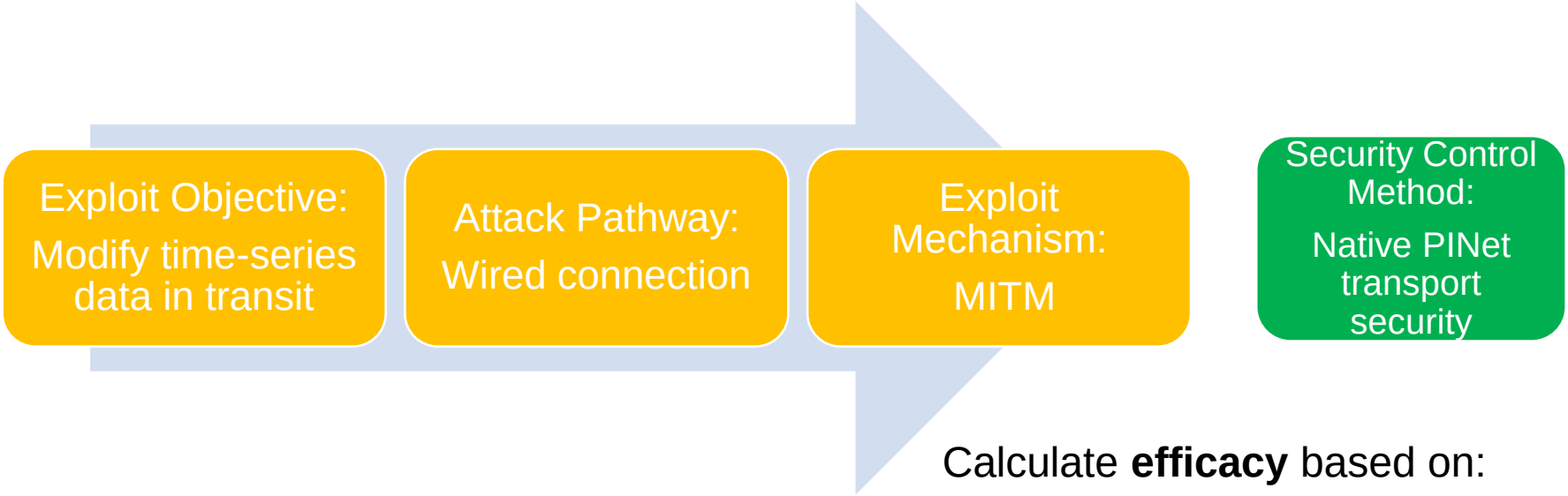
CSDS part 1 – Exploit Sequences

1	**CSDS Part 1d Identify Exploit Sequences**						
2	Refer to the separate instruction sheets for how to complete the workbook.						
3	**Manufacturer**	**Device Name**	**CSDS ID**				
4	OSIsoft	PI Data Archive 2018 SP2	PIDA2018SP2				
5							
6	**CSDS Part 1d: Exploit Sequences**						
7	**Exploit Objective**			**Description**	**Obj No.**	**Applies?**	**Applicable Attack Pathway(s)**	**Exploit Mechanism Number and D**
8	**Exploit Objectives Associated with Direct Action Against the Asset**							
9	**Component Enable/Disablement-Immediate**			**Means exist to immediately initiate or halt component operation.**	**E01**	**NO**		
10	**Component Disablement- Delayed**			**Means exist to degrade support systems or the environment for component operations, eventually resulting in component disablement.**	**E02**	**NO**		
11	**Denial of Service (DOS)**			**Means exist to interfere with the normal operation of the component by presenting false demands for component interaction at a component digital port.**	**E03**	**YES**	**A2**	**A2.X01 - Expensive queries repeatedly ex**
12	**Malware**			**Means exist to inject or install unauthorized and undetected program content on the component that does not constitute an alteration of existing authorized program content.**	**E04**	**NO**		
13	**Exploit Objectives Associated with the 6 Critical Data Types**							
14	**Operational Process Data**	**Theft**	**In Transit**	**Means exist to access and record operational process data while being transmitted to or from the component, including process variables, control signals, process element state information, alarms, and process data logs. Transmission includes digital data communication and the use of portable storage media.**	**E05**	**YES**	**A2**	**A2.X01 - Attacker intercepts PI data in tra**
15			**At Rest**	**Means exist to access and record operational process data while stored on the component, including process variables, control signals, process element state information, alarms, and process data logs.**	**E06**	**YES**	**A1,A2**	**A1.X01 - Attacker steals archive, queue o A2.X01 - Attacker reads data with PINET**
16		**Alteration**	**In Transit**	**Means exist to alter operational process data while being transmitted to or from the component, including process variables, control signals, process element state information, alarms, and process data logs. Transmission includes digital data communication and the use of portable storage media.**	**E07**	**YES**	**A2**	**A2.X01 - Attacker modifies PI data in tran**
17			**At Rest**	**Means exist to alter operational process data while stored on the component, including process variables, control signals, process element state information, alarms, and process data logs.**	**E08**	**YES**	**A2**	**A2.X01 - Attacker modifies data with PIN**
			In Transit	**Means exist to access and record program/configuration content that is installed and/or modified by the manufacturer while being transmitted to or from the component, including operating system (OS), firmware, tool software, and**	**E09**	**YES**	**A1,A2**	**A1.X01 - Steal PI configuration informati A2.X01 - Steal PI configuration informatio**

CSDS part 2

- Engineered Security Control Methods scoring and allocation

Allocating Engineered Security Control Methods



Set **Target Levels** for:
Protection
Detection
Response & Recovery

Calculate **efficacy** based on:
Protection
Detection
Response & Recovery
Persistence
Implementation cost

Allocating Engineered Security Control Methods

CSDS Part 2a Security Control Method Identification and Scoring			
Refer to the separate instruction sheets for how to complete the workbook.			
Manufacturer	**Device Name**	**CSDS ID**	
OSIsoft	PI Data Archive 2	PIDA2018SP2	
Cyber Security Control Methods			
CMID	**Method Type**	**CMID-Description**	**Control Method**
PIDA2018SP2-M-01	Engineered	PIDA2018SP2-M-01-PI Backup	PI Backup
PIDA2018SP2-M-02	Engineered	PIDA2018SP2-M-02-PI Data Archive Server Authentication Policy	PI Data Archive Server Authentication Policy
PIDA2018SP2-M-03	Engineered	PIDA2018SP2-M-03-PI Data Archive Database Security Access Control Lists	PI Data Archive Database Security Access Control Lists
PIDA2018SP2-M-04	Engineered	PIDA2018SP2-M-04-PINET Transport Security	PINET Transport Security
PIDA2018SP2-M-05	Engineered	PIDA2018SP2-M-05-PI Tuning for Expensive	PI Tuning for Expensive Query

Allocating Engineered Security Control Methods

Security Effectiveness Score			Implementation Burden				Method Efficacy		
Protect	Detect	Respond & Recover	Initial	O&M	Value	Burden	Protect	Detect	Respond & Recover
1.13	1.13	2.01	Medium	Low	1.5	Medium	3	3	4
2.01	1.13	1.13	Medium	Medium	2	Medium	4	3	3
2.01	1.13	1.13	Low	Low	1	Low	5	4	4
2.01	1.51	1.13	Medium	Medium	2	Medium	4	3	3

Allocating Engineered Security Control Methods

Manufacturer	Device Name	CSDS ID
OSIsoft	PI Data Archive 2018	PIDA2018SP2

		Combined Security Effectiveness Score				Target Levels			
Exploit Sequence	Attack Pathway	Protect	Detect	R/R	Residual Present?	Protect	Detect	R/R	Exploit Sequence Basis/Description
E03.A2.X01	A2	2.26	1.13	0.00	Yes	C	C	C	Expensive queries repeatedly executed.
E05.A2.X01	A2	2.01	1.51	0.00	Yes	C	C	C	Attacker intercepts PI data in transit.
E06.A1.X01	A1	0.00	0.00	0.00	Yes	C	C	C	Attacker steals archive, queue or snapshot files.
E06.A2.X01	A2	4.02	1.51	0.00	Yes	C	C	C	Attacker reads data with PINET requests.
E07.A2.X01	A2	2.01	1.51	2.01	Yes	C	C	C	Attacker modifies PI data in transit.
E08.A2.X01	A2	3.01	0.00	2.01	Yes	C	C	C	Attacker modifies data with PINET requests.
E09.A1.X01	A1	2.01	1.13	0.00	Yes	C	C	C	Steal PI configuration information in transit from PI backup data.

Cyber Security Data Sheets

Structured Security Documentation

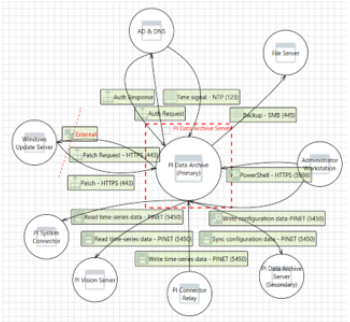
Forward looking with focus on:

- Modern Platform
- Recommended Architecture

PI Data Archive 2017 R2

CSDS Part 1: Attack Surface Characterization

CSDS Part 1a: Asset Characteristics

	General Asset Description:	Applicable Pictures/Diagrams:
1	Additional Equipment or Software Needed to Operate or Maintain: Windows Server 2016 Core, installed and configured as documented in *PI Data Archive Baseline Hardened Configuration*. The following assumptions are relevant to the scope of this CSDS: 1. The PI Data Archive is a primary node of a two-node collective. 2. There are no wireless network connections to the PI Data Archive server. 3. Physical server hardware selection is out of scope, though assumed to be commensurate to online hardware sizing tool guidance for the PI System. 4. No software is present other than the applications specified in the *PI Data Archive Baseline Hardened Configuration*. 5. Removable media is out of scope due to assumption that policy forbids use with the PI Data Archive server.	

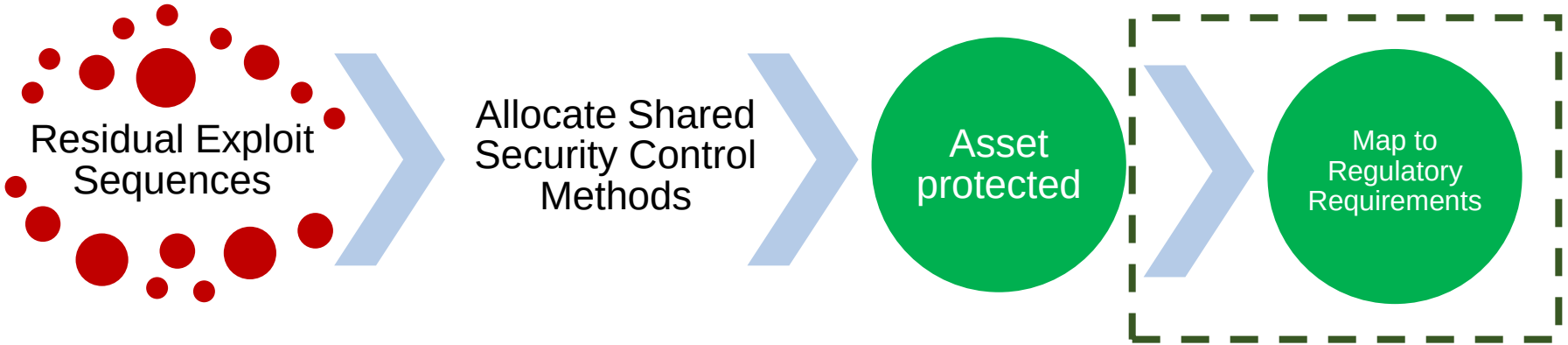
	Asset Composition, Make/Model, Functional Group, Baseline Hardened Configuration:
2	Reference CSDS? [Yes] Tailored CSDS? [ ] Describe Asset Composition: In scope is the PI Data Archive software, independent of the physical hardware or virtual host. The PI Data Archive provides efficient storage, archiving and retrieval of time series data.
	Manufacturer(s)/Model Number(s): PI Data Archive 2017 R2, OSIsoft, LLC, version 3.4.415.1188
	Higher Level Asset in Functional Group? [No] Aggregate CSDS? [No]
	Baseline Hardened Configuration? [Yes] Describe and Reference Baseline Hardening Documentation: Please see the accompanying *PI Data Archive Baseline Hardened Configuration* which describes the baseline installation of the PI Data Archive, operating system and the security controls related to this analysis.

	Vulnerability Information Availability (VIA) Level:
3	VIA Level 2 [X] Description: As detailed in the Baseline Hardened Configuration documentation, this assessment was conducted in a workbench environment where the system was examined internally and scanned. Reverse engineering and source code level review were not performed specifically for this CSDS.

TAM Step 3

- Mitigate residual Exploit Sequences
- Shared Security Control Methods

Residual Exploit Sequences are expected!



Optional, but useful:

- RG 5.71
- NEI 08-09
- NERC CIP
- NIST 800-53

Call to Action:

Cyber Security Data Sheets can be delivered by vendors as part of the supply chain

Step 1 & 2 by EPRI, Vendors, and other Stakeholders

CSDS Organization	
Step 1: Attack Surface Characterization	**Work Product**
Part 1a: Asset Characteristics	MS-Word document
Part 1b: Target Installation Configuration and Data Flow	
Part 1c: Attack Pathways	MS-Excel spreadsheet
Part 1d: Exploit Mechanisms for Applicable Classes of Exploit Objectives	MS-Excel spreadsheet
Step 2: Engineered Security Control Method Identification, Efficacy, and Allocation	
Part 2a: Engineered Security Control Method Identification and Efficacy	MS-Excel spreadsheet
Part 2b: Engineered Security Control Method Allocation	MS-Excel spreadsheet

Contact us to obtain **PI Data Archive** and **PI Vision Cyber Security Data Sheets**.

We'd love to hear your feedback!

Contact us for more information…

Lubos Mlcoch

lmlcoch@osisoft.com

Cyber Security Advisor

OSIsoft, LLC

Useful links

- OSIsoft PI System Cyber Security – Hub
- SANS - Sliding Scale of Cyber Security
- Windows Server 2019 — Server Core vs. Desktop Experience (GUI) Explained & Compared
- Hello, Windows Admin Center!
- AttackSurface Host Analyzer (AHA)
- Microsoft Attack Surface Analyzer
- EPRI - Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1

Questions?

Please wait for the **microphone**

State your **name & company**

Please remember to…

Complete Survey!

Navigate to this session in mobile agenda for survey