💻 HOW TO 💻

Extreme PI System Hardening

Harry Paul

OSIsoft Cyber Security Advisory Team, Customer Success

Agenda – a three act production

- Prologue
- **Act I: Power Tools**
- **Act II: Threat Modeling**
- **Act III: TTPs**
- Epilogue

Note: all examples in this presentation are on GitHub
https://gist.github.com/hpaul-osi/011257c57a0fd9228bca9e0f1dde23f6

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.* Calgary: Abterra

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.* Calgary: Abterra

HD Moore’s Law

> “Casual attacker power grows at the rate of Metasploit”

metasploit®   EXPLOIT DATABASE   SHODAN

Act I: Power Tools

Or, how I learned to stop worrying and love PowerShell

You’re recommending PowerShell?... For security?...

“Many targeted attack groups already use PowerShell in their attack chain”

~ Symantec Increased use of PowerShell in attacks

“52% of all attacks seen in 2017 were non-malware attacks.”

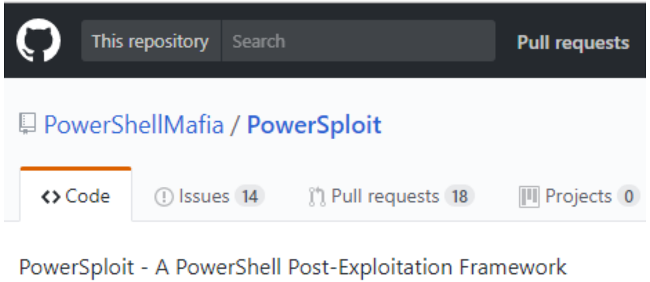
~ Carbon Black 2017 Threat Report

“PowerShell malware grow by 267% in Q4, and by 432% year over year”
~ McAfee Labs Threats Report, March 2018

Attackers are living off the land…

PS>Attack by Jared Haight

PowerShell Empire by @harmj0y, @sixdub, @enigma0x3, rvrsh3ll, @killswitch_gui, & @xorrior



PowerSploit - A PowerShell Post-Exploitation Framework

PowerSploit by PowerShellMafia

Top 10 reasons attackers <3 PS (annotated)

ubiquity ☺

- Installed by default
- Remote access by default with encryption
- Growing community
- System admins use and trust

stealth ☹

- Execute payloads from memory
- Few traces by default
- Easy to obfuscate
- Gateway sandboxes lagging on script-based malware detection

configuration dependent 😐

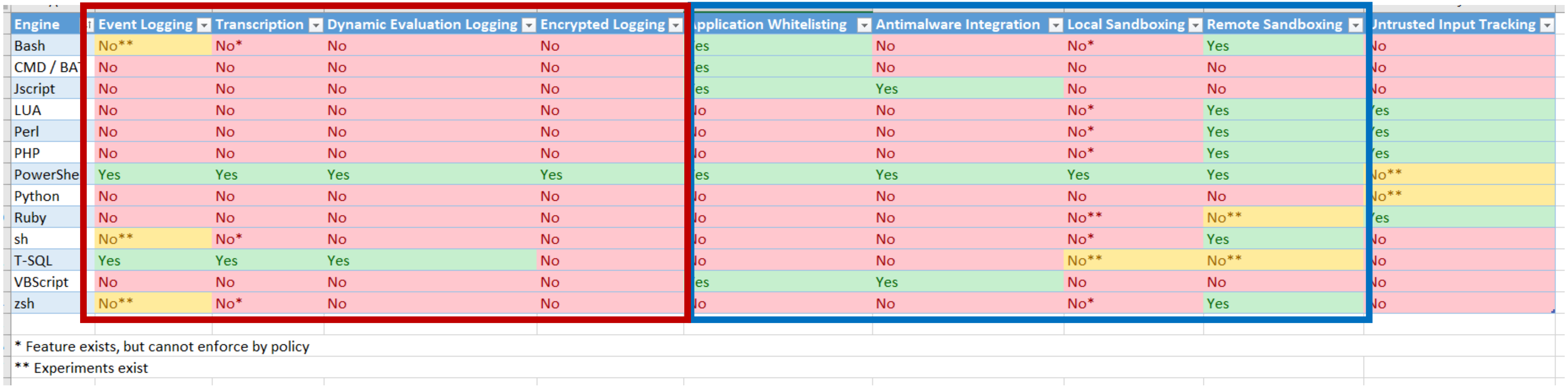
- Defenders overlook it when hardening their systems
- Bypass whitelisting tools ***depending on the configuration***

Symantec, Increased use of PowerShell in attacks

Sysadmins need to harness the power too!

Security features dramatically improved in latest platform

- Great overview in PowerShell at Enterprise Customers on MSDN
- Stealth: script block logging, module logging, & system-wide transcription
- Configuration: AuthN & AuthZ, default encryption, platform defenses



Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	pplication Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	ntrusted Input Tracking
Bash	No**	No*	No	No	es	No	No*	Yes	lo
CMD / BA	No	No	No	No	es	No	No	No	lo
Jscript	No	No	No	No	es	Yes	No	No	lo
LUA	No	No	No	No	lo	No	No*	Yes	es
Perl	No	No	No	No	lo	No	No*	Yes	es
PHP	No	No	No	No	lo	No	No*	Yes	es
PowerShe	Yes	Yes	Yes	Yes	es	Yes	Yes	Yes	lo**
Python	No	No	No	No	lo	No	No	No	lo**
Ruby	No	No	No	No	lo	No	No**	No**	es
sh	No**	No*	No	No	lo	No	No*	Yes	lo
T-SQL	Yes	Yes	Yes	No	lo	No	No**	No**	lo
VBScript	No	No	No	No	es	Yes	No	No	lo
zsh	No**	No*	No	No	lo	No	No*	Yes	lo

* Feature exists, but cannot enforce by policy

** Experiments exist

PowerShell Team Blog: A Comparison of Shell and Scripting Language Security (4/10/2017 post)

Bottom Line

"The improvements in WMF 5.0 (or WMF 4.0 with KB3000850) make PowerShell the worst tool of choice for a hacker when you enable script block logging and system-wide transcription. **Hackers will leave fingerprints everywhere**, unlike popular CMD utilities."

~ Ashley McGlone, Who's afraid of PowerShell security

With PS, we get DSC…
I mean, “Configuration as Code”

Declarative: separate intent from execution

- Decreased complexity
- Increased agility
- Consistency across applications
- Functional documentation

Broad scope (OS and applications)

- Baseline Configuration
- Hardening
- Site specific controls

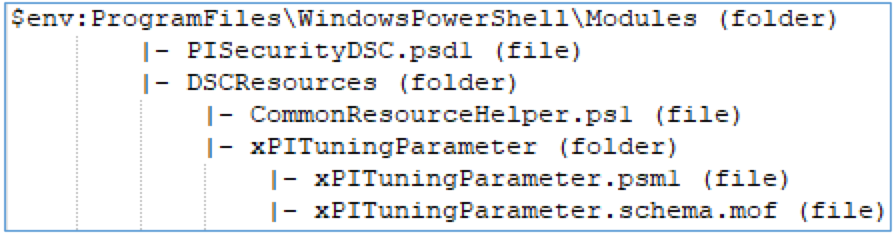
So, how does it work?

- **Configuration** – declarative script which define and configure Resources
- **Resource** – lightweight component (psm1 file) containing code to Get, Set or Test properties of an item from a Configuration
- **Local Configuration Manager (LCM)** – engine that facilitates interaction between Configurations and Resources.

DSC Resource – a special kind of module

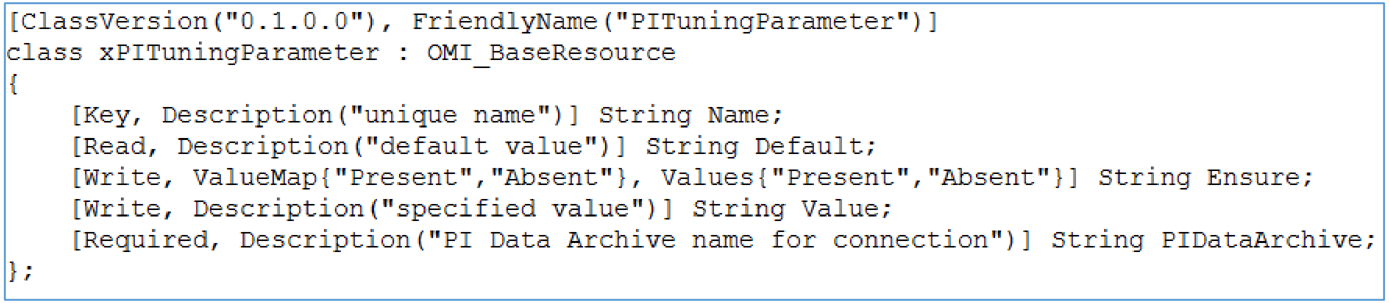
- Requires 3 functions
  - Get-TargetResource
  - Set-TargetResource
  - Test-TargetResource
- Supports helper functions

DSC Resource Structure Example



```
$env:ProgramFiles\WindowsPowerShell\Modules (folder)
        |- PISecurityDSC.psdl (file)
        |- DSCResources (folder)
            |- CommonResourceHelper.psl (file)
            |- xPITuningParameter (folder)
                |- xPITuningParameter.psml (file)
                |- xPITuningParameter.schema.mof (file)
```

DSC Resource Schema Example

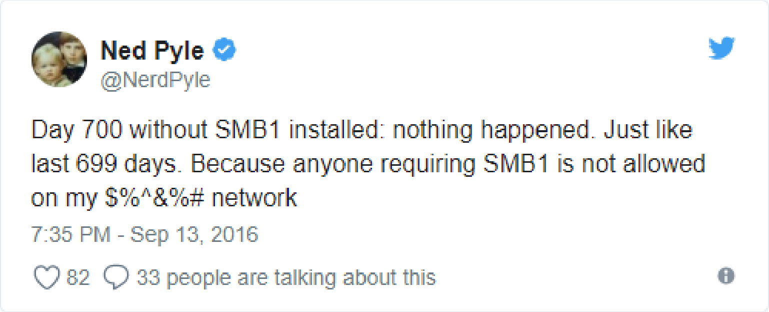


```
[ClassVersion("0.1.0.0"), FriendlyName("PITuningParameter")]
class xPITuningParameter : OMI_BaseResource
{
    [Key, Description("unique name")] String Name;
    [Read, Description("default value")] String Default;
    [Write, ValueMap{"Present","Absent"}, Values{"Present","Absent"}] String Ensure;
    [Write, Description("specified value")] String Value;
    [Required, Description("PI Data Archive name for connection")] String PIDataArchive;
};
```

Example: Windows Feature Blacklist

Pathologically unfit, yet default enabled features.

- SMBv1
  - Stop using SMB1 by Ned Pyle
  - Securing Windows Workstations by ADSecurity
- PSv2
  - Windows PowerShell 2.0 Deprecation
  - Medium severity finding with STIG Viewer (V-70637)
  - Detecting and Preventing PS Downgrade Attacks by Lee Holmes
  - All those benefits I talked about in 5.0 aren’t there!



Ned Pyle
@NerdPyle

Day 700 without SMB1 installed: nothing happened. Just like last 699 days. Because anyone requiring SMB1 is not allowed on my $%^&%# network

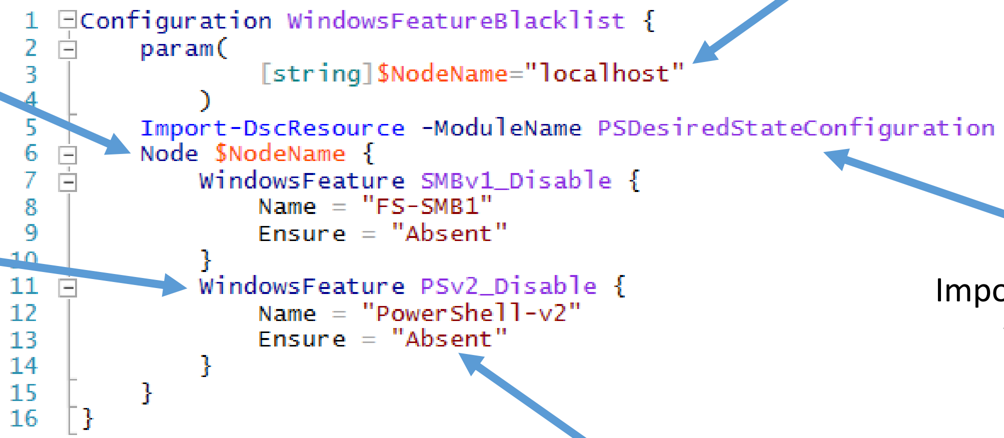
7:35 PM - Sep 13, 2016

♡ 82 33 people are talking about this

DSC Configuration – a special kind of function

Configurations can have parameters

Scope configuration items to a node



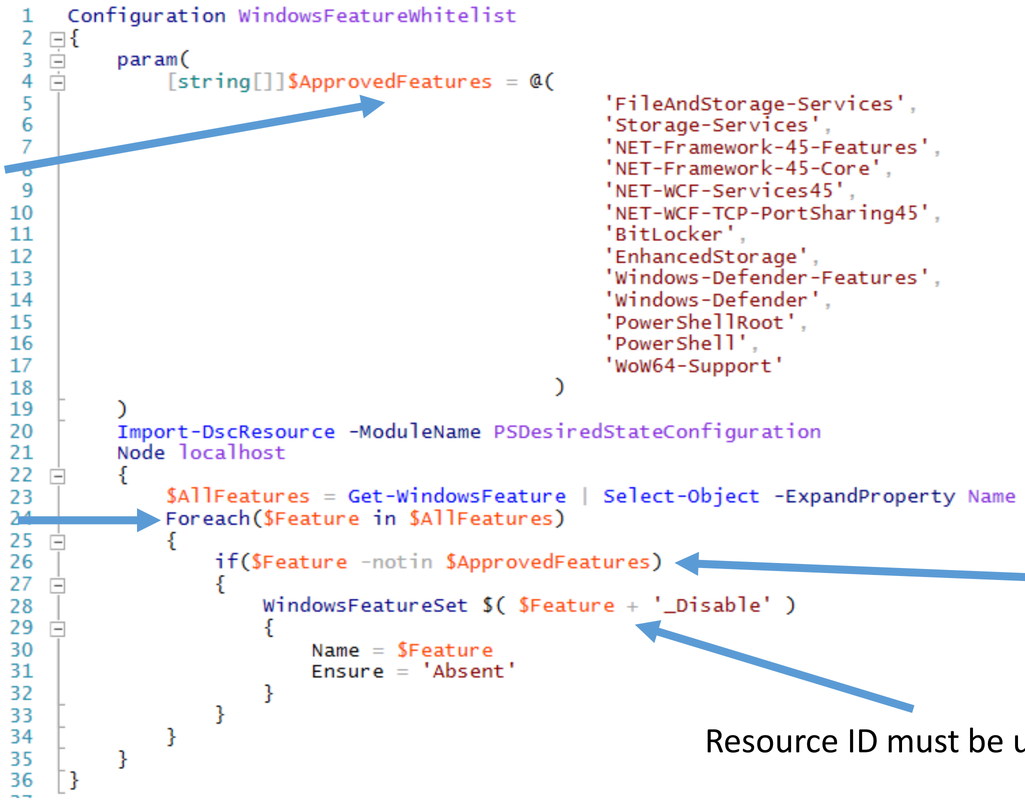
```
Configuration WindowsFeatureBlacklist {
    param(
            [string]$NodeName="localhost"
        )
    Import-DscResource -ModuleName PSDesiredStateConfiguration
    Node $NodeName {
        WindowsFeature SMBv1_Disable {
            Name = "FS-SMB1"
            Ensure = "Absent"
        }
        WindowsFeature PSv2_Disable {
            Name = "PowerShell-v2"
            Ensure = "Absent"
        }
    }
}
```

Built-in resource to manipulate features

Import whatever resources your config needs

Make sure it’s not Present

Example: Windows Feature Whitelist



```
Configuration WindowsFeatureWhitelist
{
    param(
        [string[]]$ApprovedFeatures = @(
                                          'FileAndStorage-Services',
                                          'Storage-Services',
                                          'NET-Framework-45-Features',
                                          'NET-Framework-45-Core',
                                          'NET-WCF-Services45',
                                          'NET-WCF-TCP-PortSharing45',
                                          'BitLocker',
                                          'EnhancedStorage',
                                          'Windows-Defender-Features',
                                          'Windows-Defender',
                                          'PowerShellRoot',
                                          'PowerShell',
                                          'WoW64-Support'
                                      )
    )
    Import-DscResource -ModuleName PSDesiredStateConfiguration
    Node localhost
    {
        $AllFeatures = Get-WindowsFeature | Select-Object -ExpandProperty Name
        Foreach($Feature in $AllFeatures)
        {
            if($Feature -notin $ApprovedFeatures)
            {
                WindowsFeatureSet $( $Feature + '_Disable' )
                {
                    Name = $Feature
                    Ensure = 'Absent'
                }
            }
        }
    }
}
```

Specify a whitelist

Interrogate the system

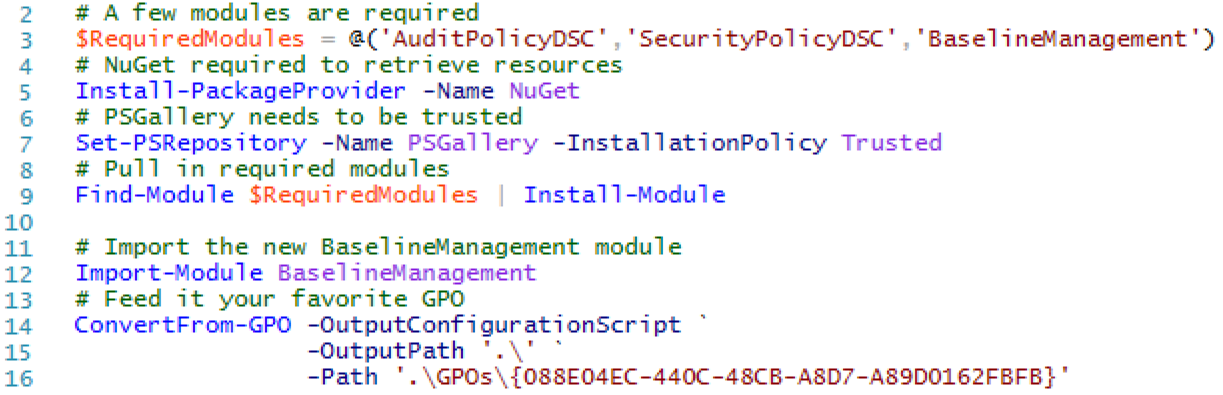
Implement logic/loops

Filter out items

Resource ID must be unique

Demo 1: Microsoft OS Baseline a la DSC

- Server 2016 Baseline from [Microsoft Security Guidance Blog]()
- Applies >100 recommended settings
- Auditing for security events, e.g.
  - Logon/Logoff
  - Removable storage
  - Policy change
- Lock down privileges, e.g.
  - SeCreatePermanentPrivilege
  - SeTcbPrivilege
  - SeTrustedCredManAccessPrivilege



```
# A few modules are required
$RequiredModules = @('AuditPolicyDSC','SecurityPolicyDSC','BaselineManagement')
# NuGet required to retrieve resources
Install-PackageProvider -Name NuGet
# PSGallery needs to be trusted
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
# Pull in required modules
Find-Module $RequiredModules | Install-Module

# Import the new BaselineManagement module
Import-Module BaselineManagement
# Feed it your favorite GPO
ConvertFrom-GPO -OutputConfigurationScript `
                -OutputPath '.\' `
                -Path '.\GPOs\{088E04EC-440C-48CB-A8D7-A89D0162FBFB}'
```

Leveraging PowerShell for the PI System

System Administration

- PowerShell Tools for the PI System
- Packaged with PI System Management Tools

Security Configuration Auditing

- PI Security Audit Tools
- Available on TS site
- Open source on GitHub [repo]

Configuration as Code

- PI Security DSC Resources
- Open source on GitHub [repo location]

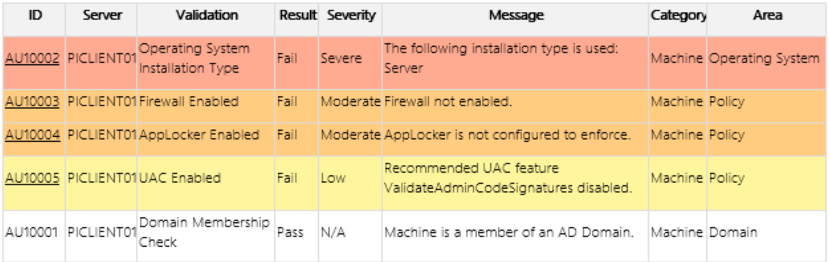
PI Security Audit Tools

Validated components:

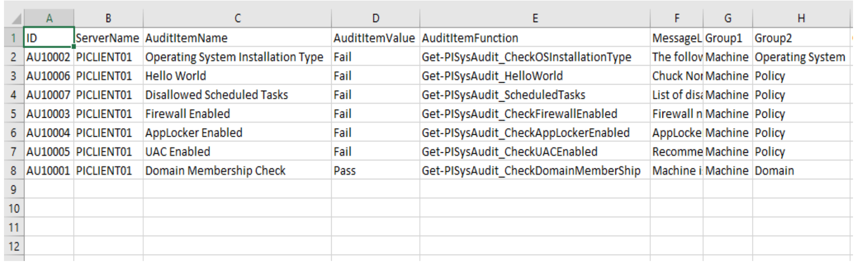
- Machine (General)
- PI Data Archive
- PI AF Server
- MS SQL Server
- PI Vision
- PI Web API

Requirements:

- PSv3+
- Run as Admin (AF & Vision)
- OSIsoft.PowerShell
- WinRM enabled (if remote)

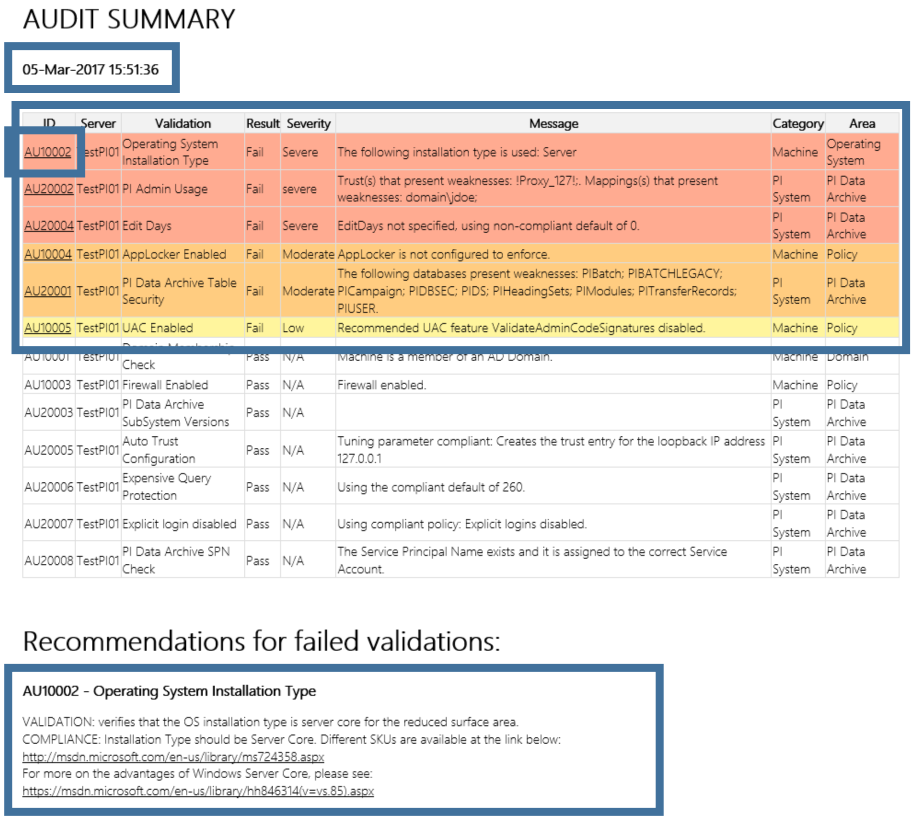


ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	PICLIENT01	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU10003	PICLIENT01	Firewall Enabled	Fail	Moderate	Firewall not enabled.	Machine	Policy
AU10004	PICLIENT01	AppLocker Enabled	Fail	Moderate	AppLocker is not configured to enforce.	Machine	Policy
AU10005	PICLIENT01	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU10001	PICLIENT01	Domain Membership Check	Pass	N/A	Machine is a member of an AD Domain.	Machine	Domain



	A	B	C	D	E	F	G	H
1	ID	ServerName	AuditItemName	AuditItemValue	AuditItemFunction	MessageL	Group1	Group2
2	AU10002	PICLIENT01	Operating System Installation Type	Fail	Get-PISysAudit_CheckOSInstallationType	The follov	Machine	Operating System
3	AU10006	PICLIENT01	Hello World	Fail	Get-PISysAudit_HelloWorld	Chuck Noı	Machine	Policy
4	AU10007	PICLIENT01	Disallowed Scheduled Tasks	Fail	Get-PISysAudit_ScheduledTasks	List of dis‹	Machine	Policy
5	AU10003	PICLIENT01	Firewall Enabled	Fail	Get-PISysAudit_CheckFirewallEnabled	Firewall n	Machine	Policy
6	AU10004	PICLIENT01	AppLocker Enabled	Fail	Get-PISysAudit_CheckAppLockerEnabled	AppLocke	Machine	Policy
7	AU10005	PICLIENT01	UAC Enabled	Fail	Get-PISysAudit_CheckUACEnabled	Recomme	Machine	Policy
8	AU10001	PICLIENT01	Domain Membership Check	Pass	Get-PISysAudit_CheckDomainMemberShip	Machine i	Machine	Domain
9								
10								
11								
12								

Demo 2: Produce an Audit Report



AUDIT SUMMARY

05-Mar-2017 15:51:36

ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	TestPI01	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU20002	TestPI01	PI Admin Usage	Fail	severe	Trust(s) that present weaknesses: !Proxy_127!;. Mappings(s) that present weaknesses: domain\jdoe;	PI System	PI Data Archive
AU20004	TestPI01	Edit Days	Fail	Severe	EditDays not specified, using non-compliant default of 0.	PI System	PI Data Archive
AU10004	TestPI01	AppLocker Enabled	Fail	Moderate	AppLocker is not configured to enforce.	Machine	Policy
AU20001	TestPI01	PI Data Archive Table Security	Fail	Moderate	The following databases present weaknesses: PIBatch; PIBATCHLEGACY; PICampaign; PIDBSEC; PIDS; PIHeadingSets; PIModules; PITransferRecords; PIUSER.	PI System	PI Data Archive
AU10005	TestPI01	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU10001	TestPI01	Domain Membership Check	Pass	N/A	Machine is a member of an AD Domain.	Machine	Domain
AU10003	TestPI01	Firewall Enabled	Pass	N/A	Firewall enabled.	Machine	Policy
AU20003	TestPI01	PI Data Archive SubSystem Versions	Pass	N/A		PI System	PI Data Archive
AU20005	TestPI01	Auto Trust Configuration	Pass	N/A	Tuning parameter compliant: Creates the trust entry for the loopback IP address 127.0.0.1	PI System	PI Data Archive
AU20006	TestPI01	Expensive Query Protection	Pass	N/A	Using the compliant default of 260.	PI System	PI Data Archive
AU20007	TestPI01	Explicit login disabled	Pass	N/A	Using compliant policy: Explicit logins disabled.	PI System	PI Data Archive
AU20008	TestPI01	PI Data Archive SPN Check	Pass	N/A	The Service Principal Name exists and it is assigned to the correct Service Account.	PI System	PI Data Archive

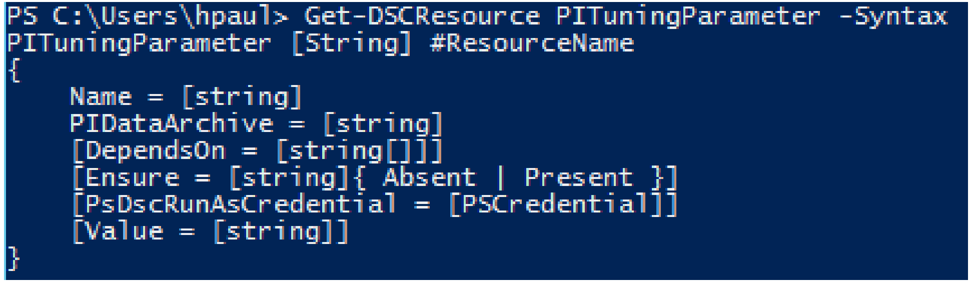
Recommendations for failed validations:

AU10002 - Operating System Installation Type

VALIDATION: verifies that the OS installation type is server core for the reduced surface area.
COMPLIANCE: Installation Type should be Server Core. Different SKUs are available at the link below:
http://msdn.microsoft.com/en-us/library/ms724358.aspx
For more on the advantages of Windows Server Core, please see:
https://msdn.microsoft.com/en-us/library/hh846314(v=vs.85).aspx

PI Security DSC Resources

- Getting Started Guide in Wiki
- Resource syntax
  - PI Security DSC Resource Reference
  - Ad hoc with Get-DscResource



```
PS C:\Users\hpaul> Get-DSCResource PITuningParameter -Syntax
PITuningParameter [String] #ResourceName
{
    Name = [string]
    PIDataArchive = [string]
    [DependsOn = [string[]]]
    [Ensure = [string]{ Absent | Present }]
    [PsDscRunAsCredential = [PSCredential]]
    [Value = [string]]
}
```

Configuration AF DB

- AFAttribute

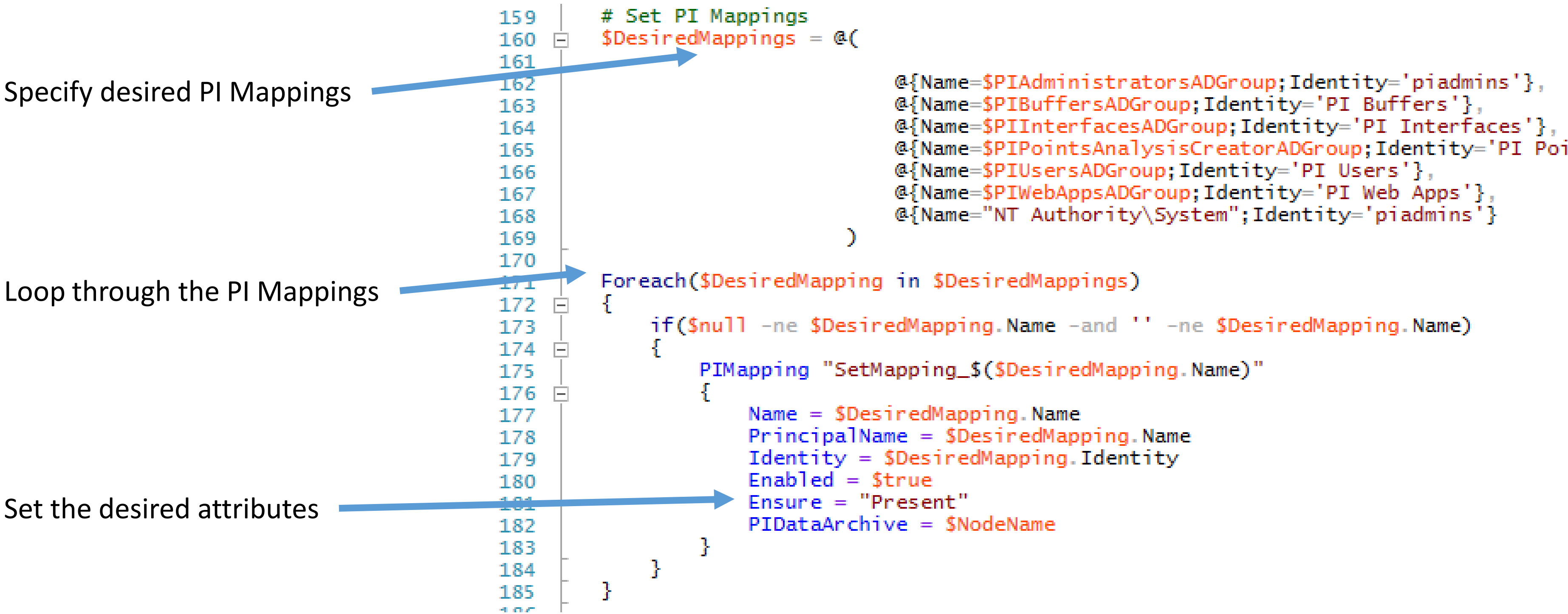
PI AF Security

- AFIdentity
- AFMapping

PI Data Archive

- PIDatabaseSecurity
- PIFirewall
- PIIdentity
- PIMapping
- PIPoint – PtSecurity & DataSecurity only
- PITrust
- PITuningParameter

Demo 3: PI Mappings (and more) via DSC



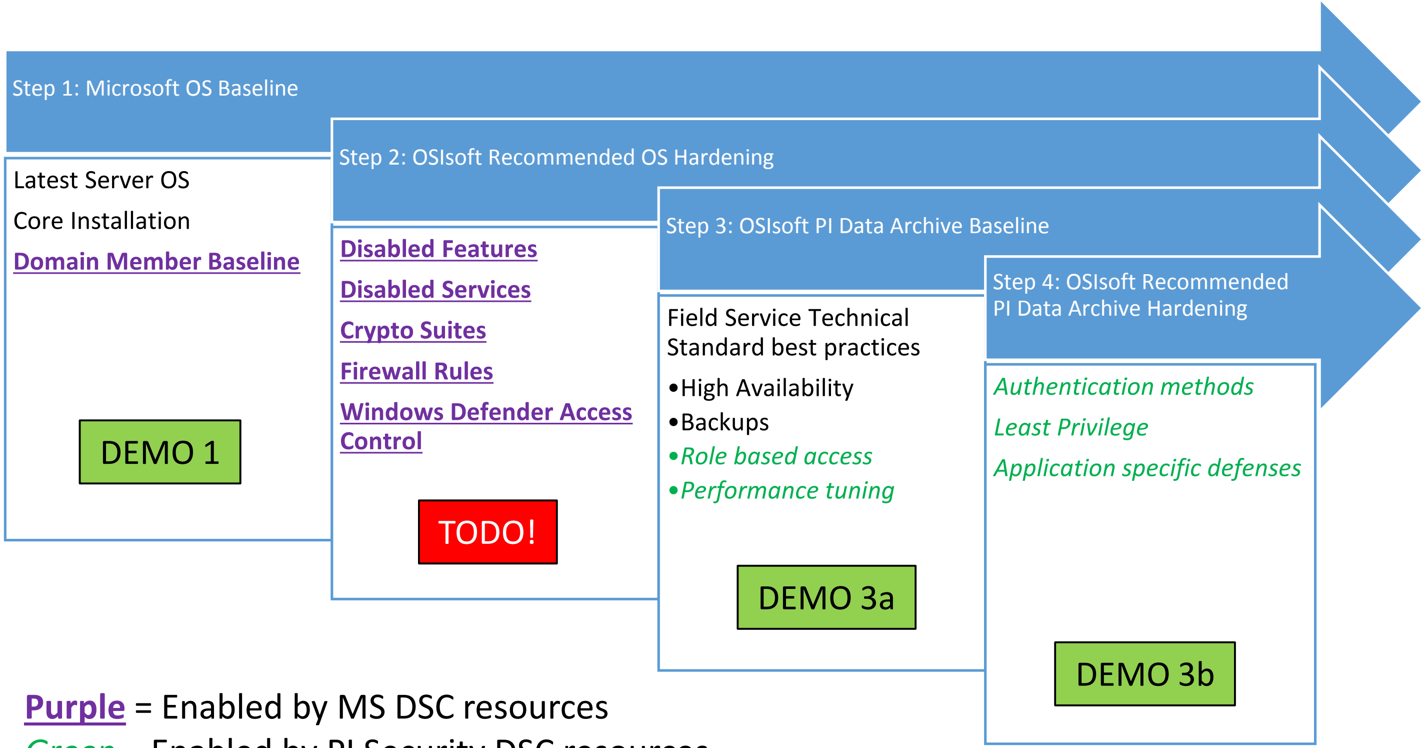
Specify desired PI Mappings

Loop through the PI Mappings

Set the desired attributes

```
# Set PI Mappings
$DesiredMappings = @(

                        @{Name=$PIAdministratorsADGroup;Identity='piadmins'},
                        @{Name=$PIBuffersADGroup;Identity='PI Buffers'},
                        @{Name=$PIInterfacesADGroup;Identity='PI Interfaces'},
                        @{Name=$PIPointsAnalysisCreatorADGroup;Identity='PI Poi
                        @{Name=$PIUsersADGroup;Identity='PI Users'},
                        @{Name=$PIWebAppsADGroup;Identity='PI Web Apps'},
                        @{Name="NT Authority\System";Identity='piadmins'}
                    )

Foreach($DesiredMapping in $DesiredMappings)
{
    if($null -ne $DesiredMapping.Name -and '' -ne $DesiredMapping.Name)
    {
        PIMapping "SetMapping_$($DesiredMapping.Name)"
        {
            Name = $DesiredMapping.Name
            PrincipalName = $DesiredMapping.Name
            Identity = $DesiredMapping.Identity
            Enabled = $true
            Ensure = "Present"
            PIDataArchive = $NodeName
        }
    }
}
```

Hardened Baseline Configuration



Step 1: Microsoft OS Baseline

Latest Server OS

Core Installation

Domain Member Baseline

DEMO 1

Step 2: OSIsoft Recommended OS Hardening

Disabled Features

Disabled Services

Crypto Suites

Firewall Rules

Windows Defender Access Control

TODO!

Step 3: OSIsoft PI Data Archive Baseline

Field Service Technical Standard best practices

- High Availability
- Backups
- *Role based access*
- *Performance tuning*

DEMO 3a

Step 4: OSIsoft Recommended PI Data Archive Hardening

Authentication methods

Least Privilege

Application specific defenses

DEMO 3b

Purple = Enabled by MS DSC resources

Green = Enabled by PI Security DSC resources

Benefits of Windows Integrated Security

Less work for administrators

- Identity and Access Management
- SSO

Improved security

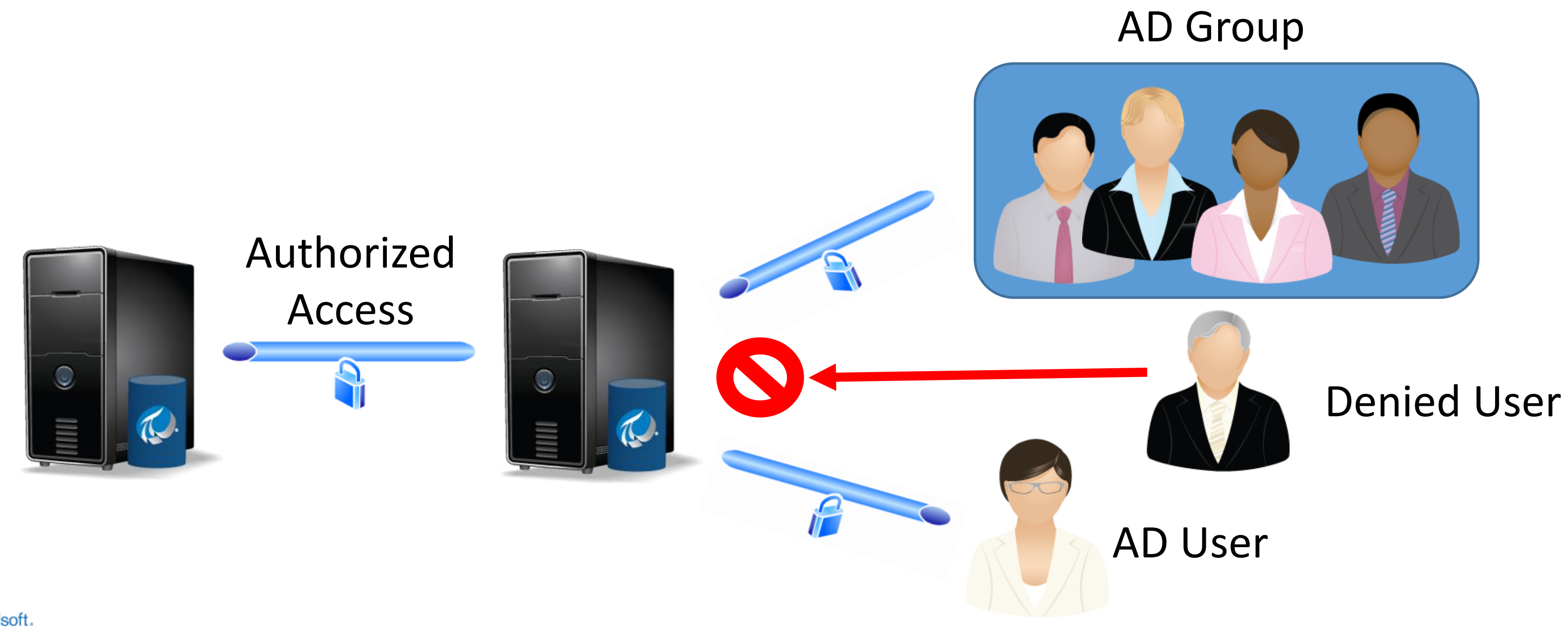
- Strong authentication
- Transport security for native protection
- Authentication management
- Audit connections

Flexibility

- Role-based access
- Leverage existing paradigm

Less work for administrators

- Leverage standard platform technologies
- AD provides SSO and Identity and Access Management



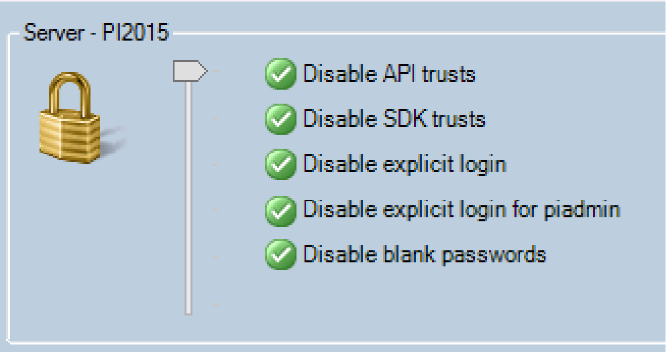
Strong Authentication

PI User and PI Trust (WEAK)

- AL00206 – Security Alert: PI Authentication Weakness
- AL00309 – Windows Integrated Security (WIS) replaces PI Trusts and Explicit Logins in PI API 2016

PI Mappings (STRONG)

- Authenticate through Windows SSPI.
- Leverage Kerberos



Server - PI2015

✓ Disable API trusts
✓ Disable SDK trusts
✓ Disable explicit login
✓ Disable explicit login for piadmin
✓ Disable blank passwords

Allow only the strongest method server-side.

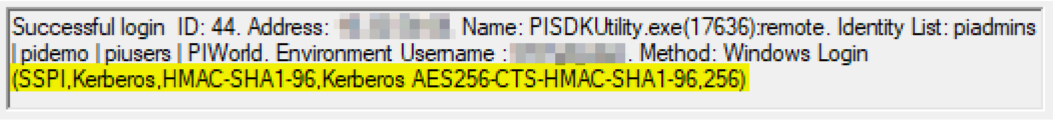
Transport Security

- Enabled automatically for WIS connections
- Messages signed for integrity and encrypted for privacy
- Supported with PI Data Archive 2015+ with the connecting client:
  - PI Buffer Subsystem 4.4 or later
  - PI AF SDK 2015 or later
  - PI SDK 2016 or later
  - PI API 2016 for WIS

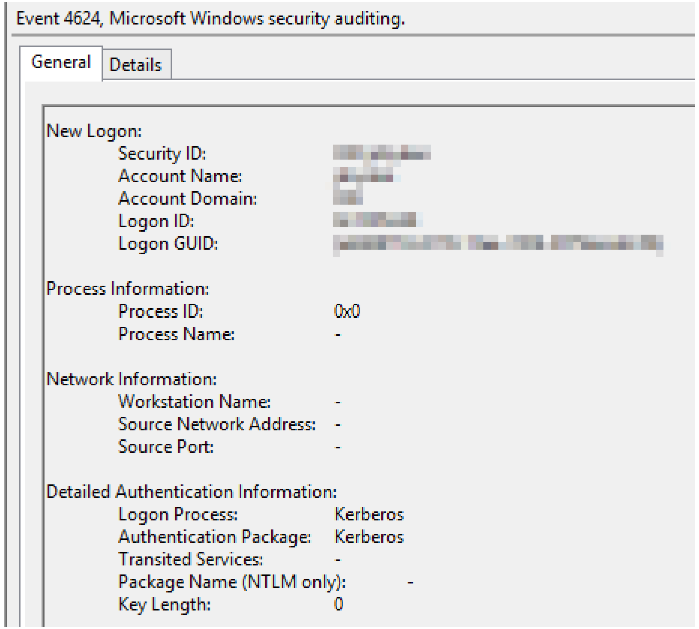
KB01092 – PI System and Data Encryption

Auditability

- Connection auditing through
  - Security event logs
  - PI Message Logs (Message ID: 7082)
  - PI Data Archive connection history



```
Successful login  ID: 44. Address: [redacted] Name: PISDKUtility.exe(17636):remote. Identity List: piadmins
| pidemo | piusers | PIWorld. Environment Username : [redacted]. Method: Windows Login
(SSPI,Kerberos,HMAC-SHA1-96,Kerberos AES256-CTS-HMAC-SHA1-96,256)
```



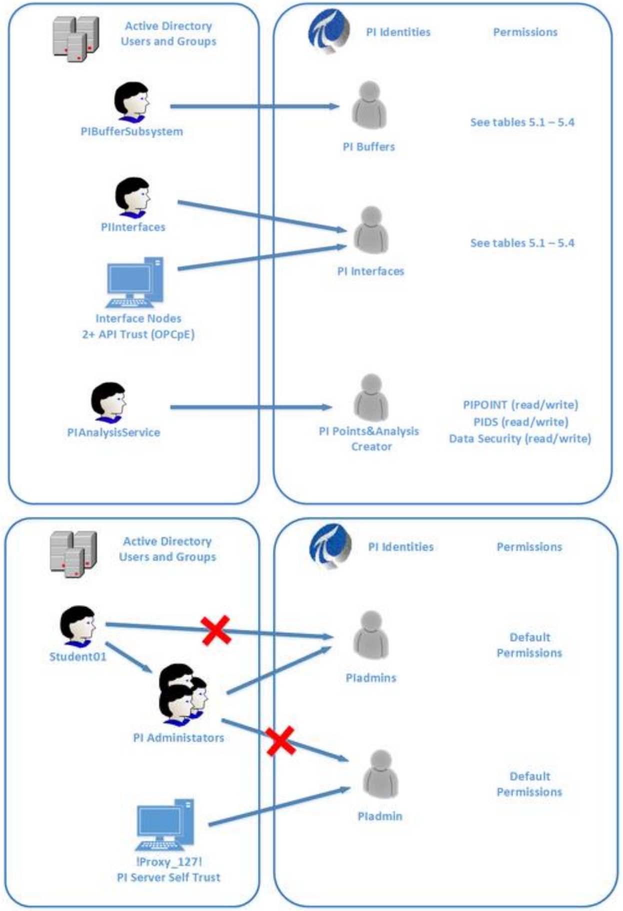
Event 4624, Microsoft Windows security auditing.

```
New Logon:
        Security ID:                [redacted]
        Account Name:               [redacted]
        Account Domain:             [redacted]
        Logon ID:                   [redacted]
        Logon GUID:                 [redacted]

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           -
        Source Network Address:     -
        Source Port:                -

Detailed Authentication Information:
        Logon Process:              Kerberos
        Authentication Package:     Kerberos
        Transited Services:         -
        Package Name (NTLM only):       -
        Key Length:                 0
```

WIS Best Practices

Codified in KB01072

- Practical Access Levels
  - Administrator
  - PI Interfaces
  - PI Buffers
  - PI Users
  - PI Point and Analysis creator
  - PI Web Apps
- No god user
  - piadmin for disaster recovery only
  - piadmins for admin tasks



Myth Busting!

MYTH #1: PI Mappings cannot be used in a workgroup

TRUTH: Applications can use PI Mappings between untrusted domains or workgroup nodes.

KB01457 – Using Windows Credential Manager with PI Applications

MYTH #2: PI Mappings require more open ports than PI Trusts

TRUTH: No additional ports required to migrate to mappings.

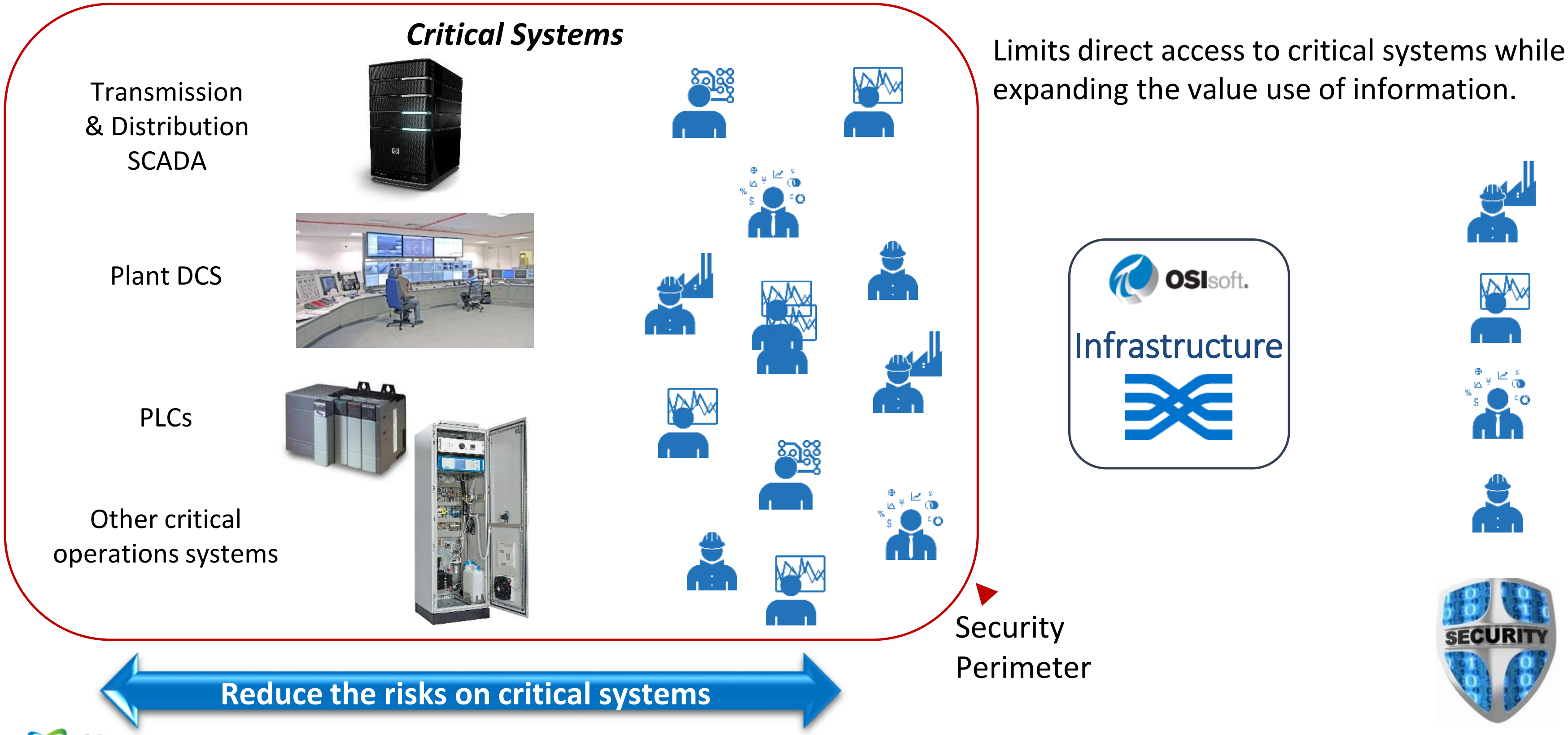
2820OSI8 – Which firewall ports should be opened for a PI Data Archive.

Act II: Threat Modeling

Beyond F!R3W@LLZ

Core Security Value of the PI System

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



Critical Systems

Transmission & Distribution SCADA

Plant DCS

PLCs

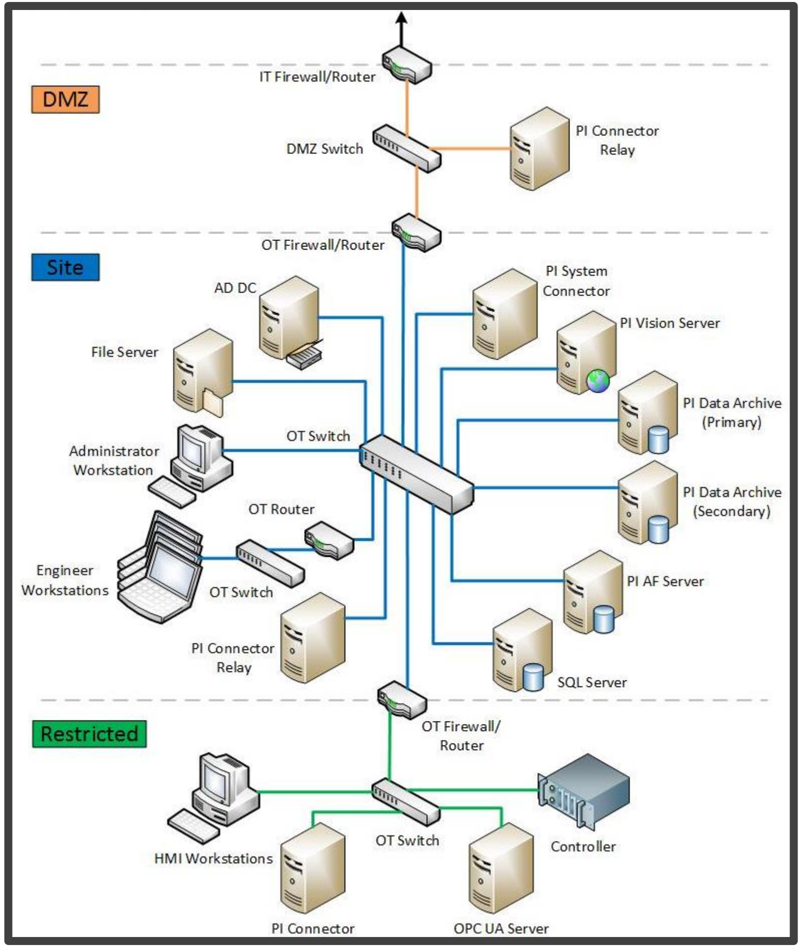
Other critical operations systems

Security Perimeter

Reduce the risks on critical systems

Data Flow Architecture

- AD DS & DNS
- Administrator Workstation
- File Server
- PI Connector Relay
- PI Data Archive Server (Primary)
- PI Data Archive Server (Secondary)
- PI System Connector
- PI Vision Server
- Windows Update Server



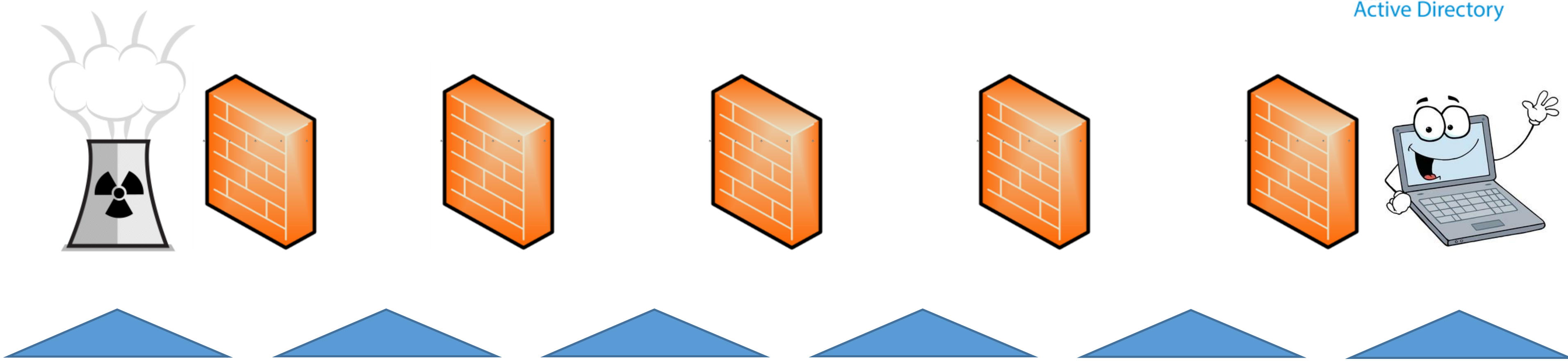
Network Zones

- Segment system components
- Data protocol only across segments

Note:

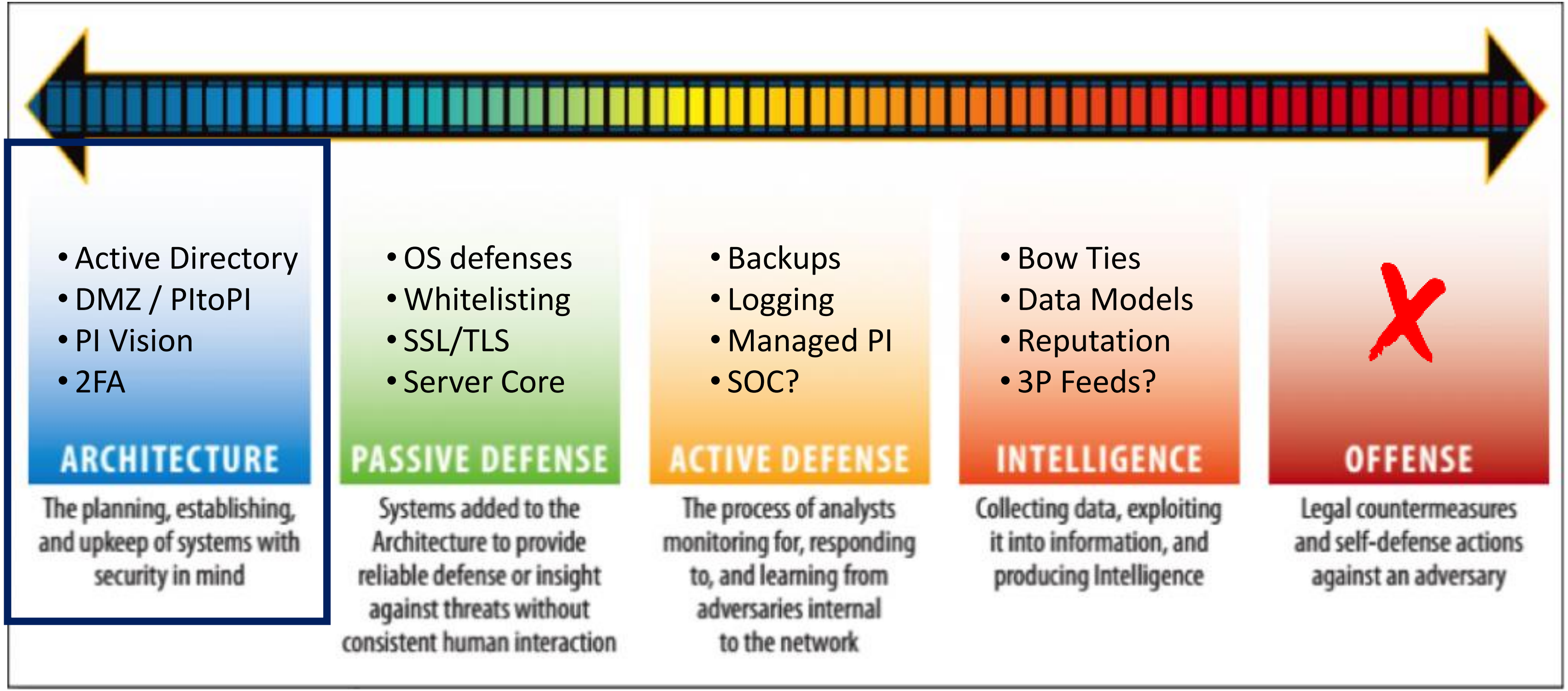
!= Security

Microsoft Active Directory



Restricted Zone Operational Zone DMZ Back End Zone Front End Zone User Zone

Built-in vs Bolt-on defenses: SANS 'Sliding Scale'



- Active Directory
- DMZ / PItoPI
- PI Vision
- 2FA

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

- OS defenses
- Whitelisting
- SSL/TLS
- Server Core

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

- Backups
- Logging
- Managed PI
- SOC?

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

- Bow Ties
- Data Models
- Reputation
- 3P Feeds?

INTELLIGENCE

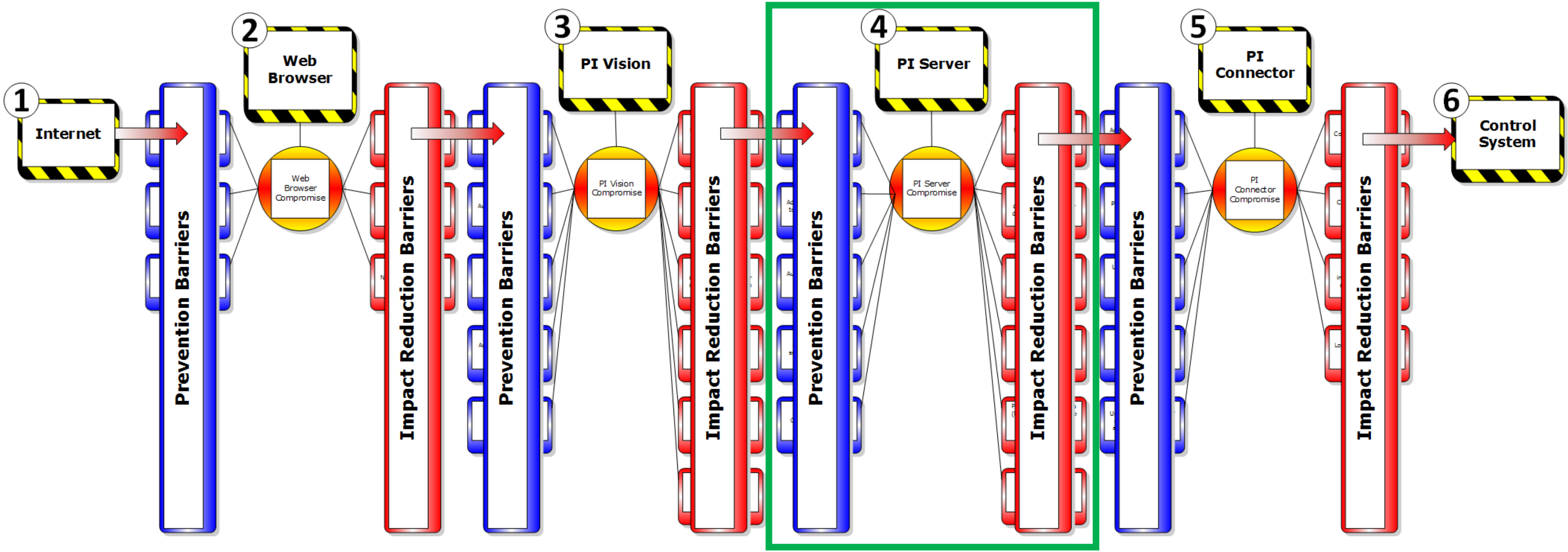
Collecting data, exploiting it into information, and producing Intelligence

✗

OFFENSE

Legal countermeasures and self-defense actions against an adversary

Modern PI System Kill Chain



Application Server Threats and Impacts

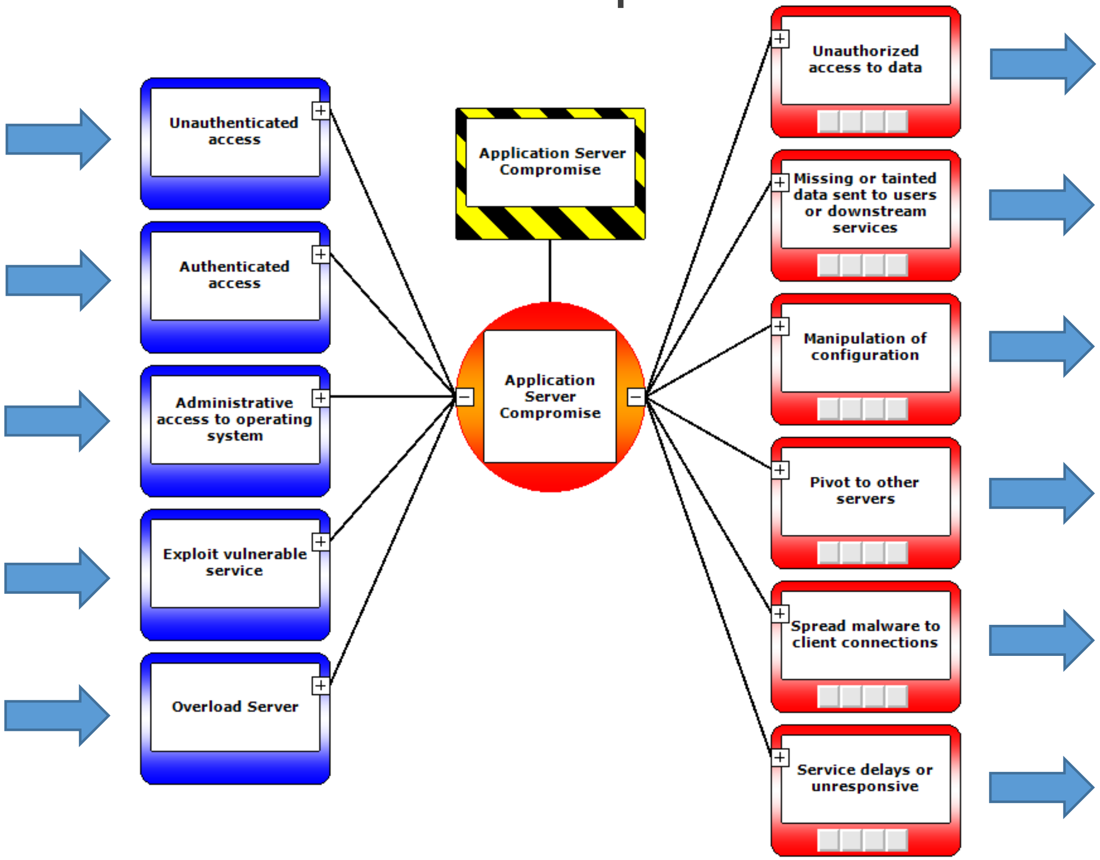
Snooping/Spoofing

Insider Threat/Stolen Creds

Pwn OS/Admin

Malware/0-Day

Expensive calls/Botnet



Application Server Compromise

Unauthenticated access

Authenticated access

Administrative access to operating system

Exploit vulnerable service

Overload Server

Application Server Compromise

Unauthorized access to data

Missing or tainted data sent to users or downstream services

Manipulation of configuration

Pivot to other servers

Spread malware to client connections

Service delays or unresponsive

Info Leakage

Misleading Reports

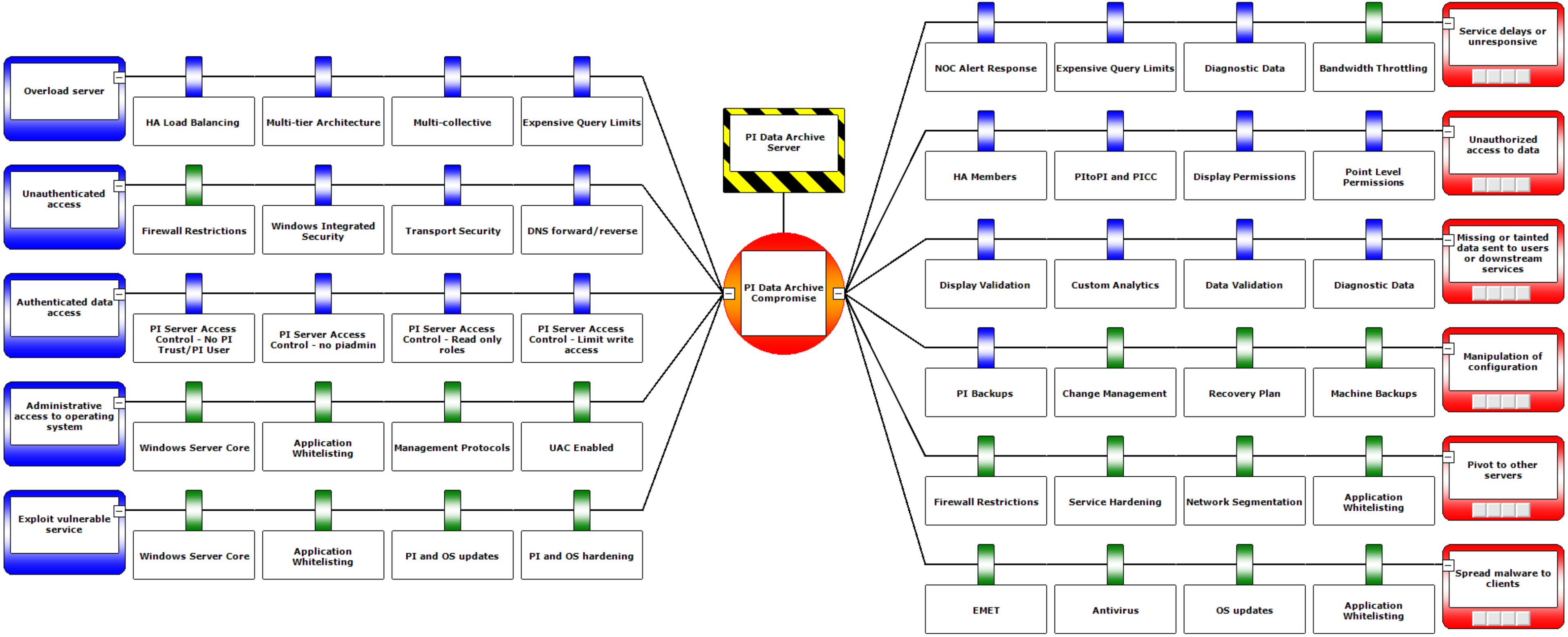
Lost Data/Backdoor

Call Home/Move Deeper

RATs/Ransomware

Critical Data Unavailable

PI Data Archive Bow Tie



Overload server
HA Load Balancing
Multi-tier Architecture
Multi-collective
Expensive Query Limits

Unauthenticated access
Firewall Restrictions
Windows Integrated Security
Transport Security
DNS forward/reverse

Authenticated data access
PI Server Access Control - No PI Trust/PI User
PI Server Access Control - no piadmin
PI Server Access Control - Read only roles
PI Server Access Control - Limit write access

Administrative access to operating system
Windows Server Core
Application Whitelisting
Management Protocols
UAC Enabled

Exploit vulnerable service
Windows Server Core
Application Whitelisting
PI and OS updates
PI and OS hardening

PI Data Archive Server

PI Data Archive Compromise

NOC Alert Response
Expensive Query Limits
Diagnostic Data
Bandwidth Throttling
Service delays or unresponsive

HA Members
PItoPI and PICC
Display Permissions
Point Level Permissions
Unauthorized access to data

Display Validation
Custom Analytics
Data Validation
Diagnostic Data
Missing or tainted data sent to users or downstream services

PI Backups
Change Management
Recovery Plan
Machine Backups
Manipulation of configuration

Firewall Restrictions
Service Hardening
Network Segmentation
Application Whitelisting
Pivot to other servers

EMET
Antivirus
OS updates
Application Whitelisting
Spread malware to clients

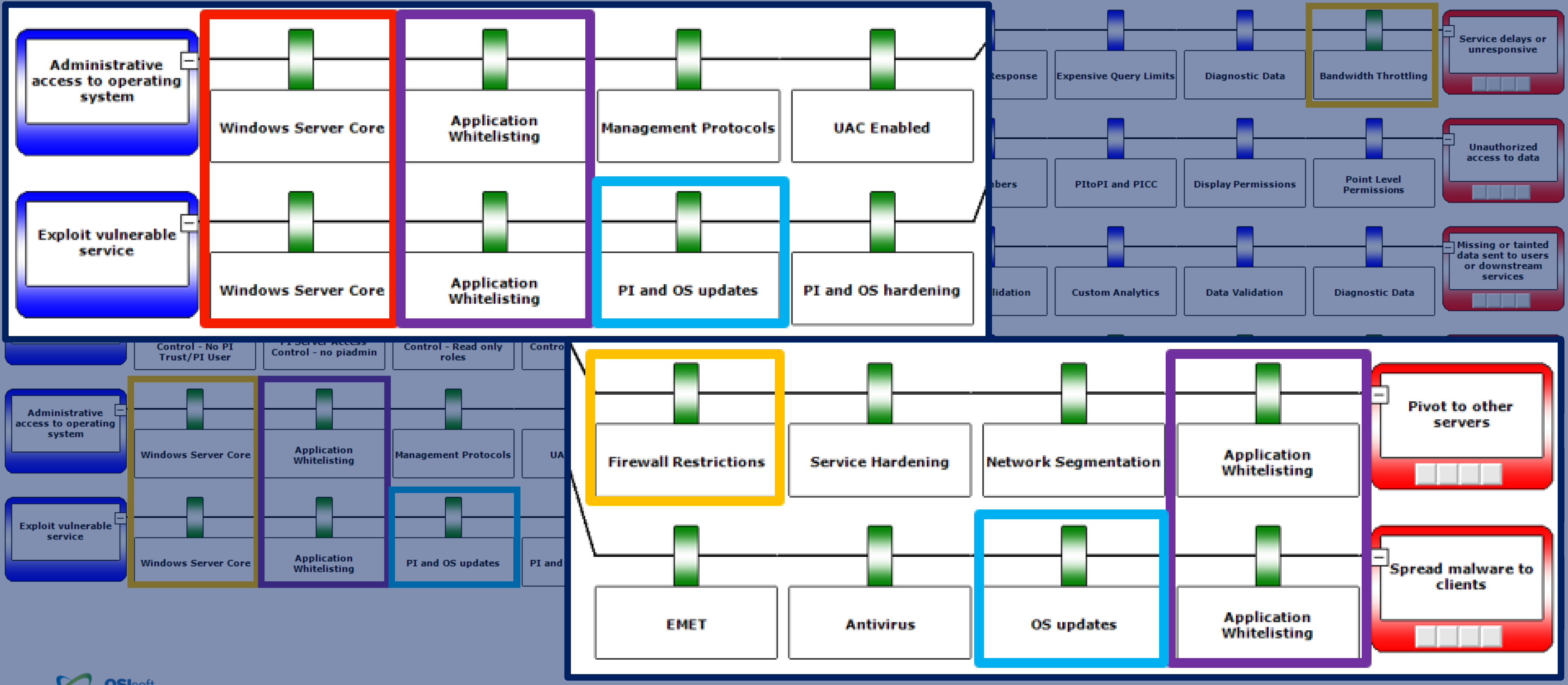
PI Data Archive Bow Ti

Windows Server Core

OS Updates

Firewall Restrictions

Application Whitelisting



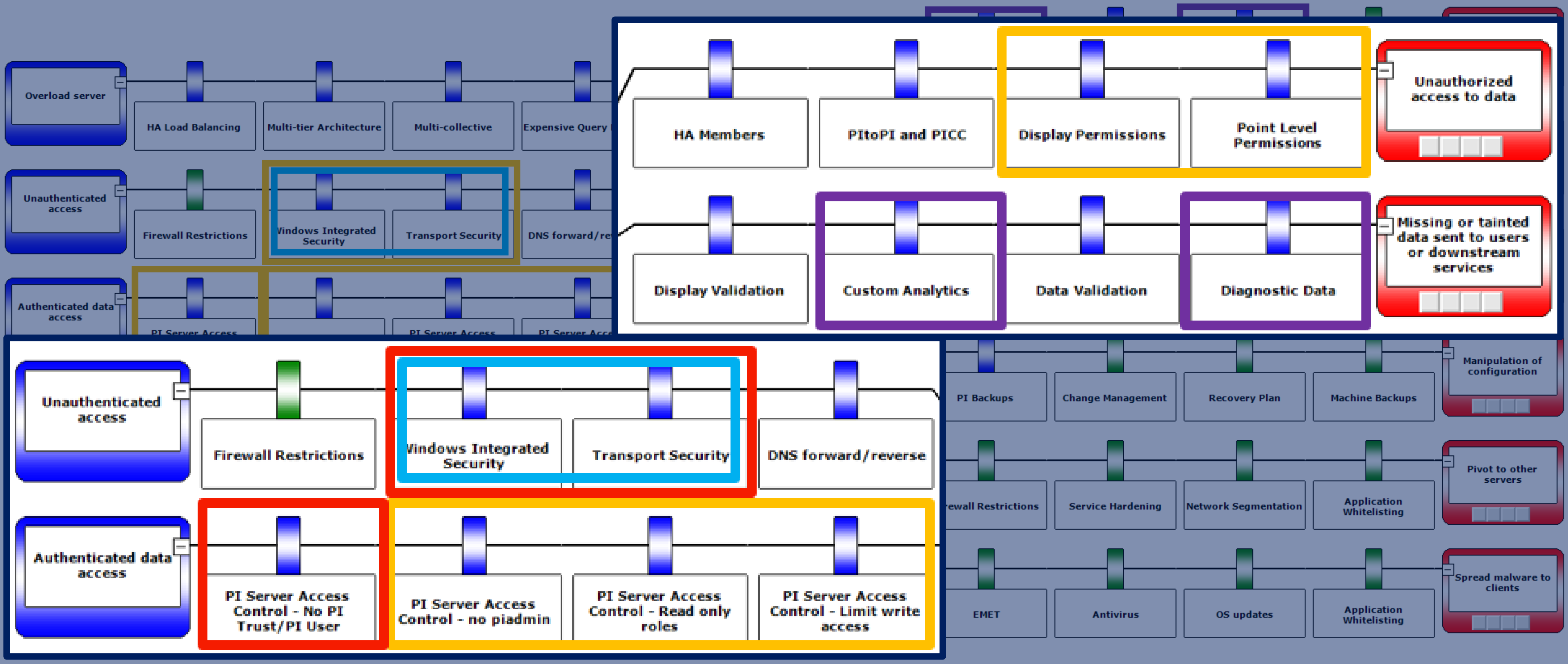
PI Data Archive Bow Ti

WIS Everywhere

PI Updates

Least Privileges

Health Monitoring



Overload server

HA Load Balancing

Multi-tier Architecture

Multi-collective

Expensive Query

Unauthenticated access

Firewall Restrictions

Windows Integrated Security

Transport Security

DNS forward/re

Authenticated data access

PI Server Access

PI Server Access

PI Server Acc

HA Members

PItoPI and PICC

Display Permissions

Point Level Permissions

Unauthorized access to data

Display Validation

Custom Analytics

Data Validation

Diagnostic Data

Missing or tainted data sent to users or downstream services

Unauthenticated access

Firewall Restrictions

Windows Integrated Security

Transport Security

DNS forward/reverse

Authenticated data access

PI Server Access Control - No PI Trust/PI User

PI Server Access Control - no piadmin

PI Server Access Control - Read only roles

PI Server Access Control - Limit write access

PI Backups

Change Management

Recovery Plan

Machine Backups

Manipulation of configuration

ewall Restrictions

Service Hardening

Network Segmentation

Application Whitelisting

Pivot to other servers

EMET

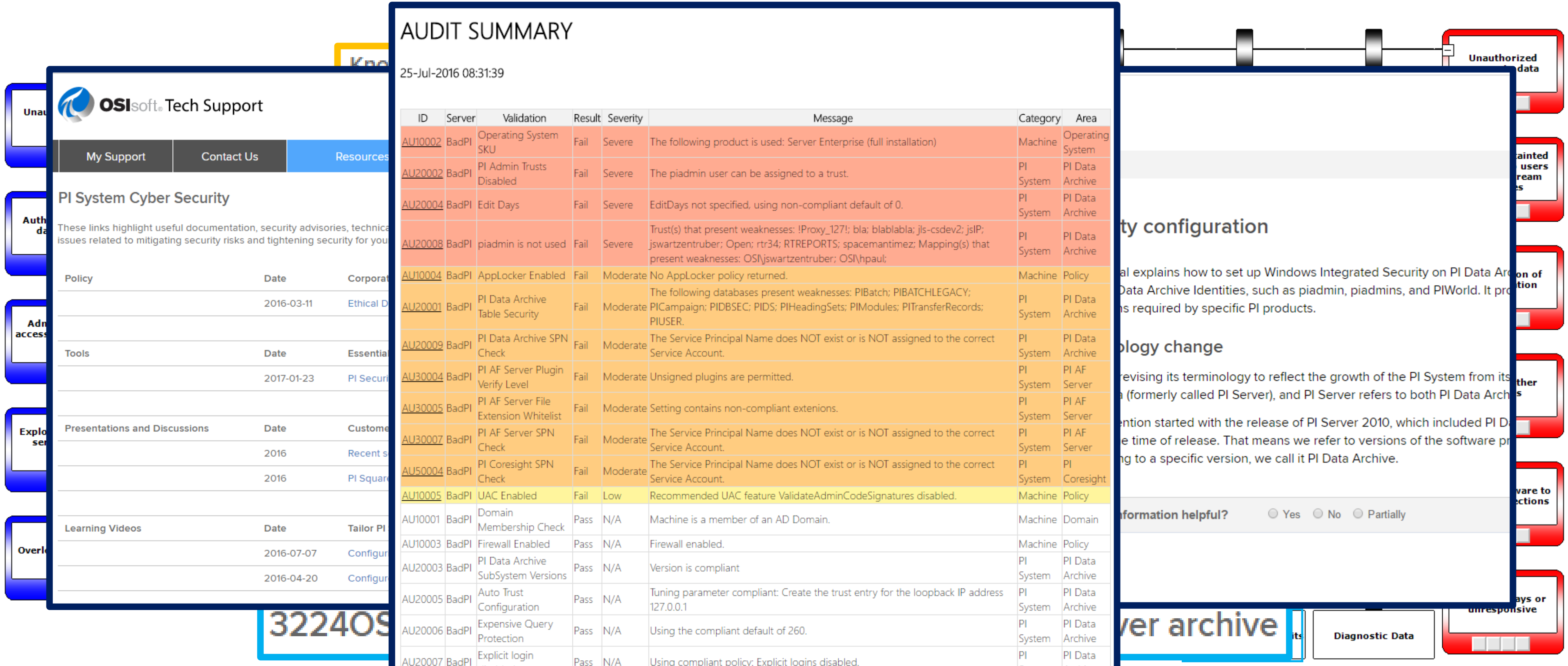
Antivirus

OS updates

Application Whitelisting

Spread malware to clients

PI Server Security: Bringing it all together…



AUDIT SUMMARY

25-Jul-2016 08:31:39

ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	BadPI	Operating System SKU	Fail	Severe	The following product is used: Server Enterprise (full installation)	Machine	Operating System
AU20002	BadPI	PI Admin Trusts Disabled	Fail	Severe	The piadmin user can be assigned to a trust.	PI System	PI Data Archive
AU20004	BadPI	Edit Days	Fail	Severe	EditDays not specified, using non-compliant default of 0.	PI System	PI Data Archive
AU20008	BadPI	piadmin is not used	Fail	Severe	Trust(s) that present weaknesses: !Proxy_127!; bla; blablabla; jls-csdev2; jsIP; jswartzentruber; Open; rtr34; RTREPORTS; spacemantimez; Mapping(s) that present weaknesses: OSI\jswartzentruber; OSI\hpaul;	PI System	PI Data Archive
AU10004	BadPI	AppLocker Enabled	Fail	Moderate	No AppLocker policy returned.	Machine	Policy
AU20001	BadPI	PI Data Archive Table Security	Fail	Moderate	The following databases present weaknesses: PIBatch; PIBATCHLEGACY; PICampaign; PIDBSEC; PIDS; PIHeadingSets; PIModules; PITransferRecords; PIUSER.	PI System	PI Data Archive
AU20009	BadPI	PI Data Archive SPN Check	Fail	Moderate	The Service Principal Name does NOT exist or is NOT assigned to the correct Service Account.	PI System	PI Data Archive
AU30004	BadPI	PI AF Server Plugin Verify Level	Fail	Moderate	Unsigned plugins are permitted.	PI System	PI AF Server
AU30005	BadPI	PI AF Server File Extension Whitelist	Fail	Moderate	Setting contains non-compliant extenions.	PI System	PI AF Server
AU30007	BadPI	PI AF Server SPN Check	Fail	Moderate	The Service Principal Name does NOT exist or is NOT assigned to the correct Service Account.	PI System	PI AF Server
AU50004	BadPI	PI Coresight SPN Check	Fail	Moderate	The Service Principal Name does NOT exist or is NOT assigned to the correct Service Account.	PI System	PI Coresight
AU10005	BadPI	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU10001	BadPI	Domain Membership Check	Pass	N/A	Machine is a member of an AD Domain.	Machine	Domain
AU10003	BadPI	Firewall Enabled	Pass	N/A	Firewall enabled.	Machine	Policy
AU20003	BadPI	PI Data Archive SubSystem Versions	Pass	N/A	Version is compliant	PI System	PI Data Archive
AU20005	BadPI	Auto Trust Configuration	Pass	N/A	Tuning parameter compliant: Create the trust entry for the loopback IP address 127.0.0.1	PI System	PI Data Archive
AU20006	BadPI	Expensive Query Protection	Pass	N/A	Using the compliant default of 260.	PI System	PI Data Archive
AU20007	BadPI	Explicit login disabled	Pass	N/A	Using compliant policy: Explicit logins disabled.	PI System	PI Data Archive

OSIsoft. Tech Support

PI System Cyber Security

These links highlight useful documentation, security advisories, technica
issues related to mitigating security risks and tightening security for you

Policy	Date	Corporat
	2016-03-11	Ethical D
Tools	**Date**	**Essentia**
	2017-01-23	PI Securi
Presentations and Discussions	**Date**	**Custome**
	2016	Recent s
	2016	PI Square
Learning Videos	**Date**	**Tailor PI**
	2016-07-07	Configur
	2016-04-20	Configur

ty configuration

al explains how to set up Windows Integrated Security on PI Data Ar
Data Archive Identities, such as piadmin, piadmins, and PIWorld. It pro
s required by specific PI products.

ology change

revising its terminology to reflect the growth of the PI System from its
a (formerly called PI Server), and PI Server refers to both PI Data Arch

ntion started with the release of PI Server 2010, which included PI D
e time of release. That means we refer to versions of the software pr
ng to a specific version, we call it PI Data Archive.

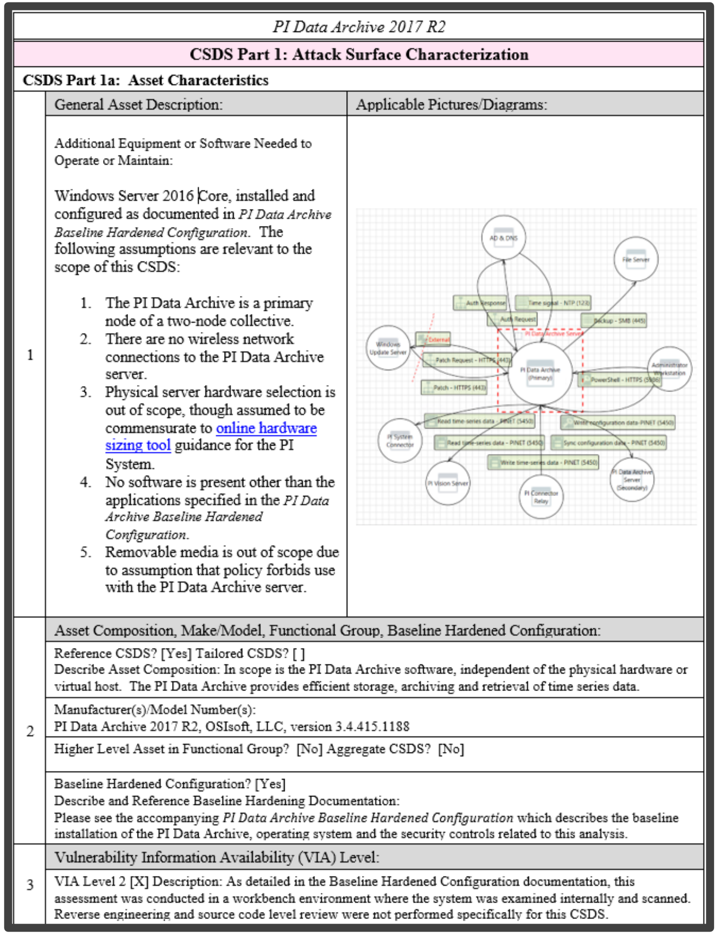
formation helpful? ○ Yes ○ No ○ Partially

Want more on Bow Tie?

- **Presentations**
  - **UC 2016:** Bow-Tying it All Together: Analyzing Your Attack Surface (Video)
  - **UC 2017:** How secure are your PI Systems? A primer for PI System security baselining (Video)
  - **S4x17:** Tying Bow Ties: Using Bow Tie Analysis to Secure ICS (Video)
- **Articles & Papers**
  - **PI Square:** Bow Tie for Cyber Security (parts 1-3) (Post)
  - **SANS White Paper:** Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology, Rebekah Mohr (PDF)

PI Data Archive CSDS

- Structured Security Documentation
- Forward looking
  - Modern Platform
  - Recommended Architecture
- Supplemental Configuration Document/Tools
  - Verification via Configuration as Code



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.	

AD & DNS
File Server
Auth Response
Time signal - NTP (123)
Auth Request
Backup - SMB (445)
PI Data Archive Server
External
Windows Update Server
Patch Request - HTTPS (443)
PI Data Archive (Primary)
Administrator Workstation
PowerShell - HTTPS (5986)
Patch - HTTPS (443)
Read time-series data - PINET (5450)
Write configuration data-PINET (5450)
PI System Connector
Read time-series data - PINET (5450)
Sync configuration data - PINET (5450)
Write time-series data - PINET (5450)
PI Vision Server
PI Connector Relay
PI Data Archive Server (Secondary)

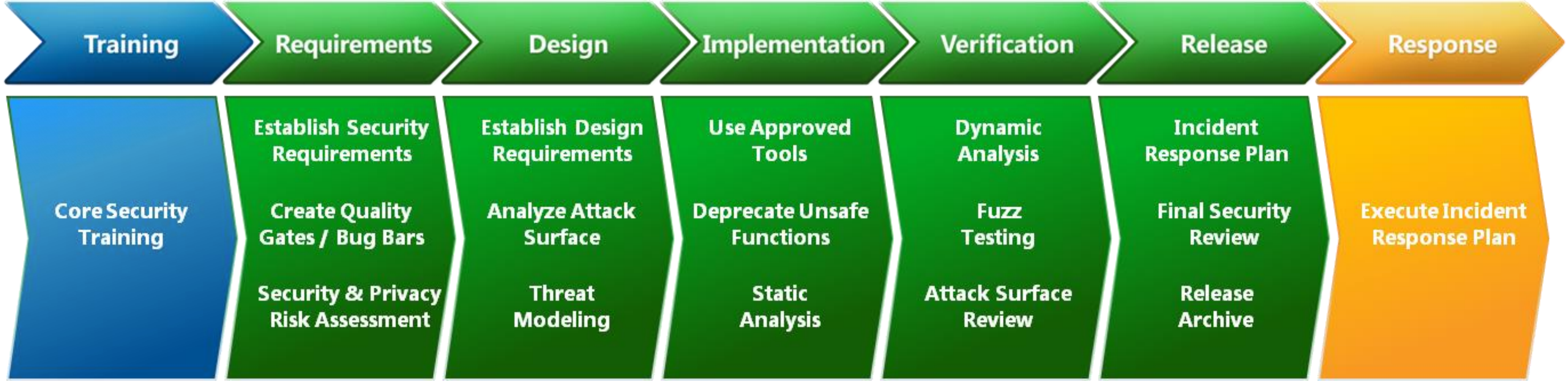
2	Asset Composition, Make/Model, Functional Group, Baseline Hardened Configuration:
	Reference CSDS? [Yes] Tailored CSDS? [ ] Describe Asset Composition: In scope is the PI Data Archive software, independent of the physical hardware or virtual host. The PI Data Archive provides efficient storage, archiving 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.
3	Vulnerability Information Availability (VIA) Level:
	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.

Act III: Tactics

The blocking and tackling of cyber security

Benefits of Server 2016 Core

- Reduced Servicing
- Reduced Management
- **Reduced Attack Surface**
  - ~40% fewer services running
  - ~50% less disk for OS



Training	Requirements	Design	Implementation	Verification	Release	Response
Core Security Training	Establish Security Requirements Create Quality Gates / Bug Bars Security & Privacy Risk Assessment	Establish Design Requirements Analyze Attack Surface Threat Modeling	Use Approved Tools Deprecate Unsafe Functions Static Analysis	Dynamic Analysis Fuzz Testing Attack Surface Review	Incident Response Plan Final Security Review Release Archive	Execute Incident Response Plan

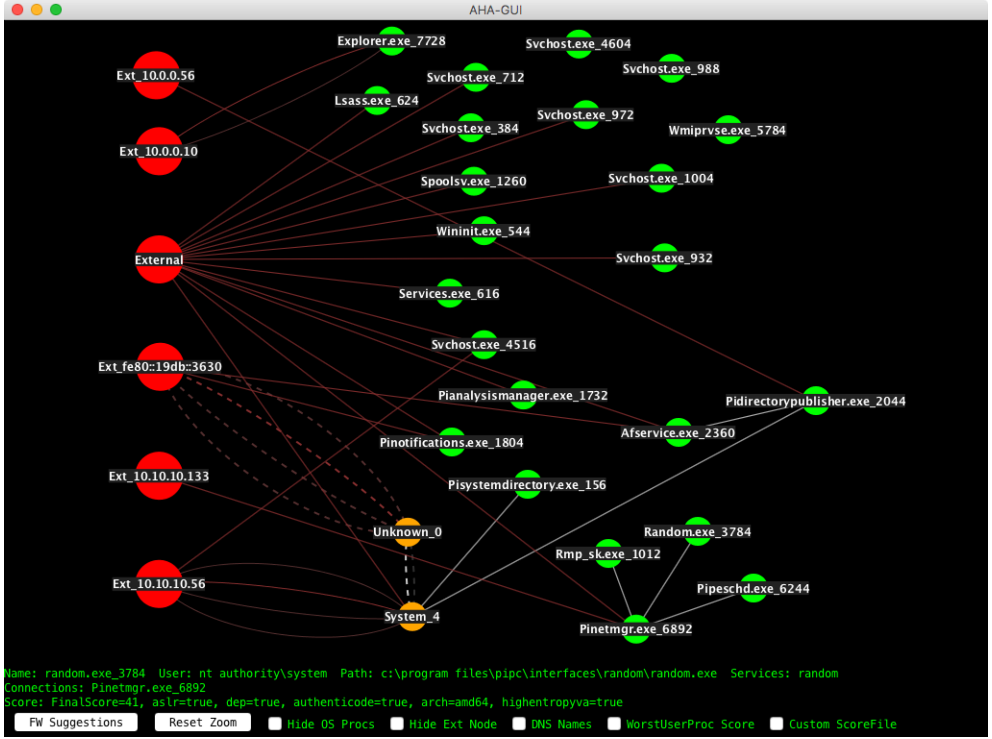
Benefits of PI Data Archive Upgrades*

Defense/**Version**	**2010**	**2012**	**2015**	**2016**	**2017**	**2017 R2**
Compiler	VC++ 2008 SP1	VC++ 2010 SP1	VC++ 2012 Update 4	VC++ 2015 Update 1	VC++2015 Update 2	VC++ 15.3.5
Heap Metadata Protection	No	Yes	Yes	Yes	Yes	Yes
Migration of buffer-overrun prone functions to safe versions	2% complete	80% complete	95% complete	95% complete	95% complete	95% complete
SDL Check	No	No	Yes	Yes	Yes	Yes
Control Flow Guard	No	No	No	No	On core subsystems	On Core Subsystems
Least Required Privileges	None	PI AFLink	PI AFLink	PI AFLink	PI AFLink	PIAFLink, PINetMgr

*All versions listed: WIS; 64-bit; core support; stack buffer overrun protection; DEP/NX; ASLR; SEHOP; SafeSEH

AttackSurface Host Analyzer

- Developed by ESIC, Washington State University
  - Dave Anderson
  - Adam Hahn
  - Repo: https://github.com/ESIC-DA/
- Analysis and Visualization Components
  - Scraper (PowerShell)
  - GUI (Java)



```
Name: random.exe_3784  User: nt authority\system  Path: c:\program files\pipc\interfaces\random\random.exe  Services: random
Connections: Pinetmgr.exe_6892
Score: FinalScore=41, aslr=true, dep=true, authenticode=true, arch=amd64, highentropyva=true
```

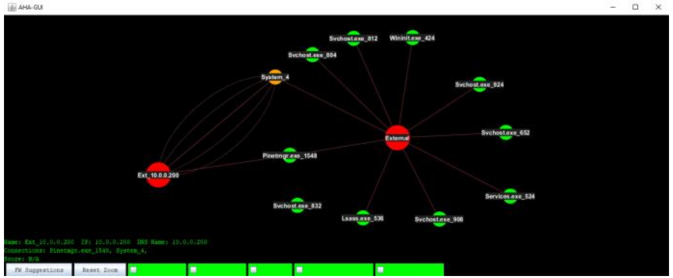
AttackSurface Analysis

Visualization

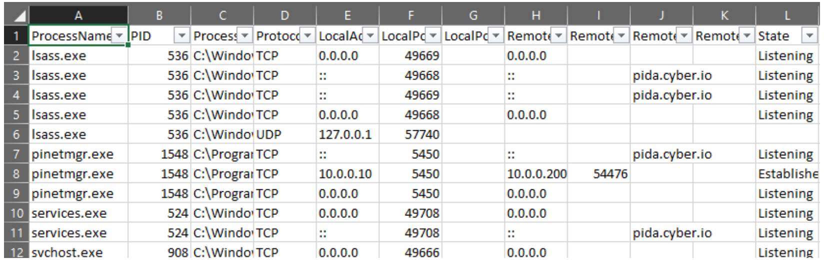
- Graphs communicating executables
- Scores executables on defenses
- Hide/Show OS processes
- Suggests FW Rules

Analysis:

- Identifies all connections with cports
- Aggregates executables for connections
- Defensive attributes:
  - Authenticode
  - ControlFlowGuard
  - HighentropyVA



```
Name: Ext_10.0.0.200  IP: 10.0.0.200  DNS Name: 10.0.0.200
Connections: Pinetmgr.exe_1548, System_4,
Score: N/A
```



	A	B	C	D	E	F	G	H	I	J	K	L
1	ProcessName	PID	Process	Protocc	LocalAc	LocalPc	LocalPc	Remote	Remote	Remote	Remote	State
2	lsass.exe	536	C:\Windo	TCP	0.0.0.0	49669		0.0.0.0				Listening
3	lsass.exe	536	C:\Windo	TCP	::	49668		::		pida.cyber.io		Listening
4	lsass.exe	536	C:\Windo	TCP	::	49669		::		pida.cyber.io		Listening
5	lsass.exe	536	C:\Windo	TCP	0.0.0.0	49668		0.0.0.0				Listening
6	lsass.exe	536	C:\Windo	UDP	127.0.0.1	57740						
7	pinetmgr.exe	1548	C:\Prograr	TCP	::	5450		::		pida.cyber.io		Listening
8	pinetmgr.exe	1548	C:\Prograr	TCP	10.0.0.10	5450		10.0.0.200	54476			Establishe
9	pinetmgr.exe	1548	C:\Prograr	TCP	0.0.0.0	5450		0.0.0.0				Listening
10	services.exe	524	C:\Windo	TCP	0.0.0.0	49708		0.0.0.0				Listening
11	services.exe	524	C:\Windo	TCP	::	49708		::		pida.cyber.io		Listening
12	svchost.exe	908	C:\Windo	TCP	0.0.0.0	49666		0.0.0.0				Listening

Demo 4: Further Reducing Surface Area

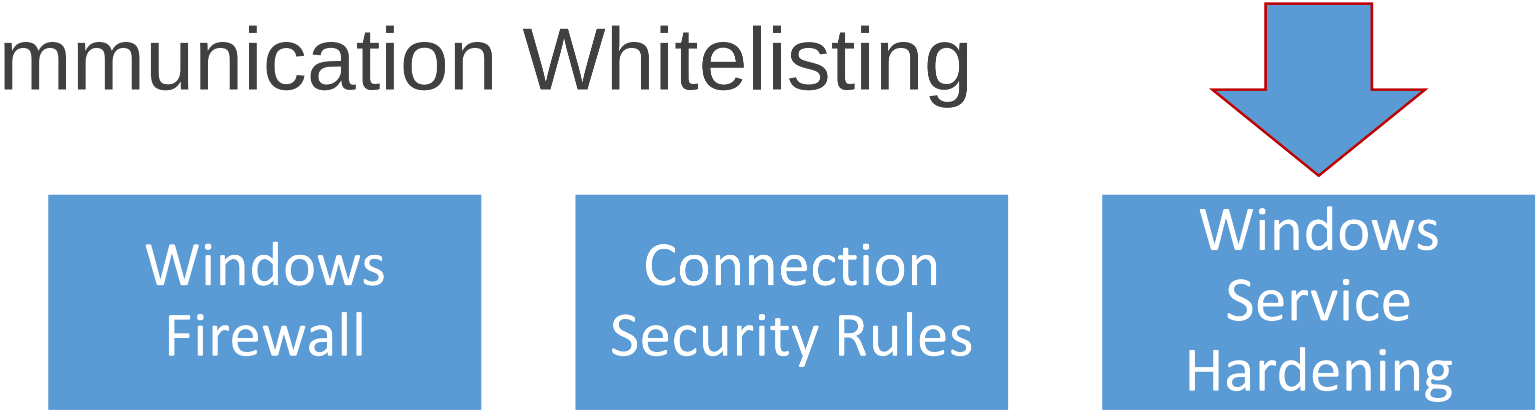
Features to Disable

- FS-SMB1 (Handled automatically as of 2016 RS3)
- Disable IPv6 Tunnels
- LLMNR, NetCease, NetBIOS (AD Security 10/21 post)

Services to Disable

- SharedAccess, lltdsvc, Spooler, PrintNotify, ScDeviceEnum, Wisvc – Microsoft Docs
- WinHttpAutoProxySvc – Project Zero December blog post
- DiagTrack, SNMPTRAP, sacsvr – Not used for PI apps

Communication Whitelisting



Windows Firewall

Connection Security Rules

Windows Service Hardening

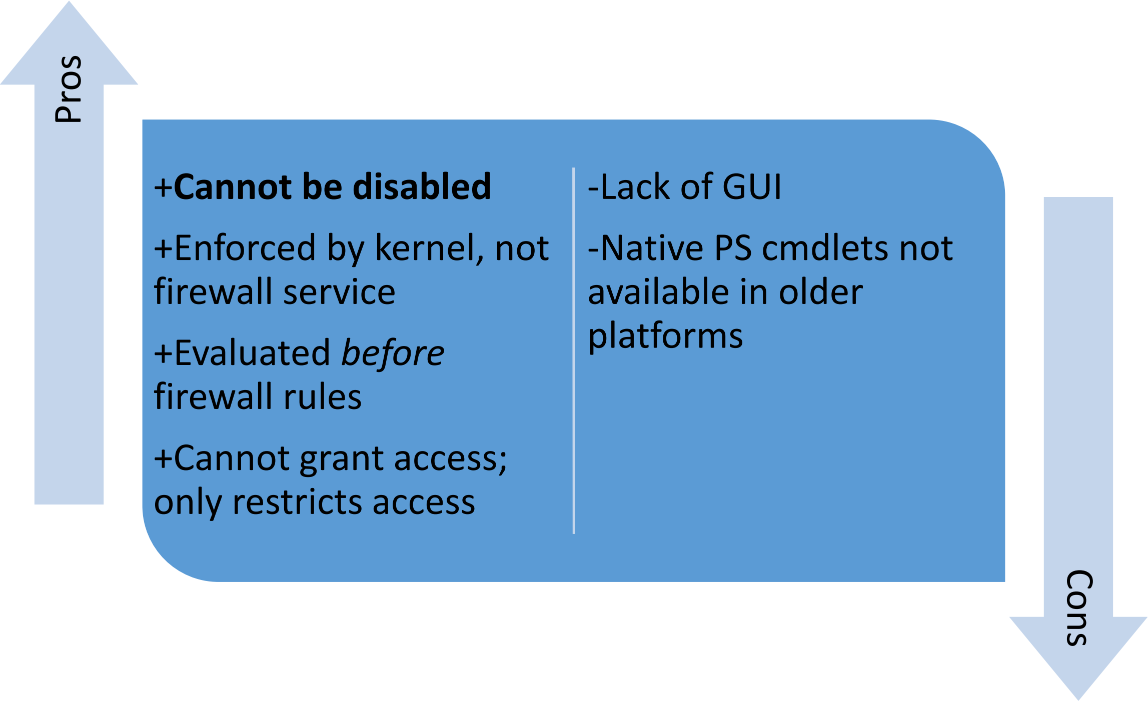
Why focus on services?

- Run without user interaction
- Always on, often on the network
- Often run with unnecessarily high privilege
- Ports are opened
- Not limited by AppLocker

Windows Filtering Platform

- Development platform
  - Windows firewall implemented using WFP
  - NetFwServiceRestriction and INetFwRule part of Windows firewall
  - Verbose tracing built into netsh (wfp capture start|stop)
- Windows Service Hardening
  - Restricted network access for service
  - Rules stored in registry keys

WSH vs. Windows Firewall



+Cannot be disabled

+Enforced by kernel, not firewall service

+Evaluated *before* firewall rules

+Cannot grant access; only restricts access

-Lack of GUI

-Native PS cmdlets not available in older platforms

Demo 5: Communication Whitelisting

Application Control with AppLocker

THE GOOD

- Granular control
- Available with OS by default
- Audit and Enforce options
- Associated logging

THE BAD

- Compliance focus, not security boundary
- Not supported on Core editions

(╯°□°) ╯︵ ┻━┻

THE UGLY

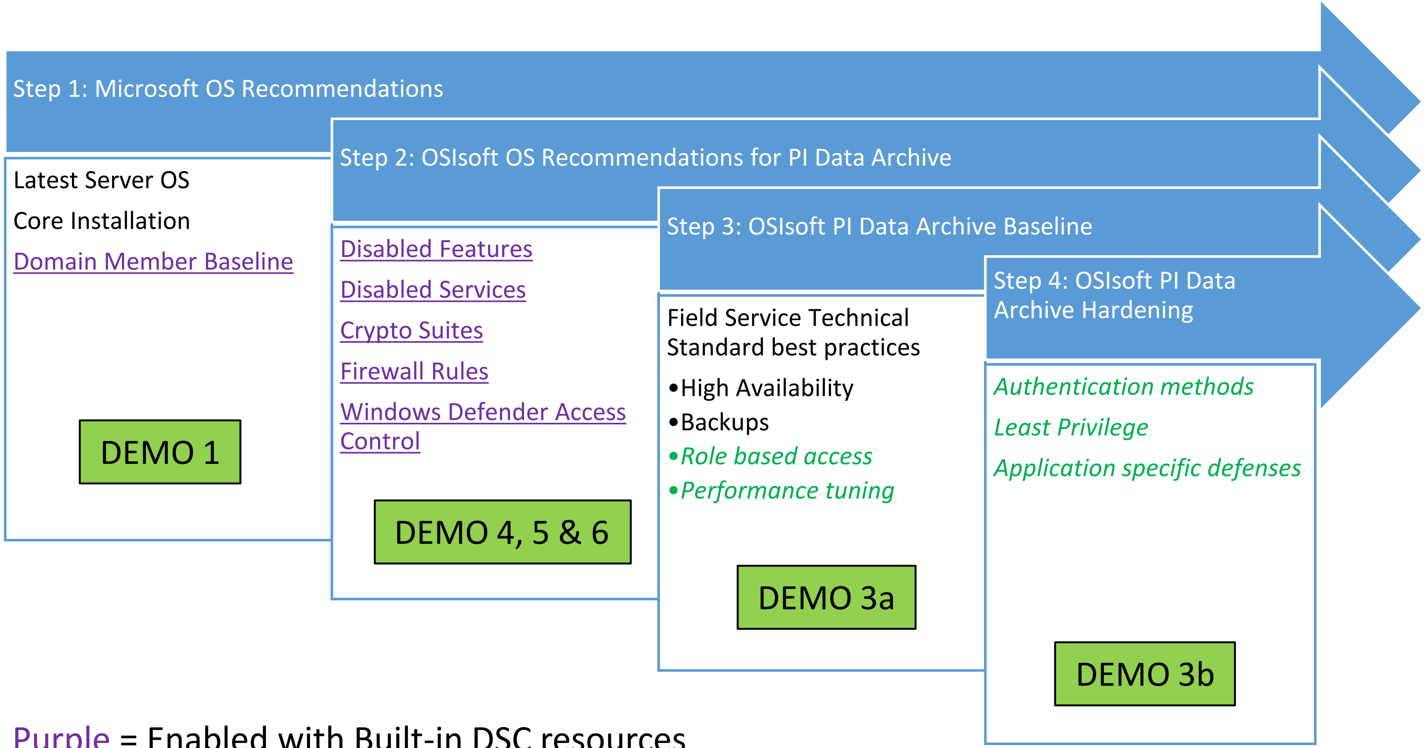
- Major limitations
  - Services
  - .WSF
  - Macros
  - MS Office embedded content
- Multiple bypasses available on metasploit
  - Regsvr32
  - InstallUtil

Device Guard & AppLocker

- Core: Device Guard & Antivirus (recommended)
  - Limit attack surface
  - Limit local server access
- Desktop Experience: Device Guard & AppLocker
  - Device Guard: strict enforcement of code integrity
  - AppLocker: granular control and role based options
  - Antivirus: detection & clean up for known threats

Demo 6: Application Control

Hardened Baseline Configuration



Step 1: Microsoft OS Recommendations

Latest Server OS

Core Installation

Domain Member Baseline

DEMO 1

Step 2: OSIsoft OS Recommendations for PI Data Archive

Disabled Features

Disabled Services

Crypto Suites

Firewall Rules

Windows Defender Access Control

DEMO 4, 5 & 6

Step 3: OSIsoft PI Data Archive Baseline

Field Service Technical Standard best practices

- High Availability
- Backups
- *Role based access*
- *Performance tuning*

DEMO 3a

Step 4: OSIsoft PI Data Archive Hardening

Authentication methods

Least Privilege

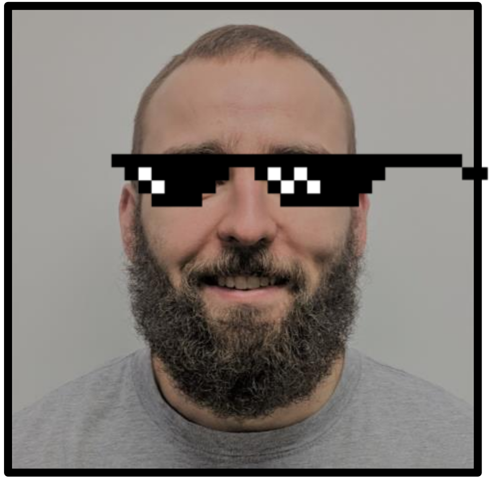
Application specific defenses

DEMO 3b

Purple = Enabled with Built-in DSC resources

Green = Enabled with PI Security DSC resources

Contact Information



Harry Paul

hpaul@osisoft.com

Cyber Security Advisor

OSIsoft, LLC

Questions

Please wait for the **microphone** before asking your questions

State your **name & company**

Please remember to…

Complete the Online Survey for this session

OSIsoft Users Conference 2017
DoubleDutch
OPEN
Details
Reviews
Related
OSIsoft USERS CONFERENCE 2017
TRANSFORM YOUR WORLD
Download on the App Store
GET IT ON Google Play
HTML

Download the Conference App for OSIsoft Users Conference 2017

- View the latest agenda and create your own
- Meet and connect with other attendees

search **OSISOFT** in the app store

Merci

谢谢

Danke

Спасибо

Gracias

Thank You

감사합니다

ありがとう

Grazie

Obrigado

Optional: Click to add a takeaway you wish the audience to leave with.