How secure are your PI Systems?: A primer for PI System security baselining

Presented by **Harry Paul**

The PI System in Context

Where you'll typically find PI Software

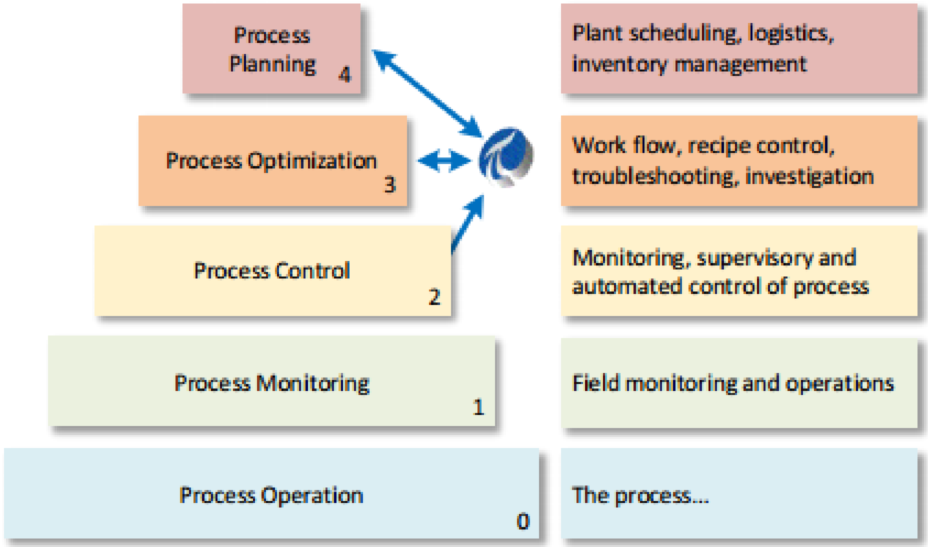

Process Planning 4
Plant scheduling, logistics, inventory management
Process Optimization 3
Work flow, recipe control, troubleshooting, investigation
Process Control 2
Monitoring, supervisory and automated control of process
Process Monitoring 1
Field monitoring and operations
Process Operation 0
The process...

Figure 1. ISA S95 Information Structure with OSIsoft PI

Core Security Value of the PI System

Critical Systems

Transmission
& Distribution
SCADA

Plant DCS

PLCs

Environmental
Systems

Other critical
operations systems

Reduce the risks on critical systems

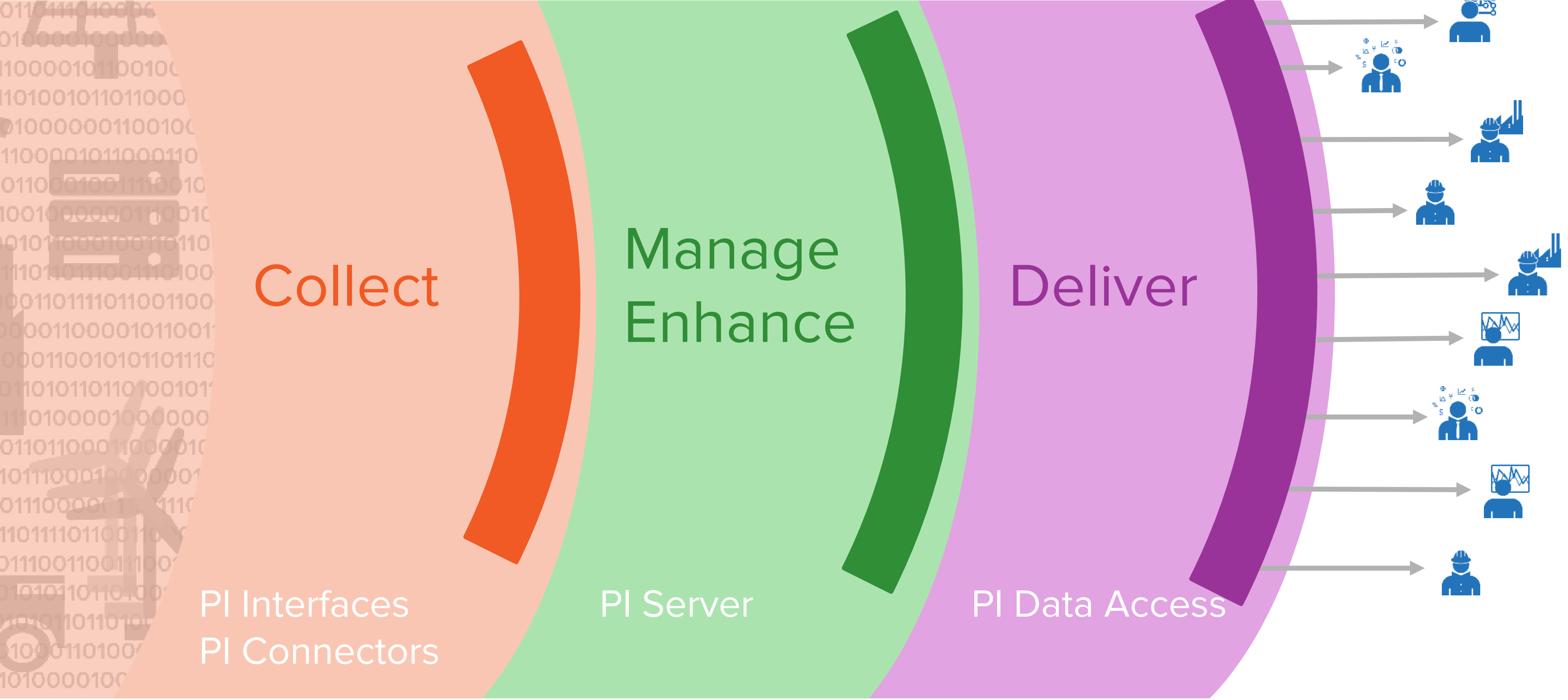
Limits direct access to critical systems while expanding the value use of information.

OSIsoft.

Infrastructure

Security Perimeter

The PI System Layers



Collect

Manage
Enhance

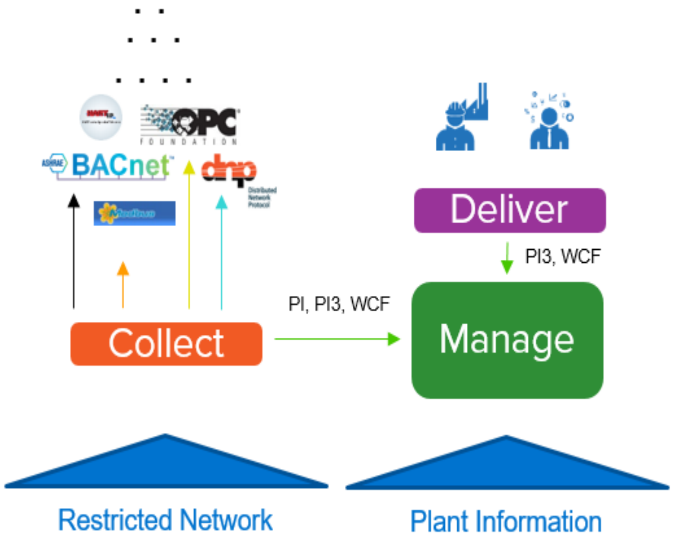
Deliver

PI Interfaces
PI Connectors

PI Server

PI Data Access

Operations Scenario



Deliver

PI3, WCF

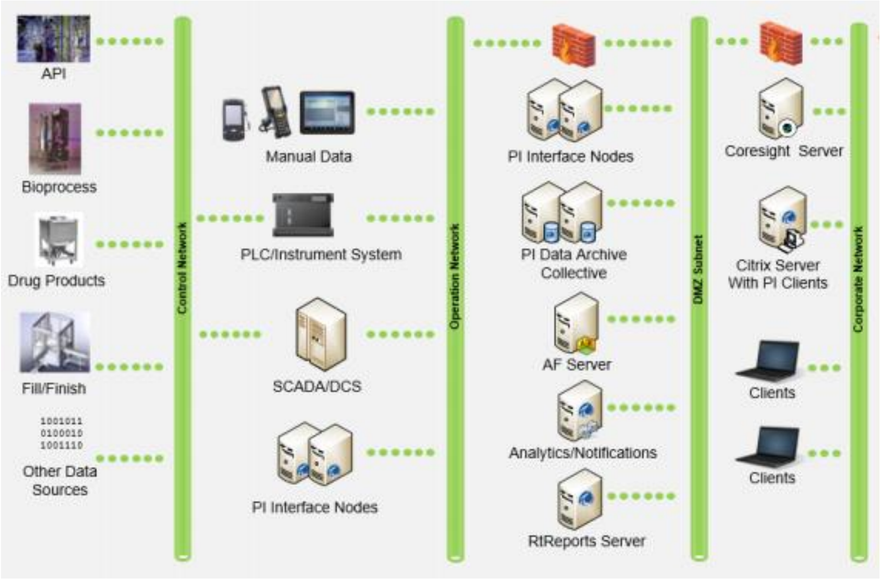
PI, PI3, WCF

Collect

Manage

Restricted Network

Plant Information



API

Bioprocess

Drug Products

Fill/Finish

Other Data Sources

Control Network

Manual Data

PLC/Instrument System

SCADA/DCS

PI Interface Nodes

Operation Network

PI Interface Nodes

PI Data Archive Collective

AF Server

Analytics/Notifications

RtReports Server

DMZ Subnet

Coresight Server

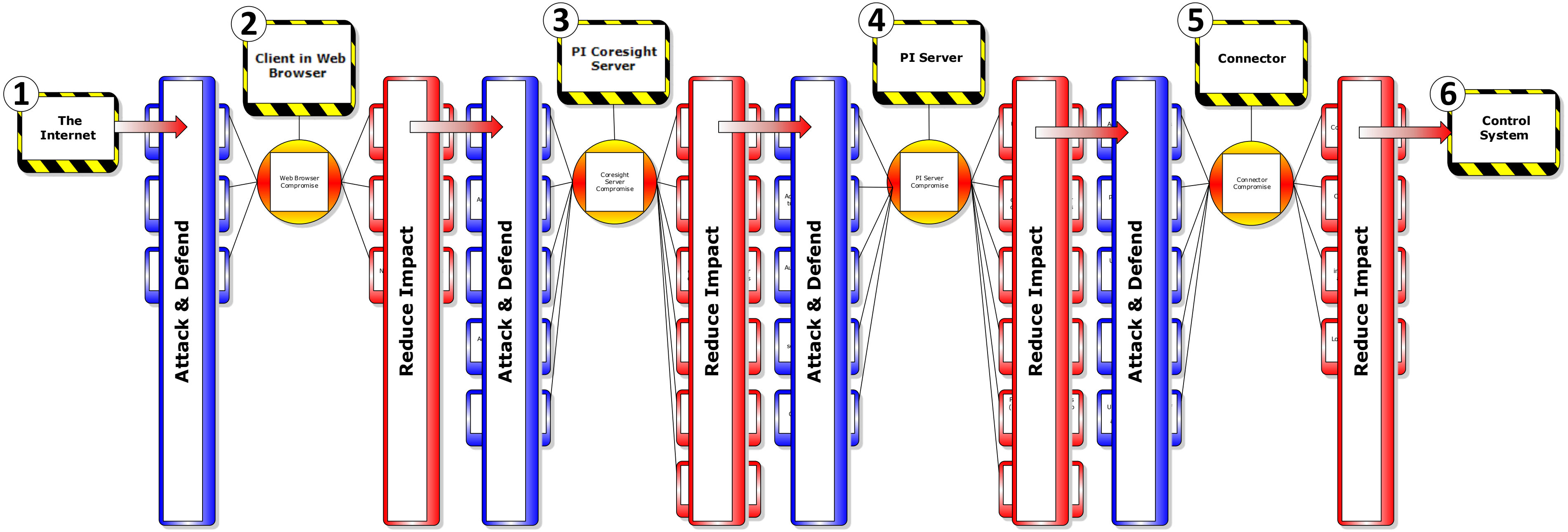
Citrix Server With PI Clients

Clients

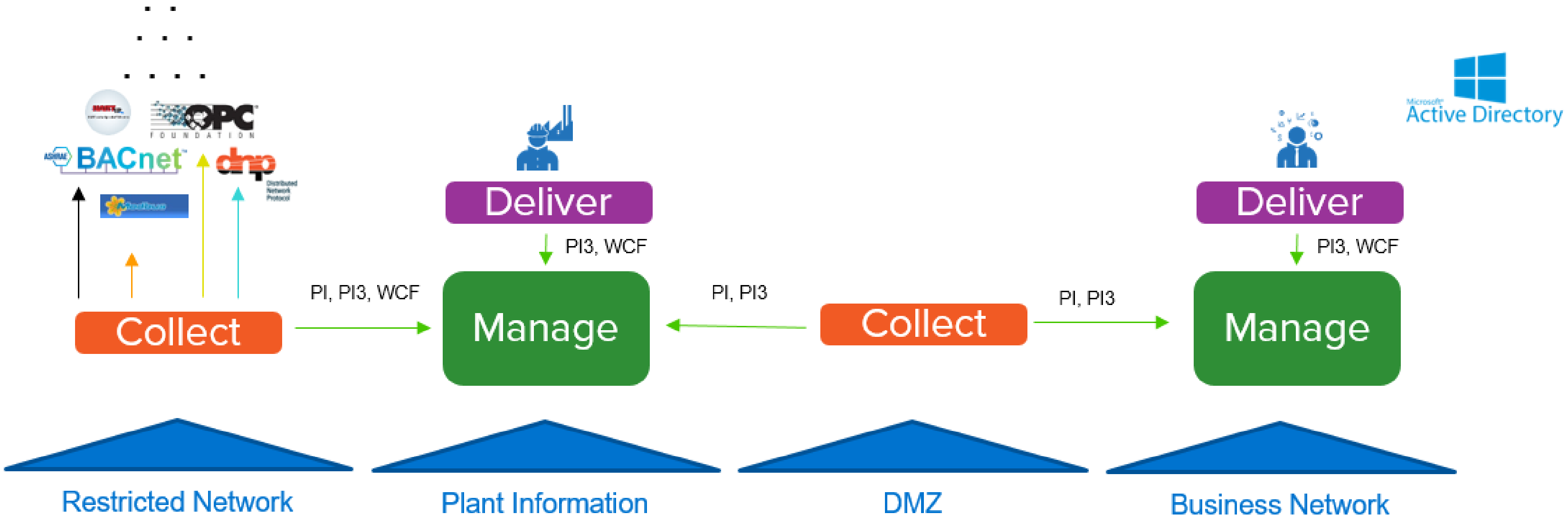
Clients

Corporate Network

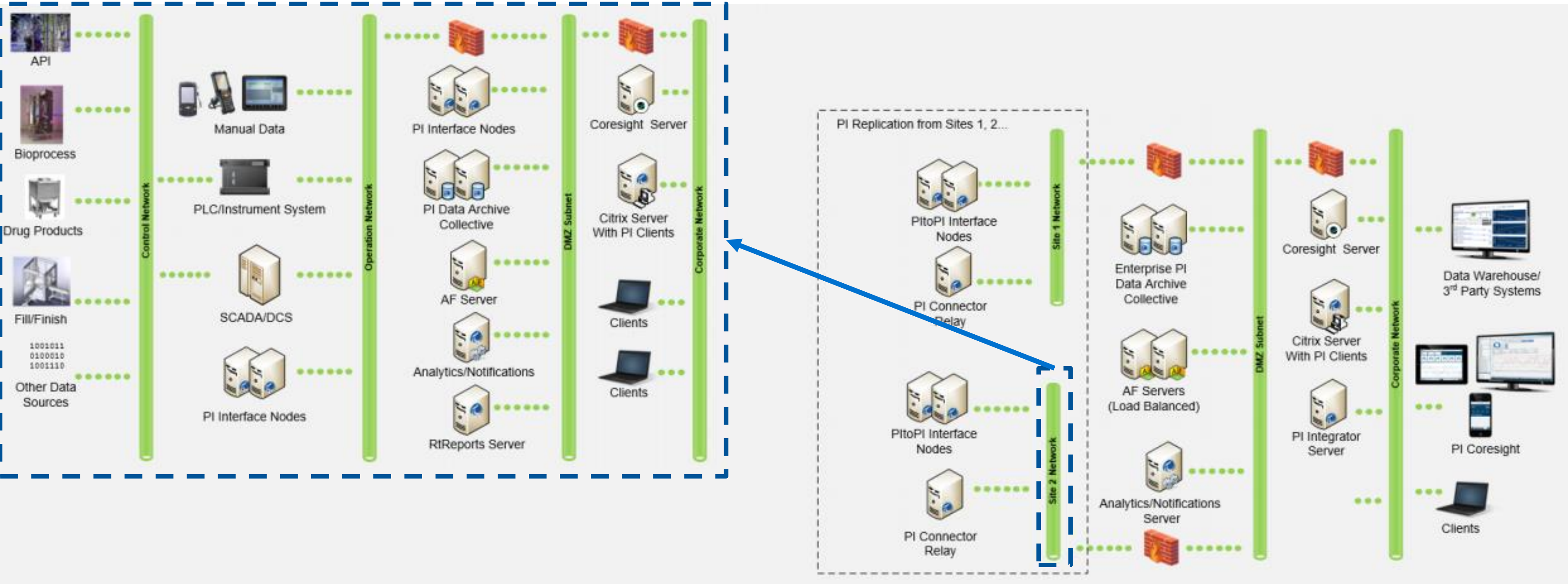
Operations Scenario Killchain



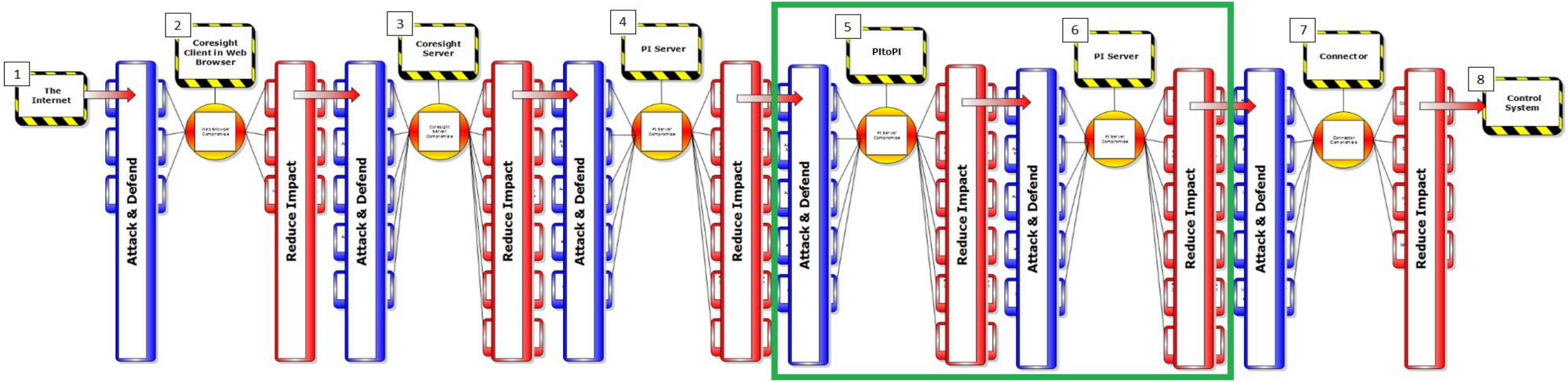
Operations and Business Scenario



Operations and Business Scenario



Operations and Business Scenario Killchain



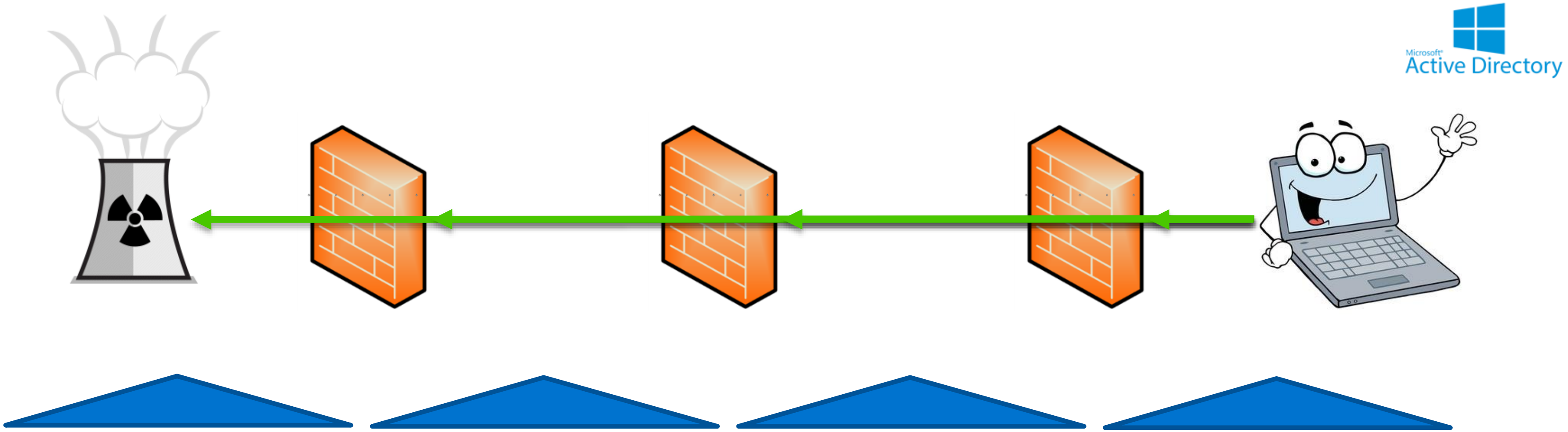
Network Zones

Segment system components

Data protocol only across segments

Note:

!= Security



Restricted Network

Plant Information

DMZ

Business Network

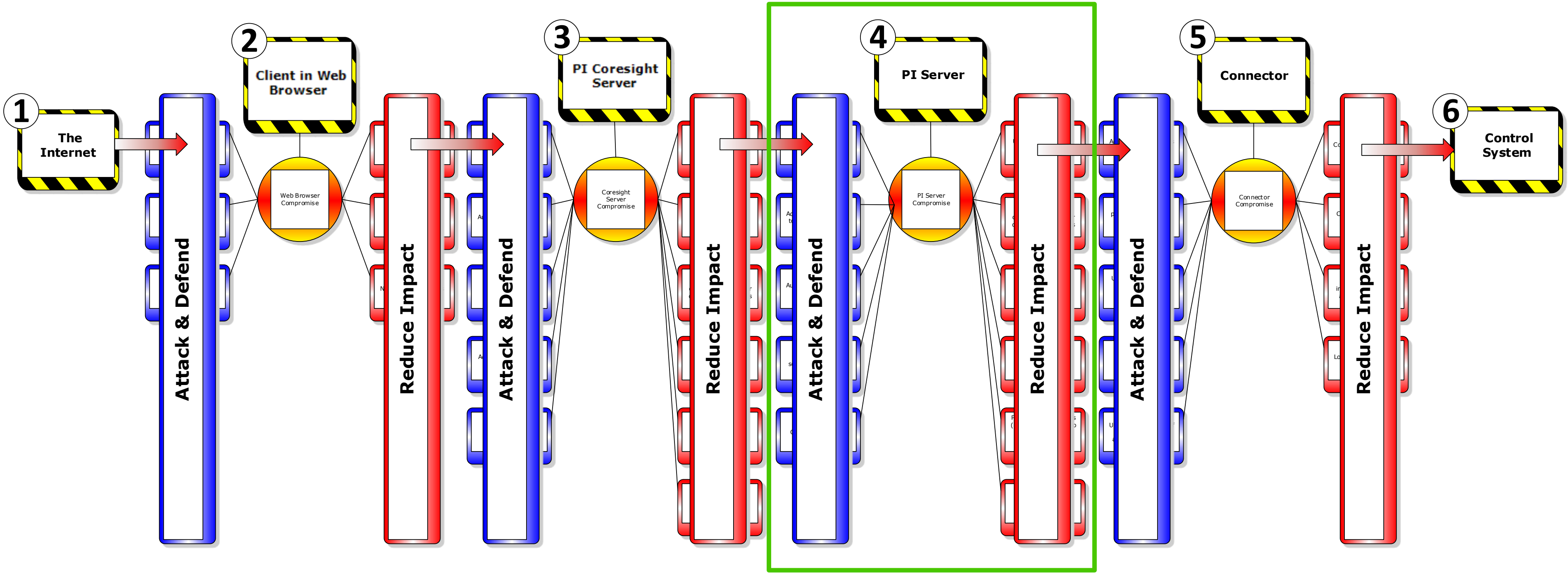
F!R3W@11Z

1. Use one of the dial-in lines that doesn't go through the firewall.
2. Use a network connection via a partner that doesn't go through the firewall.
3. Use the maintenance ports from vendors that don't go through the firewall.
4. Send in a false update disk that initiates communication from inside the firewall to you.
5. #4 with a word virus as the delivery system.
6. #4 with a pornography pointer spread sheet as the delivery method.
7. #4 with a free CD as the delivery method.
8. #4 with a downloadable executable as the delivery mechanism.
9. #4 with a web page (< img gopher://another internal.computer.com/0[attack-code]>)
10. #4 with an automated update from Microsoft or Netscape.
11. #4 with a java applet.
12. #4 with an ActiveX program.
13. #4 with a new computer purchase (pre-installed attack).
14. #4 with a processor upgrade (the chip has a Trojan horse).
15. Pay off an insider to start the session to you on the outside.
16. Trick an insider into starting the session to you on the outside.
17. Hijack a TCP session that runs through the firewall (for example using "hunt") and gain insider access.
18. Sniff traffic that passes through the firewall and steal a password used to gain additional access.
19. Exploit a vulnerability in a bastion host and use it to springboard attacks against the rest of the outside world.
20. #19 but use it to attack other bastion hosts.
21. #19 but use it to get into back-end processing systems.
22. #21 and use the back-end systems to get into the rest of the internal network.
23. #22 and use those systems to open up sessions to the outside world.
24. #20 or #21 and use those systems to sniff firewall management traffic and forge firewall configuration changes.
25. #20 or #21 and use them to take over firewall management sessions.
26. Any of the last 10 examples and use them to corrupt information in the firewall.
27. Any of the last 10 attacks and use them to change firewall protection settings.
28. Flood the firewall with requests to deny service to the network.
29. Overwhelm the bastion hosts in the firewall to deny services.
30. Corrupt the domain name system so the firewall can't deliver traffic properly.
31. Corrupt routing tables so the firewall can't route traffic.
32. Break into one of the systems used by insiders to connect directly (via modem) to AOL and create a bridge that bypasses the firewall.
33. Forge IP addresses so the firewall thinks attacks are coming from innocent locations and cuts off service.
34. Send mal-formed packets to the firewall and cause it to crash.
35. Set up a popular Web page as an anonymizer and redirect outbound traffic through your site for observation.
36. Setup a free mail service and sniff all the email passing through it from people behind the firewall.
37. #36 but alter the email to include Trojan Horses.
38. #36 and add free telnet service via the Web (port 80) so that insiders can telnet even though it is not 'authorized'.
39. #37 with gopher.
40. #37 with file transfer.
41. #37 with real-audio.
42. #37 with any other service you want to provide as a firewall bypass.
43. Any of the last few with encrypted services to make it harder for the people who run the firewall to tell what is hapenning.
44. Any of the last few but with Trojan horse download software plug-ins to make it all work.
45. Send in a Trojan horse that dials out to bypass the firewall.
46. Send free 'radio-LAN cards to select insiders who experiment with new technologies and use a Trojan horse to get into the Radio LAN.
47. Break into a wire closet and attack a radio-LAN to the inside LAN.
48. Break into the phone system and redirect telephonically controlled digital traffic through your location.
49. Convince upper management that they need to day trade and provide a free day-trading service with your custom (Trojan horse) software.
50. Provide firewall services to companies who don't want to or have decided not to provide their own, and expliot at will.

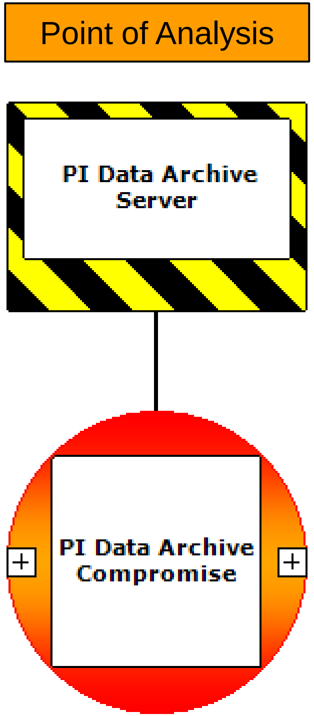
Source: 50 Ways to Defeat Your Firewalls, Fred Cohen, http://all.net/journal/50/firewall.html

Threat Modeling

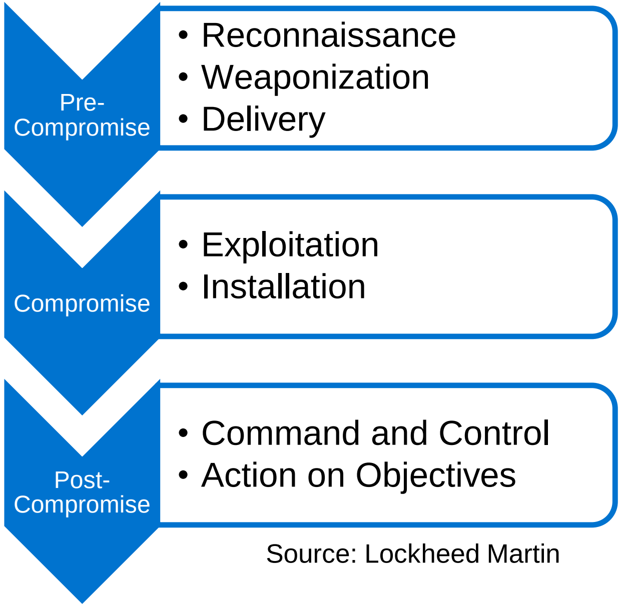
Points of Interest



Analyzing a Module



Cyber Kill Chain



Pre-Compromise
- Reconnaissance
- Weaponization
- Delivery

Compromise
- Exploitation
- Installation

Post-Compromise
- Command and Control
- Action on Objectives

Source: Lockheed Martin

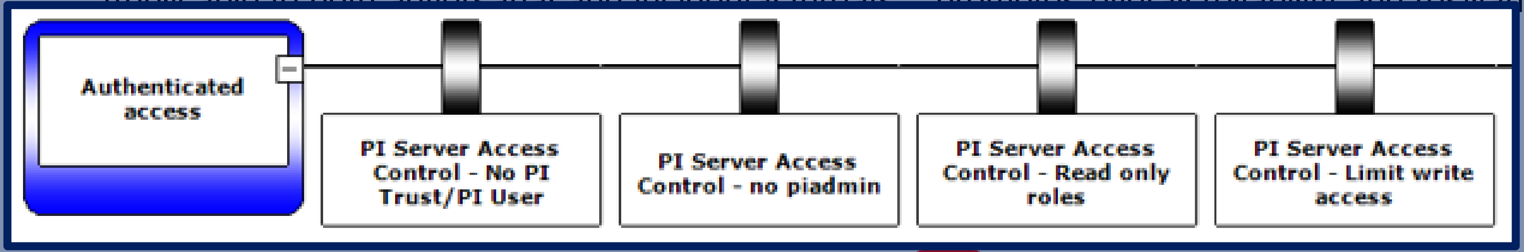
Bow Tie Methodology: Software Component

Top event defined as the compromise of a software component

The context for each event includes:

- software component
- environment

Applicable to both adversarial and incidental threats – promotes overall reliability and resiliancy



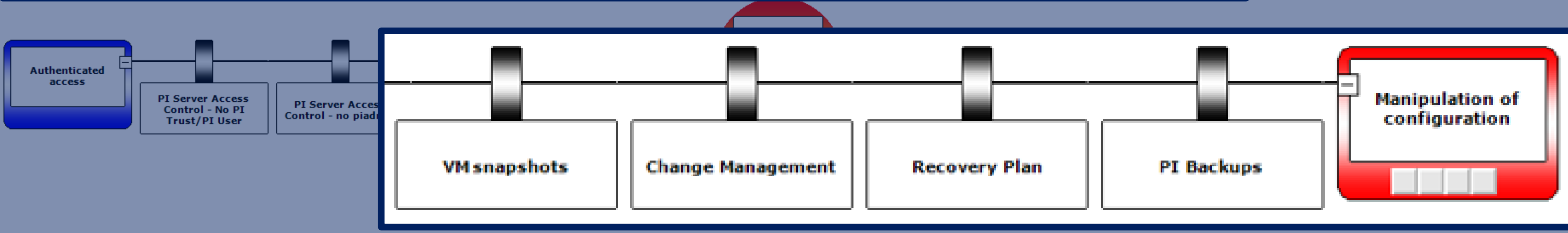
Authenticated access

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



Authenticated access
PI Server Access Control - No PI Trust/PI User
PI Server Acces Control - no piadı

VM snapshots

Change Management

Recovery Plan

PI Backups

Manipulation of configuration

Think like an attacker!

Application Server Threats and Impacts

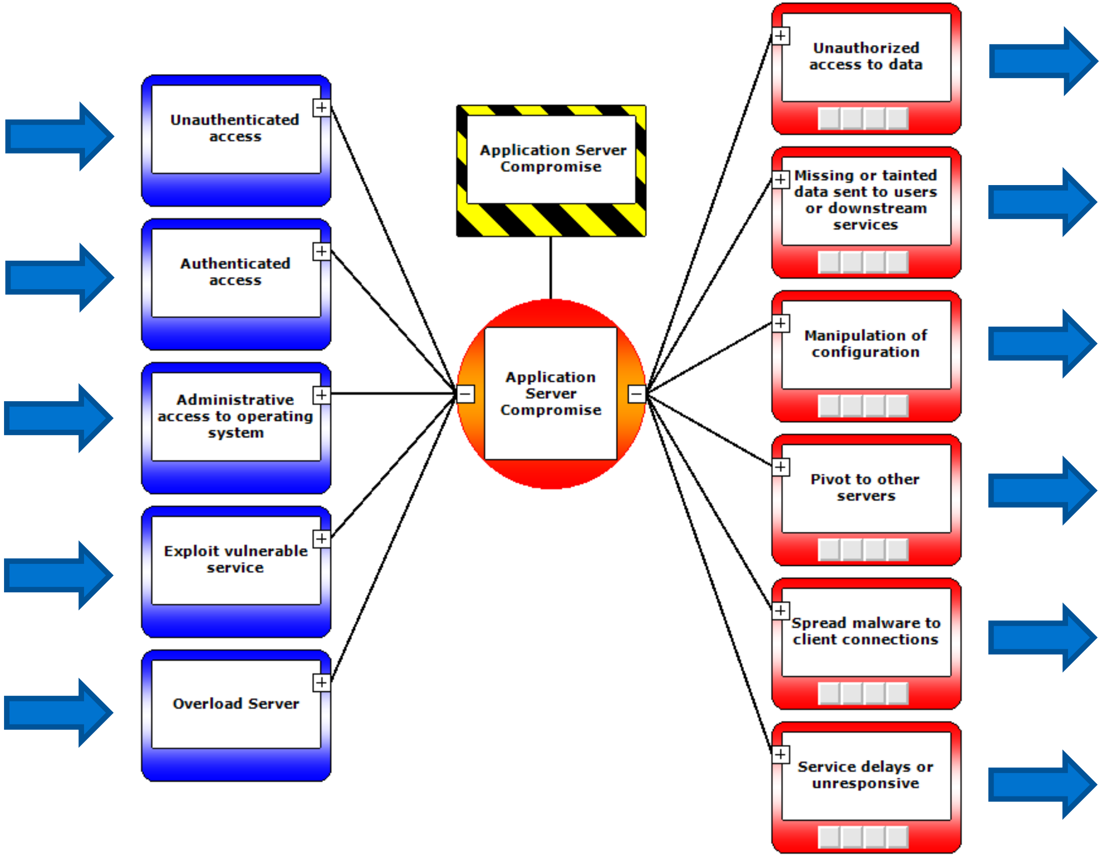
Snooping/Spoofing

Insider Threat/Stolen Creds

Pwn OS/Admin

Malware/0-Day

Expensive calls/Botnet


Unauthenticated access
Authenticated access
Administrative access to operating system
Exploit vulnerable service
Overload Server
Application Server Compromise
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

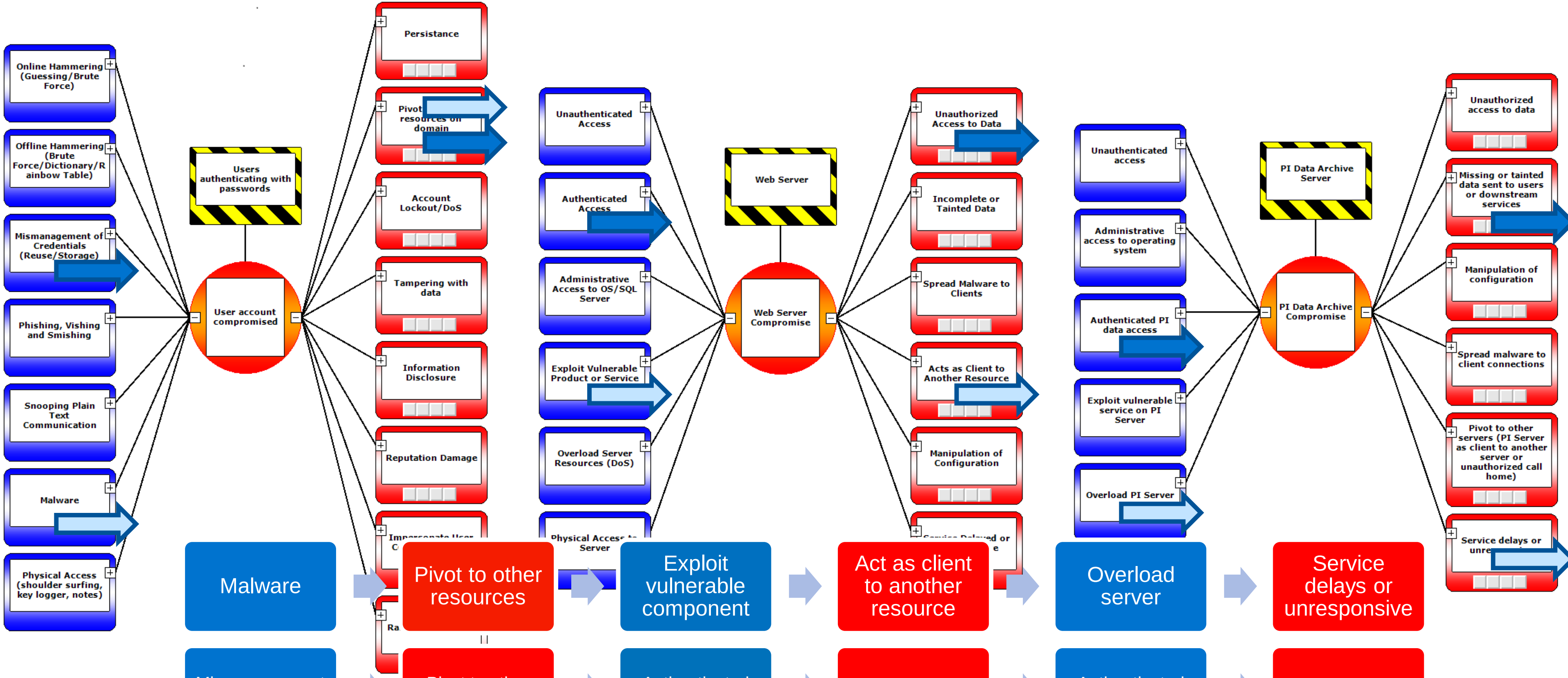
Misleading Reports

Lost Data/Backdoor

Call Home/Move Deeper

RATs/Ransomware

Critical Data Unavailable

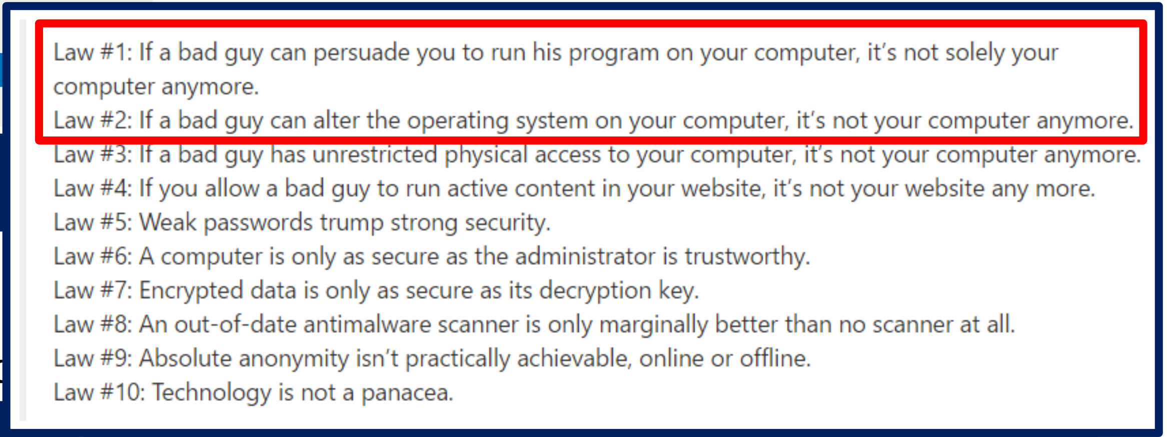

Online Hammering (Guessing/Brute Force)
Offline Hammering (Brute Force/Dictionary/Rainbow Table)
Mismanagement of Credentials (Reuse/Storage)
Phishing, Vishing and Smishing
Snooping Plain Text Communication
Malware
Physical Access (shoulder surfing, key logger, notes)
Users authenticating with passwords
User account compromised
Persistance
Pivot resources on domain
Account Lockout/DoS
Tampering with data
Information Disclosure
Reputation Damage
Impersonate User C
Ra
Unauthenticated Access
Authenticated Access
Administrative Access to OS/SQL Server
Exploit Vulnerable Product or Service
Overload Server Resources (DoS)
Physical Access to Server
Web Server
Web Server Compromise
Unauthorized Access to Data
Incomplete or Tainted Data
Spread Malware to Clients
Acts as Client to Another Resource
Manipulation of Configuration
Service Delayed or e
Unauthenticated access
Administrative access to operating system
Authenticated PI data access
Exploit vulnerable service on PI Server
Overload PI Server
PI Data Archive Server
PI Data Archive Compromise
Unauthorized access to data
Missing or tainted data sent to users or downstream services
Manipulation of configuration
Spread malware to client connections
Pivot to other servers (PI Server as client to another server or unauthorized call home)
Service delays or unre

Malware → Pivot to other resources → Exploit vulnerable component → Act as client to another resource → Overload server → Service delays or unresponsive

Mismanagement of Credentials → Pivot to other resource → Authenticated access → Access Data → Authenticated access → Send tainted data

Hardening the Platform

Why focus on the platfor



Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

Law #4: If you allow a bad guy to run active content in your website, it's not your website any more.

Law #5: Weak passwords trump strong security.

Law #6: A computer is only as secure as the administrator is trustworthy.

Law #7: Encrypted data is only as secure as its decryption key.

Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all.

Law #9: Absolute anonymity isn't practically achievable, online or offline.

Law #10: Technology is not a panacea.

Windows OS is ubiquitous

- Greater familiarity for attackers
- Greater value to compromise
- Defenses consistent with IT and

Platform security is prerequisite

- Remember the first two immutable laws of cyber security
  https://blogs.technet.microsoft.com/rhalbheer/2011/06/16/ten-immutable-laws-of-security-version-2-0/

PI System defenses depend on platform technologies

- Strong authentication with Kerberos enabled through AD infrastructure
- Transport security provides encryption and signing for confidentiality and integrity

Why defend the platform?

HD Moore's Law: casual Attacker power grows at the rate of Metasploit

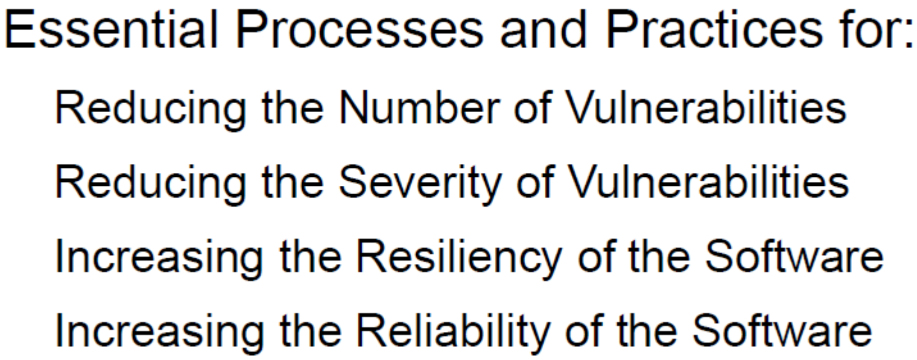
metasploit® EXPLOIT DATABASE SHODAN

1) Deploy the most robust software available

Upgrade to the latest OS

Apply regular updates

Get the benefit of the SDL work MS developers are doing!



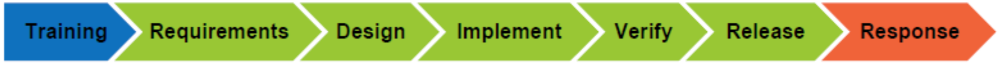
Essential Processes and Practices for:

Reducing the Number of Vulnerabilities

Reducing the Severity of Vulnerabilities

Increasing the Resiliency of the Software

Increasing the Reliability of the Software



Training → Requirements → Design → Implement → Verify → Release → Response

2) Use Windows Server Core

Less Installed, Less Running

- No Graphical User Interface (GUI)
- No Graphic Based Applications

Less Patching (~40%)

Less Maintenance

Smaller Faster Code Base

More Resources Available

Lower Total Cost of Ownership

3) & 4) Leverage Whitelisting features built into the OS

Audit Only or Enforce modes

AD Integrated

AppLocker (KB00944)

- Executable, Windows Installer, Script and DLL rules
- Conditions based on Publisher, Path or File hash.

Windows Advanced Firewall (KB01162)

- Filter by source/destination, ports/applications
- IPsec available for additional protection

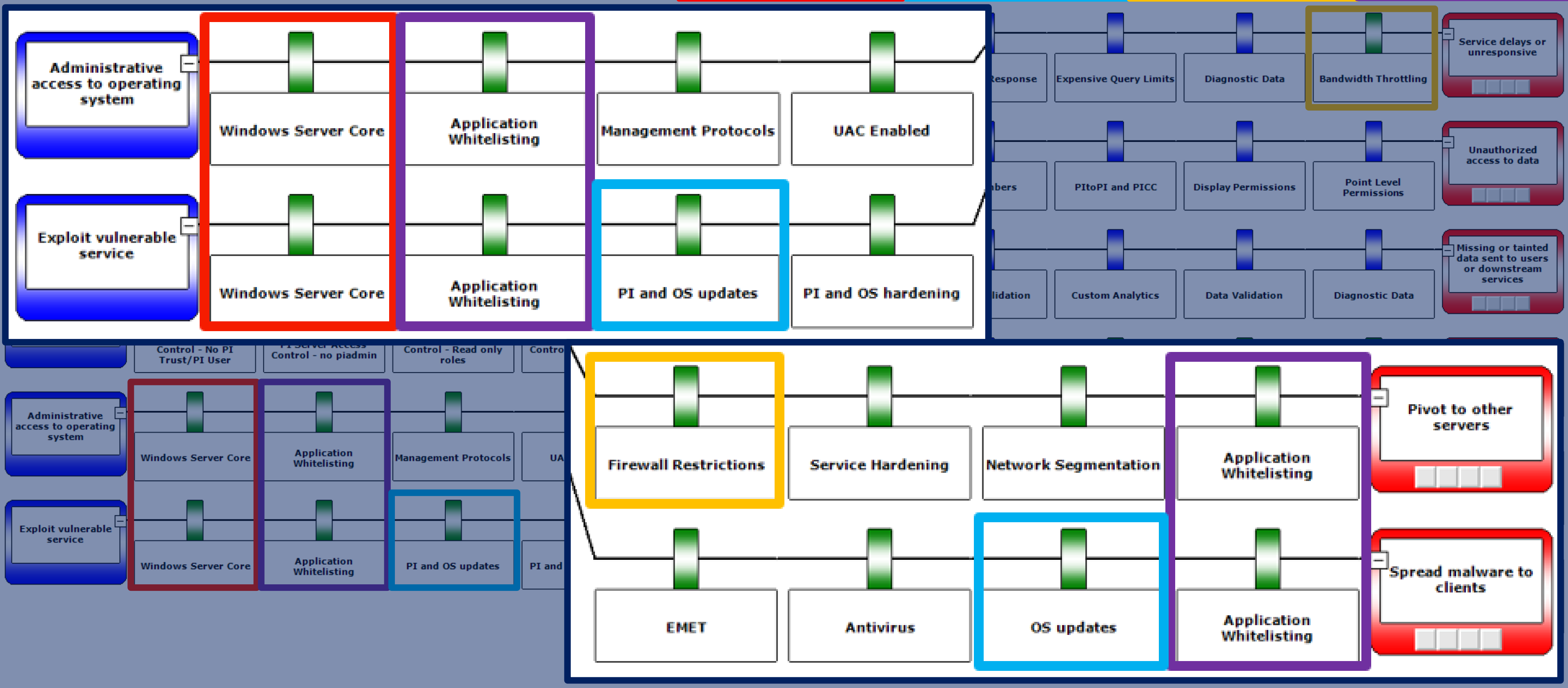
PI Data Archive Bow Tie

🟥 Windows Server Core

🟦 OS Updates

🟨 Firewall Restrictions

🟪 Application Whitelisting



Hardening the PI System

Where do I focus with the PI System?

Update to the latest versions

- The most robust codebase
- Leverage the latest security features

Use Windows Integrated Security everywhere

- Transport security enabled by default
- Allows disabling PI Trust and Explicit Login globally
- Manage access in a consistent approach with other systems

Least Privilege

- No super user; piadmin and AF Server Admin role for disaster recovery only
- Read-only roles for users
- Least privilege for applications with write access

Health Monitoring

- Know your system
- Identify anomalies

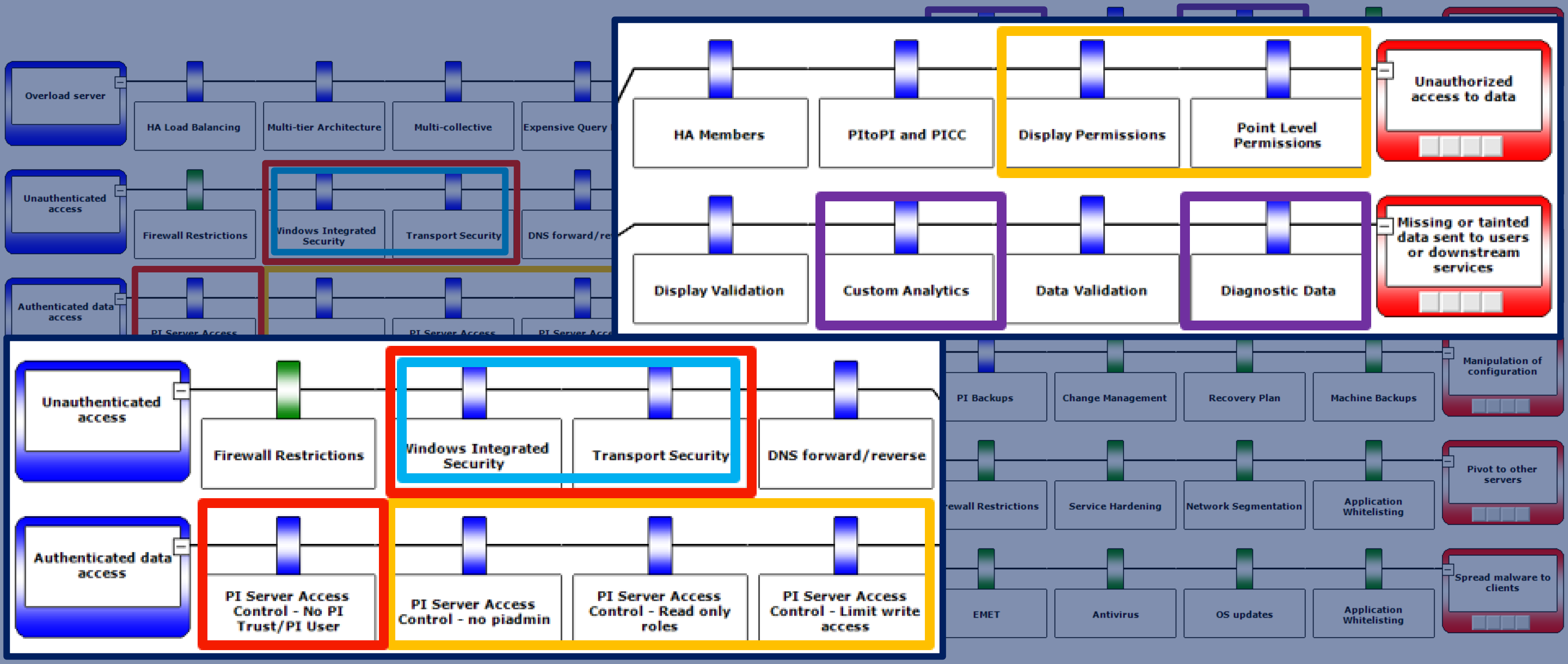
PI Data Archive Bow Tie

WIS Everywhere

PI Updates

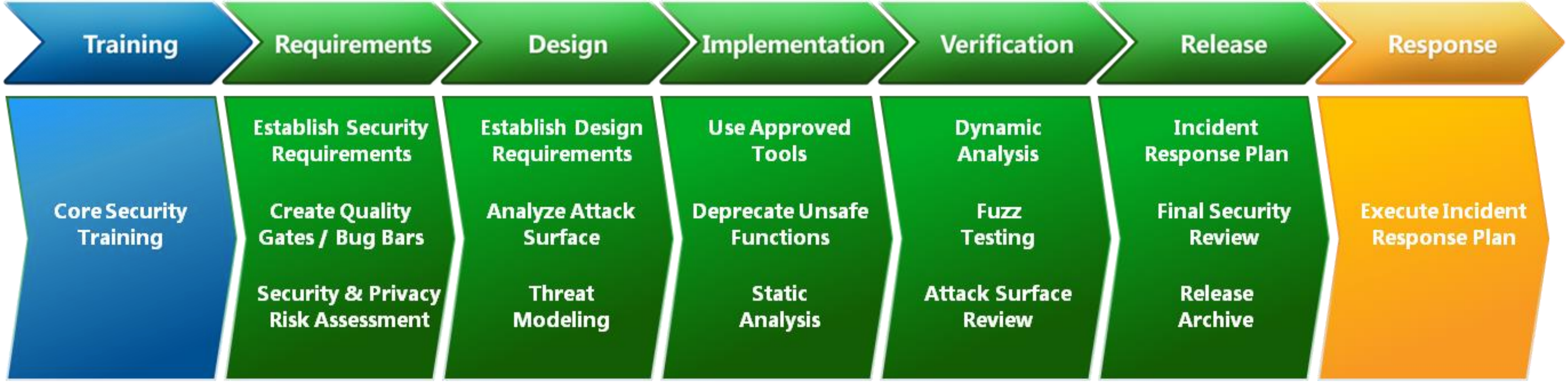
Least Privileges

Health Monitoring



Upgrade: Why use the latest versions?

OSIsoft Security Development Lifecycle (SDL)



Training

Core Security Training

Requirements

Establish Security Requirements

Create Quality Gates / Bug Bars

Security & Privacy Risk Assessment

Design

Establish Design Requirements

Analyze Attack Surface

Threat Modeling

Implementation

Use Approved Tools

Deprecate Unsafe Functions

Static Analysis

Verification

Dynamic Analysis

Fuzz Testing

Attack Surface Review

Release

Incident Response Plan

Final Security Review

Release Archive

Response

Execute Incident Response Plan

Source: https://technet.microsoft.com/en-us/security/gg622918.aspx

Upgrade: Why use the latest versions?

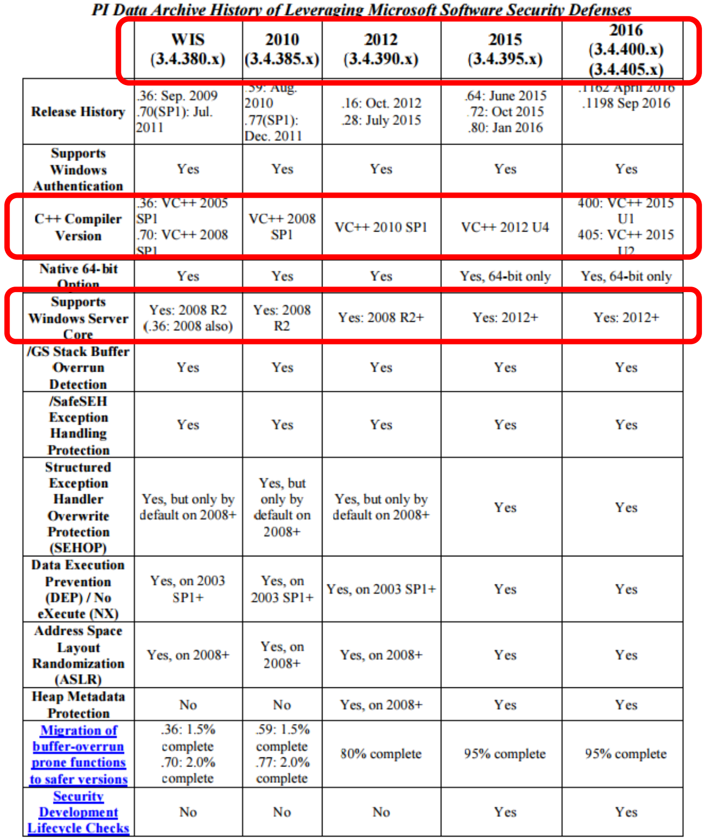
Engagements and Assessments

- **Idaho National Lab**
  - 2005 Assessment
  - 2008/2009/2012 vCampus Live!
  - 2011 Cooperative Research
- **US Army NetCom**
  - 2009/2013 CoN #201006618
- **US NRC**
  - 2010 DISA, NIST
- **NIST NCCoE**
  - 2016 Cooperative Research
- **SAP QBS Certification**
  - 2012/2013/2015 Veracode
- **Windows Logo Certification**
  - 2008 Windows 2008 Server Core
  - 2011 Windows 2008 R2 Server Core
  - 2012 Windows 2012 Server Core
- **Azure Penetration Testing**
  - 2014 PI Cloud Connect (Utility Partner)
  - 2014 PI Cloud Access (IOActive)

- **Information Security Consulting**
  - 2009 PI Server (Microsoft)
  - 2010 PI Agent (Microsoft)
  - 2011 PI Coresight (Microsoft)
  - 2011 PI AF (Microsoft)
  - 2012 PI ProcessBook (Microsoft)
  - 2012 Products in Design (3x - Microsoft)
  - 2013 Engineering Management
  - 2013 Products in Design (3x – Microsoft)
  - 2013/2015 SDL for Security Champions (Microsoft)
  - 2013/2014/2015 Defensive Programming (Cigital)
  - 2015 PI Connectors (Microsoft)
  - 2015 PI Transport Security (IOActive)
  - 2015 PI System Security Review (Microsoft)
  - 2015/2016/2017 Springfield Fuzzer (15x Microsoft)
  - 2016 PI Coresight (IOActive)
  - 2016 PI Coresight Claims (Public/Private Consortium)
- **'Capture the Flag' Challenge**
  - 2016/2017 DigitalBond S4

Upgrade: Recent PI Data Archive Security Changes

- 2015
  - Compiler Defenses
  - Code Safety
  - Transport Security
- 2016
  - Auto Recovery
  - Archive Reprocessing
- 2017
  - Control Flow Guard

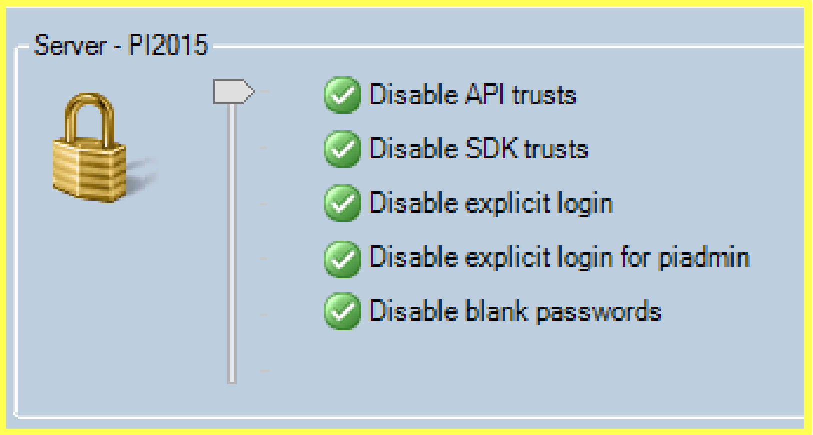


PI Data Archive History of Leveraging Microsoft Software Security Defenses

	WIS (3.4.380.x)	2010 (3.4.385.x)	2012 (3.4.390.x)	2015 (3.4.395.x)	2016 (3.4.400.x) (3.4.405.x)
Release History	.36: Sep. 2009 .70(SP1): Jul. 2011	.59: Aug. 2010 .77(SP1): Dec. 2011	.16: Oct. 2012 .28: July 2015	.64: June 2015 .72: Oct 2015 .80: Jan 2016	.1162 April 2016 .1198 Sep 2016
Supports Windows Authentication	Yes	Yes	Yes	Yes	Yes
C++ Compiler Version	.36: VC++ 2005 SP1 .70: VC++ 2008 SP1	VC++ 2008 SP1	VC++ 2010 SP1	VC++ 2012 U4	400: VC++ 2015 U1 405: VC++ 2015 U2
Native 64-bit Option	Yes	Yes	Yes	Yes, 64-bit only	Yes, 64-bit only
Supports Windows Server Core	Yes: 2008 R2 (.36: 2008 also)	Yes: 2008 R2	Yes: 2008 R2+	Yes: 2012+	Yes: 2012+
/GS Stack Buffer Overrun Detection	Yes	Yes	Yes	Yes	Yes
/SafeSEH Exception Handling Protection	Yes	Yes	Yes	Yes	Yes
Structured Exception Handler Overwrite Protection (SEHOP)	Yes, but only by default on 2008+	Yes, but only by default on 2008+	Yes, but only by default on 2008+	Yes	Yes
Data Execution Prevention (DEP) / No eXecute (NX)	Yes, on 2003 SP1+	Yes, on 2003 SP1+	Yes, on 2003 SP1+	Yes	Yes
Address Space Layout Randomization (ASLR)	Yes, on 2008+	Yes, on 2008+	Yes, on 2008+	Yes	Yes
Heap Metadata Protection	No	No	Yes, on 2008+	Yes	Yes
Migration of buffer-overrun prone functions to safer versions	.36: 1.5% complete .70: 2.0% complete	.59: 1.5% complete .77: 2.0% complete	80% complete	95% complete	95% complete
Security Development Lifecycle Checks	No	No	No	Yes	Yes

WIS Everywhere: Enabled by PI API for WIS

- Compiler Defenses
- Code Safety
- Transport Security
  - Data Integrity and Privacy
- Backward Compatible
  - No changes to existing PI Interfaces



Server - PI2015

✓ Disable API trusts

✓ Disable SDK trusts

✓ Disable explicit login

✓ Disable explicit login for piadmin

✓ Disable blank passwords

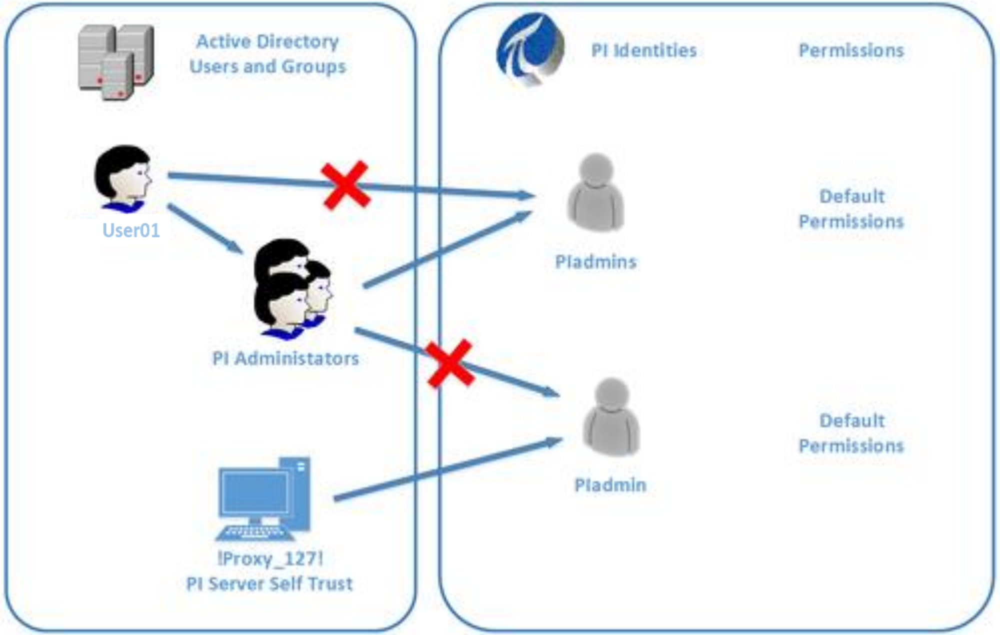
PI Mapping is <u>Required</u>, PI API 2016 does not attempt PI Trust connection!

WIS Everywhere: Transport Security Everywhere

Connection From	PI Trust	NTLM RC4/MD5	Active Directory (Kerberos) AES256/SHA1*
PI Buffer Subsystem	✗	✓	✓
PI Connectors	✗	✓	✓
PI Datalink	✗	✓	✓
PI Processbook	✗	✓	✓
PI Interfaces	✗	✓	✓

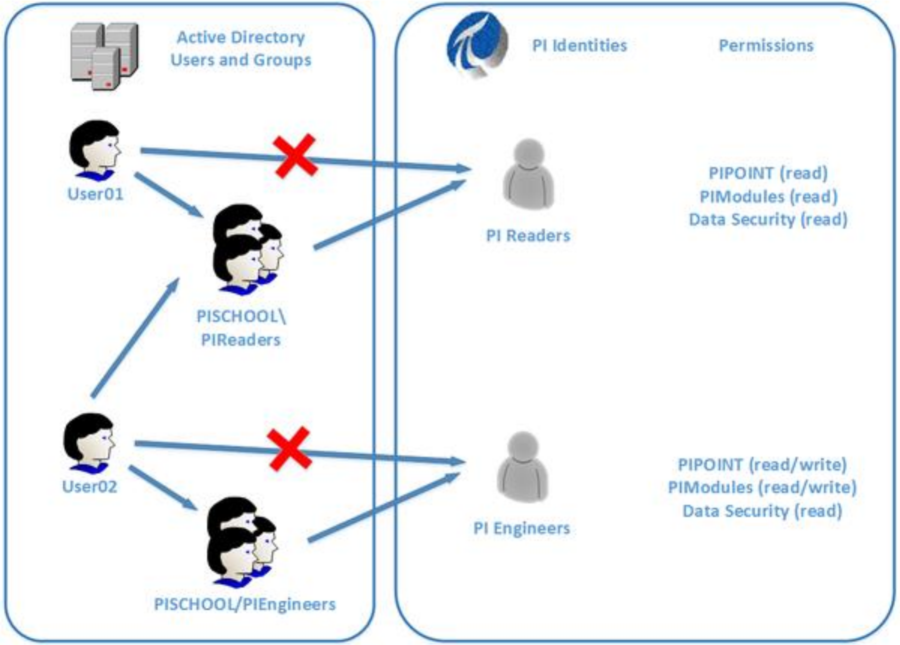
Least Privilege: do not use piadmin

- only use piadmin for disaster recovery
- use piadmins instead



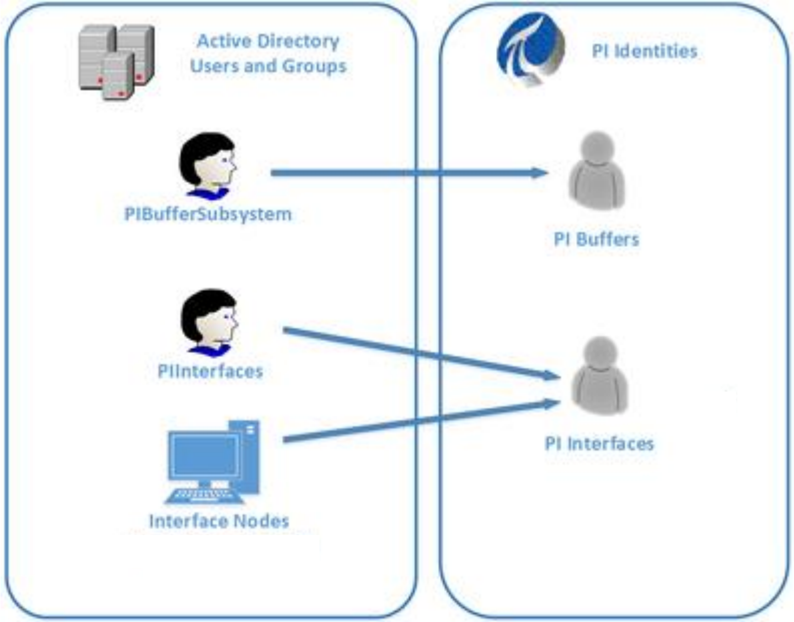
Least Privilege: Read Only Roles

Implement Read Only Roles with mappings to AD groups



Least Privilege: Control Write Access

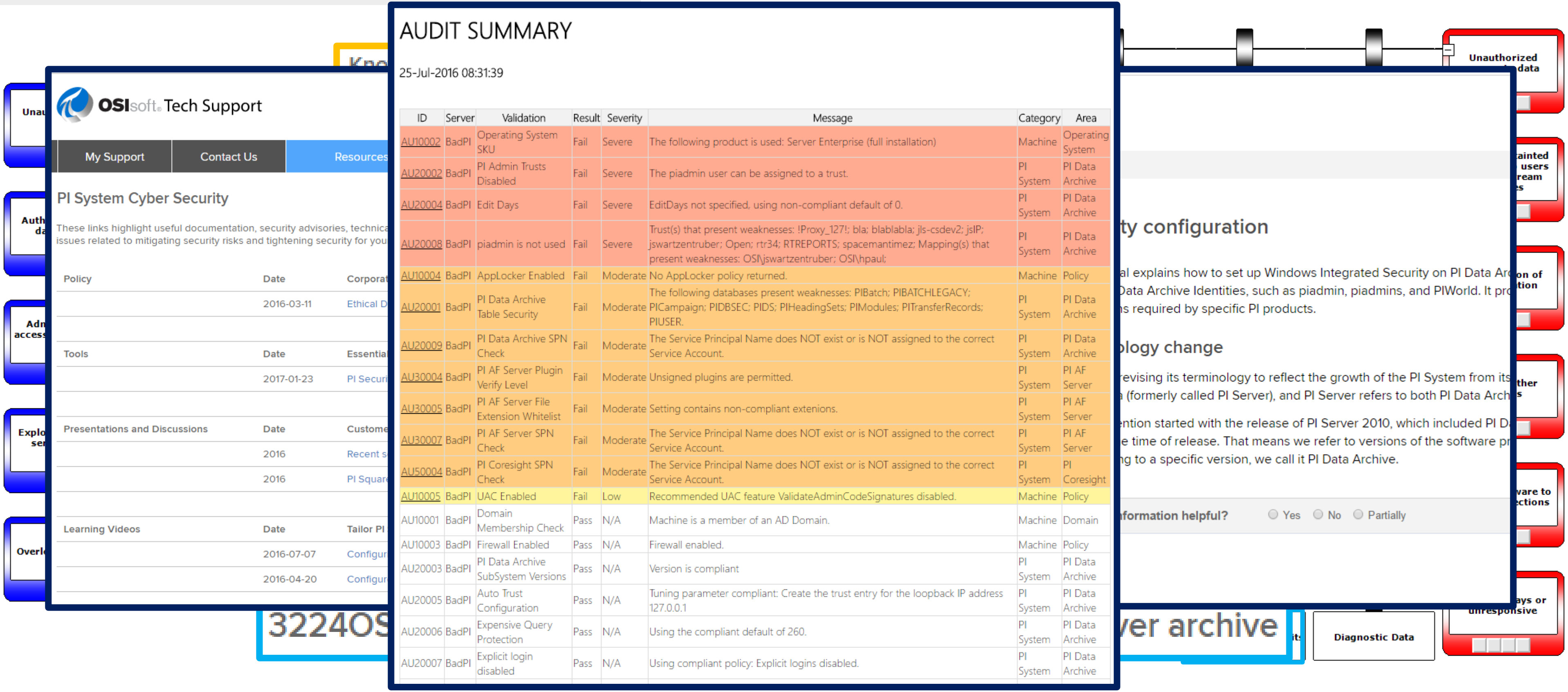
Create Identities and Mappings based on Least Privilege



Process	Read Access	Write Access
Interface	PIPoint, PtSecurity	None
Buffering	PIPoint, PtSecurity, DataSecurity	DataSecurity

Bringing it all together: PI Security Audit Tools

PI Data Archive Bow Tie



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

My Support | Contact Us | Resources

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 pr
s required by specific PI products.

ology change

revising its terminology to reflect the growth of the PI System from its
(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
g to a specific version, we call it PI Data Archive.

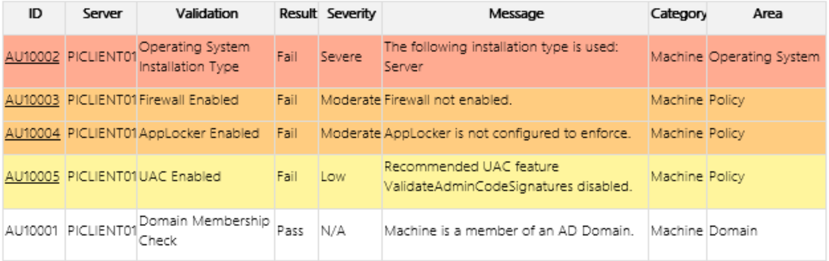
formation helpful? ○ Yes ○ No ○ Partially

PI Security Audit Tools – Baseline your PI System

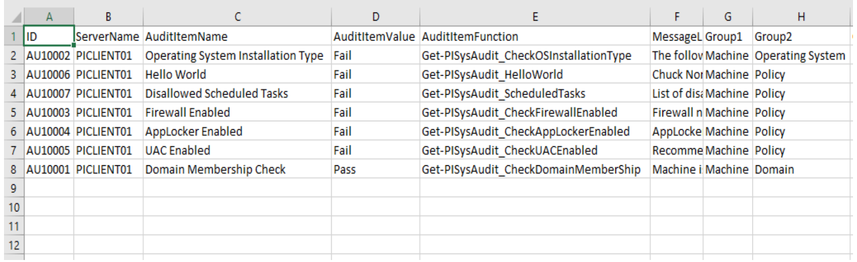
Validated components:

- Machine (General)
- PI Data Archive
- PI AF Server
- MS SQL Server
- PI Coresight

HTML

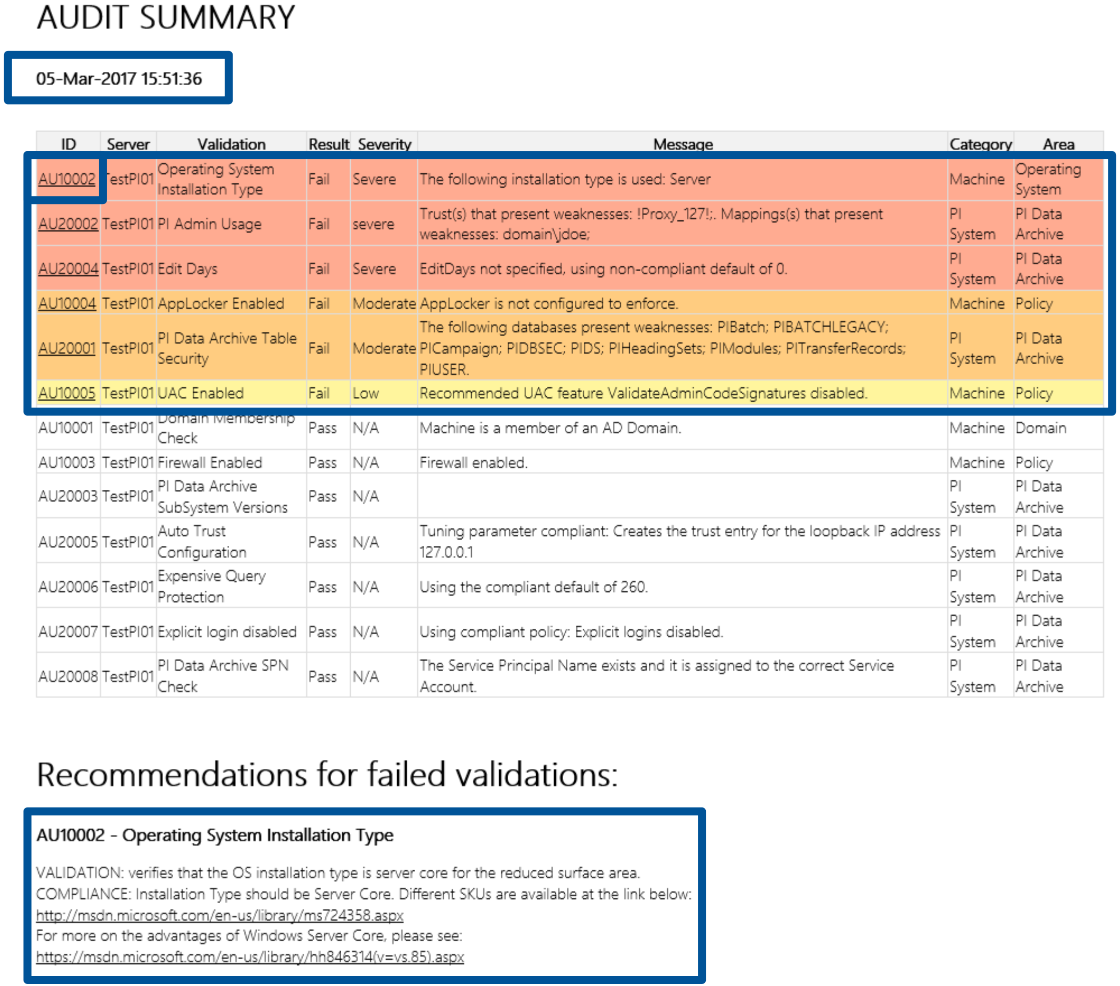


ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	PICLIENT01	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU10003	PICLIENT01	Firewall Enabled	Fail	Moderate	Firewall not enabled.	Machine	Policy
AU10004	PICLIENT01	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 Nor	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								

The Audit Report



AUDIT SUMMARY

05-Mar-2017 15:51:36

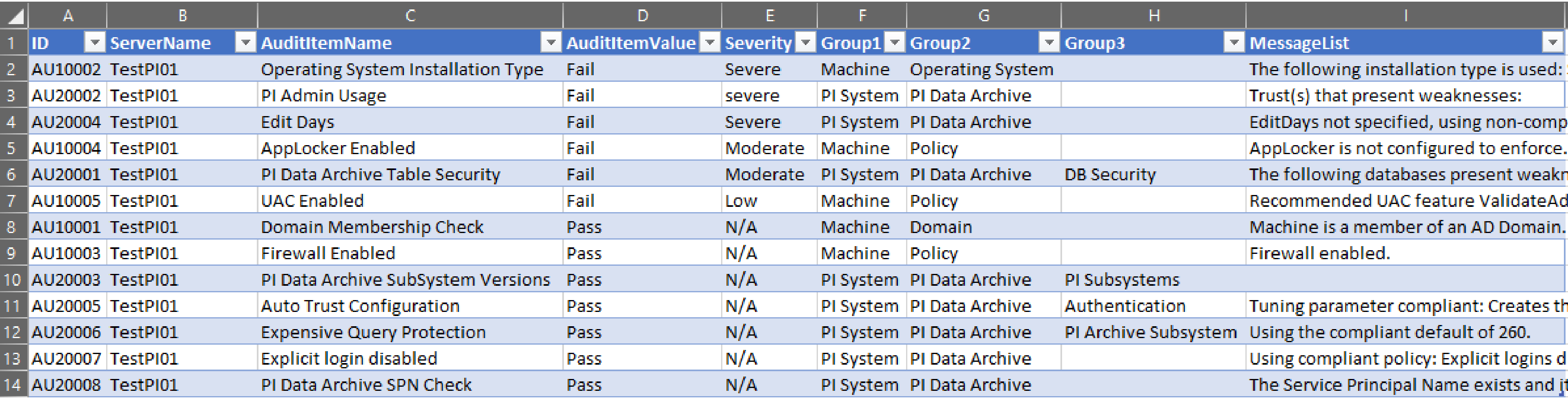
ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	TestPI01	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU20002	TestPI01	PI Admin Usage	Fail	severe	Trust(s) that present weaknesses: !Proxy_127!;. Mappings(s) that 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

The Raw Data



	A	B	C	D	E	F	G	H	I
1	ID	ServerName	AuditItemName	AuditItemValue	Severity	Group1	Group2	Group3	MessageList
2	AU10002	TestPI01	Operating System Installation Type	Fail	Severe	Machine	Operating System		The following installation type is used:
3	AU20002	TestPI01	PI Admin Usage	Fail	severe	PI System	PI Data Archive		Trust(s) that present weaknesses:
4	AU20004	TestPI01	Edit Days	Fail	Severe	PI System	PI Data Archive		EditDays not specified, using non-comp
5	AU10004	TestPI01	AppLocker Enabled	Fail	Moderate	Machine	Policy		AppLocker is not configured to enforce.
6	AU20001	TestPI01	PI Data Archive Table Security	Fail	Moderate	PI System	PI Data Archive	DB Security	The following databases present weakn
7	AU10005	TestPI01	UAC Enabled	Fail	Low	Machine	Policy		Recommended UAC feature ValidateAd
8	AU10001	TestPI01	Domain Membership Check	Pass	N/A	Machine	Domain		Machine is a member of an AD Domain.
9	AU10003	TestPI01	Firewall Enabled	Pass	N/A	Machine	Policy		Firewall enabled.
10	AU20003	TestPI01	PI Data Archive SubSystem Versions	Pass	N/A	PI System	PI Data Archive	PI Subsystems	
11	AU20005	TestPI01	Auto Trust Configuration	Pass	N/A	PI System	PI Data Archive	Authentication	Tuning parameter compliant: Creates th
12	AU20006	TestPI01	Expensive Query Protection	Pass	N/A	PI System	PI Data Archive	PI Archive Subsystem	Using the compliant default of 260.
13	AU20007	TestPI01	Explicit login disabled	Pass	N/A	PI System	PI Data Archive		Using compliant policy: Explicit logins d
14	AU20008	TestPI01	PI Data Archive SPN Check	Pass	N/A	PI System	PI Data Archive		The Service Principal Name exists and i

Requirements

- PowerShell version 2+
- ‘Run As’ administrator (AF and Coresight checks)
- Windows remote management enabled (WinRM)

GitHub Wiki

https://github.com/osisoft/PI-Security-Audit-Tools/wiki

Core Library

Wrappers for consistent local and remote use of several utilities and cmdlets

Public functions to retrieve:

- Environmental Variables
- Registry Keys
- Service Properties
- Process Privilege
- Installed Programs, Updates and Features
- Firewall State
- AppLocker State
- IIS Properties

Invocations for Utilities and Tools:

- AFDiag
- piconfig
- piversion
- sqlcmd
- setspn

Machine Library

Leverages Native PowerShell cmdlets and wrappers for Windows utilities in the core library.

Validation	Issue	Barrier
□ AU10001 – Domain Membership	□ Unauthenticated Access	□ Strong Authentication
□ AU10002 – Windows Server Core	□ Exploit Vulnerability	□ Windows Server Core
□ AU10003 – Windows Firewall State	□ Unauthenticated Access	□ Firewall Restrictions
□ AU10004 – AppLocker State	□ Exploit Vulnerability	□ Application Whitelisting
□ AU10005 – UAC Setting	□ Administrative Access to OS	□ UAC Enabled

Disclaimer – Specialized tools exist for overall platform hardening, e.g. IISCrypto, WACA, MS SCM Industry Profiles, Mozilla Observatory, etc.

PI Data Archive Library

Leverages PowerShell Tools for the PI System with fallback to PI Utilities

Validation	Issue	Barrier
□ AU20001 – PI Database Security	□ Authenticated Access	□ Read only roles
□ AU20002 – Limit piadmin Usage	□ Authenticated Access	□ Access Control – do not use piadmin
□ AU20003 – Software Version	□ Exploit Vulnerability	□ PI Updates
□ AU20004 – Archive EditDays	□ Manipulate Data	□ Change control configuration
□ AU20005 – Trust Configuration	□ Unauthenticated Access to Data	□ Access Control - Limit use of Trusts
□ AU20006 – Limit Expensive Queries	□ Overload Server	□ Terminate expensive queries
□ AU20007 – Disable Explicit Login	□ Authenticated Access to Data	□ Access Control – No Explicit Login
□ AU20008 – SPN Set Properly	□ Unauthenticated Access	□ Strong Authentication

PI AF Server Library

Leverages AFDiag and PowerShell Tools for the PI System to access server configuration settings

Validation	Issue	Barrier
□ AU30001 – Service Account	□ Access to Data	□ Least Privilege
□ AU30002 – Data Set Impersonation	□ Access to Data	□ Impersonation by Service
□ AU30003 – Service Access	□ Pivot to Other Resources	□ Service Hardening
□ AU30004 – Plugin Verify Level	□ Spread Malware to Clients	□ Verify Digital Signature and Trusted Provider
□ AU30005 – Extension Whitelist	□ Spread Malware to Clients	□ Application Whitelisting
□ AU30006 – Software Version	□ Exploit Vulnerability	□ PI Updates
□ AU30007 – SPN	□ Unauthenticated Access	□ Strong Authentication
□ AU30008 – Server Admin Right	□ Authenticated Access	□ Access Control – Limit Administrative Privilege

MS SQL Server Library

Leverages SQLPS module with fallback to sqlcmd to access server configuration

- Intended to provide guidance for PIFD and PI Coresight database hosting SQL Servers

Validation	Issue	Barrier
□ AU40001 – XP Command Shell	□ Pivot to other resources	□ Service Hardening
□ AU40002 – Ad Hoc Queries	□ Access to Data	□ Service Hardening
□ AU40003 – DB Mail XPS	□ Pivot to other resource	□ Service Hardening
□ AU40004 – OLE Automation Procs	□ Pivot to other resource	□ Service Hardening
□ AU40005 – sa	□ Authenticated Access	□ Access Control – Disable super user
□ AU40006 – Remote Access	□ Authenticated Access	□ Service Hardening
□ AU40007 – Cross DB Ownership Chaining	□ Unauthenticated Access	□ Service Hardening
□ AU40008 – CLR	□ Exploit Vulnerability	□ Service Hardening

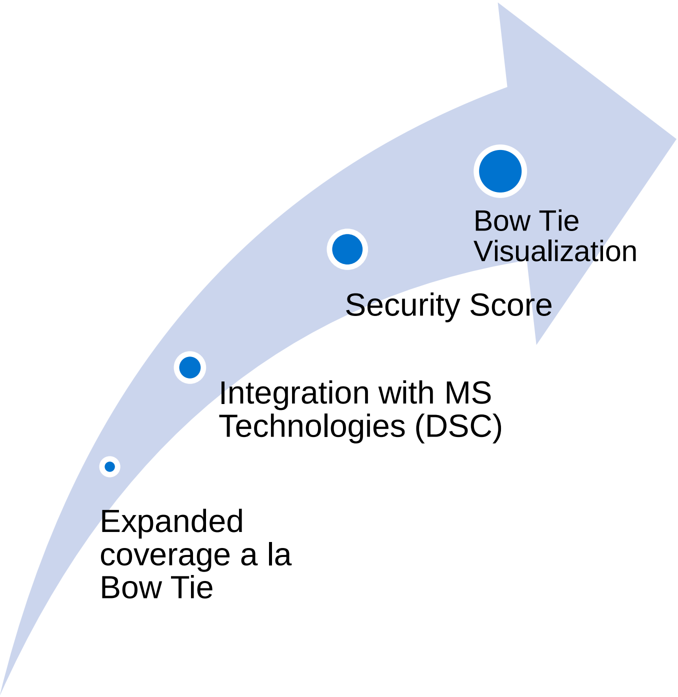
PI Coresight Library

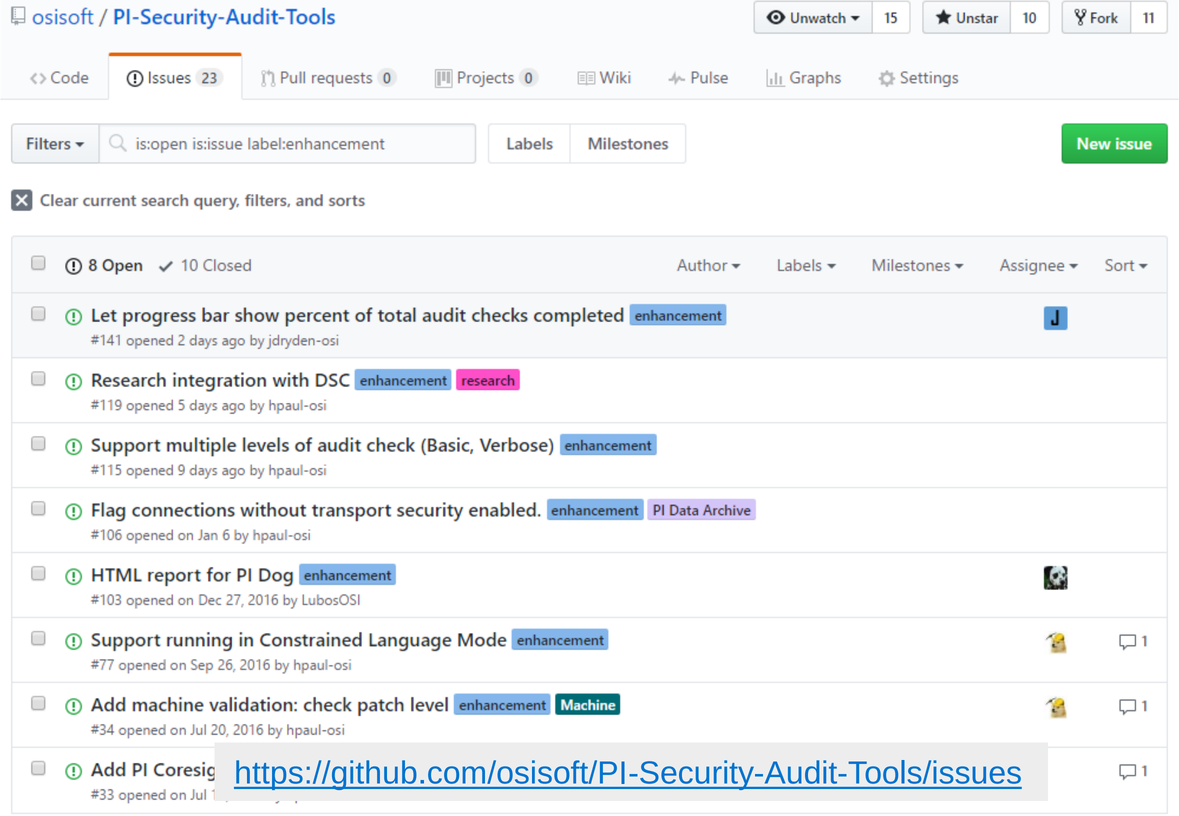
Leverages WebAdministration Module to inspect IIS configuration.

Validation	Issue	Barrier
□ AU50001 – Software Version	□ Exploitation of Vulnerability	□ PI Updates
□ AU50002 – AppPool Identity	□ Authenticated Access to Data	□ Least Privilege
□ AU50003 – TLS Configured	□ Unauthenticated Access	□ Transport Layer Security
□ AU50004 – SPN Configured	□ Unauthenticated Access	□ Strong Authentication

Note: IISCrypto is a reliable tool to set allowed TLS ciphers

What’s next for the PI Security Audit Tools?


Bow Tie Visualization
Security Score
Integration with MS Technologies (DSC)
Expanded coverage a la Bow Tie



is:open is:issue label:enhancement

☒ Clear current search query, filters, and sorts

□ 8 Open ✓ 10 Closed

□ Let progress bar show percent of total audit checks completed enhancement
#141 opened 2 days ago by jdryden-osi

□ Research integration with DSC enhancement research
#119 opened 5 days ago by hpaul-osi

□ Support multiple levels of audit check (Basic, Verbose) enhancement
#115 opened 9 days ago by hpaul-osi

□ Flag connections without transport security enabled. enhancement PI Data Archive
#106 opened on Jan 6 by hpaul-osi

□ HTML report for PI Dog enhancement
#103 opened on Dec 27, 2016 by LubosOSI

□ Support running in Constrained Language Mode enhancement 1
#77 opened on Sep 26, 2016 by hpaul-osi

□ Add machine validation: check patch level enhancement Machine 1
#34 opened on Jul 20, 2016 by hpaul-osi

□ Add PI Coresig 1
#33 opened on Jul 1

https://github.com/osisoft/PI-Security-Audit-Tools/issues

LAB: Using and Building the PI Security Audit Tools, a tool to baseline your PI System security

Today @ 2:15 PM

Part I: Learn how to use the tools to evaluate deployments and use the output to prioritize improvements to defenses.

Part II: Learn how to extend the libraries to include validation checks specific to an organization's needs and how to implement new libraries with the tool.

감사합니다

谢谢

Danke

Merci

Gracias

Thank You

ありがとう

Спасибо

Obrigado

Stop by the PI Security booth in the expo!

Questions

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

State your **name & company**

Please remember to…

Complete the Online Survey for this session

Download the Conference App for OSIsoft Users Conference 2017

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

Download on the App Store

GET IT ON Google Play

HTML

search **OSISOFT** in the app store

http://bit.ly/uc2017-app

Contact Information

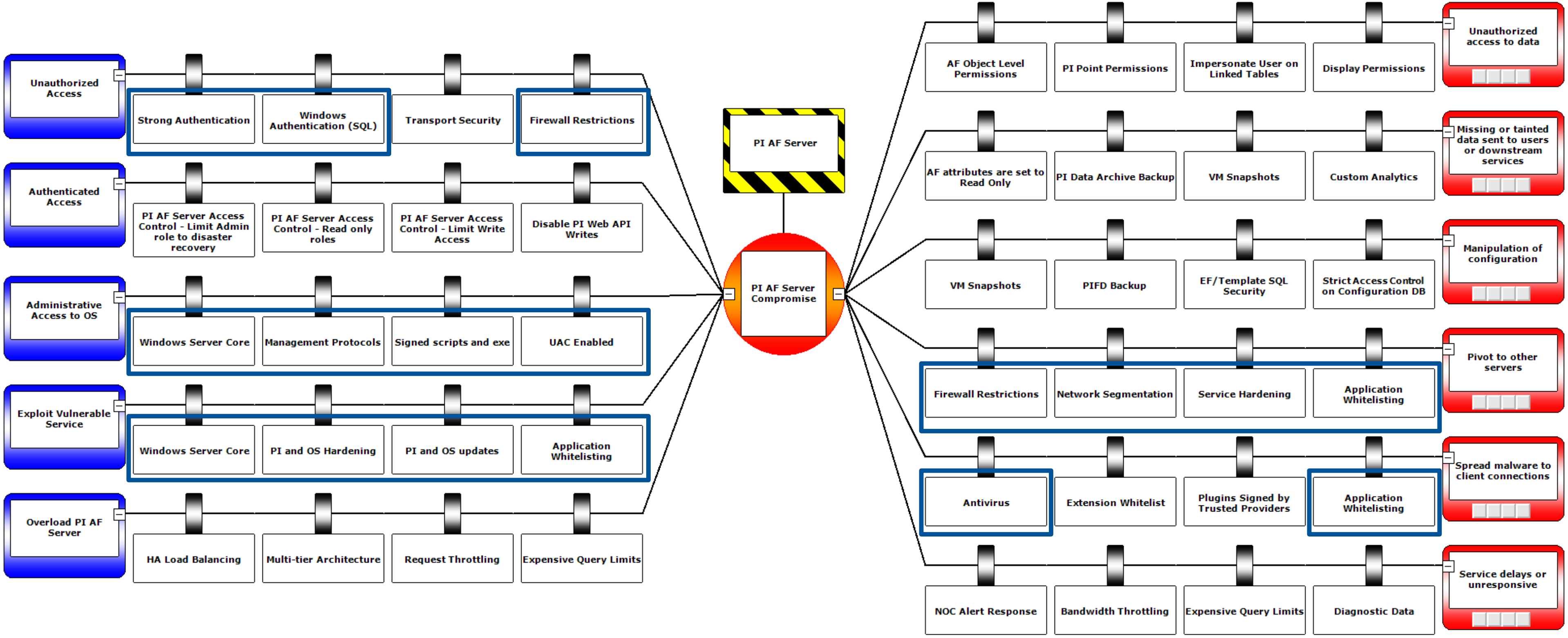
Harry Paul

hpaul@osisoft.com

Cyber Security Advisor,
Customer Success

OSIsoft, LLC

PI AF Server Bow Tie



PI AF Server

PI AF Server Compromise

Unauthorized Access	Strong Authentication	Windows Authentication (SQL)	Transport Security	Firewall Restrictions
Authenticated Access	PI AF Server Access Control - Limit Admin role to disaster recovery	PI AF Server Access Control - Read only roles	PI AF Server Access Control - Limit Write Access	Disable PI Web API Writes
Administrative Access to OS	Windows Server Core	Management Protocols	Signed scripts and exe	UAC Enabled
Exploit Vulnerable Service	Windows Server Core	PI and OS Hardening	PI and OS updates	Application Whitelisting
Overload PI AF Server	HA Load Balancing	Multi-tier Architecture	Request Throttling	Expensive Query Limits

AF Object Level Permissions	PI Point Permissions	Impersonate User on Linked Tables	Display Permissions	Unauthorized access to data
AF attributes are set to Read Only	PI Data Archive Backup	VM Snapshots	Custom Analytics	Missing or tainted data sent to users or downstream services
VM Snapshots	PIFD Backup	EF/Template SQL Security	Strict Access Control on Configuration DB	Manipulation of configuration
Firewall Restrictions	Network Segmentation	Service Hardening	Application Whitelisting	Pivot to other servers
Antivirus	Extension Whitelist	Plugins Signed by Trusted Providers	Application Whitelisting	Spread malware to client connections
NOC Alert Response	Bandwidth Throttling	Expensive Query Limits	Diagnostic Data	Service delays or unresponsive

Detailed Flow and Topics to Consider

- Title
- Agenda
- About “Company Name”
  - Industry
  - Market(s) Served
  - Organization/Sites
  - etc.
- Business Challenge/Problem /Initiative Addressed
- Problem Detail
- Solution
- OSIsoft Products and Services Employed
  - Field Service, TechSupport, Training, vCampus, Enterprise Agreement (including EPM, CoE, NOC)
- PI System Architecture
- Implementation Details (How?)
- Results … consider the following:
  - Productivity
  - Visibility
  - Data Integration
  - One Version of the Truth
  - Security
  - Reliability
  - Compliance
  - Quality
  - Scalability
  - Availability
  - etc.
- Impact on Business
- Tangible Benefits
  - Quantified in dollars if possible
  - ROI
  - etc.
- Intangible Benefits
- Future Plans and Next Steps
- Summary slide
- Conclusion/Takeaway(s)
- Contact Information
- Questions
- Thank you

Items the Audience Likes To Hear About

- What was the business reason and justification for rolling out your system
- What was the measurable value that you gained
- How was it implemented – explain in detail
- How did you build momentum in the organization
- What were critical components for success
- What do you see as next steps
- What is the business impact

OSIsoft Product, Component, Subcomponent and Services names

Advanced Services
Advanced Integrations
- when referring to PI Integrators as a whole
AF Builder
AF SDK
Asset Based PI Jumpstart
Incorrect: AF Jumpstart
AutoPointSync (APS)
Center of Excellence (CoE)
Connected Services
Enterprise Agreement (EA)
Enterprise Agreement Program
Enterprise Program Manager (EPM)
Enterprise Services
Field Service
Field Service Engineers
Learning
Incorrect: Training

OSIsoft Field Service
OSIsoft MDUS™
OSIsoft Utilities Gateway™
Incorrect: PI Utilities Gateway, Utilities Gateway
PI ActiveView™
PI API®
PI BatchView
PI Cloud Services
PI Cloud Connect™
PI Connectors
PI Collective™
PI COM Connectors
PI Coresight™
PI DataLink®
Incorrect: Datalink, DataLink, PI Datalink
PI DataLink Server™
PI Developer Technologies
PI JDBC™

Contd. on next slide

OSIsoft Product, Component, Subcomponent and Services names

PI OLEDB™
PI OLEDB Provider
PI OLEDB Enterprise
PI ODBC™
PI Web Services™
PI Interface™
PI Interfaces
PI Interface for “name of source system”
Examples:
- PI Interface for OPC HDA
- PI Interface for ABB IMS Advant
- PI Interface for Honeywell PHD

PI Interface Configuration Utility™ (PI ICU)
PI Integrator for Esri ArcGIS
- *Note:* When distinguishing between the cloud and on premise versions of the PI Integrator for Esri ArcGIS the product name should be written as:

PI Integrator for Esri ArcGIS (cloud)
PI Inegrator for Esri ArcGIS (on-premise)
- *Note:* If Esri and ArcGIS have not been mentioned and trademarked as Esri® and ArcGIS® elsewhere in your document, then the first instance the PI Integrator for Esri ArcGIS should be written as: PI Integrator for Esri® ArcGIS®
- *Incorrect:* PI Cloud Integrator for Esri ArcGIS

PI Integrators
PI Manual Logger™ (PI ML)
PI Manual Logger Mobile™ (PI ML Mobile)
PI OPC DA/HDA Server™
PI ProcessBook®
- *Incorrect:* Processbook, ProcessBook, PI Process Book, PI Processbook

PI Server™
- *Incorrect:* PI, PI Historian

Contd. on next slide

OSIsoft Product, Component, Subcomponent and Services names

Advanced Computing Engine (ACE)

Incorrect: Advanced Calculation Engine (ACE), Advanced Computation Engine (ACE), PI Advanced Calculation Engine (PI ACE), Advanced Computation Engine (PI ACE), PI Advanced Computing Engine (PI ACE)

Asset Analytics

Incorrect: Asset Based Analytics, PI Analytics

Asset Framework (AF)

Incorrect: Analysis Framework (AF), PI Asset Framework (PI AF), PI Analysis Framework (PI AF)

Batch

Incorrect: PI Batch

Data Archive

Incorrect: PI Archive

Event Frames

High Availability (HA)

PI Interfaces for System Monitoring

Notifications

Incorrect: PI Notifications

Performance Equations (PE)

Incorrect: Performance Equations (PEs), PI Performance Equations (PI PE), PI Performance Equation (PI PE), Performance Equation (PE)

Steam Tables

System Management Tools (SMT)

Incorrect: PI System Management Tools (PI SMT)

Totalizers

PI Smart Connectors™

PI Smart Connector Container™

PI SQC™

PI System®

Incorrect: PI, PI System Historian

PI System Access™ (PSA)

PI System Access™ (PSA) - Named User

PI System Access™ (PSA) - Server