



# Cyber Security

Bryan Owen PE – Principal Cyber Security Manager

October 11, 2016



# Agenda

- Overview
- What's new in PI Security
- Demo
- What's coming next
- Call to Action

# Cyber Security is more of a Marathon than a Sprint

- Release Cadence
  - Quicker response time
  - More agile and predictable
  - Most, not all products
- Ethical Disclosure Policy
  - Transparency
  - Do no harm



<https://techsupport.osisoft.com/Troubleshooting/Ethical-Disclosure-Policy>

# Boundary Protection is Essential

## Critical Systems

Transmission  
& Distribution  
SCADA

Plant DCS

PLCs

Environmental  
Systems

Other critical  
operations systems



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



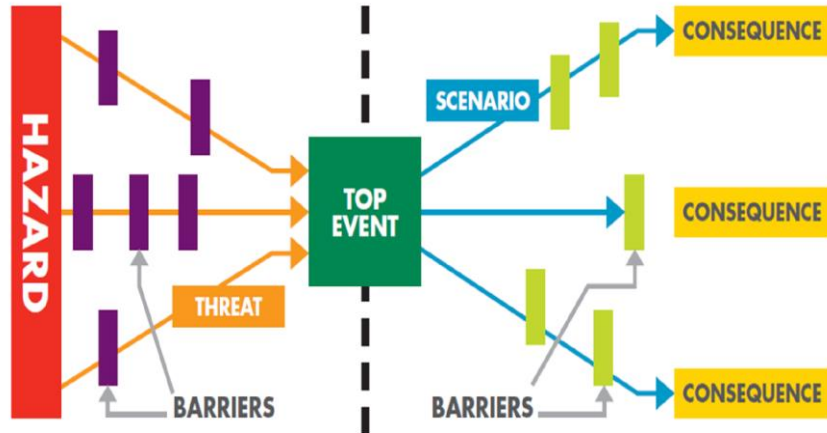
Security Perimeter



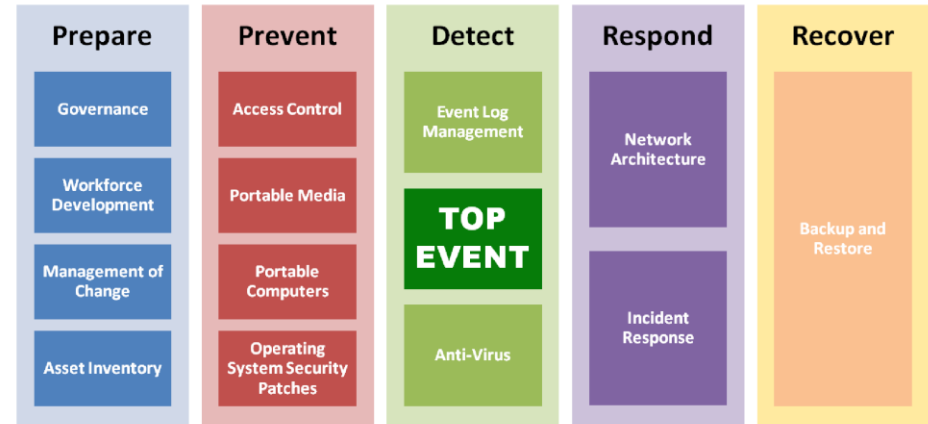
Reduce the risks on critical systems

# Best Practices are Advancing

## Engineering Bow-Tie Model



## ICS Security Bow-Tie

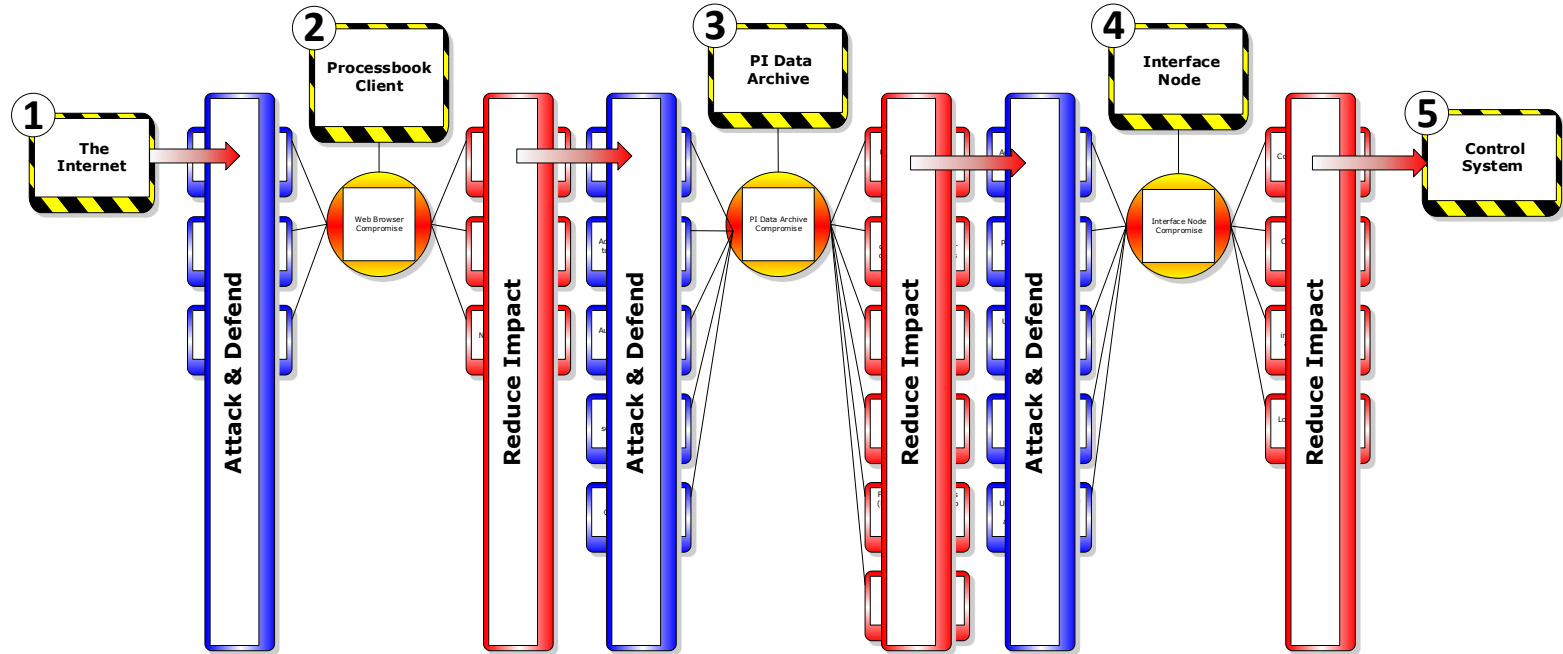


## Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology

<https://www.sans.org/reading-room/whitepapers/ICS/evaluating-cyber-risk-engineering-environments-proposed-framework-methodology-37017>

# Classic PI System Kill Chain

- Many opportunities to defend
- Attack scenarios are complex
- Resists common malware



<https://pisquare.osisoft.com/groups/security/blog/2016/08/02/bow-tie-for-cyber-security-0x01-how-to-tie-a-cyber-bow-tie>



# What's New in PI Security



# Classic PI Client Desktop

- Processbook 2015 R2
  - Memory corruption defenses (VS2013)
  - Removes .NET Framework 3.5 dependency
  - Improves support for EMET
- PI SDK 2016
  - Memory corruption defenses (VS2015)
  - MS Runtime Updates
  - Transport Security (Data Integrity and Privacy)

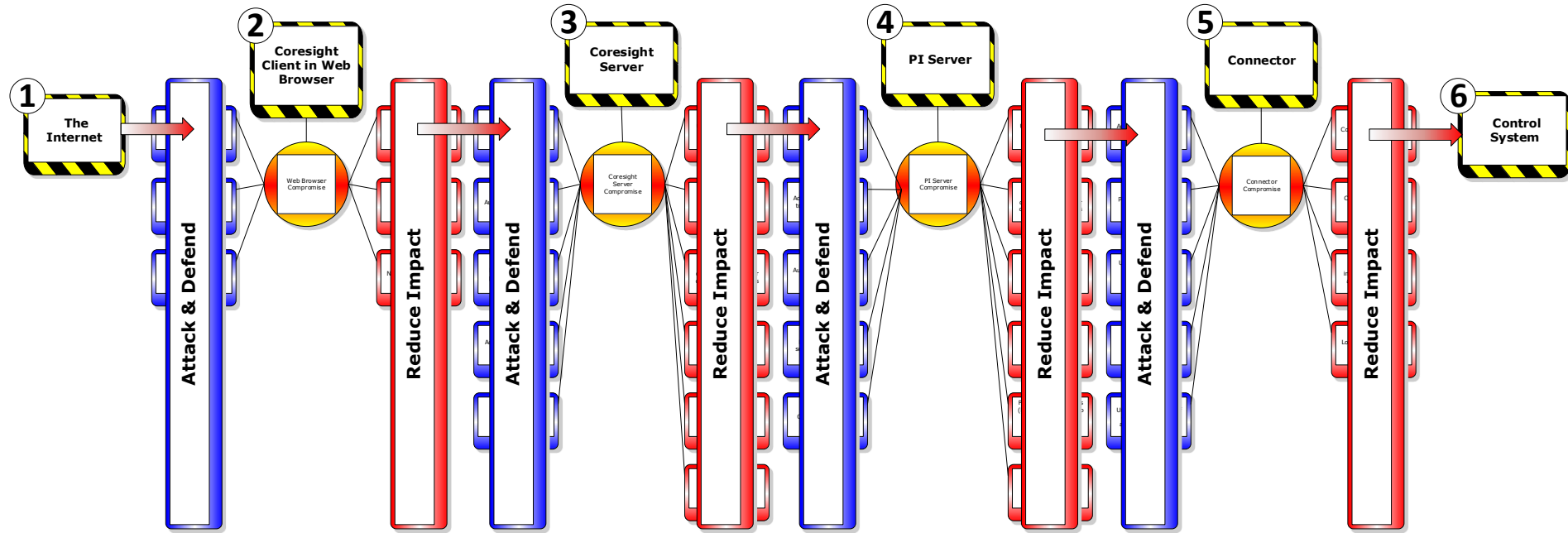


[KB01289 - How To Enhance Security in PI ProcessBook Using EMET](#)



# Modern PI System Kill Chain

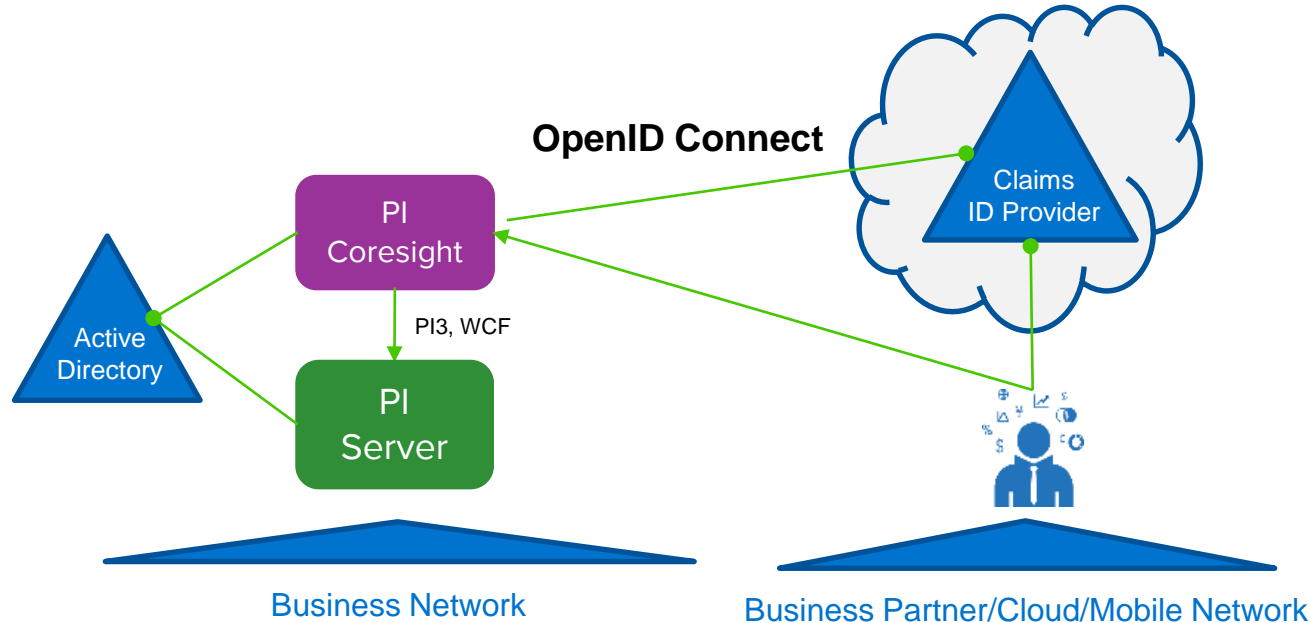
- Latest defensive technology
- More separation from threat to target
- Shifts cost from defender to attacker



PI Square: [Hardcore PI Coresight Hardening](#)

# Advanced Security in PI Coresight 2016 R2

- Login using an external Identity Provider
  - No need to expose corporate AD credentials





# Security Changes for PI Server

# PI AF – Recent Security Changes

- 2015
  - Identity Mappings
  - Service Hardening
  - AF Client to Data Archive Transport Security
- 2016
  - IsManualDataEntry
  - Annotate Permission
  - File Attachment Checks

File Type	Allowed Extensions
MS Office	csv, docx, pdf, xlsx
Text	rtf, txt
Image	gif, jpeg, jpg, png, svg, tiff
ProcessBook	pdi

PI System Explorer 2016 User Guide: “Security for Annotations”

# PI Data Archive – Recent Security Changes

- 2015
  - Compiler Defenses
  - Code Safety
  - Transport Security
- 2016
  - Auto Recovery
  - Archive Reprocessing

*PI Data Archive History of Leveraging Microsoft Software Security Defenses*

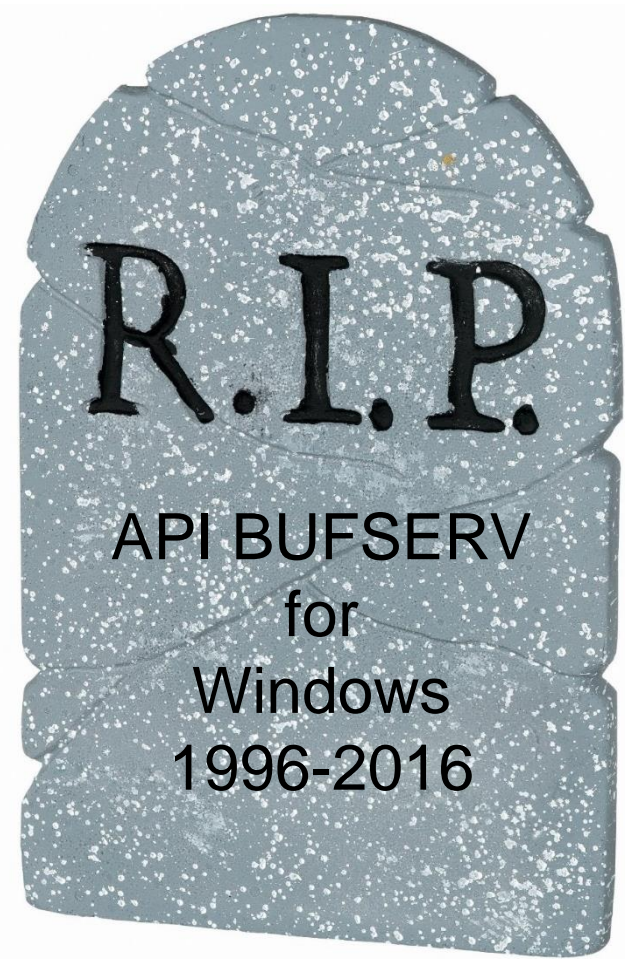
	WIS (3.4.380.x)	2010 (3.4.385.x)	2012 (3.4.390.x)	2015 (3.4.395.x)	2016 (3.4.400.x)
Release History	.36: Sep. 2009 .70(SP1): Jul. 2011	.59: Aug. 2010 .77(SP1): Dec. 2011	.16: Oct. 2012 .28: July 2015	.64: June 2015 .72: Oct 2015 .80: Jan 2016	.1162 April 2015
Supports Windows Authentication	Yes	Yes	Yes	Yes	Yes
C++ Compiler Version	VC++ 2005 SP1 .70: VC++ 2008 SP1	VC++ 2008 SP1	VC++ 2010 SP1	VC++ 2012 Update 4	VC++ 2015 Update 1
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+
OS 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



# Security Changes for PI System Interfaces

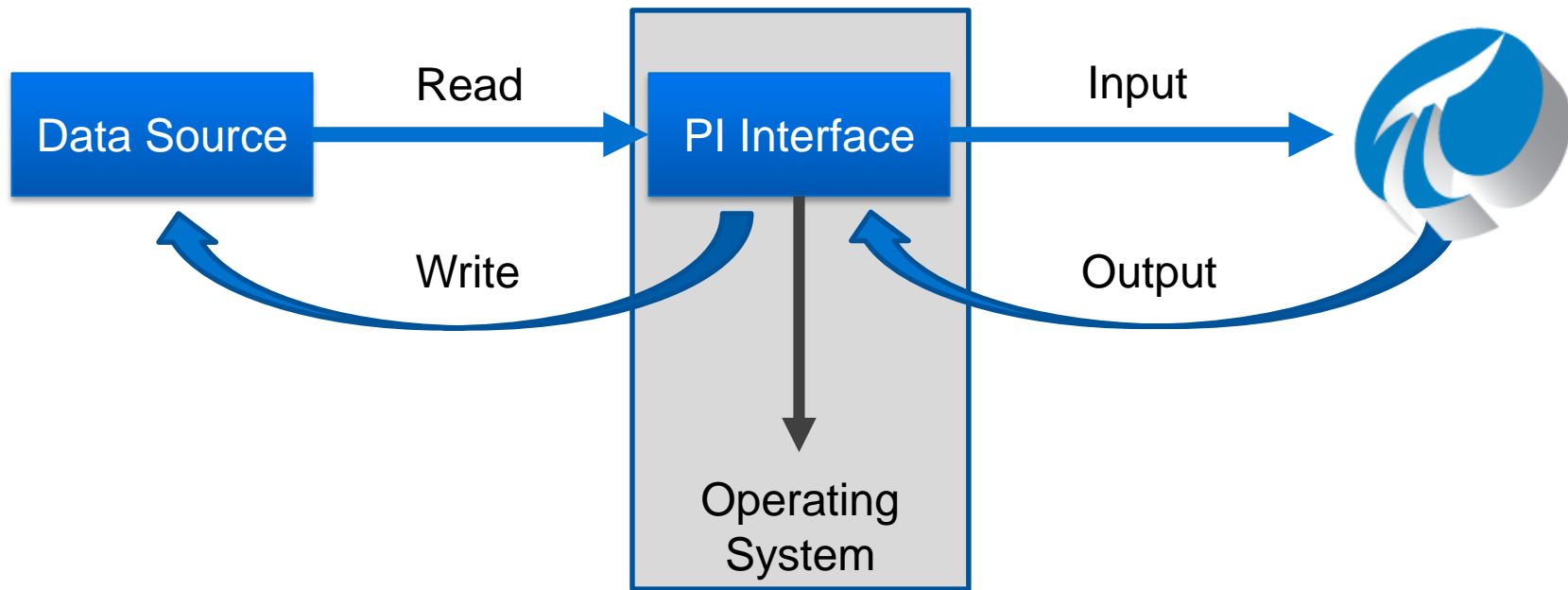
# PI Buffer Subsystem

- 2015
  - Code Safety
  - Transport Security with Windows Authentication
- 2016
  - Service Accounts
    - Managed Service Account (Domain only)
    - Virtual Service Account

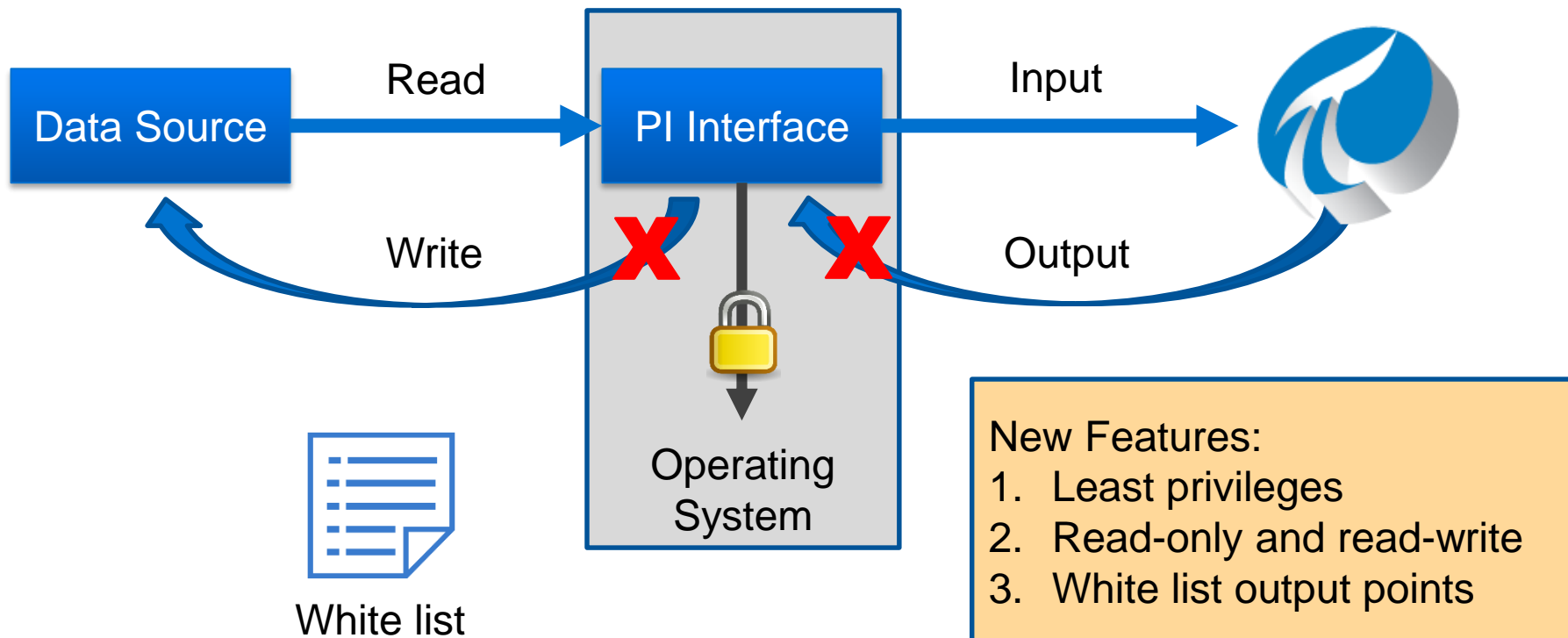




# PI Interfaces – New options for securing


















# PI Interfaces – New options for securing



# Code Hardened PI Interfaces

Hardened	Hardened + Read-Only Available
PI Interface for ESCA HABConnect Alarms and Events	PI Interface for Foxboro I/A 70 Series
PI Interface for Cisco Phone	PI Interface for Metso maxDNA
PI Interface for ESCA HABConnect	PI Interface for Citect
PI to PI Interface	PI Interface for SNMP Trap
PI Interface for CA ISO ADS Web Service	PI Interface for Modbus Ethernet PLC
PI Interface for IEEE C37.118	PI Interface for OPC HDA
PI Interface for Performance Monitor	PI Interface for GE FANUC Cimplicity HMI
PI Interface for Siemens Spectrum Power TG	PI Interface for ACPLT/KS
PI Interface for OPC DA	
PI Interface for Relational Database (RDBMS via ODBC)	
PI Interface for Universal File and Stream Loading (UFL)	

# Transport Security Everywhere

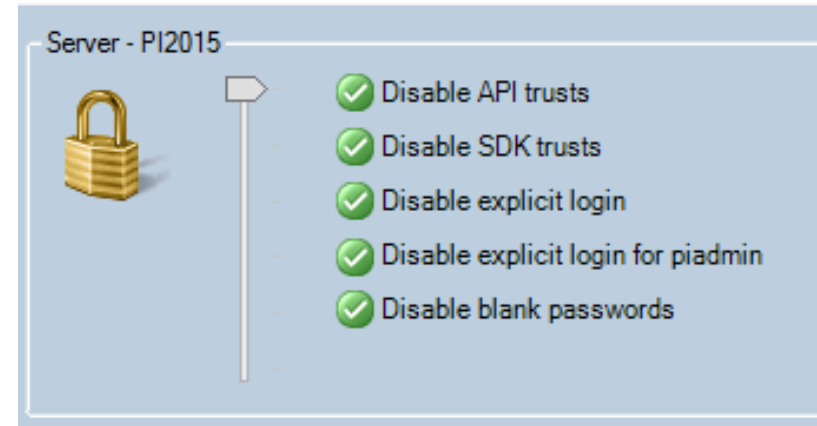
Connection From	PI Trust	NTLM RC4/MD5	Active Directory (Kerberos) AES256/SHA1*
PI Buffer Subsystem			
PI Connectors			
PI Datalink			
PI Processbook			
PI Interfaces			



# Introducing PI API 2016 for Windows Integrated Security

# PI API 2016 for Windows Integrated Security

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



**PI Mapping is Required, PI API 2016 does not attempt PI Trust connection!**

File View Tools Help

Collectives and Servers

Search

Servers

☒ PIDEOMVM

System Management Tools

Search

- Alarms
- Batch
- Data
- Interfaces
- IT Points
- Operation
- Points
- Security

Alarm Groups SGC Alarms

# Task 1: Identify all PI trusts and corresponding PI Identities/PI Users

Session Record

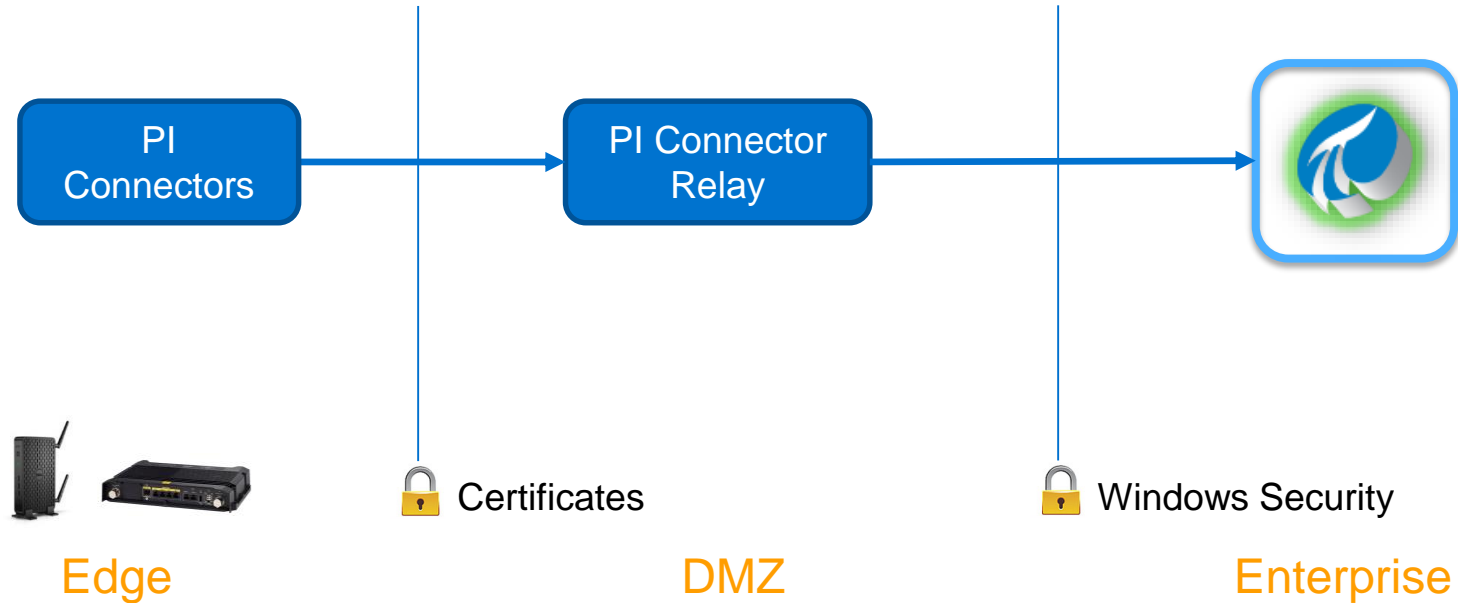
PIDEMOVM\Administrator | piadmin, piadmins, PIWorld



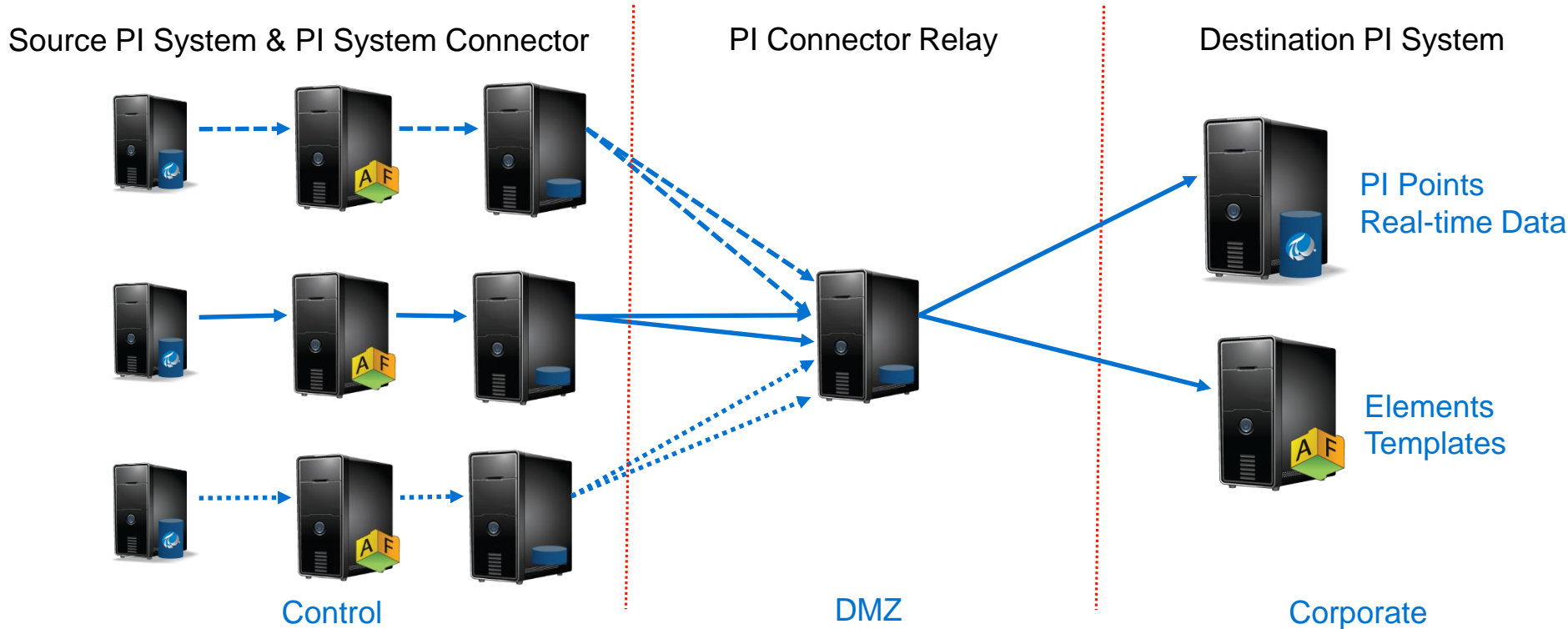


# Security Changes in Progress

# PI Connector Architecture

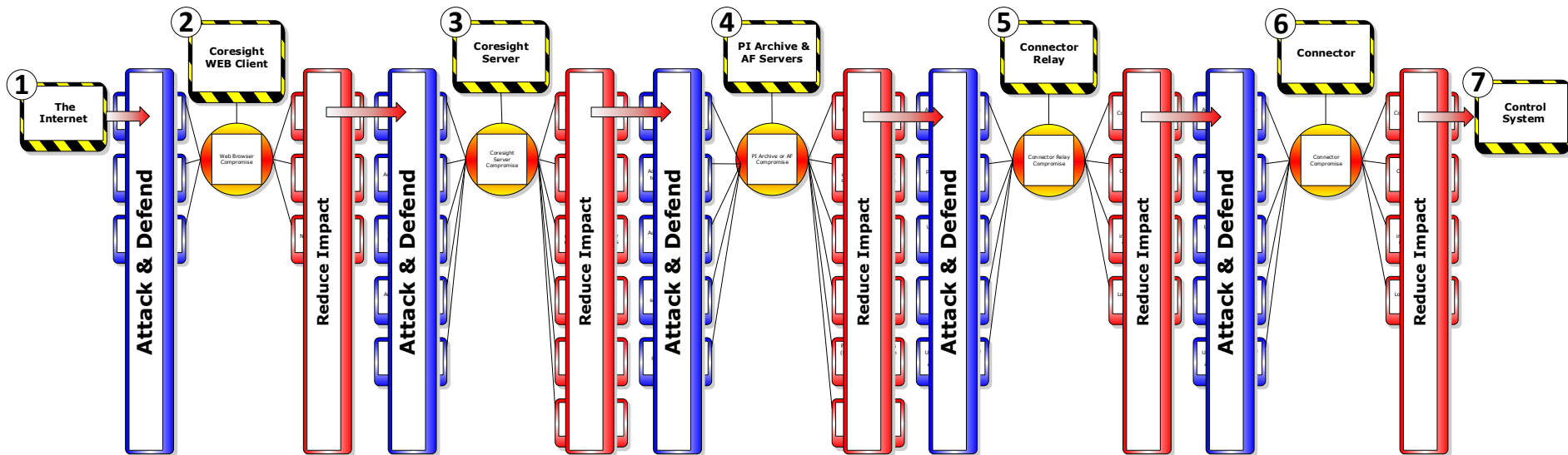


# PI System Connector



# PI System Kill Chain with Relay

- Latest defensive technology
- More separation from threat to target
- Flexible and defensible architecture





# “Infrastructure Hardened” PI System

Global. Trusted. Sustainable.

# What is “Infrastructure Hardened”?

- Extremely Reliable
  - Well Tested
  - Proven Capability
- “Trusted”



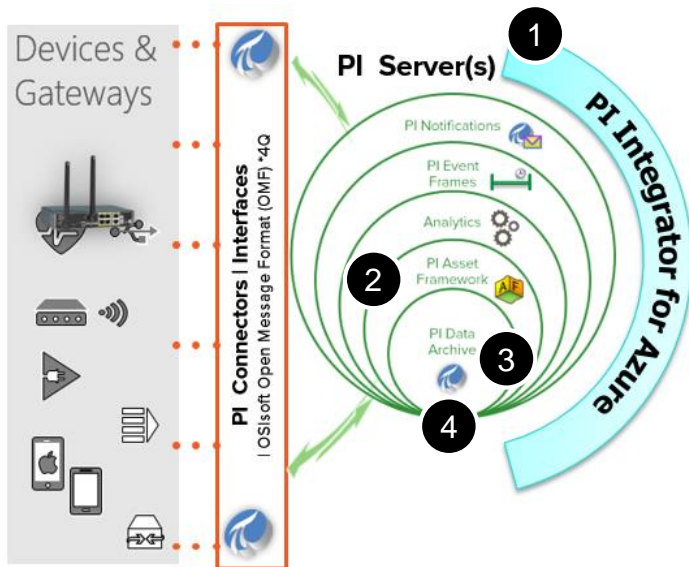
## Security Development Lifecycle Process







# Microsoft Project Springfield Early Adopter



**1** Resists pathological PI SQL data queries

**2** Safe import and export of AF asset structures

**3** Robust support for intensive bulk data calls

**4** Reliable access to archive data



# Key PI System Security Resources

<https://techsupport.osisoft.com/Troubleshooting/PI-System-Cyber-Security>

The image displays three overlapping browser windows showcasing OSiSoft's security resources:

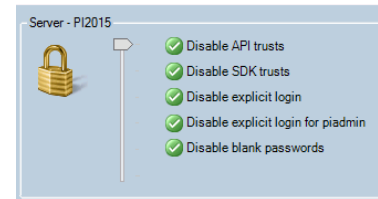
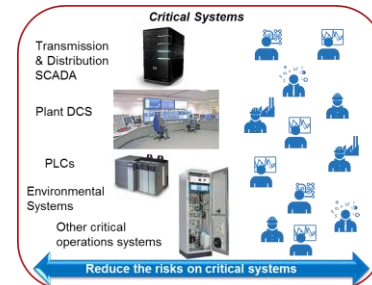
- Top Left Window:** The "PI System Cyber Security" page on [techsupport.osisoft.com](https://techsupport.osisoft.com). It features a navigation bar with "OSiSoft Home", "PI Square Community", "Learning", and "Live Library". The main content area is titled "PI System Cyber Security" and includes a table of resources.
- Top Right Window:** The "Security | PI Square" group page on [pisquare.osisoft.com/groups/security](https://pisquare.osisoft.com/groups/security). It shows the "PI Square" logo and navigation tabs for "Home", "News", "Spaces", "People", "Ideas", and "Content". The group page includes sections for "LINKS", "WELCOME TO THE OSISOFT SECURITY GROUP!", "FEATURED CONTENT", "ASK SECURITY", and "UPCOMING EVENTS".
- Bottom Window:** A YouTube channel page for "OSiSoft Learning" with the title "Configure PI Server Security". It lists several videos related to PI system security, including "OSiSoft: What are PI Identities, Mappings, & Trusts?", "OSiSoft: PI Data Archive Security Deep Dive Map- Security Areas, Defaults, & Customization", and "OSiSoft: Configure Overall PI Data Archive Security for Users & SDK Applications".

<https://www.youtube.com/user/OSiSoftLearning/>

<https://pisquare.osisoft.com/groups/security>

# Actions

- Defend your critical systems
- Establish an update cadence
- Take advantage of integrated security



# Contact Information



## **Brian Bostwick**

[Brian@OSIsoft.com](mailto:Brian@OSIsoft.com)

Market Principal, Cyber Security

## **Bryan Owen PE**

[Bryan@OSIsoft.com](mailto:Bryan@OSIsoft.com)

Principal Cyber Security Manager

# Thank You



**OSI**soft®