What's New in PI Security?

Presented by **Bryan Owen PE**

Felicia Mohan

BERLIN SEPT 26-29 GERMANY

OSIsoft.

EMEA USERS CONFERENCE

BERLIN, GERMANY • SEPT 26-29, 2016

Agenda

- Overview
- What’s new
- Demo
- What’s coming next
- Call to Action

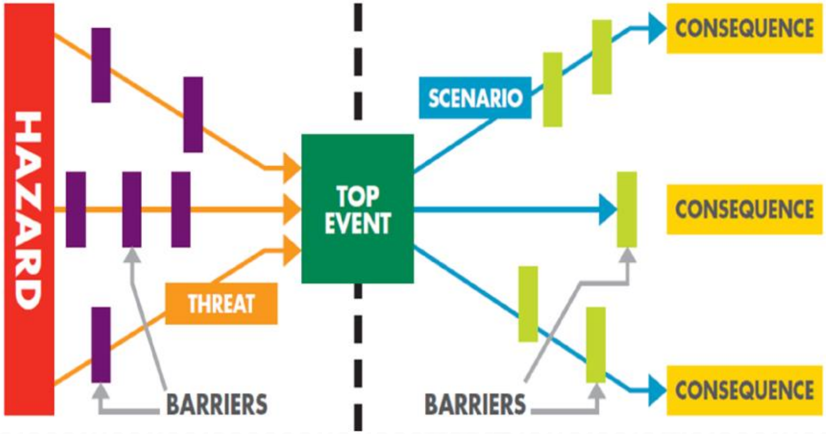
Cyber Security is more of a Marathon than a Sprint

- 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

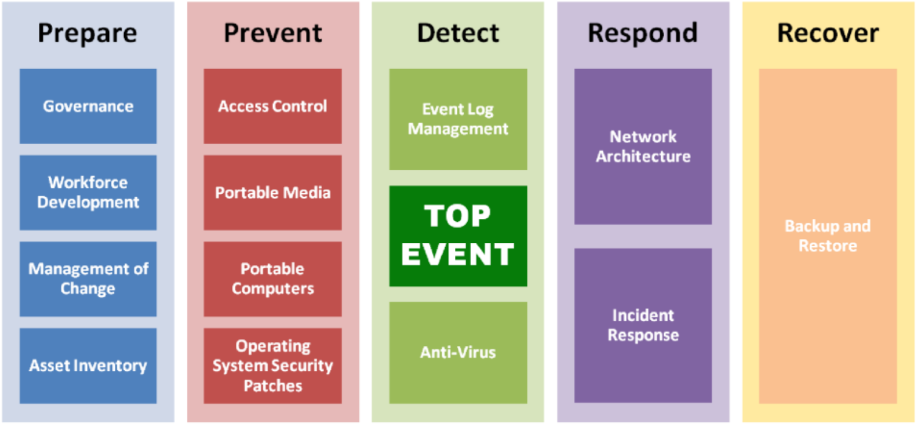
Best Practices are Advancing

Engineering Bow-Tie Model



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

ICS Security Bow-Tie



Prepare
- Governance
- Workforce Development
- Management of Change
- Asset Inventory

Prevent
- Access Control
- Portable Media
- Portable Computers
- Operating System Security Patches

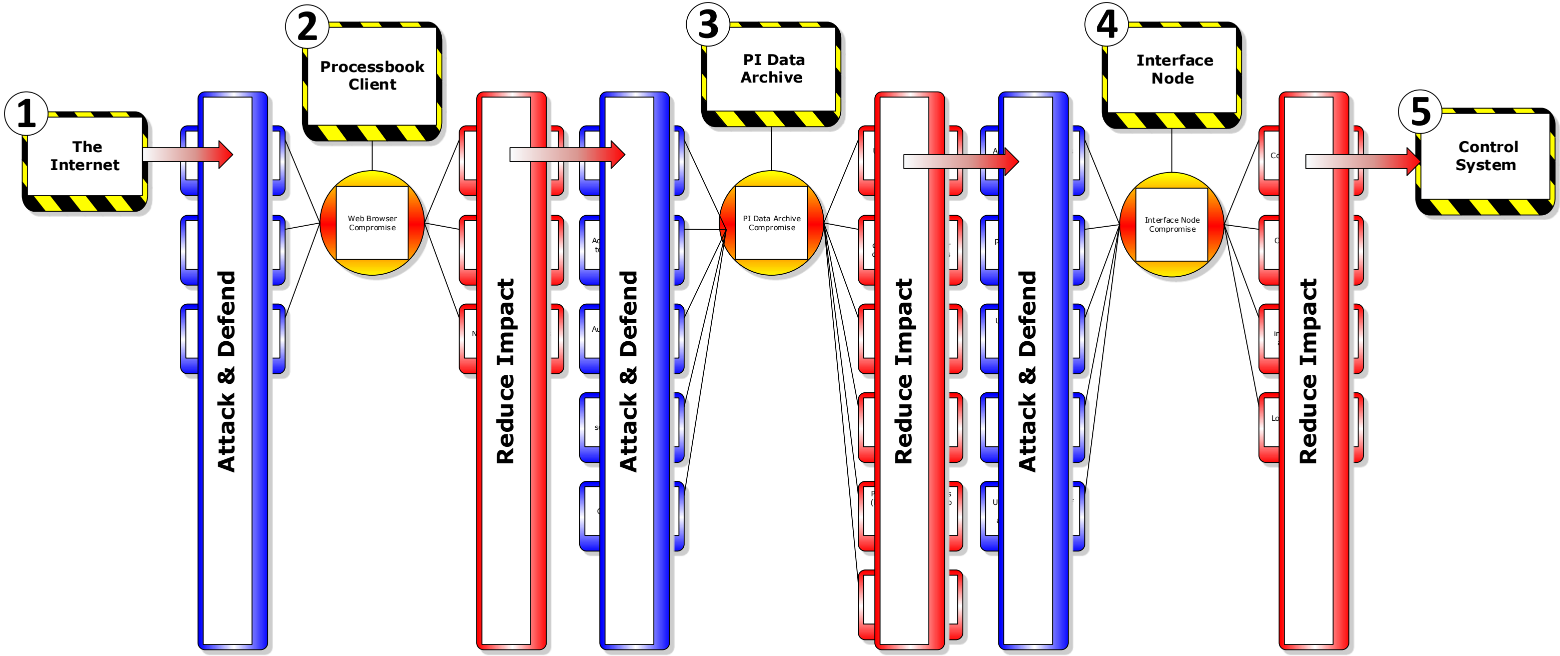
Detect
- Event Log Management
- TOP EVENT
- Anti-Virus

Respond
- Network Architecture
- Incident Response

Recover
- Backup and Restore

Classic PI System Kill Chain

- Many opportunities to defend
- Attacks are complex
- Successful attacks require high skill levels



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

Deep Dive into Security Changes

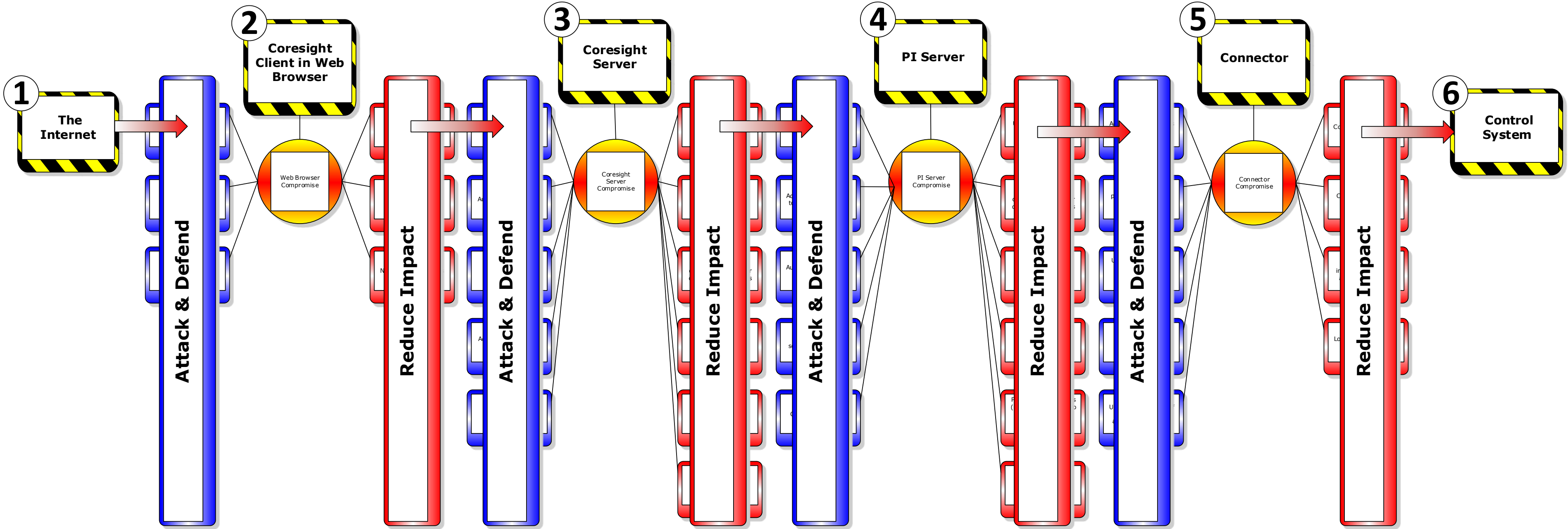
Classic PI Client Desktop

- 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

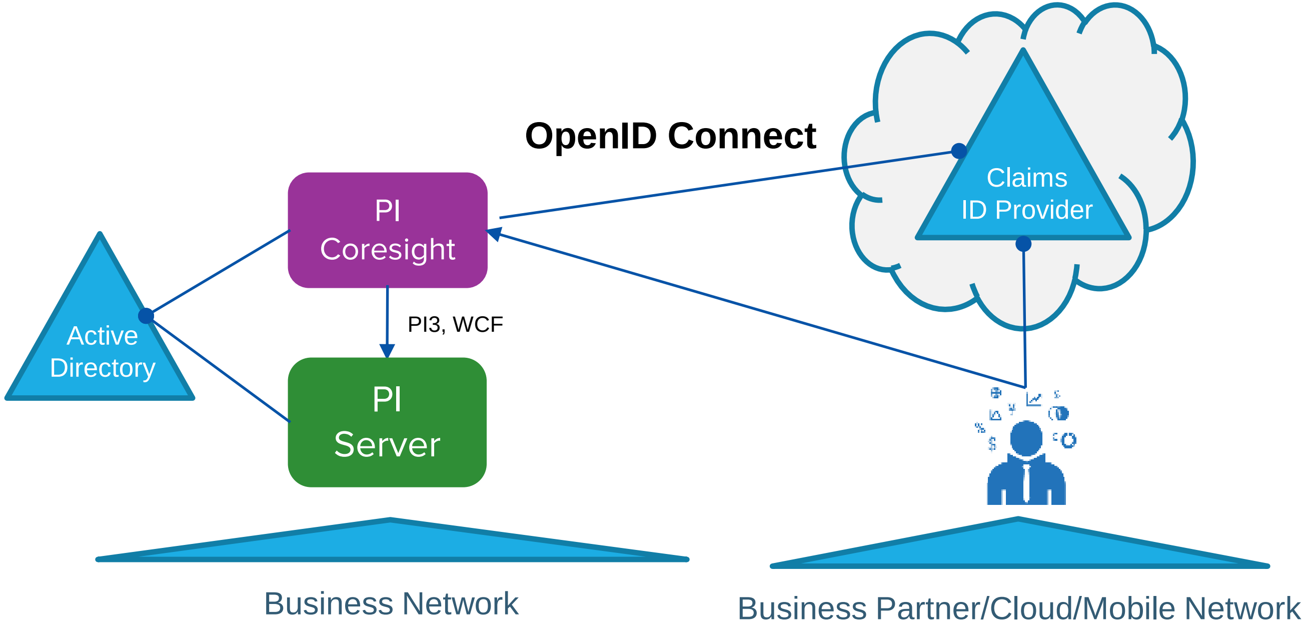
- Newer more secure development technologies
- Attack complexity Increased by additional layer
- Successful attacks require high skill levels



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

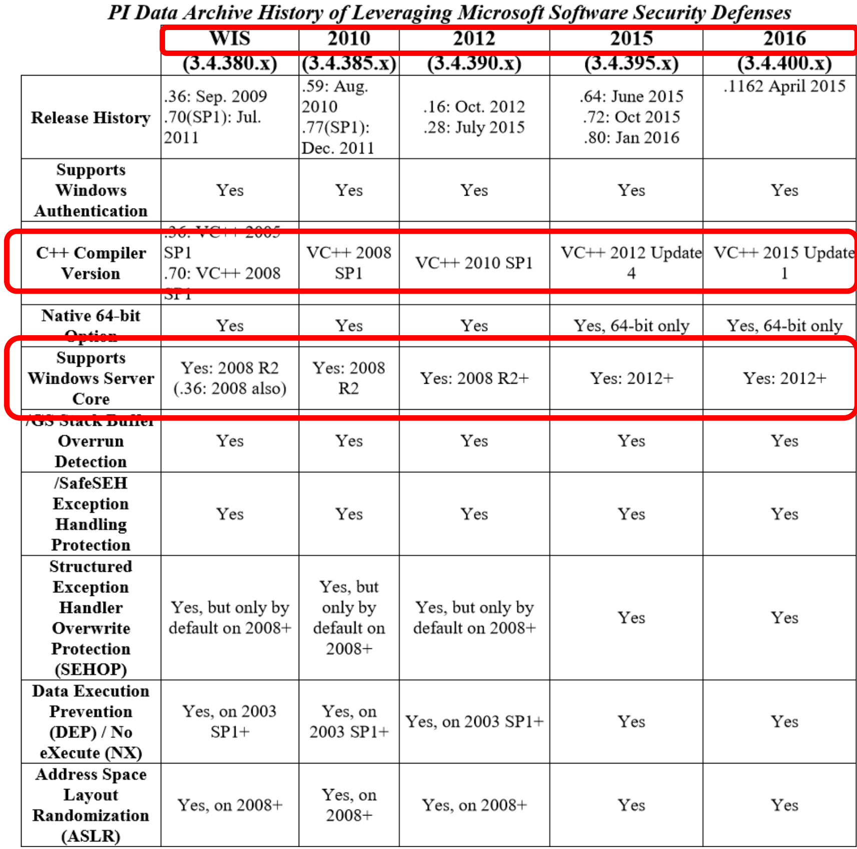
- 2015
  - Identity Mappings
  - Service Hardening
  - AF Client to Data Archive Transport Security
- 2016
  - IsManualDataEntry
  - Annotate Permission
  - File Attachment Checks

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



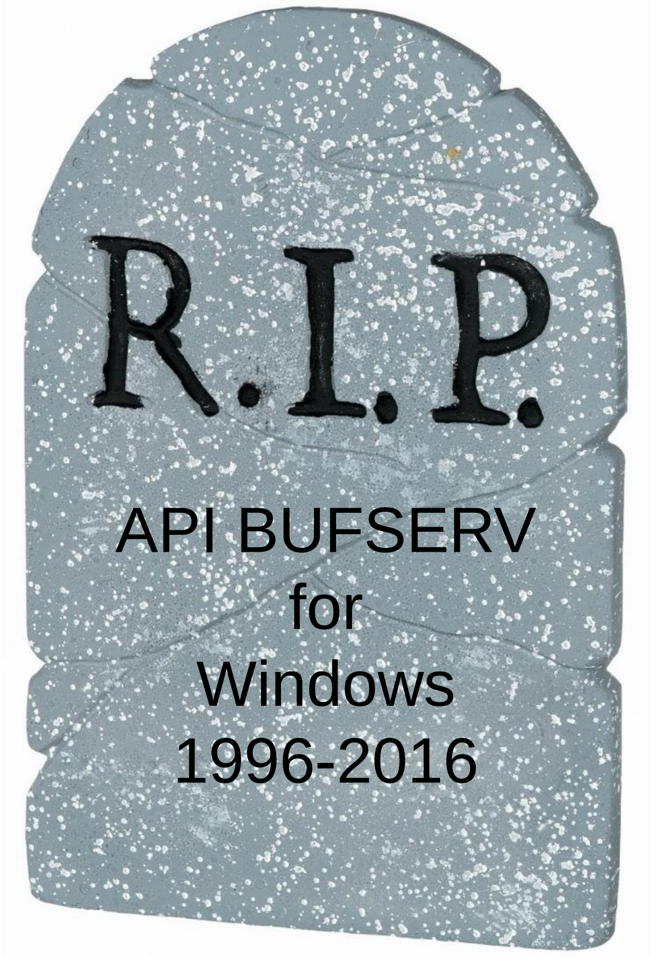
PI Data Archive History of Leveraging Microsoft Software Security Defenses

	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	.36: 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+
/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

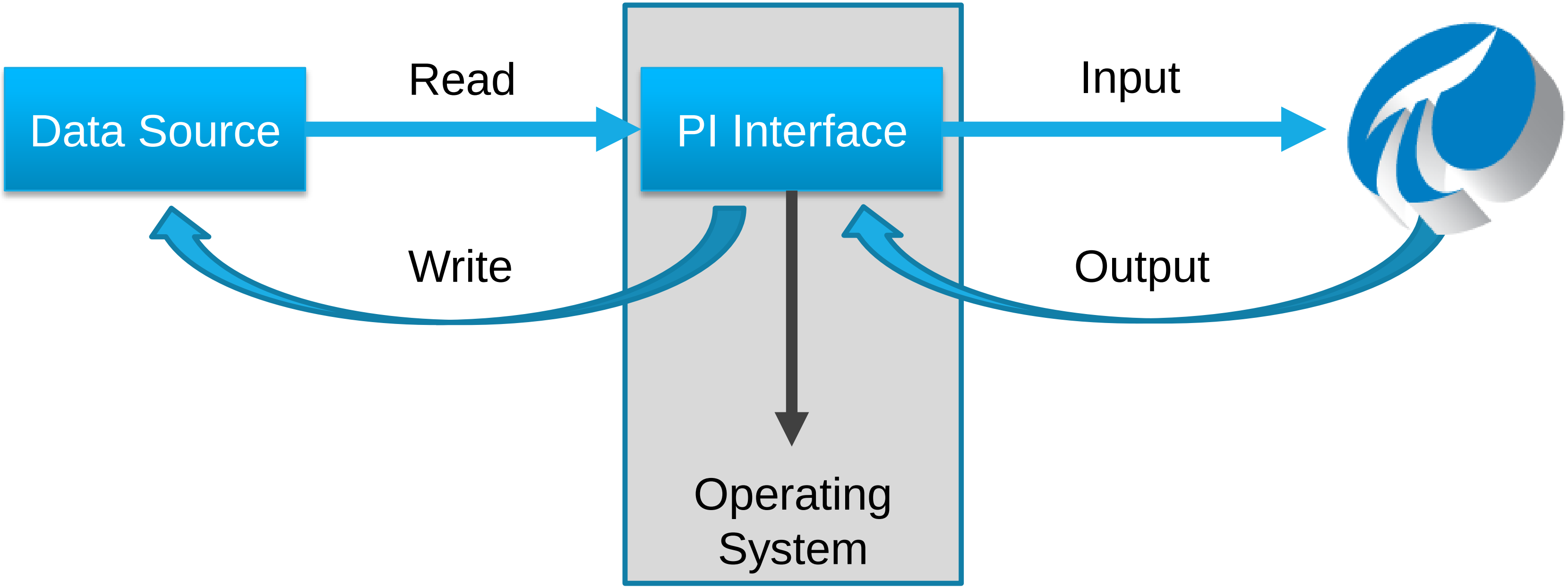
Security Changes for PI System Interfaces

PI Buffer Subsystem

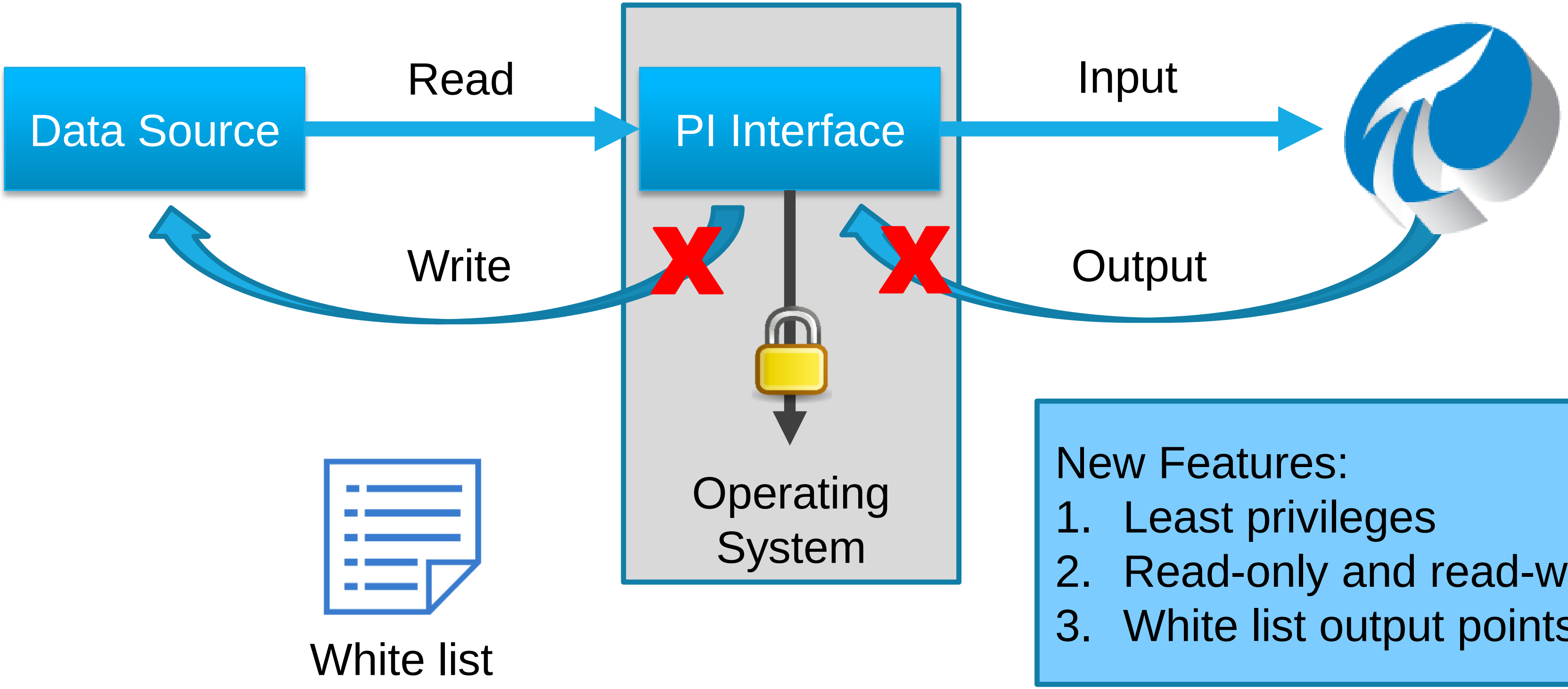
- 2015
  - Code Safety
  - Transport Security with Windows Authentication
- 2016
  - Service Accounts
    - Managed Service Account (Domain only)
    - Virtual Service Account



PI Interfaces – New options for securing



PI Interfaces – New options for securing



New Features:

1. Least privileges
2. Read-only and read-write
3. White list output points

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)	

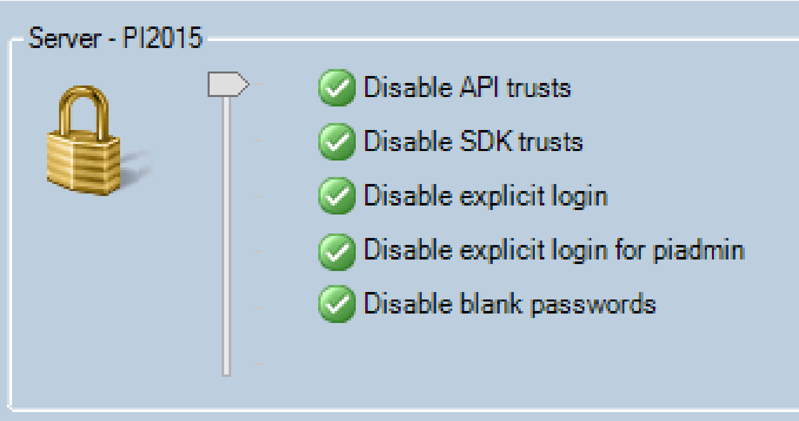
Transport Security Everywhere

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



Server - PI2015

✓ Disable API trusts

✓ Disable SDK trusts

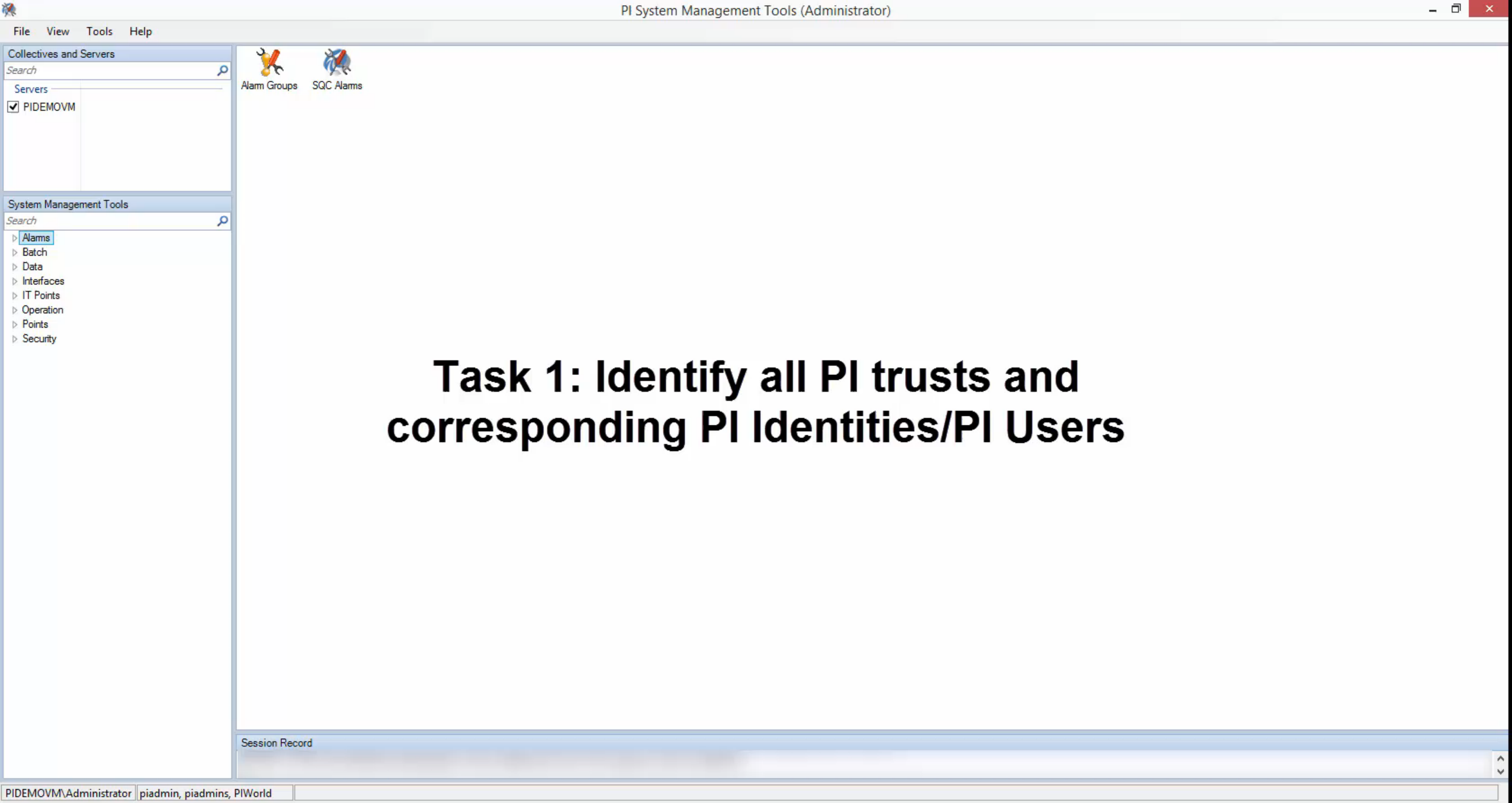
✓ Disable explicit login

✓ Disable explicit login for piadmin

✓ Disable blank passwords

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

DEMO

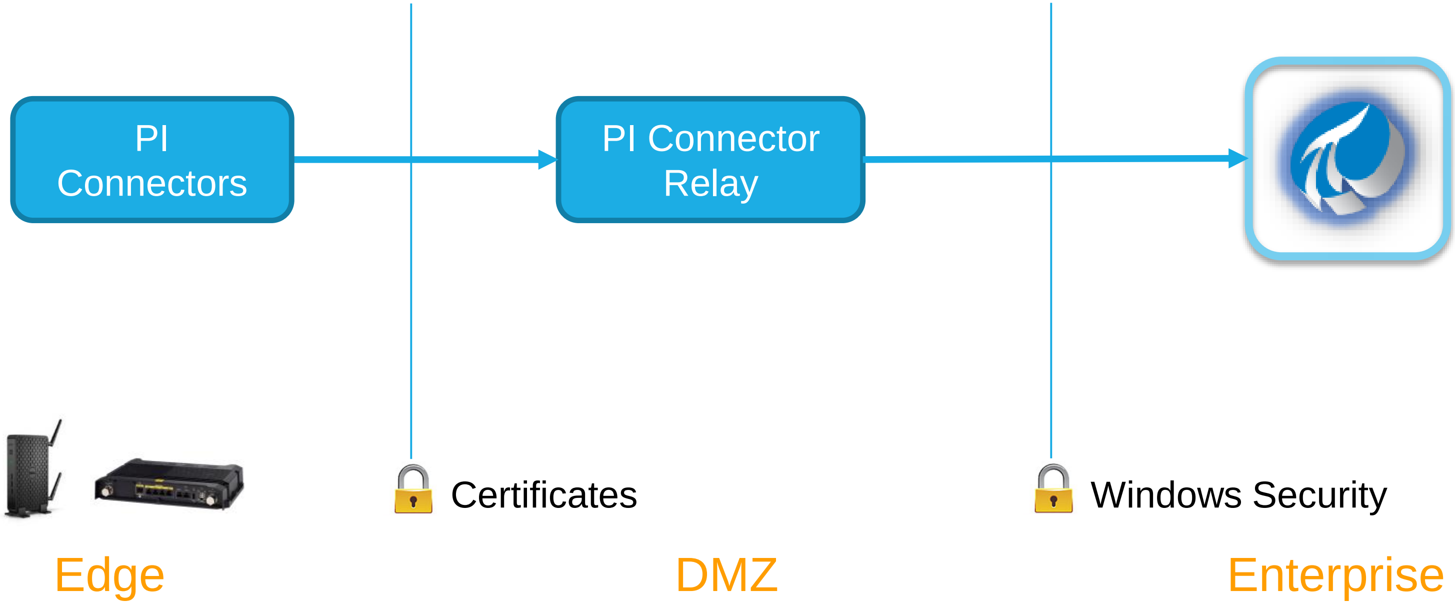


PIDEMOVM\Administrator | piadmin, piadmins, PIWorld

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

Security Changes in Progress

PI Connector Architecture



PI Connectors

PI Connector Relay

Certificates

Windows Security

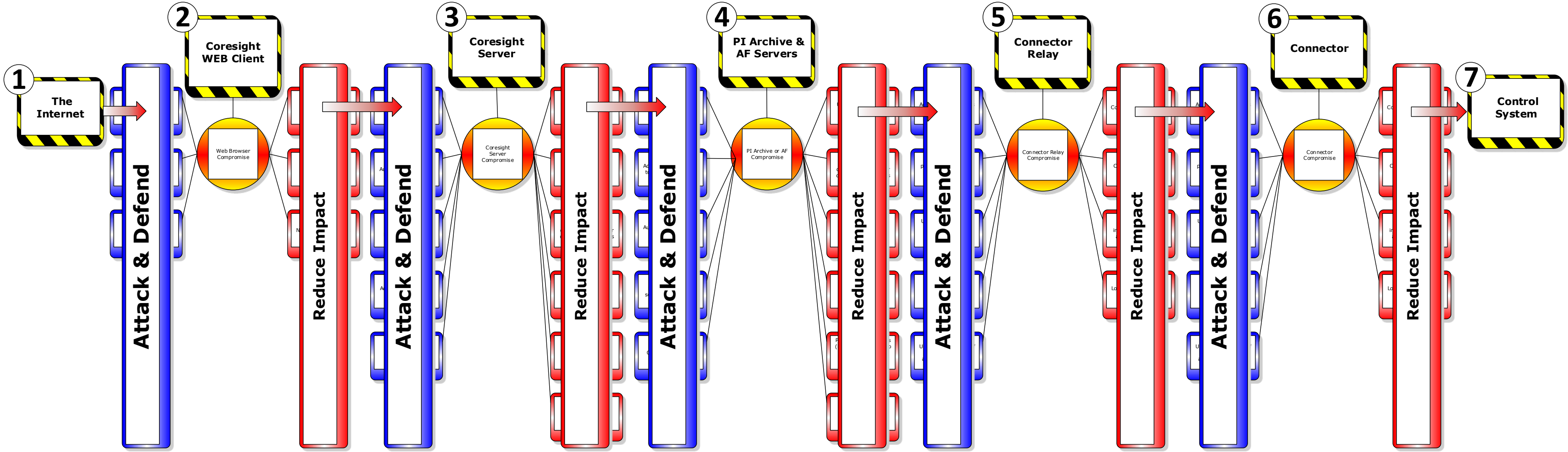
Edge

DMZ

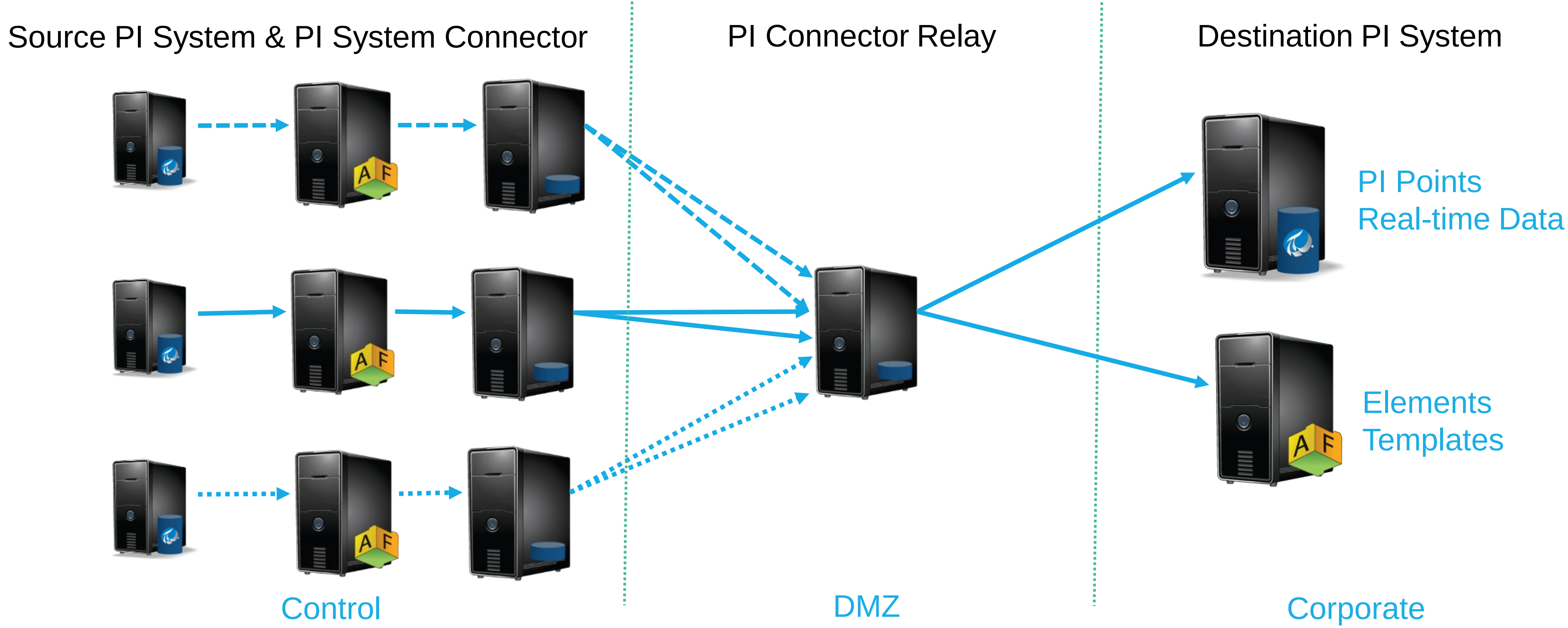
Enterprise

PI System Kill Chain with Relay

- Enhanced development technologies
- Attack complexity Increased by additional layer
- Successful attacks require high skill levels



PI System Connector



Call to Action

- Plan roll out for PI SDK 2016 and PI API 2016
- Update PI Buffering and PI Interfaces too
- Get started with PI Connectors

enisa
European Network
and Information
Security Agency

Under the NIS Directive, essential service providers must adopt requirements within 21 months of August 2016 or **face fines of up to €10m or 2% globally**.

Contact Information

Bryan Owen

bryan@osisoft.com

Principal Cyber Security Manager

Felicia Mohan

ftan@osisoft.com

Systems Engineer

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 EMEA Users Conference 2016

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

search **OSISOFT** in the app store

http://ddut.ch/osisoft

감사합니다

謝謝

Danke

Merci

Gracias

Thank You

ありがとう

Спасибо

Obrigado

BERLIN
SEPT 26-29
GERMANY

OSIsoft

EMEA USERS CONFERENCE

BERLIN, GERMANY • SEPT 26-29, 2016