



Cyber Security

Presented by **Brian Bostwick**
OSIsoft Market Principal for Cyber Security

eSecurity Planet

2 US Power Plants affected with Malware

In both cases the malware was delivered with a USB drive.
January 16, 2013

By Jeff Goldman, eSecurityPlanet.com

InformationWeek

Saudi Aramco Restores Network After Shamoon Malware Attack

Hackivist-launched virus takes out 75% of state-owned oil company's workstations, signals the growing power of attackers with social or political agendas.



DHS warns Siemens 'flaw' could allow power plant hack

The U.S. Department of Homeland Security is probing Siemens' technology that may allow hackers to attack critical

Krebs on Security
In-depth security news and analysis

Chinese Hackers Blame Energy Industry Giant

A company whose software remotely administer and monitor energy industry began warning investigating a sophisticated operations in the United States



Confirmation of a Coordinated Attack on the Ukrainian Power Grid

After analyzing the information that has been made available by affected power companies, researchers, and the media it is clear that cyber attacks were directly responsible for power outages in Ukraine.

Michael J. Assante, January 9, 2016

BBC NEWS
TECHNOLOGY

Hack attack causes 'massive damage' at steel works

[T]hey showed familiarity with both conventional IT security systems but also the specialized software used to oversee and administer the plant.
December 22, 2014



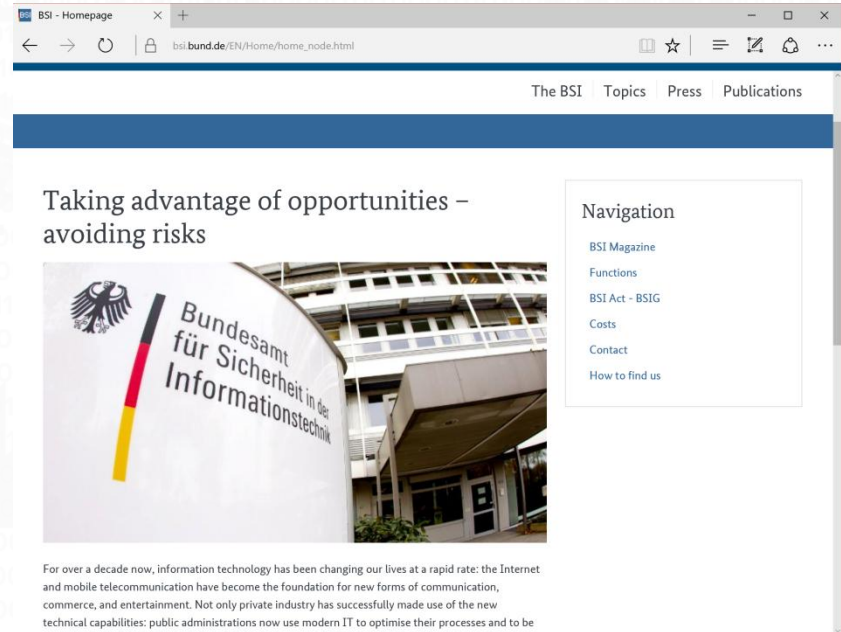
OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC

BSI Top Threats

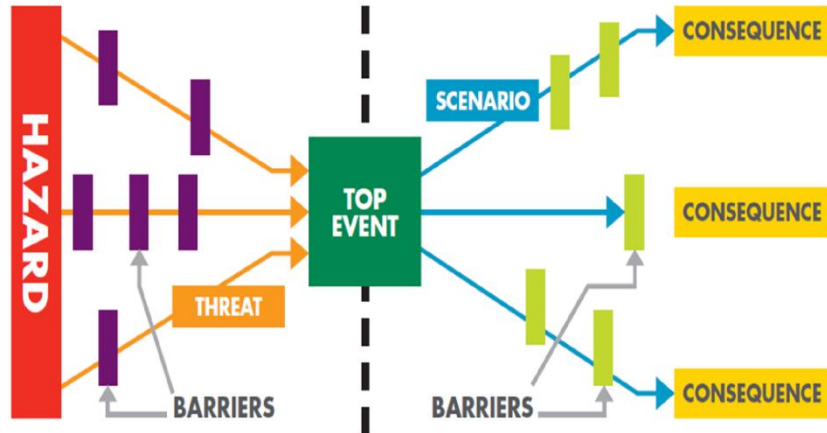
- Threats against humans
Social Engineering, USB devices, accidents
- Boundary exploits
Exploits of internet facing systems, remote access, critical systems, cloud apps
- Internal threats
Old systems and software, DDoS attacks, Smartphones



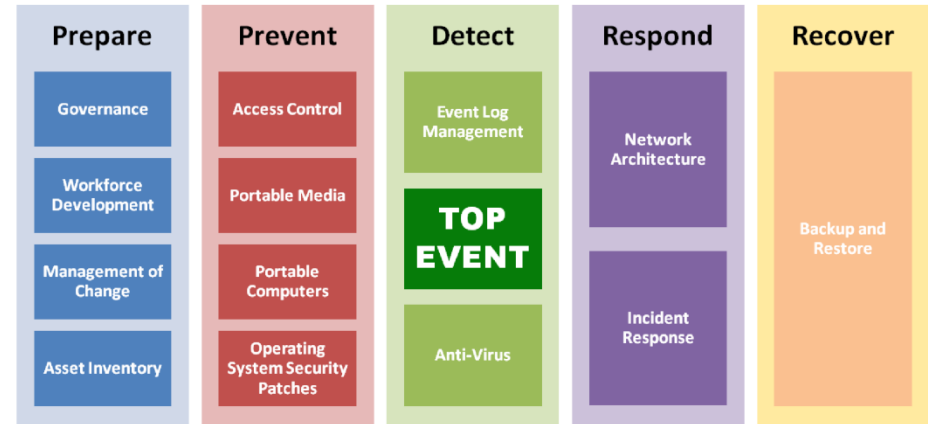
Federal Office for Information Security

Bow Tie Diagrams: Introduced by Shell

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>



OSIsoft.

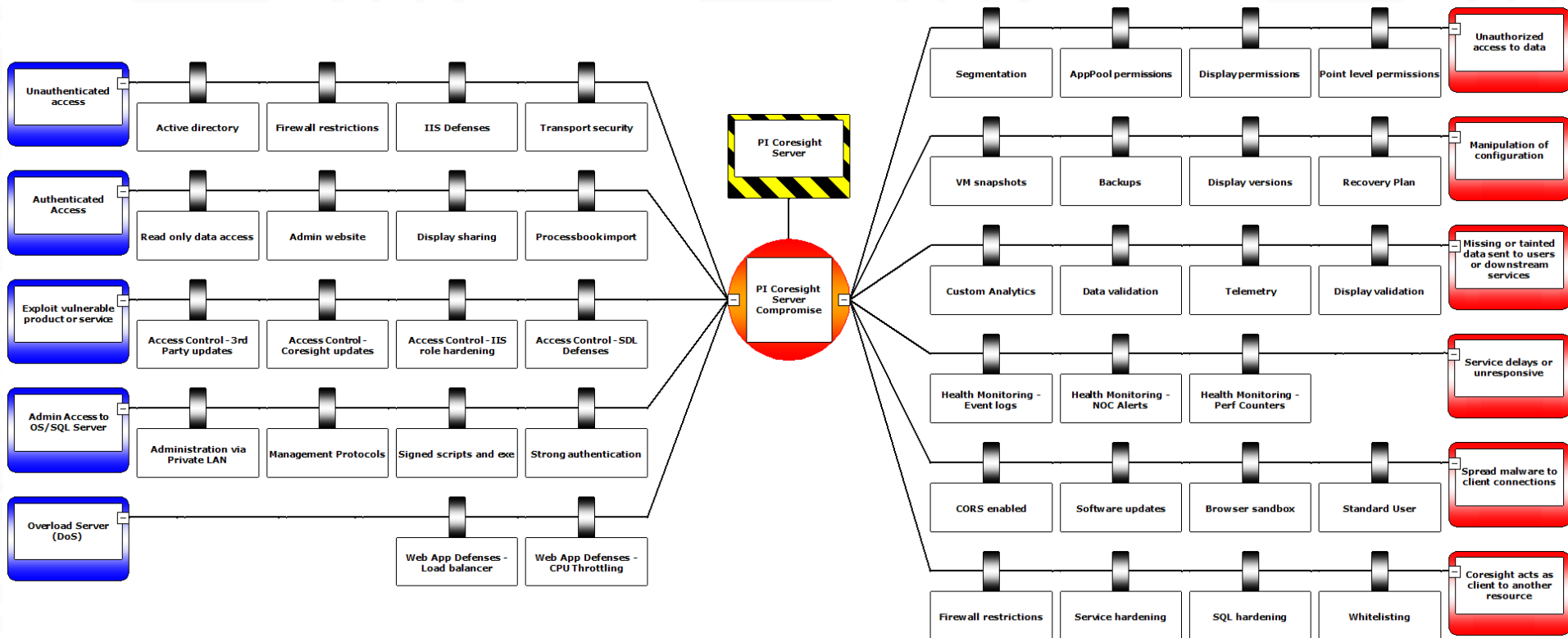
EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC

Attacks & Defenses

Point of Analysis

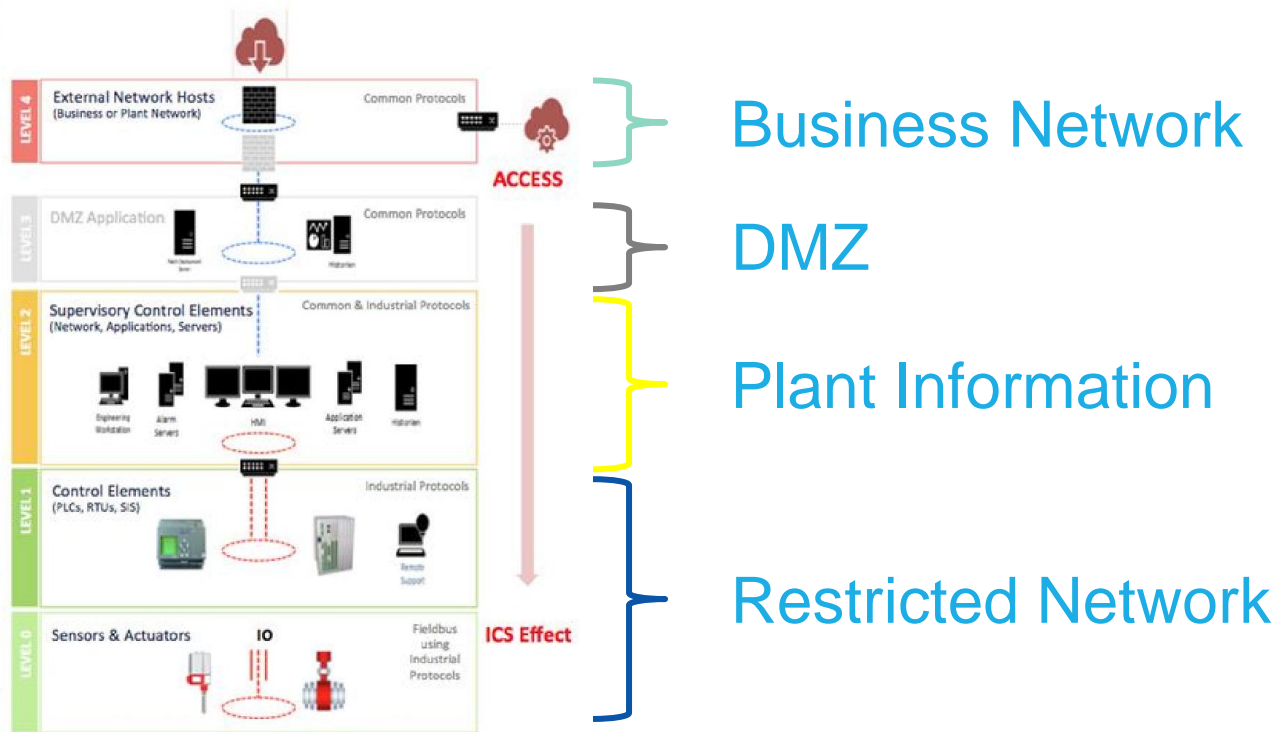
Impacts & Reductions



Keep the bad guys out

But if they get in, limit the damage

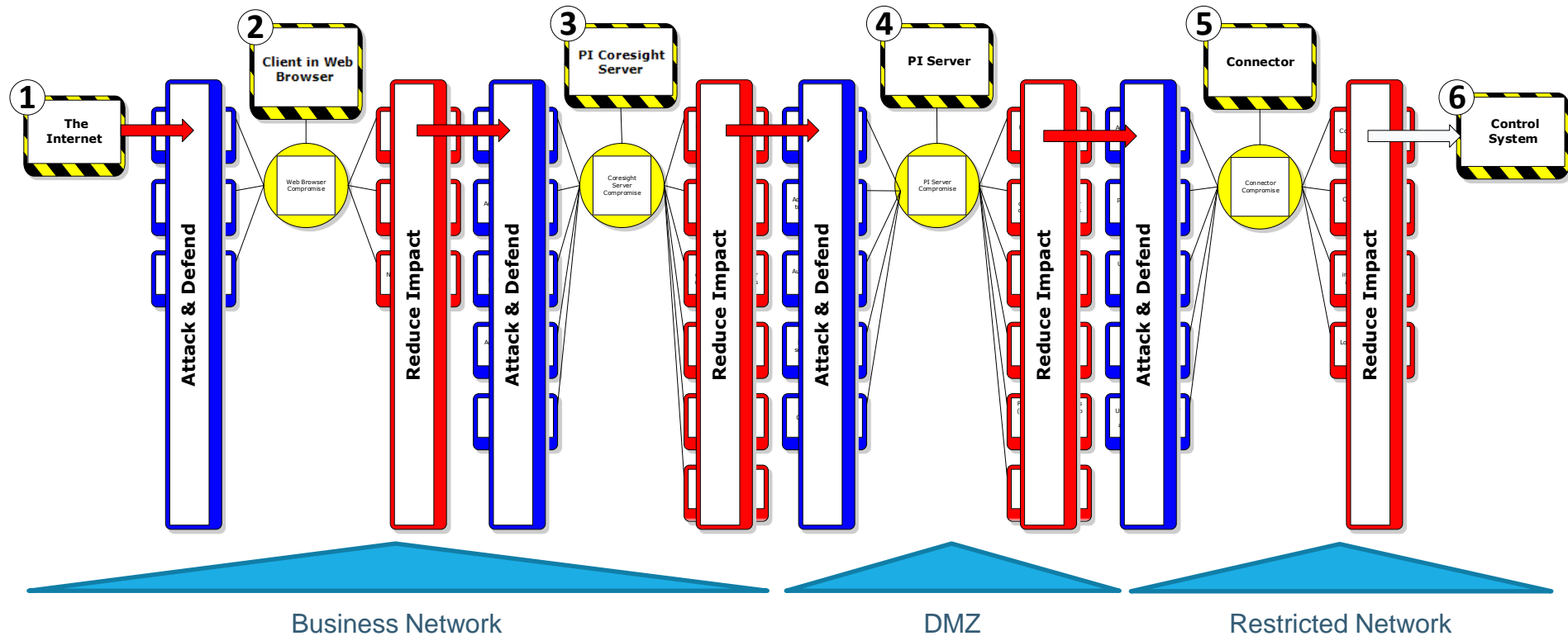
Ukraine Power: ICS Cyber Kill Chain Mapping



[Analysis of the cyber attack on the Ukraine Power Grid, SANS.org](#)

Modern PI System Kill Chain

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



OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC

Top Three DHS ICS-CERT Weaknesses

1. Boundary Protection:

Poor architecture including ICS discoverable on the internet

2. Least Functionality:

Unnecessary open ports

3. Authenticator Management:

Simple passwords and lack of encryption



Industrial Control Systems Assessment Summary Report FY 2015

1. Boundary Protection

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.

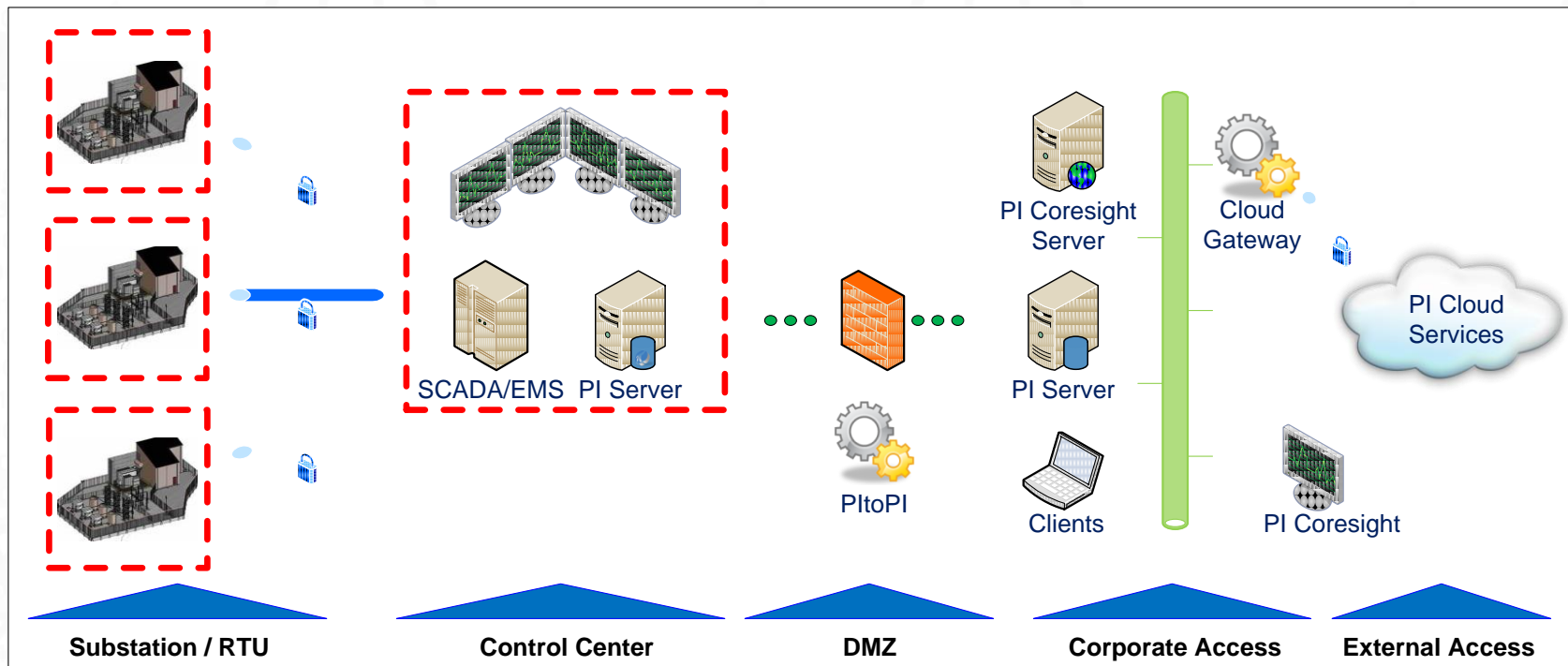


Security Perimeter



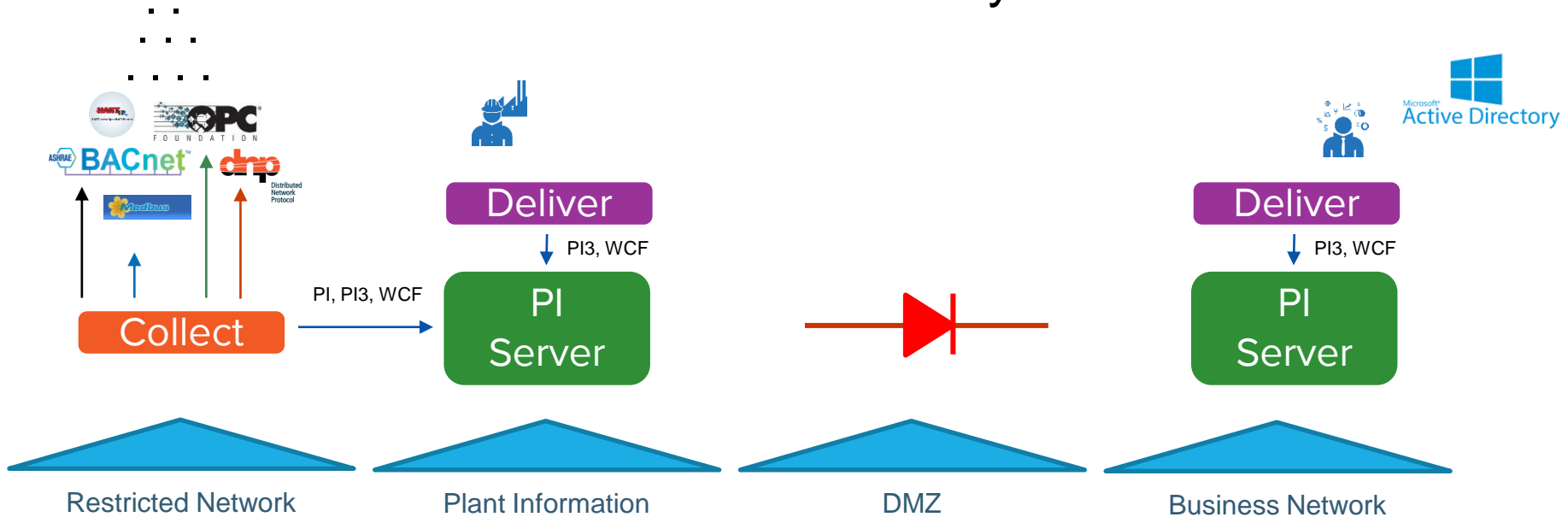
Reduce the risks on critical systems

1. Boundary Protection: PI – to – PI



1. Boundary Protection: Data Diode Partners

- Separation of access for operation and business user
- Absolute enforcement with one-way data flow

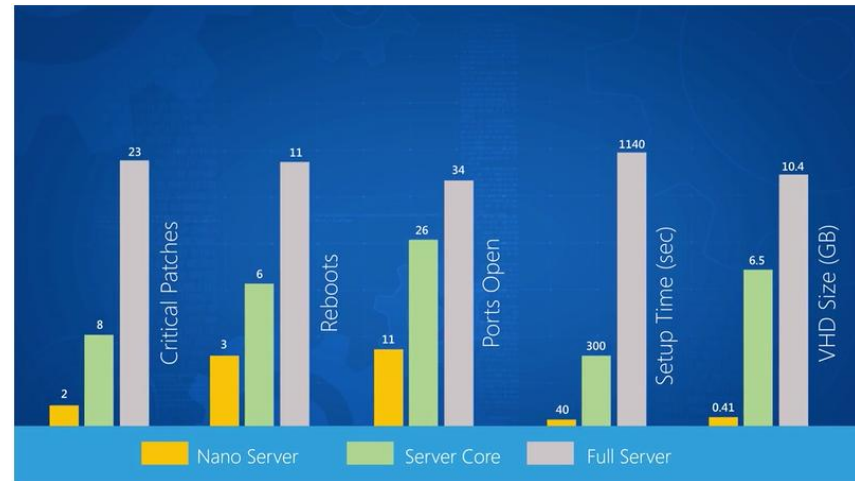


2. Least Functionality

PI Server – Certified for Windows Server Core

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

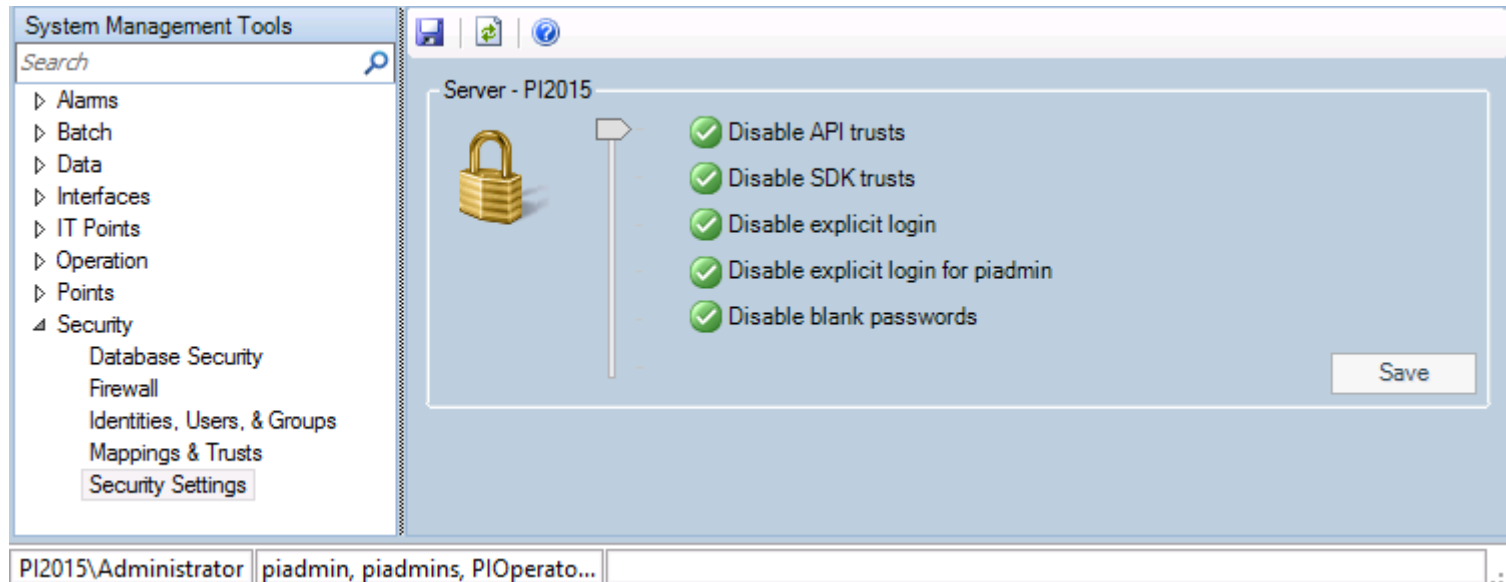
.... More Secure



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

3. Authentication Management

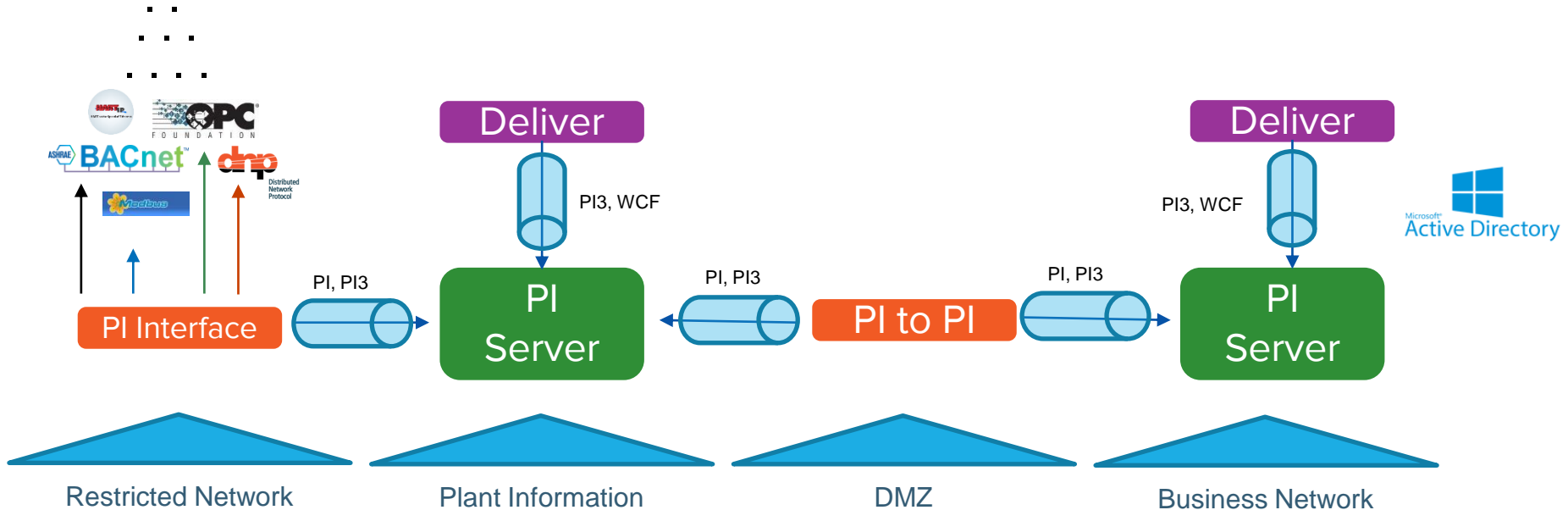
Use Windows Integrated Security (WIS)



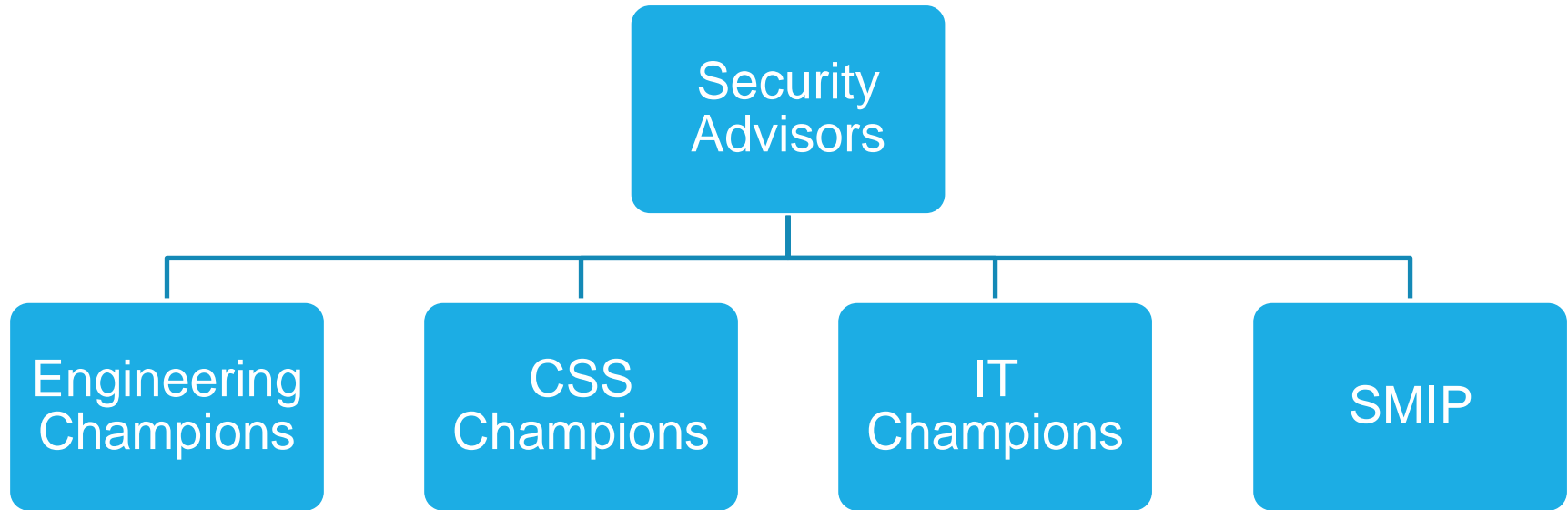
3. Authentication Management: The Modern PI System

Using Windows Integrated Security -

- PI System communication is encrypted by default
- PI Interfaces are configurable with transport security



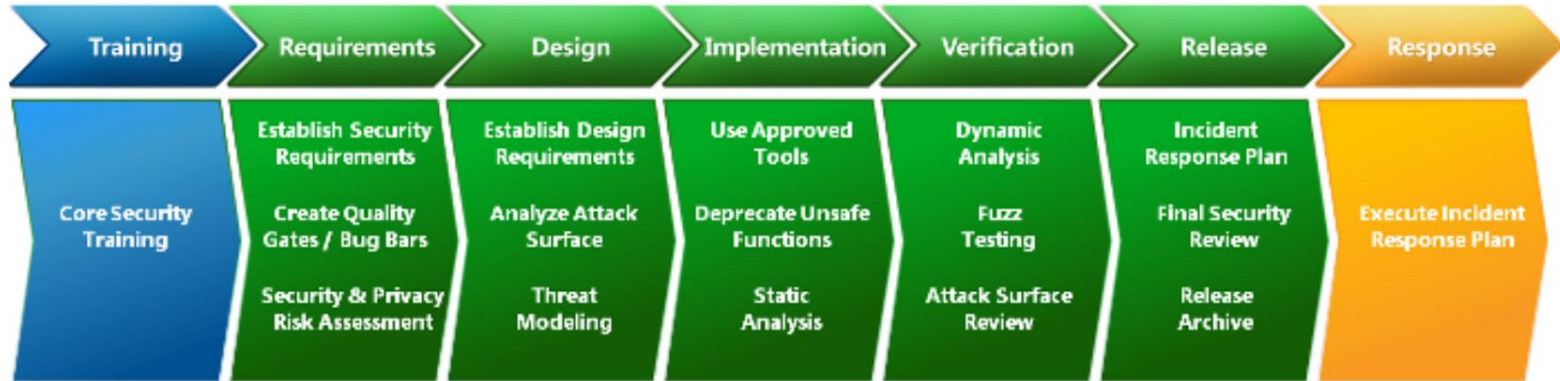
Work in Security is Ongoing



secure@osisoft.com

OSIsoft Security Development Lifecycle

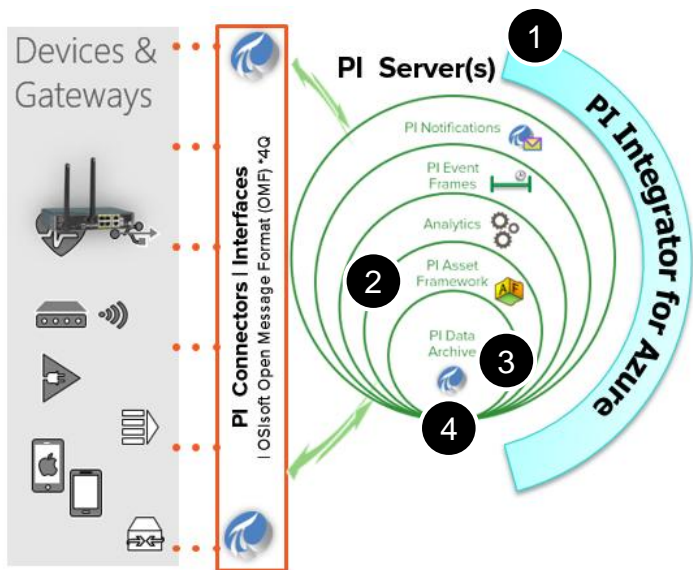
Microsoft SDL model



Note

- Video replay has been removed to keep download size down. See the video on the replay for this conference session at osisoft.com > About OSIsoft > Presentations.

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 collage displays three overlapping web browser windows:

- Top-left window:** Shows the "PI System Cyber Security" page on [techsupport.osisoft.com](https://techsupport.osisoft.com/Troubleshooting/PI-System-Cyber-Security). It features a table with links to documentation, security advisories, and technical articles related to mitigating security risks.
- Top-right window:** Shows the "Security | PI Square" group page on [pisure.osisoft.com](https://pisure.osisoft.com/groups/security). It includes a welcome message, a list of links (Ethical Disclosure Policy, PI Security Tech Support), featured content (Bow Tie for Cyber Security), and upcoming events (OSiSoft EMEA Users Conference 2016).
- Bottom window:** Shows a YouTube playlist titled "Configure PI Server Security" by OSiSoftLearning. The playlist contains five videos, including "OSiSoft: What are PI Identities, Mappings, & Trusts? (High Level PI Server Security Map)" and "OSiSoft: PI Data Archive Security Deep Dive Map- Security Areas, Defaults, & Customization".

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

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

Actions

- Defend boundaries to critical systems by providing operational data through the PI System to business applications
- Achieve least functionality by removing unnecessary services or running on Microsoft Windows Server Core
- Manage authentication using Windows Integrated Security and encrypt all PI System messages and communication

Contact Information

Brian Bostwick

Brian@OSIsoft.com

Market Principal, Cybersecurity
OSIsoft, LLC



Please keep the conversation going....

Other OSIsoft Security talks:

“State of PI System Security and the EU NIS Directive,” Wed. 11:45-12:15

“What's New in PI Security?” Thursday, 15:45-16:15

Security Booth in the Product Expo

Questions

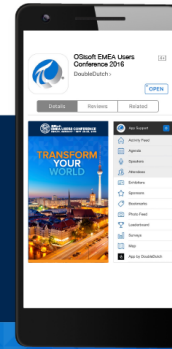
Please wait for the **microphone** before asking your questions



State your **name & company**

Please remember to...

Complete the Online Survey for this session



Download the Conference App for OSISOFT 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

谢谢

Danke

Merci

Gracias

Thank You

ありがとう

Спасибо

Obrigado



OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC



OSIsoft®

EMEA USERS CONFERENCE

BERLIN, GERMANY • SEPT 26-29, 2016



OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC