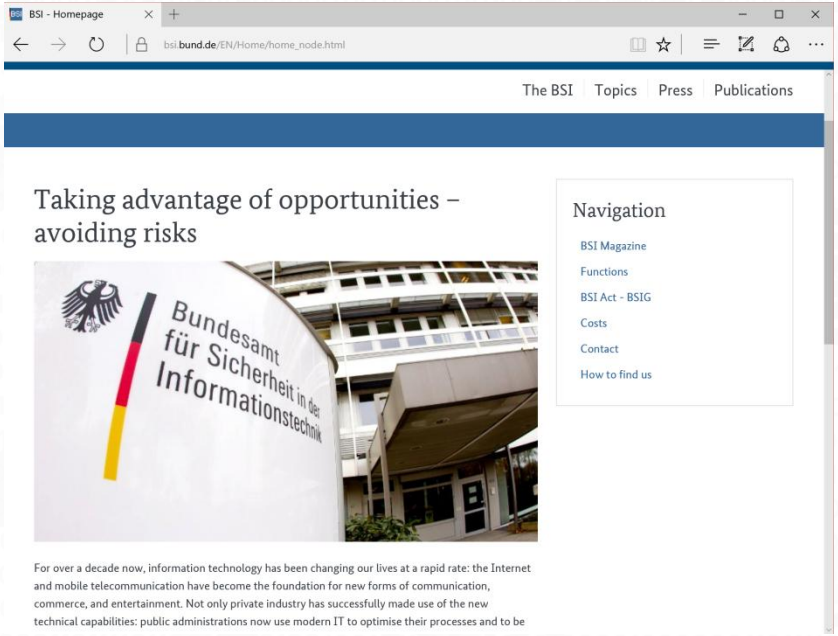
Cyber Security

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

BSI Top Threats

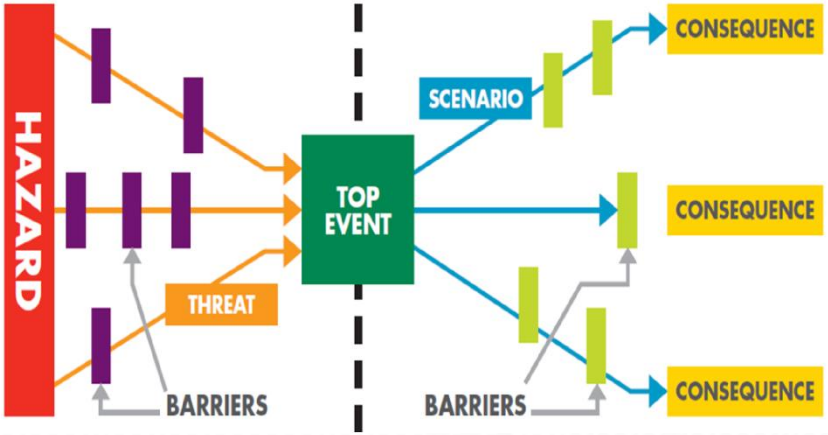
- Threats against humans
  - Social Engineering, USB devices, accidents
- Boundary exploits
  - Exploits of internet facing systems, remote access, critical systems, cloud apps
- Internal threats
  - Old systems and software, DDoS attacks, Smartphones



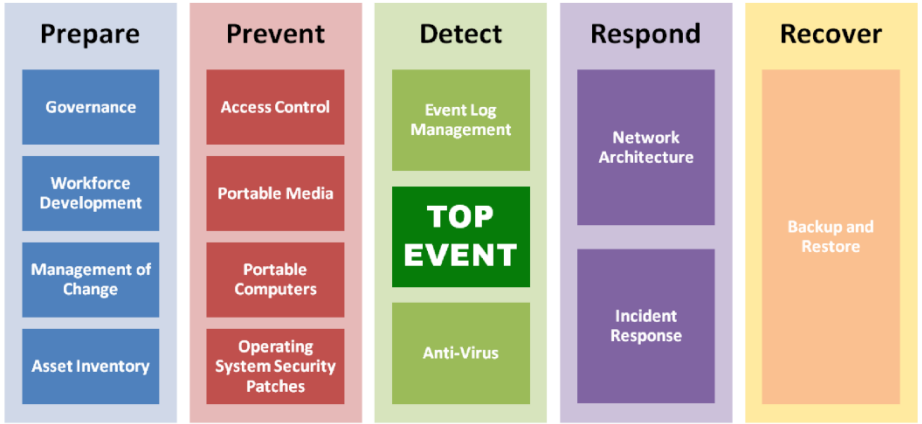
Federal Office for Information Security

Bow Tie Diagrams: Introduced by Shell

Engineering Bow-Tie Model

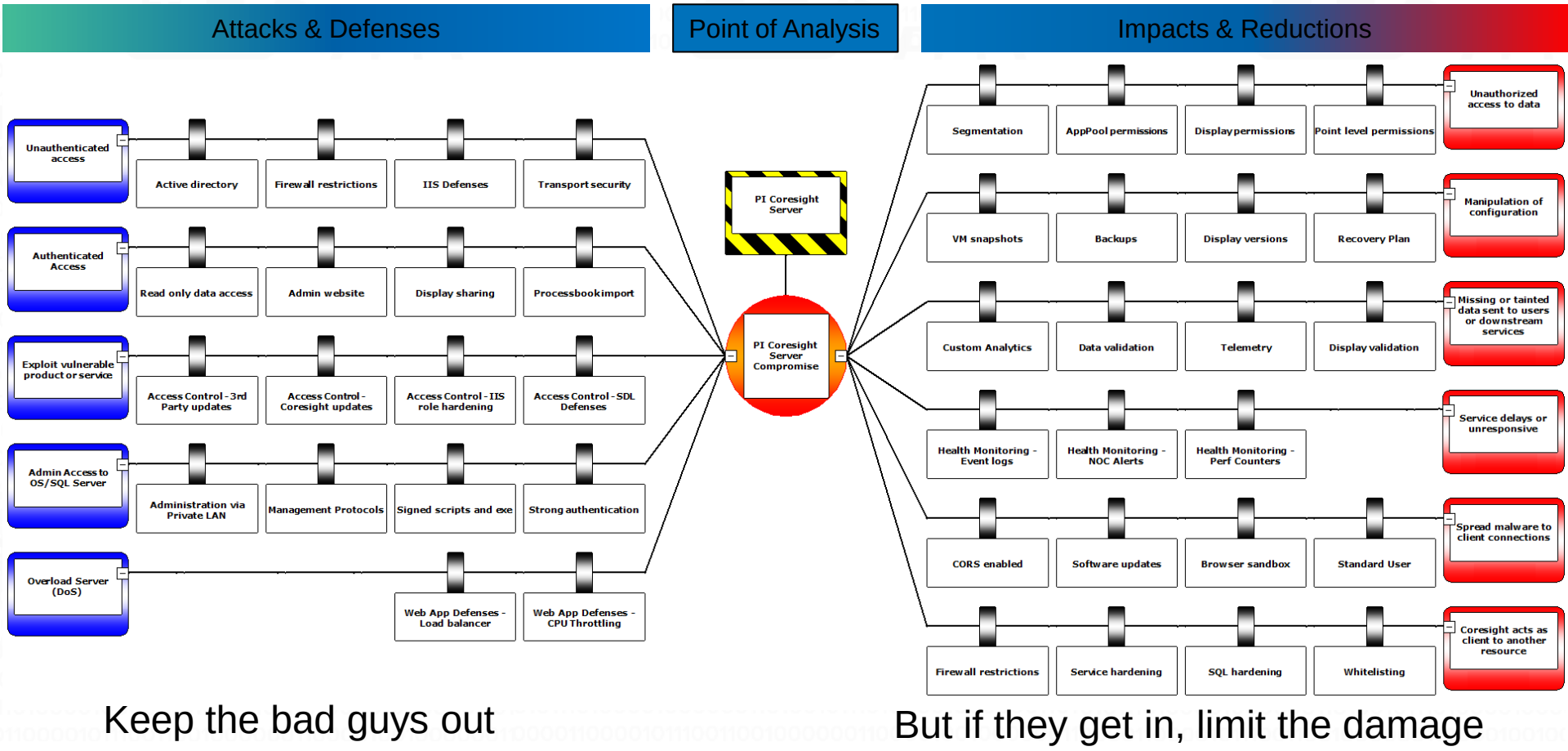


ICS Security Bow-Tie



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

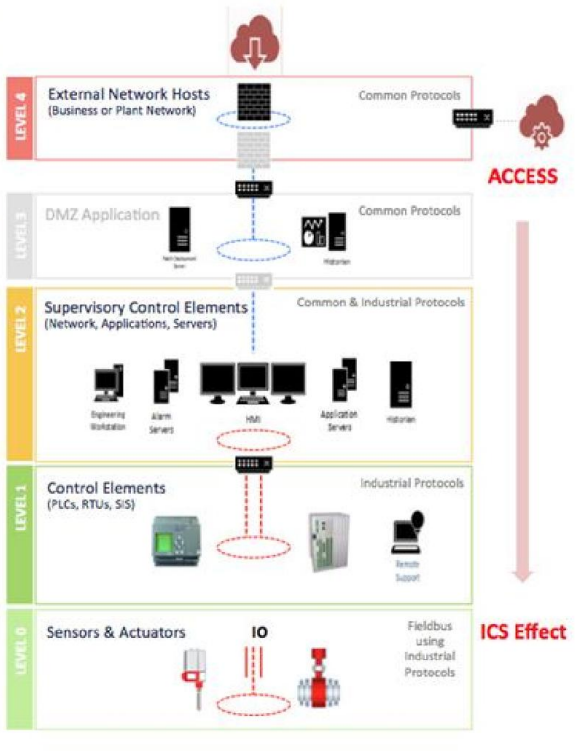
https://www.sans.org/reading-room/whitepapers/ICS/evaluating-cyber-risk-engineering-environments-proposed-framework-methodology-37017



Keep the bad guys out

But if they get in, limit the damage

Ukraine Power: ICS Cyber Kill Chain Mapping



Business Network

DMZ

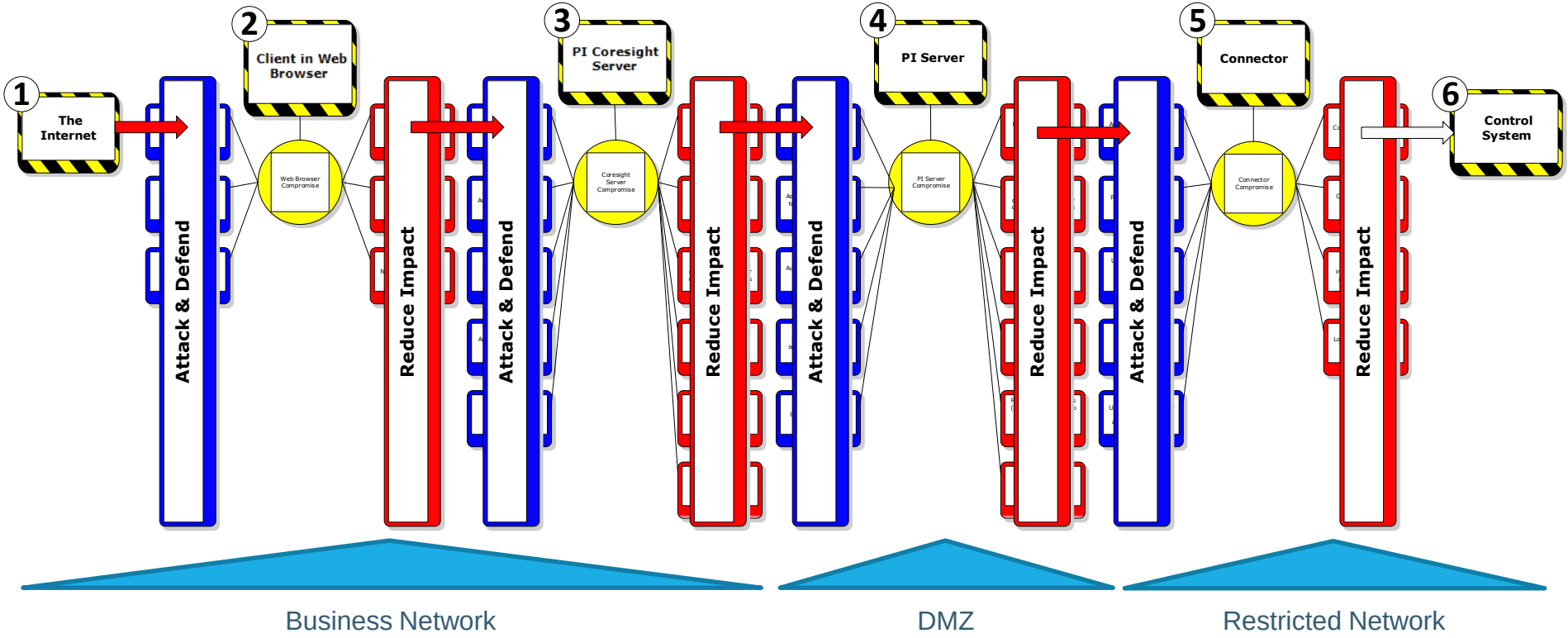
Plant Information

Restricted Network

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



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

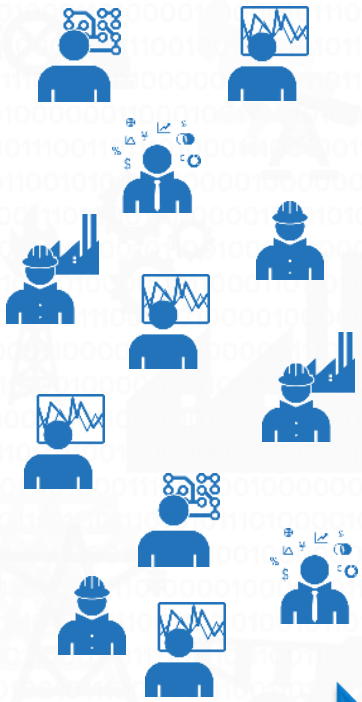
Transmission & Distribution SCADA

Plant DCS

PLCs

Environmental Systems

Other critical operations systems



Reduce the risks on critical systems

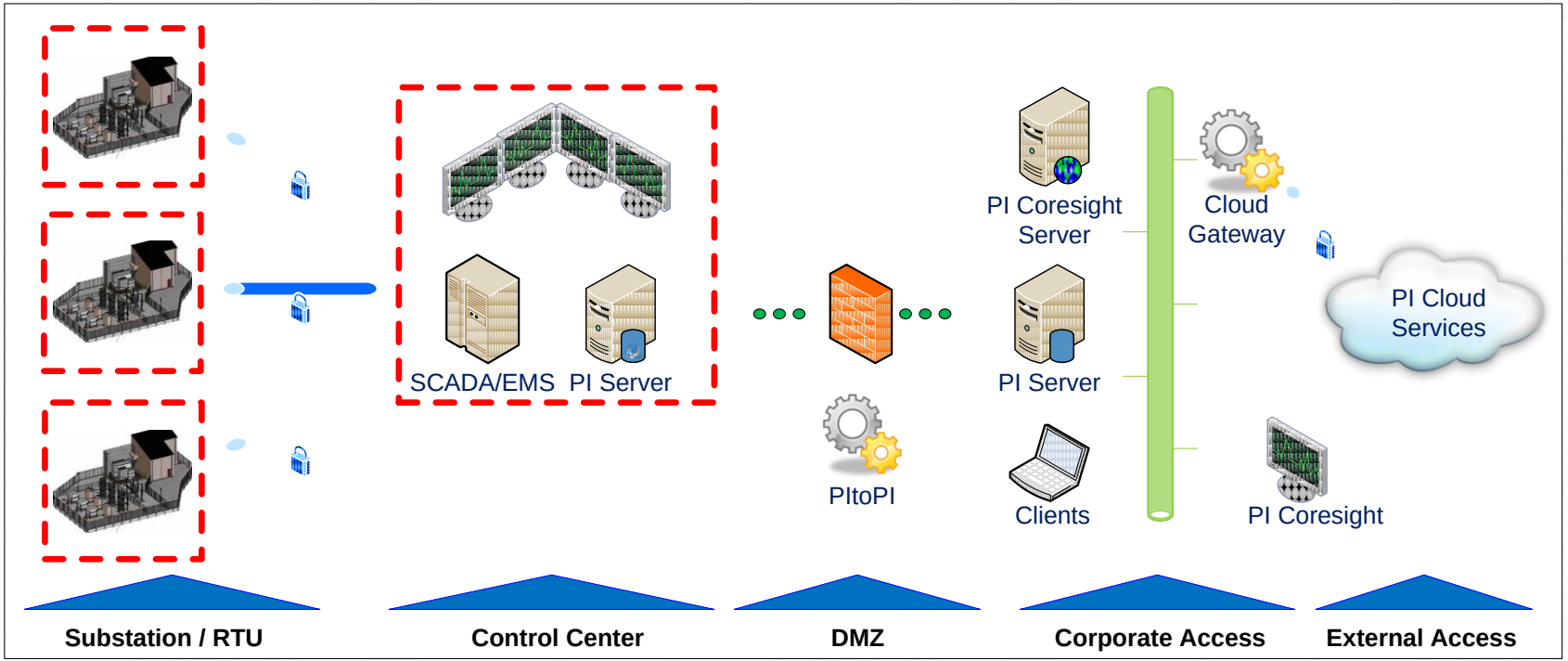
Limits direct access to critical systems while expanding the value use of information.

OSIsoft.

Infrastructure

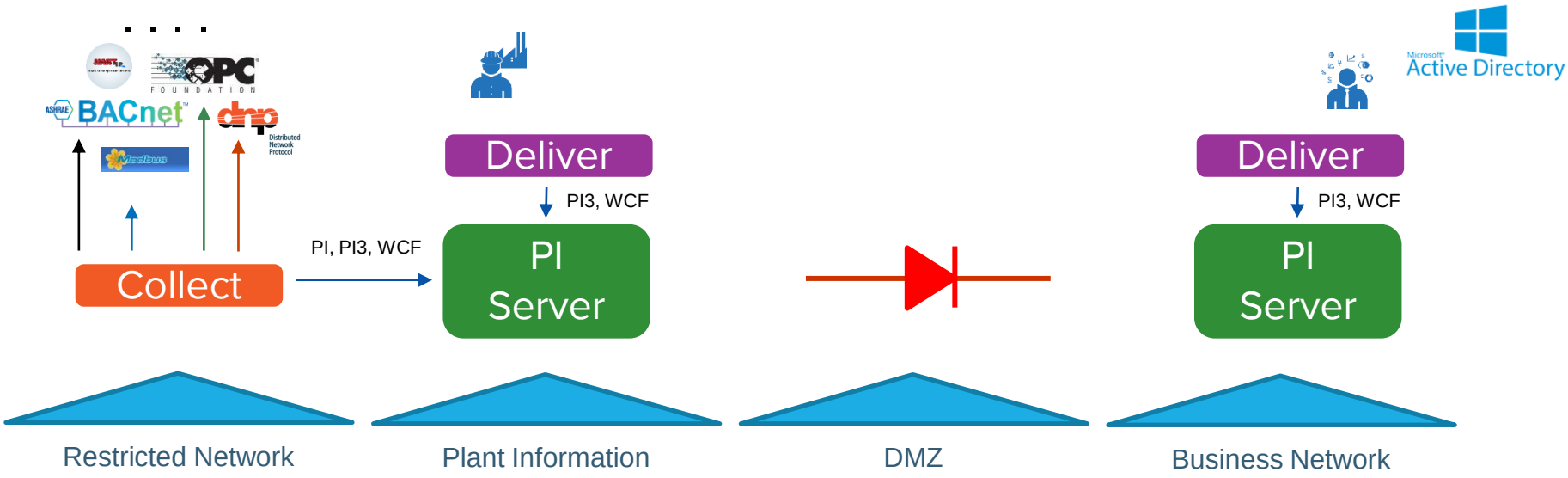
Security Perimeter

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

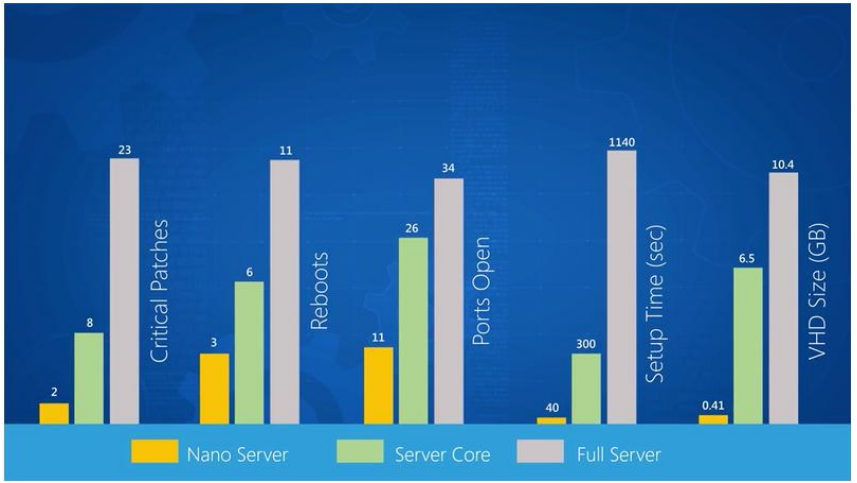


2. Least Functionality

PI Server – Certified for Windows Server Core

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

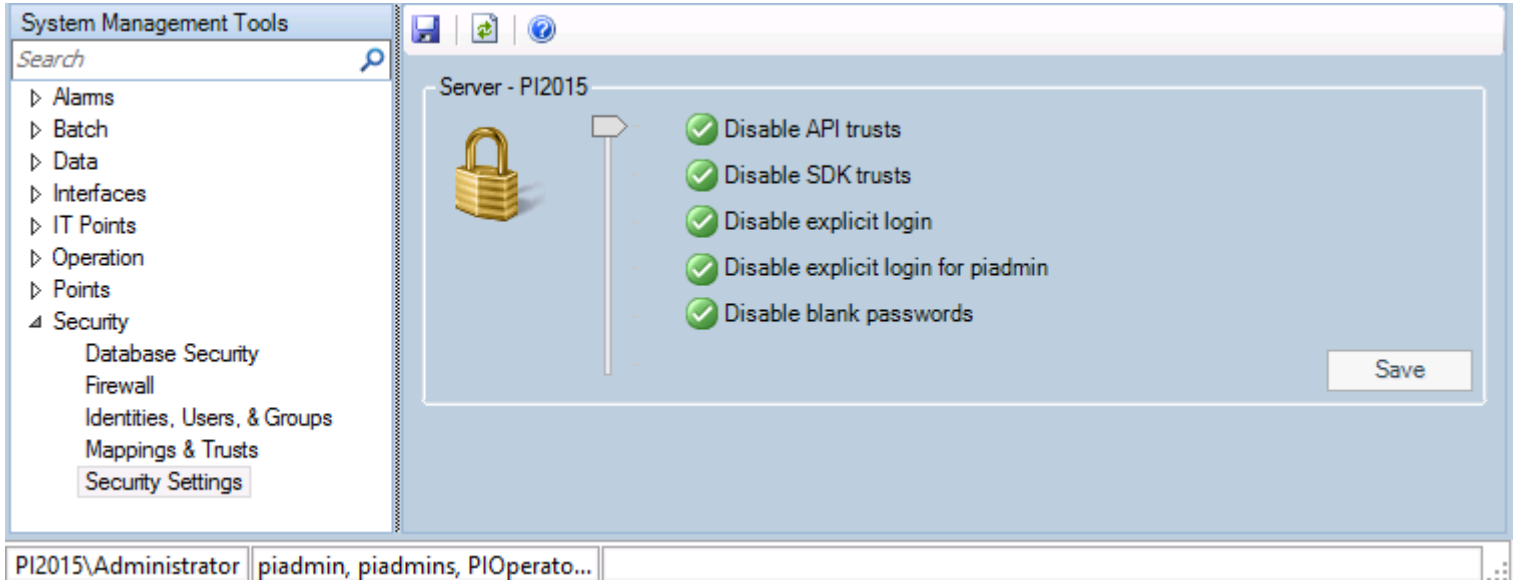
…. More Secure



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

3. Authentication Management

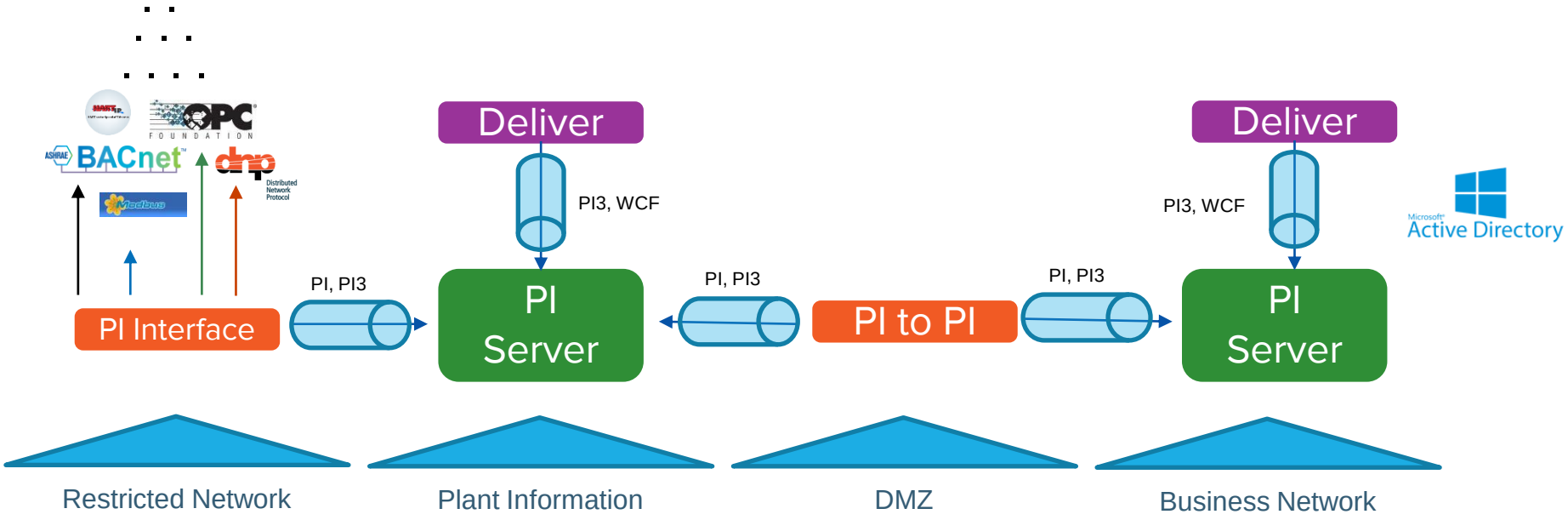
Use Windows Integrated Security (WIS)



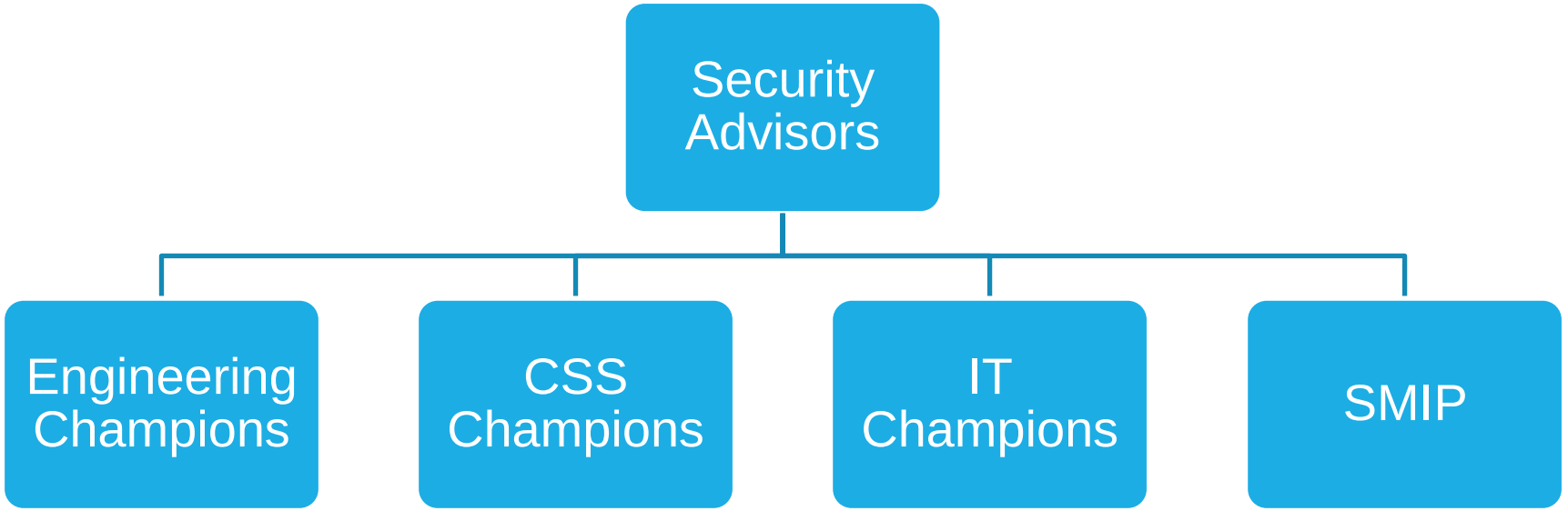
3. Authentication Management: The Modern PI System

Using Windows Integrated Security -

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



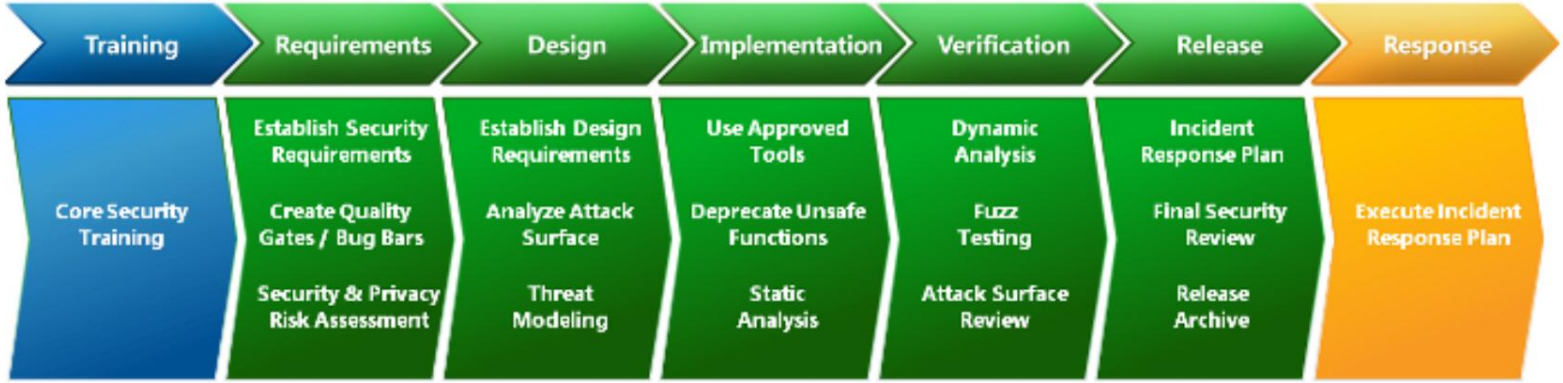
Work in Security is Ongoing



secure@osisoft.com

OSIsoft Security Development Lifecycle

Microsoft SDL model



Cigital

QUALYS

IOActive

Coverity

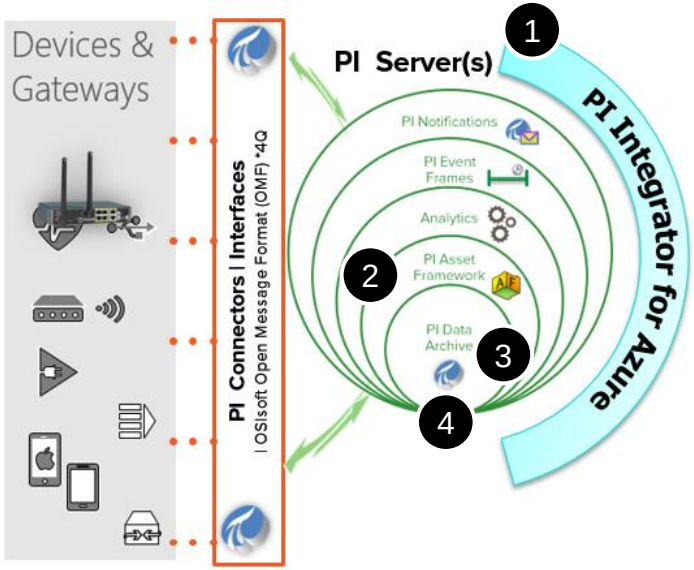
INL Idaho National Laboratory

Microsoft

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

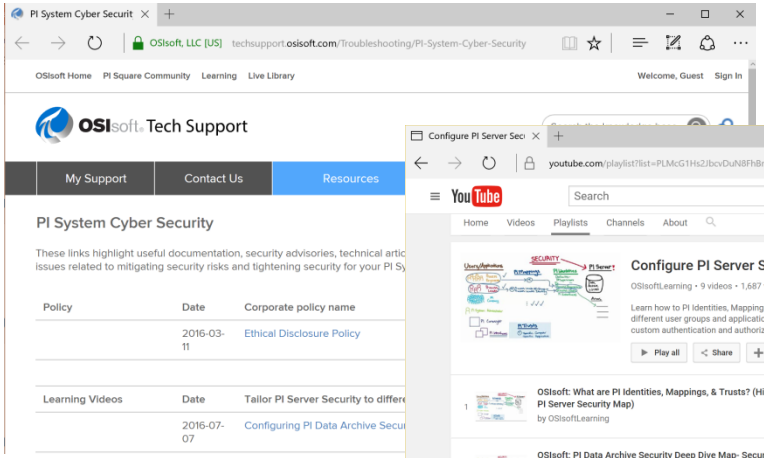


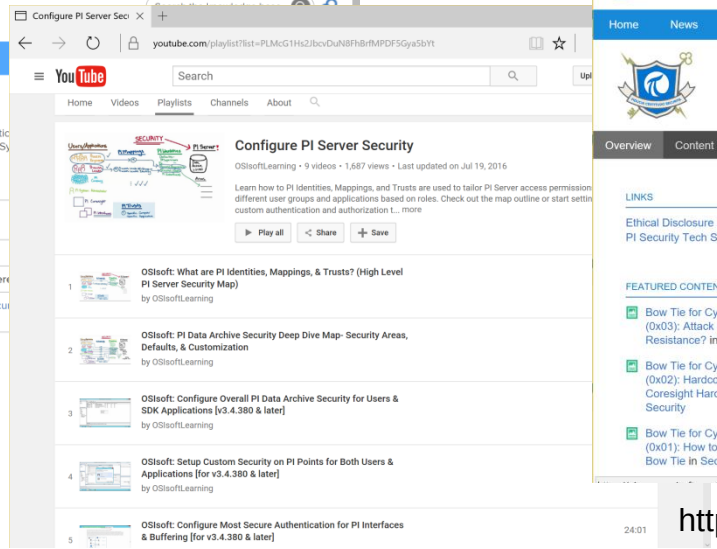
1. Resists pathological PI SQL data queries
2. Safe import and export of AF asset structures
3. Robust support for intensive bulk data calls
4. Reliable access to archive data

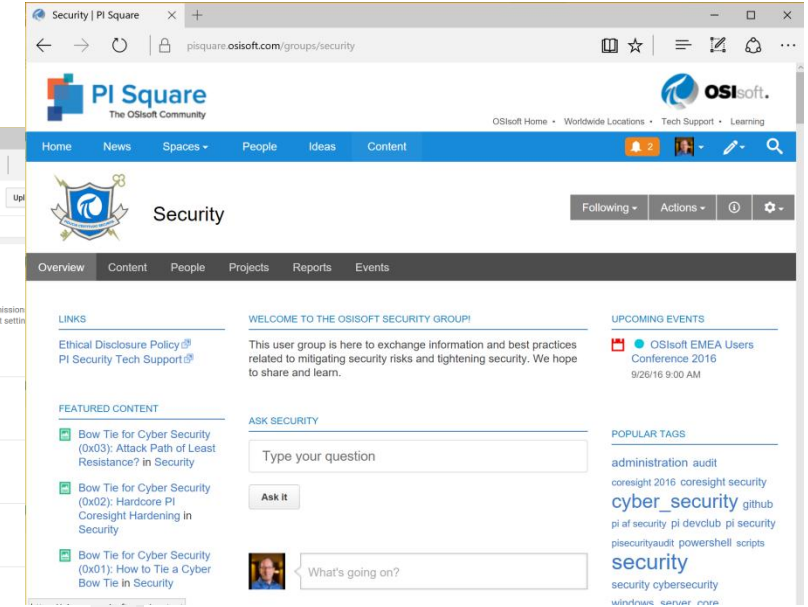
Microsoft

Key PI System Security Resources

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







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

https://www.youtube.com/user/OSIsoftLearning/

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

http://ddut.ch/osisoft

감사합니다

谢谢

Danke

Gracias

Merci

Thank You

ありがとう

Спасибо

Obrigado