



OSIsoft.

USERS 2013 CONFERENCE

The Power of Data

E M E A

THRIVING IN A WORLD OF CHANGE





Cyber Security

Presented by **Bryan S. Owen PE**

OSIsoft – Cyber Security Manager

Agenda

Trauma Center



Deployment Patterns



Security Development

eSecurity Planet

2 US Power Plants affected with Malware

In both cases the malware was delivered with a USB drive.

January 16, 2013

Krebs on Security
In-depth security news and insight

Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent

A company whose software and services are used to remotely administer and monitor large sections of the energy industry began warning customers last week that it is investigating a sophisticated hacker attack spanning its operations in the United States, Canada and Spain

InformationWeek

Saudi Aramco Restores Network After Shamoon Malware Attack

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

Matthew J. Schwartz

Updated: 12:22 p.m. August 27, 2012

BBC NEWS
TECHNOLOGY

Computer virus hits second energy firm

Computer systems at energy firm RasGas have been taken offline by a computer virus only days after a similar attack on oil giant Aramco.



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 infrastructure such as power plants.

Zack Whittaker

Updated: 2:44 p.m. PDT August 22, 2012

OSIsoft Technical Support Cases

- 20 Cyber incident cases (2012 to 2013.Q3)
 - Some false positives
 - Most were not
- Observation
 - Very disruptive
 - Trending higher (8 in 2012)
 - We take it serious



What happened, is my PI System ok?

- Malware protection false positive (5)
- Generic malware (4)
- 3rd party security update (4)
- PI System security update (3)
- Architecture/configuration (2)
- Compromised credential (1)
- Hacking (1)



Emergency Preparedness is Key



NERC CIP version 4 and version 5
NRC 5.71 and NEI 08-09
Presidential Policy Directive PPD-21
Executive Order - Improving Critical Infrastructure Cyber Security



אין ירידה מהשביל
סכנה
בזמן טיפוס
DANGER
DO NOT LEAVE THE PATH
DEEP MUD

**Regulatory Uncertainty
continues for Power Generation**

Support Capability Levels

- Personnel surety
 - Background checks
 - Role based cyber security education
- Multi-factor authentication
 - Extend beyond services and admins
- Incident response plan
 - Design and exercise the plan

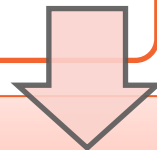
Managed (MIL3)

Initiated (MIL1)

Incomplete (MIL0)

Agenda

Trauma Center



Deployment Patterns



Security Development

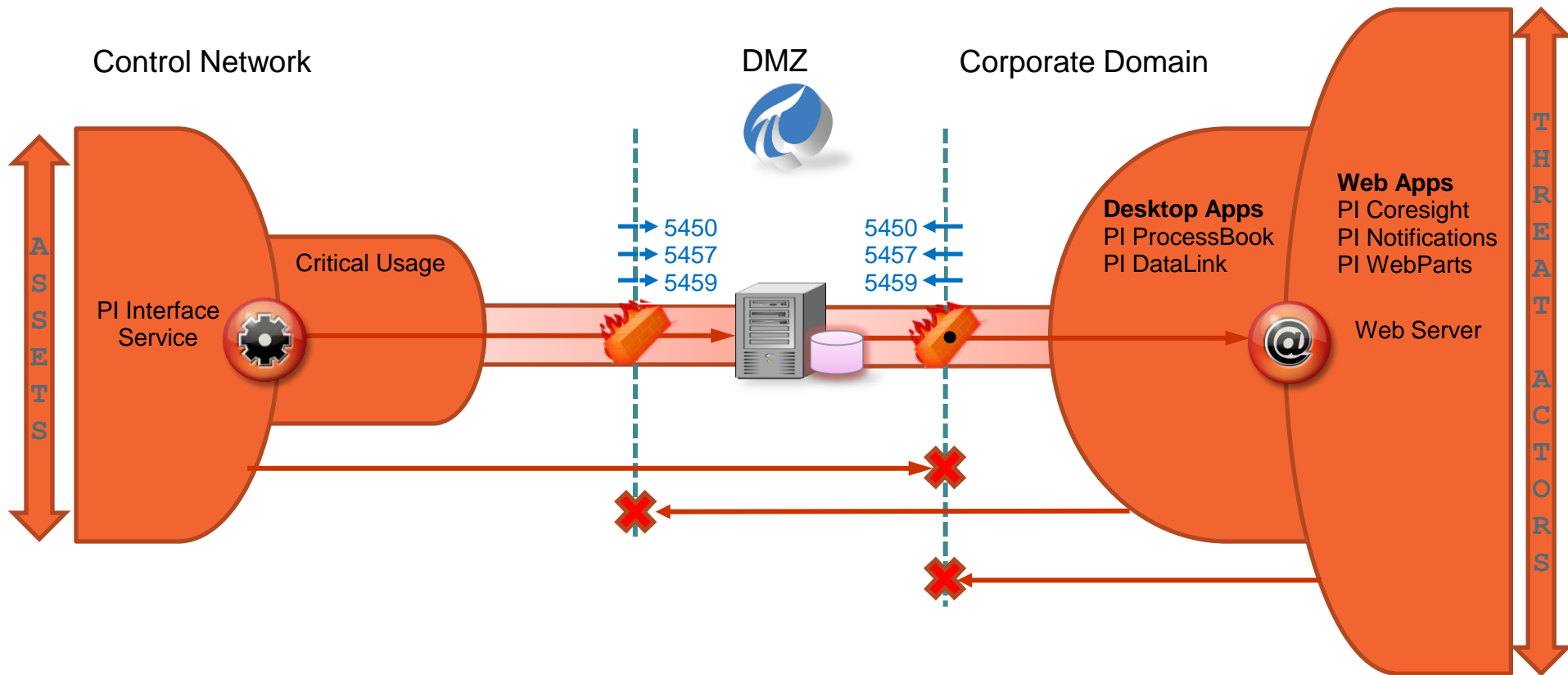
Threat Interaction Categories

Visibility

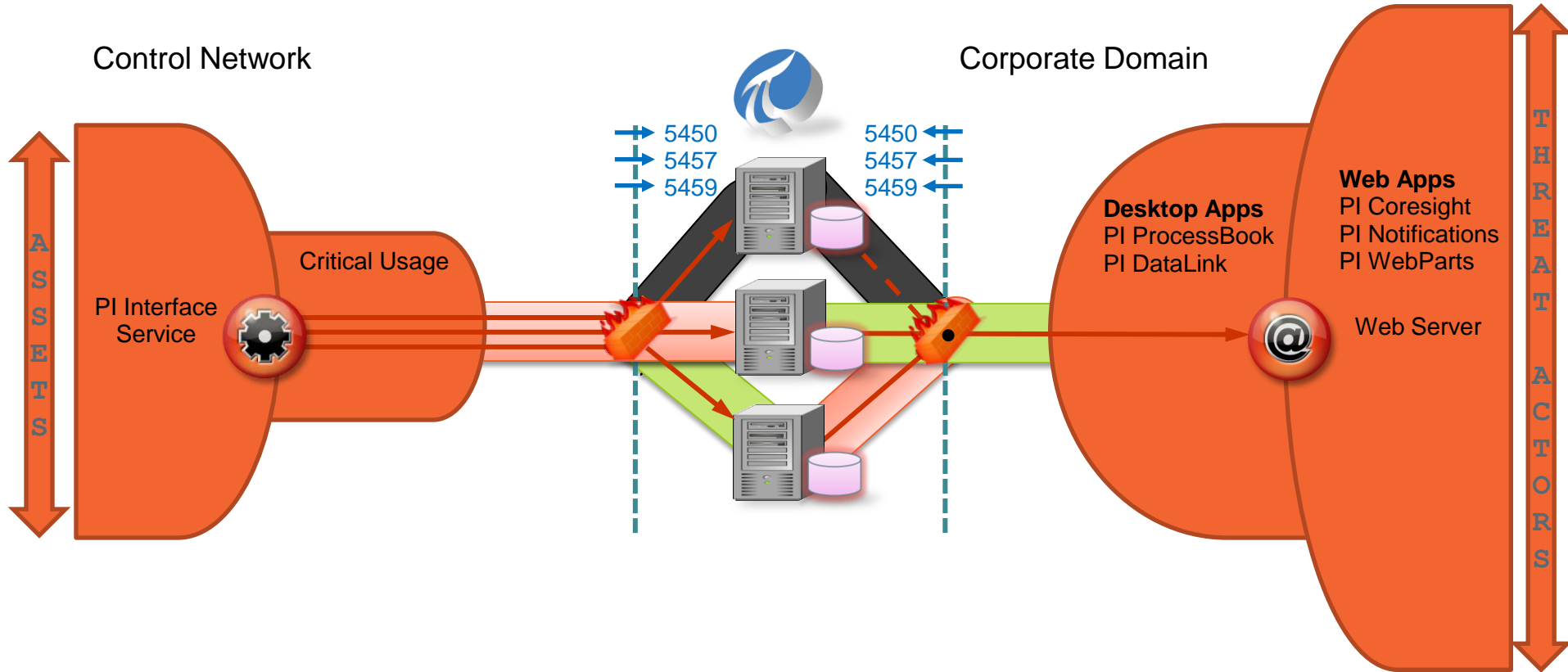
Access

Trust

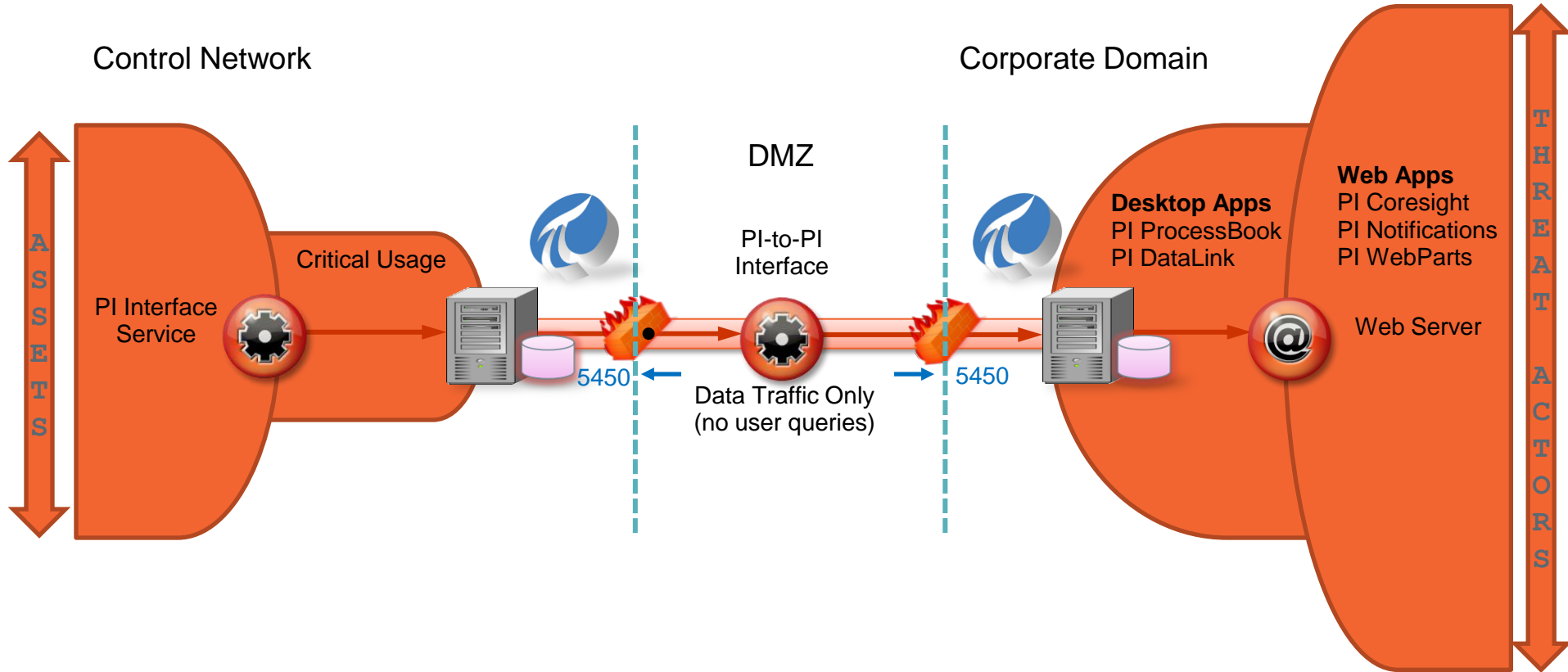
Pattern 1: DMZ PI



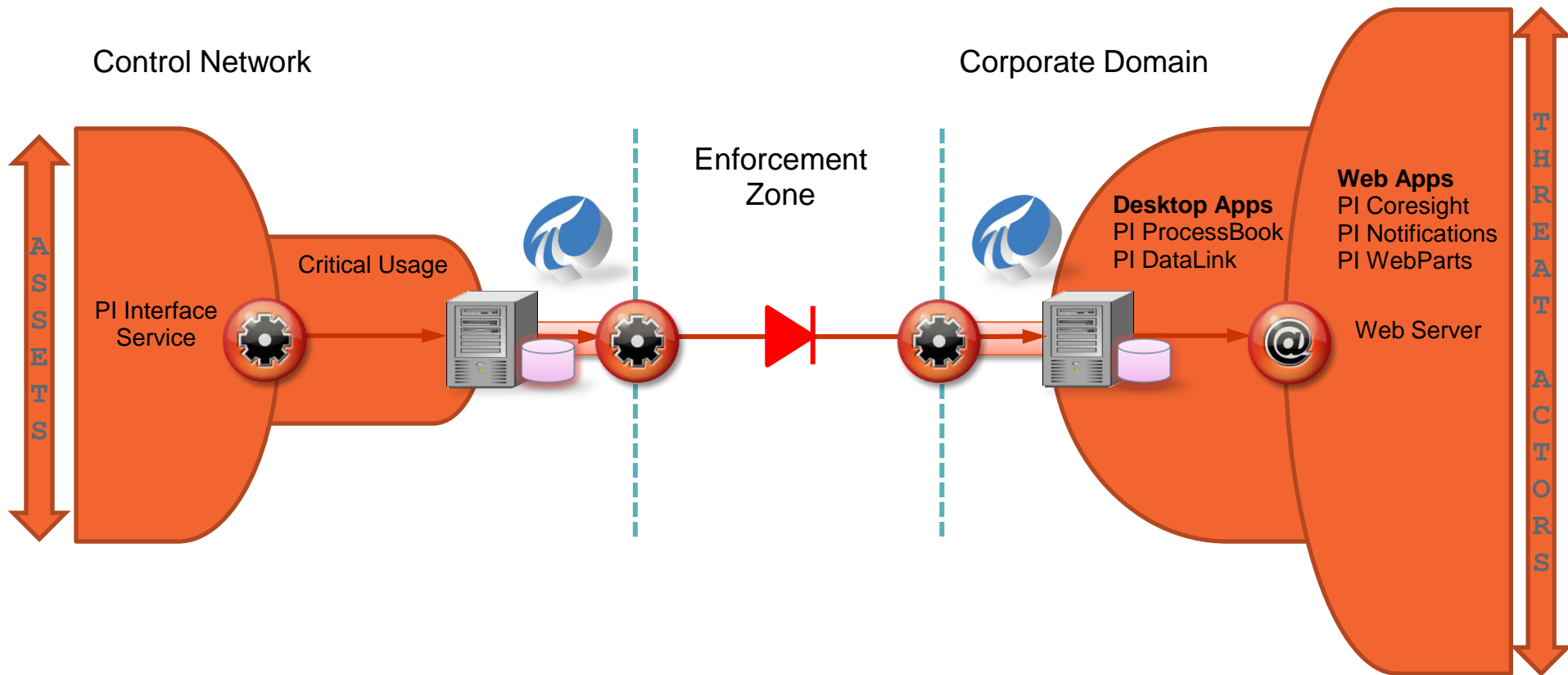
Pattern 2: PI High Availability



Pattern 3: DMZ PI to PI



Pattern 3+: Absolute Enforcement





Tuesday
(3:20 PM – 3:50PM)

**New Technologies for
Cyber Security**



Tuesday
(4:30 PM and 5:30 PM)

**Expo “EA Hot Spot”:
Keep the PI System Alive and
Working for you 365**

Security Development



Trusted Advisors:

- Idaho National Lab
- Microsoft

Security Engagements

- Idaho National Lab
 - 2005 Assessment
 - 2008 vCampus Live!
 - 2009 vCampus Live!
 - 2011 Cooperative Research
 - 2012 vCampus Live!
- US Army NetCom
 - 2009 CoN #201006618
 - 2013 CoN (recertified)
- US NRC
 - 2010 DISA, NIST
- SAP QBS Certification
 - 2012 Veracode
- Microsoft Information Security Consulting
 - 2009 PI Server
 - 2010 PI Agent
 - 2011 PI Coresight
 - 2011 PI AF
 - 2012 PI ProcessBook
 - 2012 Products in Design (3)
 - 2013 Engineering Management
 - 2013 Products in Design (2)
 - 2013 SDL for Security Champions
- Windows Logo Certification
 - 2008 Server Core
 - 2011 Server Core R2

PI System Network Ports and Services

Service Endpoint	Platform Library	Port (TCP)	Transport Security	Comment
MS SQL Server	Winsock	1433		See MS189067 to enable SSL
Managed PI Agent	WCF	5449	✓	
PI Server	Winsock	5450		Secure authentication via SSPI Post assessment mitigations Transport security on roadmap
ACE Web Service	ASP.Net	5456		PI Web Services alternative
AF Server	WCF	5457	✓	
PI Notifications	WCF	5458	✓	
AF Server (Streaming)	WCF	5459	✓	
PI SQL Data Access Server	WCF	5461	✓	

Open Communication on Cyber Security



Bottom line: OSIssoft is actively finding and fixing issues.



Monday-Tuesday-Wednesday

Product Expo PI Security Pod
(12:35 PM - 5:20 PM)



Thursday

PI System Security Workshop
(10:00 AM and 1:30 PM)

Migrating to PI Server 2012 with
PI AF and WIS
(10:00 AM and 1:30 PM)

Summary

- What happens to one company affects us all
- Security is better with newer versions
- Critical infrastructure protection is a shared mission
 - Start now at **#UC2013!**

Bryan S. Owen PE

bryan@osisoft.com

Cyber Security Manager

OSIsoft, LLC

@bryansowen



THANK YOU

Brought to you by



Get hands on knowledge of how to
use and get value from the PI System



DECEMBER 3 - 6, GRAND HYATT SAN FRANCISCO

vCampus Live! 2013

WHERE PI GEEKS MEET



SAVE THE DATE

