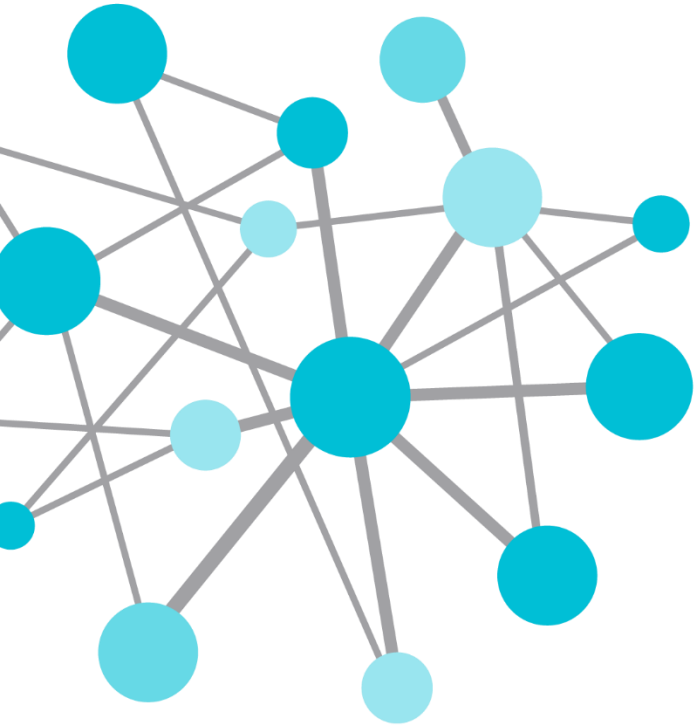
OSIsoft.

USERS CONFERENCE 2014

The Power of Data

DECISION READY IN REAL-TIME



Challenge:
Harden the PI System against cyber threats

Presented by **Bryan S. Owen PE**

The Top 4

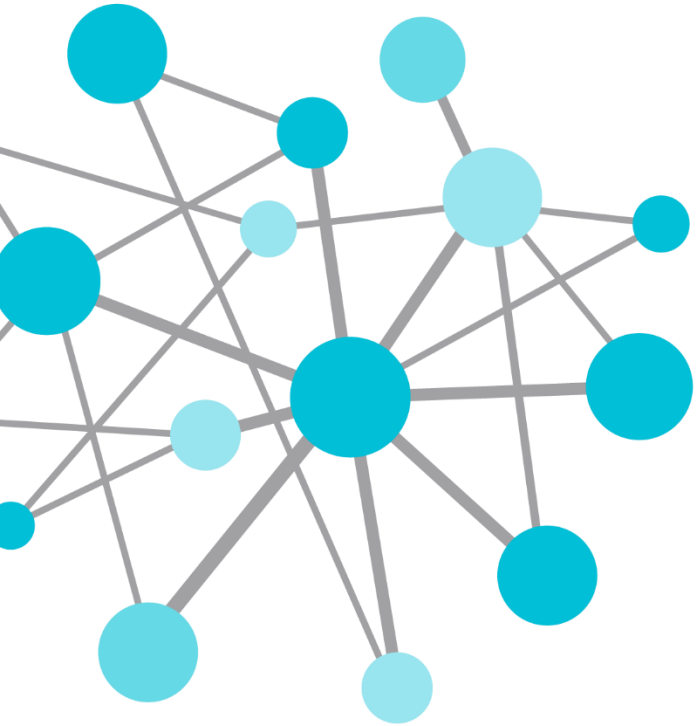
1: Use Whitelisting Techniques

2: Upgrade your Applications

3: Upgrade your Operating System

Use Windows Server Core for Servers

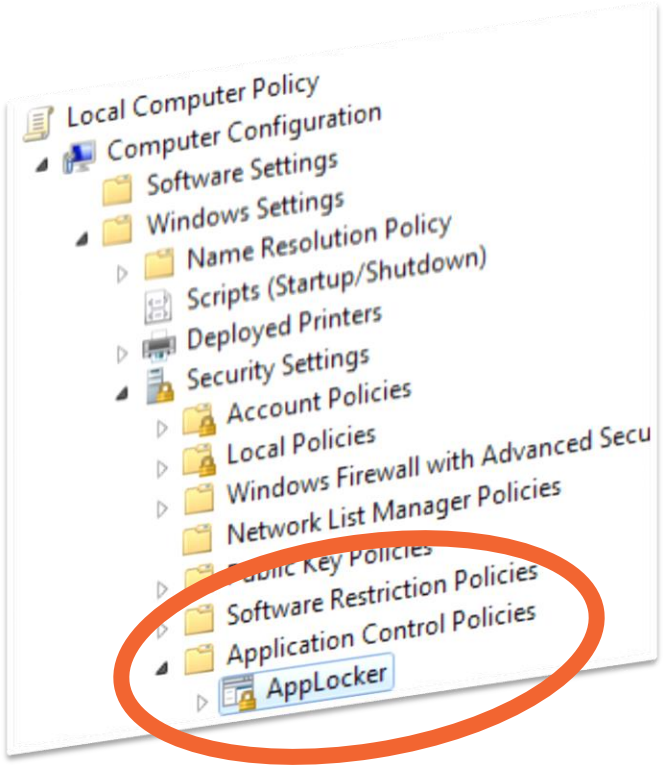
4: Least Privileges

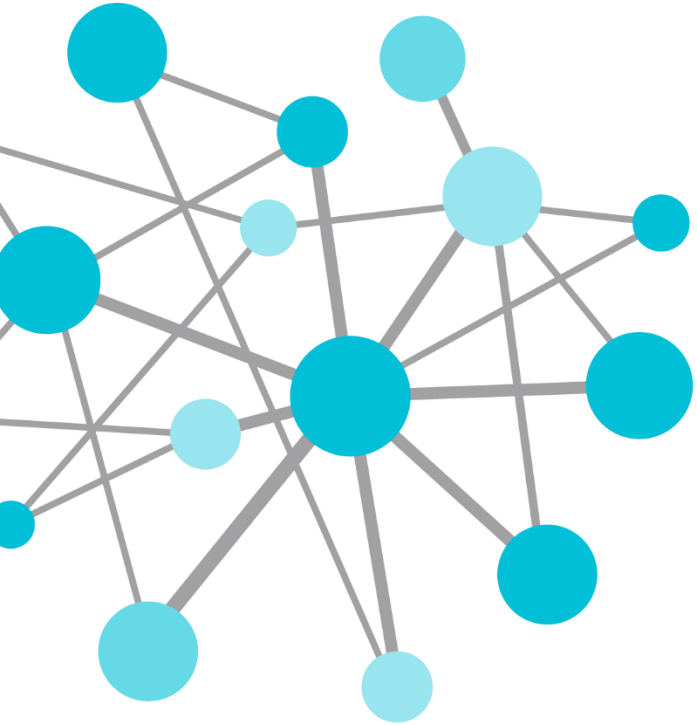


Hmmm.

How do we get started?

Knowledge Base “Step by Step”





Excellent!

We are just getting started.

What else should we know?

Learning from history…

Steelmaking

- Very expensive prior to 1860's
  - knives, swords, armor, etc.
- Engineering innovation
- Now basic to the world industrial economy

Hardened in Development

Steel

- Fe, C, Mn, Ni, Cr, etc…
- Heat treating

Software

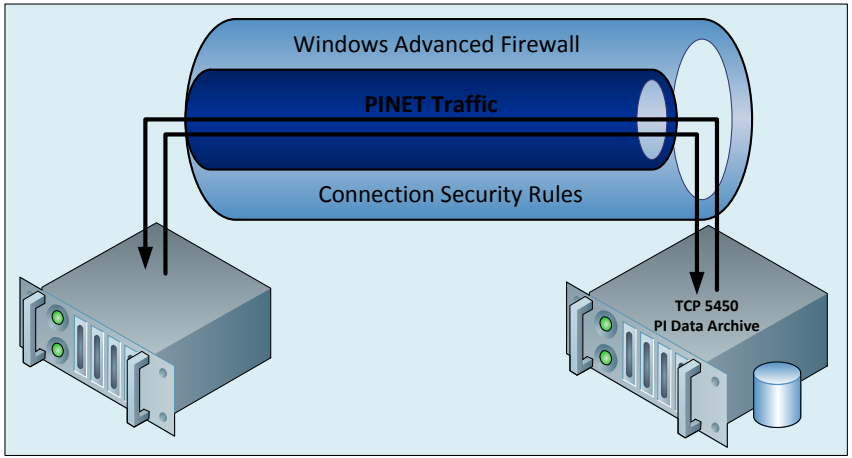
- Input validation, Least privilege
- SDL process

PI Server Version SDL Defense		PR1 3.4.375.38	WIS 3.4.380.36	2010 3.4.385	2012 3.4.390
Code	Pointer Encoding				Future
	/Analyze				Adhoc
	Heap corruption detection				100%
	Safe function migration				80%
Linker	SEHOP (*)	Win 2008+	Win 2008+	Win 2008+	Win 2008+
	/SAFESEH (*)	100%	100%	100%	100%
	/DYNAMICBASE (ASLR)		Win 2008+	Win 2008+	Win 2008+
	/NXCOMPAT (*)		Win 2003 SP1+	Win 2003 SP1+	Win 2003 SP1+
Compiler	/GS	/GS V2	/GS V2	/GS V2	/GS V3
	Compiler Version	VC++ 2005	VC++ 2005 SP1	VC++ 2008 SP1	VC++ 2010 SP1
Platform	Windows Server Core		Win 2008+	Win 2008 R2	Win 2008 R2+
	Native x64 (*)	Supported	Supported	Supported	Supported

Hardened in Deployment

Epoxy coated pipe

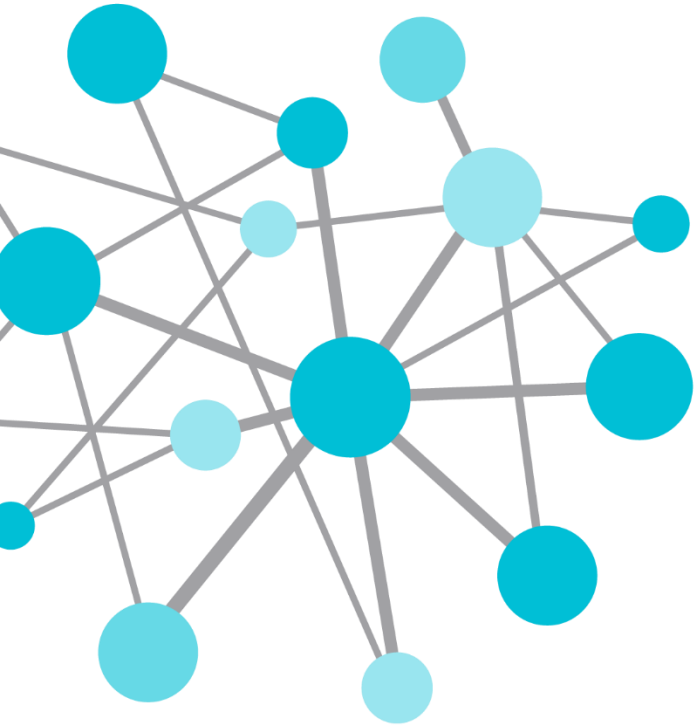
Connection Tunnels



Build Complimentary Knowledge

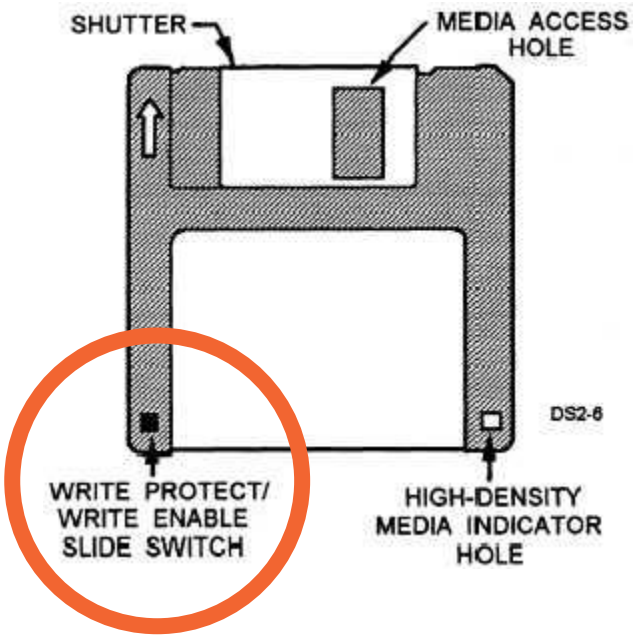
Domains

- Software Development
- System Integration
- Operational Excellence
- Security Research



Early days of Cyber Hardening…

Ideas based on physical security



Portable Media

- Floppy disks
- CDROM
- WORM
- Flash (R/W)
- Mobile Devices (R/W)

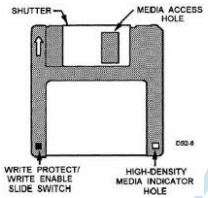
Physical and logical hybrids

PLC5 Key Switch

- Program
- Run
- Remote
  - Remote Program
  - Remote Test
  - Remote Run

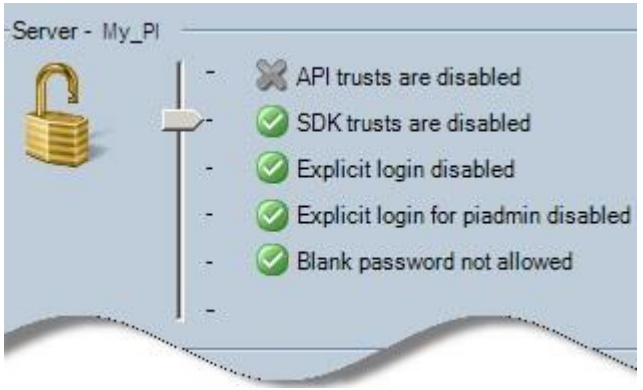
Security is Evolving

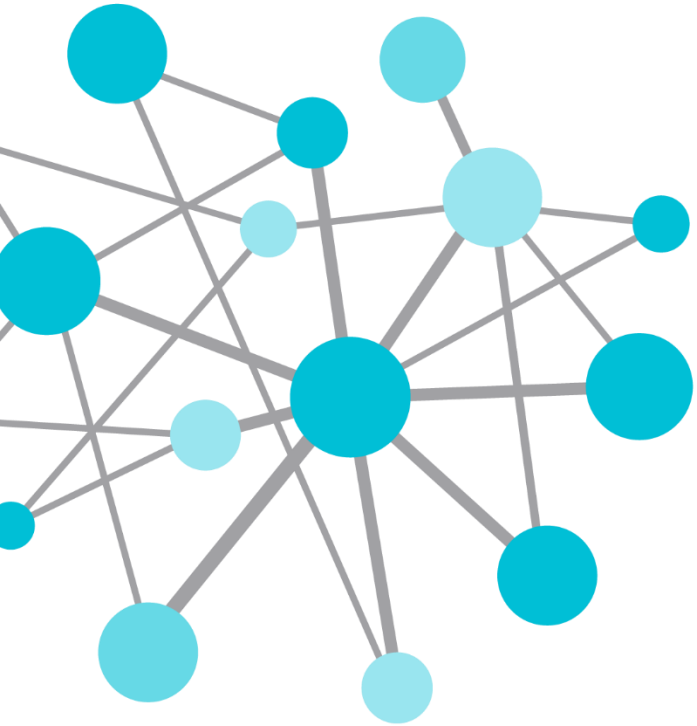
Physical



Hybrid

Logical





Software Based Hardening

Hardening Objectives

- Maintain a sustainable system
- Increase difficulty of cyber breach
- Increase detection capability
- Reduce consequences

HD Moore's Law

"Casual Attacker power grows at the rate of Metasploit"

Corollary:

Metasploit won't tell you you've done "enough" but it just might prove if you haven't.

Cyber Security (301) - 5 days
http://ics-cert.us-cert.gov

Cyber Attack Simulations

DAY 0 | Tuesday, December 3

Time	Union Square Room
Noon - 7:30 PM	Security Hackathon ANSWER BAR SOLD OUT
07:30 - 08:00 PM	Security Hackathon Judging

IEC's Cyber-Gym toughens up Israel's infrastructure

Cyber-defenders at the Israel Electric Company have to mitigate up to 6,000 'fake' hacker attacks per second, helping them practice for the real thing

US Cyber Challenge

http://uscc.cyberquests.org/

Infrastructure/Application Security Challenge (April):

Date	Description
Wed. Apr. 2, 2014 10:00am EDT	Registration opens
Wed. Apr. 16, 2014 7:00am EDT	Quiz opens
Tue. Apr. 29, 2014 9:00pm EDT	Registration closes
Wed. Apr. 30, 2014 11:59pm EDT	Quiz closes

Hardening is hard

Technical dependencies

- Platform and network
- Application stack
- System integration
- Critical information
- Operational mission

Cyber criminal methods

- Bogus configuration
- Software vulnerability
- Post exploitation and pivoting
- Data exfiltration
- Command and control

IT Security Baselines

Microsoft Security Compliance Manager (SCM) 3.0 | Solution Accelerators

- ✓ Microsoft Products
- ✓ Free Download

Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

- ✓ Multi-Platform + Device
- ✓ Limited Free Download
- ✓ Subscription Model*
- ✓ Hardened Virtual Images*

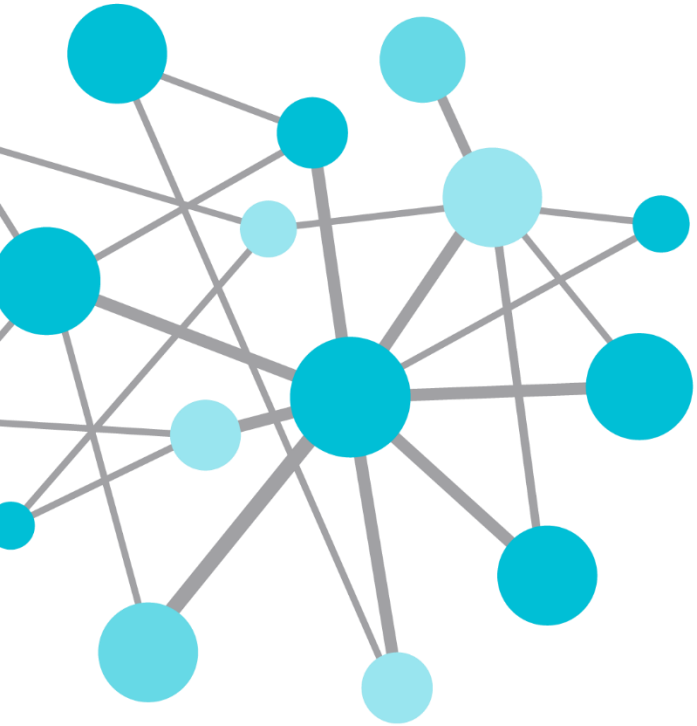
DEFENSE INFORMATION SYSTEMS AGENCY

- ✓ NIST + FISMA
- ✓ Multi-Platform + Device
- ✓ Free and Government Only Download

Before you start…

- A single mistake can result in total system failure
- Test on virtual machines

- Harden before acceptance testing and commissioning
- Verify hardening in maintenance testing

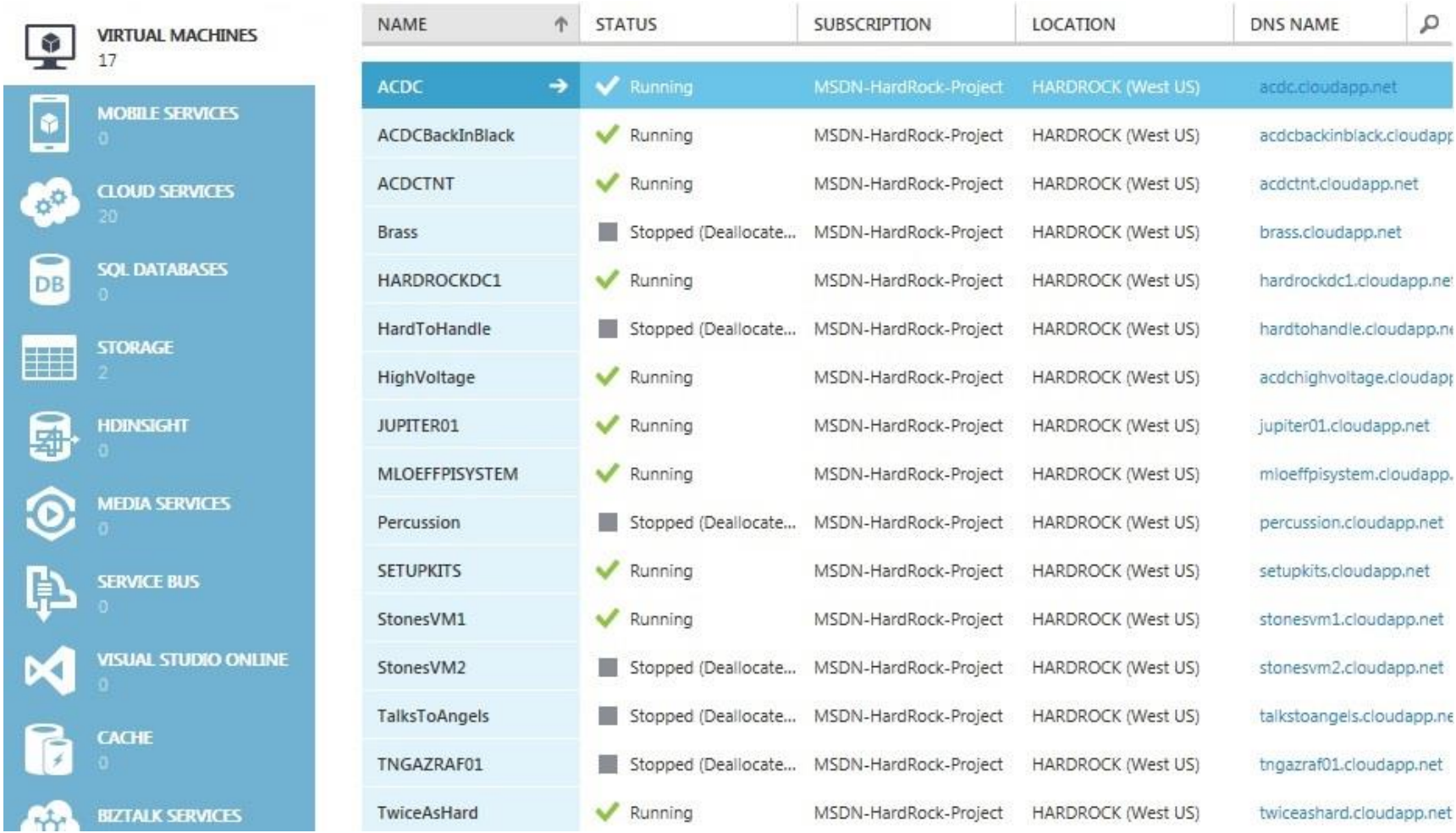


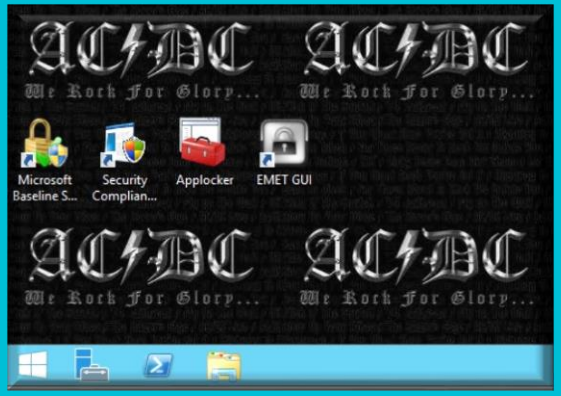
Call to Action

Hardened Image Challenge Series

Project “Hard Rock PI”

- Internal OSIsoft Challenge
  - Create virtual images in Azure
  - Prizes!
- Enable security features
  - Operating system
  - PI System

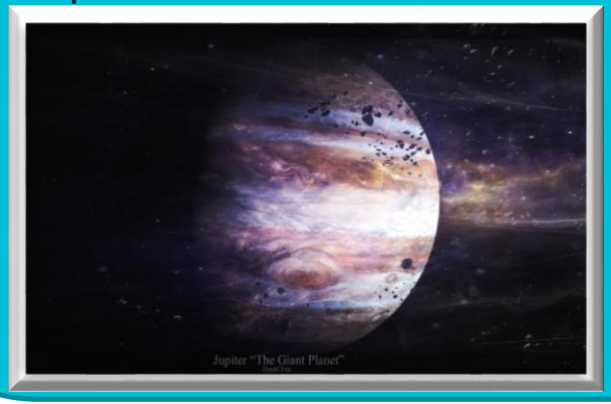




"ACDC" – Omar Mohsen

"Black Crowes" – Derek Endres

"Jupiter" – Marcos Vainer Loeff

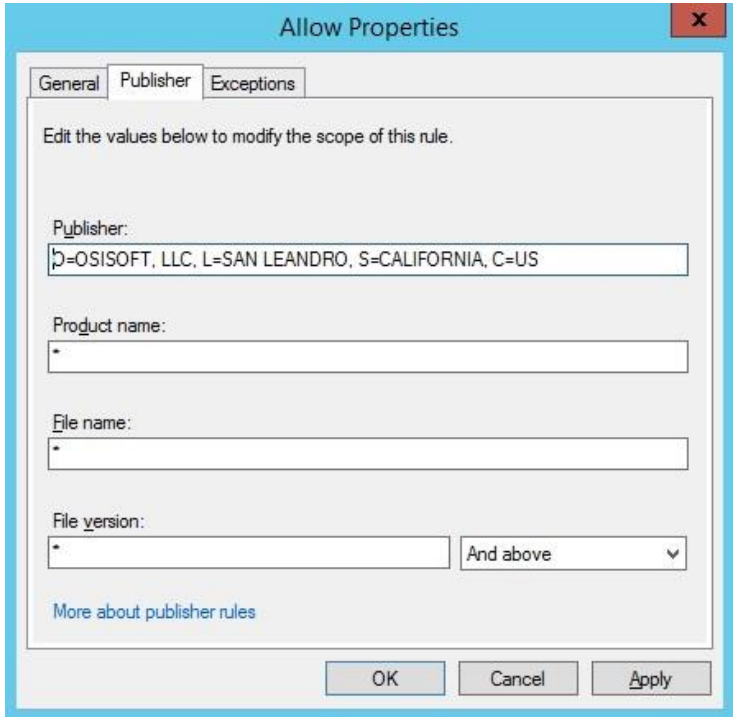


"Metallica" – Dan Brooks & Ram Kathiresan

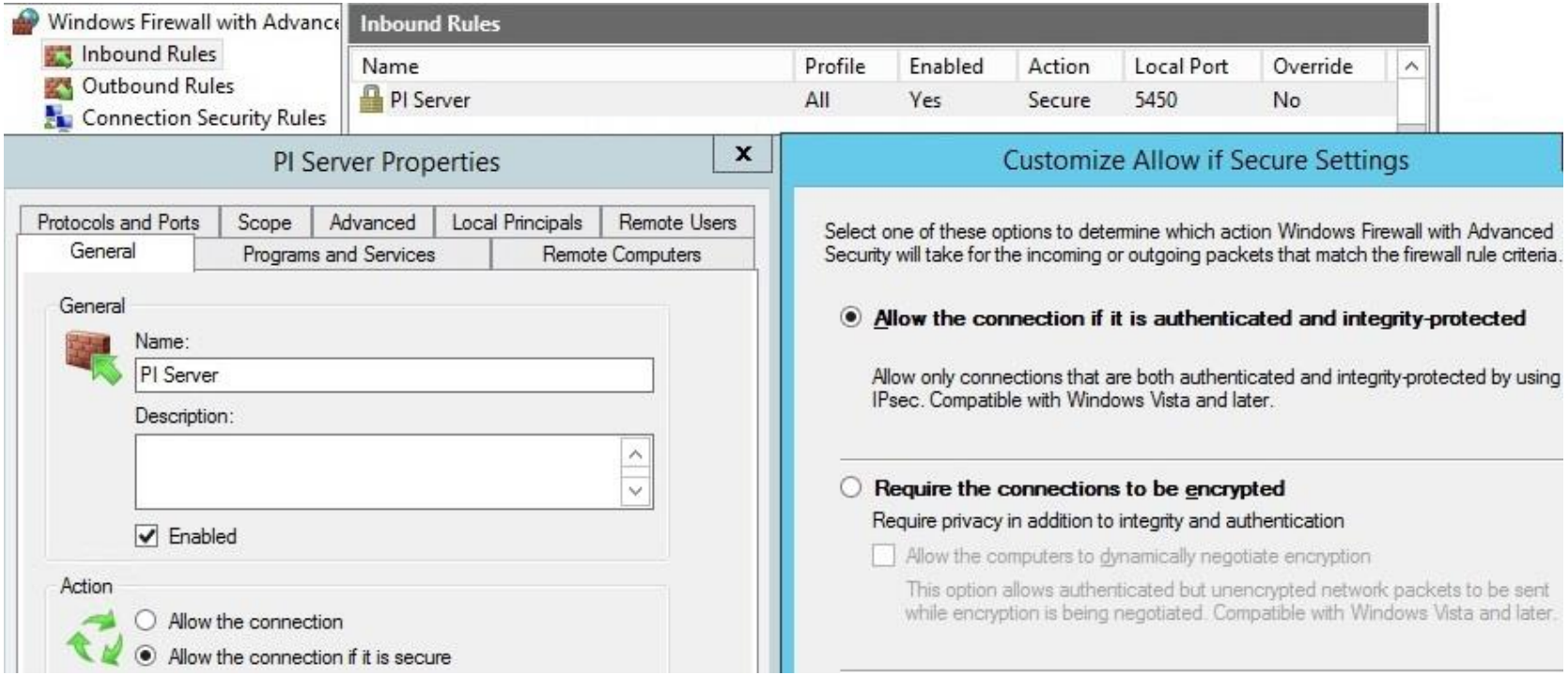
Top 4 and More…

	ACDC	Black Crowes	Jupiter	Metallica
Applocker				
Firewall Input Rules				
Firewall Output Rules				
Server Core				

Applocker – OSIsoft Publisher Rule



Windows Firewall



Server Core

```
PS C:\> get-windowsfeature -name *gui*

Display Name                                            Name                       Install State
------------                                            ----                       -------------
    [ ] Graphical Management Tools and Infrastructure   Server-Gui-Mgmt-Infra          Available
    [ ] Server Graphical Shell                          Server-Gui-Shell               Available
```

GUI is add/remove feature as of Windows Server 2012

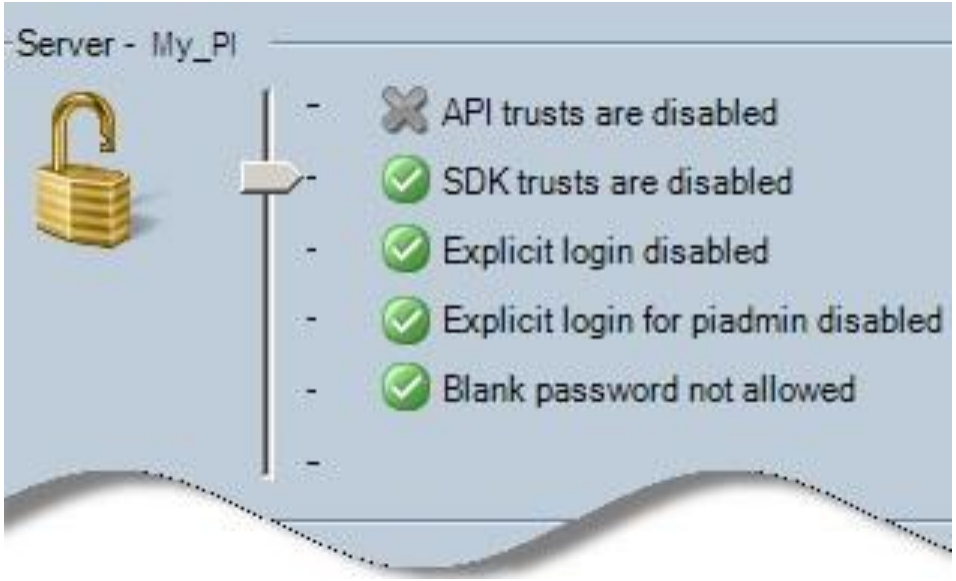
Eg. Add the management GUI without full desktop:

Install-WindowsFeature -name Server-Gui-Mgmt-Infra

Least Privilege…

Data Archive	ACDC	Black Crowes	Jupiter	Metallica
Authentication Policy				
Disabled piadmin				
Audit trail **Configuration Changes**				
Buffering & Interface **Service Hardening**				

Recommended Authentication Policy



API trusts can be disabled for servers without classic interfaces.

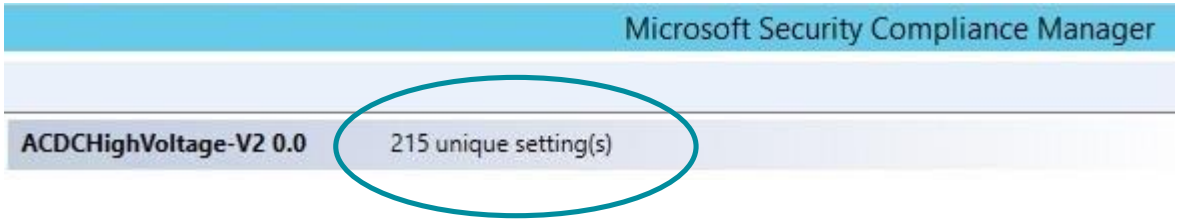
Eg. **Receiving all data from PI Cloud Connect**

Extra, Extra…

	ACDC	Black Crowes	Jupiter	Metallica
PI Security Audit				
Baseline Security Analyzer				
Security Compliance Manager				
EMET				

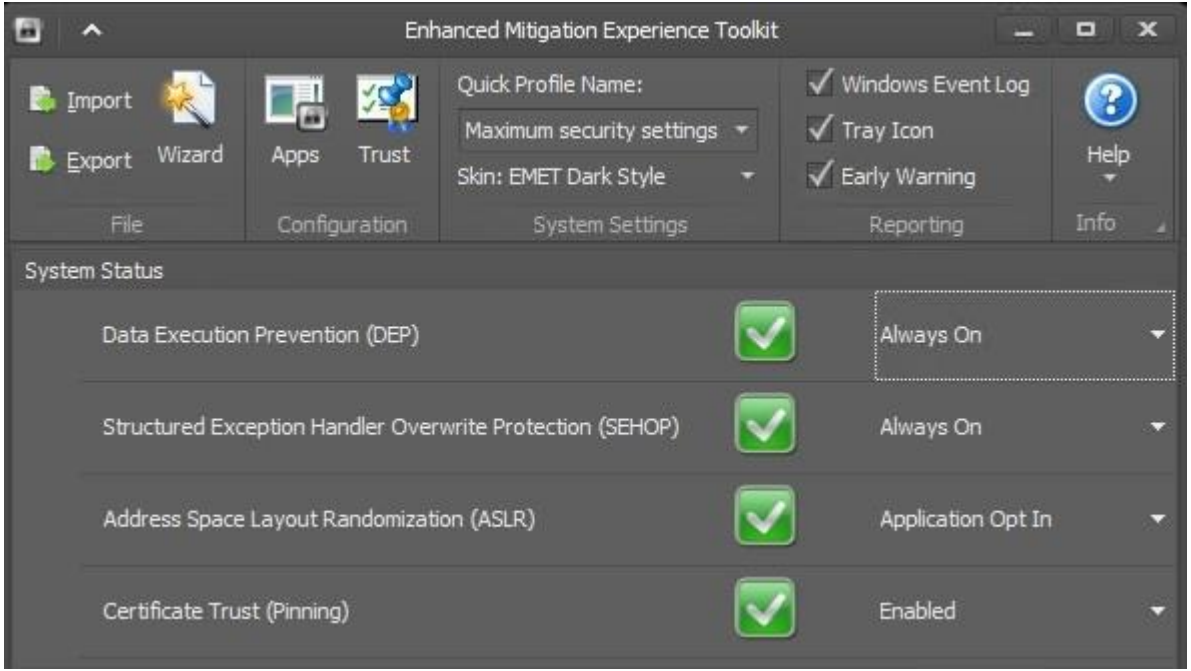
Security Compliance Manager

Microsoft Security Compliance Manager (SCM) 3.0 | Solution Accelerators

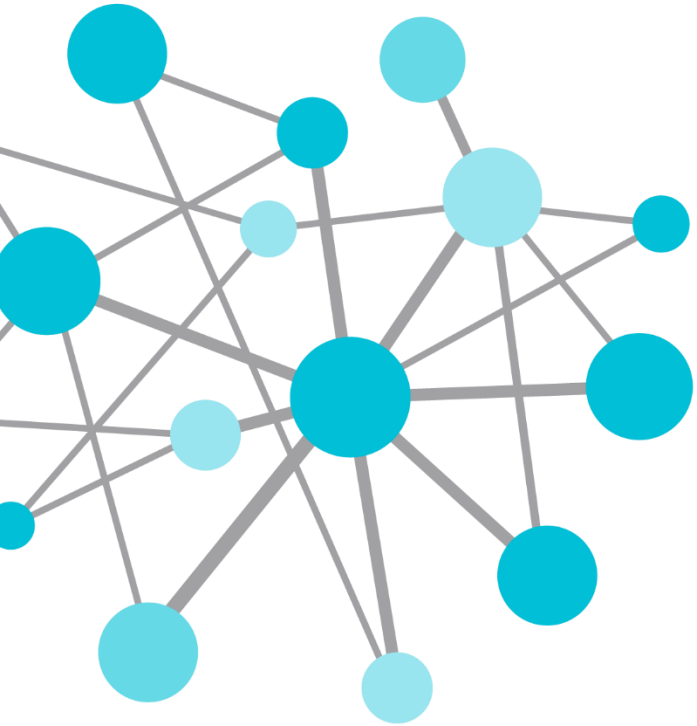


Windows 2012 Server Baseline – 215 Critical Items!

EMET



Process Name	Running EMET
pialarm - PI Alarm Subsystem	
piarchss - PI Archive Subsystem	
pibackup - PI Backup Subsystem	
pibasess - PI Base Subsystem	
pibatch - PI Batch Subsystem	
pilicmgr - PI License Manager	
pilogsrv - PI log server	
pilogsrv - PI log server	
pimsgss - PI Message Subsystem	
pinetmgr - PI Network Manager	
pipeschd - PI PE Scheduler	
pisnapss - PI Snapshot Subsystem	
pisqlss - PI SQL Subsystem	
pitotal - PI Totalizer	
piupdmgr - PI Update Manager	
random - random	



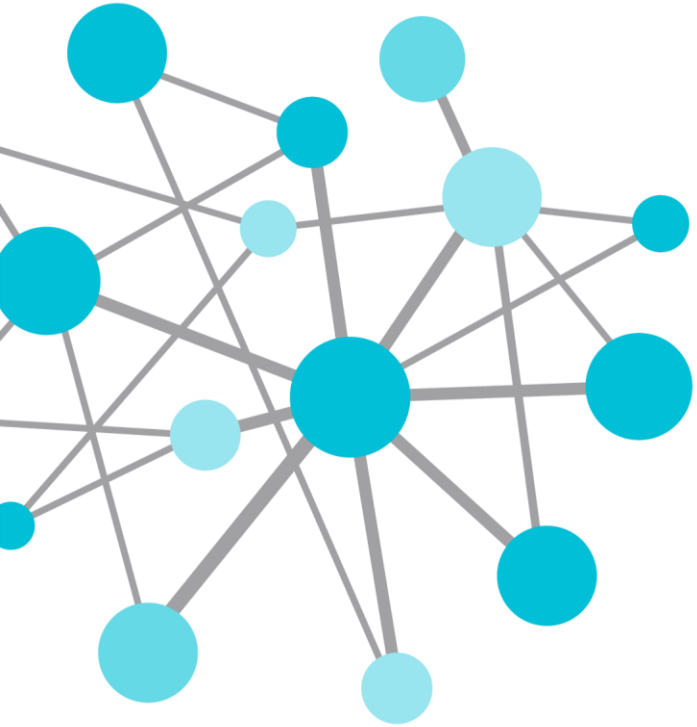
What about the grand prize?

Hard Rock PI

Omar Mohsen
OSIsoft Bahrain

Summary: Hard Rock PI

- Increases domain knowledge
- Transforms learning and advice
- Strengthens collaboration



THANK YOU

Brought to you by OSIsoft.

Bryan Owen

bryan@osisoft.com

@bryansowen

Cyber Security Manager

OSIsoft, LLC