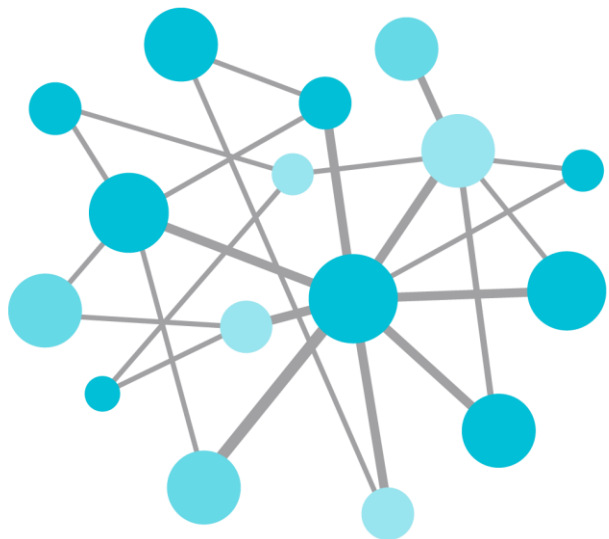




Cyber Threats: What Should I Do to Harden my PI System?

Presented by **Vadim Sizykh**
Omar Mohsen



OSIsoft[®]

USERS 2014

CONFERENCE

The **Power** of **Data**

E M E A



DECISION READY IN REAL-TIME

The Top 4

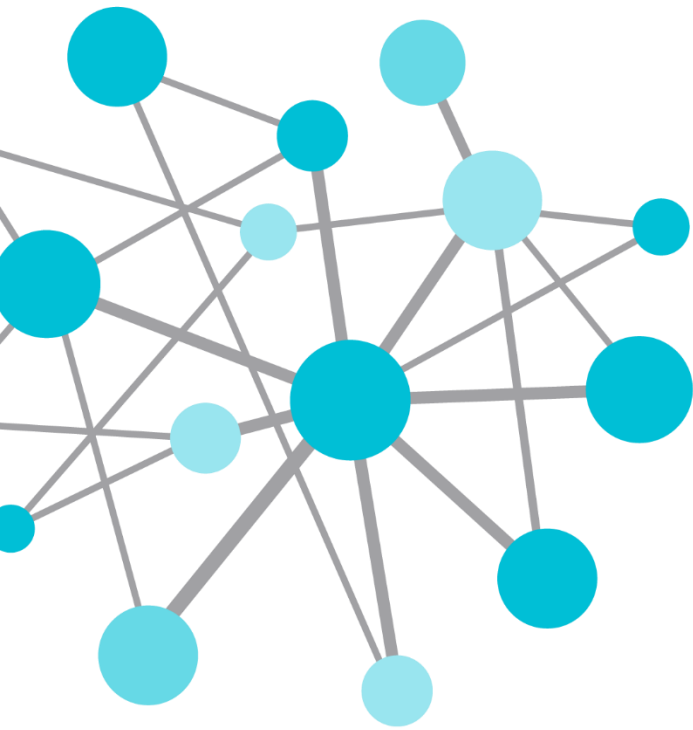
1: Use Whitelisting Techniques

2: Upgrade your Applications

3: Upgrade your Operating System

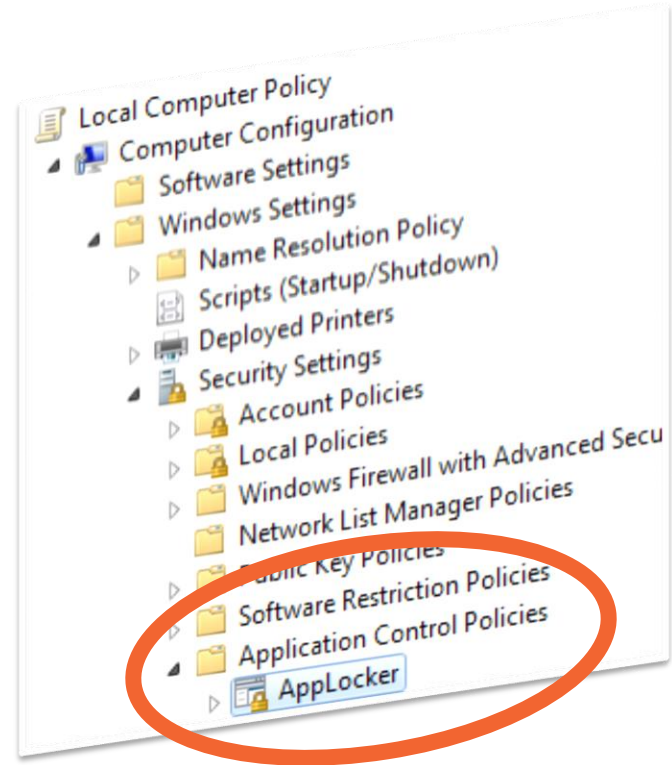
Use Windows Server Core for Servers

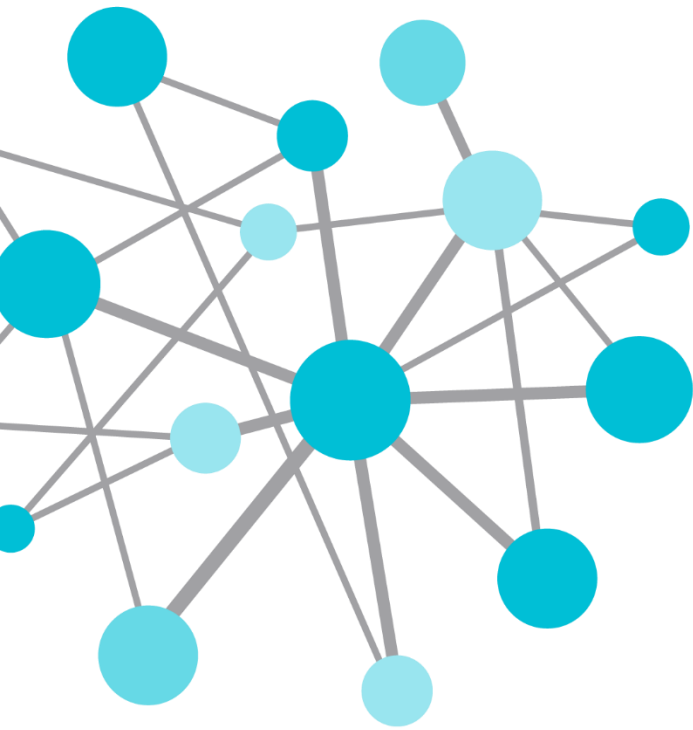
4: Least Privileges



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

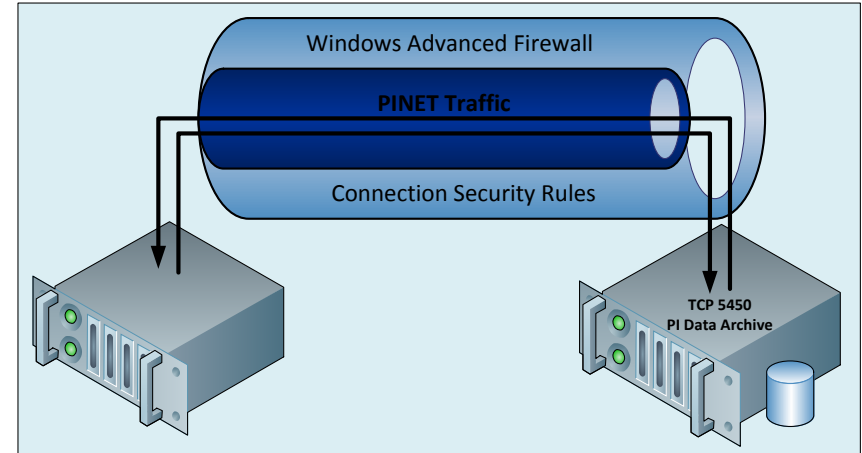
PI Server Version SDL Defense		PR1 3.4.375.38	WIS 3.4.380.36	2010 3.4.385	2012 3.4.390
Code	Pointer Encoding				Future
	/Analyze				Adhoc
	Heap corruption detection				100%
	Safe function migration				80%
Linker	SEHOP (*)	Win 2008+	Win 2008+	Win 2008+	Win 2008+
	/SAFESEH (*)	100%	100%	100%	100%
	/DYNAMICBASE (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

IT Security Baselines

Microsoft
Security Compliance
Manager (SCM) 3.0

Solution
Accelerators

- ✓ Microsoft Products
- ✓ Free [Download](#)



- ✓ NIST + FISMA
- ✓ Multi-Platform + Device
- ✓ Free and Government Only [Download](#)

 **Security
Benchmarks™**
A DIVISION OF  **CENTER FOR
INTERNET SECURITY**

- ✓ Multi-Platform + Device
- ✓ Limited Free [Download](#)
- ✓ Subscription Model*
- ✓ Hardened Virtual Images*

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
07:30 - 08:00 PM	ANSWER BAR SOLD OUT
	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

Cyber Challenges



Hardened Image Challenge Series

Project “Hard Rock PI”

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



Hardening Features in “ACDC”

Development

- Windows Server 2012 R2
- PI Coresight 2013
- PI Server 2012

Deployment

- Whitelisting
- Configuration
- Security Tools

Secure by
Design

Secure by
Default

Secure in
Deployment

ALL
ITEMSCLOUD SERVICES
2SQL DATABASES
1STORAGE
1

all items

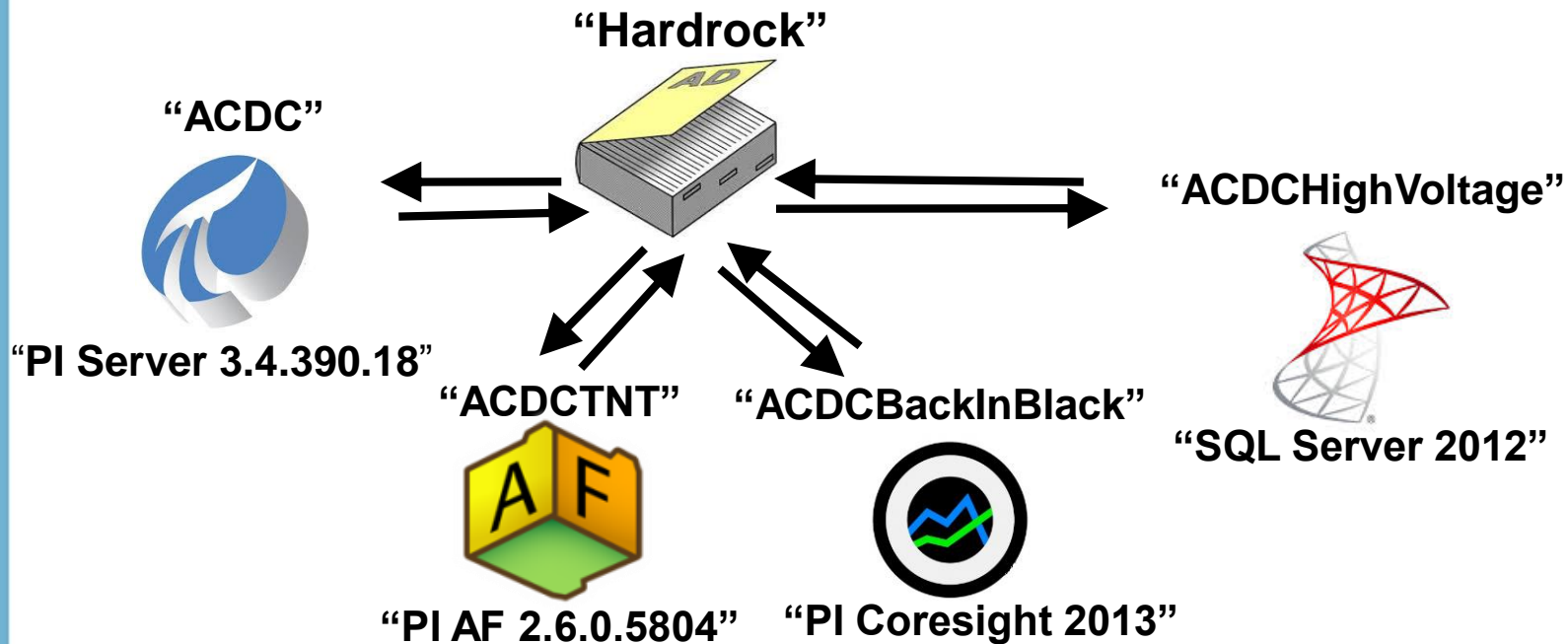
NAME

TYPE

STATUS

SUBSCRIPTION

LOCATION



NEW



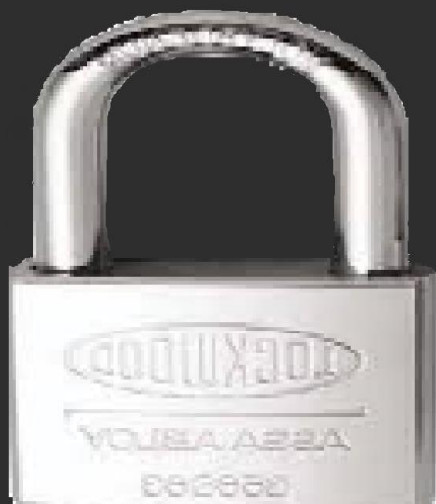
Securing PI Coresight with SSL certificates


1. Open IIS and click on your Web Server name
2. Open “Server certificates”
3. Import the “Personal Information Exchange” certificate and place it in the web hosting store
4. Select the newly imported certificate in the PI Coresight website bindings





Recycle Bin



 Windows Server 2012 R2

Windows Server 2012 R2 Datacenter Preview

Evaluation copy. Build 9431

6/25/2013



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

Whitelisting with Applocker

- Run only approved files
 - By user or group
- Rules based on:
 - ✓ Publisher
 - ✓ Path
 - ✓ File hash
- Action modes
 - ✓ Audit only
 - ✓ Enforce allow or deny

Allow Properties

General Publisher Exceptions

Edit the values below to modify the scope of this rule.

Publisher:
P=OSISOFT, LLC, L=SAN LEANDRO, S=CALIFORNIA, C=US

Product name:
*

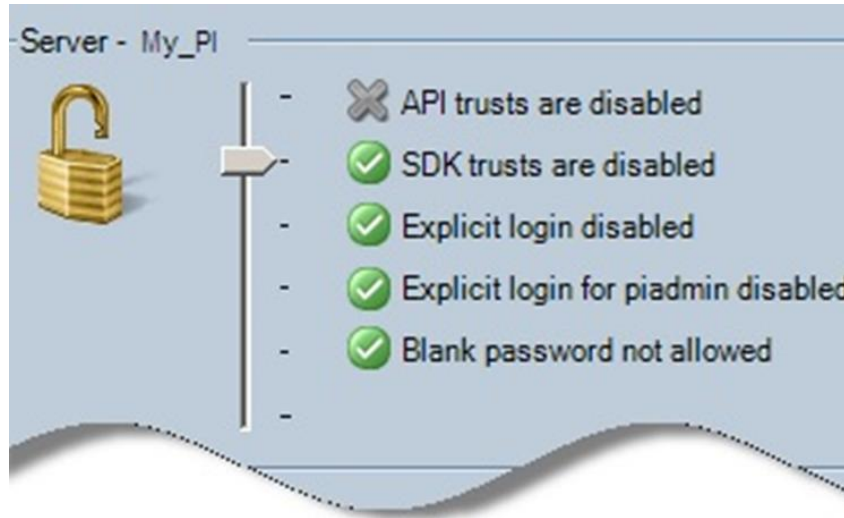
File name:
*

File version:
* And above

[More about publisher rules](#)





OK Cancel Apply

PI Server Authentication Policy



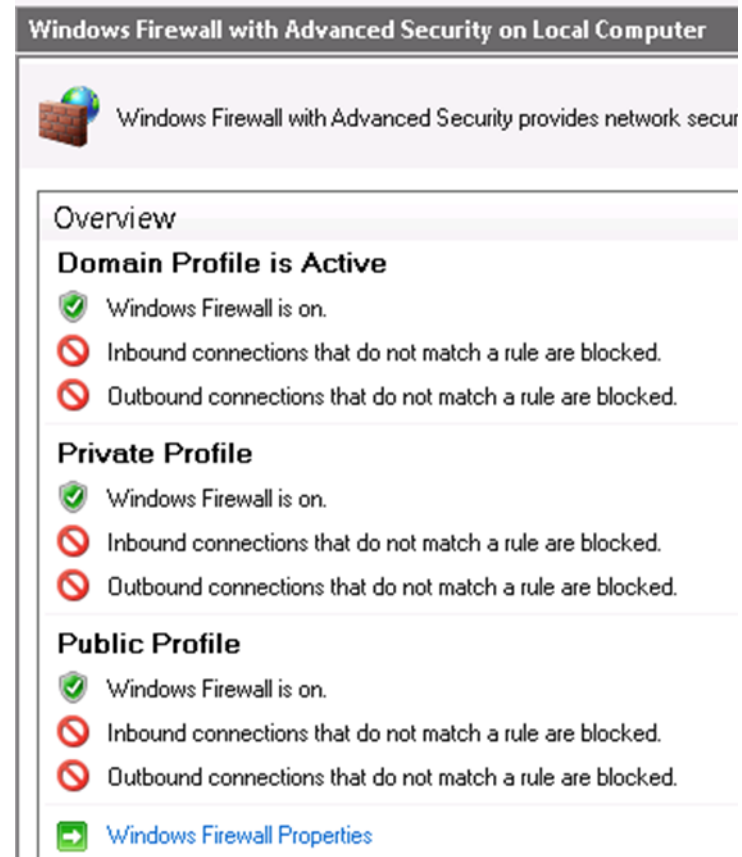
PISYSAUDIT Configuration Baseline

- 16 Critical checks
 - Windows Server
 - PI Server
 - PI AF Server
 - SQL Server

AuditItemName	AuditItemValue	Severity	
Domain Membership Check	Pass	Severe	
Domain Membership Check	Pass	Severe	
Domain Membership Check	Pass	Severe	
Operating System SKU	Fail	Severe	
Operating System SKU	Fail	Severe	
Operating System SKU	Fail	Severe	
Firewall Enabled	Fail	Moderate	
Firewall Enabled	Pass	Moderate	
Firewall Enabled	Fail	Moderate	
PI Data Archive Table Security	Pass	Moderate	
PI Admin Trusts Disabled	Pass	Severe	
PI Server SubSystem Versions	Pass	Severe	
Edit Days	Pass	Severe	
Auto Trust Configuration	Pass	Severe	
Expensive Query Protection	Pass	Severe	
Configured Account Check	Pass	Severe	
Impersonation mode for AF Data Sets	Pass	Low	
PI AF Server Service privileges	Pass	Severe	
SQL Server xp_cmdshell Check	Pass	Severe	
SQL Server Adhoc Queries Check	Pass	Severe	
SQL Server DB Mail XPs Check	Pass	Severe	
SQL Server OLE Automation Procedures Check	Pass	Severe	

Windows Firewall

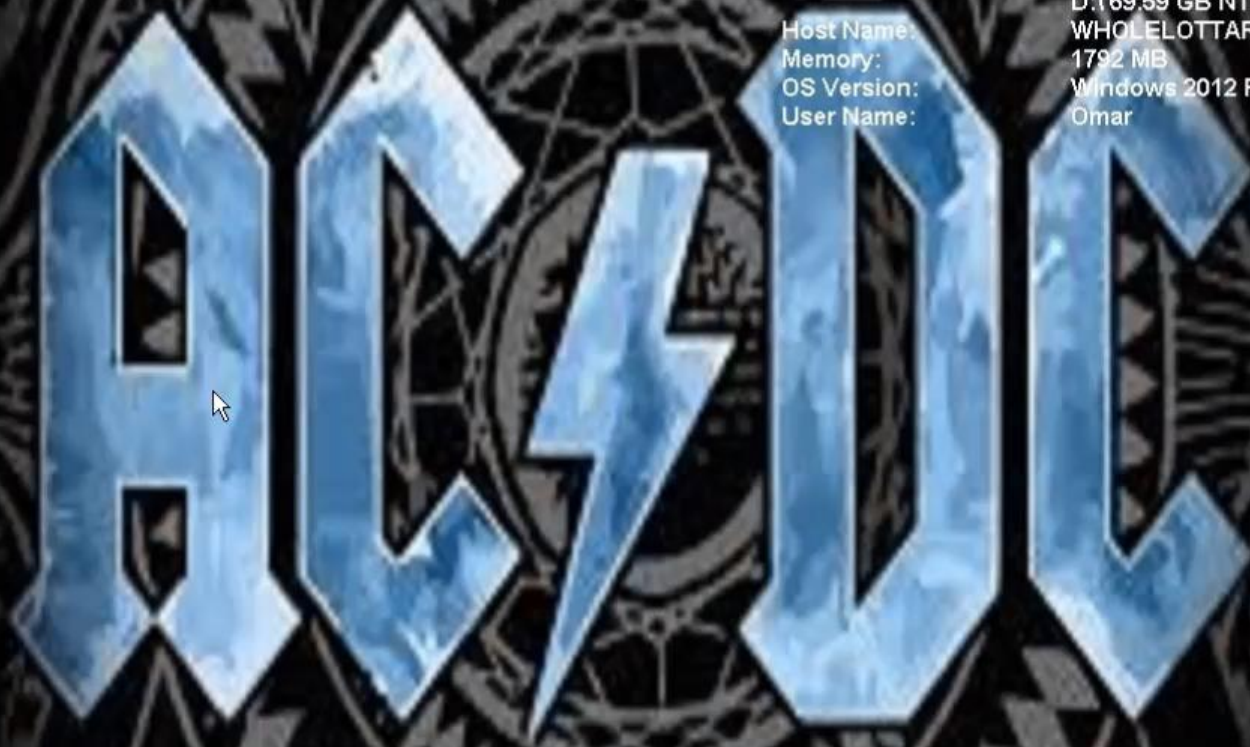
- Control inbound and outbound network traffic
- Connection security rules



Securing the network with IPsec

1. Open “Windows Firewall with Advanced security”
2. Open “Connection security rules” and create a new connection security rule
3. Create a new inbound rule for port 5450 and choose “Allow the connection if it is secure”
4. Add more restrictions such as allowing only specific users and computers

Internal IP: 192.168.96.8
Public IP: 65.52.115.6
Boot Time: 9/12/2014 12:50 PM
Free Space: C:\ 116.06 GB NTFS
D:\ 69.59 GB NTFS
Host Name: WHOLELOTTAROSIE
Memory: 1792 MB
OS Version: Windows 2012 R2
User Name: Omar



Windows Security Tools

1. Security Compliance Manager (SCM)
2. Microsoft Security Baseline Analyzer (MBSA)
3. Enhanced Mitigation Experience Toolkit (EMET)

1. Security Compliance Manager

- Baseline configuration database and tools
 - Microsoft recommendations
 - Industry best practices
 - Guide documents and attack surface reports
- Group policy objects
 - Customize baseline settings
 - Import and export capability

Name	Default	Microsoft	Customized	Severity
^ Protocol Configuration 50 Setting(s)				
Domain controller: LDAP server signing requirements	Not defined	Not Defined	Not Defined	Critical
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled	Enabled	Critical
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled	Enabled	Critical
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled	Enabled	Critical
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Enabled	Enabled	Critical
Interactive logon: Number of previous logons to cache (in case domain controller is n	10 logons	4 logon(s)	4 logon(s)	Critical
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Disabled	Disabled	Critical
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled	Enabled	Critical
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled	Enabled	Critical
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled	Critical
Microsoft network server: Digitally sign communications (always)	Disabled	Enabled	Enabled	Critical

[Collapse](#)

Severity: Critical
[Customize this setting by duplicating the baseline](#)

Value must be equal to Enabled.

Customize setting value Enabled

Comments:








▼ Setting Details

2. Microsoft Baseline Security Analyzer

- Checks for missing security updates and common configuration issues
 - Operating System
 - SQL Server
 - Web Server

Instance MICROSOFTSCM

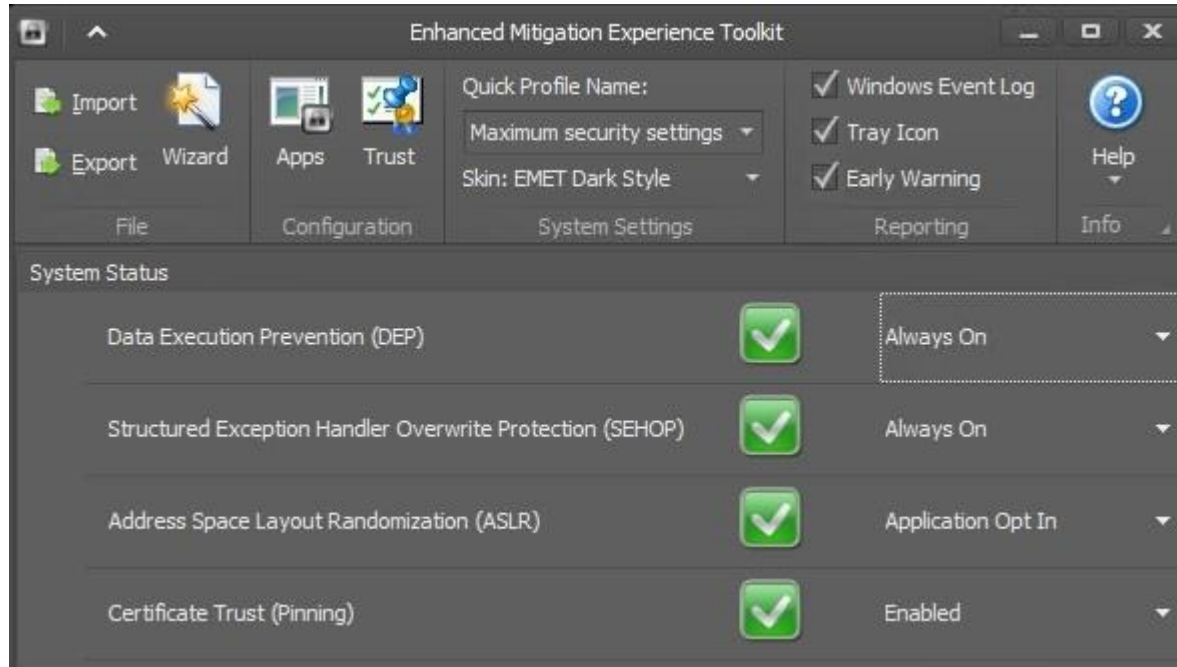
Administrative Vulnerabilities

Score	Issue	Result
	Guest Account	The Guest account is not enabled in any of the databases. What was scanned
	Folder Permissions	What was scanned Result details
	CmdExec role	CmdExec is restricted to sysadmin only. What was scanned
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys. What was scanned
	Domain Controller Test	SQL Server and/or MSDE is not running on a domain controller. What was scanned
	Sysdtstlog	Sysdtstlogs90 table does not exist in the Master or MSDB databases What was scanned
	SSIS Roles	The BUILTIN Admin does not belong to the SSIS roles.

3. Enhanced Mitigation Experience Toolkit (EMET v5.0)

- Microsoft ‘bolt-on’ tool for Windows
 - supports management with group policy
- Guards common memory corruption exploits
 - DEP, ASLR, SEHOP
 - EAF, return-oriented programming
- “certificate trust” feature

It's ok to enable EMET with PI System.

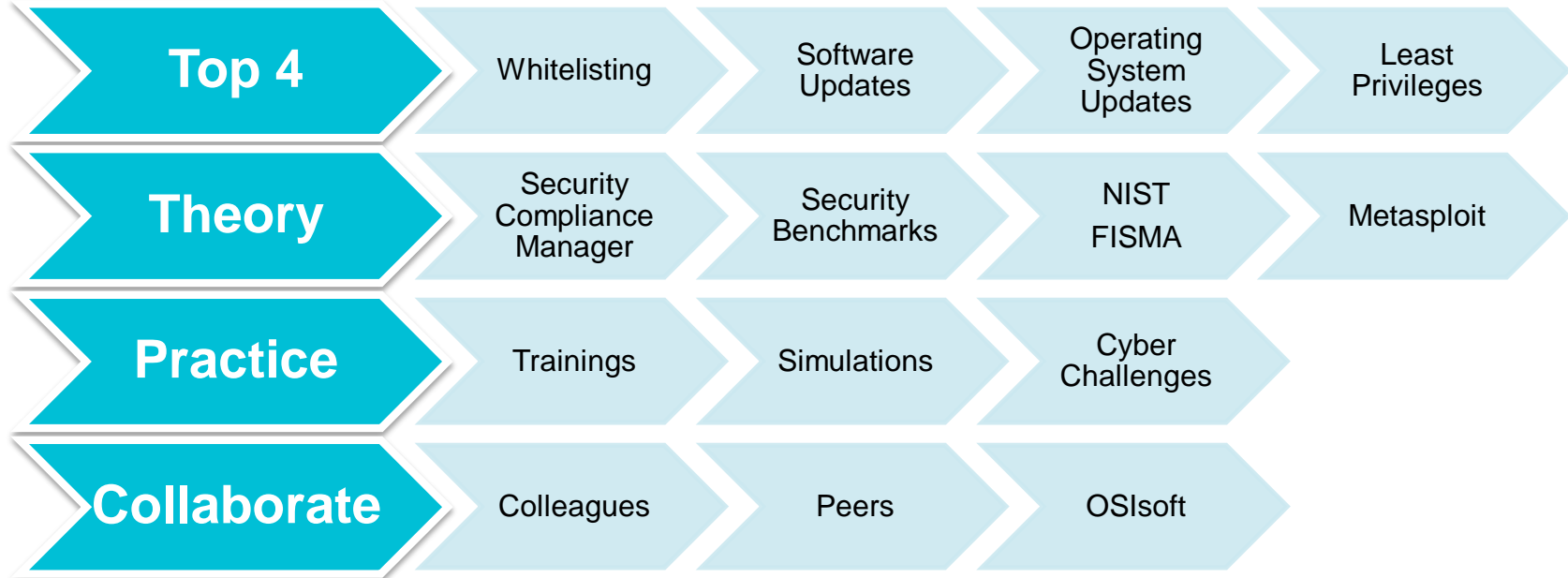


Process Name	Running EMET
pialarm - PI Alarm Subsystem	✓
piarchss - PI Archive Subsystem	✓
pibackup - PI Backup Subsystem	✓
pibasess - PI Base Subsystem	✓
pibatch - PI Batch Subsystem	✓
pilicmgr - PI License Manager	✓
pilogsrv - PI log server	✓
pilogsrv - PI log server	✓
pimsgss - PI Message Subsystem	✓
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	✓

My takeaways from the Hard Rock PI

- Cyber security became a passion
- Helped me in protecting myself against Cyber attack
- Improved my field service experience

Summary



Summary

**Learn
More**



Vadim Sizykh

vsizykh@osisoft.com

Systems Engineer,
Russia

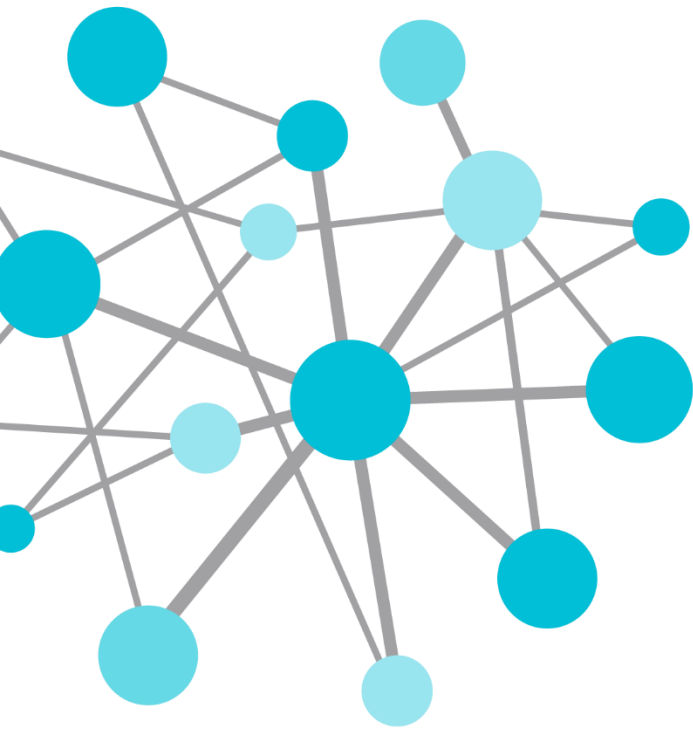
OSIsoft, LLC

Omar Mohsen

omohsen@osisoft.com

Computer Software
Specialist, Bahrain

OSIsoft, LLC



Questions

Bryan Owen bowen@osisoft.com

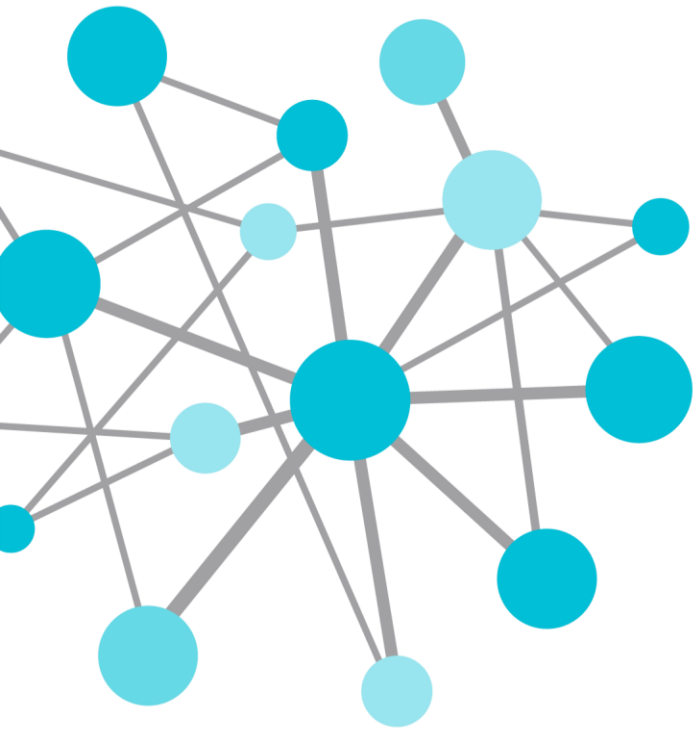
Principal Cyber Security Manager

Jim Davidson jdavidson@osisoft.com

Principal Cyber Security Advisor

Mike Lemley mlemley@osisoft.com

Senior Cyber Security Developer



THANK
YOU

Brought to you by  **OSI**soft.

Please don't forget to...

Complete the online survey for
this session

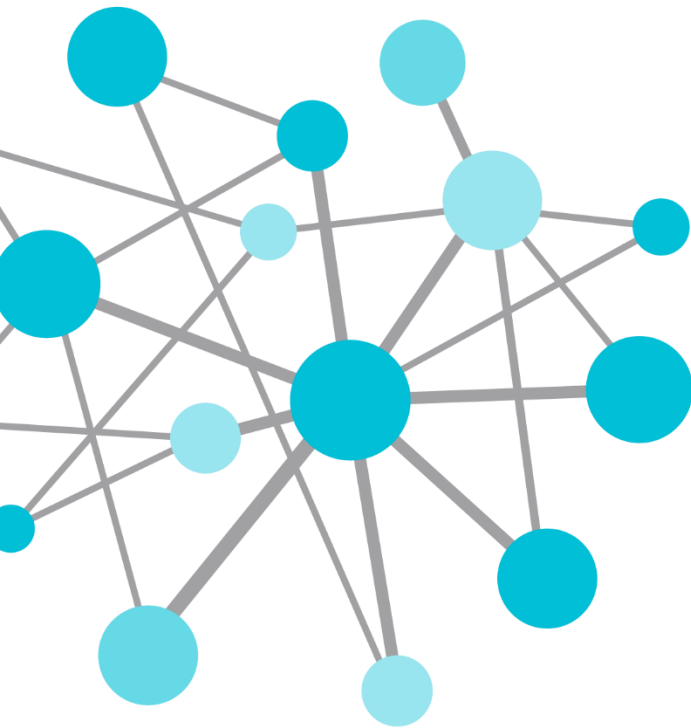
eventmobi.com/emeauc14



Share with your friends

#UC2014





References

Technical Support

KB00354 - Windows Security Requirements for PI Server

KB00833 - Seven best practices for securing your PI Server

KB00994 - Whitelisting with AppLocker

KB01062 - Anti-virus Software and the PI System

OSIsoft Users Community → Forums → Cyber Security

PISysAudit - Introduction of a new security tool

vCampus → Downloads → Extras

Live 2012 Hands-on Labs:

Security for PI System Admins

Whitelisting, Firewalls, & Windows Core

Live 2013 Hands-on Labs:

Securing PI Interfaces

Users Conference 2013

WECC Reliability Coordination:

Security Baseline and Configuration Management