Hardcore PI System Hardening

Jozef Sujan, Lubos Mlcoch

Agenda

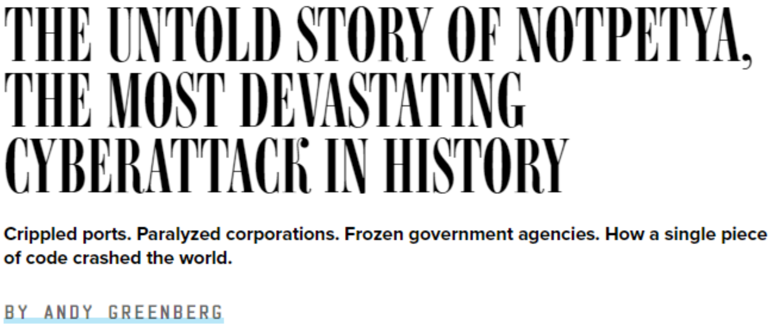
1. No-nonsense approach to Cyber Security

2. The Power of ... PowerShell

3. Deadly Sins of PI Administrators

Note: All examples in this presentation are available on GitHub
https://gist.github.com/hpaul-osi/011257c57a0fd9228bca9e0f1dde23f6

WannaCry about NotPetya



THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

BY ANDY GREENBERG

Three Laws of SCADA Security

1. Nothing is secure

2. All software can be hacked

3. Every piece of information can be an attack

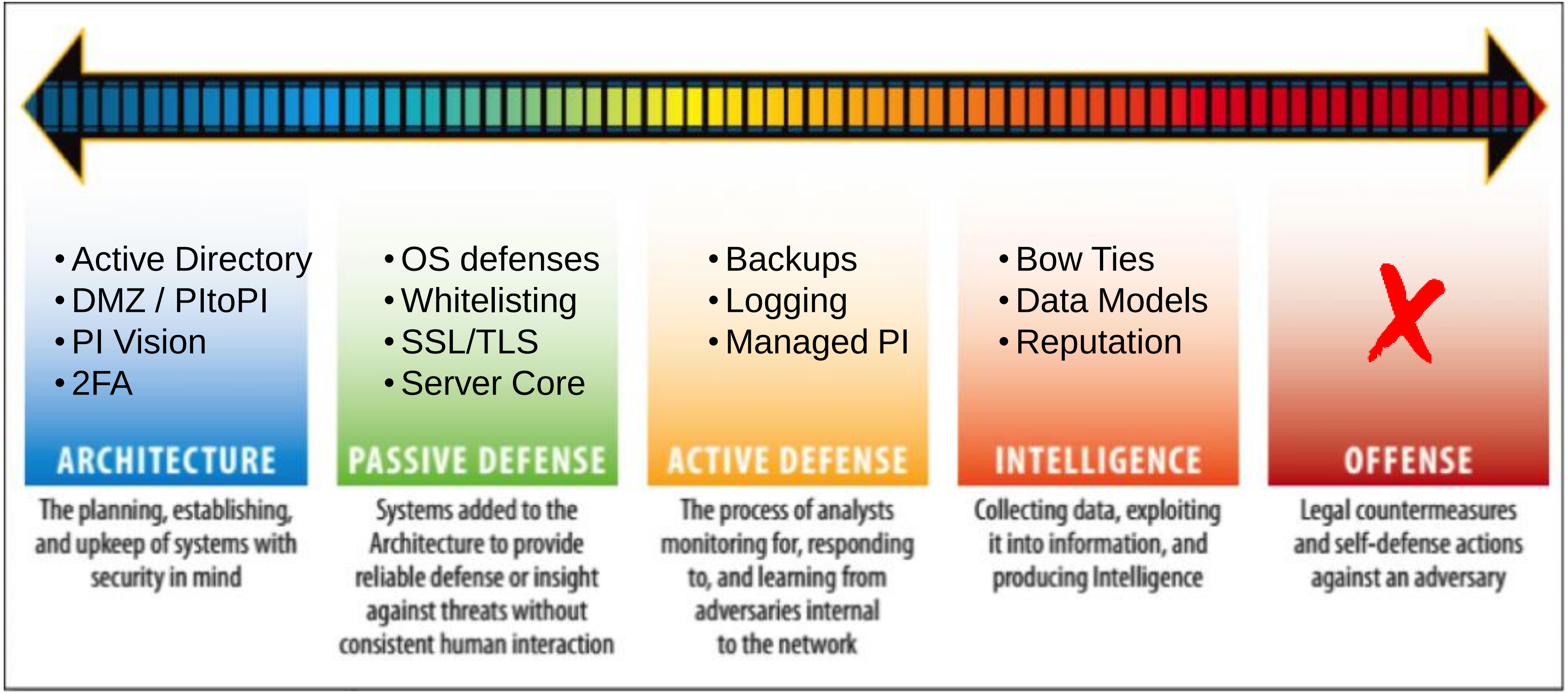
Ginter, Andrew (2016) *SCADA Security: What's broken and how to fix it.* Calgary: Abterra

Threat Spectrum

Threat	Resources	Attacks
Nation States Military Grade	Nearly Unlimited	Autonomous Targeted Malware
Intelligence Agencies	Professional	Remote Control 0-Day Vulnerabilities
Hacktivists	Skilled Amateur	Remote Control Exploit Permissions
SCADA Insiders	Amateur	Exploit Permissions
Organized Crime	Professional	Malware Known vulnerabilities
Corporate Insiders	Amateur	Exploit Permissions

Ginter, Andrew (2016) *SCADA Security: What's broken and how to fix it.* Calgary: Abterra

SANS ‘Sliding Scale’: Built-in vs Bolt-on defenses



- Active Directory
- DMZ / PItoPI
- PI Vision
- 2FA

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

- OS defenses
- Whitelisting
- SSL/TLS
- Server Core

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

- Backups
- Logging
- Managed PI

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

- Bow Ties
- Data Models
- Reputation

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

✗

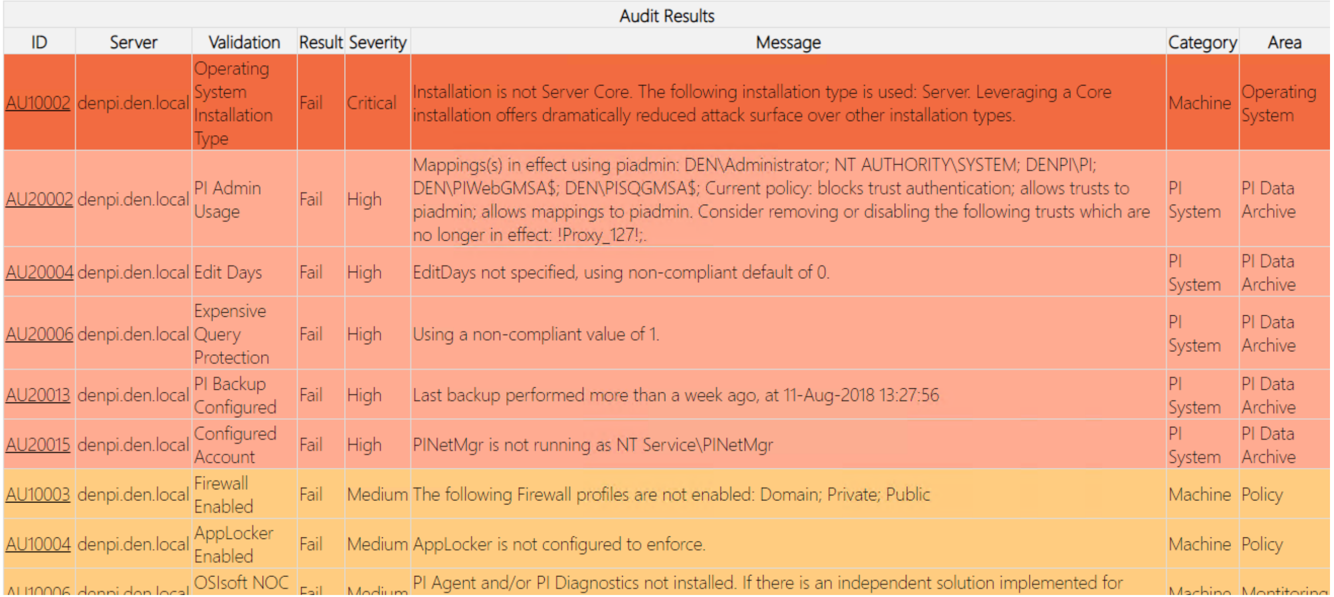
OFFENSE

Legal countermeasures and self-defense actions against an adversary

PI Security Audit Tools

Checks configuration of:

- Machine itself
- PI Data Archive Server
- PI Asset Framework Server
- PI Vision
- PI Web API
- MS SQL Server



Audit Results

ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	denpi.den.local	Operating System Installation Type	Fail	Critical	Installation is not Server Core. The following installation type is used: Server. Leveraging a Core installation offers dramatically reduced attack surface over other installation types.	Machine	Operating System
AU20002	denpi.den.local	PI Admin Usage	Fail	High	Mappings(s) in effect using piadmin: DEN\Administrator; NT AUTHORITY\SYSTEM; DENPI\PI; DEN\PIWebGMSA$; DEN\PISQGMSA$; Current policy: blocks trust authentication; allows trusts to piadmin; allows mappings to piadmin. Consider removing or disabling the following trusts which are no longer in effect: !Proxy_127!;.	PI System	PI Data Archive
AU20004	denpi.den.local	Edit Days	Fail	High	EditDays not specified, using non-compliant default of 0.	PI System	PI Data Archive
AU20006	denpi.den.local	Expensive Query Protection	Fail	High	Using a non-compliant value of 1.	PI System	PI Data Archive
AU20013	denpi.den.local	PI Backup Configured	Fail	High	Last backup performed more than a week ago, at 11-Aug-2018 13:27:56	PI System	PI Data Archive
AU20015	denpi.den.local	Configured Account	Fail	High	PINetMgr is not running as NT Service\PINetMgr	PI System	PI Data Archive
AU10003	denpi.den.local	Firewall Enabled	Fail	Medium	The following Firewall profiles are not enabled: Domain; Private; Public	Machine	Policy
AU10004	denpi.den.local	AppLocker Enabled	Fail	Medium	AppLocker is not configured to enforce.	Machine	Policy
AU10006	denpi.den.local	OSIsoft NOC	Fail	Medium	PI Agent and/or PI Diagnostics not installed. If there is an independent solution implemented for	Machine	Monitoring

PI Security Audit Tools Requirements

- PowerShell version 3+
- OSIsoft.PowerShell module (bundled with PI SMT)

- ‘Run As’ Admin (PI AF and PI Vision checks)
- WinRM enabled (for remote audits)

GitHub Wiki
https://github.com/osisoft/PI-Security-Audit-Tools/wiki

DEMO

PI Security Audit Tools

Powershell DSC

DSC = Desired State Configuration

Principle of Configuration As Code

- **Separation of intent from execution**
  - Decreased complexity
  - Increased agility
  - Consistency across the board
  - Documentation
- **Broad scope**
  - Baseline configuration
  - Hardening
  - Targeted control

PowerShell DSC - Components

- **Configuration** – declarative script (ps1 file) which defines and configures **Resources**
  - *Typically created or modified by end-users (PI Admins ..)*

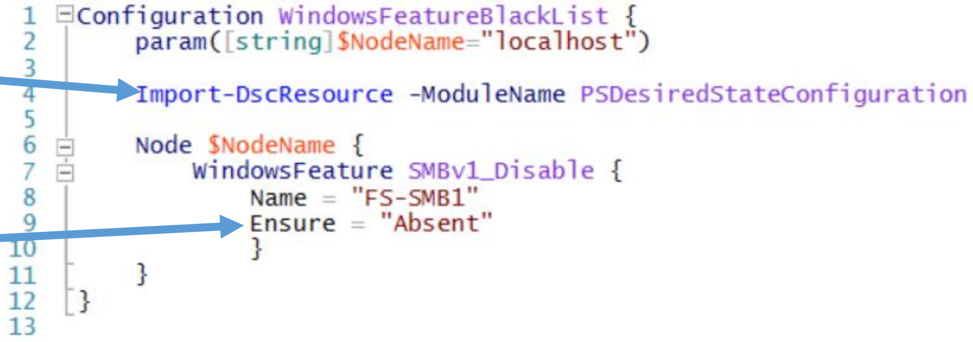
- **Resource** – lightweight component (psm1 file) containing code to Get, Set or Test properties of an item from a **Configuration**
  - *Typically provided to end-users by 3rd party (Microsoft, OSIsoft ..)*

- **Local Configuration Manager (LCM)** – engine that facilitates interaction between **Configurations** and **Resources**.

Example: Windows Feature Blacklist

Built-in resource to manipulate features

Ensure that it is removed if Present



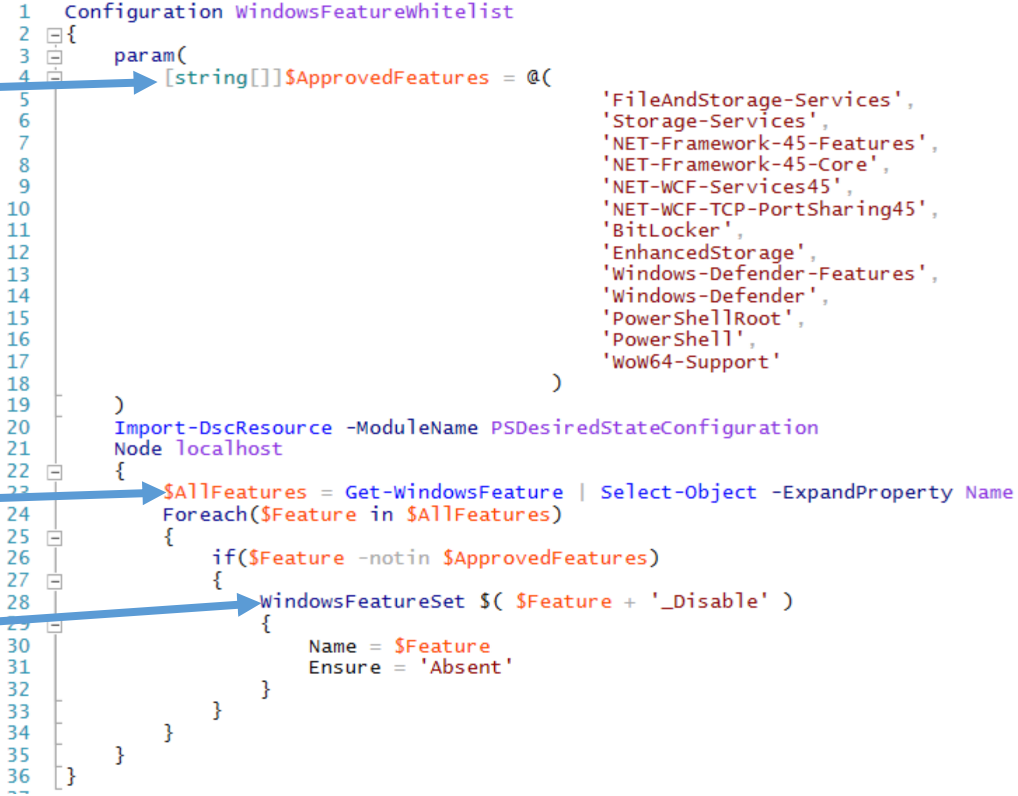
```
Configuration WindowsFeatureBlackList {
    param([string]$NodeName="localhost")

    Import-DscResource -ModuleName PSDesiredStateConfiguration

    Node $NodeName {
        WindowsFeature SMBv1_Disable {
            Name = "FS-SMB1"
            Ensure = "Absent"
        }
    }
}

```

Example: Windows Feature Whitelist

Specify whitelist of approved services

Retrieve all available features

Remove any features not on the list



```
Configuration WindowsFeatureWhitelist
{
    param(
        [string[]]$ApprovedFeatures = @(
                                            'FileAndStorage-Services',
                                            'Storage-Services',
                                            'NET-Framework-45-Features',
                                            'NET-Framework-45-Core',
                                            'NET-WCF-Services45',
                                            'NET-WCF-TCP-PortSharing45',
                                            'BitLocker',
                                            'EnhancedStorage',
                                            'Windows-Defender-Features',
                                            'Windows-Defender',
                                            'PowerShellRoot',
                                            'PowerShell',
                                            'WoW64-Support'
                                        )
    )
    Import-DscResource -ModuleName PSDesiredStateConfiguration
    Node localhost
    {
        $AllFeatures = Get-WindowsFeature | Select-Object -ExpandProperty Name
        Foreach($Feature in $AllFeatures)
        {
            if($Feature -notin $ApprovedFeatures)
            {
                WindowsFeatureSet $( $Feature + '_Disable' )
                {
                    Name = $Feature
                    Ensure = 'Absent'
                }
            }
        }
    }
}
```

DEMO

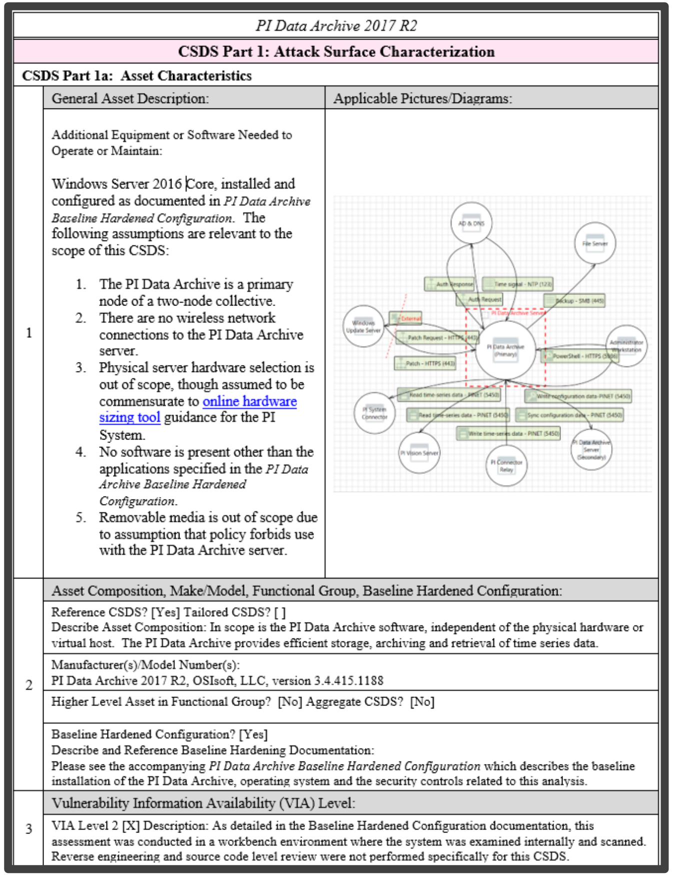
DSC Demo – applying Microsoft Baseline

DEMO

DSC Demo – applying PI DA FSTS

Cyber Security Data Sheet

- Structured Security Documentation
- Forward looking
  - Modern Platform
  - Recommended Architecture
- Supplemental Configuration Document/Tools
  - Verification via Configuration as Code
  - Open source on GitHub



PI Data Archive 2017 R2

CSDS Part 1: Attack Surface Characterization

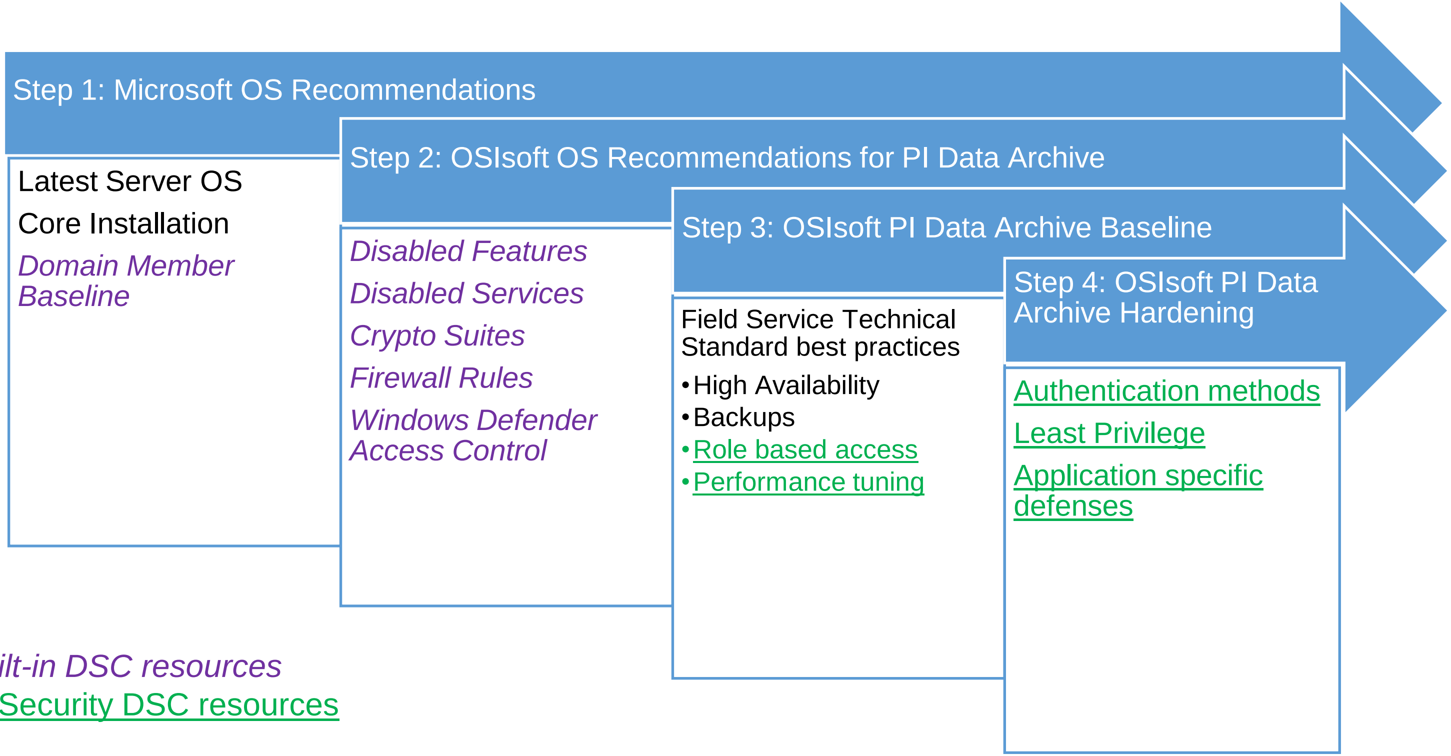
CSDS Part 1a: Asset Characteristics

	General Asset Description:	Applicable Pictures/Diagrams:
1	Additional Equipment or Software Needed to Operate or Maintain: Windows Server 2016 Core, installed and configured as documented in *PI Data Archive Baseline Hardened Configuration*. The following assumptions are relevant to the scope of this CSDS: 1. The PI Data Archive is a primary node of a two-node collective. 2. There are no wireless network connections to the PI Data Archive server. 3. Physical server hardware selection is out of scope, though assumed to be commensurate to online hardware sizing tool guidance for the PI System. 4. No software is present other than the applications specified in the *PI Data Archive Baseline Hardened Configuration*. 5. Removable media is out of scope due to assumption that policy forbids use with the PI Data Archive server.	

AD & DNS
File Server
Auth Response
Time signal - NTP (123)
Auth Request
Backup - SMB (445)
PI Data Archive Server
External
Windows Update Server
Patch Request - HTTPS (443)
PI Data Archive (Primary)
Administrator Workstation
PowerShell - HTTPS (5986)
Patch - HTTPS (443)
Read time-series data - PINET (5450)
Write configuration data-PINET (5450)
PI System Connector
Read time-series data - PINET (5450)
Sync configuration data - PINET (5450)
Write time-series data - PINET (5450)
PI Vision Server
PI Connector Relay
PI Data Archive Server (Secondary)

2	Asset Composition, Make/Model, Functional Group, Baseline Hardened Configuration:
	Reference CSDS? [Yes] Tailored CSDS? [ ] Describe Asset Composition: In scope is the PI Data Archive software, independent of the physical hardware or virtual host. The PI Data Archive provides efficient storage, archiving and retrieval of time series data.
	Manufacturer(s)/Model Number(s): PI Data Archive 2017 R2, OSIsoft, LLC, version 3.4.415.1188
	Higher Level Asset in Functional Group? [No] Aggregate CSDS? [No]
	Baseline Hardened Configuration? [Yes] Describe and Reference Baseline Hardening Documentation: Please see the accompanying *PI Data Archive Baseline Hardened Configuration* which describes the baseline installation of the PI Data Archive, operating system and the security controls related to this analysis.
3	Vulnerability Information Availability (VIA) Level:
	VIA Level 2 [X] Description: As detailed in the Baseline Hardened Configuration documentation, this assessment was conducted in a workbench environment where the system was examined internally and scanned. Reverse engineering and source code level review were not performed specifically for this CSDS.

Build a Hardened Baseline Automatically with DSC



Step 1: Microsoft OS Recommendations

Latest Server OS

Core Installation

Domain Member Baseline

Step 2: OSIsoft OS Recommendations for PI Data Archive

Disabled Features

Disabled Services

Crypto Suites

Firewall Rules

Windows Defender Access Control

Step 3: OSIsoft PI Data Archive Baseline

Field Service Technical Standard best practices

- High Availability
- Backups
- Role based access
- Performance tuning

Step 4: OSIsoft PI Data Archive Hardening

Authentication methods

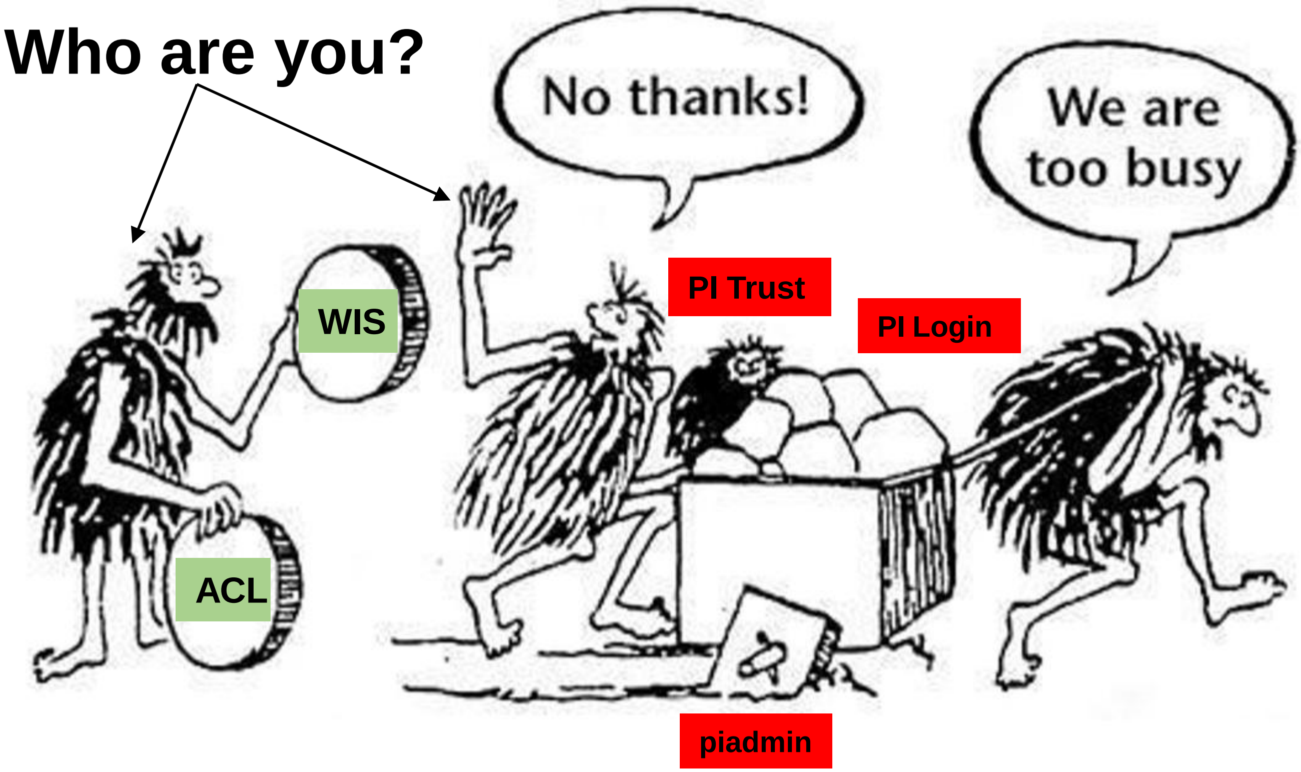
Least Privilege

Application specific defenses

Enabled with Built-in DSC resources

Enabled with PI Security DSC resources

Deadly sins of PI Administrators

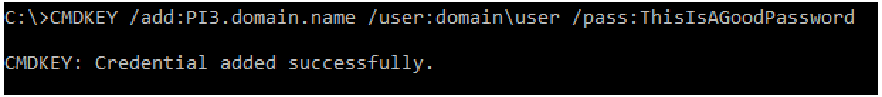


MYTH #1:
PI Mappings cannot be used in a workgroup

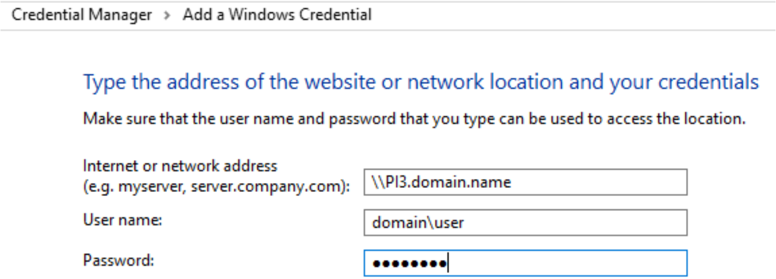
TRUTH: Applications can use PI Mappings between untrusted domains or workgroup machines.

KB01457 – Using Windows Credential Manager with PI Applications

Configurable via CMD and Credential Manager App



```
C:\>CMDKEY /add:PI3.domain.name /user:domain\user /pass:ThisIsAGoodPassword

CMDKEY: Credential added successfully.
```



Type the address of the website or network location and your credentials

Make sure that the user name and password that you type can be used to access the location.

Internet or network address (e.g. myserver, server.company.com): \\PI3.domain.name

User name: domain\user

Password: ●●●●●●●●

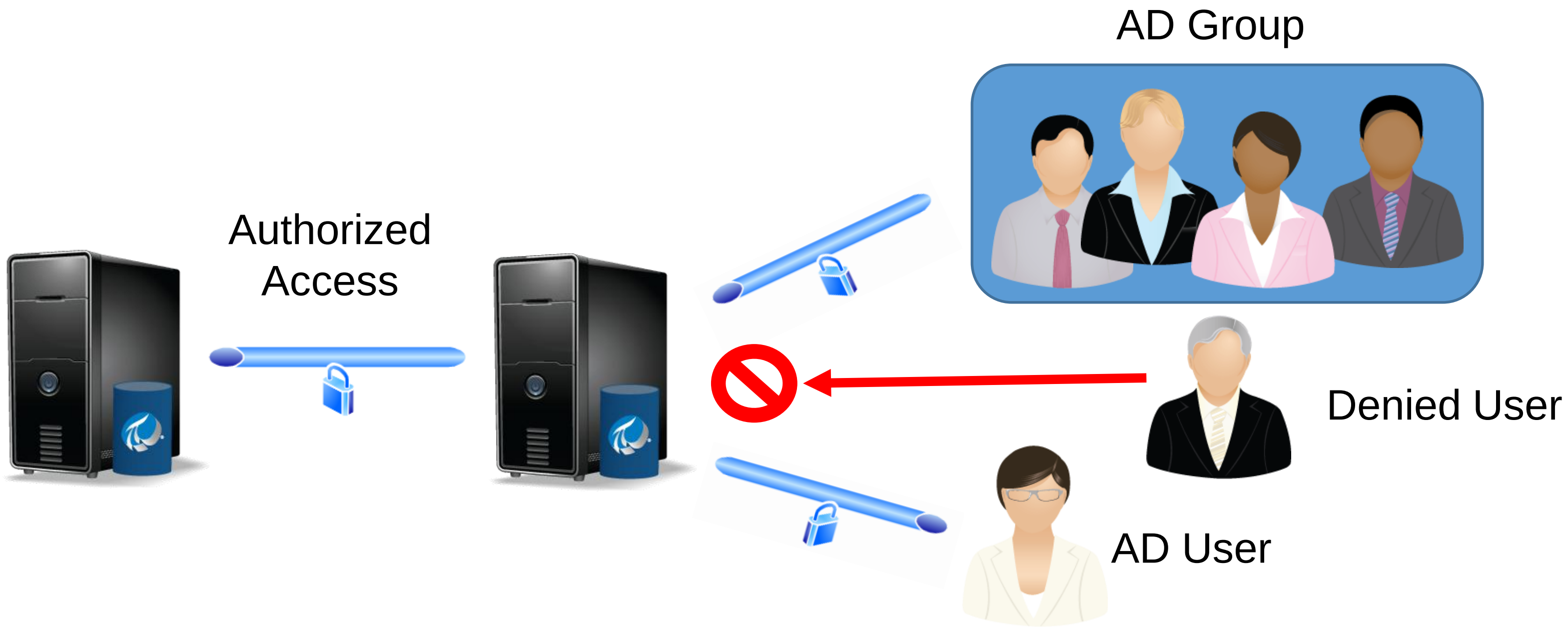
MYTH #2:
PI Mappings require more open ports than PI Trusts

TRUTH: No additional ports are required to migrate from trusts to mappings.

2820OSI8 – Which firewall ports should be opened for a PI Data Archive.

Less work for administrators

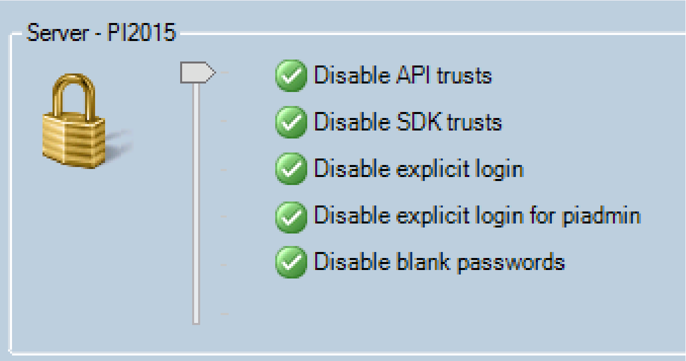
Leverage standard platform technologies: Active Directory and Windows Integrated Security provides SSO and Identity and Access Management.



Strong Authentication

PI User and **PI Trust** authentication are **weak**.

- AL00206 – Security Alert:
  PI Authentication Weakness
- AL00309 –WIS replaces PI Trusts and Explicit Logins in PI API 2016



Server - PI2015

✓ Disable API trusts

✓ Disable SDK trusts

✓ Disable explicit login

✓ Disable explicit login for piadmin

✓ Disable blank passwords

PI Mappings – strong authentication

- Connections authenticated through Windows SSPI
- Kerberos

Transport Security

- Enabled automatically for WIS connections

- Messages signed for integrity and encrypted for privacy

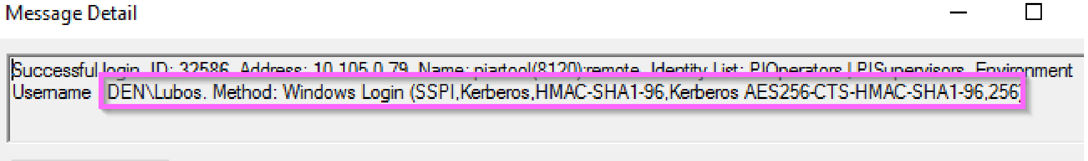
- Supported with PI Data Archive 2015+ with the connecting client:
  - PI Buffer Subsystem 4.4 or later
  - PI AF SDK 2015 or later
  - PI SDK 2016 or later
  - PI API 2016 for WIS

Audit Connections

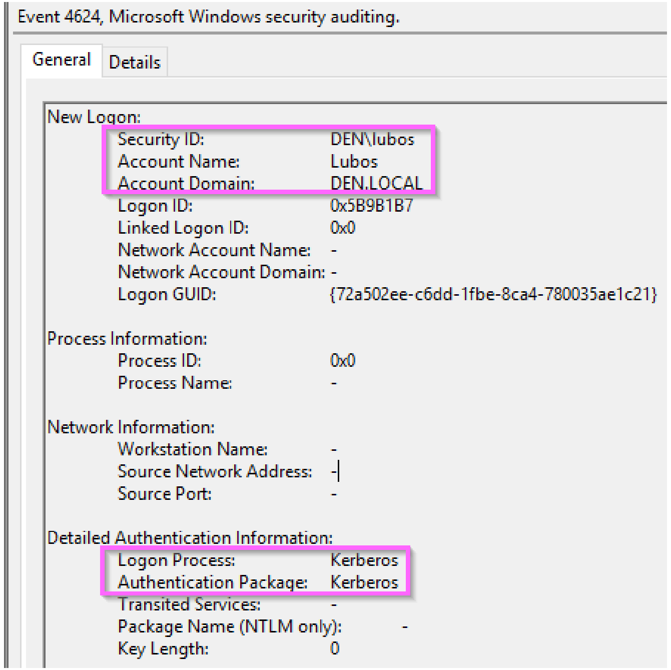
- Built-in connection auditing using Security event logs

- PI Message Logs provide connection auditing (Message ID: **7082**)

- PI Data Archive connection history

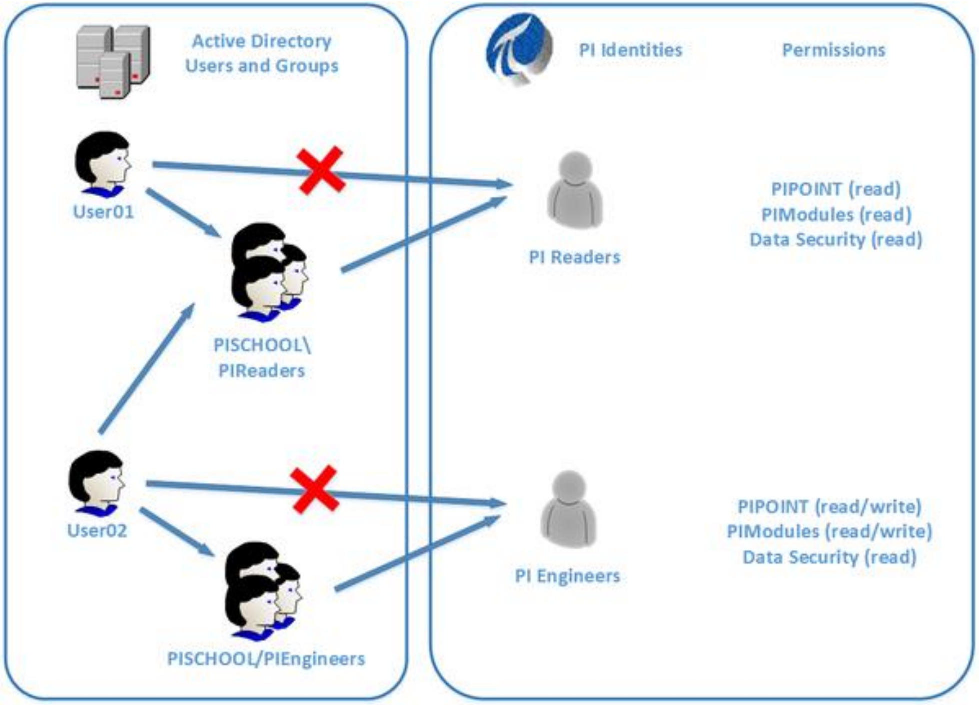


```
Successful login. ID: 32586. Address: 10.105.0.79. Name: piartool(8120):remote. Identity List: PIOperators | PISupervisors. Environment
Username DEN\Lubos. Method: Windows Login (SSPI,Kerberos,HMAC-SHA1-96,Kerberos AES256-CTS-HMAC-SHA1-96,256)
```



```
Event 4624, Microsoft Windows security auditing.

New Logon:
        Security ID:                DEN\lubos
        Account Name:               Lubos
        Account Domain:             DEN.LOCAL
        Logon ID:                   0x5B9B1B7
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {72a502ee-c6dd-1fbe-8ca4-780035ae1c21}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           -
        Source Network Address:     -
        Source Port:                -

Detailed Authentication Information:
        Logon Process:              Kerberos
        Authentication Package:     Kerberos
        Transited Services:         -
        Package Name (NTLM only):         -
        Key Length:                 0
```

WIS Flexibility

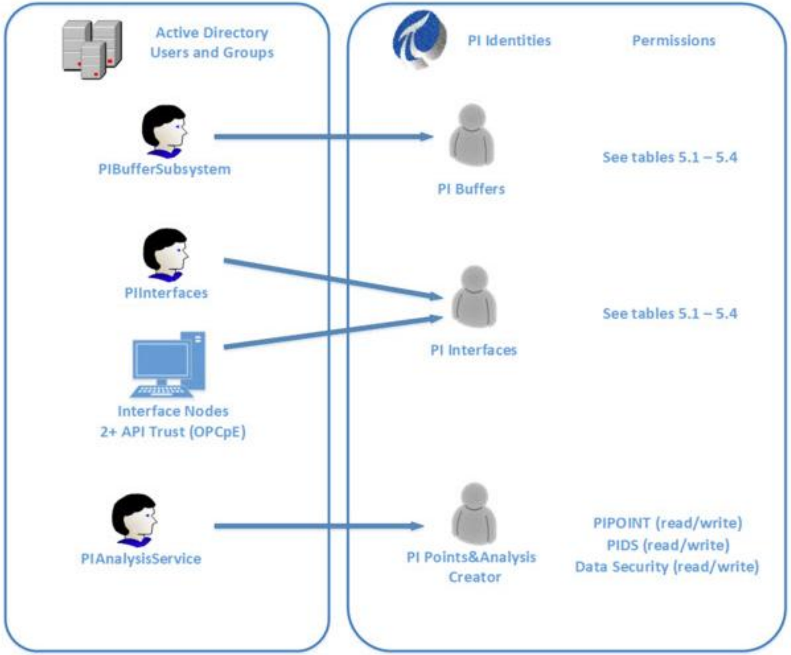


- Create Identities and Mappings based on **Least Privilege**
- Use **piadmins** for normal admin role
  - Reserve piadmin for disaster recovery

WIS Best Practices

Practical Access Levels

- Administrator
- PI Interfaces
- PI Buffers
- PI Users
- PI Point and Analysis creator
- PI Web Apps



Codified in KB01072

Contact Information

Jozef Sujan
jozef@osisoft.com
Regional Services Lead
OSIsoft, LLC

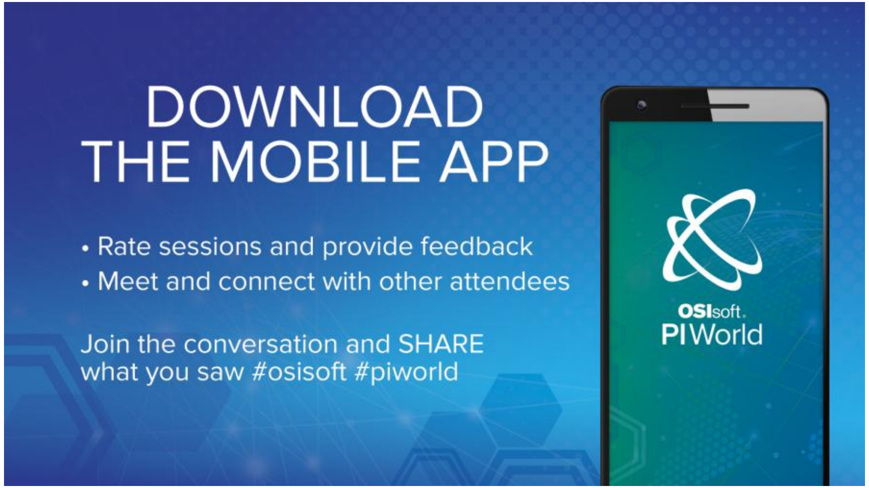
Lubos Mlcoch
lmlcoch@osisoft.com
Technical Support
OSIsoft, LLC

Questions?

Please wait for the **microphone**

State your **name & company**

Please rate this session in the mobile app!



DOWNLOAD THE MOBILE APP

- Rate sessions and provide feedback
- Meet and connect with other attendees

Join the conversation and SHARE what you saw #osisoft #piworld

Download on the App Store

GET IT ON Google Play

謝謝 KEA LEBOHA

DZIĘKUJĘ CI TAPADH LEIBH 고맙습니다

NGIYABONGA GRÀCIES БАЯРЛАЛАА MISAOTRA ANAO SALAMAT

TEŞEKKÜR EDERIM OBRIGADO شكرا

KÖSZÖNÖM DANKIE TERIMA KASIH DANKON TANK TAPADH LEAT

СПАСИБО MULȚUMESC

РАКМЕТ СІЗГЕ OSIsoft PI World HVALA FAAFETAI

GO RAIBH MAITH AGAT ESKERRIK ASKO

БЛАГОДАРЯ GRACIAS MAHADSANID **THANK YOU** HVALA ХВАЛА ВАМ

ТИ БЛАГОДАРАМ TEŞEKKÜR EDERIM

TAK DANKE DANK JE ΕΥΧΑΡΙΣΤΩ GRATIAS TIBI ДЗЯКУЙ GRAZIE

RAHMAT MERCI AČIŪ SALAMAT MAHALO IĀ ʻOE TAKK SKAL DU HA DI OU MÈSI

GRAZZI ÞAKKA ÞÉR FALEMINDERIT ありがとうございました ĎAKUJEM

HATUR NUHUN РАХМАТ САҒА SIPAS JI WERE TERIMA KASIH MATUR NUWUN

CẢM ƠN BẠN UA TSAUG RAU KOJ

WAZVIITA ТИ БЛАГОДАРАМ

СИПОС

You’re recommending PowerShell?...
For security?...

“Many targeted attack groups already use PowerShell in their attack chain”

~ Symantec Increased use of PowerShell in attacks

“52% of all attacks seen in 2017 were non-malware attacks.”

~ Carbon Black 2017 Threat Report

“PowerShell malware grow by 267% in Q4, and by 432% year over year”

~ McAfee Labs Threats Report, March 2018

Top 10 reasons attackers <3 PS

ubiquity

- Installed by default
- Remote access by default with encryption
- Growing community
- System admins use and trust

stealth

- Execute payloads from memory
- Few traces by default
- Easy to obfuscate
- Gateway sandboxes lagging on script-based malware detection

configuration dependent

- Defenders overlook it when hardening their systems
- Bypass whitelisting tools ***depending on the configuration***

WMF (PS) 5.0+

- Script block logging and system-wide transcription can be enabled.
  - Hackers will leave fingerprints everywhere, unlike popular CMD utilities.
- PowerShell should be the only tool you allow for remote administration.

- Ashley McGlone, Who’s afraid of PowerShell security

References

- GitHub repos
  - PI-Security-Audit-Tools
  - PI-Security-DSC
  - PI Data Archive: Cyber Security Data Sheet
- OSIsoft Tech Support web site
  - PI System Cyber Security (alerts, news, downloads)