What's new in PI System Security?

Presented by **Brian Bostwick**
Felicia Mohan

“Infrastructure Hardened” PI System

Global. Trusted. Sustainable.

What is “Infrastructure Hardened”?

- Extremely Reliable
- Well Tested
- Proven Capability

“Trusted”

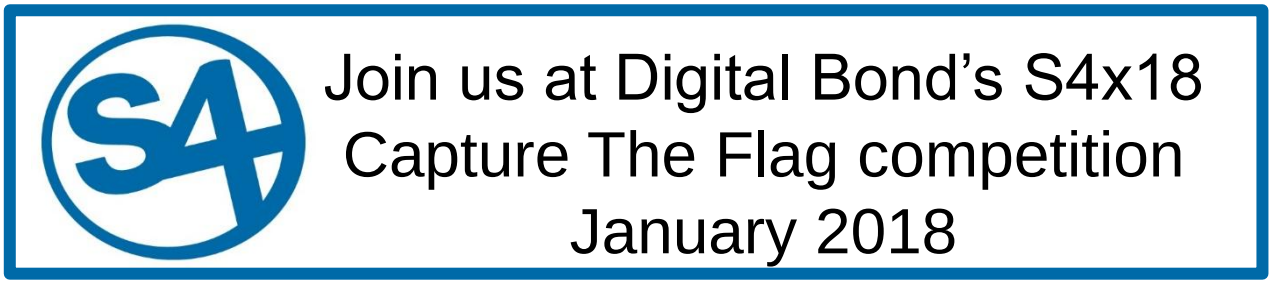
Security Development Lifecycle Process

Training → Requirements → Design → Implementation → Verification → Release → Response

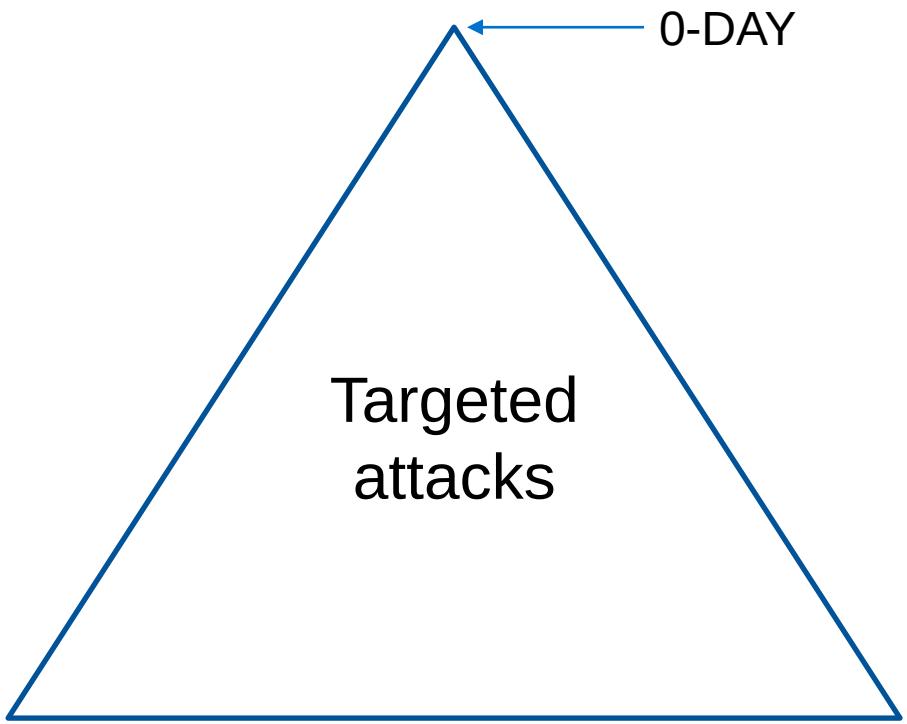
Cigital Coverity IOActive Microsoft QUALYS

OSIsoft Focusing on Software Security

1. Lifecycle Security	Even for our longest lived software
2. Modern Bits	Programs are built with smarter tools
3. Future Ready	Runs on safer technology stacks
4. Authenticity	Digital signatures for tamper detection
5. Native Security	Extra add-ons are not required

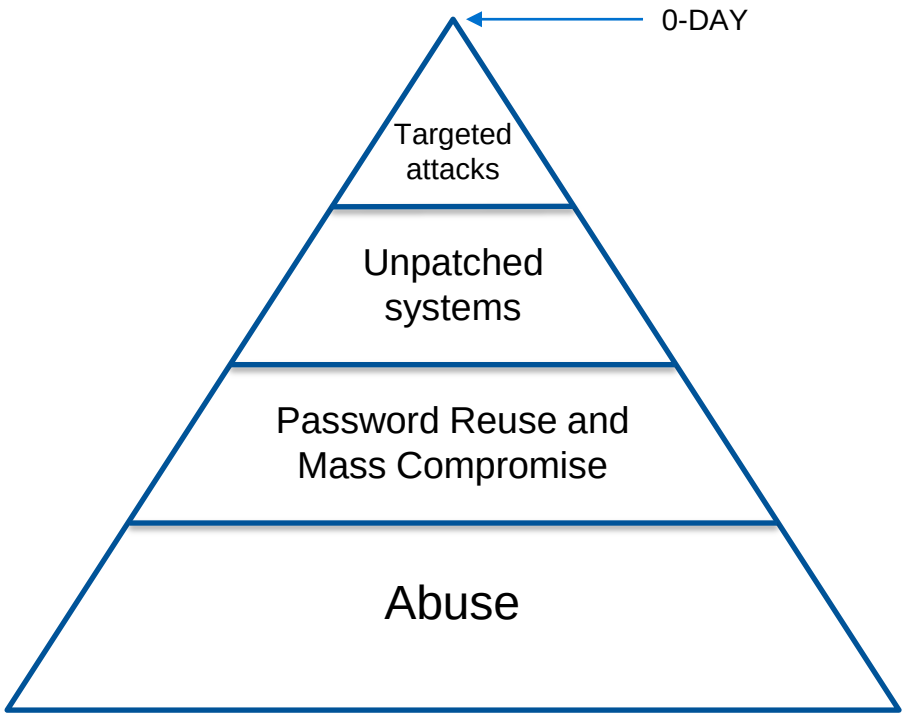


Refrain from focusing on complexity

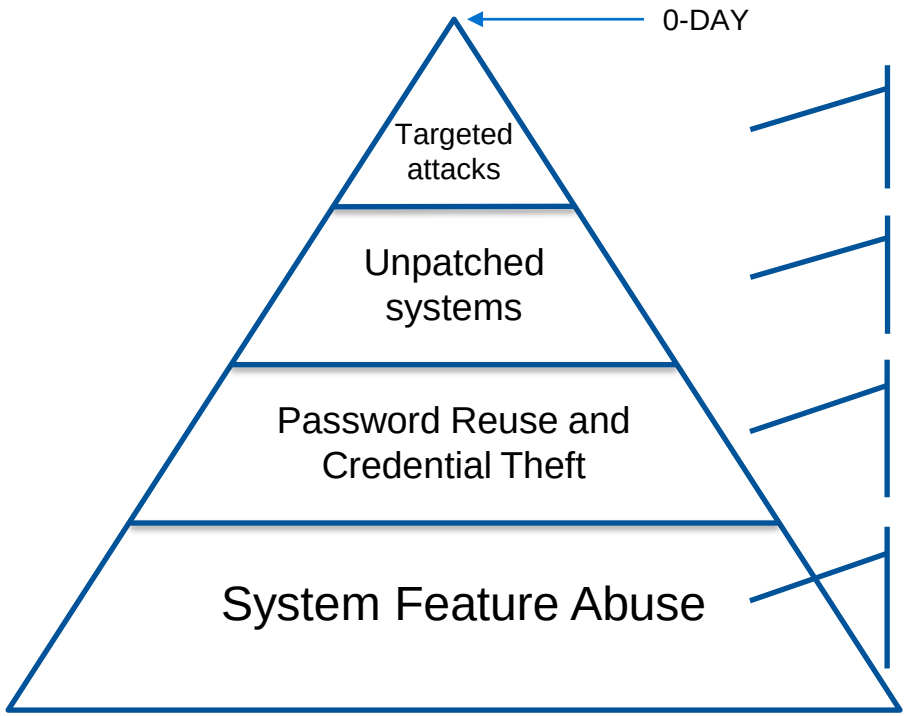


Alex Stamos, Facebook Chief Security Officer at Black Hat 2017

Focus on potential harm



Focus on potential harm



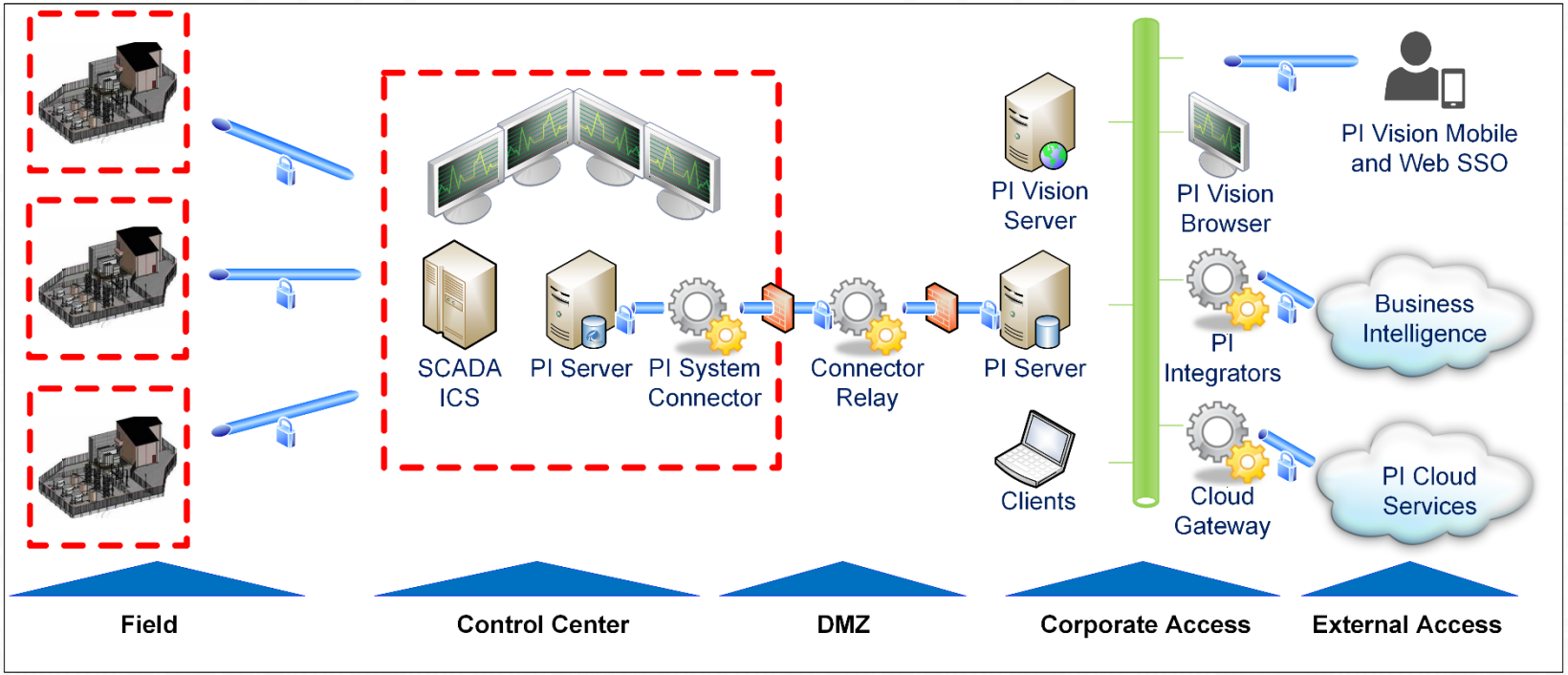
- Application whitelisting
- Communication whitelisting
- Digital signatures

- Patch compatibility program
- PI Vision architecture
- NOC Monitoring

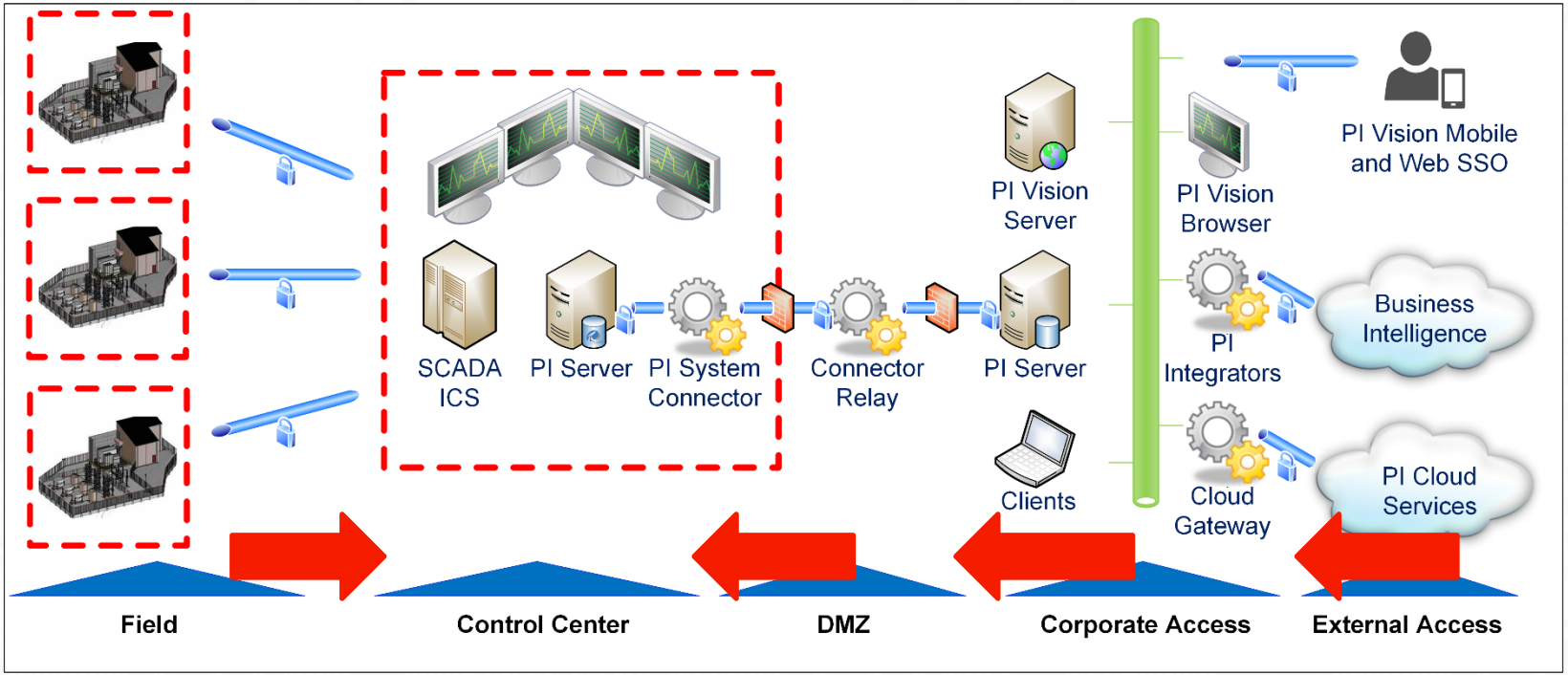
- Active Directory SSO
- Credential Manager
- Transport security

- Read only roles & archives
- Expensive query protection
- Output whitelist

PI System 2017 Reference Architecture



Direction of Cyber Attacks



NERC CIP, NIST 800-53, and NIST 800-82

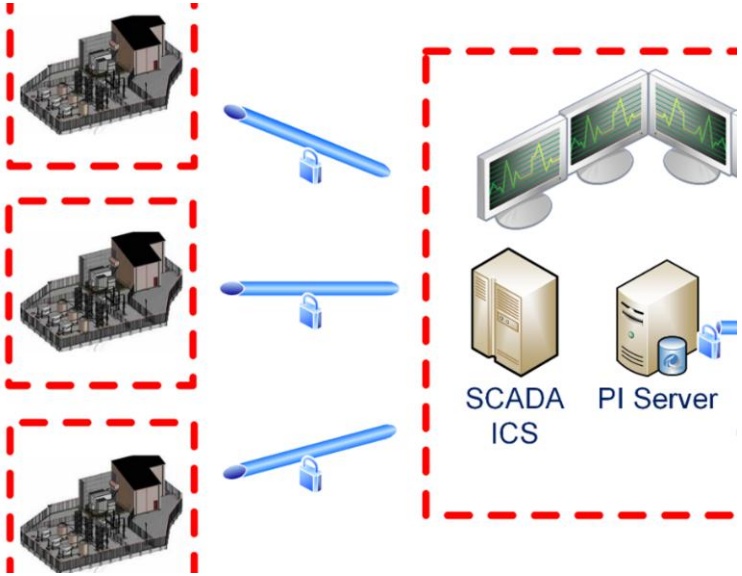
Secure PI Connectors and PI Interfaces

Encrypted communication

Read-only Options

PI API 2016 for WIS

- In place upgrade
- Same port, 5450
- AD not required
- Rollback available

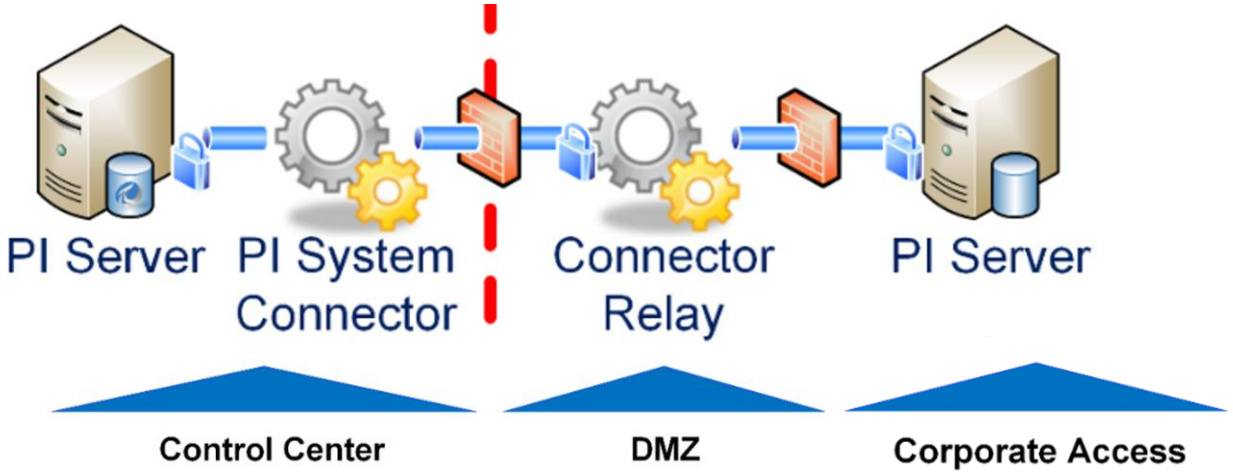


PI System Connector and Connector Relay

Protocol change in DMZ

Outbound rules only

Secure to Hosted PI Server

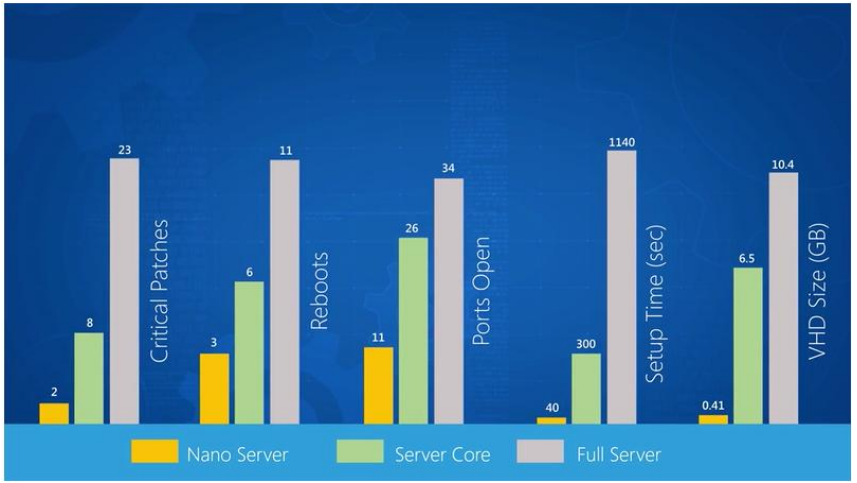


Least Functionality – Server Core

PI Server – Recommended on Windows Server Core

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

…. More Secure

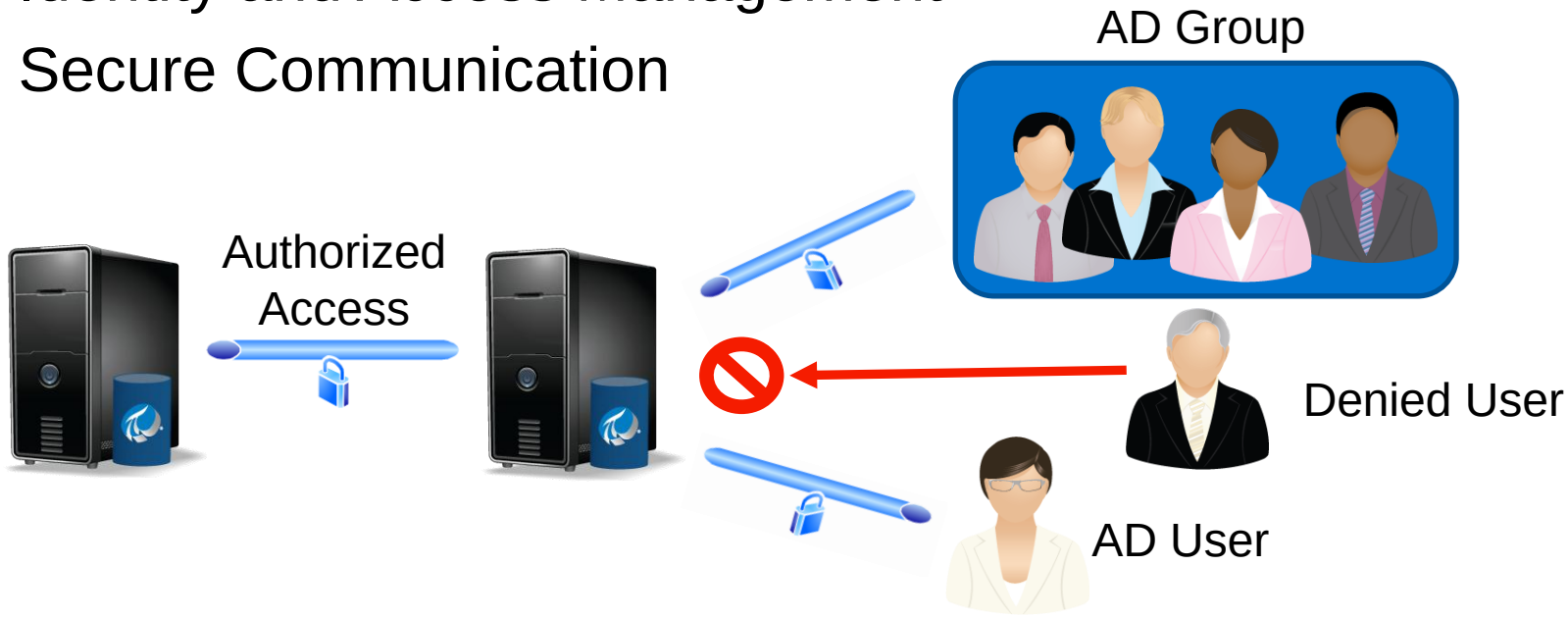


Microsoft Mechanics. "Exploring Nano Server for Windows Server 2016 with Jeffrey Snover." Online video clip. YouTube, 10 Feb. 2016

Leverage Standard Security Technologies

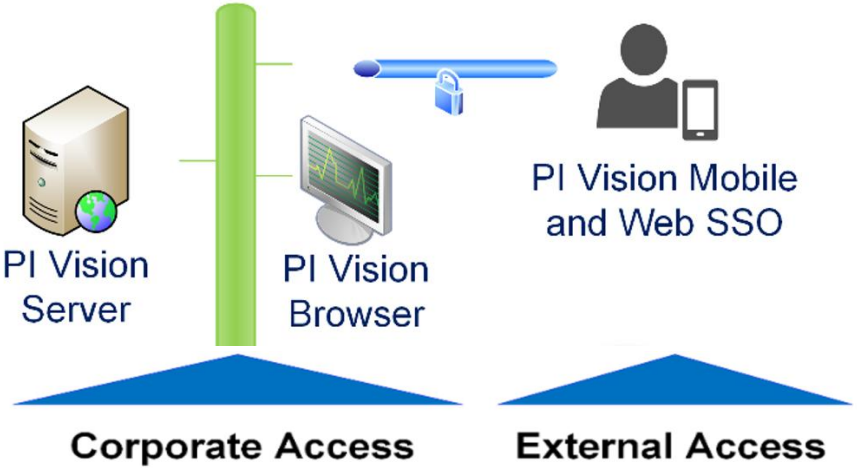
Active Directory and Windows Integrated Security provides

- Identity and Access Management
- Secure Communication



PI Vision 2017 and Mobile Access

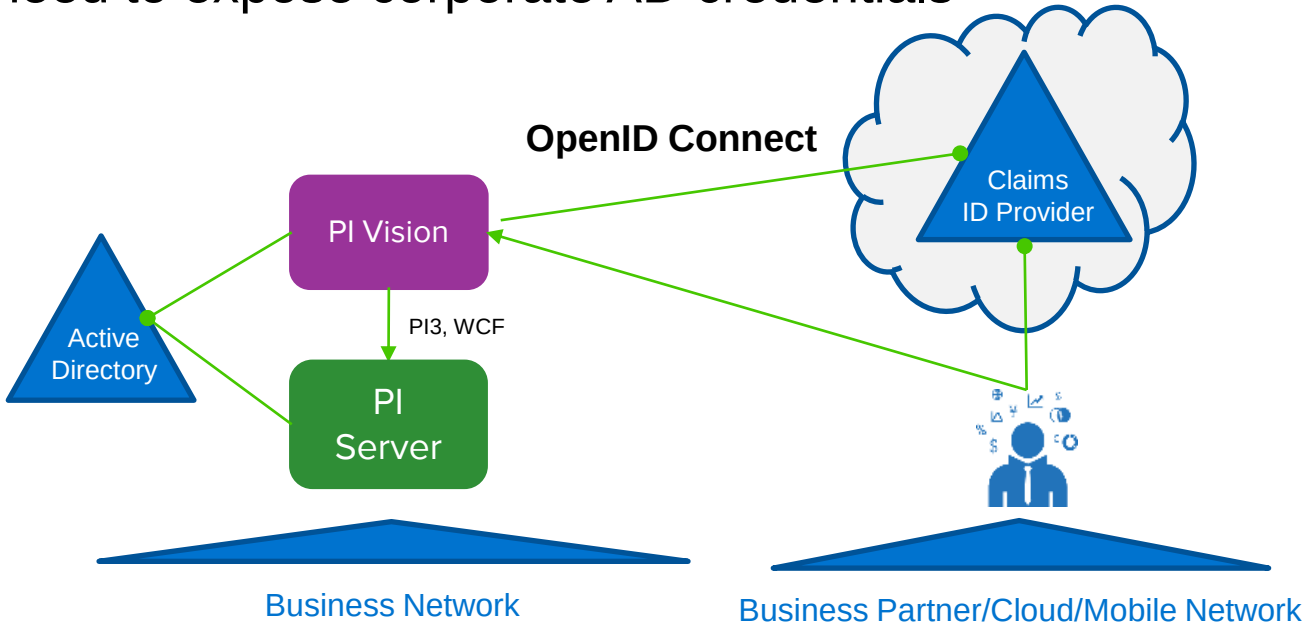
- Browser Based Client
  - Less installed, less running
  - Less patching
  - Less Maintenance
  - Lower TCO
- Manage Corporate Users with AD
- Manage Mobile Users with Claims



Boundary Protection: Claims Authentication

Advanced Security in PI Vision 2017 and PI WebAPI 2017

- Login using an external Identity Provider
- No need to expose corporate AD credentials

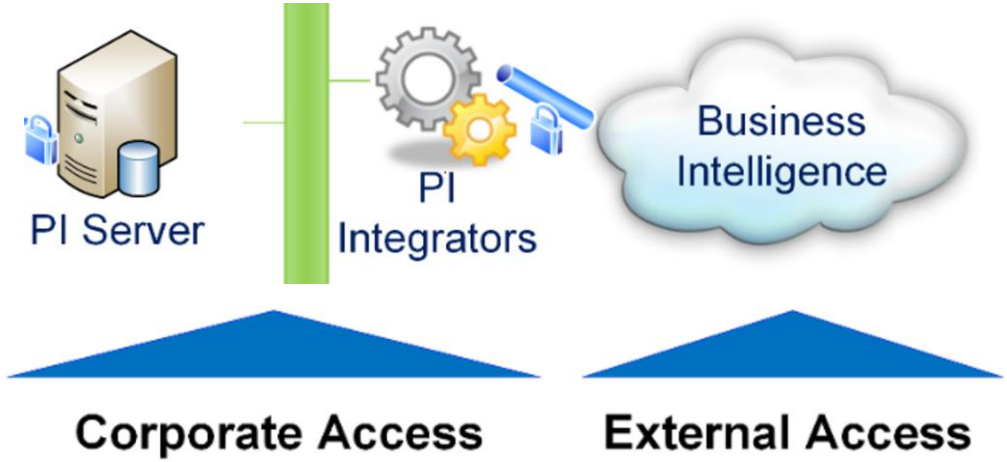


PI Integrators

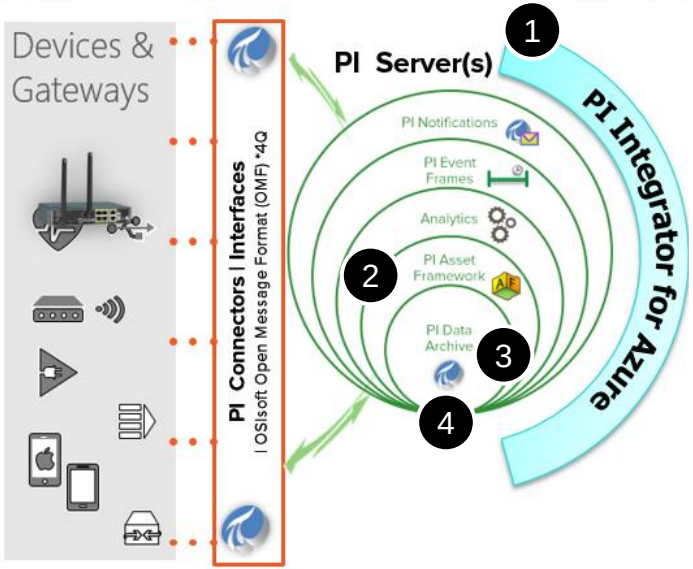
Extract from the Corporate PI Server

Stability: Handle significant queries

Secure access communication



PI Integrators



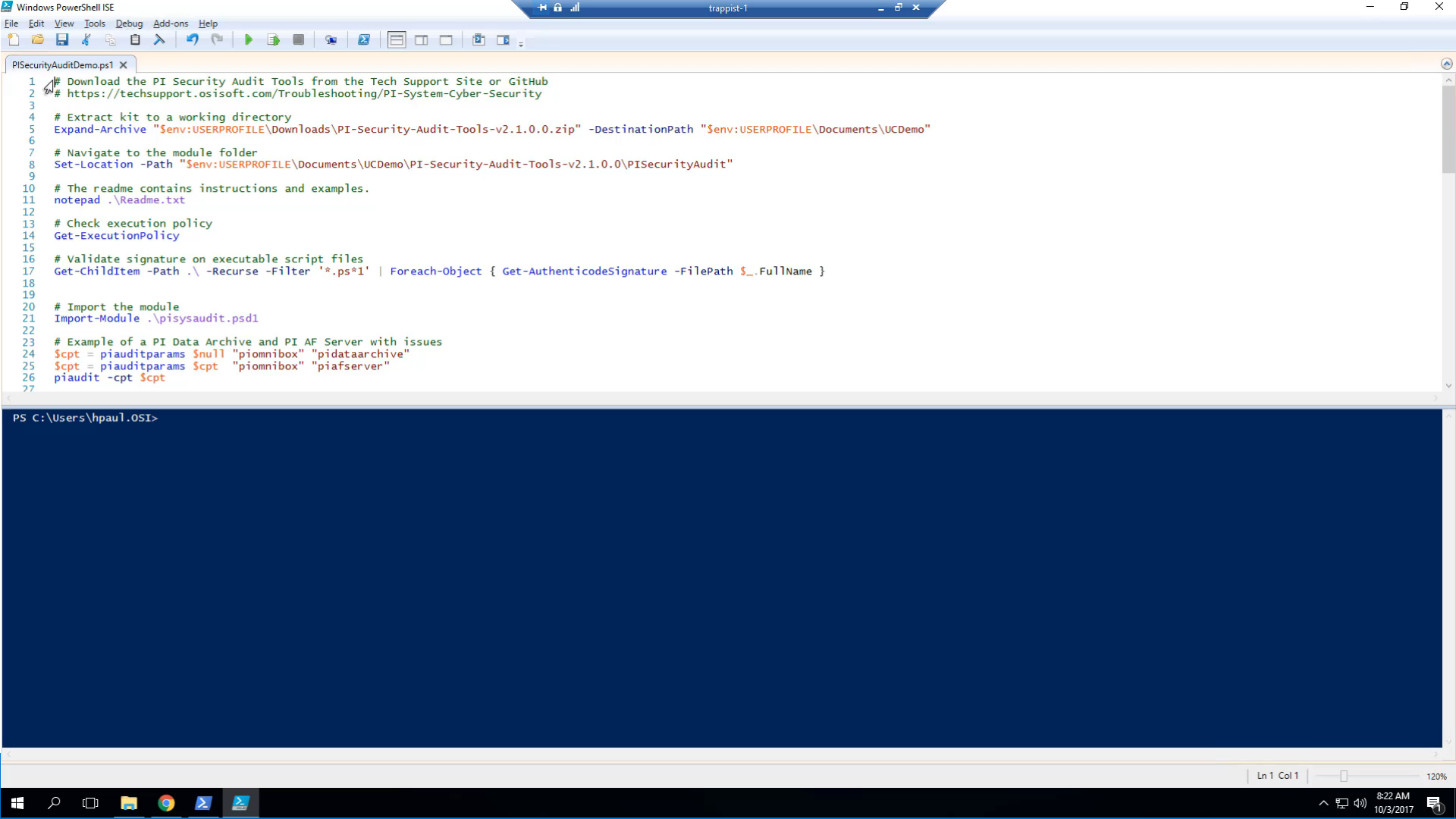
1. Resists pathological PI SQL data queries
2. Safe import and export of AF asset structures
3. Robust support for intensive bulk data calls
4. Reliable access to archive data

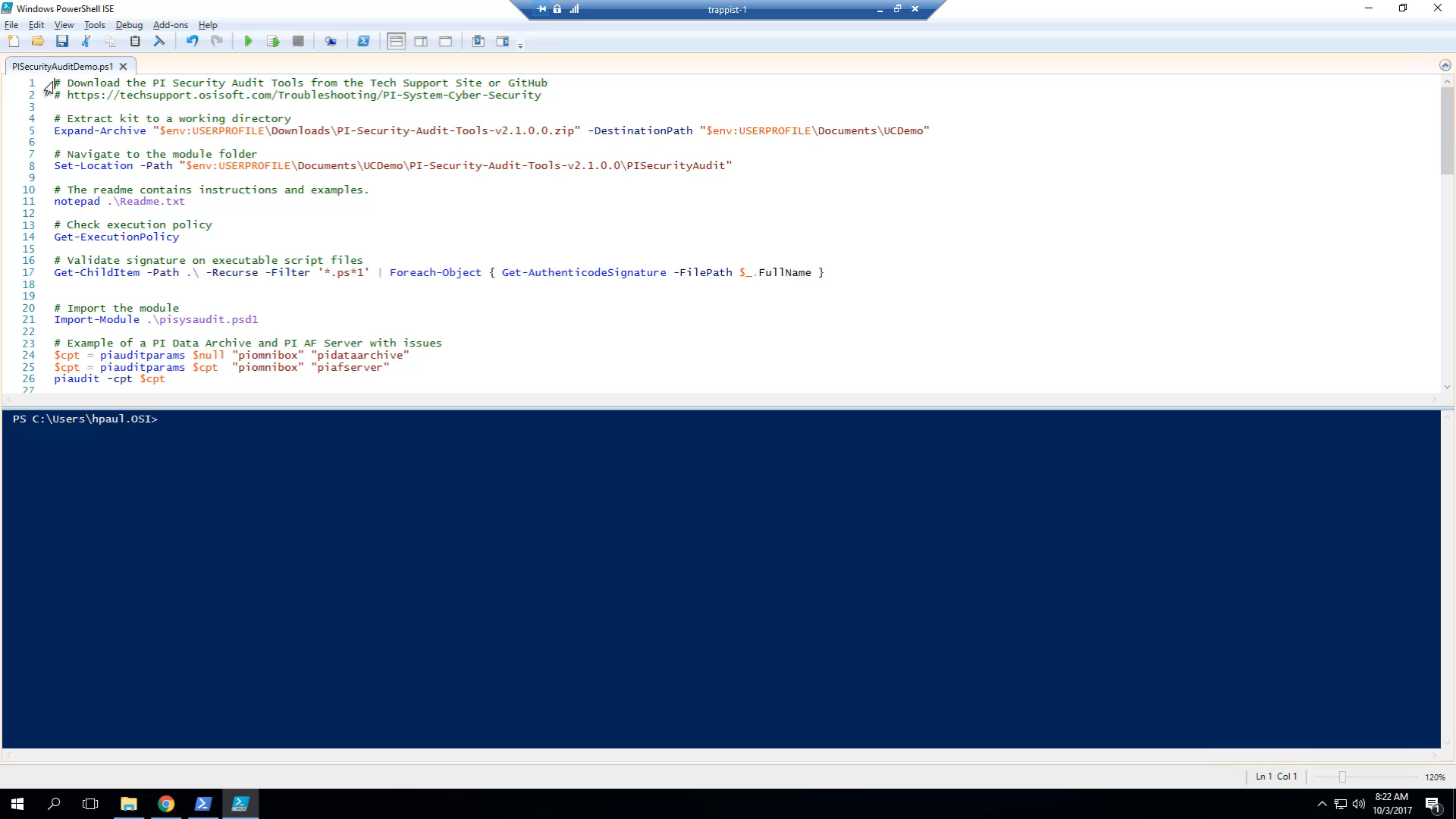
Microsoft

Baseline PI System Security

Use the PI Security Audit Tool to assess and improve PI System defenses.

ID	Server	Validation	Result	Severity	Message	Category	Area
AU10001	CP-VM1	Domain Membership Check	Fail	Severe	Machine is not a member of an AD Domain.	Machine	Domain
AU10002	CP-VM1	Operating System SKU	Fail	Severe	The following product is used: Server Standard	Machine	Operating System
AU20002	CP-VM1	PI Admin Trusts Disabled	Fail	Severe	The piadmin user can be assigned to a trust.	PI System	PI Data Archive
AU20004	CP-VM1	Edit Days	Fail	Severe	EditDays not specified, using non-compliant default of 0.	PI System	PI Data Archive
AU10004	CP-VM1	AppLocker Enabled	Fail	Moderate	AppLocker is not configured to enforce.	Machine	Policy
AU20001	CP-VM1	PI Data Archive Table Security	Fail	Moderate	The following databases present weaknesses: PIBatch; PIBATCHLEGACY; PICampaign; PIDBSEC; PIDS; PIHeadingSets; PIModules; PITransferRecords; PIUSER.	PI System	PI Data Archive
AU20009	CP-VM1	PI Data Archive SPN Check	Fail	Moderate	The Service Principal Name does NOT exist or is NOT assigned to the correct Service Account.	PI System	PI Data Archive
AU10005	CP-VM1	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU10003	CP-VM1	Firewall Enabled	Pass	N/A	Firewall enabled.	Machine	Policy
AU20003	CP-VM1	PI Data Archive SubSystem Versions	Pass	N/A	Version is compliant	PI System	PI Data Archive
AU20005	CP-VM1	Auto Trust Configuration	Pass	N/A	Tuning parameter compliant: Create the trust entry for the loopback IP address 127.0.0.1	PI System	PI Data Archive
AU20006	CP-VM1	Expensive Query Protection	Pass	N/A	Using the compliant default of 260.	PI System	PI Data Archive
AU20007	CP-VM1	Explicit login disabled	Pass	N/A	Using compliant policy: All authentication options enabled.	PI System	PI Data Archive
AU20008	CP-VM1	piadmin is not used	Pass	N/A	No Trust(s) or Mapping(s) identified as weaknesses.	PI System	PI Data Archive


Windows PowerShell ISE
trappist-1
File Edit View Tools Debug Add-ons Help
PISecurityAuditDemo.ps1
Download the PI Security Audit Tools from the Tech Support Site or GitHub
https://techsupport.osisoft.com/Troubleshooting/PI-System-Cyber-Security
Extract kit to a working directory
Expand-Archive "$env:USERPROFILE\Downloads\PI-Security-Audit-Tools-v2.1.0.0.zip" -DestinationPath "$env:USERPROFILE\Documents\UCDemo"
Navigate to the module folder
Set-Location -Path "$env:USERPROFILE\Documents\UCDemo\PI-Security-Audit-Tools-v2.1.0.0\PISecurityAudit"
The readme contains instructions and examples.
notepad .\Readme.txt
Check execution policy
Get-ExecutionPolicy
Validate signature on executable script files
Get-ChildItem -Path .\ -Recurse -Filter '*.ps*1' | Foreach-Object { Get-AuthenticodeSignature -FilePath $_.FullName }
Import the module
Import-Module .\pisysaudit.psd1
Example of a PI Data Archive and PI AF Server with issues
$cpt = piauditparams $null "piomnibox" "pidataarchive"
$cpt = piauditparams $cpt "piomnibox" "piafserver"
piaudit -cpt $cpt
PS C:\Users\hpaul.OSI>
Ln 1 Col 1
120%
8:22 AM
10/3/2017


Windows PowerShell ISE
trappist-1
File Edit View Tools Debug Add-ons Help
PISecurityAuditDemo.ps1
Download the PI Security Audit Tools from the Tech Support Site or GitHub
https://techsupport.osisoft.com/Troubleshooting/PI-System-Cyber-Security
Extract kit to a working directory
Expand-Archive "$env:USERPROFILE\Downloads\PI-Security-Audit-Tools-v2.1.0.0.zip" -DestinationPath "$env:USERPROFILE\Documents\UCDemo"
Navigate to the module folder
Set-Location -Path "$env:USERPROFILE\Documents\UCDemo\PI-Security-Audit-Tools-v2.1.0.0\PISecurityAudit"
The readme contains instructions and examples.
notepad .\Readme.txt
Check execution policy
Get-ExecutionPolicy
Validate signature on executable script files
Get-ChildItem -Path .\ -Recurse -Filter '*.ps*1' | Foreach-Object { Get-AuthenticodeSignature -FilePath $_.FullName }
Import the module
Import-Module .\pisysaudit.psd1
Example of a PI Data Archive and PI AF Server with issues
$cpt = piauditparams $null "piomnibox" "pidataarchive"
$cpt = piauditparams $cpt "piomnibox" "piafserver"
piaudit -cpt $cpt
PS C:\Users\hpaul.OSI>
Ln 1 Col 1
120%
8:22 AM
10/3/2017

PI Security Audit Tool Updates

- 17 new validation checks
- Support for PI Vision
- Allow computer parameters to be specified in a CSV file
- Revised validation check severity based on Bow Tie analysis methodology
- PI Security Configuration Export utility to export security settings for analysis

AUDIT SUMMARY

11-Feb-2017 15:17:43

ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	SPACEMANTIMEZ	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU10004	SPACEMANTIMEZ	AppLocker Enabled	Fail	Moderate	AppLocker is not configured to enforce.	Machine	Policy
AU30007	SPACEMANTIMEZ	PI AF Server SPN Check	Fail	Moderate	The Service Principal Name does NOT exist or is NOT assigned to the correct Service Account.	PI System	PI AF Server
AU10005	SPACEMANTIMEZ	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU30002	SPACEMANTIMEZ	Impersonation mode for AF Data Sets	N/A	N/A	AFDiag output not found. Cannot continue processing the validation check	PI System	PI AF Server
AU30003	SPACEMANTIMEZ	PI AF Server Service privileges	N/A	N/A	Elevation required to check process privilege. Run Powershell as Administrator to complete these checks	PI System	PI AF Server
AU30004	SPACEMANTIMEZ	PI AF Server Plugin Verify Level	N/A	N/A	AFDiag output not found. Cannot continue processing the validation check	PI System	PI AF Server
AU30005	SPACEMANTIMEZ	PI AF Server File Extension Whitelist	N/A	N/A	AFDiag output not found. Cannot continue processing the validation check	PI System	PI AF Server
AU10001	SPACEMANTIMEZ	Domain Membership Check	Pass	N/A	Machine is a member of an AD Domain.	Machine	Domain
AU10003	SPACEMANTIMEZ	Firewall Enabled	Pass	N/A	Firewall enabled.	Machine	Policy
AU30001	SPACEMANTIMEZ	Configured Account	Pass	N/A	AFService is not running as Local System	PI System	PI AF Server
AU30006	SPACEMANTIMEZ	PI AF Server Version	Pass	N/A	Server version is compliant.	PI System	PI AF Server

Recommendations for failed validations:

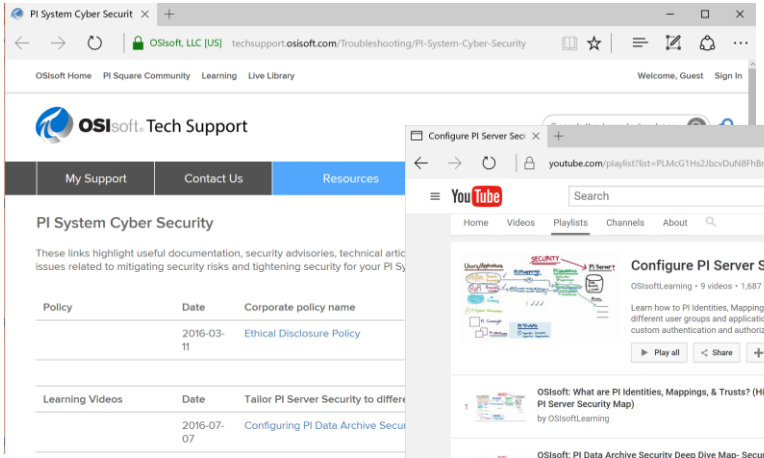
AU10002 - Operating System Installation Type

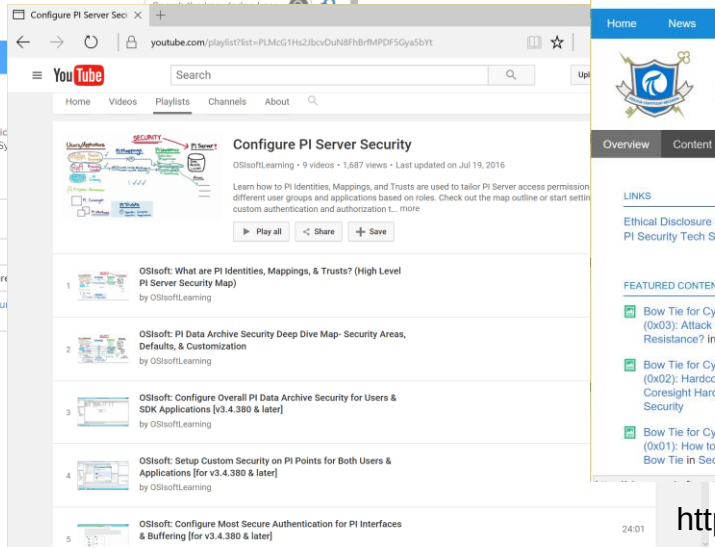
VALIDATION: verifies that the OS installation type is server core for the reduced surface area.
COMPLIANCE: Installation Type should be Server Core. Different SKUs are available at the link below:
http://msdn.microsoft.com/en-us/library/ms724358.aspx
For more on the advantages of Windows Server Core, please see:
https://msdn.microsoft.com/en-us/library/hh846314(v=vs.85).aspx

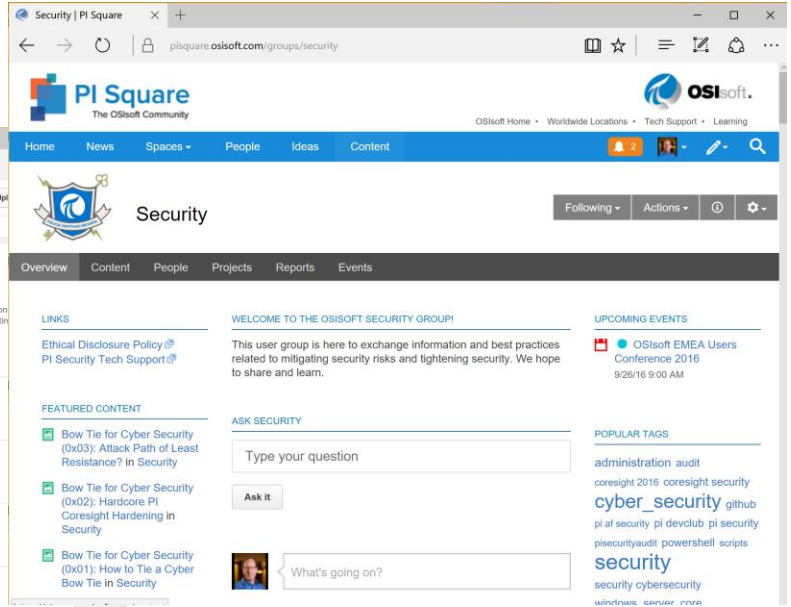
AU10004 - AppLocker Enabled

Key PI System Security Resources

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



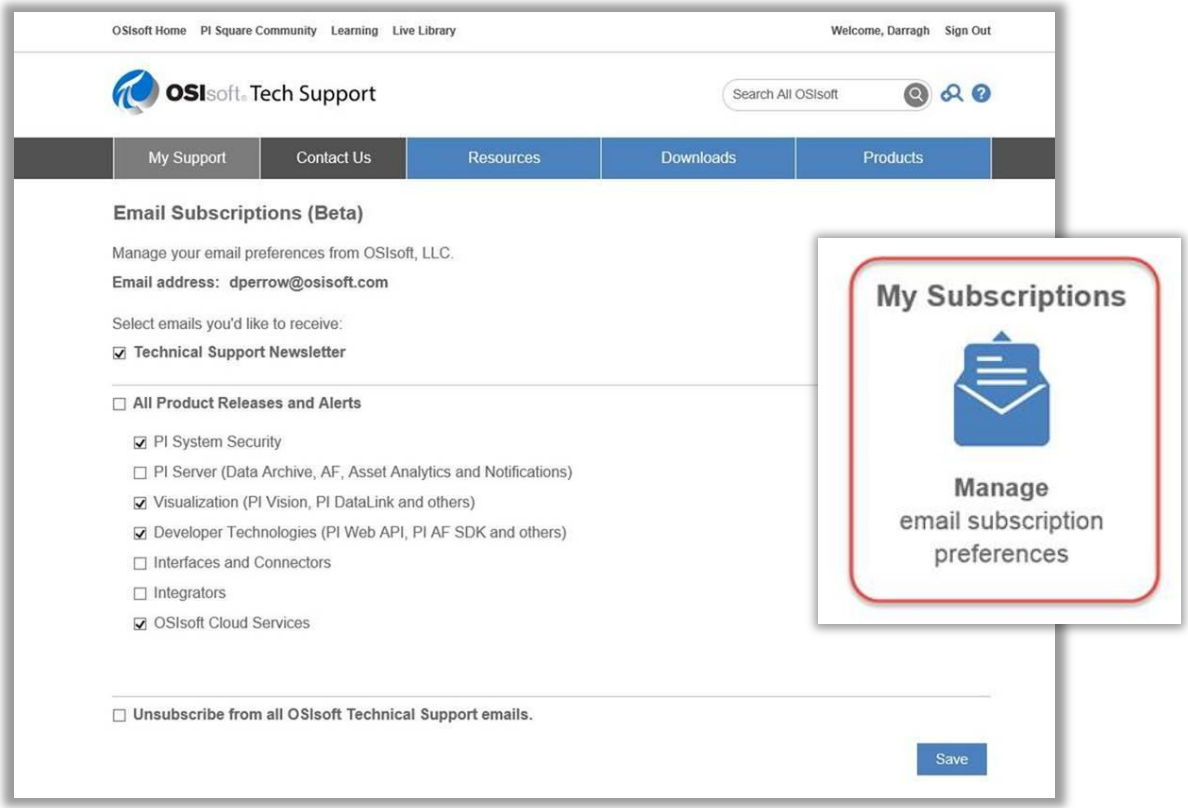




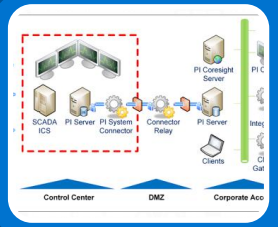
https://pisquare.osisoft.com/groups/security

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

Get Security Alerts through My Support Page



Actions



Review best practices

Validation	Result	Severity	Message
Domain Membership Check	Fail	Severe	Machine is
Operating System SKU	Fail	Severe	The followin
PI Admin Trusts Disabled	Fail	Severe	The piadmir
Edit Days	Fail	Severe	EditDays no
AppLocker Enabled	Fail	Moderate	AppLocker
PI Data Archive Table Security	Fail	Moderate	The followin PIBATCHLE PIHeadingS
PI Data Archive SPN Check	Fail	Moderate	The Service assigned to
UAC Enabled	Fail	Low	Recommend disabled.
Firewall Enabled	Pass	N/A	Firewall ena
PI Data Archive SubSystem Versions	Pass	N/A	Version is c

Baseline with PI Security Audit Tool

Prioritize and take the first step….

Contact Information

Brian Bostwick
Brian@OSIsoft.com
Cyber Security Market Principal
OSIsoft, LLC

Felicia Mohan
FMohan@OSIsoft.com
Northern European
Regional Services Lead
OSIsoft, LLC

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://bit.ly/uc2017-app

감사합니다

谢谢

Danke

Gracias

Merci

Thank You

ありがとう

Спасибо

Obrigado