

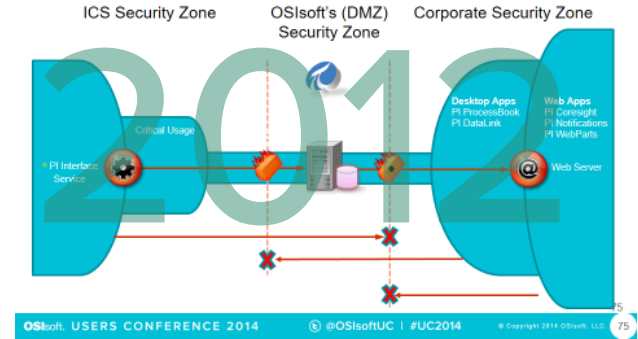


What Should I do to Harden my PI System?

Presented by **Bryan Owen PE**
Mike Lemley

Hardening Agenda

- Architectural Patterns
- Web Server Tips
- Operational Countermeasures



Securing PI Interfaces

Presented by **Mike Lemley**
Tony Cantele

OSIsoft. USERS CONFERENCE 2014 @OSIsoftUC | #UC2014 Copyright 2014 OSIsoft, LLC



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**

OSIsoft. USERS CONFERENCE 2014 @OSIsoftUC | #UC2014 Copyright 2014 OSIsoft, LLC 5

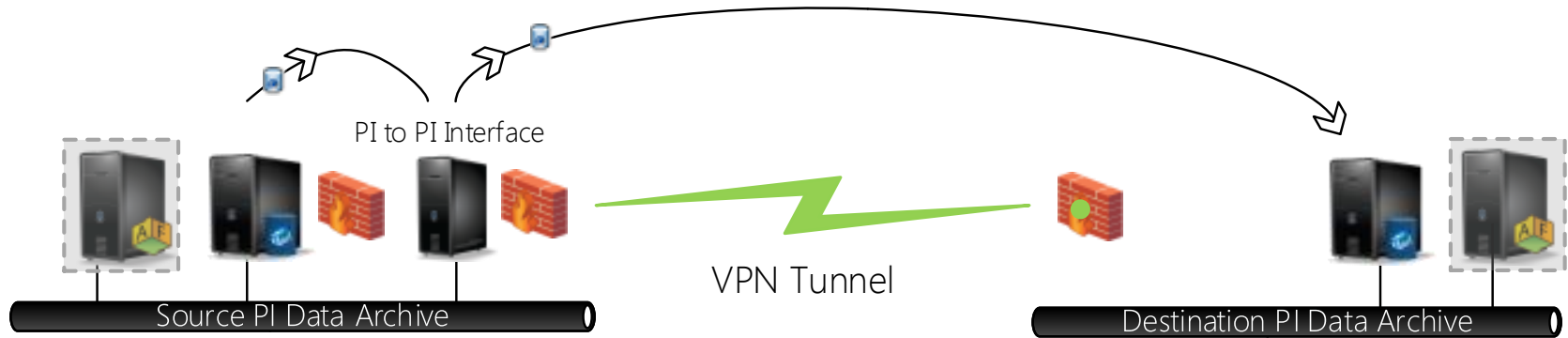


Architectural Patterns: External Connections with the PI Infrastructure



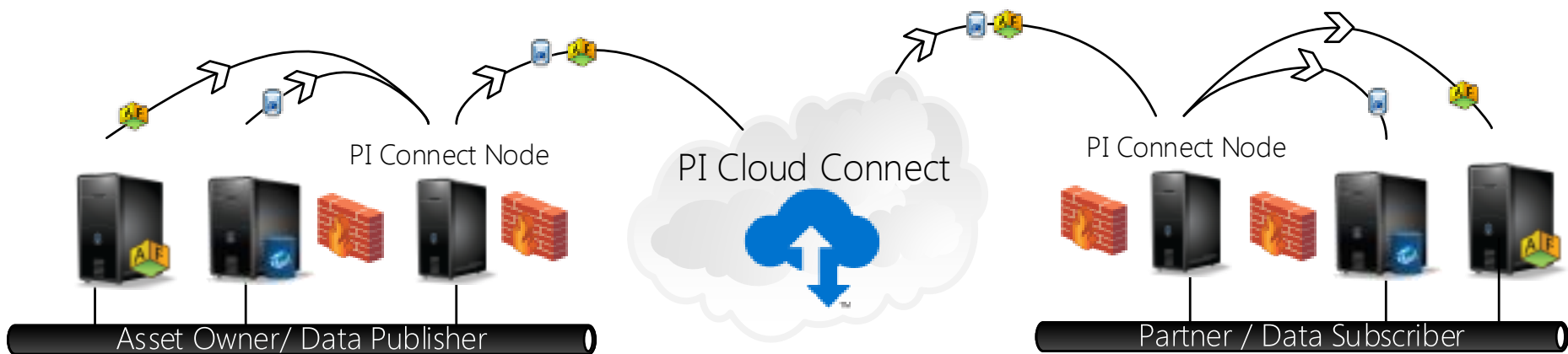
VPNs are General Purpose

A network tunnel between two large companies:
...what could go wrong?

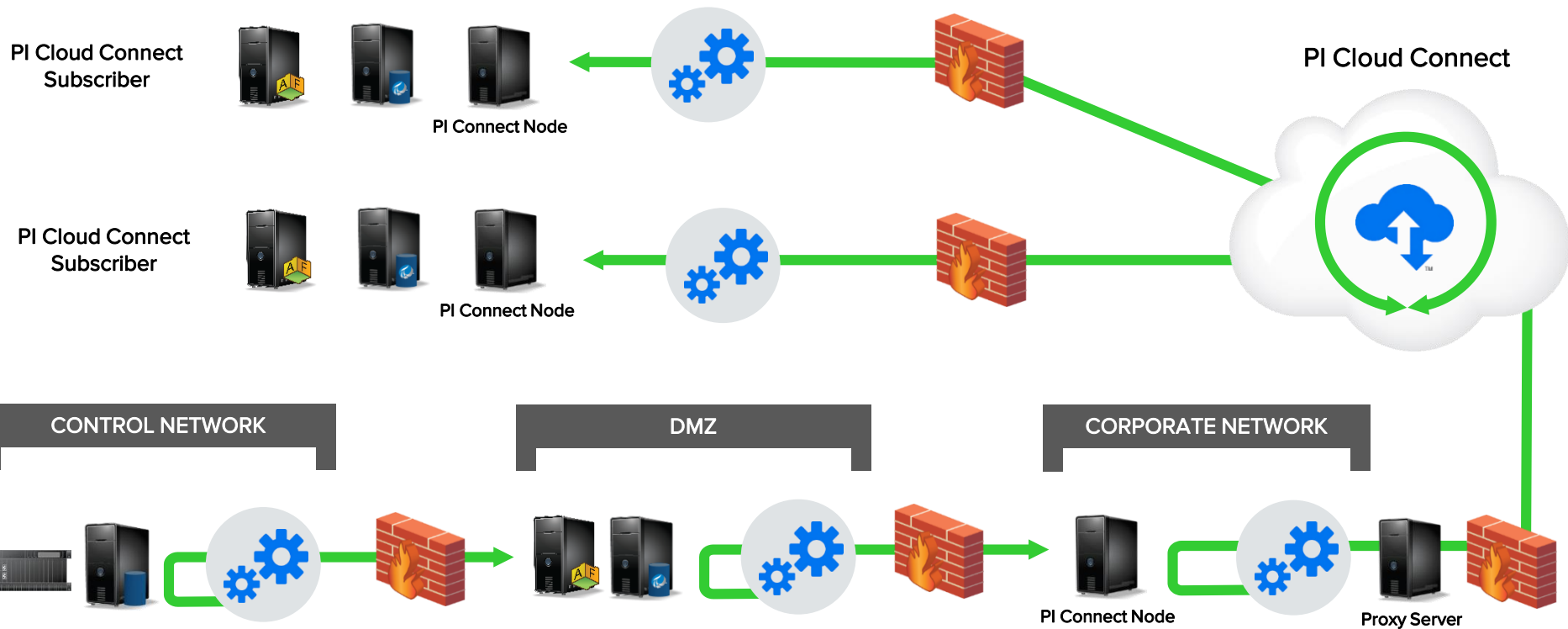


PI Cloud Connect is Purpose Built

- Data Sharing Service for PI System Data
 - PI connect nodes publish and subscribe to the service

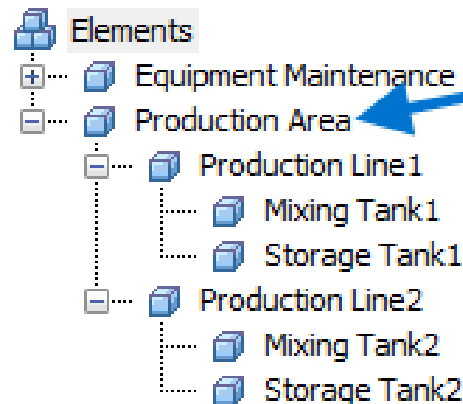


Overall Security Architecture



Delegating Security

- Select the publication data source from AF
- Delegate management by AF permissions



**Data source for
Publication**



Architectural Patterns: External Connections with PI Coresight

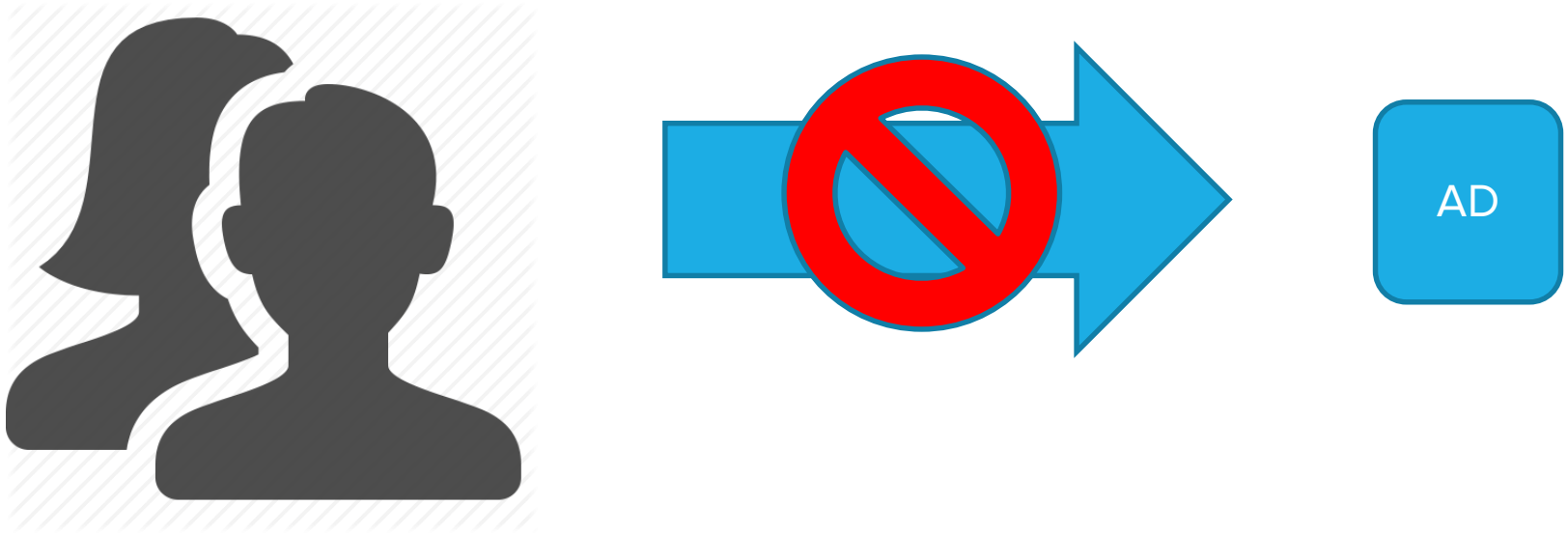




More and More Passwords?

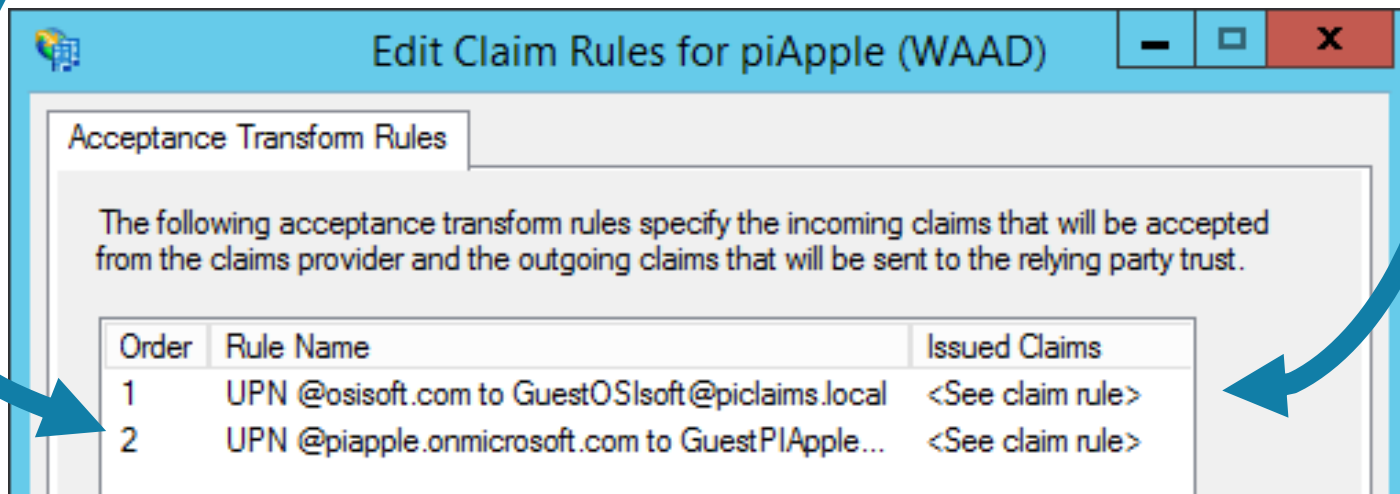
Bad Idea

- Foreign user logon to Active Directory (eg NTLM)



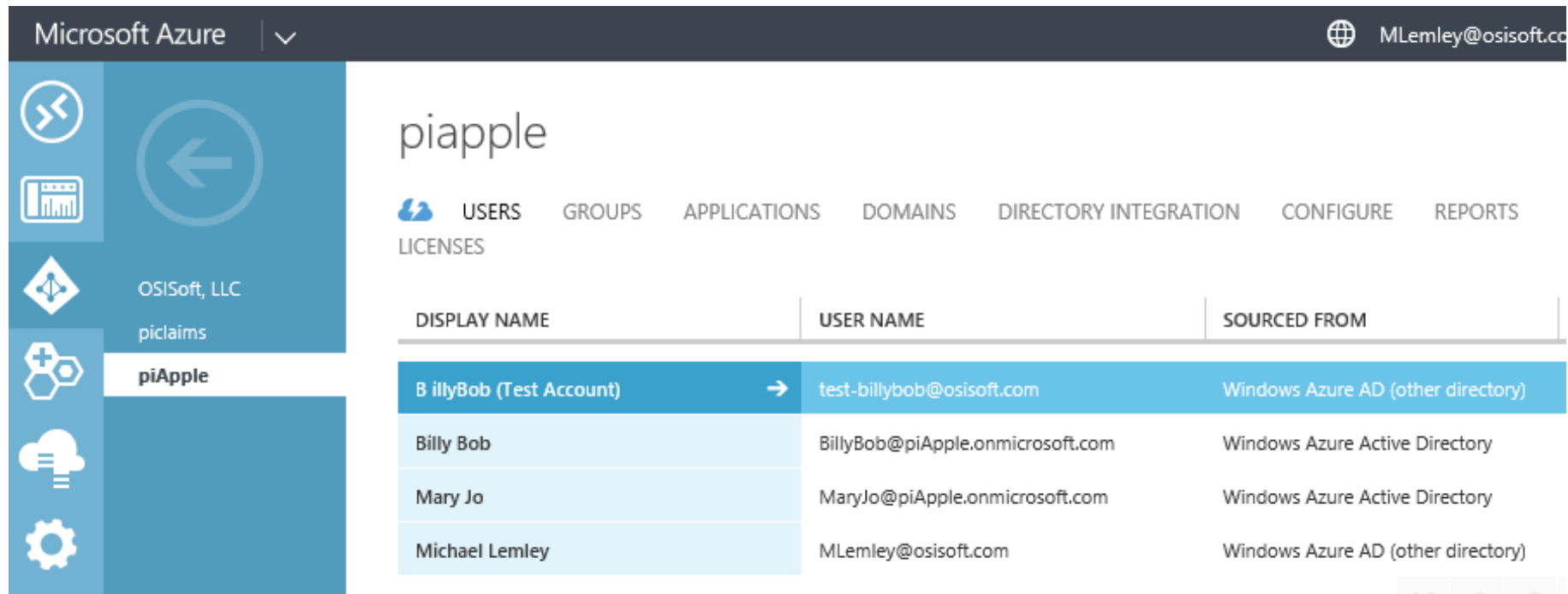
Map External Users to a Local Account (ADFS)



External User	External Domain	piclaims.local
<any>	osisoft.com	GuestOSIsoft
piapple	onmicrosoft.com	GuestPIApple




Windows Azure Active Directory (WAAD)

Example of WAAD as a foreign Identity Provider



Microsoft Azure |   MLemley@osisoft.co

piApple

 USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS

LICENSES

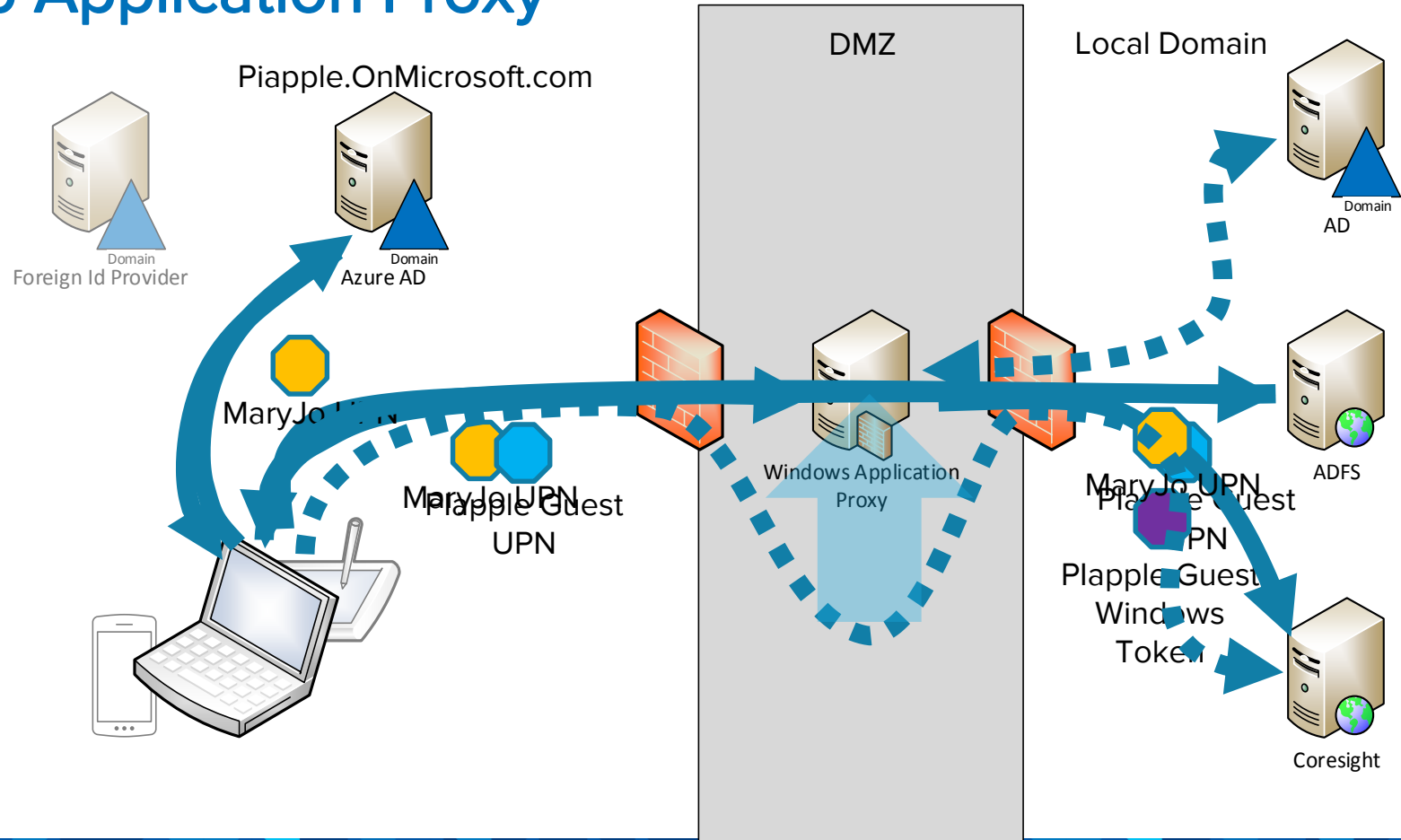
DISPLAY NAME	USER NAME	SOURCED FROM
B illyBob (Test Account) →	test-billybob@osisoft.com	Windows Azure AD (other directory)
Billy Bob	BillyBob@piApple.onmicrosoft.com	Windows Azure Active Directory
Mary Jo	MaryJo@piApple.onmicrosoft.com	Windows Azure Active Directory
Michael Lemley	MLemley@osisoft.com	Windows Azure AD (other directory)

Demo: Accessing PI Coresight

- Logon using a foreign identity



Web Application Proxy



Fewer Passwords!

- Manage AD credentials for internal employees only
- Avoids unnecessary Personally Identifiable Information
- Stronger authentication

Avoid account resets for 1000's of external accounts!



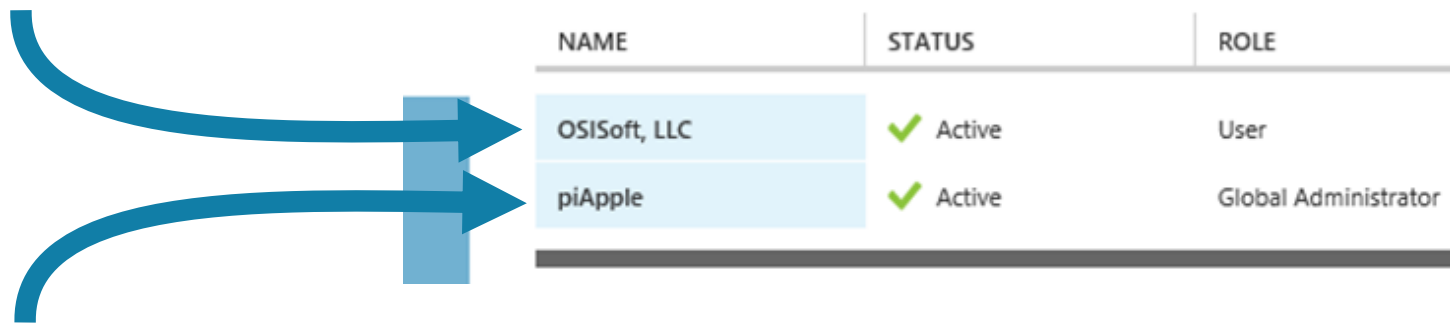
WAAD Teaser

What is Azure Active Directory?



Foreign Identity Provider (IdP)

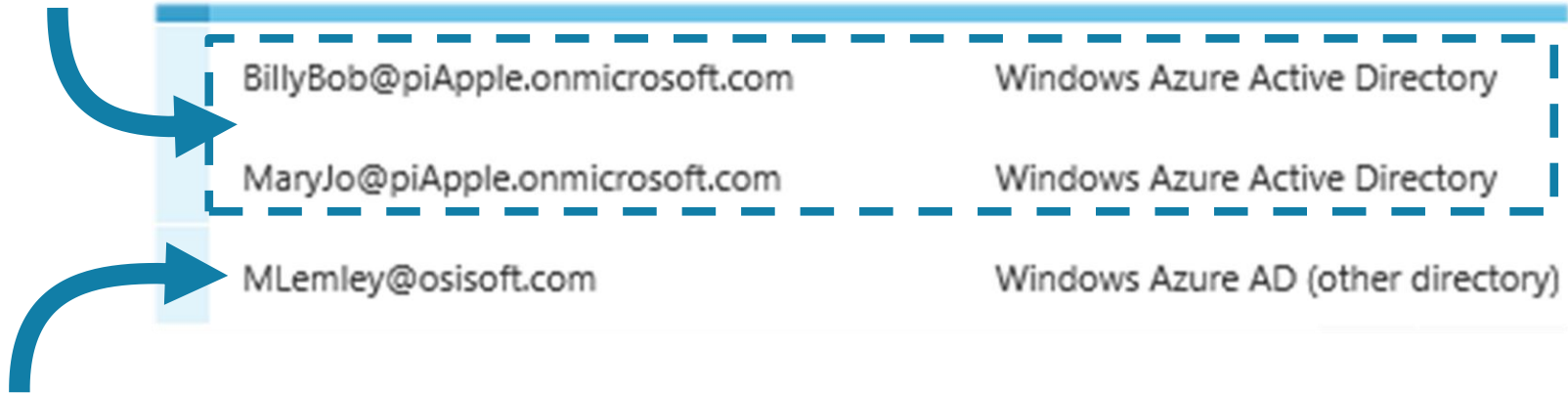
- Synchronize with foreign Identity Provider (DirSync)



- Individual users added to your Azure Active Directory

Identity Types

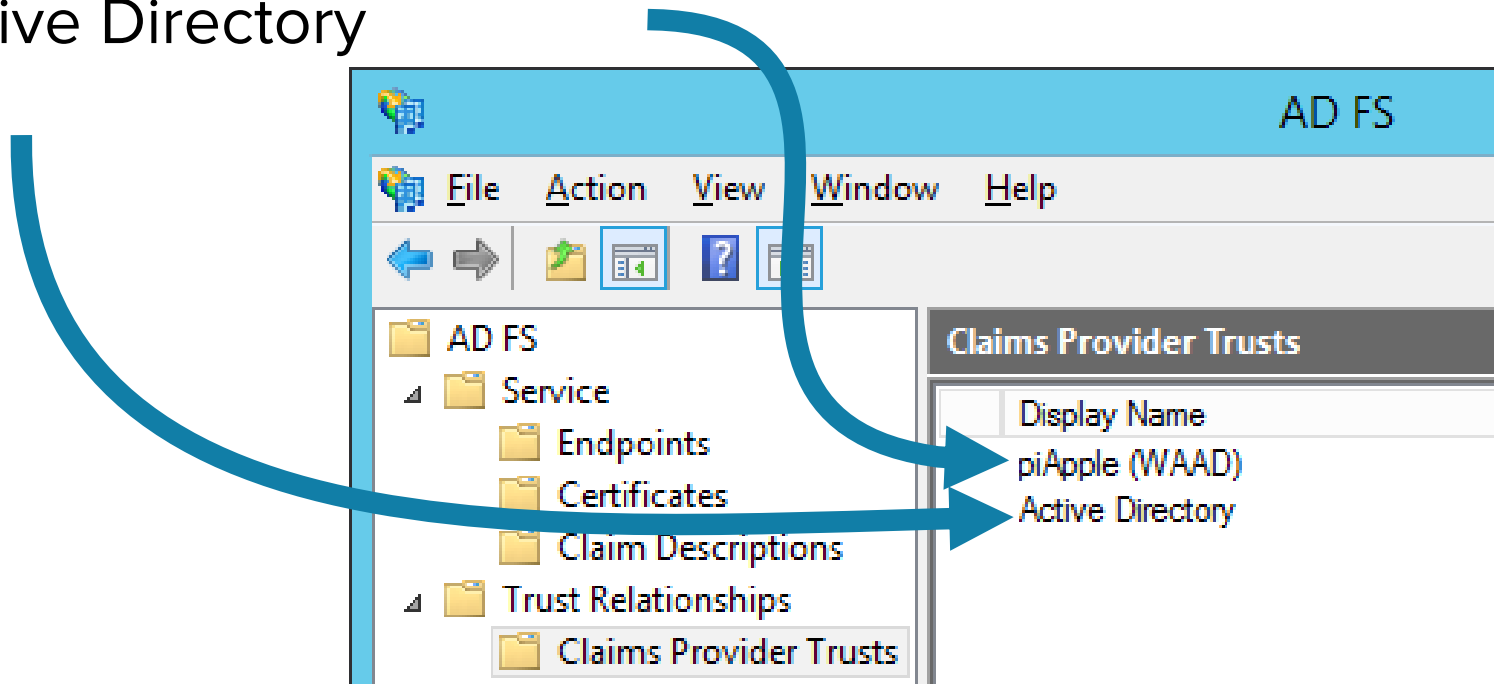
- Locally created domain in Azure (piApple)



- Foreign Identity Provider (osisoft.com)
- Microsoft Live account

Configure as Trusted Claims Provider in ADFS

- Windows Azure Active Directory
- Active Directory



Multi-factor Authentication

users service settings

app passwords

- ☒ Allow users to create app passwords to sign into non-browser applications
- ☐ Do not allow use of app passwords (users enabled for multi-factor auth will not be able to sign in to non-browser applications)

manage user devices **PREVIEW**

- ☐ Allow users to suspend Multi-Factor Authentication by remembering their devices

Days before a device must re-authenticate using Multi-Factor Authentication (1-60):

save

Intrusion Detection Reports

▲ ANOMALOUS ACTIVITY

Sign ins from unknown sources

May indicate an attempt to sign in without being traced.

Sign ins after multiple failures

May indicate a successful brute force attack.

Sign ins from multiple geographies

May indicate that multiple users are signing in with the same account.

▲ ACTIVITY LOGS

Audit report

Audited events in your directory

▲ INTEGRATED APPLICATIONS

Account provisioning activity

Provides a history of attempts to provision accounts to external applications.

Account provisioning errors

Indicates an impact to users' access to external applications.

▲ PREMIUM REPORTS

Sign ins from IP addresses with suspicious activity

May indicate a successful sign in after a sustained intrusion attempt.

Sign ins from possibly infected devices

May indicate an attempt to sign in from possibly infected devices.

Irregular sign in activity

May indicate events anomalous to users' sign in patterns.



Web Server Tips

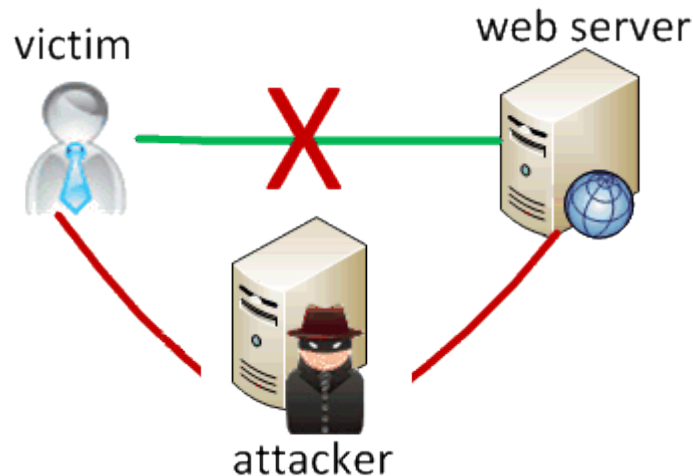


SSL Certificates for PI Coresight / PI WebAPI

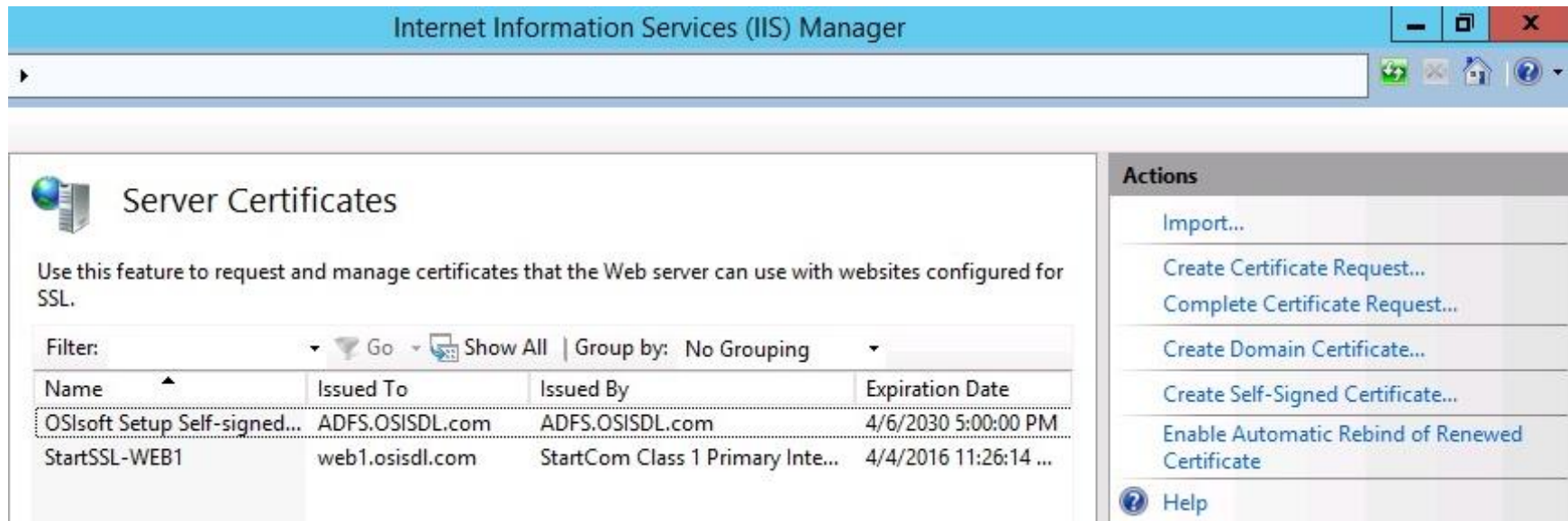
Who do you and your users trust?

(...for key management)

- Public Certificate Authority
- Private Certificate Authority
- Web Server (Self-Signed)



Installing a SSL Certificate for PI Coresight



The screenshot shows the Internet Information Services (IIS) Manager window. The title bar reads "Internet Information Services (IIS) Manager". The main content area is titled "Server Certificates" and includes a description: "Use this feature to request and manage certificates that the Web server can use with websites configured for SSL." Below the description is a table of certificates. The table has columns for Name, Issued To, Issued By, and Expiration Date. There are two certificates listed: "OSIsoft Setup Self-signed..." and "StartSSL-WEB1". To the right of the table is an "Actions" pane with several options: Import..., Create Certificate Request..., Complete Certificate Request..., Create Domain Certificate..., Create Self-Signed Certificate..., Enable Automatic Rebind of Renewed Certificate, and Help.

Internet Information Services (IIS) Manager

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date
OSIsoft Setup Self-signed...	ADFS.OSISDL.com	ADFS.OSISDL.com	4/6/2030 5:00:00 PM
StartSSL-WEB1	web1.osisdl.com	StartCom Class 1 Primary Inte...	4/4/2016 11:26:14 ...

Actions

- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- Enable Automatic Rebind of Renewed Certificate
- Help

Web Application Configuration Analyzer (WACA)

Quick Actions

[> Scan machines](#)

[> View scan results](#)

[> Compare scan results](#)

[> Generate suppressions file](#)

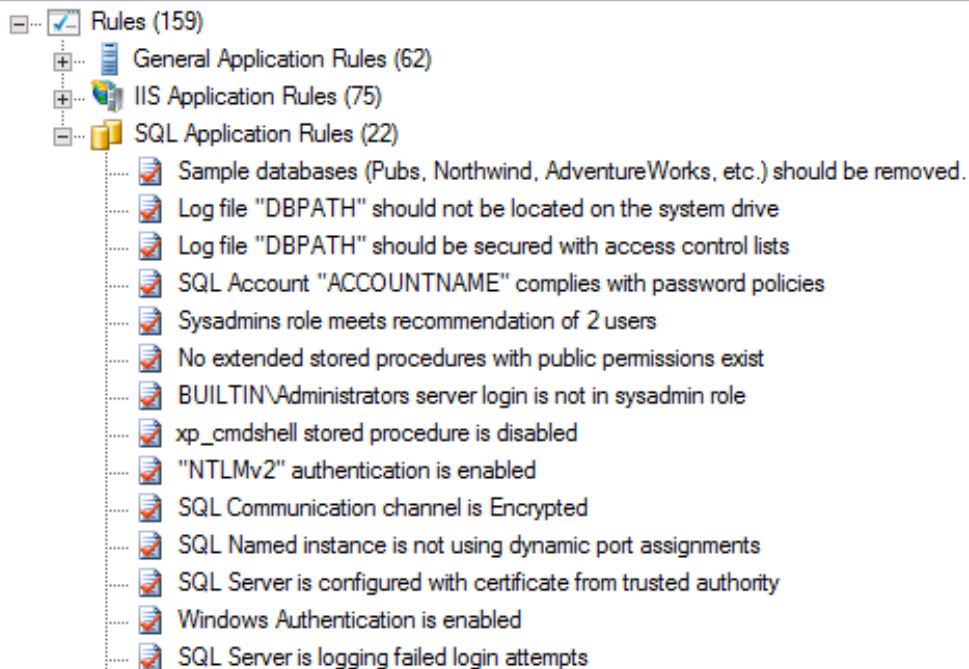
[> Map Team Foundation Server fields](#)

About

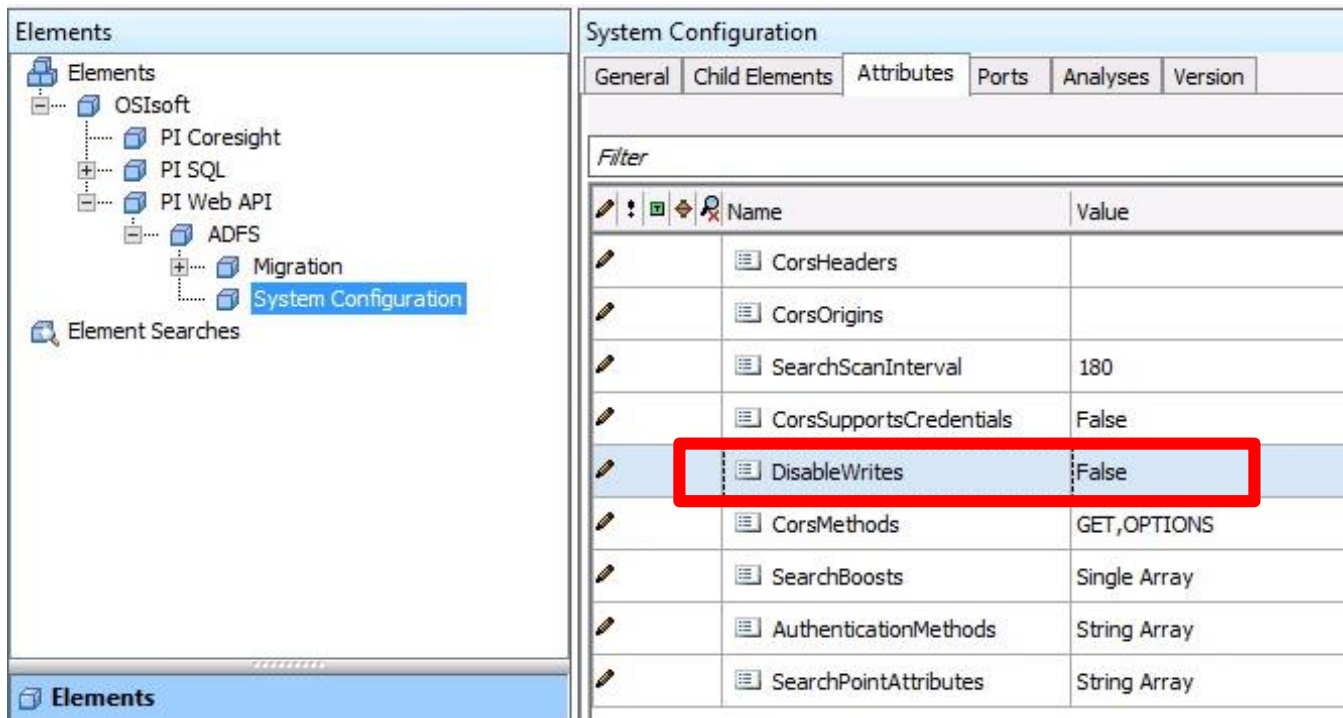
Web Application Configuration Analyzer (WACA) analyzes application configuration for security best practices related to General Application, IIS, ASP.NET Application and SQL Server settings. Machine can be scanned remotely to identify any misconfigurations. It provides detailed report on multiple instances of checks for further analysis. Violations in the report can be exported to Excel or Visual Studio Team Foundation Server®.

Rules

The following tree lists the breakdown of rules that are currently checked by the tool.

- 
- Rules (159)
 - General Application Rules (62)
 - IIS Application Rules (75)
 - SQL Application Rules (22)
 - Sample databases (Pubs, Northwind, AdventureWorks, etc.) should be removed.
 - Log file "DBPATH" should not be located on the system drive
 - Log file "DBPATH" should be secured with access control lists
 - SQL Account "ACCOUNTNAME" complies with password policies
 - Sysadmins role meets recommendation of 2 users
 - No extended stored procedures with public permissions exist
 - BUILTIN\Administrators server login is not in sysadmin role
 - xp_cmdshell stored procedure is disabled
 - "NTLMv2" authentication is enabled
 - SQL Communication channel is Encrypted
 - SQL Named instance is not using dynamic port assignments
 - SQL Server is configured with certificate from trusted authority
 - Windows Authentication is enabled
 - SQL Server is logging failed login attempts

PI WebAPI Hardening – Disable Writes

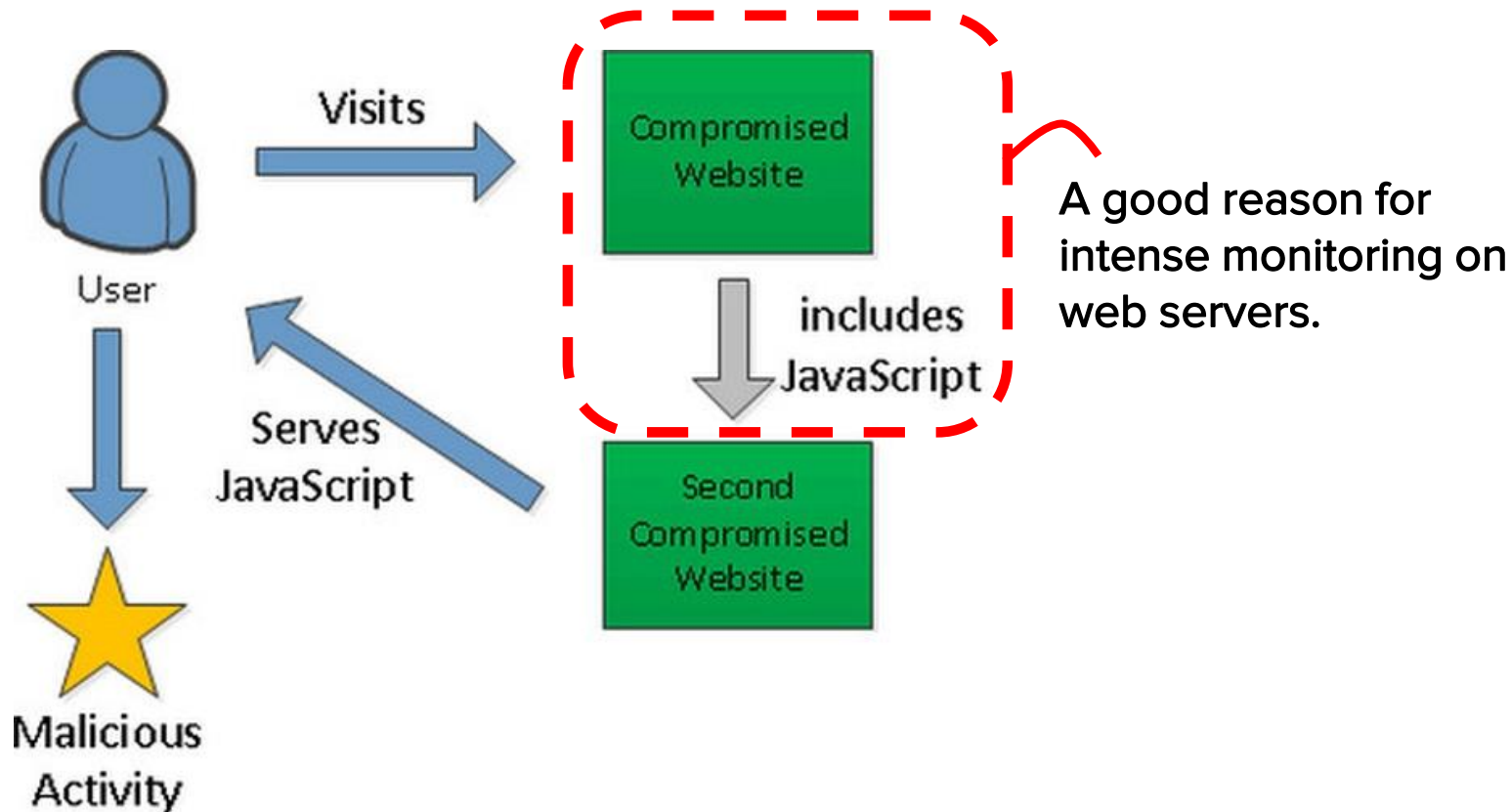


The screenshot displays the PI WebAPI configuration interface. On the left, the 'Elements' tree shows the hierarchy: Elements > OSIssoft > PI Coresight > PI SQL > PI Web API > ADFS > Migration > System Configuration. The 'System Configuration' tab is selected, showing a list of configuration items. The 'DisableWrites' item is highlighted with a red rectangle, indicating its current value is 'False'.

Name	Value
CorsHeaders	
CorsOrigins	
SearchScanInterval	180
CorsSupportsCredentials	False
DisableWrites	False
CorsMethods	GET,OPTIONS
SearchBoosts	Single Array
AuthenticationMethods	String Array
SearchPointAttributes	String Array

Operational Countermeasures

Modern Web Attacks



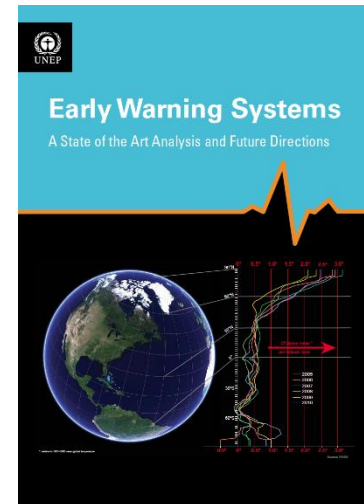
Sysinternals Sysmon 3.0

Sysmon Event ID	Description
1	Process create
2	File creation time
3	Network connection detected
5	Process terminated
6	Driver loaded
7	Image loaded
8	Create remote thread detected



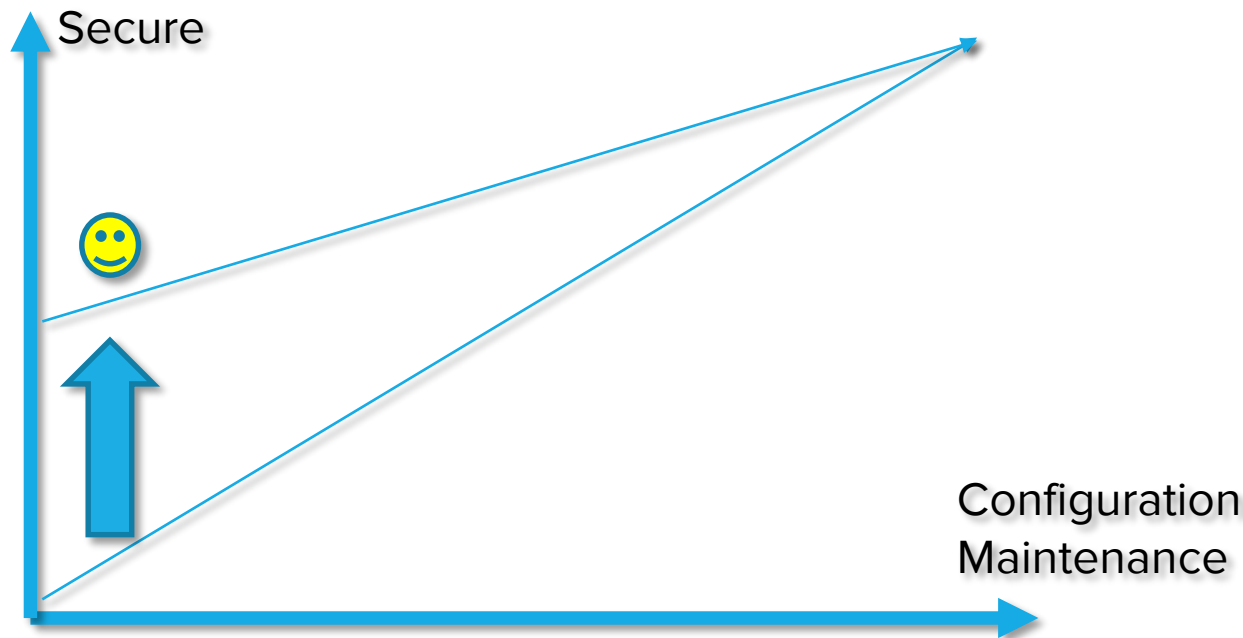
Good Idea

- Automate alerts on unexpected changes!
 - PI System Interfaces & Notifications
 - System Center Configuration Manager
 - ...



Hardening is Hard

Objective: Deploy with secure defaults that just work. Harder for us, not you.



OSISoft Security Advisor Team

Bryan Owen

bryan@osisoft.com

Principal Cyber Security Manager

Jim Davidson

jdavidson@osisoft.com

Principal Cyber Security Advisor

Mike Lemley

mlemley@osisoft.com

Senior Cyber Security Developer



Questions

Please wait for the **microphone**
before asking your questions

State your
name & company





THANK YOU



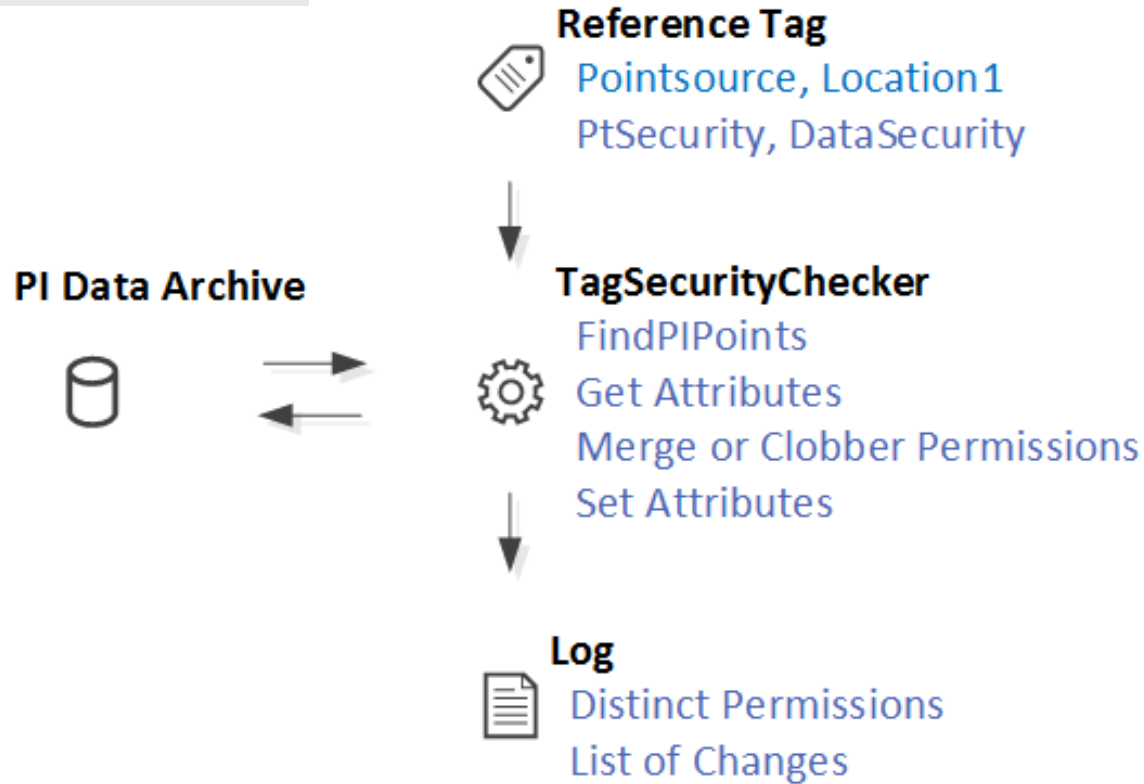
Bonus Material



Tag Level Permissions for Interfaces

Task	Service	DBSecurity (PIPOINT)	PtSecurity	DataSecurity
Find points	Interface	R	R	-
Buffered Write	Bufss	-	-	W
Read Event Triggers	Interface	-	R	R
Read Source Tag Events for Outputs	Interface	-	R	R
Unbuffered Write	Interface	-	R	W
Create points	Interface	RW	RW	-

Tag Security Checker



Code Snip: FindPIPoints

```
'Find rest of points in this Pointsource AND Location1
Dim ptSRC, ptLOC1, TagSearchStr As String
myPt.LoadAttributes(PICCommonPointAttributes.PointSource, _
                   PICCommonPointAttributes.Location1)

ptSRC = myPt.GetAttribute("Pointsource").ToString
ptLOC1 = myPt.GetAttribute("Location1").ToString
TagSearchStr = "PointSource:=" + ptSRC + " AND Location1:=" + ptLOC1

Dim myPts As IEnumerable(Of PIPoint)
myPts = PIPoint.FindPIPoints(myPI, TagSearchStr, False)
```

```
.....
```

Code Snip: Load,Set,Save Attribute

```
' set and save security attributes to PI Server
' ...for collection of tags with missing reference ACEs
If ACLchanged Or Clobber Then
    myTAGSperACL = myACLTags(i)
    For Each tagname In myTAGSperACL
        myPt = PIPoint.FindPIPoint(myPI, tagname)
        myPt.LoadAttributes(PICommonPointAttributes.PointSecurity, _
                           PICommonPointAttributes.DataSecurity)
        myPt.SetAttribute("PtSecurity", PtACL)
        myPt.SetAttribute("DataSecurity", DataACL)
        Dim errors As AFErrors(Of String) = _
            myPt.SaveAttributes(PICommonPointAttributes.PointSecurity, _
                               PICommonPointAttributes.DataSecurity)
    Next
End If
```