

```
point.Snapshot;  
2. Dim srv As PISDK.Server  
3. Fore*%^(%) (point in server.PIPoints)?!!??  
4. Dim srv A PISDK.Server  
5. if (time_to_market > expected)  
{  
    solution = vCampus;}  
6. if (time_to_market > expected)  
{  
    solution = vCampus;}  
}
```

"where PI geeks meet"

OSIsoft®

V CAMPUS

2009

LIVE!

Palace Hotel, San Francisco, CA ▪ Dec. 1-2, 2009

```
1. foreach (point in server.PIPoints)  
{  
    point.Snapshot;  
}  
2. Dim srv As PISDK.Server  
3. Fore*%^(%) (point in server.PIPoints)?!!??  
4. Dim srv A PISDK.Server  
5. if (time_to_market > expected)  
{  
    solution = vCampus;}  
6. if (time_to_market > expected)  
{  
    solution = vCampus;}  
}
```

OSIsoft®

V

CAMPUS

2009

LIVE!

Considerations of the new PI Security Model

Bryan S. Owen – OSIsoft Cyber Security Manager

```
1. foreach (point in server.PIPoints)
{
    point.Snapshot;
}
2. Dim srv As PISDK.Server
3. Fore*%*% (point in server.PIPoints)?!!??
4. Dim srv A PISDK.Server
5. if (time to market > expected)
```


Security Roadmap...

CADILLAC ONE: THE CAR THAT THINKS IT'S A TANK

PETROL TANK:

Armour-plated and filled with a specially designed foam which prevents it from exploding even if it suffers a direct hit.

REAR COMPARTMENT:

Seats four passengers with glass partition - only Obama has a switch to lower it. Windows larger than on previous presidential cars. Panic button installed for Obama to summon help.

DOORS: Armour-plated, eight inches thick and the weight of a cabin door on a Boeing 757 jet.

CHAUFFEUR: Trained by CIA to cope in the most demanding of driving conditions.

DRIVER'S WINDOW: Tough enough to withstand armour-piercing bullets. The only window that opens - by just three inches - so the driver can pay a toll or talk with secret service agents running alongside.

BODYWORK:

Combination of dual hardness steel, aluminium, titanium and even ceramic to break up possible projectiles.

DRIVER'S COMPARTMENT:

Standard steering wheel, but dash board contains a communications centre and GPS tracking system.

BOOT:

Holds oxygen supply and a firefighting system.

FACTFILE

- Price: £300,000
- Length: 18ft
- Height: 5ft 10in
- Engine: 6.5 litre diesel engine.
- Max speed: 60mph.
- 0-60mph: 15secs
- Fuel consumption: About eight miles to the gallon.

REAR SEATS:

Obama's seat has an executive package featuring a foldaway desktop, laptop computer with wi-fi, state of the art satellite phone and direct line to the vice president and the Pentagon.

DEFENCE ACCESSORIES: Equipped with night vision cameras and pump-action shotguns. Also armed with tear gas cannons. Bottles of the president's blood kept on board in case he needs an emergency transfusion.

CHASSIS: A reinforced five inch steel plate runs under the car for protection in the unlikely event of a bomb being placed underneath.

TYRES: Kevlar-reinforced, shred and puncture-resistant, with steel rims underneath, enabling the car to escape at speed even if tyres are blasted away.



The unfinished Cadillac under test this week

Graphic by John Lawson

Security Reality Today

- State of denial is over
 - Transference of risk is next
...getting more difficult
- Compliance mandates
 - Duty to protect the public
...not just assets
- Cost escalation
 - 10% of IT budget and growing
...not sustainable, need a better approach



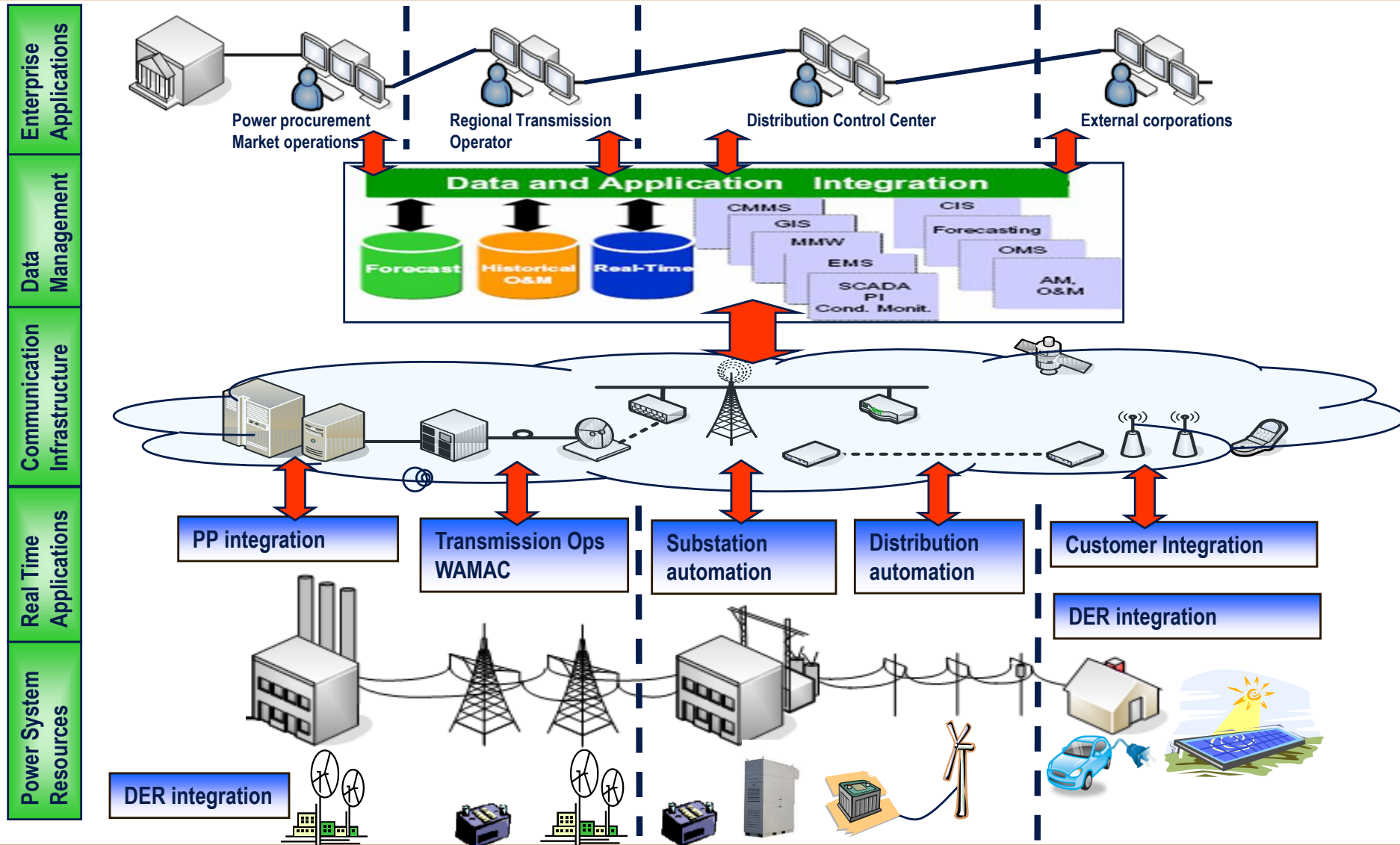
Network is the Battlefield

- Now()
 - Practically all critical infrastructure and key resource elements have an IT backbone
 - Needs to be available, reliable, and secure
- Tomorrow()
 - New initiatives and more dependency on internet
 - Cloud Computing
 - Energy distribution
 - Transportation

1-Watt GPS Jammer



EPRI IntelliGrid – Real Time Integration



Trust

Application services must trust infrastructure
and

Application services must be trusted

What is the basis for trust?

A Non-Trivial Challenge

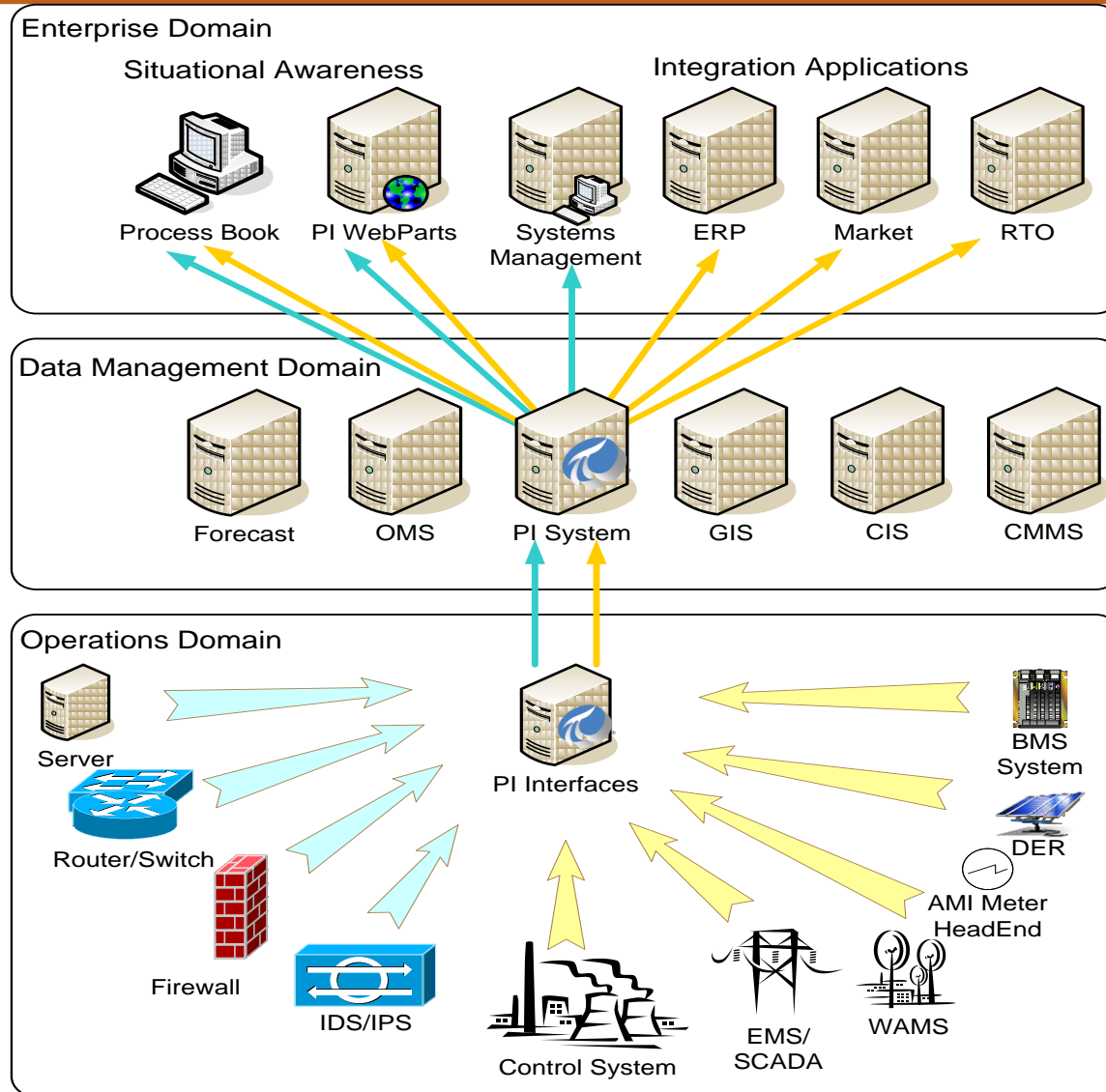
- Cyber security is asymmetric warfare
 - Defend against all possible attacks, even the unknown
 - New defenses are expensive, new attacks are cheap
 - Deterrence can't be measured, but exploits can

Approach

- Plugging holes faster is not enough
 - Need to build a proactive stance
 - Effectively block attackers
 - Delay, disrupt and “disincentivize”
 - Technical and non-technical means
- Use all available intelligence
 - Tap security features and resources
 - Enable defenses
 - Instrument, collect, and analyze logs
 - Effective collaboration



Operational Data Management

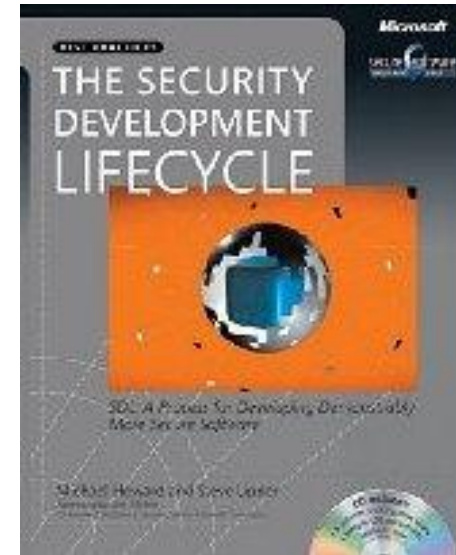


Digital Bond – Portaledge

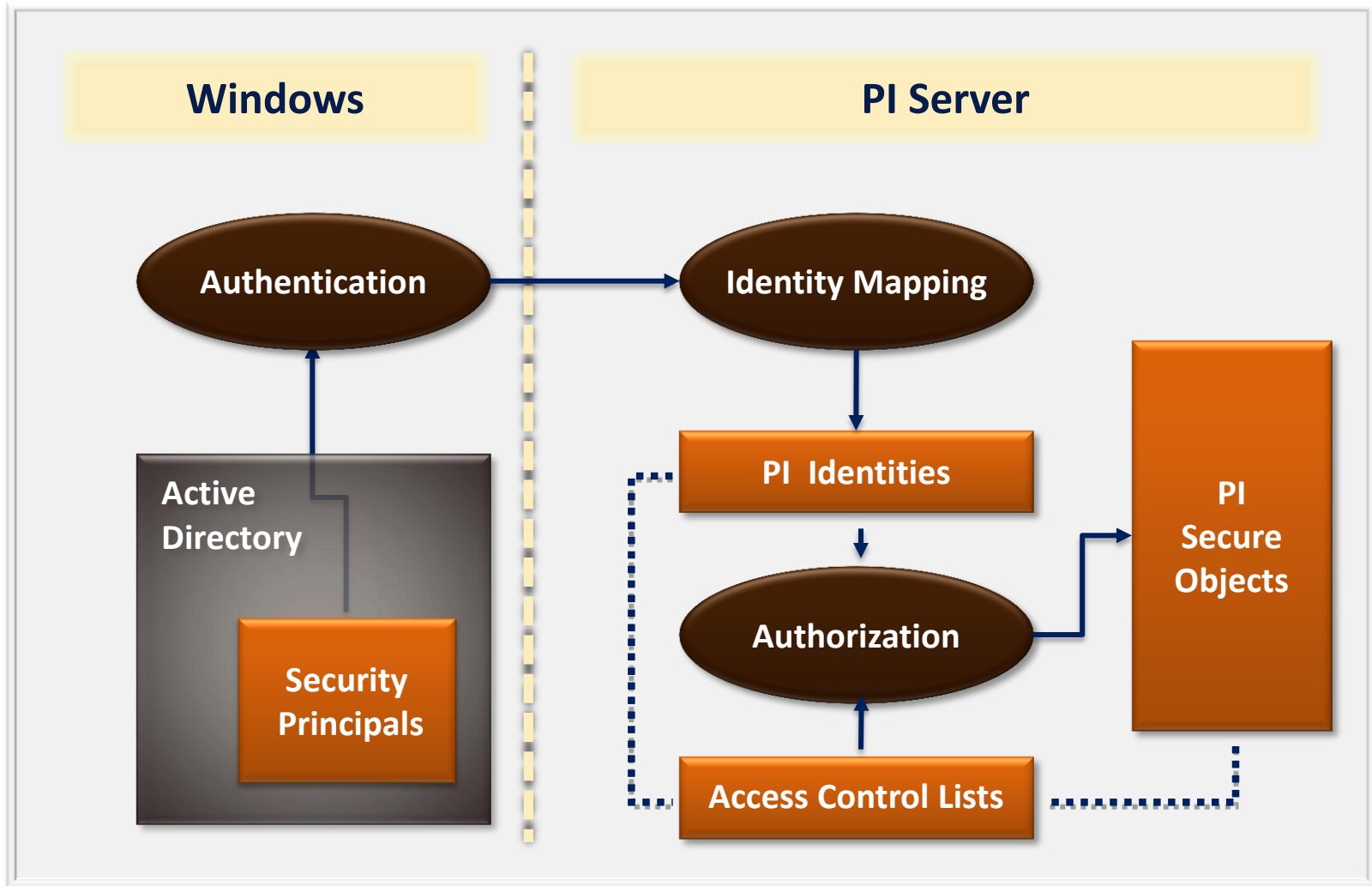
- Project funded by the U.S. Department of Energy
 - PI is widely deployed in the energy sector
- Adds capability to detect cyber attacks
 - Aggregate and correlate security events in PI
 - Uses IT Monitor + PI ACE
- Design, manuals and source online: “Scadapedia”
 - Released modules
 - Availability – computer, network, system degradation
 - Enumeration – port scan, anomalous network traffic

Affect on ISV Solutions

- Accountable
 - Verify software supply chain
...minimize on-going risk
- Agile
 - Build for security not just compliance
...adapt to emerging threats
- Affordability
 - Leverage infrastructure services
...Windows integrated security “WIS”



WIS Overview



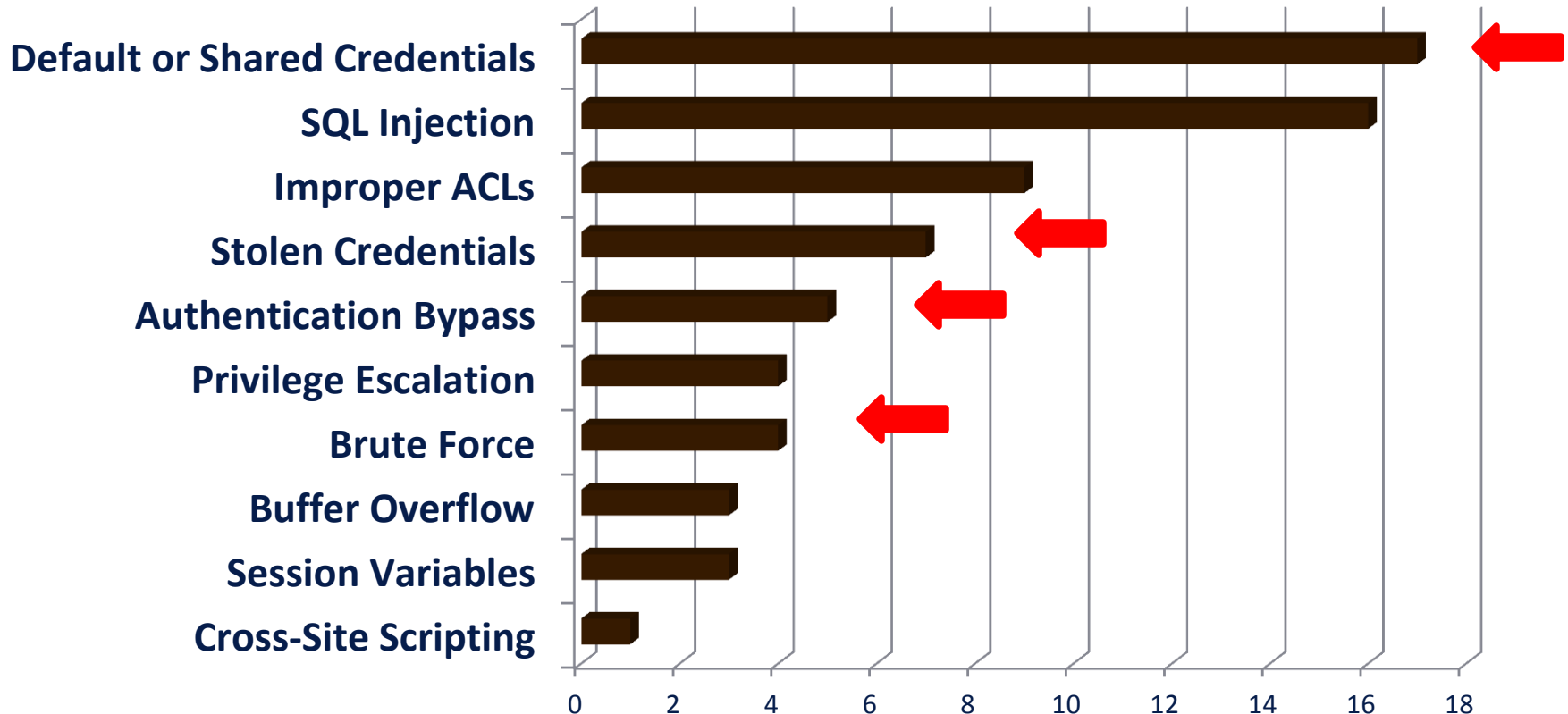
WIS Implementation Benefits

- **Enhanced security**
 - Increased control and flexibility
 - Standards and compliance templates
- **Less Maintenance**
 - Stability
 - Domain accounts
- **Better Manageability**
 - System Management Tools (SMT)
 - Group policy tools
- **Lifecycle Support**
 - Backward compatible
 - Windows 2008 R2 (x64) on Server Core



Authentication – Still the Weakest Link

Hacking Breach by Type



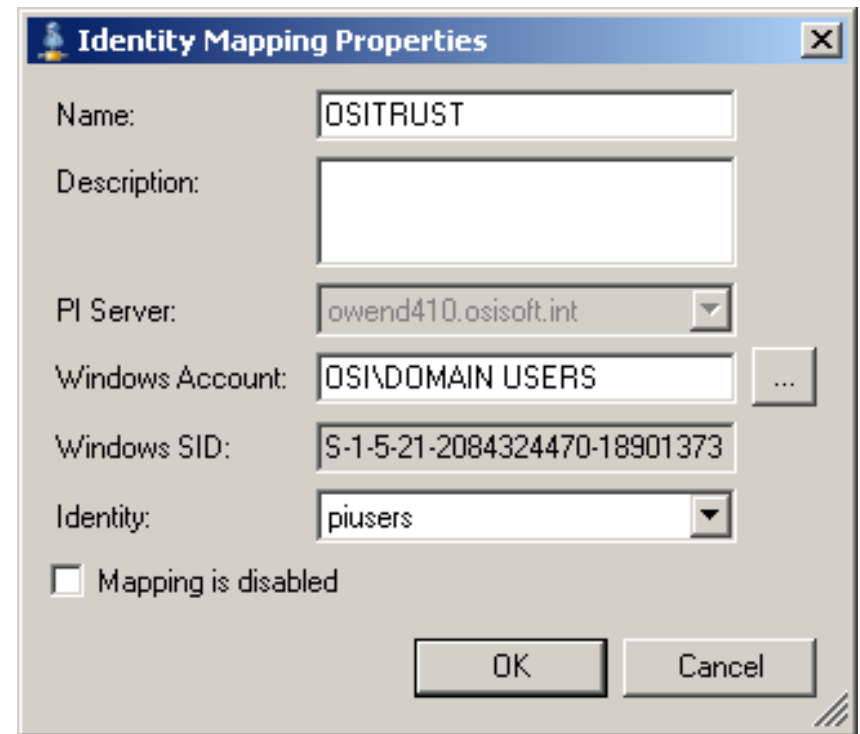
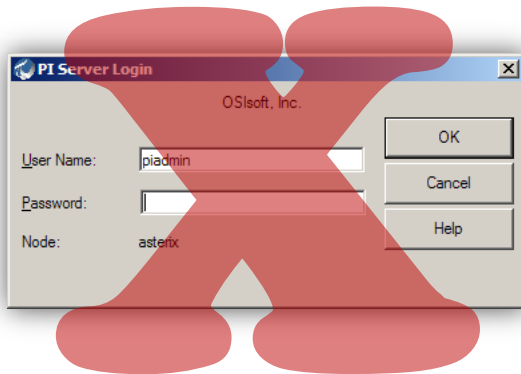
Source: 2009 Verizon Data Breach Report

WIS Prerequisites

- Client application using PI-SDK 1.3.6
- PI Server 3.4.380
- Domain membership strongly recommended
 - Clients, application servers, database servers
 - PI Interface nodes remain centric to data source

Mapping Active Directory Groups

- Single Sign On – Windows Security (Kerberos)
 - One time mapping for Active Directory Groups



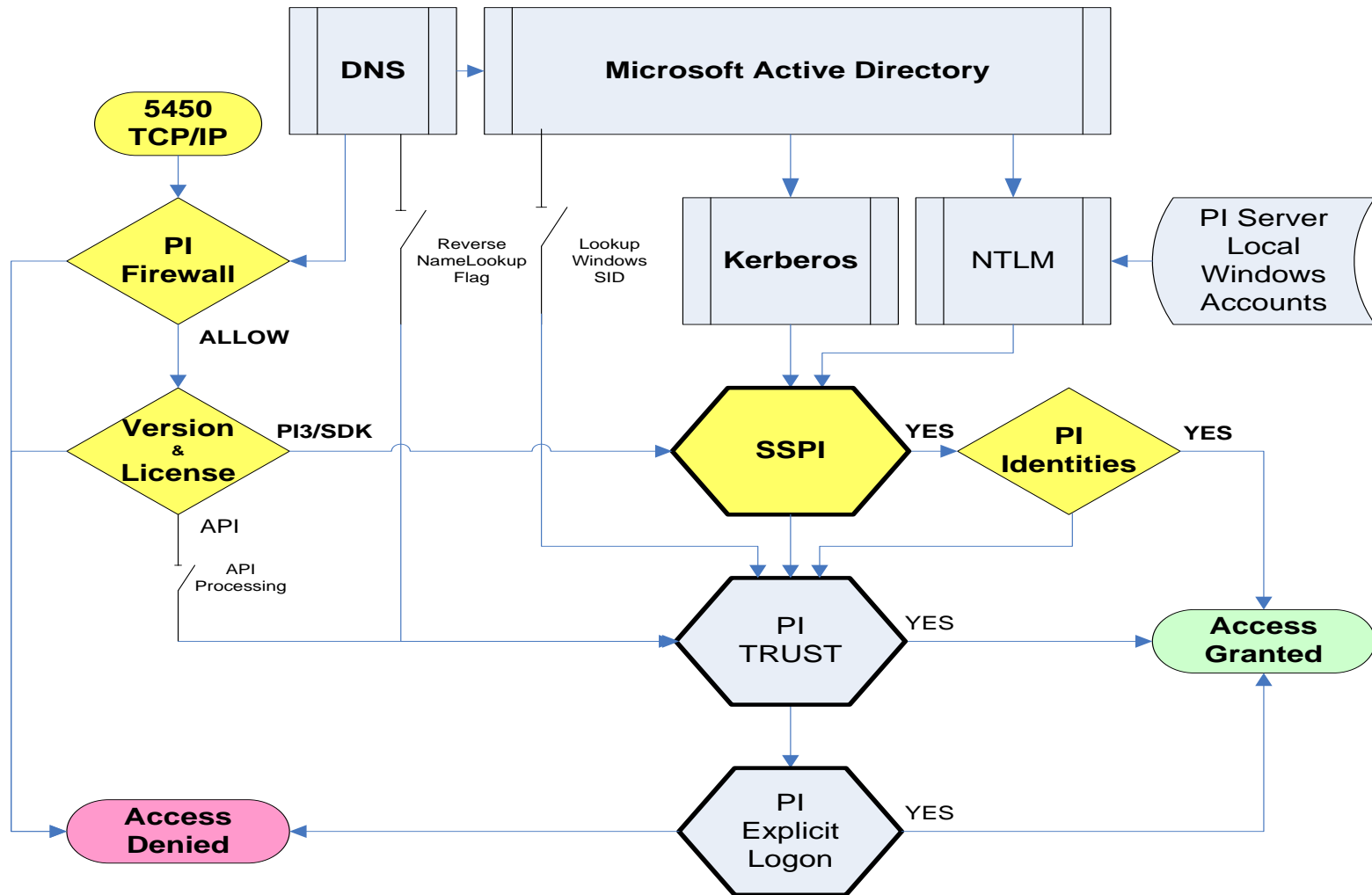
Legacy Methods are Weak

- Security Alert: PI Authentication Weakness
 - [OSIsoft Technical Support Bulletin](#)
 - Eliminate use of PI User passwords in versions prior to WIS (KB Article # [KB00304](#))
 - 2009/09/30 C4 SCADA Security Advisory
 - US CERT [CVE-2009-0209](#)

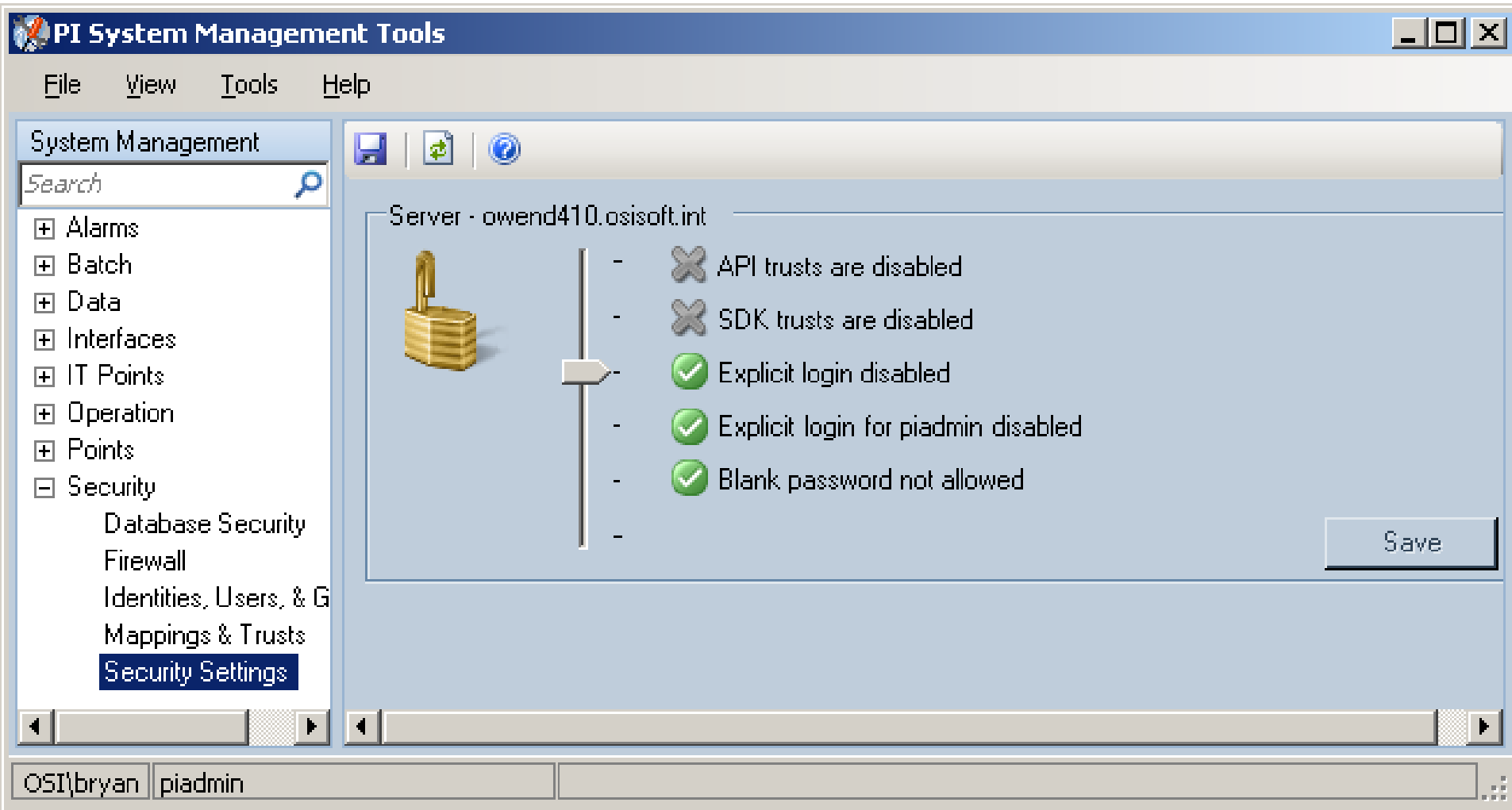
Installation Warning



Authentication Path

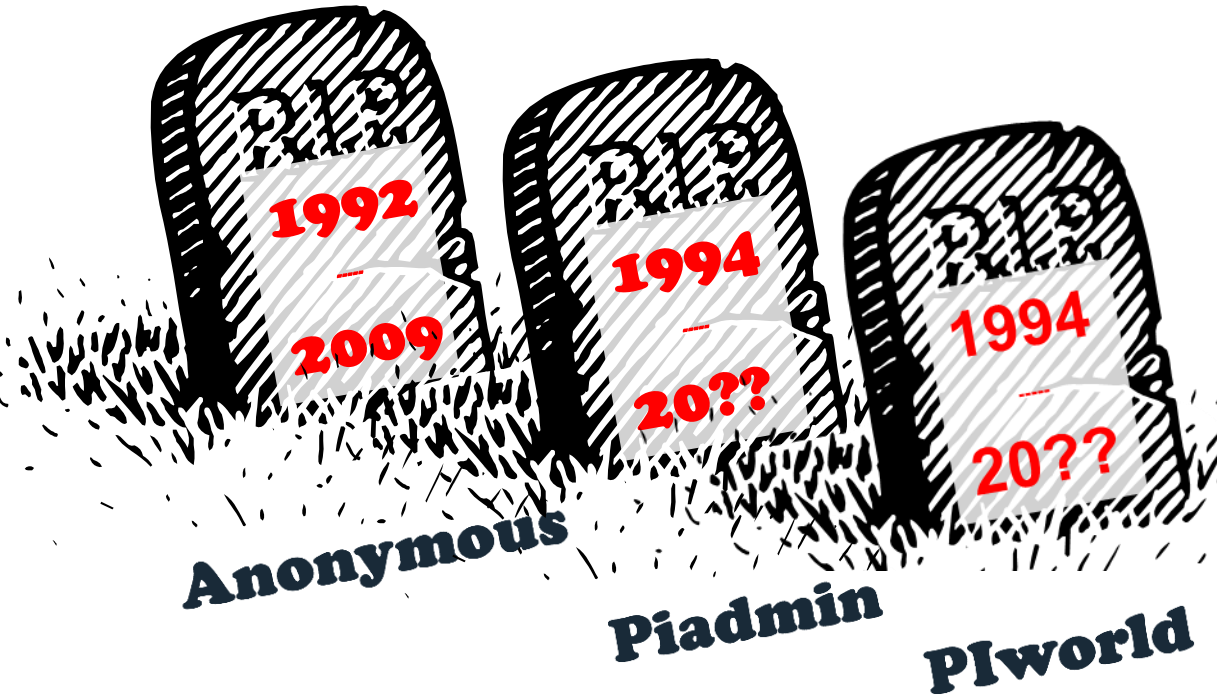


PI-SMT Security Settings



Authentication Policy

- Policies to Allow and Prioritize Methods
 - Windows SSPI
 - PI Trust
 - Explicit Login
- Granular Scope
 - Server
 - Client
 - Each Identity



Group Policy for WIS

- Access this computer from the network
 - Remove “Everyone” default
- NTLM
 - Sharing and security model for local accounts
 - Change “Guest” to “Classic” (guest is Windows XP default)
 - Lan Manager authentication level
 - Run at level 5 to prevent downgrade attacks
- Kerberos
 - Configure PI WebParts for SSO using Kerberos (KB Article # KB00100)

PI-SDK Programming and WIS

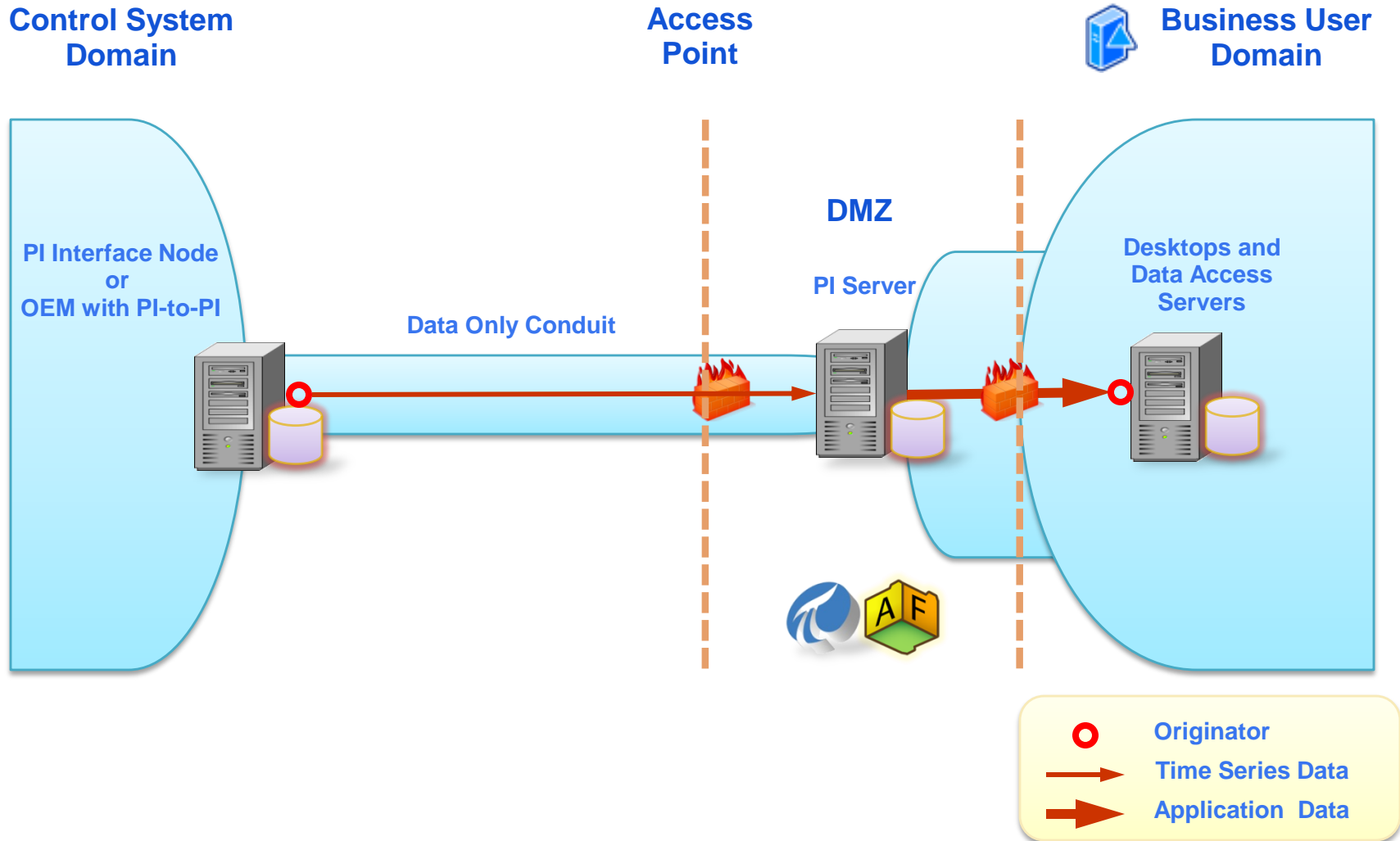
- Server Object “CurrentUser”
 - List of PI identities granted for this connection
- New: IServerConnect interface “DisplayUser”
 - Normally represents the Windows user
- Unimplemented methods are documented
 - Is programmatic access to WIS configuration needed?
 - Is Piconfig enough?

Authentication Summary

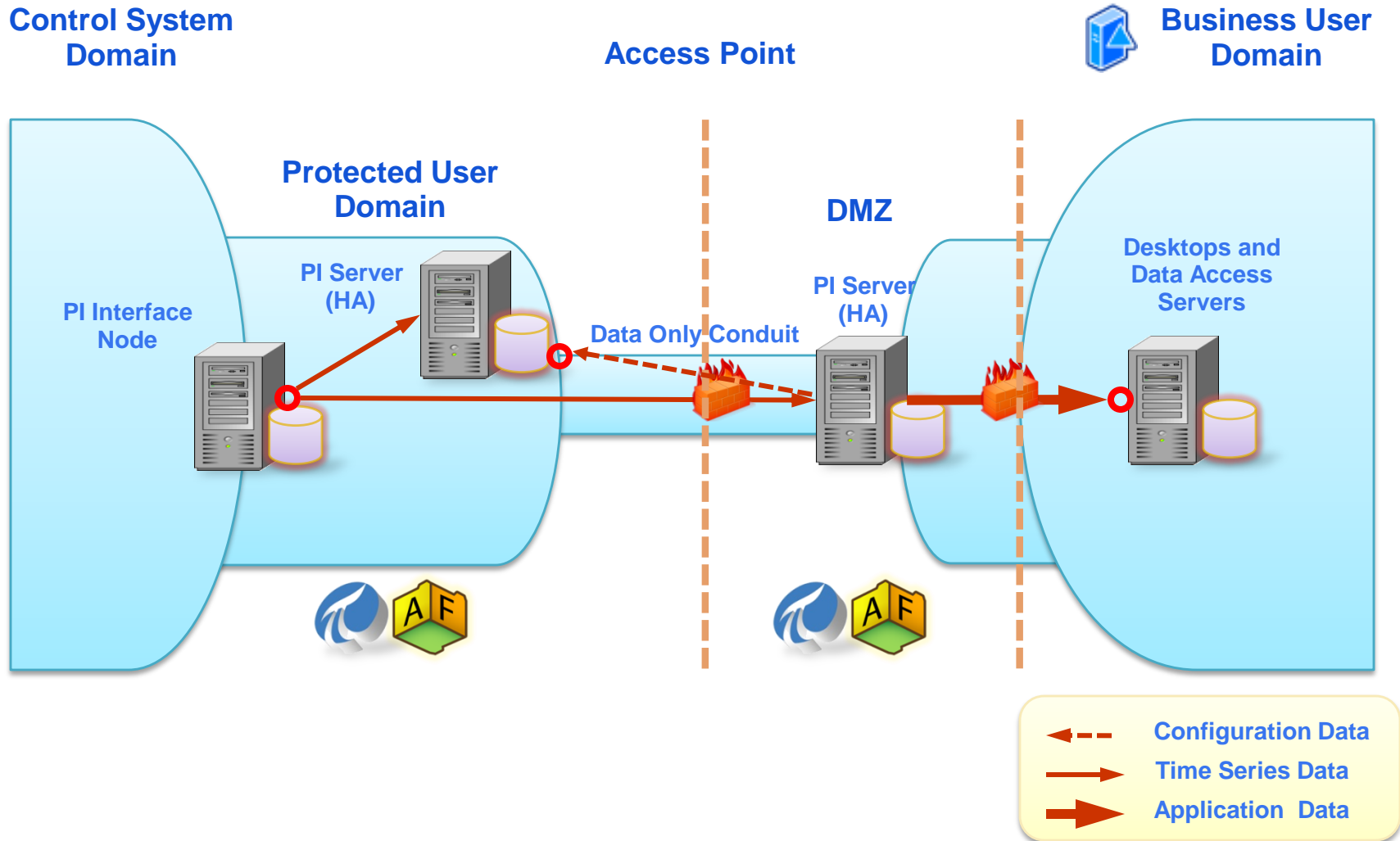


- Domain Membership
 - Strongly Recommended
 - Clients and Servers
- Manage Users and Groups
 - Centrally in Windows
 - One time association in PI
- Explicit Login and Trust
 - You have control

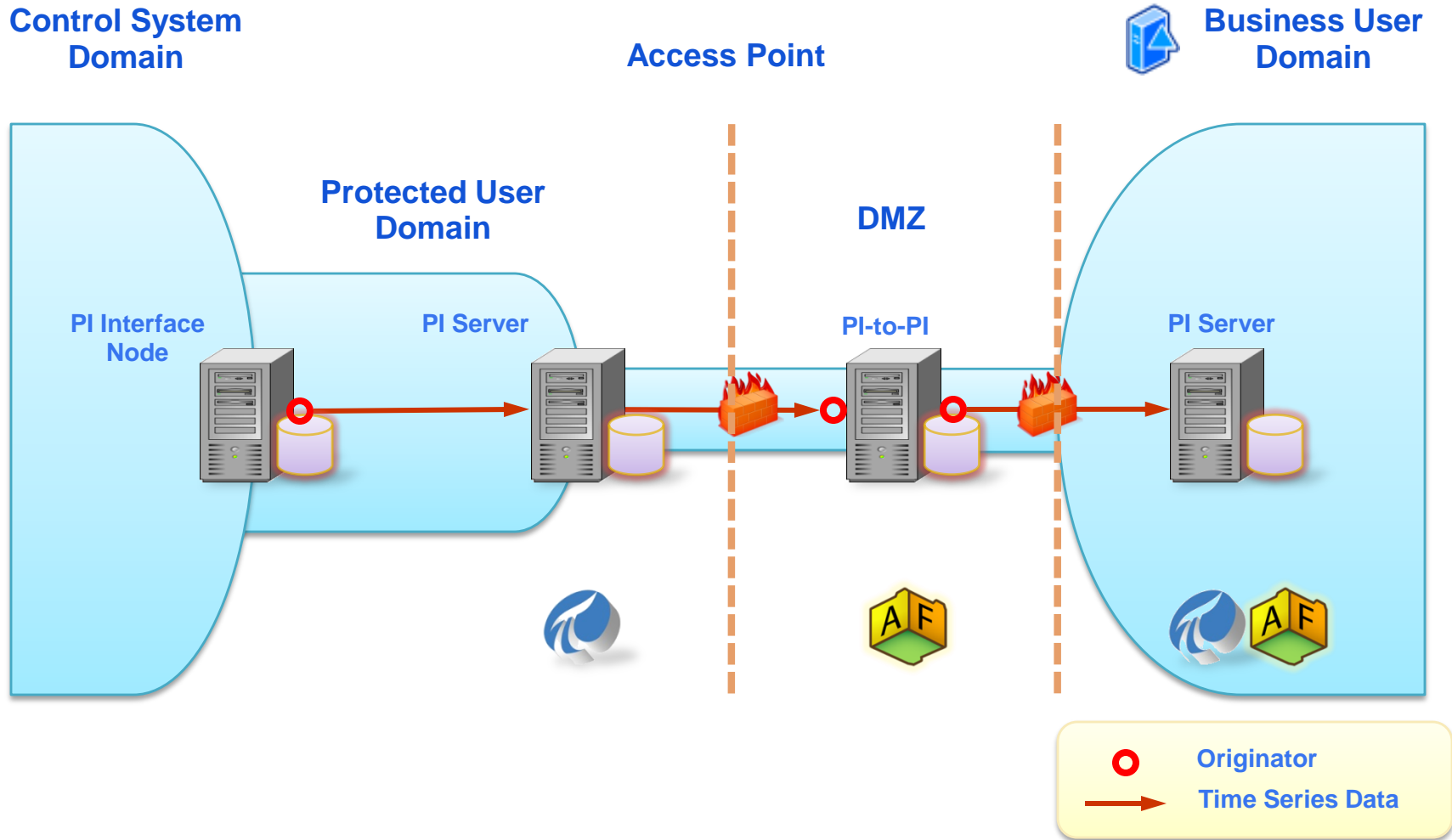
Basic Deployment Pattern



High Availability Deployment Pattern



PI to PI Deployment Pattern



What else in PI 3.4.380?

- PI Network Manager
 - Stability and hardened stack
 - Performance
 - Enhanced SMT plug-in
- Message Log Subsystem
 - Filter by severity
 - Critical, Error, Warning, Informational, Debug
- Audit Trail
 - Windows user preserved



Backup Enhancements

- Backup
 - Performs incremental backup
 - Checks integrity
 - Maintains “Last Known Good”
 - New SMT plug-in
 - On demand copy backup
 - Viewing backup history



Certification and Security

- Windows Server 2008 R2 'Certified' program
 - Goal: increase quality of applications
 - More compatible, reliable, secure
- A few of the security requirements
 - Instrument for User Account Control (UAC)
 - SSPI authentication must use secure default
 - Digitally sign all executables
 - Must not relax default security settings
 - Document exceptions: AntiVirus, Firewall

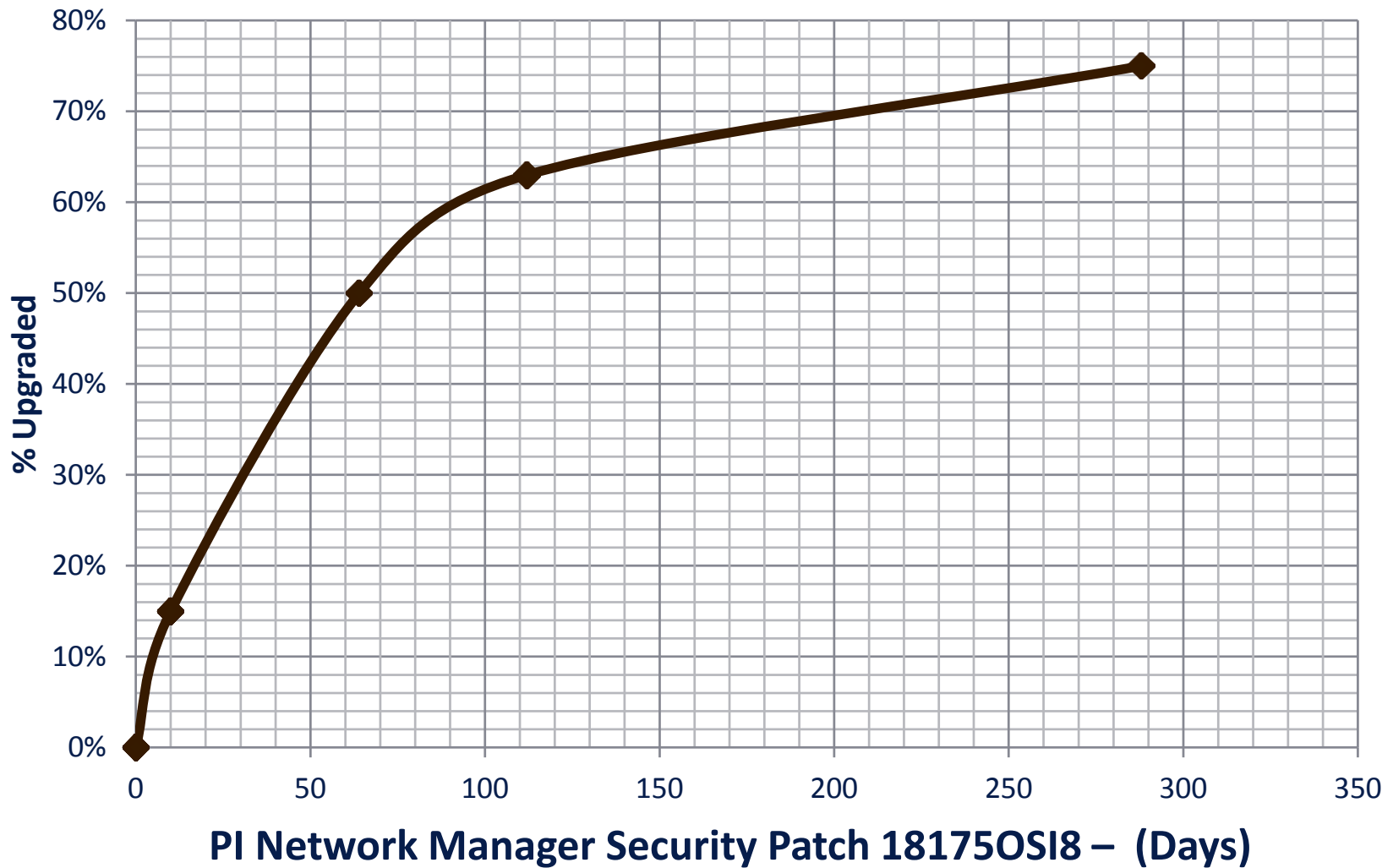


Our Commitment to You

- Ongoing focus of Security Development Lifecycle
 - Help you with Best Practices
 - Reduce effort and improve usability
 - Eliminate Weakest Code
 - Cumulative QA effort with every release
 - Collaborate with Security Experts
 - Industry, Government, Academia, Partners, Customers



When will you Upgrade?



Being Secure Is...

- More than regulations and features
 - Technology can help
- A state of mind, knowing
 - Your systems
 - What to do
 - Who you trust
 - OSIsoft wants to earn your trust



```
1. point.Snapshot;  
2. Dim srv As PISDK.Server  
3. Fore*%*) (point in server.PIPoints)?!!??  
4. Dim srv A PISDK.Server  
5. if (time_to_market > expected)  
2. Dim srv As PISDK.Server  
3. Fore*%*) (point in server.PIPoints)?!!??  
4. Dim srv A PISDK.Server  
5. if (time_to_market > expected)
```

OSIsoft®

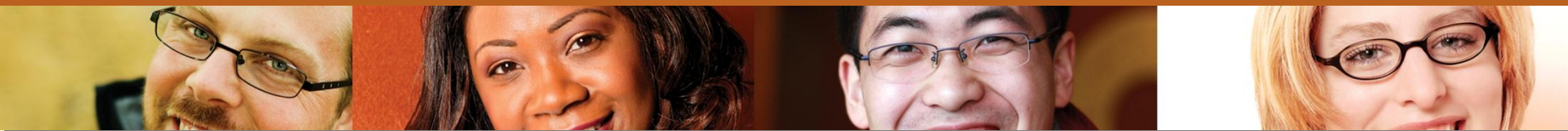
V

CAMPUS | LIVE!

2009

"where
PI geeks
meet"

THANK YOU.



```
1. foreach (point in server.PIPoints)  
{  
    point.Snapshot;  
}  
2. Dim srv As PISDK.Server  
3. Fore*%*) (point in server.PIPoints)?!!??  
4. Dim  
point.Snapshot;  
2. Dim srv As PISDK.Server  
3. Fore*%*) (point in server.PIPoints)?!!??  
4. Dim srv A PISDK.Server  
5. if (time_to_market > expected)
```

© 2009 OSIsoft, LLC. | OSIsoft vCampus Live! | where PI geeks meet