



OSIsoft®

USERS CONFERENCE 2012

The Power of Data



Have you done enough with Cyber Security?

Presented by **Bryan Owen**, OSIsoft
Joel Langill, SCADAhacker

Agenda

Moore's Law



Attack Patterns and Demo



Domain Services in a DMZ

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.*



Anatomy of an Attack

Information
Gathering



Scanning
Enumeration
Fingerprinting

*Turning point ...
When a threat
becomes an attack!*

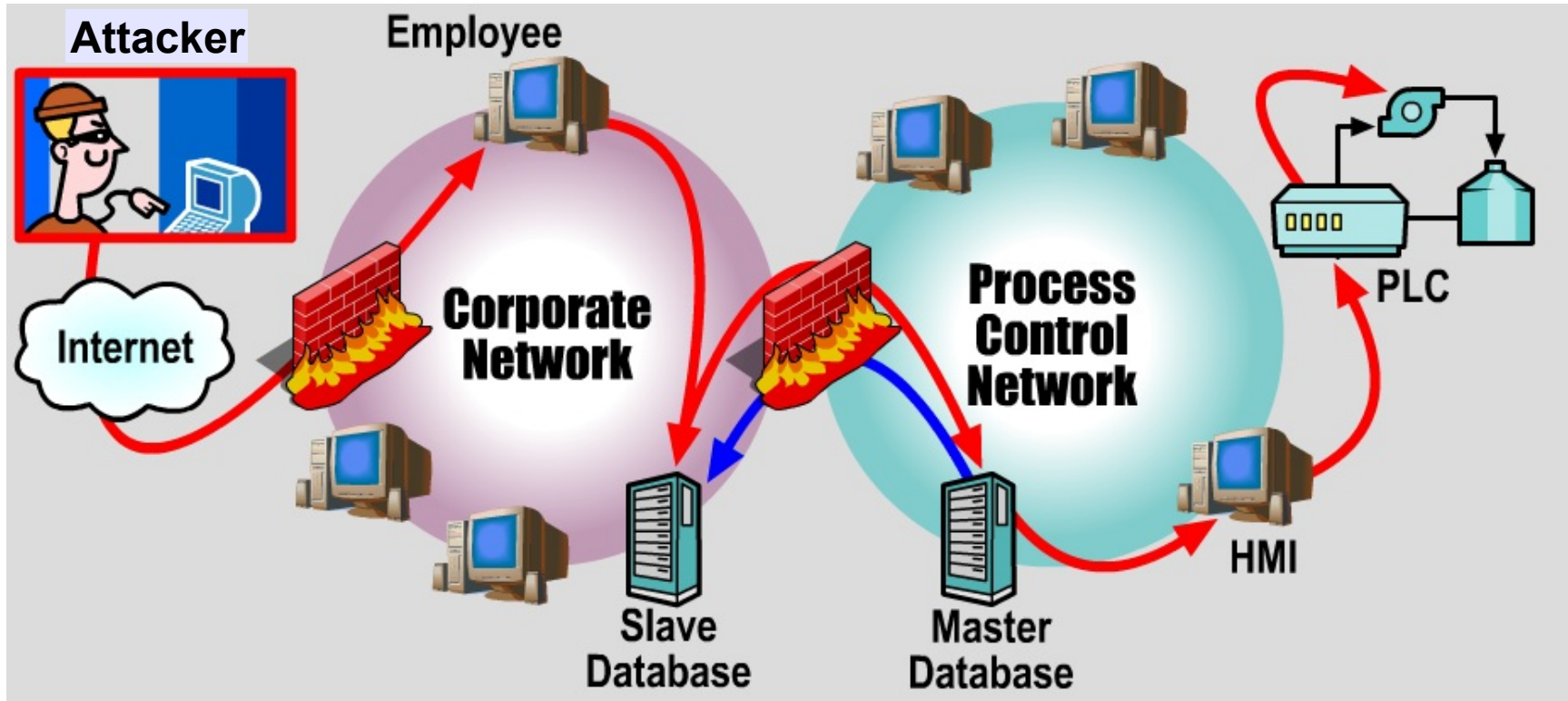
Gaining
Access

Maintaining
Access

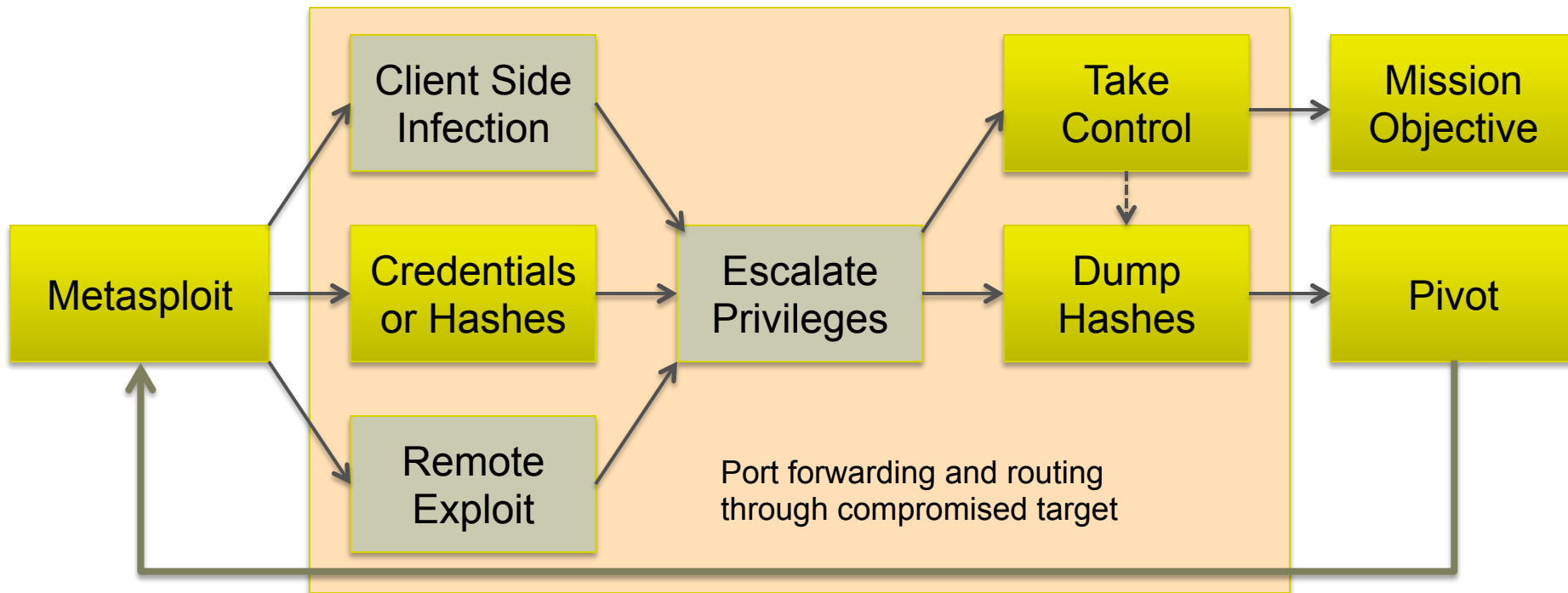
Covering
Tracks



Attack Process



Pivot Attacks



Pivot using “Pass the Hash”

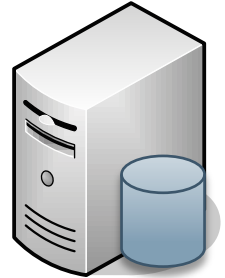
LMhash=fn(“password”)
NThash=fn(“password”)



Request Access

Random Challenge

fn(Hash,Challenge)



Stolen hash is as good as a password!

Windows password hashes are protected except:

- Administrators and users with ‘Debug programs’ rights
- Processes with ‘Act as part of the operating system’ rights

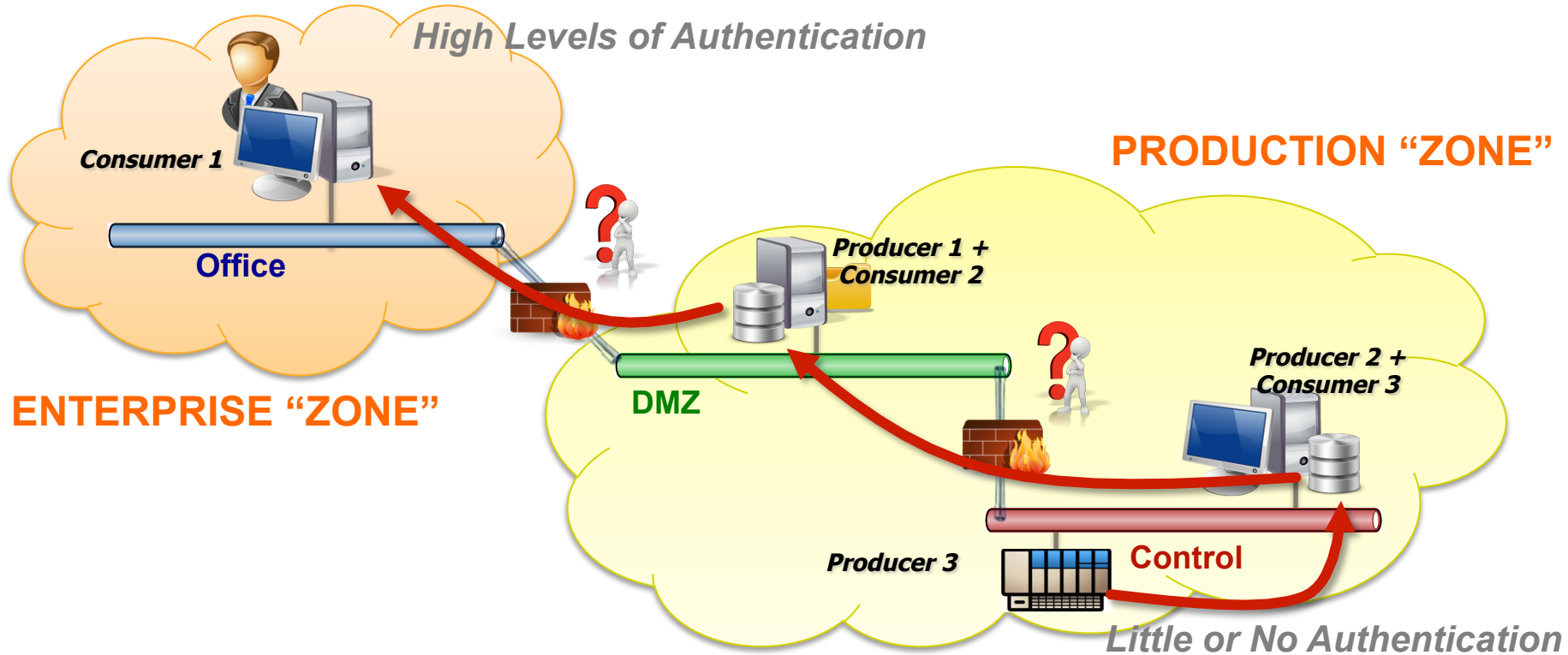


PLEASE
PAUSE
FOR
DEMO

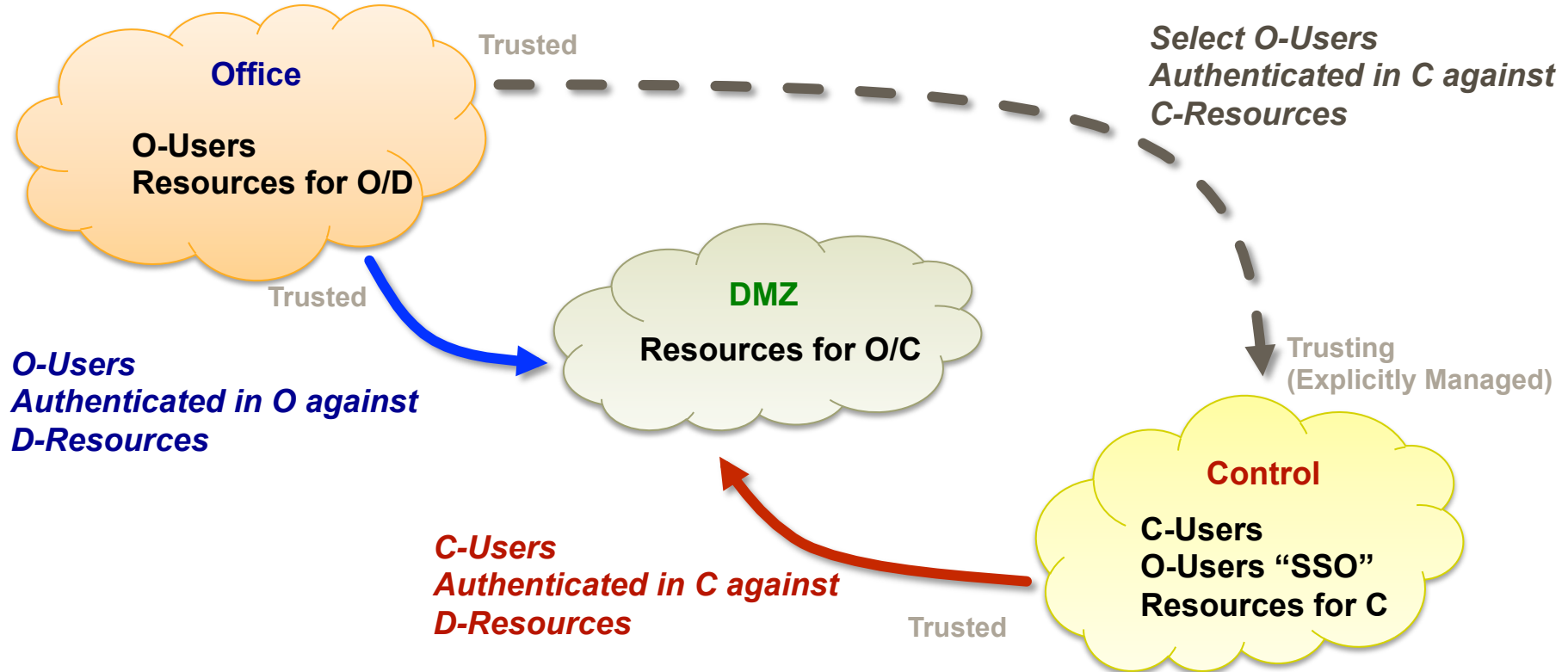
Finding the 'Right' Balance

- Access to Information, Ease of Administration
 - Many companies are moving the direction of a “single sign-on” or SSO approach
 - Authentication and Credential Management remain as a top vulnerability within manufacturing systems
- Network segmentation, Domain services
 - Enterprise and control are often separated by a “DMZ” network
 - Administration, Cost and Compliance burden are top concerns

Manufacturing Info Data Flow



Trust and the 3-Zone Model

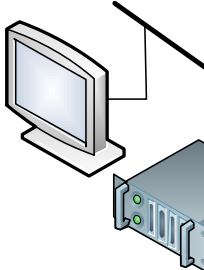


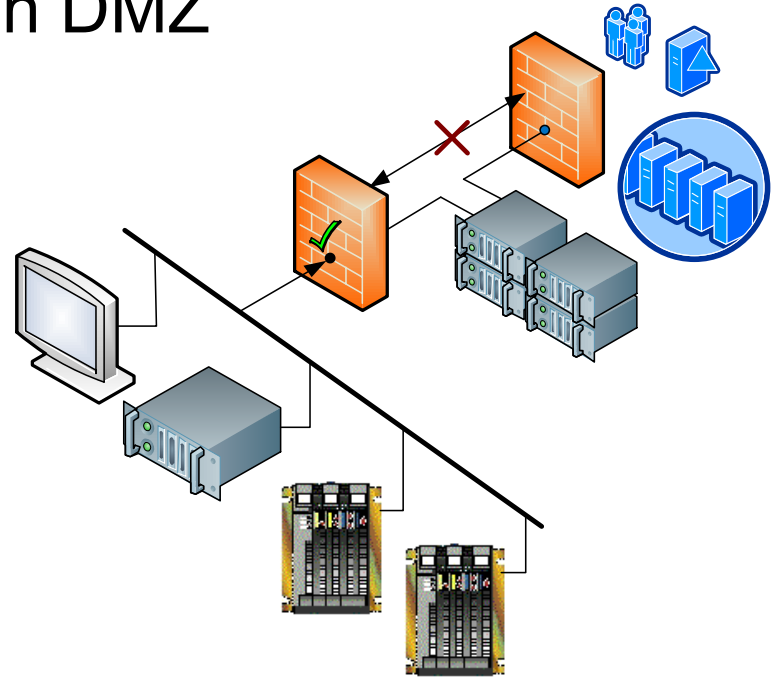
Network Segmentation Standards

DHS CSSP, ISA 99, NERC CIP, NIST 800-82

**... no systems other than
firewalls should be configured as
dual-homed ...
[to span security zones]**

PI System DMZ Practices

- Terminate cross boundary traffic in DMZ
 - No thru traffic bypass exceptions
 - Block DMZ to internet
 - Restrict local logons and RDP
 - Control network
 - PI Interface node with buffering
 - Minimize office and web protocols
 - Monitor DMZ traffic
 - Separate logon authority
- 
- A diagram showing a computer monitor connected to a network switch or router. The monitor is on the left, and the switch is on the right. A line connects the monitor to the switch, indicating a network connection. The switch has multiple ports and a small display or indicator light.



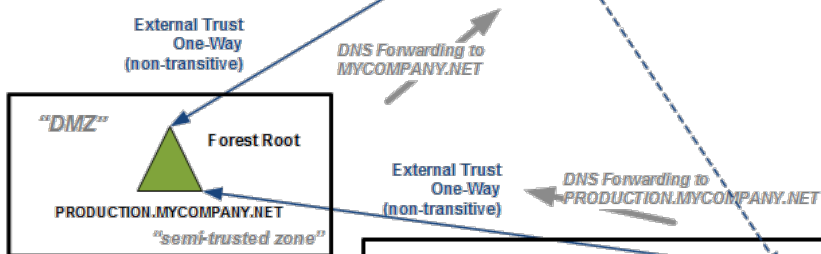
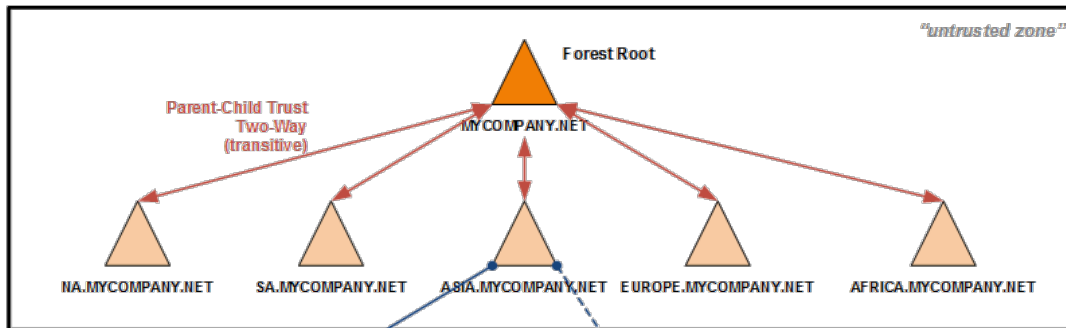
Considerations for Authentication

- Active Directory Domains and Forests
 - Levels of Autonomy (trust) vs Isolation (no trust)
 - Differences in Group Policies
 - Separation of “General” & “Administrative” Rights
- Network
 - Active Directory Replication (Global Catalog Integrity)
 - Kerberos or NTLM

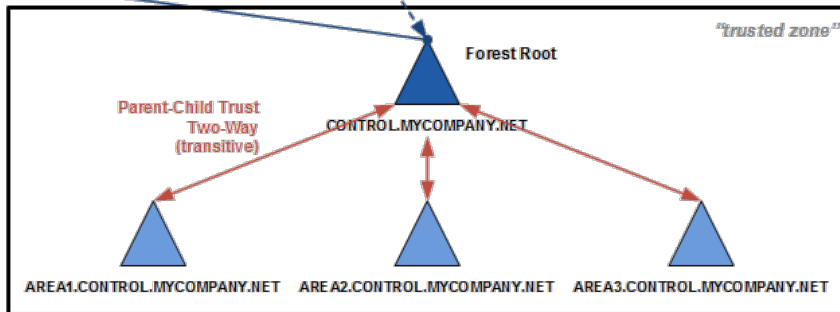
SSO Authentication Options

1. Synchronized Credentials (Password Managers)
- ~~2. Integrated Forest – Single Domain~~
3. Integrated Forest – Unique Domains
4. Unique Forests

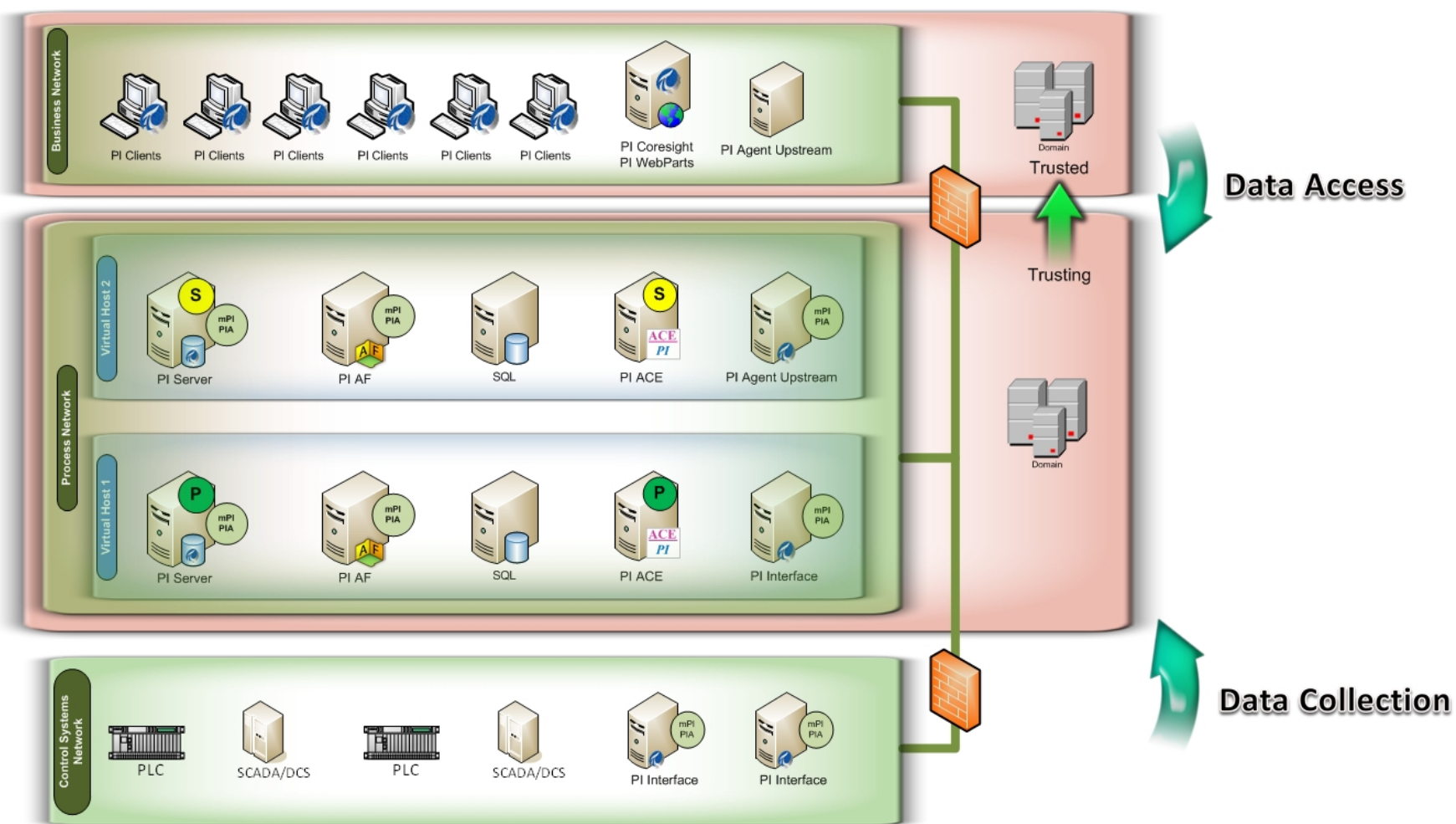
FEATURES vs AUTHENTICATION OPTIONS	SYNCHRONIZED CREDENTIALS	SINGLE FOREST	MULTIPLE FORESTS
Single Account to Manage	No	Yes	Yes
Password Hashes Shared between Office/Production	2	1	n/a – Tickets
Segregation of Administrative Rights	Yes	No	Yes
Trust Transitivity between Office/Production Domains	n/a	Transitive	Non-Transitive
Trust Definition between Office/Production	n/a	Implicit Explicit	None
Trust Direction	n/a	2-way	1-way
Scope of Authentication	Local	Any Domain in Forest	Any Domain in Forest
Global Catalog / Schema	n/a	1	2
Replication across Firewall	n/a	Yes	No
Replication Requirements (DC to DC)	2 tcp / 2 udp	9 tcp / 3 udp (2003) 10 tcp / 6 udp (2008)	1 tcp / 1 udp



Forest: PRODUCTION.MYCOMPANY.NET



Forest: CONTROL.MYCOMPANY.NET



Call to Action

- Restrict access with DMZ and AD domain services
- Caution on use of administrator accounts
- Maintain applications, operating system, and network
- Decide on an approach you can sustain
 - Involve subject matter experts in your process

Bryan Owen

bowen@osisoft.com

Cyber Security Manager
510-347-2630

Jim Davidson

jdavidson@osisoft.com

Security Products Manager
208-520-2806

Joel Langill

joel@scadahacker.com

ICS Security Specialist
SCADAhacker

@bryansowen
@davijim
@SCADAhacker



Additional References

- Active Directory Replication Over Firewalls
<http://social.technet.microsoft.com/wiki/contents/articles/active-directory-replication-over-firewalls.aspx>
- How to Configure a Firewall for Domains and Trusts
<http://social.technet.microsoft.com/wiki/contents/articles/active-directory-replication-over-firewalls.aspx>
- Active Directory Domain Services in the Perimeter
[http://technet.microsoft.com/en-us/library/dd728034\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd728034(WS.10).aspx)
- Windows Security Requirements for PI Server 3.4.380.36 and later (OSIsoft KB00354)



THANK YOU

Brought to you by  **OSIsoft.**



OSIsoft®

USERS CONFERENCE 2012

The Power of Data