Cyber Security for Industrial Systems

Norton Green – Director, Executive Briefing Program

Harry Paul – Technical Support Escalation Engineer, Cyber Security Advisory Team

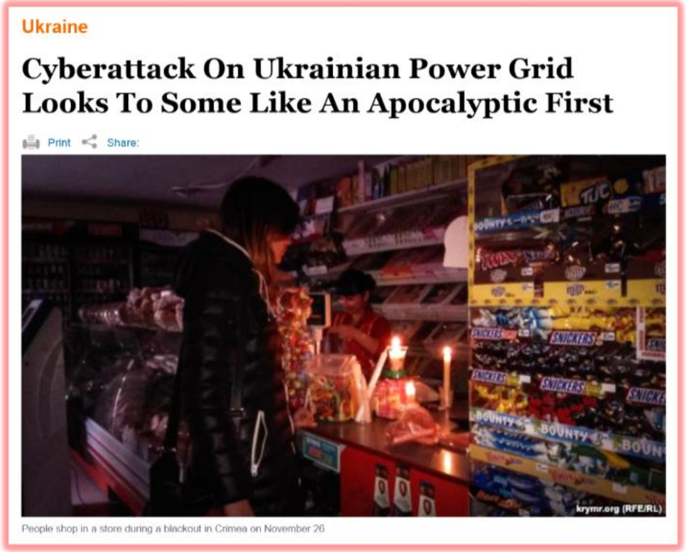
February, 18, 2016

Agenda

- Drivers for Cyber Security
- Review opportunities to Improve your security strategy

Takeaway: Cyber Security needs to be a top priority today. OSIsoft and the PI System can play a critical role in your security strategy of your Industrial systems

What keeps me up at night?



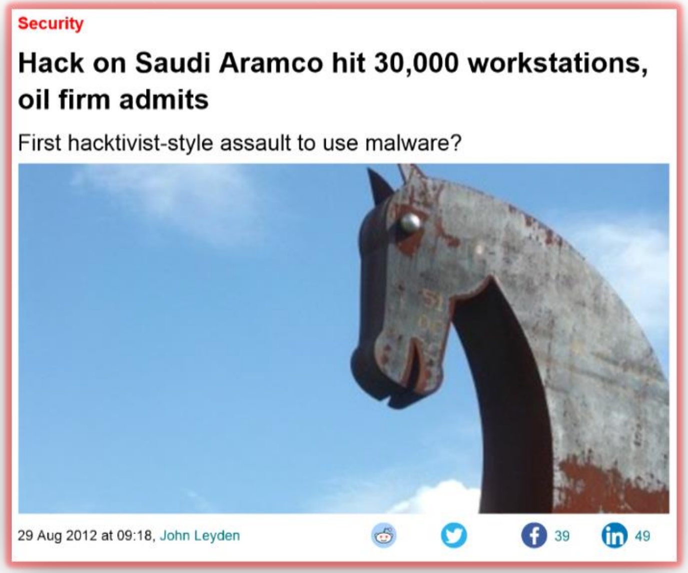
Ukraine

Cyberattack On Ukrainian Power Grid Looks To Some Like An Apocalyptic First

Print Share:

People shop in a store during a blackout in Crimea on November 26

A power company in western Ukraine, Prykarpattyaoblenergo, said on Dec. 23 that a swath of the area it serves had been left without energy, including the regional capital Ivano-Frankivsk, due to "interference" in the work of the system.



Security

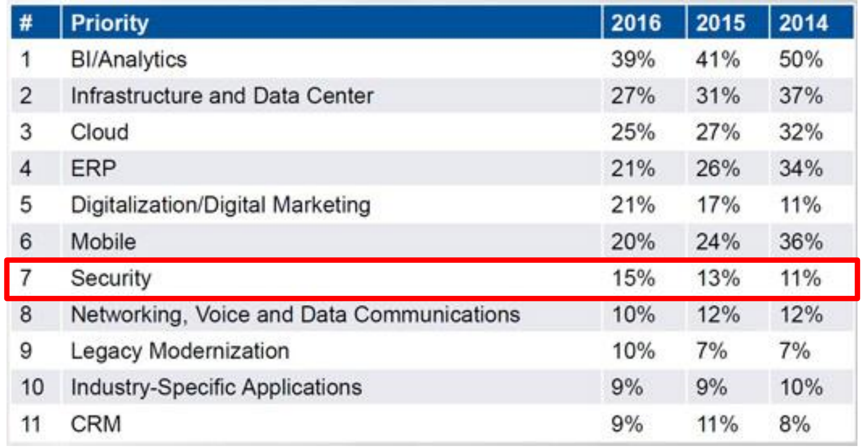
Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacktivist-style assault to use malware?

29 Aug 2012 at 09:18, John Leyden

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations. The workstations have since been cleaned and restored to service. As a precaution, remote Internet access to online resources was restricted. Saudi Aramco employees returned to work August 25, 2012, following the Eid holidays, resuming normal business.

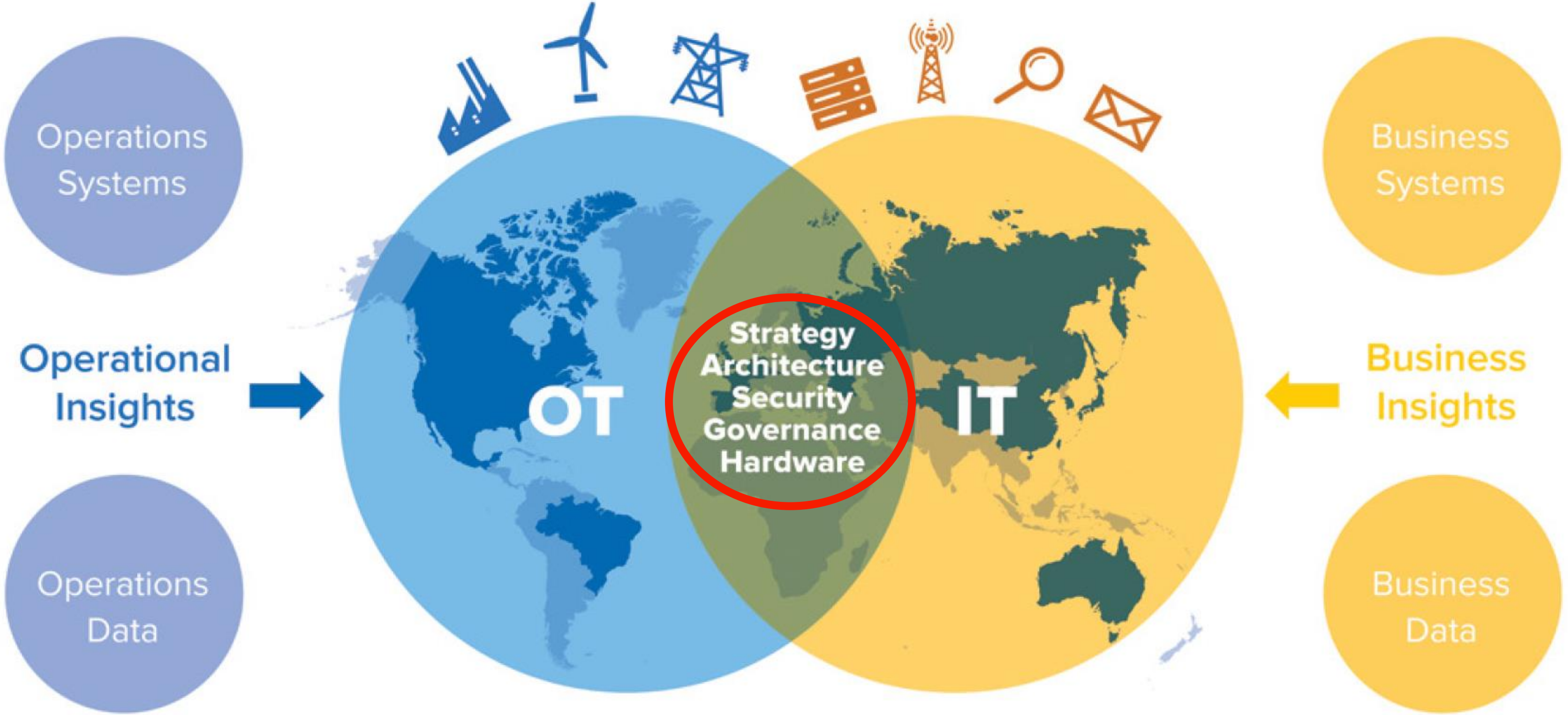
Is Cyber Security a priority for your CIO?



#	Priority	2016	2015	2014
1	BI/Analytics	39%	41%	50%
2	Infrastructure and Data Center	27%	31%	37%
3	Cloud	25%	27%	32%
4	ERP	21%	26%	34%
5	Digitalization/Digital Marketing	21%	17%	11%
6	Mobile	20%	24%	36%
7	Security	15%	13%	11%
8	Networking, Voice and Data Communications	10%	12%	12%
9	Legacy Modernization	10%	7%	7%
10	Industry-Specific Applications	9%	9%	10%
11	CRM	9%	11%	8%

Gartner Symposium IT Expo 2015

The Challenges of IT/OT Convergence



Operations Systems

Operational Insights

Operations Data

OT

Strategy
Architecture
Security
Governance
Hardware

IT

Business Systems

Business Insights

Business Data

IoT means... More sensors + More data = Larger attack surface!

30 BILLION

Sensor enabled objects connected to networks by 2020

212 BILLION

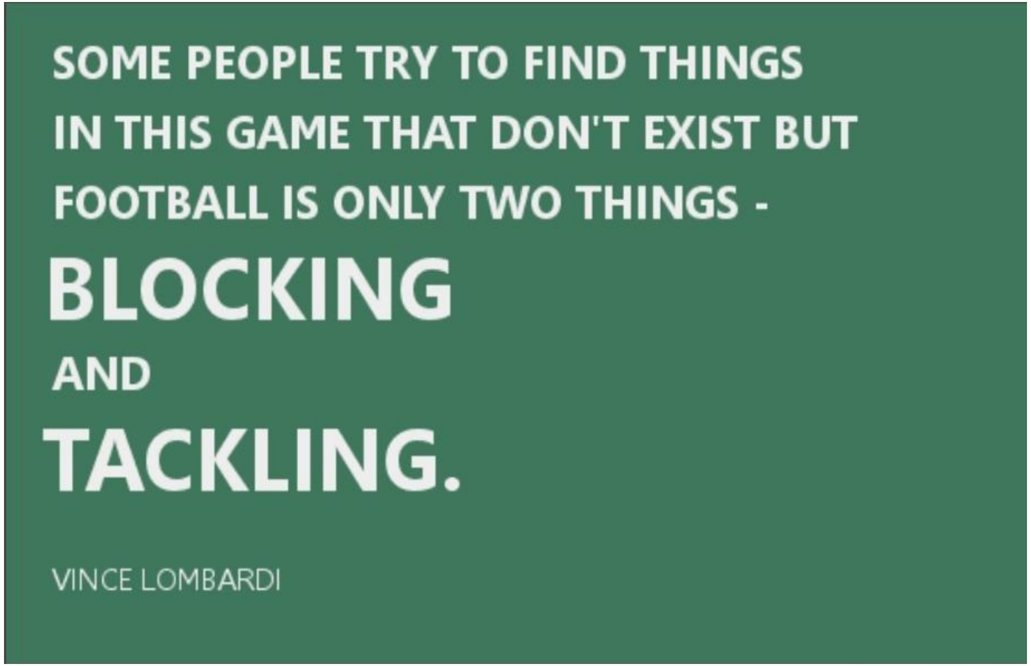
Total number of available sensor enabled objects by 2020

212B is **28x** the total population of the world

IBM Infographic for IoT and Sensors

Opportunities to improve

The “Blocking & Tackling” of Cyber Security



SOME PEOPLE TRY TO FIND THINGS IN THIS GAME THAT DON'T EXIST BUT FOOTBALL IS ONLY TWO THINGS -

BLOCKING

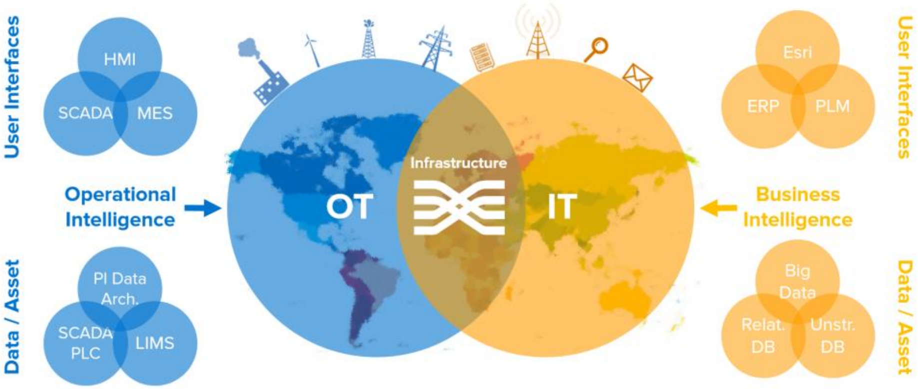
AND

TACKLING.

VINCE LOMBARDI

- ✓ Application Whitelisting
- ✓ Patch Management
- ✓ Reduce attack surface area
- ✓ Build a Defendable environment
- ✓ Manage Authentication
- ✓ Monitor and Respond
- ✓ Manage Remote access closely

Cyber Security is a team effort



- ✓ Requires participation from IT & OT with full support of Executives

- ✓ The PI System serves as the infrastructure that creates a secure “bridge” between IT and OT

There cannot be prosperity without security.

Francois Hollande
President of France

Networks are hard, people are soft

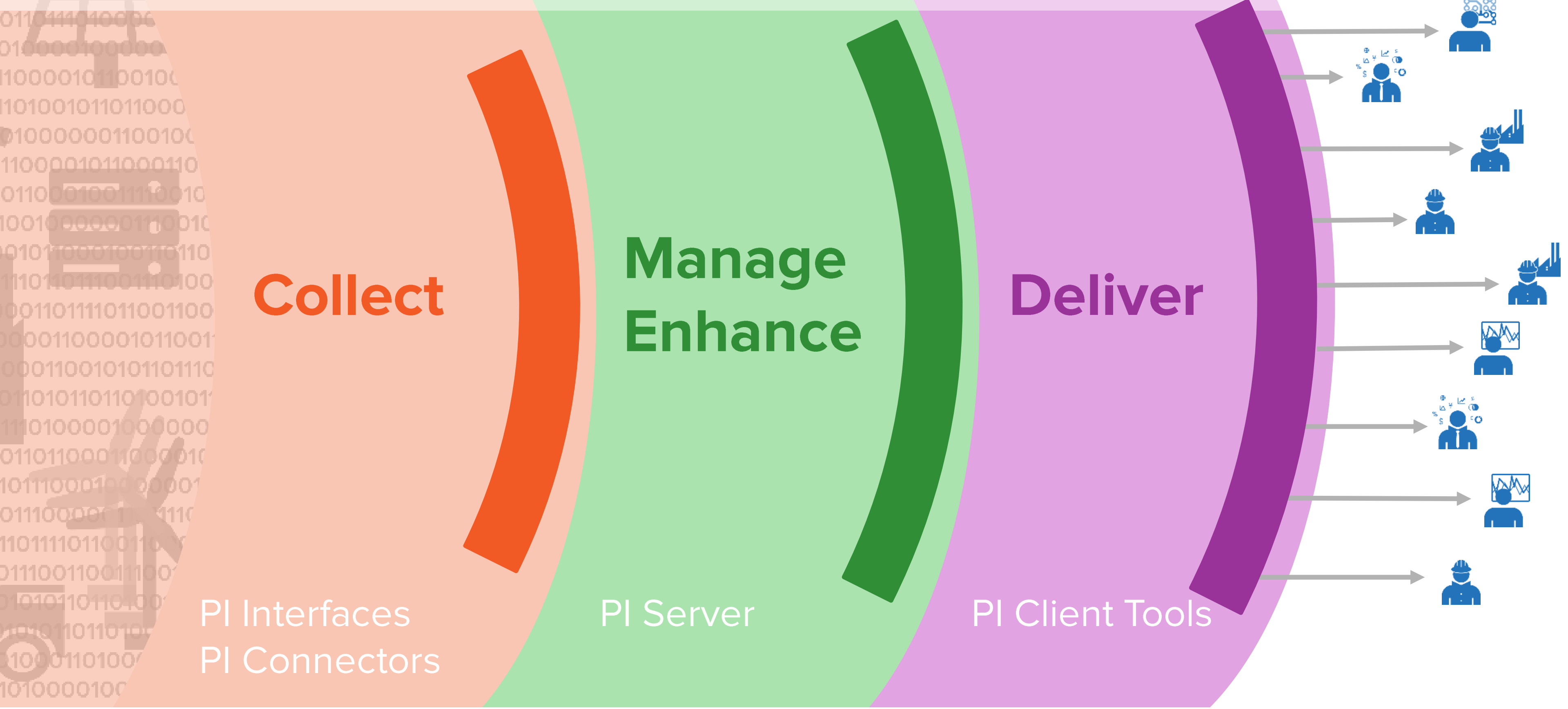
" I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

Where is the PI System in your infrastructure?

The PI System Layers



Collect

Manage
Enhance

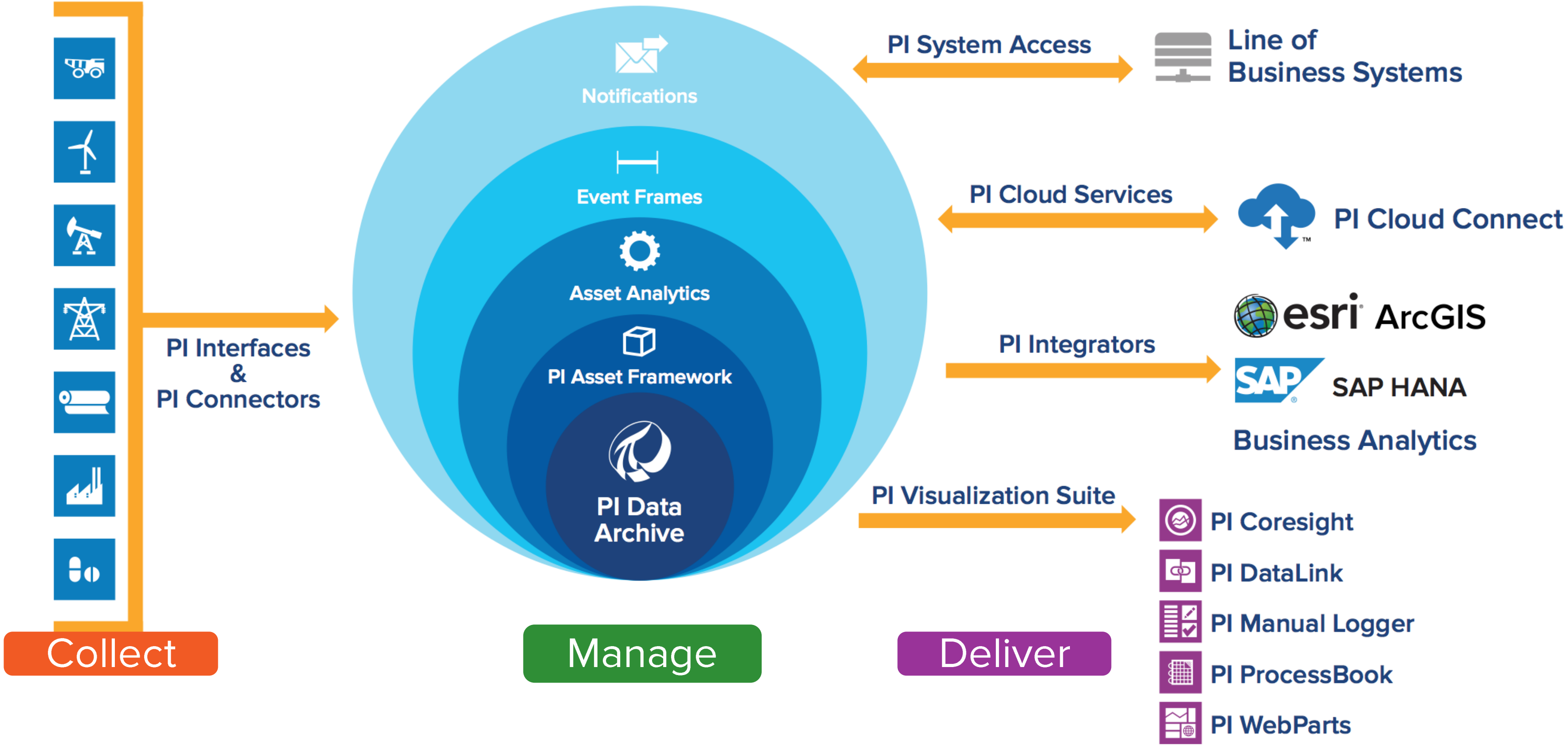
Deliver

PI Interfaces
PI Connectors

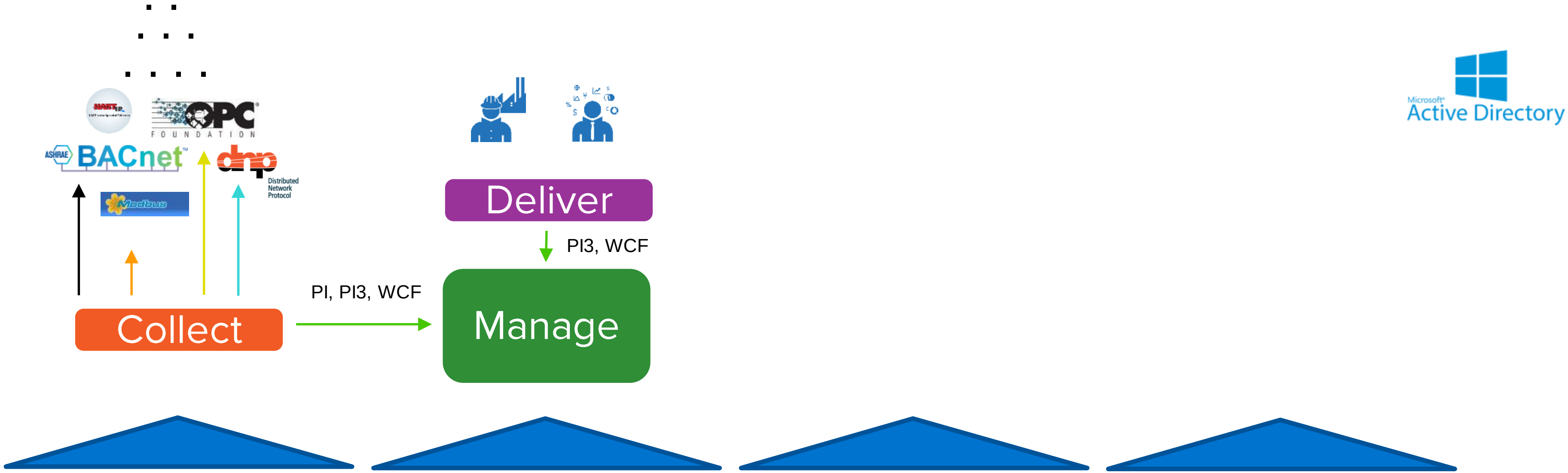
PI Server

PI Client Tools

The PI System Components



Deploy – Operation Scenario



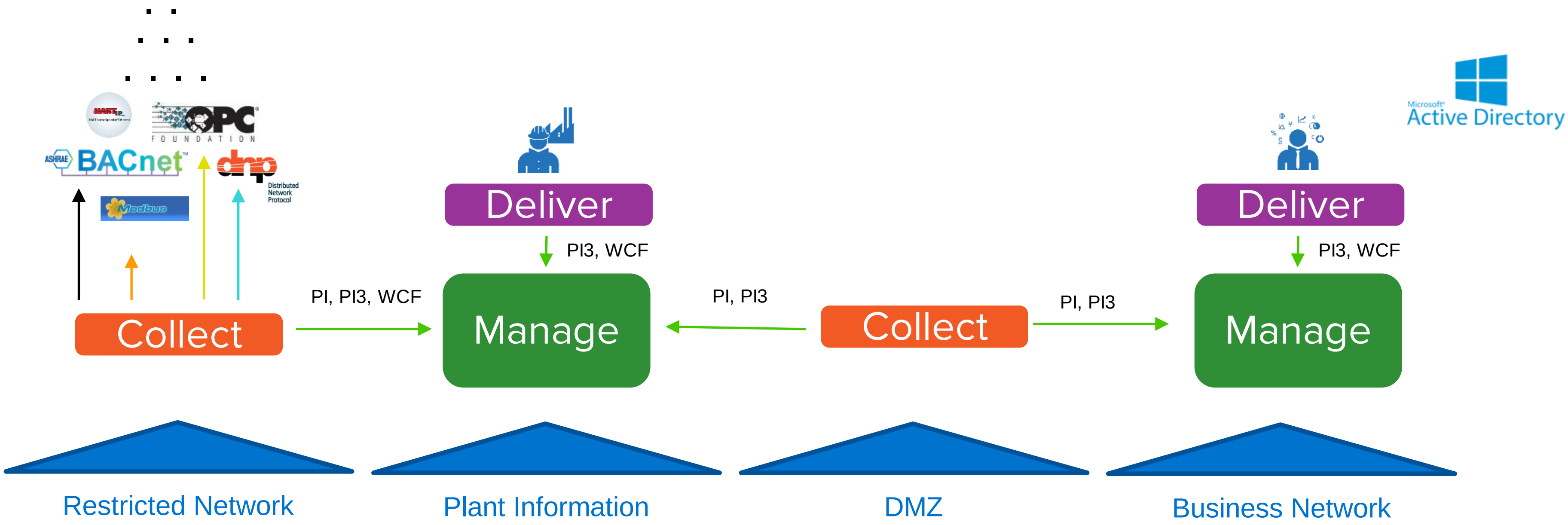
Restricted Network

Plant Information

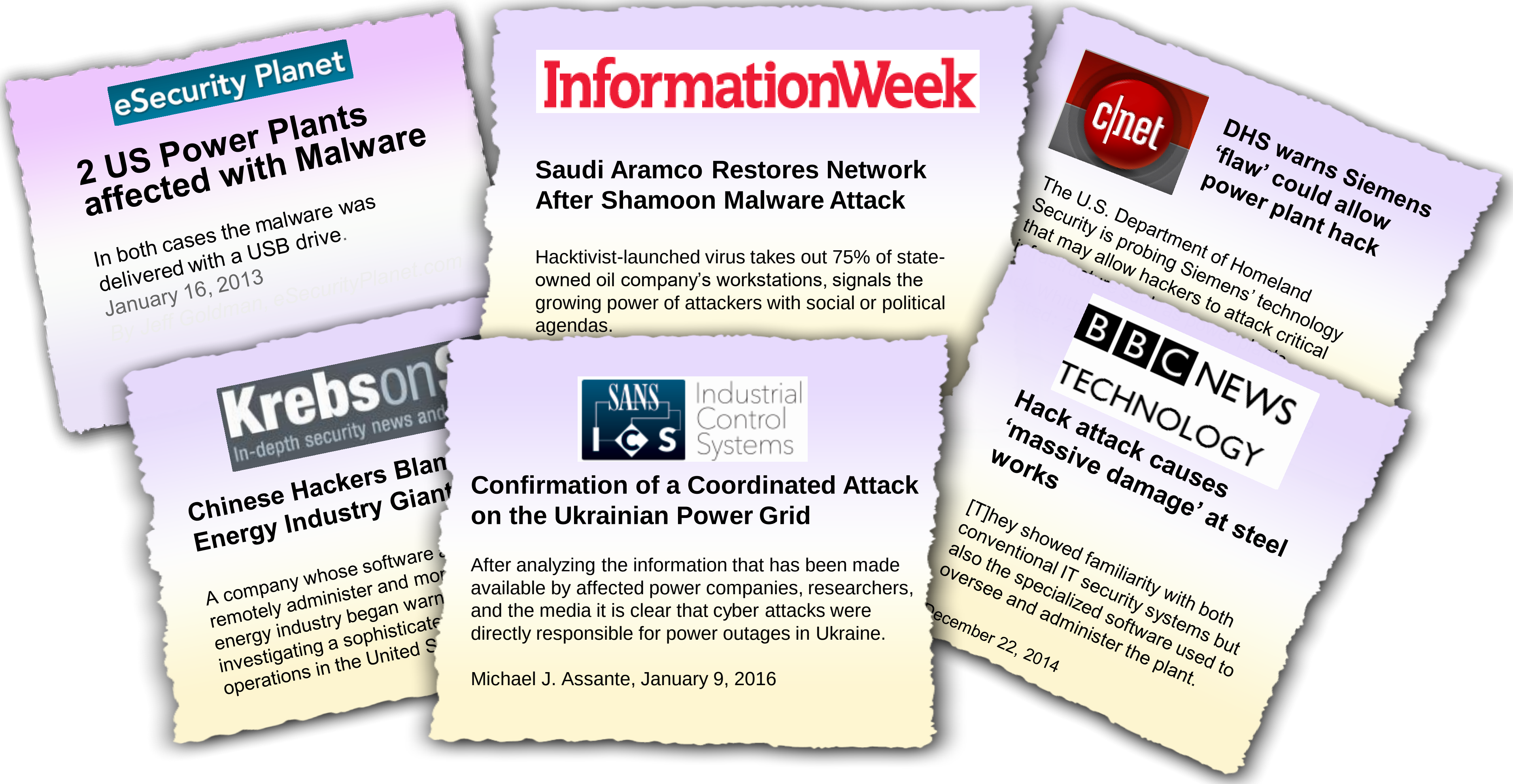
DMZ

Business Network

Deploy – Operation & Business Scenario



What is our fear?



eSecurity Planet

2 US Power Plants affected with Malware

In both cases the malware was delivered with a USB drive.

January 16, 2013

By Jeff Goldman, eSecurityPlanet.com

InformationWeek

Saudi Aramco Restores Network After Shamoon Malware Attack

Hacktivist-launched virus takes out 75% of state-owned oil company's workstations, signals the growing power of attackers with social or political agendas.

c|net

DHS warns Siemens 'flaw' could allow power plant hack

The U.S. Department of Homeland Security is probing Siemens' technology that may allow hackers to attack critical

KrebsonS

In-depth security news and

Chinese Hackers Blan Energy Industry Giant

A company whose software a remotely administer and mor energy industry began warn investigating a sophisticate operations in the United S

SANS ICS Industrial Control Systems

Confirmation of a Coordinated Attack on the Ukrainian Power Grid

After analyzing the information that has been made available by affected power companies, researchers, and the media it is clear that cyber attacks were directly responsible for power outages in Ukraine.

Michael J. Assante, January 9, 2016

BBC NEWS TECHNOLOGY

Hack attack causes 'massive damage' at steel works

[T]hey showed familiarity with both conventional IT security systems but also the specialized software used to oversee and administer the plant.

ecember 22, 2014

“32% indicated their control system assets or networks had been infiltrated or infected at some point”

-The State of Security in Control Systems Today, SANS Institute, June 2015

HD Moore’s Law

> “Casual Attacker power grows at the rate of Metasploit”

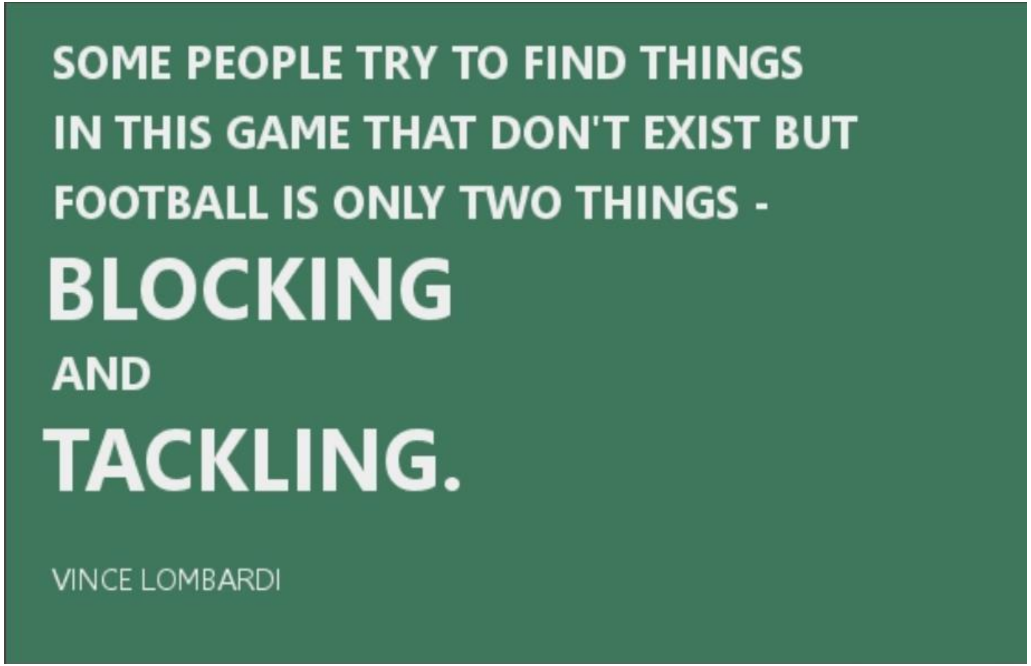
metasploit®

EXPLOIT DATABASE

SHODAN

What can be done?

The “Blocking & Tackling” of Cyber Security



SOME PEOPLE TRY TO FIND THINGS IN THIS GAME THAT DON'T EXIST BUT FOOTBALL IS ONLY TWO THINGS -

BLOCKING

AND

TACKLING.

VINCE LOMBARDI

- ✓ Application Whitelisting
- ✓ Patch Management
- ✓ Reduce attack surface area
- ✓ Build a Defendable environment
- ✓ Manage Authentication
- ✓ Monitor and Respond
- ✓ Manage Remote access closely

Blocking & Tackling: The Top 4

1. Use Whitelisting Techniques
2. Upgrade Your Software
3. Implement Least Privileges
4. Reduce Your Attack Surface

Whitelisting: Whitelisting vs Blacklisting

All Applications: A, B, C

Blacklist: Allow All, Deny A, C

Whitelist: Deny All, Allow B

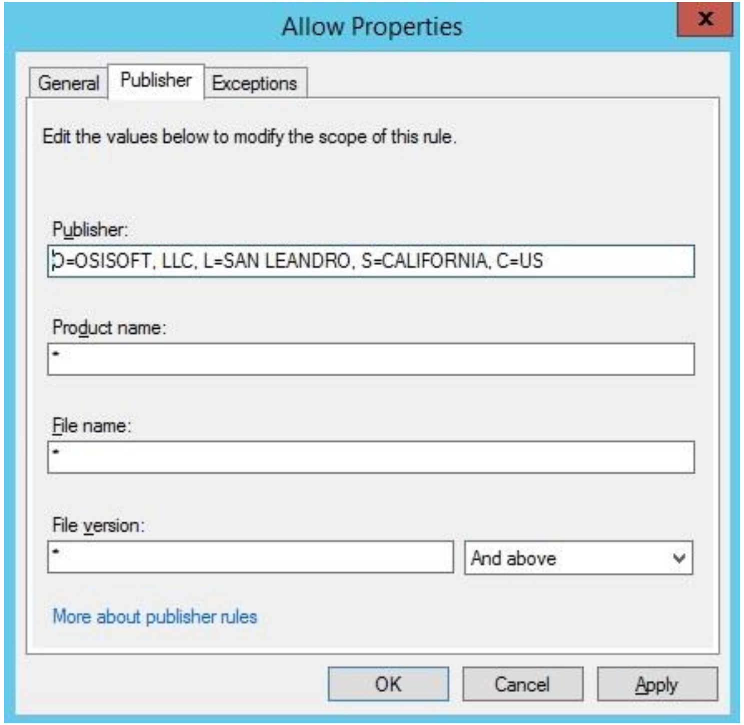
All Applications: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, …

Blacklist: Allow All, Deny A, C, E, F, G, H, I, J, K, L, M, N, O, P, …

Whitelist: Deny All, Allow B, D

Whitelisting: Implementing with AppLocker

- **Run only approved files**
  - By user or group
- **Rules based on:**
  - Publisher
  - Path
  - File hash
- **Action modes**
  - Audit only
  - Enforce allow or deny



Edit the values below to modify the scope of this rule.

Publisher:
O=OSISOFT, LLC, L=SAN LEANDRO, S=CALIFORNIA, C=US

Product name:
*

File name:
*

File version:
* And above

Whitelisting: Where does my antivirus fit in?

Updates: Does upgrading PI Really Make a Difference?

- **Idaho National Lab**
  - 2005 Assessment
  - 2008 vCampus Live!
  - 2009 vCampus Live!
  - 2011 Cooperative Research
  - 2012 vCampus Live! “Detect & Defend”
- **US Army NetCom**
  - 2009 CoN #201006618
  - 2013 CoN (recertified)
- **US NRC**
  - 2010 DISA, NIST
- **SAP QBS Certification**
  - 2012 Veracode
  - 2013 Veracode
- **Windows Logo Certification**
  - 2008 Windows 2008 Server Core
  - 2011 Windows 2008 R2 Server Core
  - 2012 Windows 2012 Server Core
- **Azure Penetration Testing**
  - 2014 PI Cloud Connect (Utility Partner)
  - 2014 PI Cloud Access (IOActive)

- **Microsoft Information Security Consulting**
  - 2009 PI Server
  - 2010 PI Agent
  - 2011 PI Coresight
  - 2011 PI AF
  - 2012 PI ProcessBook
  - 2012 Products in Design (3)
  - 2013 Engineering Management
  - 2013 Products in Design (3)
  - 2013/2015 SDL for Security Champions
  - 2013/2014/2015 Defensive Programming (Cigital)
  - 2015 PI Connectors
  - 2015 PI Transport Security (IOActive)
  - 2015 PI System Security Review
  - 2015 Advanced Tools provided by Microsoft

Updates: OSIsoft Security Development Lifecycle

- Security release gate
  - Threat model
  - Binscope
  - Banned.h

- Training

  Cigital

- Tool adoption
  - Static & dynamic analysis; fuzzing,

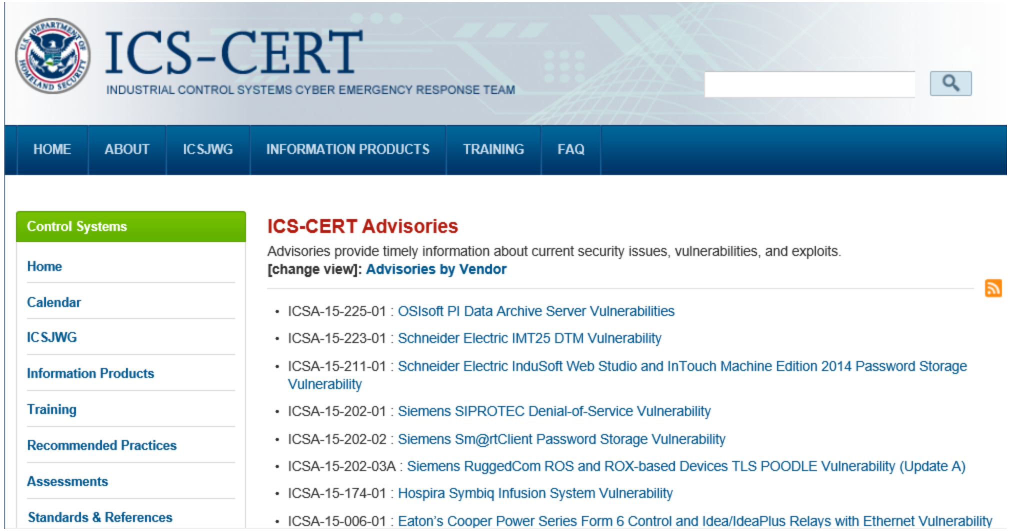
- 3rd party review & consulting

  IOActive Microsoft

  - Code review, Vulnerability assessments and penetration testing

- In progress/Future
  - Dashboard - “releasability”
  - Evaluating metrics for vulns. CVSS, CVE, CWE
  - SDL outside of development
  - New technologies

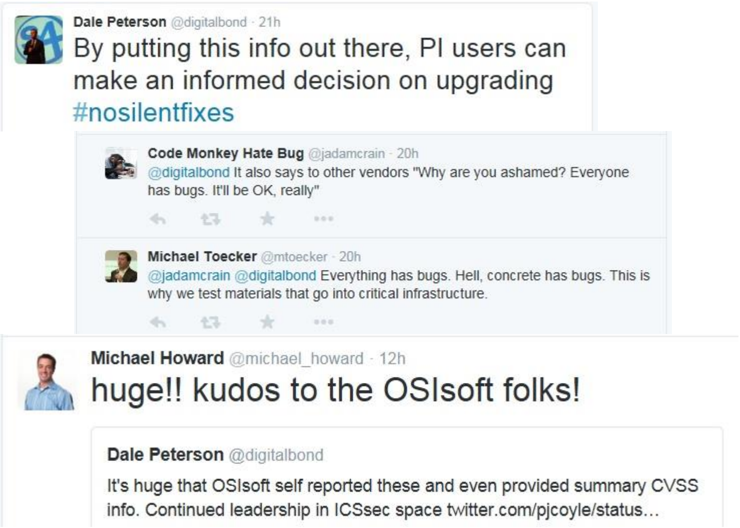
Updates: Vulnerability Disclosure



ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: Advisories by Vendor

- ICSA-15-225-01 : OSIsoft PI Data Archive Server Vulnerabilities
- ICSA-15-223-01 : Schneider Electric IMT25 DTM Vulnerability
- ICSA-15-211-01 : Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Password Storage Vulnerability
- ICSA-15-202-01 : Siemens SIPROTEC Denial-of-Service Vulnerability
- ICSA-15-202-02 : Siemens Sm@rtClient Password Storage Vulnerability
- ICSA-15-202-03A : Siemens RuggedCom ROS and ROX-based Devices TLS POODLE Vulnerability (Update A)
- ICSA-15-174-01 : Hospira Symbiq Infusion System Vulnerability
- ICSA-15-006-01 : Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPlus Relays with Ethernet Vulnerability



Dale Peterson @digitalbond · 21h
By putting this info out there, PI users can make an informed decision on upgrading #nosilentfixes

Code Monkey Hate Bug @jadamcrain · 20h
@digitalbond It also says to other vendors "Why are you ashamed? Everyone has bugs. It'll be OK, really"

Michael Toecker @mtoecker · 20h
@jadamcrain @digitalbond Everything has bugs. Hell, concrete has bugs. This is why we test materials that go into critical infrastructure.

Michael Howard @michael_howard · 12h
huge!! kudos to the OSIsoft folks!

Dale Peterson @digitalbond
It's huge that OSIsoft self reported these and even provided summary CVSS info. Continued leadership in ICSsec space twitter.com/pjcoyle/status…

https://ics-cert.us-cert.gov/advisories

Updates: Upgrade your OS and Apply Patches

- Servers
  - Windows Server 2012 R2
  - Windows Server 2012
- Clients
  - Windows 10
  - Windows 8.1
- Windows OS End of Support
  - Windows XP (4/2014)
  - Windows Server 2003 (7/2015)
  - Windows Vista (4/2017)

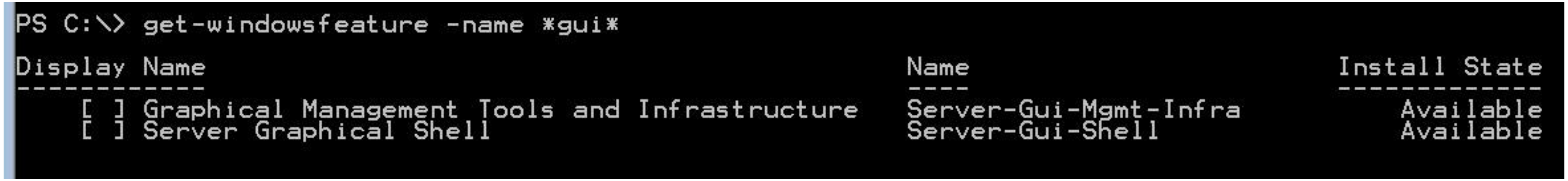
Updates: The Takeaway

Only the latest version of software contains the sum of all development efforts.

Reduce Attack Surface: Windows Server Core

- Less Installed, Less Running
  - No Graphical User Interface (GUI)
  - No Graphic Based Applications
- Less Patching (~40%)
- Less Maintenance
- Smaller Faster Code Base
- More Resources Available
- Lower Total Cost of Ownership

Reduce Attack Surface: Windows Server Core



```
PS C:\> get-windowsfeature -name *gui*

Display Name                                            Name                       Install State
------------                                            ----                       -------------
    [ ] Graphical Management Tools and Infrastructure   Server-Gui-Mgmt-Infra          Available
    [ ] Server Graphical Shell                          Server-Gui-Shell               Available
```

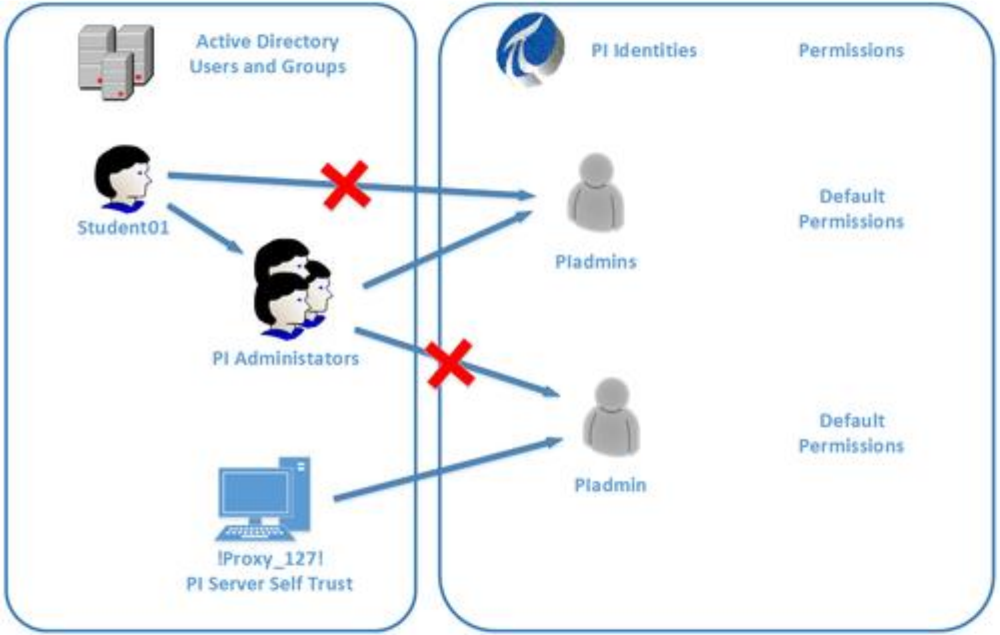
GUI is add/remove feature as of Windows Server 2012

Eg. Add the management GUI without full desktop:

Install-WindowsFeature -name Server-Gui-Mgmt-Infra

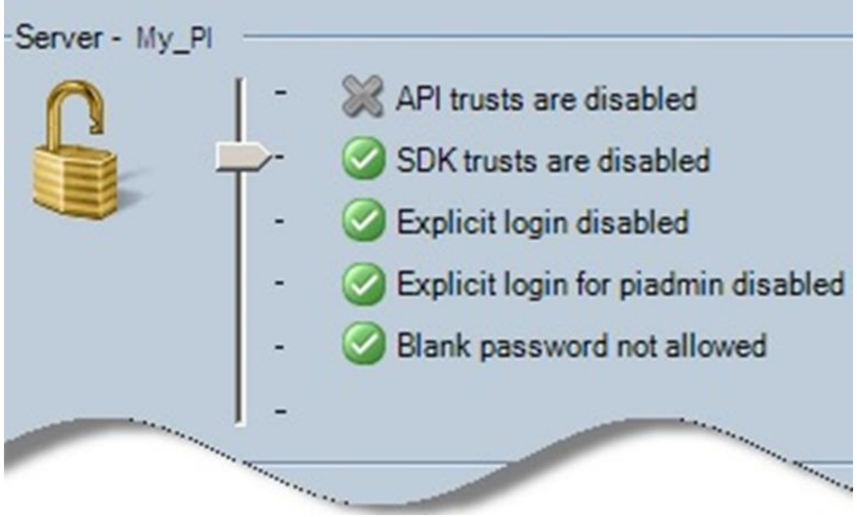
Least Privileges: The Super User

Do not use the piadmin account



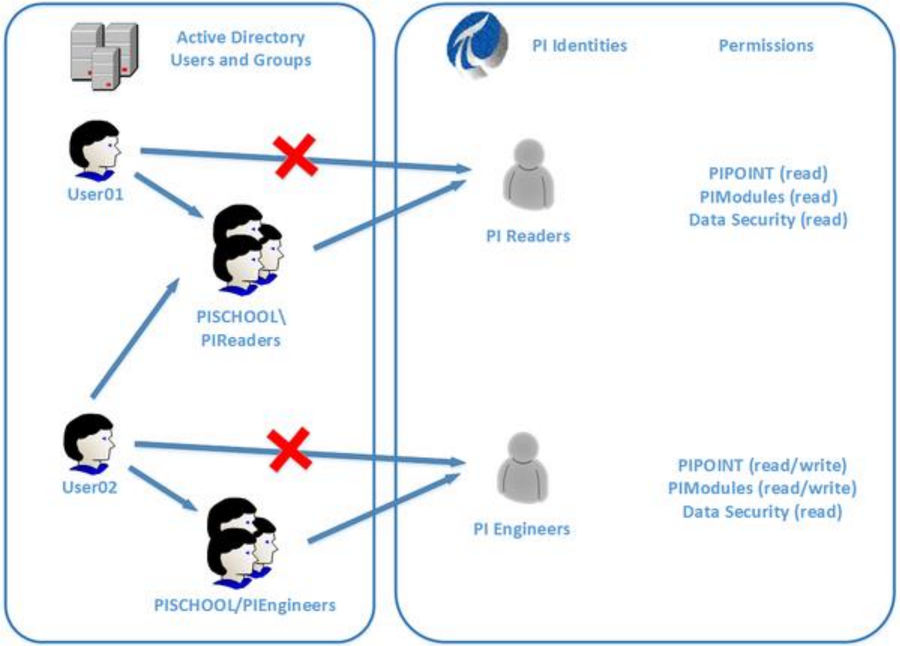
Least Privileges: The Most Secure Option Available

Use Windows Integrated Security (WIS)



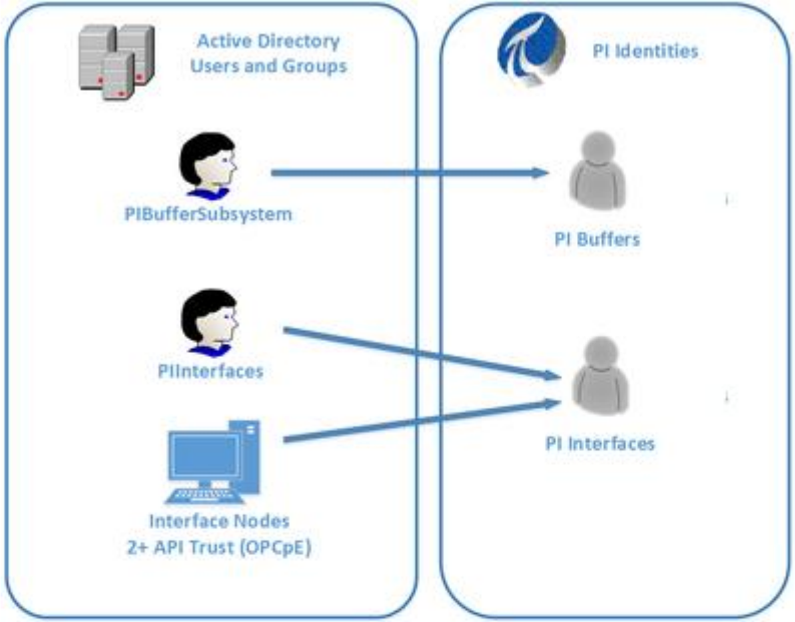
Server - My_PI

- ☒ API trusts are disabled
- ✓ SDK trusts are disabled
- ✓ Explicit login disabled
- ✓ Explicit login for piadmin disabled
- ✓ Blank password not allowed



Least Privileges: Grant Minimum Access

Create Users and Trusts based on Least Privilege

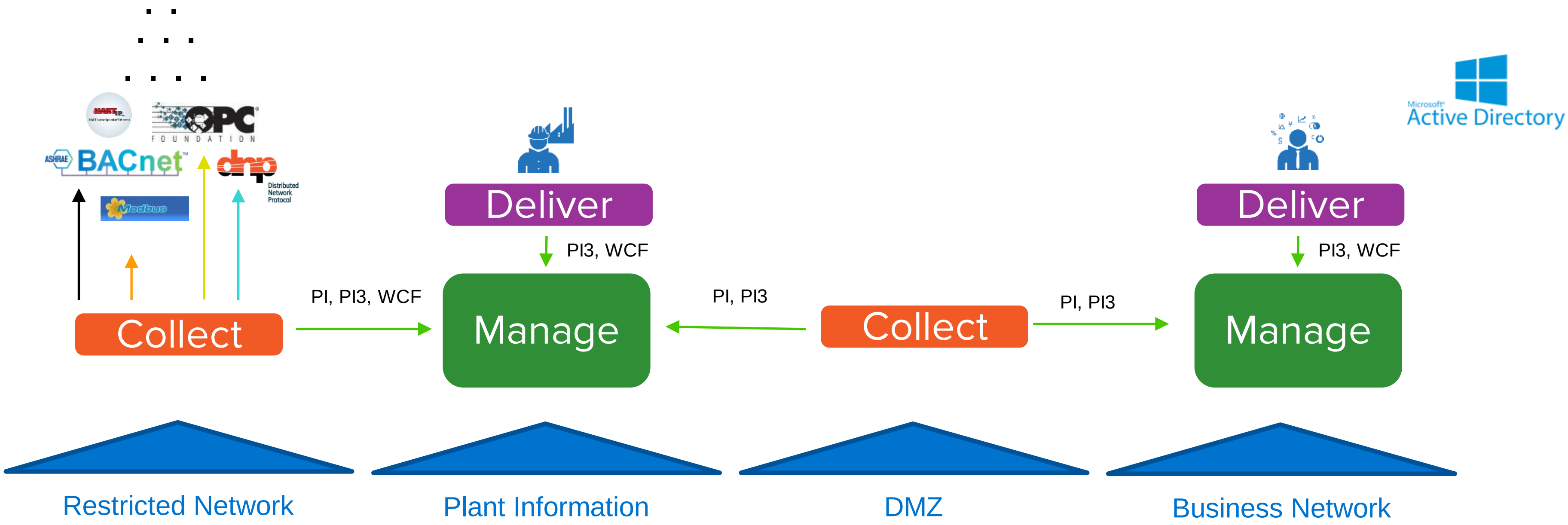


Process	Read Access	Write Access
Interface (No Output)	PIPoint, PtSecurity	None
Interface (Output)	PIPoint, PtSecurity, DataSecurity (output source points)	None
Buffering	PIPoint, PtSecurity, DataSecurity	DataSecurity

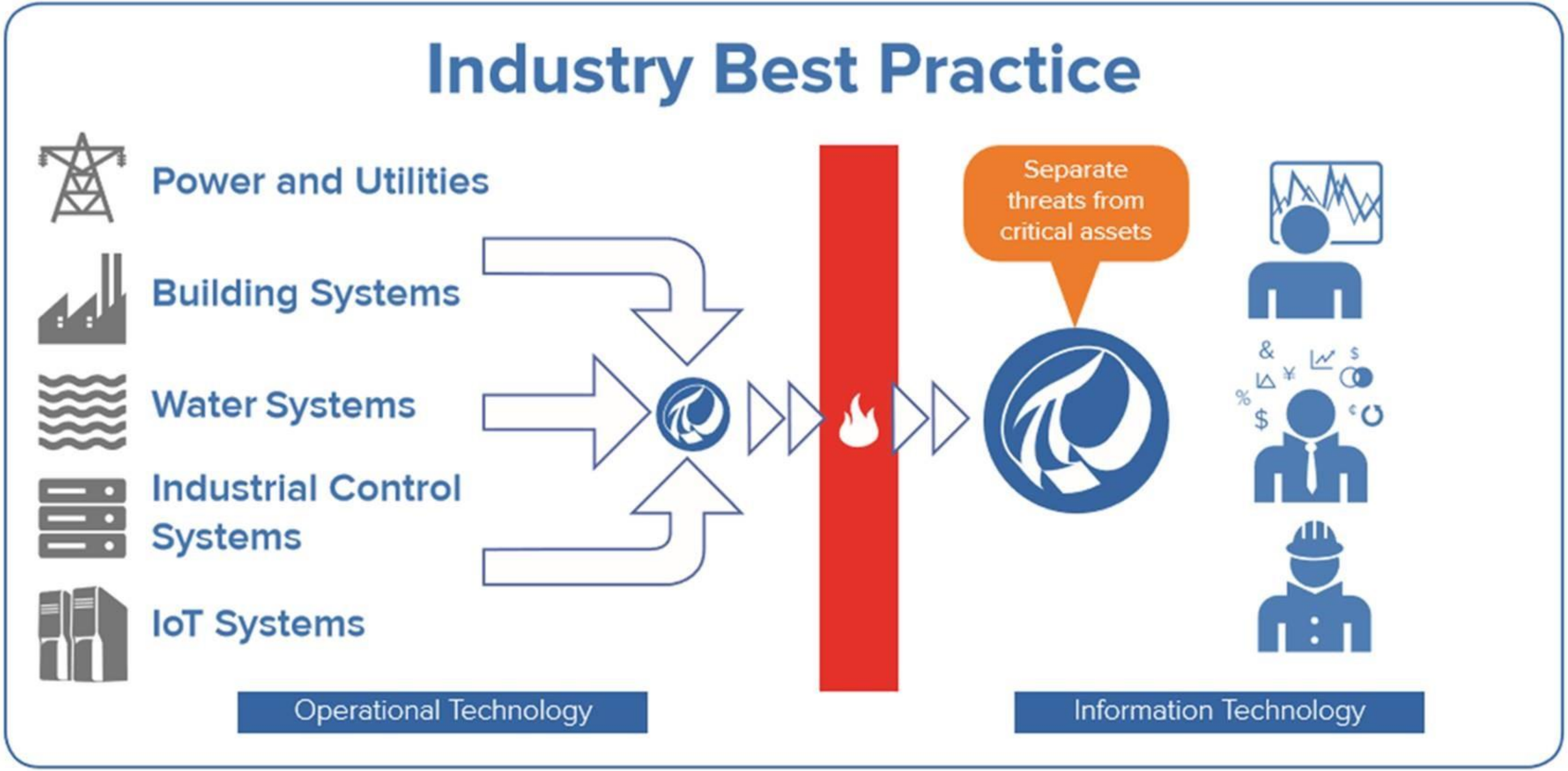
Least Privileges: UAC

Enable Windows User Account Control

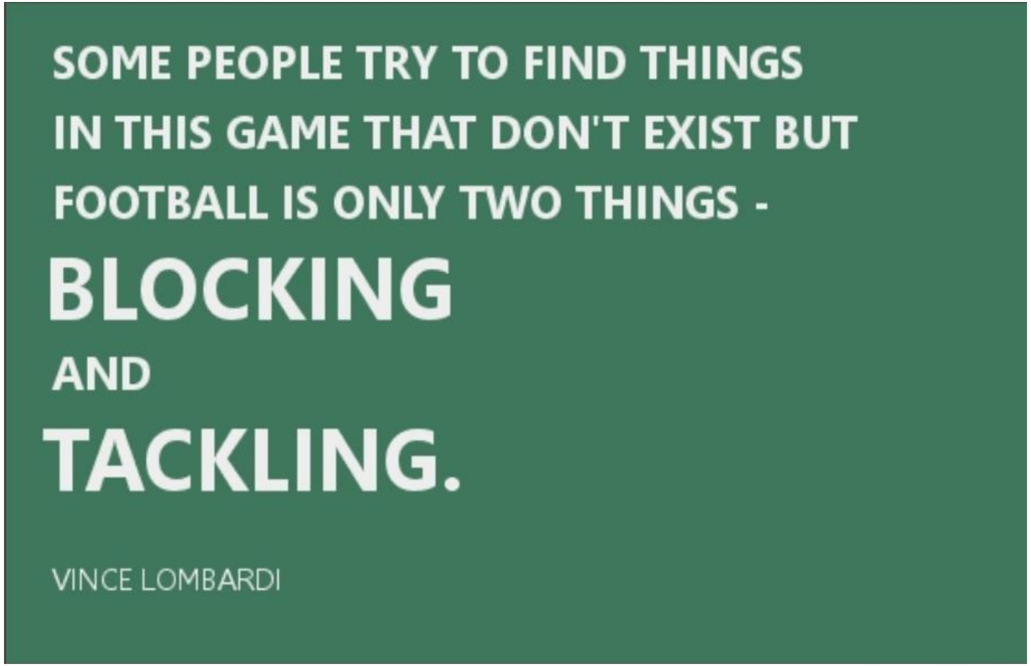
Reduce Attack Surface: Network Architecture



Reduce Attack Surface: Network Architecture



The "Blocking & Tackling" of Cyber Security



SOME PEOPLE TRY TO FIND THINGS IN THIS GAME THAT DON'T EXIST BUT FOOTBALL IS ONLY TWO THINGS -

BLOCKING

AND

TACKLING.

VINCE LOMBARDI

- ✓ Application Whitelisting
- ✓ Patch Management
- ✓ Reduce attack surface area
- ✓ Build a Defendable environment
- ✓ Manage Authentication
- ✓ Monitor and Respond
- ✓ Manage Remote access closely

Additional Information

OSIsoft Resources

Integrating OT and IT with the Modern PI System

Integrating IIoT Sensors with Industrial Data Ecosystems

PI System Cyber Security Page

KB00994 - Whitelisting with AppLocker

KB01160 – Securing PI Interfaces with Service Hardening

KB01092 - PI System and Data Encryption

Configure PI Security Youtube Playlist

Other Resources

SANS Institute:
The State of Security in Control Systems Today: A SANS Survey

ICS-CERT:
Seven Steps to Defend Industrial Control Systems

NSA:
Application Whitelisting Using Microsoft AppLocker

Norton Green

ngreen@osisoft.com
Director
Executive Briefing Program
OSIsoft, LLC

Harry Paul

hpaul@osisoft.com
Cyber Security Advisory Team
Technical Support Escalation Engineer
OSIsoft, LLC

Thank You

OSIsoft®