A Novel Approach to Secure Industrial Networking & Cyber Security

Mr. Rohit Kotian & Mr. Pratap Mondal

17th March 2018

A Rich Heritage

- Founded by **Joseph Belden** in **1902** in **Chicago**
- A long **history of innovation** for communications technologies
- Early customers included **Thomas Edison**

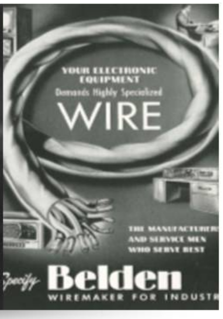
Radio in the 1920s

TV in the 1950s

Computer Networking in the 1980s and 1990s

Joseph Belden

Thomas Edison


YOUR ELECTRONIC EQUIPMENT
Demands Highly Specialized
WIRE
THE MANUFACTURERS AND SERVICE MEN WHO SERVE BEST
Specify Belden
WIREMAKER FOR INDUSTRY

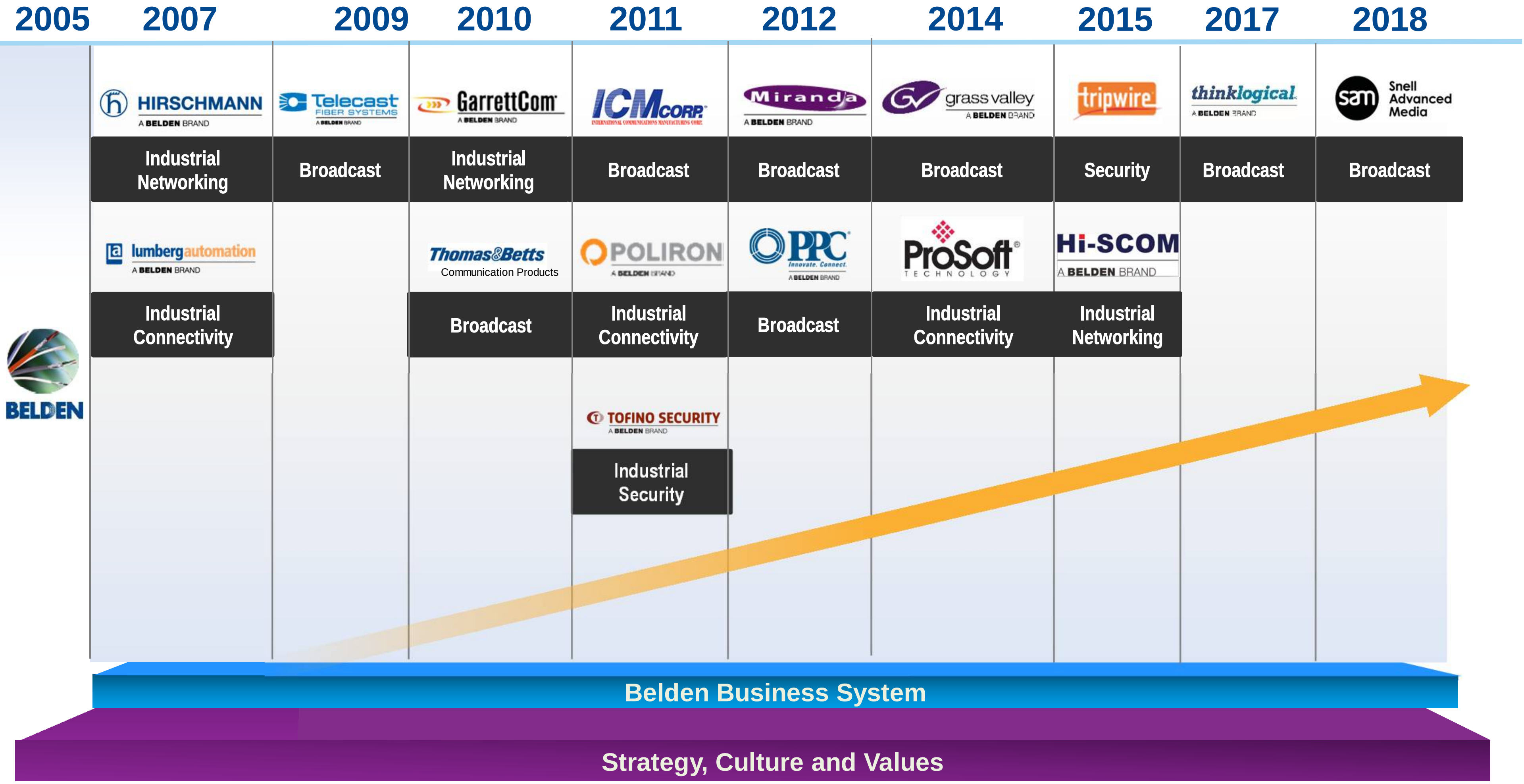
Belden Today

- John Stroup, CEO
- Headquartered in **St. Louis, MO**
- **10,000** employees
- NYSE: **BDC**
- Operations in **North and South America**, **Europe**, **Middle East**, **Africa** and **Asia Pacific**
- Revenue **$2.39B**
- **20+** Sales Offices; **25+** Manufacturing Facilities

Delivering highly engineered signal transmission solutions for mission-critical applications in a diverse set of global markets

Key Markets	Applications	Solutions
Enterprise *Smart Buildings* *Final Mile Broadband* *Live Media Production* **Industrial** *Discrete Manufacturing* *Process Facilities* *Transportation* *Energy*	Video Audio Data	Cable Connectivity Networking Software

A Purposeful Transformation from a Cable Supplier to a Global Signal Transmission Solutions Provider



2005
BELDEN

2007
HIRSCHMANN A BELDEN BRAND
Industrial Networking
lumberg automation A BELDEN BRAND
Industrial Connectivity

2009
Telecast FIBER SYSTEMS A BELDEN BRAND
Broadcast

2010
GarrettCom A BELDEN BRAND
Industrial Networking
Thomas&Betts Communication Products
Broadcast

2011
ICM CORP. INTERNATIONAL COMMUNICATIONS MANUFACTURING CORP.
Broadcast
POLIRON A BELDEN BRAND
Industrial Connectivity
TOFINO SECURITY A BELDEN BRAND
Industrial Security

2012
Miranda A BELDEN BRAND
Broadcast
PPC Innovate. Connect. A BELDEN BRAND
Broadcast

2014
grass valley A BELDEN BRAND
Broadcast
ProSoft TECHNOLOGY
Industrial Connectivity

2015
tripwire
Security
Hi-SCOM A BELDEN BRAND
Industrial Networking

2017
thinklogical A BELDEN BRAND
Broadcast

2018
sam Snell Advanced Media
Broadcast

Belden Business System

Strategy, Culture and Values

BELDEN India, Chakan, Pune – Inaugurated on 15th Nov 2018

- Built-up area of 10,000 Sq Meters in Phase I
- Built-up area of over 10,000 Sq Meters in Phase II
- Capability to make Coaxial and Multi conductor cables
- Assembly options of Fiber and Copper cables
- Hirschmann Switch Assembly
- Over 100 employees including managers and technicians in Phase I

Industrial IT Core Networking Capabilities

MACH1000
Gigabit Ethernet Switch for harsh industrial environments

SPIDER

Unmanaged PoE/non-PoE switches for various industrial applications

BAT

Access Points & Clients that work together for maximum mobility, flexibility & network

Managed & Unmanaged Switches
HIRSCHMANN classic rail switches

RSP30/40
High Performance Managed Rail Switches

Customised Value Addition Capabilities

Repair and Service facility

In-house facility for service and repair of Network Switch products

Quick Turn-Around Time

Shortened turnaround time for service and repair of Network Switching Products…!

Industrial Wire & Cables Capabilities

Audio/Video Cable

Co-axial, A\V Cable, Speaker Cables

Electronics Cables

UL Multi-conductor and Paired Cables, as well as Hook-up Lead Wires & MachFlex^{TM} ONE

Networking and DataBus cables

RS-485, Foundation Fieldbus, CANBus, Modbus, Profibus, Category LAN cables

CANopen PROFIBUS® PROFINET® Fieldbus Foundation

Control and Instrumentation Cables

MachFlex^{TM} specialty flexible cable, Fire Survival Cables, Marine Cables, EN 50288-7 C&I Cables

Customised Value Addition Capabilities

Customized Jacketing

Different jacket materials like PVC, LSZH, FR-PVC, FRLS-PVC with optional anti-rodent, anti-termite, UV resistance properties

Multiple outer jacket color options

⬛ ⬜ 🟥 🟩 🟨 🟪 🟦 🟧 🟦

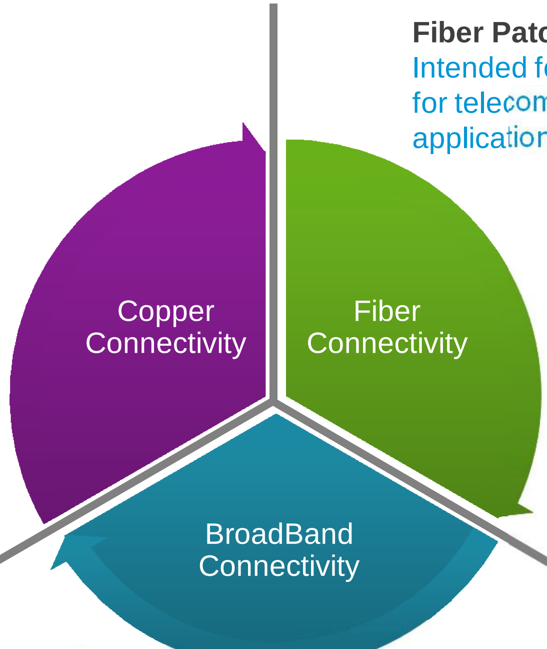
Customized Armoring

Options in Steel Wire Armor (SWA) and Steel Wire Braid armor (SWB)

Enterprise Connectivity Solution

Copper Patch Cords
Intended for Datacenter/LAN & Ethernet/IP applications in LSZH & PVC Versions

Fiber Patch Cords
Intended for high-speed high-bandwidth applications for telecommunications and high density patching applications.

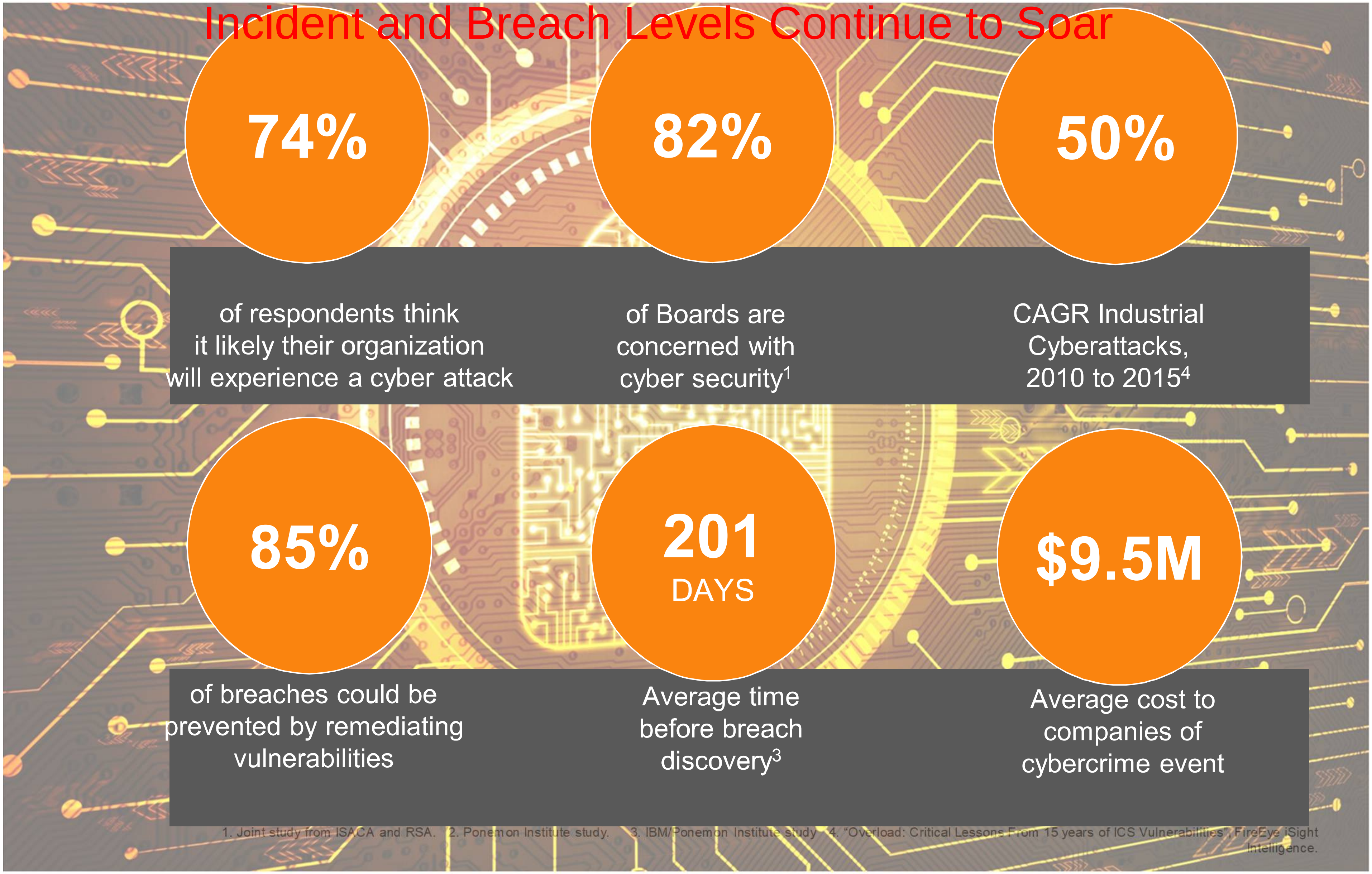


Coaxial Patch Cords
Intended for use for RF signals and Audio/Video connectivity

Agenda

- ❑ What is ICS Cybersecurity?
- ❑ Overall security philosophy
- ❑ Example system architecture
- ❑ Introduction to Firewalls
- ❑ What Solutions Belden can offer?

Incident and Breach Levels Continue to Soar



74%

of respondents think it likely their organization will experience a cyber attack

82%

of Boards are concerned with cyber security[1]

50%

CAGR Industrial Cyberattacks, 2010 to 2015[4]

85%

of breaches could be prevented by remediating vulnerabilities

201
DAYS

Average time before breach discovery[3]

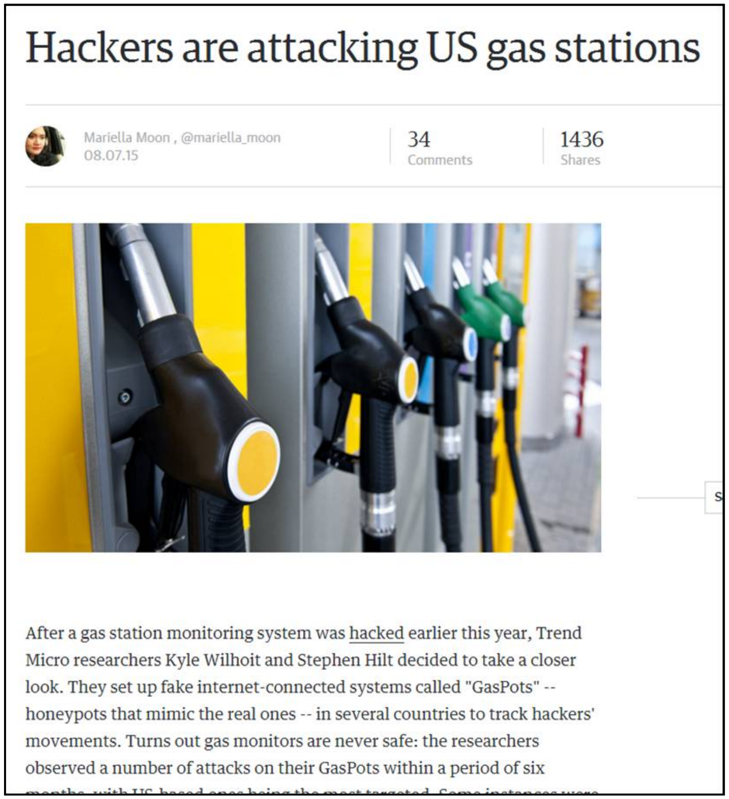
$9.5M

Average cost to companies of cybercrime event

[1] Joint study from ISACA and RSA. [2] Ponemon Institute study. [3] IBM/Ponemon Institute study [4] “Overload: Critical Lessons From 15 years of ICS Vulnerabilities”, FireEye iSight Intelligence.

Control System Security Is Gaining Public Recognition

The Stuxnet Worm – July 2018
Shamoon – Aug 2012
Dragonfly – Feb 2013

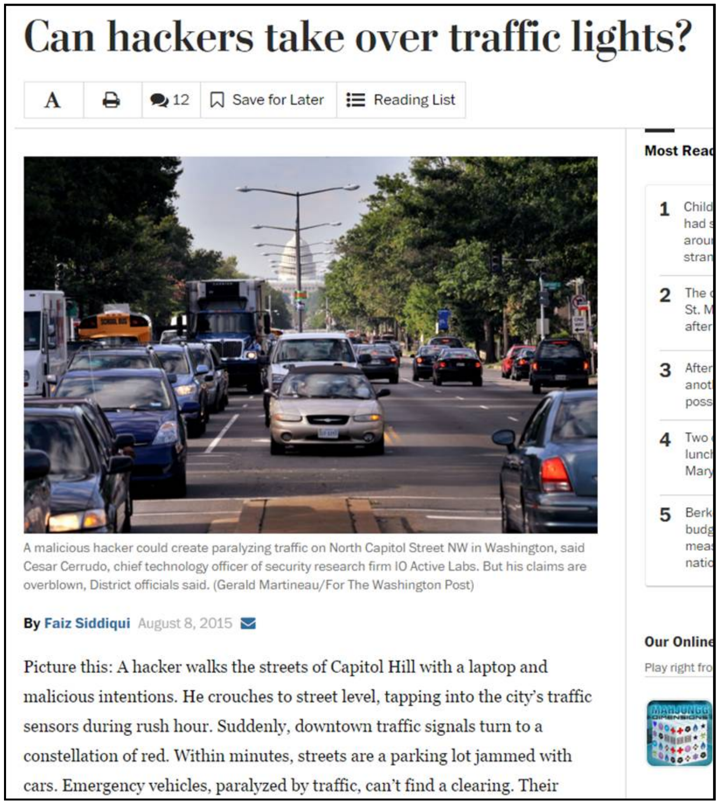


Hackers are attacking US gas stations

Mariella Moon , @mariella_moon
08.07.15

34 Comments | 1436 Shares

After a gas station monitoring system was hacked earlier this year, Trend Micro researchers Kyle Wilhoit and Stephen Hilt decided to take a closer look. They set up fake internet-connected systems called "GasPots" -- honeypots that mimic the real ones -- in several countries to track hackers' movements. Turns out gas monitors are never safe: the researchers observed a number of attacks on their GasPots within a period of six



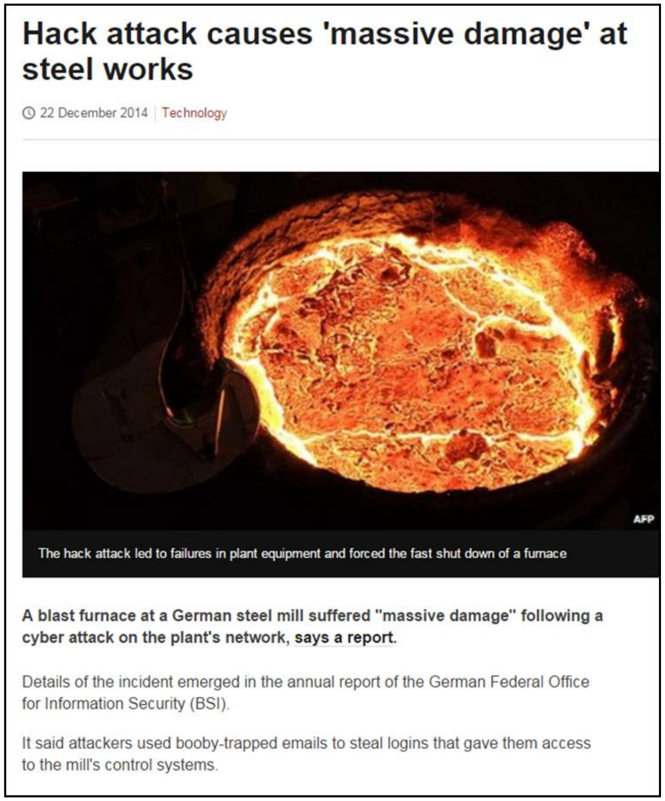
Can hackers take over traffic lights?

A malicious hacker could create paralyzing traffic on North Capitol Street NW in Washington, said Cesar Cerrudo, chief technology officer of security research firm IO Active Labs. But his claims are overblown, District officials said. (Gerald Martineau/For The Washington Post)

By Faiz Siddiqui August 8, 2015

Picture this: A hacker walks the streets of Capitol Hill with a laptop and malicious intentions. He crouches to street level, tapping into the city's traffic sensors during rush hour. Suddenly, downtown traffic signals turn to a constellation of red. Within minutes, streets are a parking lot jammed with cars. Emergency vehicles, paralyzed by traffic, can't find a clearing. Their

Control System Security Is Gaining Public Recognition



Hack attack causes 'massive damage' at steel works

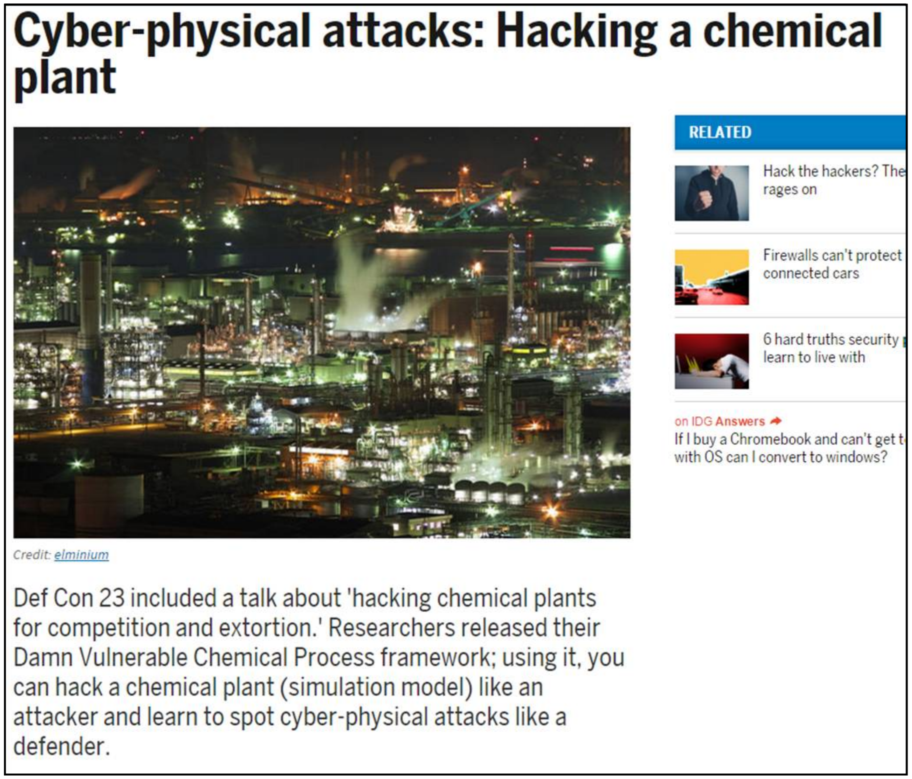
22 December 2014 | Technology

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI).

It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.



Cyber-physical attacks: Hacking a chemical plant

Credit: elminium

Def Con 23 included a talk about 'hacking chemical plants for competition and extortion.' Researchers released their Damn Vulnerable Chemical Process framework; using it, you can hack a chemical plant (simulation model) like an attacker and learn to spot cyber-physical attacks like a defender.

RELATED

Hack the hackers? The
rages on

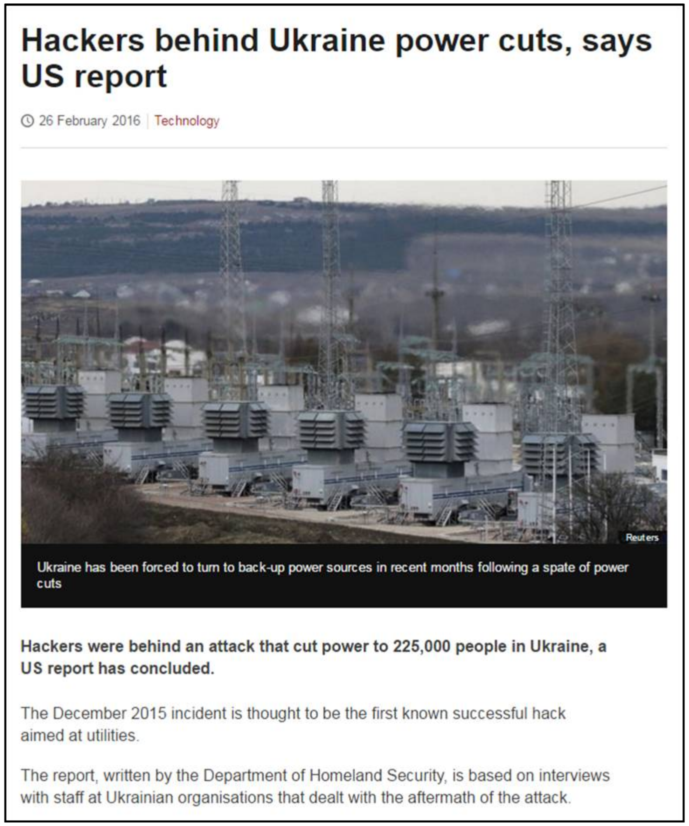
Firewalls can't protect
connected cars

6 hard truths security
learn to live with

on IDG Answers
If I buy a Chromebook and can't get t
with OS can I convert to windows?

Control System Security Is Gaining Public Recognition

BlackEnergy – Dec 2016



Hackers behind Ukraine power cuts, says US report

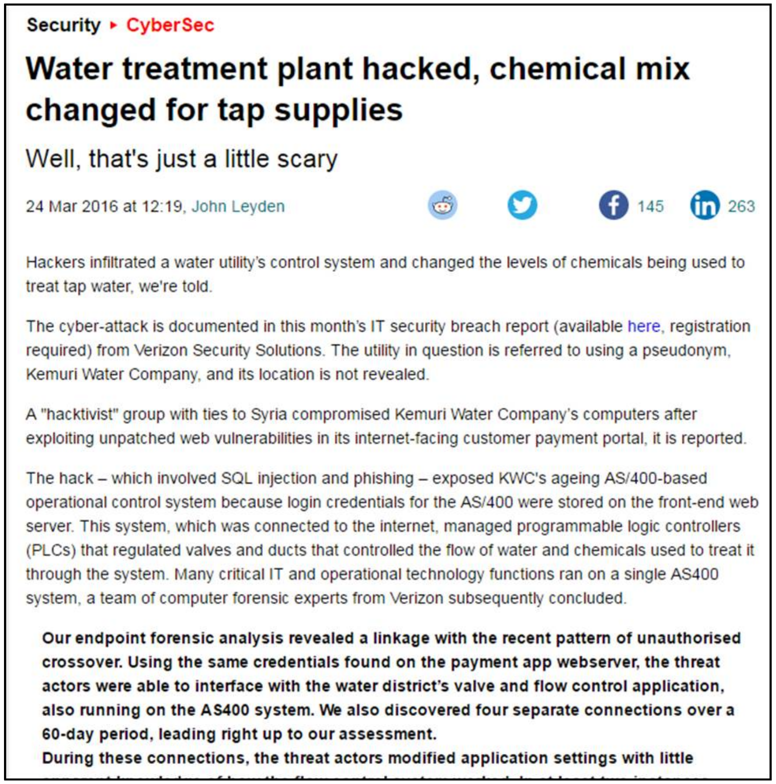
26 February 2016 | Technology

Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

Hackers were behind an attack that cut power to 225,000 people in Ukraine, a US report has concluded.

The December 2015 incident is thought to be the first known successful hack aimed at utilities.

The report, written by the Department of Homeland Security, is based on interviews with staff at Ukrainian organisations that dealt with the aftermath of the attack.



Security ▸ CyberSec

Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

24 Mar 2016 at 12:19, John Leyden

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told.

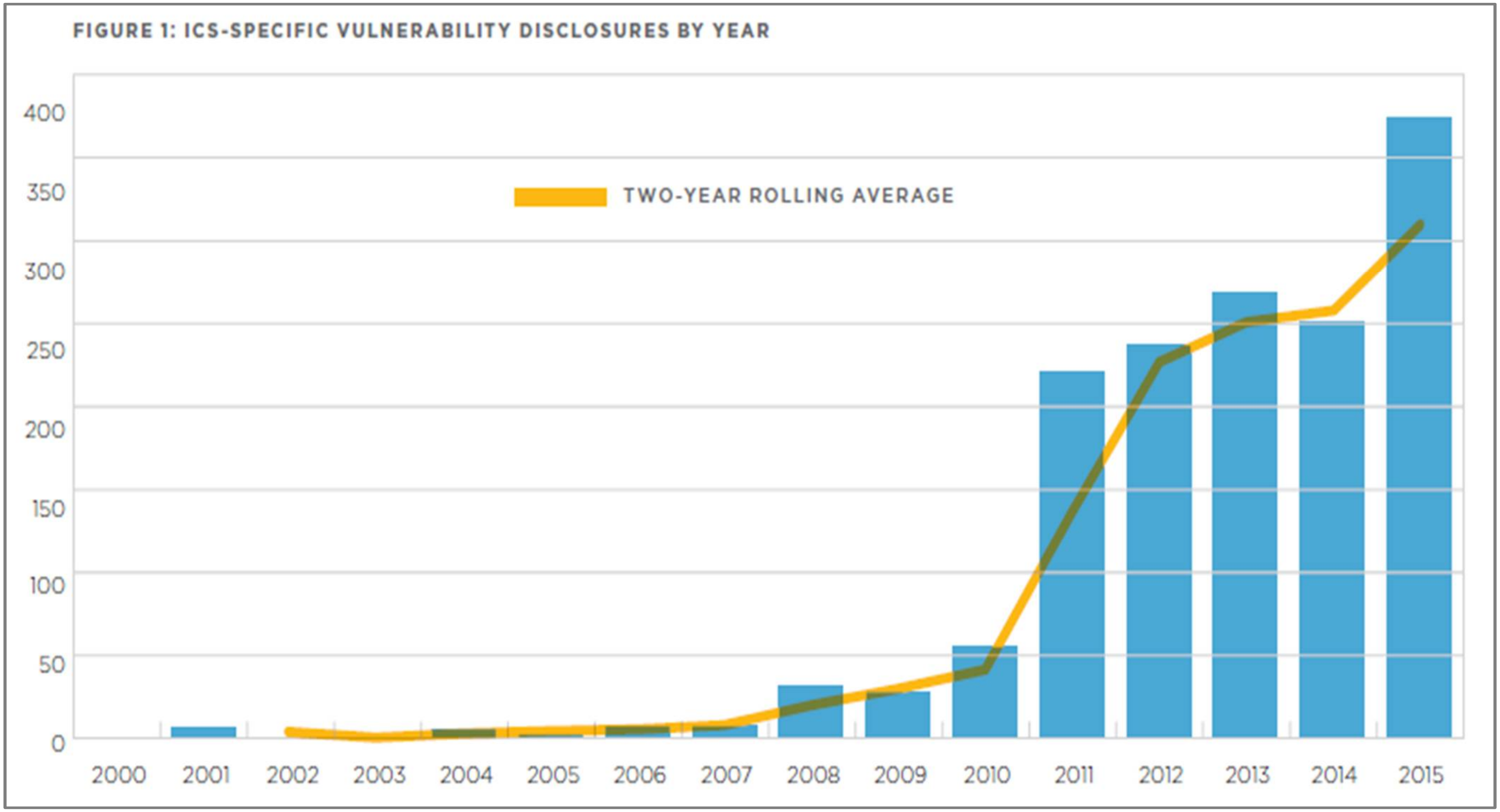
The cyber-attack is documented in this month's IT security breach report (available here, registration required) from Verizon Security Solutions. The utility in question is referred to using a pseudonym, Kemuri Water Company, and its location is not revealed.

A "hacktivist" group with ties to Syria compromised Kemuri Water Company's computers after exploiting unpatched web vulnerabilities in its internet-facing customer payment portal, it is reported.

The hack – which involved SQL injection and phishing – exposed KWC's ageing AS/400-based operational control system because login credentials for the AS/400 were stored on the front-end web server. This system, which was connected to the internet, managed programmable logic controllers (PLCs) that regulated valves and ducts that controlled the flow of water and chemicals used to treat it through the system. Many critical IT and operational technology functions ran on a single AS400 system, a team of computer forensic experts from Verizon subsequently concluded.

> **Our endpoint forensic analysis revealed a linkage with the recent pattern of unauthorised crossover. Using the same credentials found on the payment app webserver, the threat actors were able to interface with the water district's valve and flow control application, also running on the AS400 system. We also discovered four separate connections over a 60-day period, leading right up to our assessment.**
>
> **During these connections, the threat actors modified application settings with little**

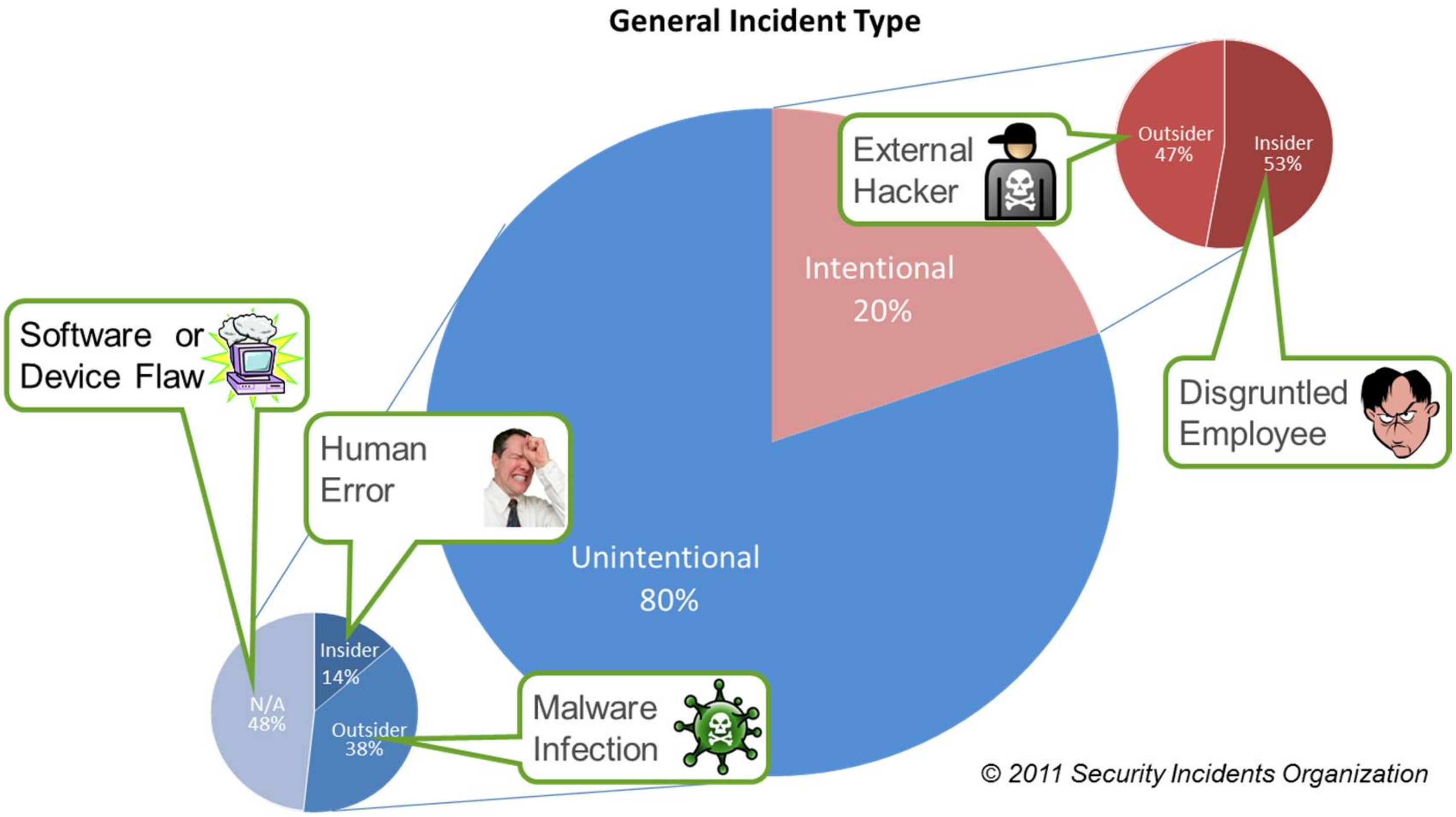
Reported Vulnerabilities & Incidents are Increasing



Source: FireEye iSight Intelligence 2016 ICS Vulnerability Trend Report

But ICS Cybersecurity Is Much More than Hackers

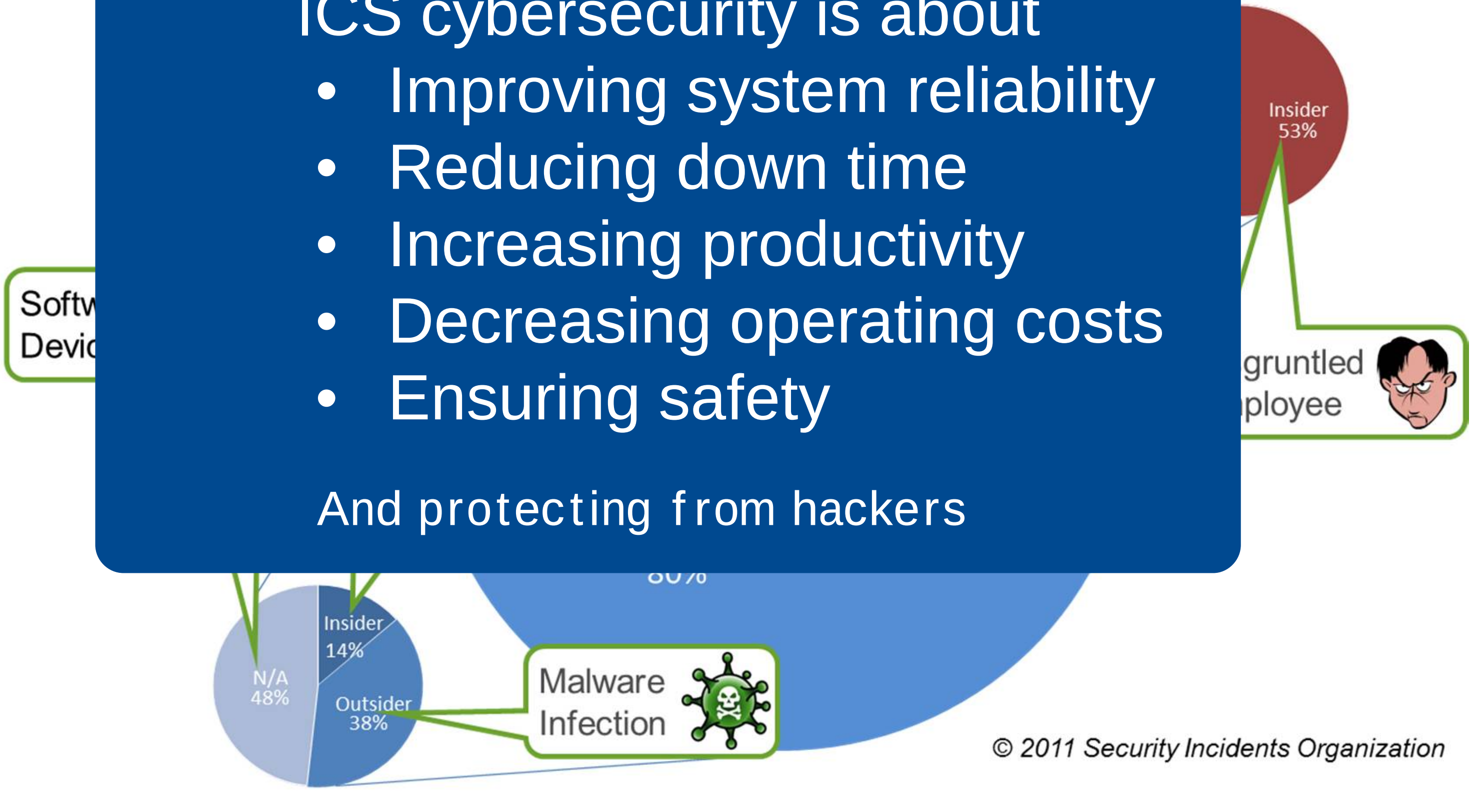
- <10% of issues are related to hackers
- Most “attacks” are device or human errors



© 2011 Security Incidents Organization

But ICS Cybersecurity Is Much More than Hackers

- <10% of issues are related to hackers
- Most “attacks” are device or human errors



ICS cybersecurity is about

- Improving system reliability
- Reducing down time
- Increasing productivity
- Decreasing operating costs
- Ensuring safety

And protecting from hackers

© 2011 Security Incidents Organization

Where do I start?

Overall Security Philosophy

- ☑ What is ICS Cybersecurity?
- ❑ Overall security philosophy
- ❑ Example system architecture
- ❑ Introduction to Firewalls
- ❑ What Solutions Belden can offer?

Key Security Principles

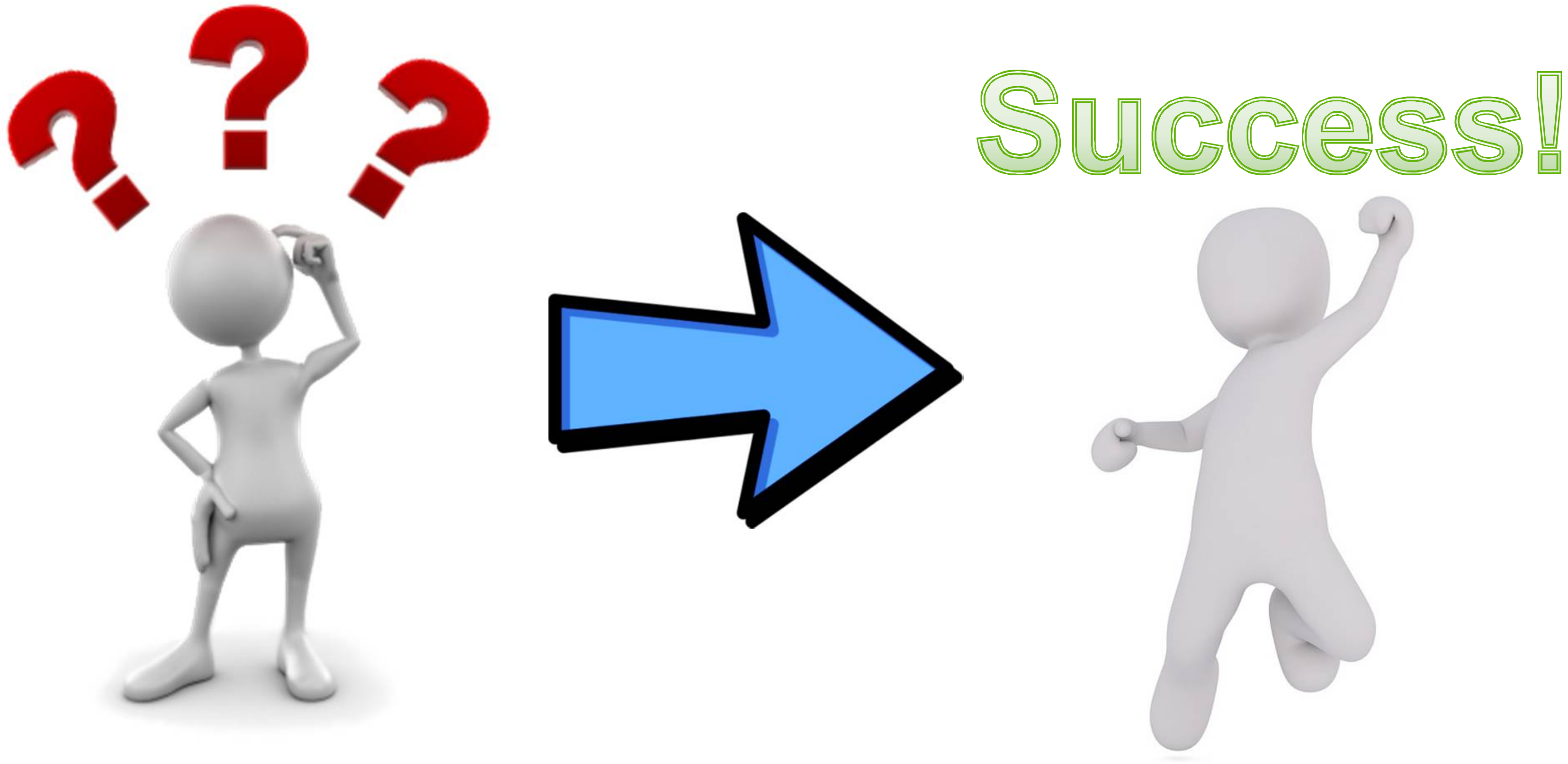
- Security is not just about firewalls

- Firewalls are important, but security is a system-level property

- Security needs to be woven throughout the network fabric – including switches

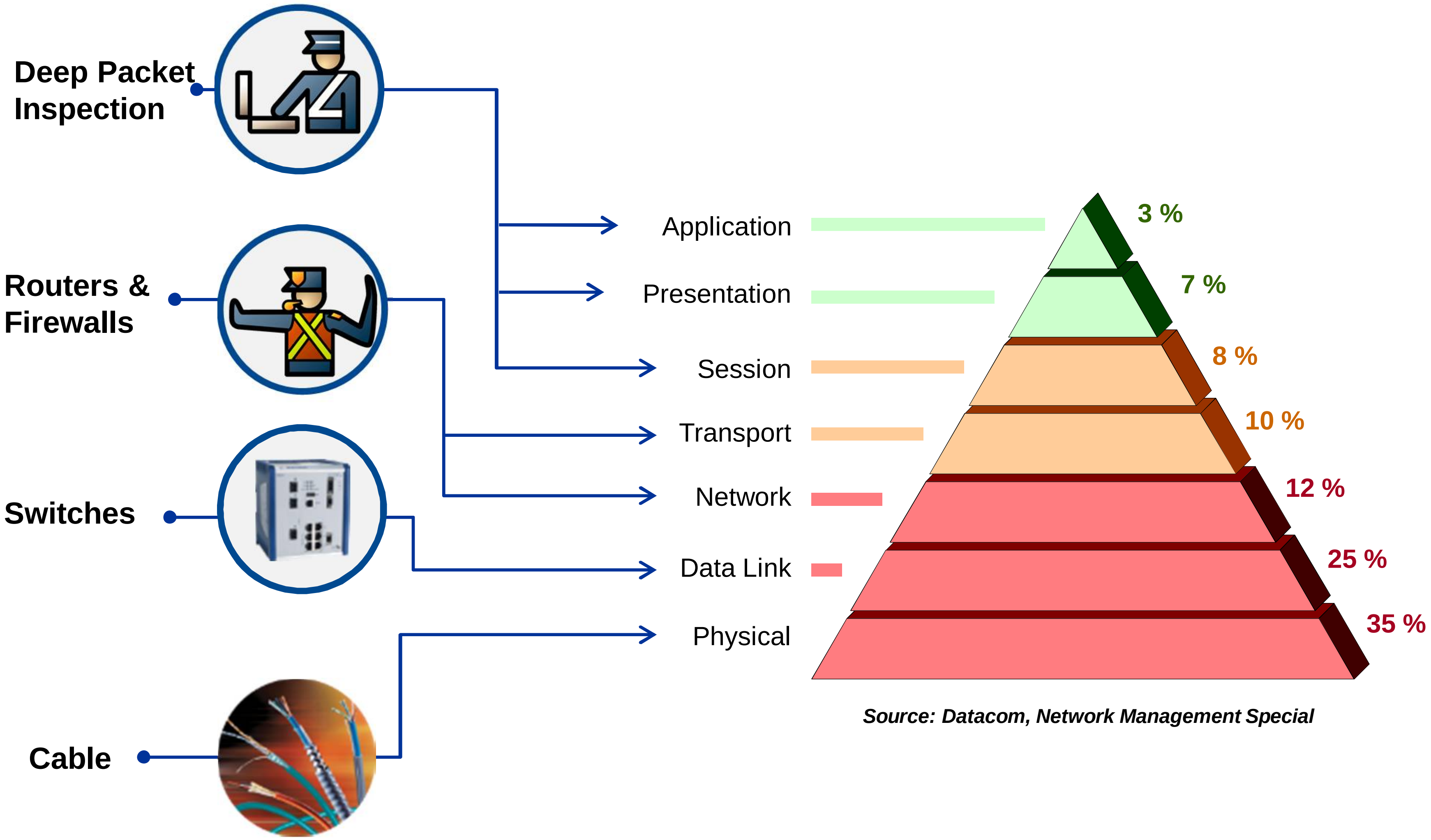
- Security management and visibility needs to span the entire system
  - Not just firewall management
  - System security management

Combination of Software and Hardware Tools Can Help You Answer These Questions



Where network failures occur…

Solutions You Can Deploy



Deep Packet Inspection

Routers & Firewalls

Switches

Cable

Application 3 %

Presentation 7 %

Session 8 %

Transport 10 %

Network 12 %

Data Link 25 %

Physical 35 %

Source: Datacom, Network Management Special

Belden offers Four Firewall Families

Price

DPI Capabilities

Eagle 30
2x GE + 4x FE

Eagle 20
4x FE

Tofino Xenon
2x FE

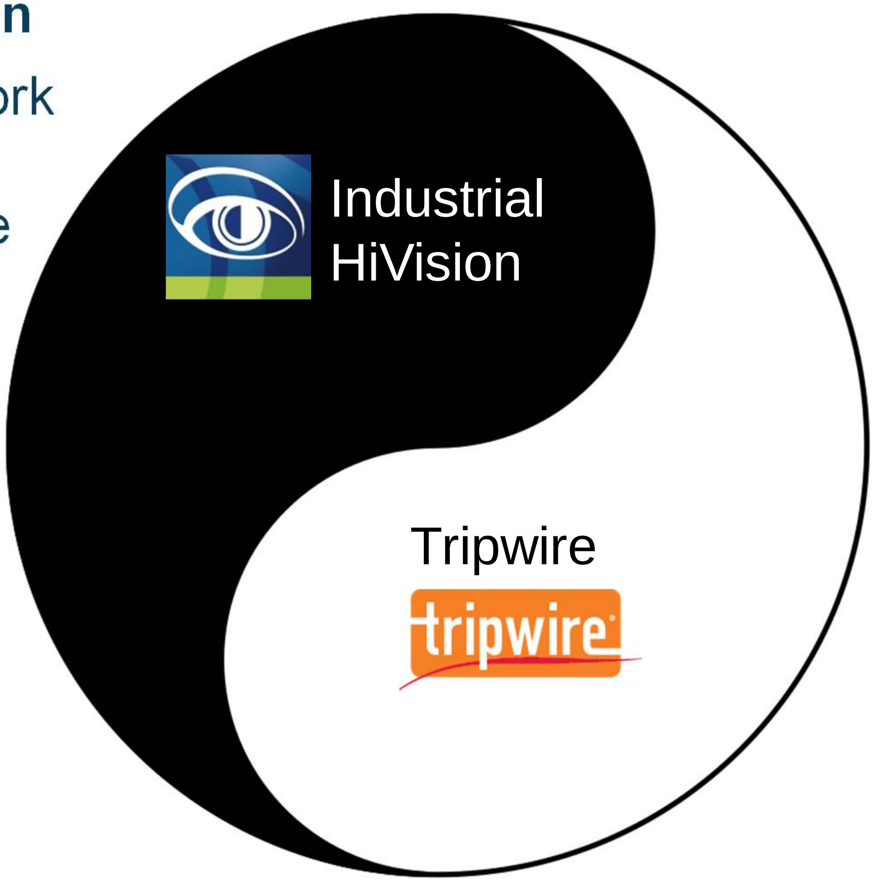
Eagle One
2x FE

Throughput

Belden Offers Two Software Platforms To Help

Industrial HiVision

- ❑ Graphical Network Management System software



Tripwire

- ❑ Like SCADA for security
- ❑ Detect threats, identify vulnerabilities, and harden configurations in real time

BELDEN
SENDING ALL THE RIGHT SIGNALS

Example System Architecture

☑ What is ICS Cybersecurity?

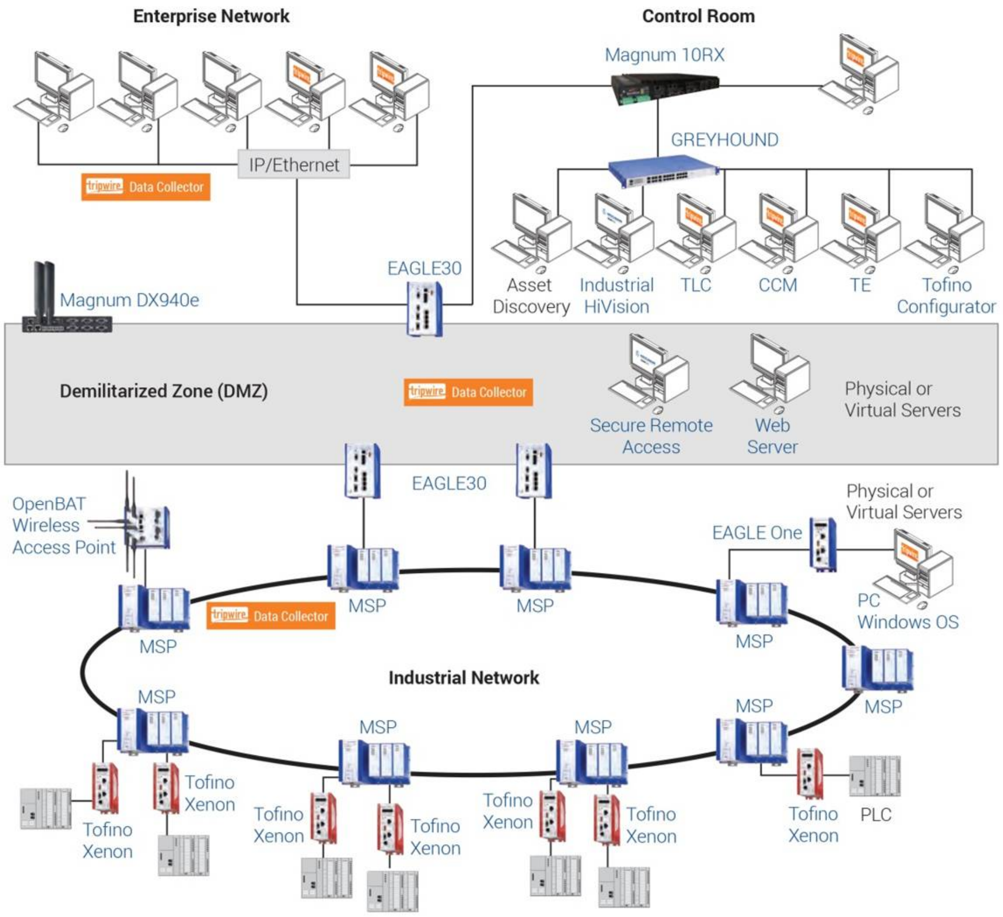
☑ Overall security philosophy

□ Example system architecture

□ Introduction to Firewalls

□ What Solutions Belden can offer?

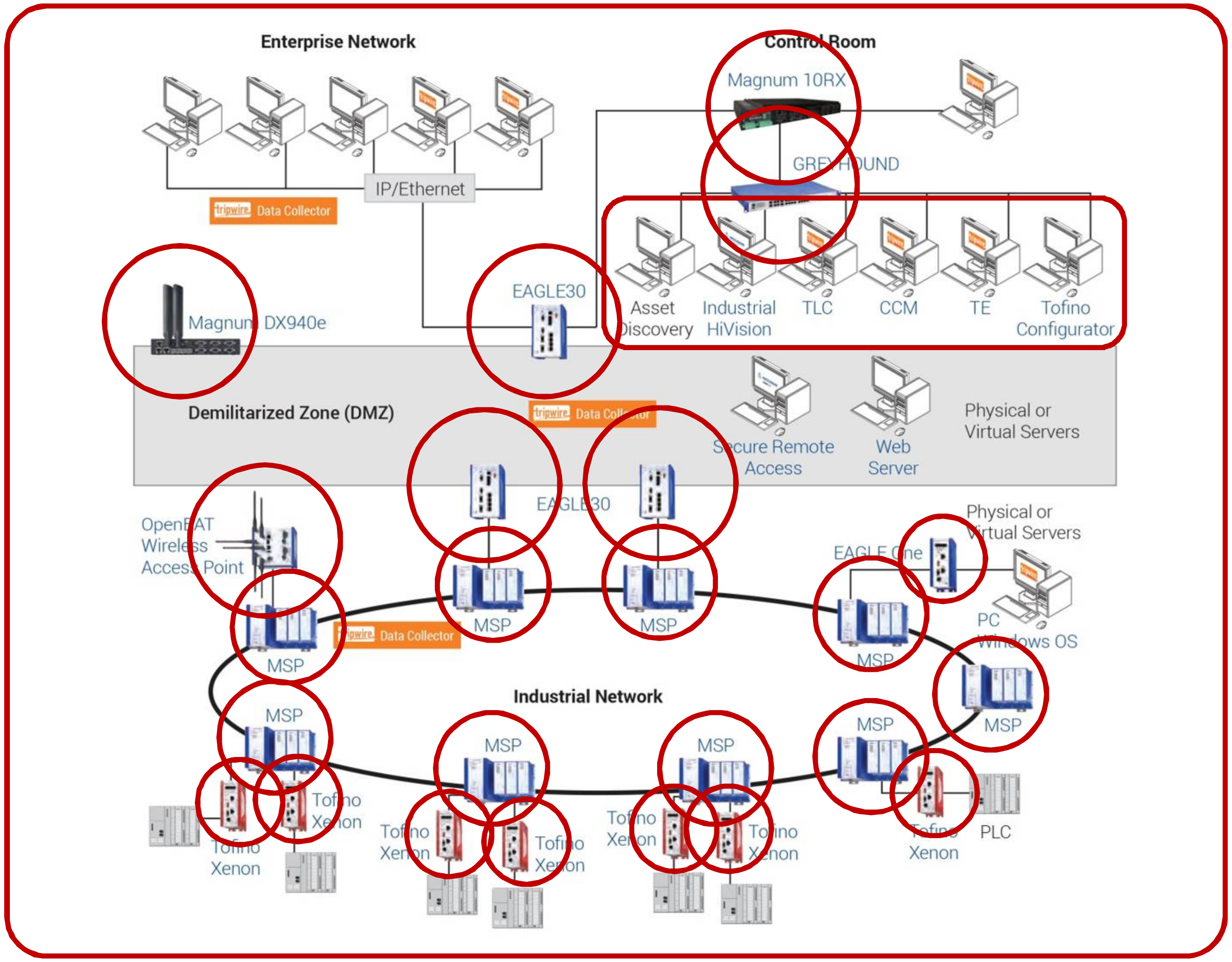
Example System Architecture



TLC = Tripwire Log Center | CCM = Configuration Compliance Manager | TE = Tripwire Enterprise

Example System Architecture

- Protect access to the Internet and other networks
- Protect access to the local network
- Protect critical assets
- Ensure policy enforcement and monitoring



TLC = Tripwire Log Center | CCM = Configuration Compliance Manager | TE = Tripwire Enterprise

BELDEN
SENDING ALL THE RIGHT SIGNALS

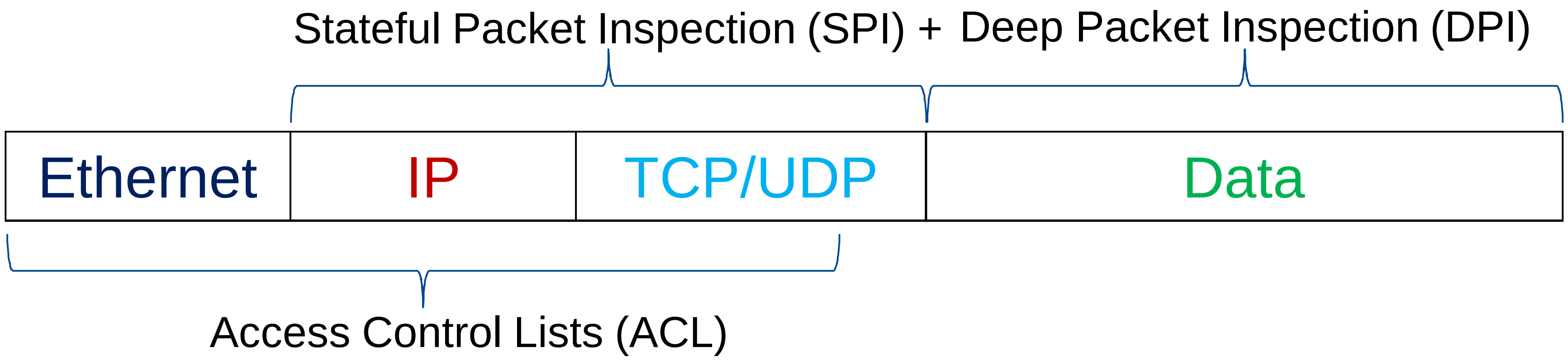
Introduction to Firewalls

- ☑ What is ICS Cybersecurity?
- ☑ Overall security philosophy
- ☑ Example system architecture
- □ Introduction to Firewalls
- □ What Solutions Belden can offer?

Core Functionality of Every Firewall: Packet Filtering

Packets are analyzed and filtered based on different information in the data packet:

- Source / Destination MAC address (ACL)
- Ethertype, VLAN, Priority (ACL)
- Source / Destination IP address (ACL / SPI)
- Protocol (ACL / SPI)
- Source / Destination TCP/UDP port (ACL / SPI)
- State of a TCP session (SPI)
- Data (DPI)


Stateful Packet Inspection (SPI) + Deep Packet Inspection (DPI)
Ethernet
IP
TCP/UDP
Data
Access Control Lists (ACL)

Core Functionality of Every Firewall: Packet Filtering

- Firewalls are a key component to controlling information flow
  - Should I pass this packet on, or report it, and/or drop it?

- Different types of firewall technology make their forwarding decisions based on different criteria

- Different types of firewall technology are targeted toward different needs within the system

- Complete protection comes from using all of them – in the right place

Variations of Firewalls

- Until recently, the following marketing punchline was often used:
  - “You need a secure network? Go get a firewall!”

- But:
  - Firewalls are not magical devices that somehow create security
  - Firewalls are very diverse. Not every firewalls fits every use case.
  - Firewalls must be applied and configured properly to provide any security

Network-Firewall

Client-Firewall

IP Firewall

Deep Packet Inspecton

Layer 2 Firewall

Stateless

Access Control Lists

Stateful Packet Inspection

MAC Filter

Learning Mode

Industrial Firewall

WLAN Firewall

Transparent Firewall

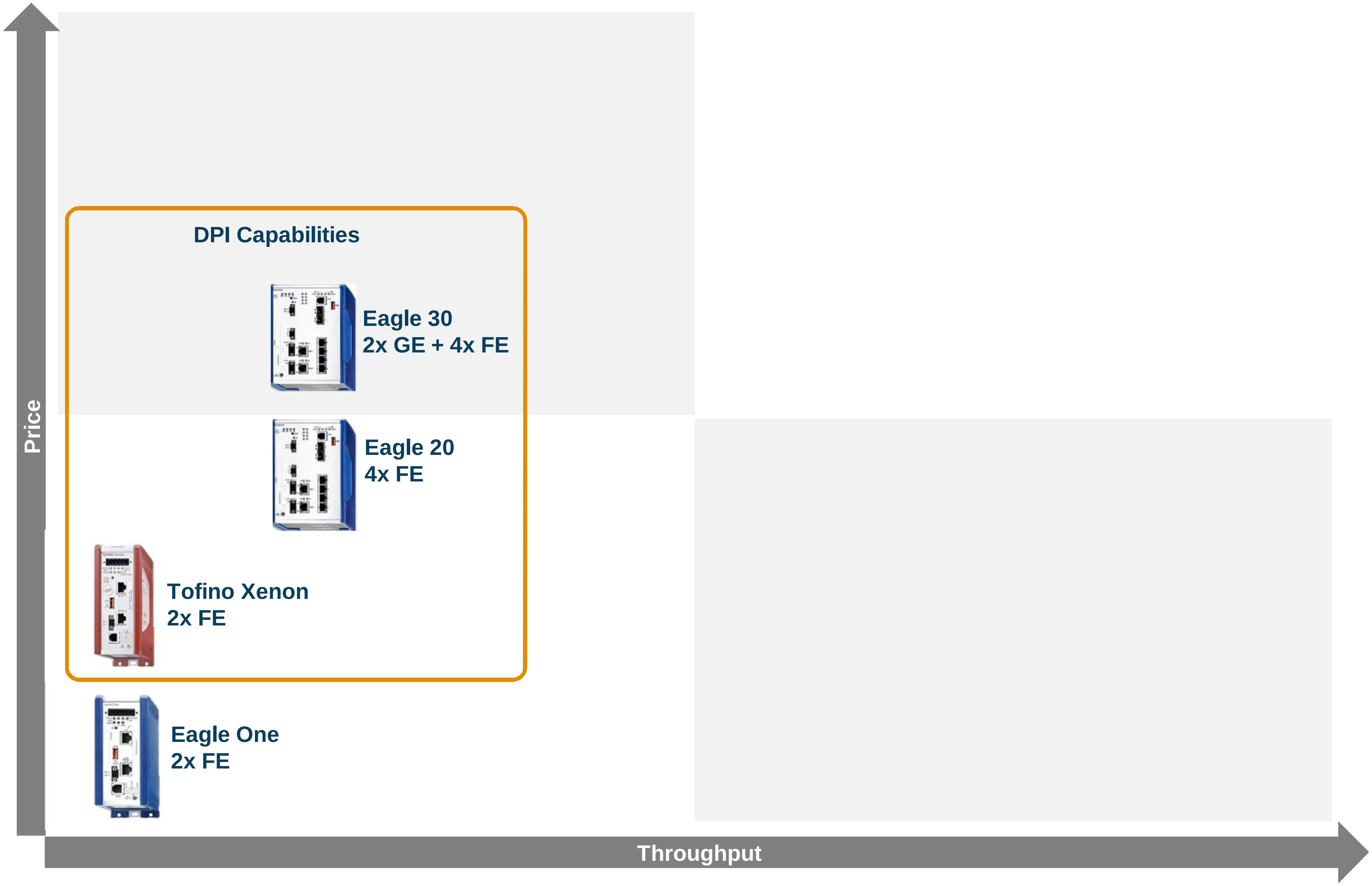
SPI

BELDEN
SENDING ALL THE RIGHT SIGNALS

What Solutions Belden can offer?

- ☑ What is ICS Cybersecurity?
- ☑ Overall security philosophy
- ☑ Example system architecture
- ☑ Introduction to Firewalls
- □ What Solutions Belden can offer?

Belden offers Four Firewall Families



DPI Capabilities

Eagle 30
2x GE + 4x FE

Eagle 20
4x FE

Tofino Xenon
2x FE

Eagle One
2x FE

Different Firewall Technologies For Different Needs

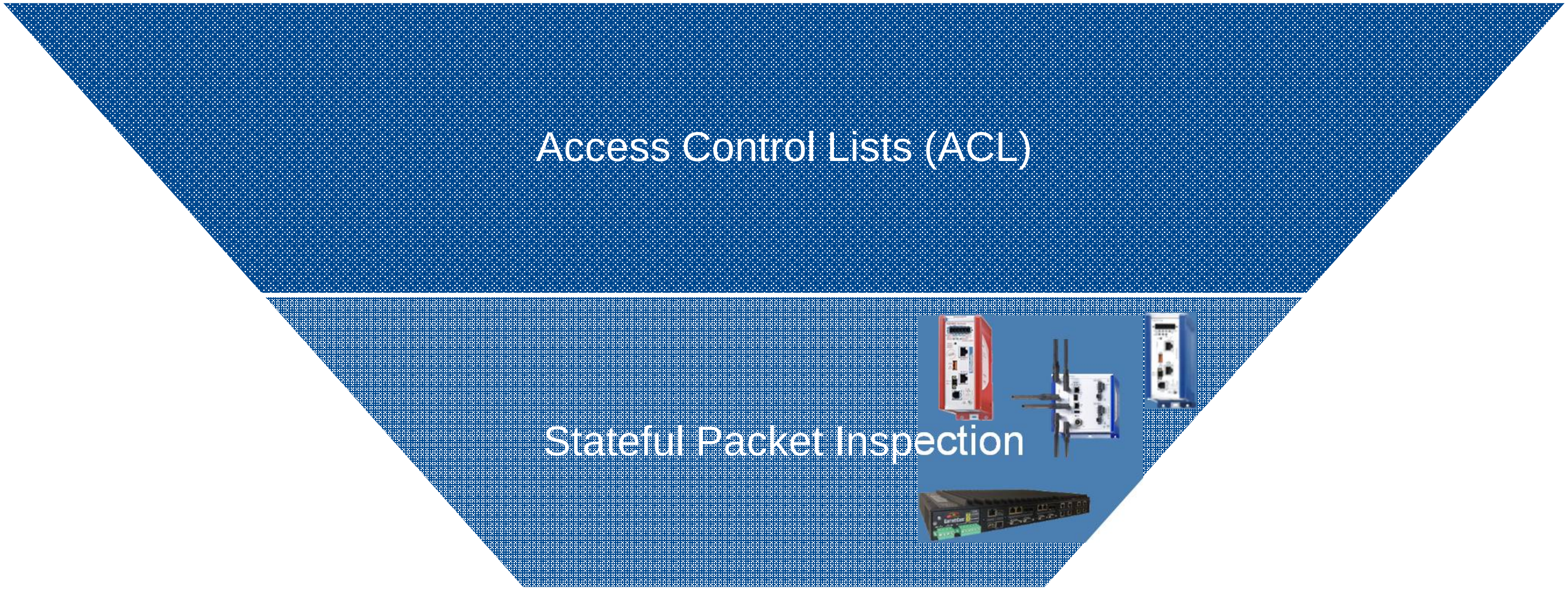
Access Control Lists (ACL)

- A list of who can to talk to whom based on values within the Ethernet, IP and TCP/UDP headers

- Can also specify bandwidth limitations and prioritize specific communications

- No memory across packets – each packet looked at in isolation

Different Firewall Technologies For Different Needs

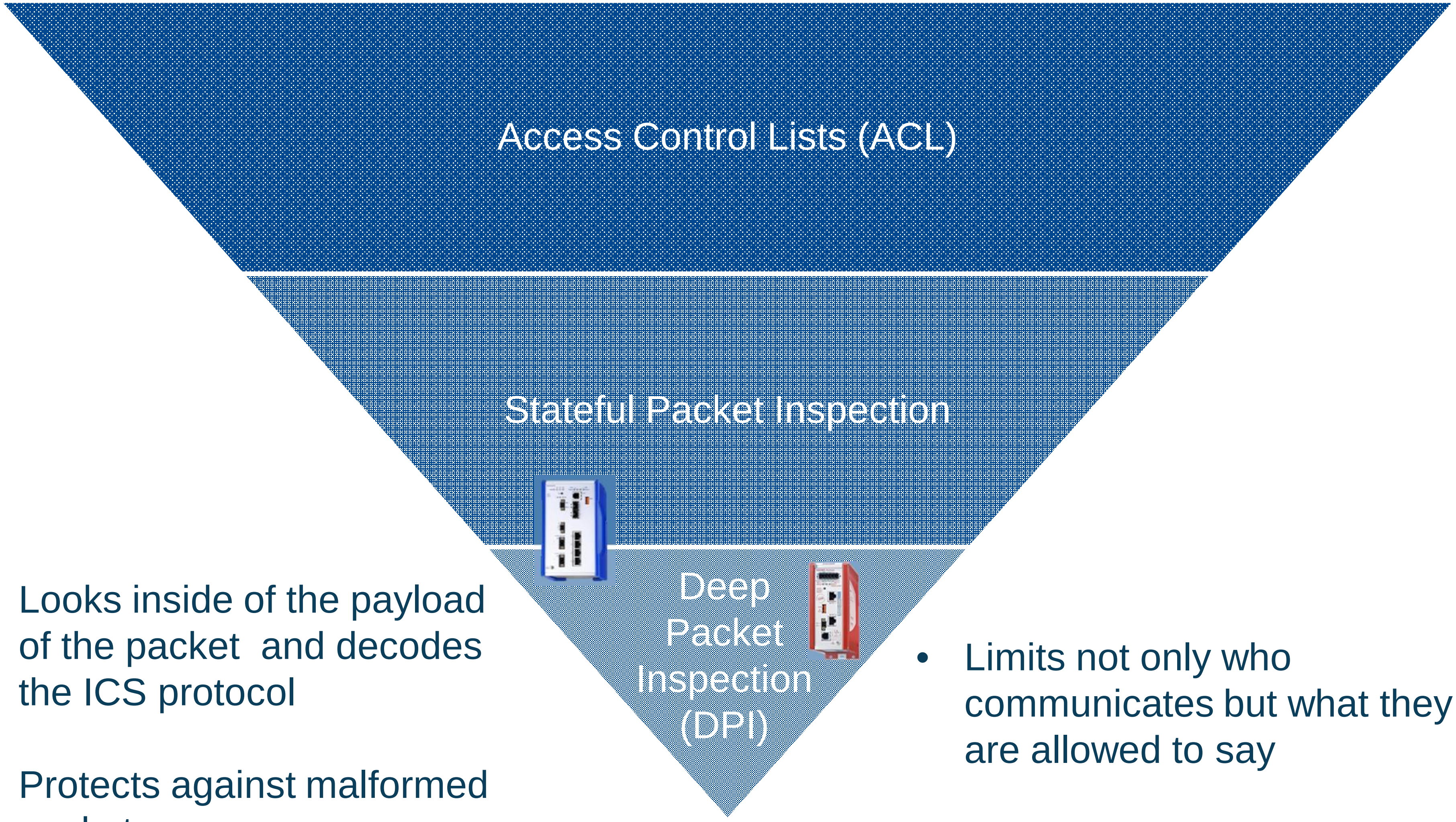


Access Control Lists (ACL)

Stateful Packet Inspection

- Has memory across packets – looks at each packet in context
- If this is a response, was there a request?
- Protects against denial of service attracts

Different Firewall Technologies For Different Needs



Access Control Lists (ACL)

Stateful Packet Inspection

Deep Packet Inspection (DPI)

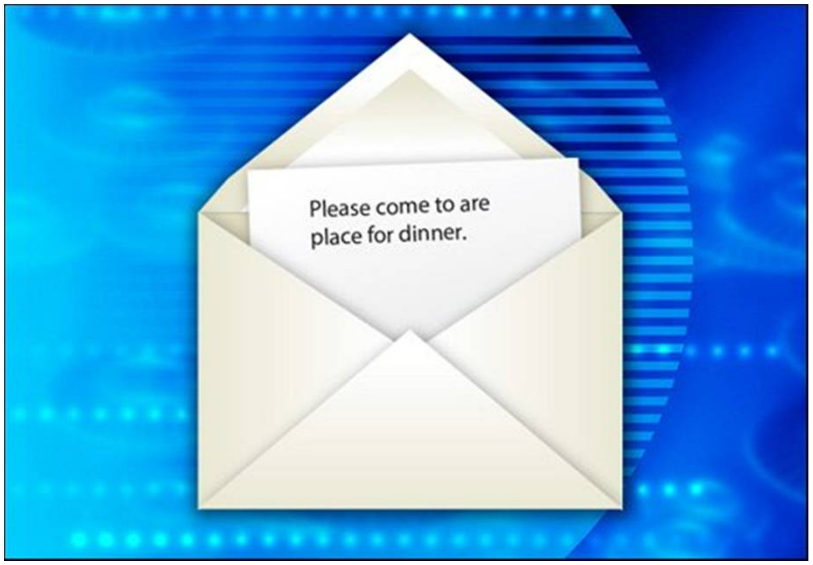
- Looks inside of the payload of the packet and decodes the ICS protocol

- Protects against malformed packets

- Limits not only who communicates but what they are allowed to say

Deep Packet Inspection

Belden Inc.
USA
Belden India Pvt. Ltd
India



- Standard firewalls identify only:
  - who a message is from (source),
  - where it is going (destination) and
  - maybe the language of the contents (port).
  - You don’t know anything about the letter’s content though.

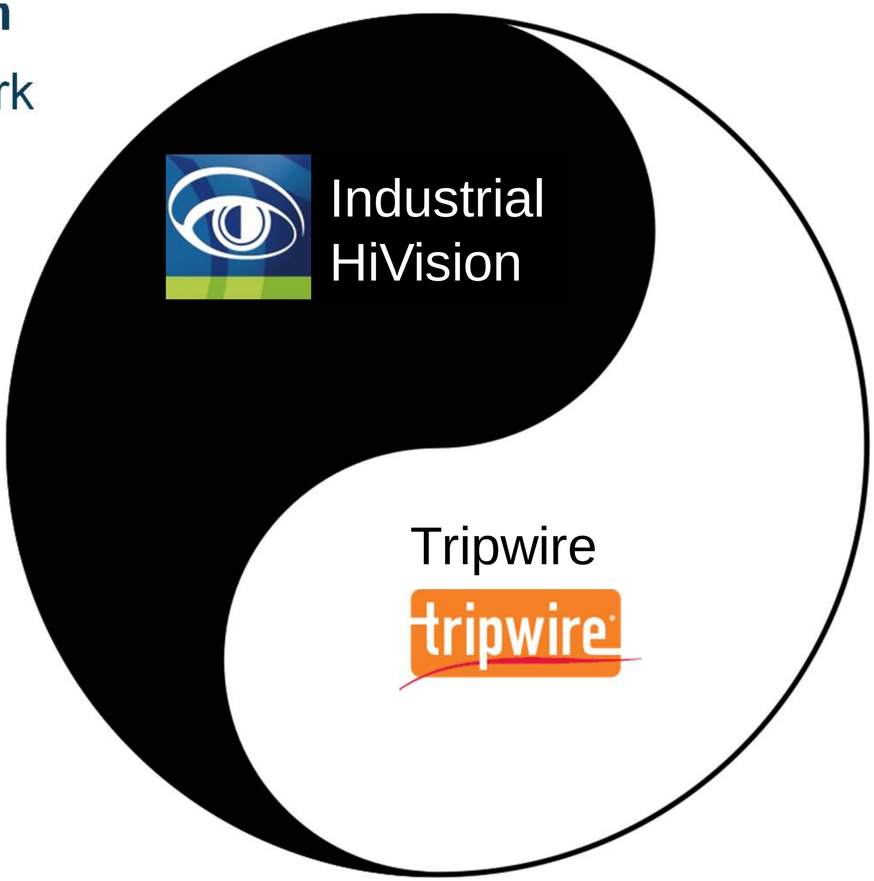
- With Signature-based DPI:
  - This message would be rejected only if it is in the signature database in this exact format.

- With Protocol-specific DPI:
  - Has the smarts to know this is “bad grammar” and would proactively block it.

Belden Offers Two Software Platforms

Industrial HiVision

- ❑ Graphical Network Management System software



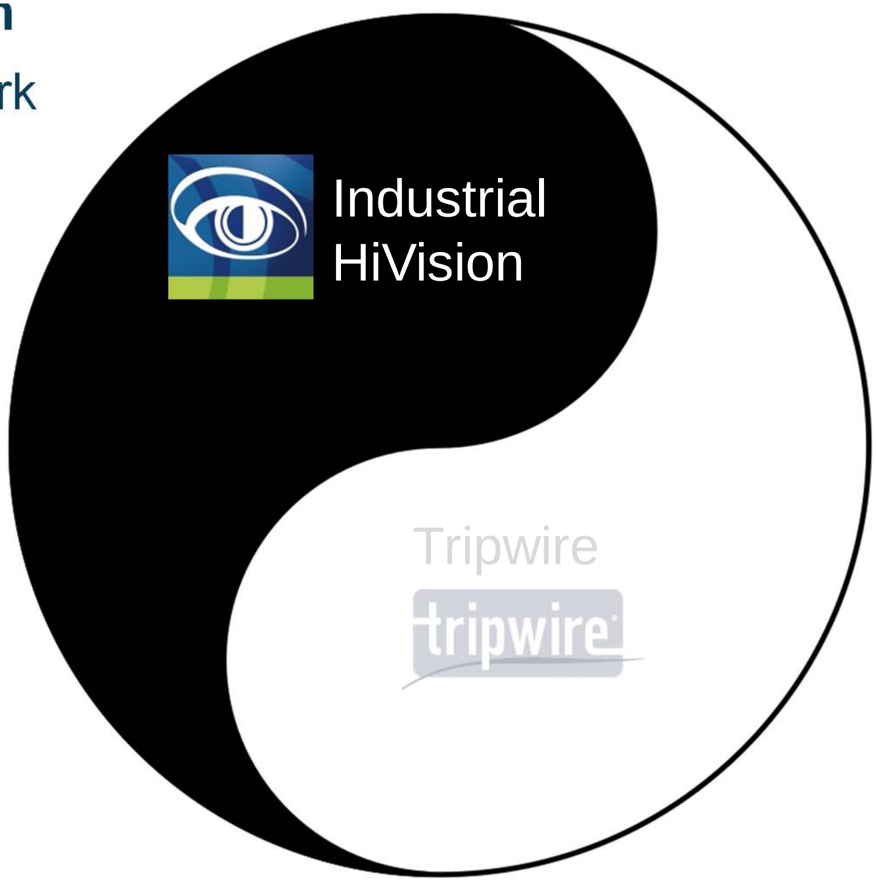
Tripwire

- ❑ Like SCADA for security
- ❑ Detect threats, identify vulnerabilities, and harden configurations in real time

Belden Offers Two Software Platforms

Industrial HiVision

- ❑ Graphical Network Management System software



Industrial HiVision

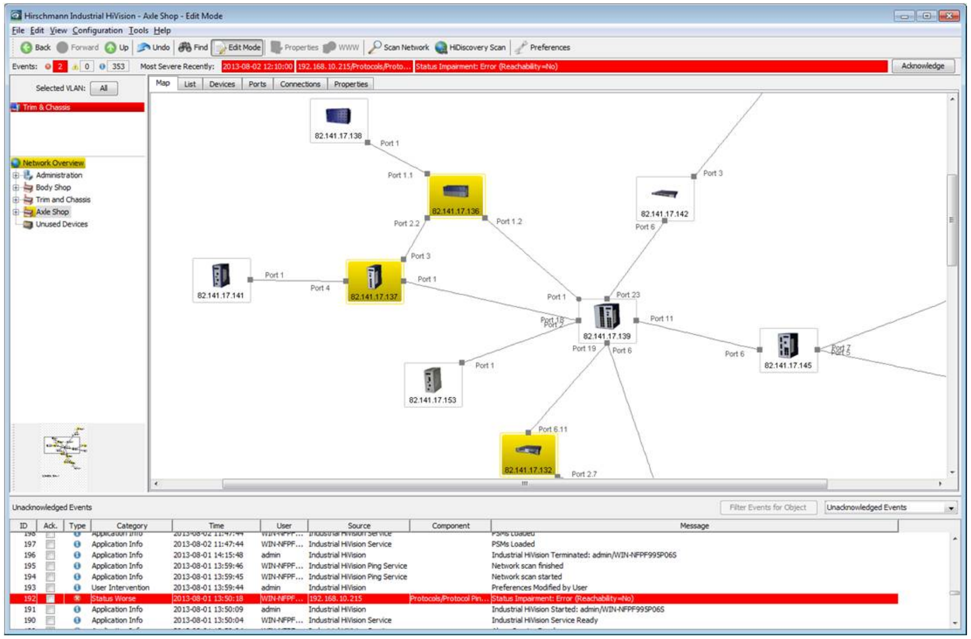
Tripwire

Tripwire

- Like SCADA for security
- Detect threats, identify vulnerabilities, and harden configurations in real time

What is Industrial HiVision?

- Hirschmann’s graphical Network Management System software
- Specifically developed for configuration and supervision of industrial networks
- Can be used to supervise devices from any manufacturer
- Designed for use by Automation Engineers
- Provides interfaces to SCADA systems



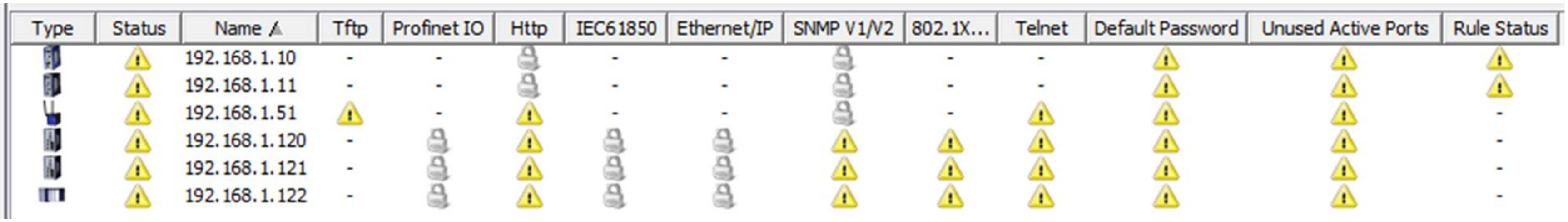
Events: 2 0 353 Most Severe Recently: 2013-08-02 12:10:00 192.168.10.215/Protocols/Proto... Status Impairment: Error (Reachability=No)

Unacknowledged Events

ID	Ack.	Type	Category	Time	User	Source	Component	Message
197	□	ℹ	Application Info	2013-08-02 11:47:44	WIN-NFPF...	Industrial HiVision Service		PSMs Loaded
196	□	ℹ	Application Info	2013-08-01 14:15:48	admin	Industrial HiVision		Industrial HiVision Terminated: admin/WIN-NFPF995P06S
195	□	ℹ	Application Info	2013-08-01 13:59:46	WIN-NFPF...	Industrial HiVision Ping Service		Network scan finished
194	□	ℹ	Application Info	2013-08-01 13:59:45	WIN-NFPF...	Industrial HiVision Ping Service		Network scan started
193	□	ℹ	User Intervention	2013-08-01 13:59:44	admin	Industrial HiVision		Preferences Modified by User
192	□	⊗	Status Worse	2013-08-01 13:50:18	WIN-NFPF...	192.168.10.215	Protocols/Protocol Pin...	Status Impairment: Error (Reachability=No)
191	□	ℹ	Application Info	2013-08-01 13:50:09	admin	Industrial HiVision		Industrial HiVision Started: admin/WIN-NFPF995P06S
190	□	ℹ	Application Info	2013-08-01 13:50:04	WIN-NFPF...	Industrial HiVision Service		Industrial HiVision Service Ready

Network Management Software – Industrial HiVision

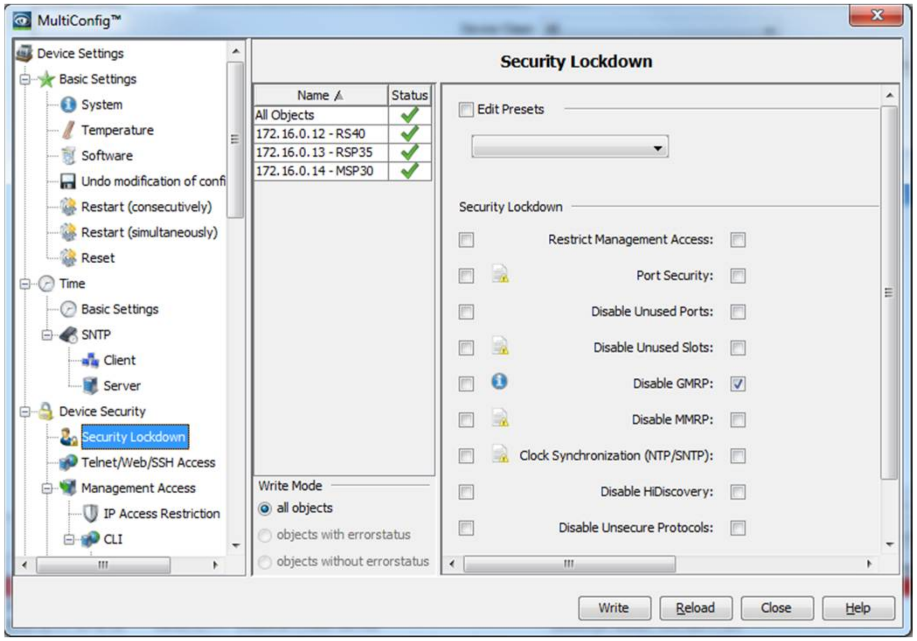
- Network infrastructure security status



Type	Status	Name ⩓	Tftp	Profinet IO	Http	IEC61850	Ethernet/IP	SNMP V1/V2	802.1X...	Telnet	Default Password	Unused Active Ports	Rule Status
	⚠	192.168.1.10	-	-	🔒	-	-	🔒	-	-	⚠	⚠	⚠
	⚠	192.168.1.11	-	-	🔒	-	-	🔒	-	-	⚠	⚠	⚠
	⚠	192.168.1.51	⚠	-	⚠	-	-	🔒	-	⚠	⚠	⚠	-
	⚠	192.168.1.120	-	🔒	⚠	🔒	🔒	⚠	⚠	⚠	⚠	⚠	-
	⚠	192.168.1.121	-	🔒	⚠	🔒	🔒	⚠	⚠	⚠	⚠	⚠	-
	⚠	192.168.1.122	-	🔒	⚠	🔒	🔒	⚠	⚠	⚠	⚠	⚠	-

Network Management Software – Industrial HiVision

- Network infrastructure security status
- Security lockdown



Security Lockdown

Name	Status
All Objects	✓
172.16.0.12 - RS40	✓
172.16.0.13 - RSP35	✓
172.16.0.14 - MSP30	✓

Write Mode
● all objects
○ objects with errorstatus
○ objects without errorstatus

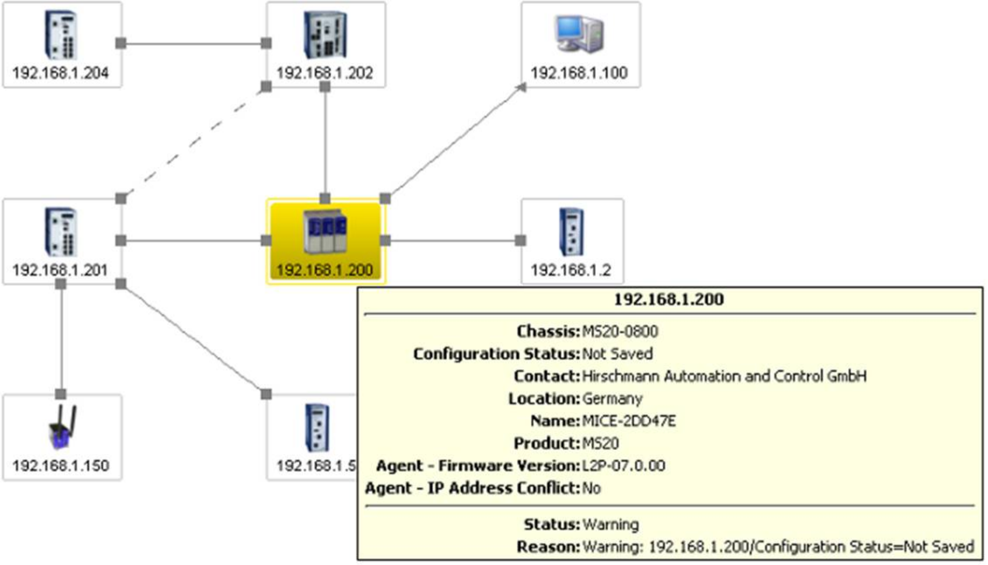
□ Edit Presets

Security Lockdown

□	Restrict Management Access:	□
□	Port Security:	□
□	Disable Unused Ports:	□
□	Disable Unused Slots:	□
□	Disable GMRP:	☑
□	Disable MMRP:	□
□	Clock Synchronization (NTP/SNTP):	□
□	Disable HiDiscovery:	□
□	Disable Unsecure Protocols:	□

Network Management Software – Industrial HiVision

- Network infrastructure security status
- Security lockdown
- Configuration status display



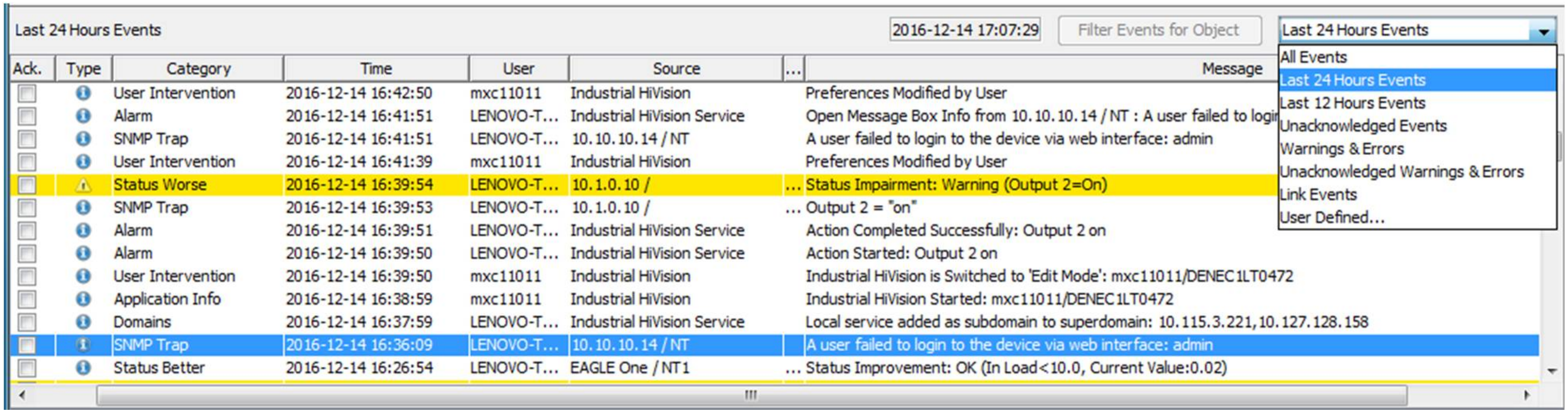
192.168.1.200

Chassis: MS20-0800
Configuration Status: Not Saved
Contact: Hirschmann Automation and Control GmbH
Location: Germany
Name: MICE-2DD47E
Product: MS20
Agent - Firmware Version: L2P-07.0.00
Agent - IP Address Conflict: No

Status: Warning
Reason: Warning: 192.168.1.200/Configuration Status=Not Saved

Network Management Software – Industrial HiVision

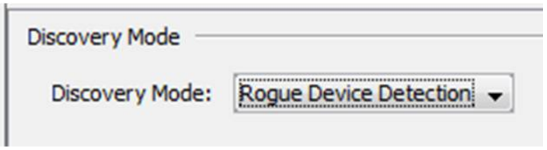
- Network infrastructure security status
- Security lockdown
- Configuration status display
- Event logging, reporting and forwarding



Ack.	Type	Category	Time	User	Source	...	Message
□	ℹ	User Intervention	2016-12-14 16:42:50	mxc11011	Industrial HiVision		Preferences Modified by User
□	ℹ	Alarm	2016-12-14 16:41:51	LENOVO-T...	Industrial HiVision Service		Open Message Box Info from 10.10.10.14 / NT : A user failed to logi
□	ℹ	SNMP Trap	2016-12-14 16:41:51	LENOVO-T...	10.10.10.14 / NT		A user failed to login to the device via web interface: admin
□	ℹ	User Intervention	2016-12-14 16:41:39	mxc11011	Industrial HiVision		Preferences Modified by User
□	⚠	Status Worse	2016-12-14 16:39:54	LENOVO-T...	10.1.0.10 /	...	Status Impairment: Warning (Output 2=On)
□	ℹ	SNMP Trap	2016-12-14 16:39:53	LENOVO-T...	10.1.0.10 /	...	Output 2 = "on"
□	ℹ	Alarm	2016-12-14 16:39:51	LENOVO-T...	Industrial HiVision Service		Action Completed Successfully: Output 2 on
□	ℹ	Alarm	2016-12-14 16:39:50	LENOVO-T...	Industrial HiVision Service		Action Started: Output 2 on
□	ℹ	User Intervention	2016-12-14 16:39:50	mxc11011	Industrial HiVision		Industrial HiVision is Switched to 'Edit Mode': mxc11011/DENEC1LT0472
□	ℹ	Application Info	2016-12-14 16:38:59	mxc11011	Industrial HiVision		Industrial HiVision Started: mxc11011/DENEC1LT0472
□	ℹ	Domains	2016-12-14 16:37:59	LENOVO-T...	Industrial HiVision Service		Local service added as subdomain to superdomain: 10.115.3.221,10.127.128.158
□	ℹ	SNMP Trap	2016-12-14 16:36:09	LENOVO-T...	10.10.10.14 / NT		A user failed to login to the device via web interface: admin
□	ℹ	Status Better	2016-12-14 16:26:54	LENOVO-T...	EAGLE One / NT1	...	Status Improvement: OK (In Load<10.0, Current Value:0.02)

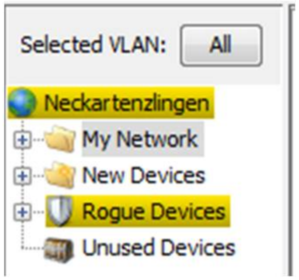
Network Management Software – Industrial HiVision

- Network infrastructure security status
- Security lockdown
- Configuration status display
- Event logging, reporting and forwarding
- Rogue device detection

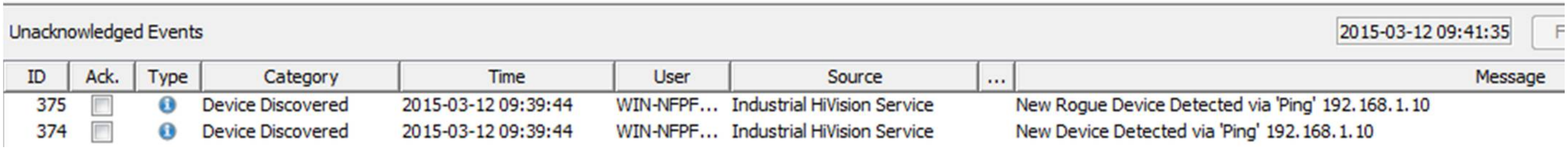


Discovery Mode

Discovery Mode: Rogue Device Detection



Selected VLAN: All

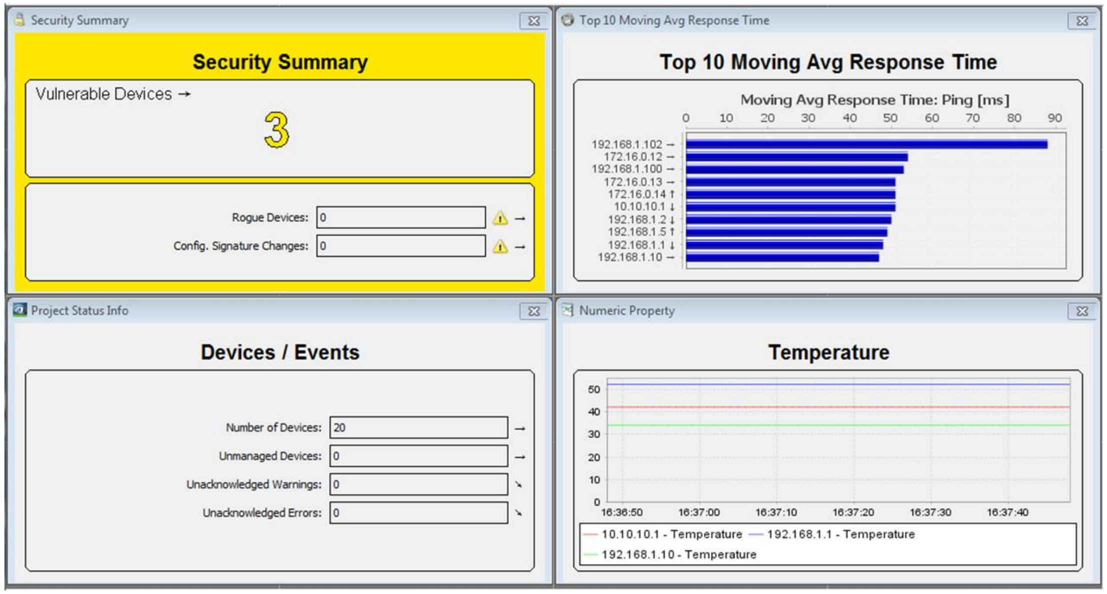


Unacknowledged Events 2015-03-12 09:41:35

ID	Ack.	Type	Category	Time	User	Source	...	Message
375	□	ℹ	Device Discovered	2015-03-12 09:39:44	WIN-NFPF...	Industrial HiVision Service		New Rogue Device Detected via 'Ping' 192.168.1.10
374	□	ℹ	Device Discovered	2015-03-12 09:39:44	WIN-NFPF...	Industrial HiVision Service		New Device Detected via 'Ping' 192.168.1.10

Network Management Software – Industrial HiVision

- Network infrastructure security status
- Security lockdown
- Configuration status display
- Event logging, reporting and forwarding
- Rogue device detection
- Network dashboard



Security Summary

Security Summary

Vulnerable Devices →

3

Rogue Devices: 0 →

Config. Signature Changes: 0 →

Top 10 Moving Avg Response Time

Top 10 Moving Avg Response Time

Project Status Info

Devices / Events

Number of Devices: 20 →

Unmanaged Devices: 0 →

Unacknowledged Warnings: 0 ↘

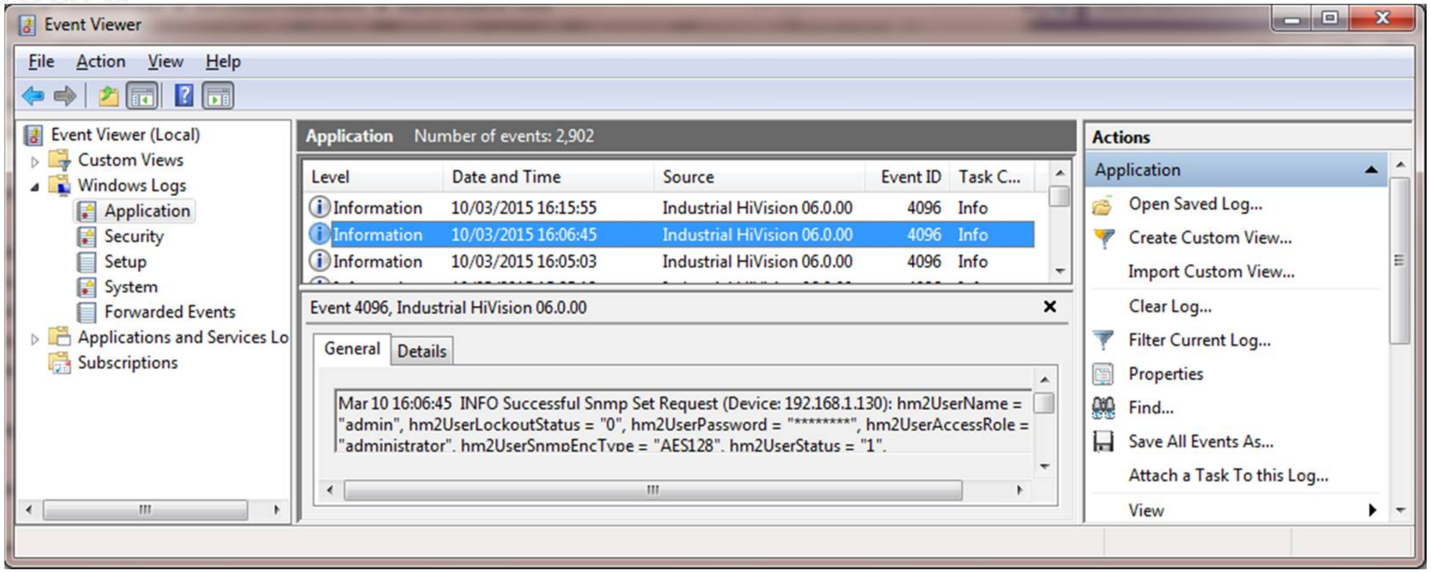
Unacknowledged Errors: 0 ↘

Numeric Property

Temperature

Network Management Software – Industrial HiVision

- Network infrastructure security status
- Security lockdown
- Configuration status display
- Event logging, reporting and forwarding
- Rogue device detection
- Network dashboard
- Audit Trail



Application Number of events: 2,902

Level	Date and Time	Source	Event ID	Task C...
Information	10/03/2015 16:15:55	Industrial HiVision 06.0.00	4096	Info
Information	10/03/2015 16:06:45	Industrial HiVision 06.0.00	4096	Info
Information	10/03/2015 16:05:03	Industrial HiVision 06.0.00	4096	Info

Event 4096, Industrial HiVision 06.0.00

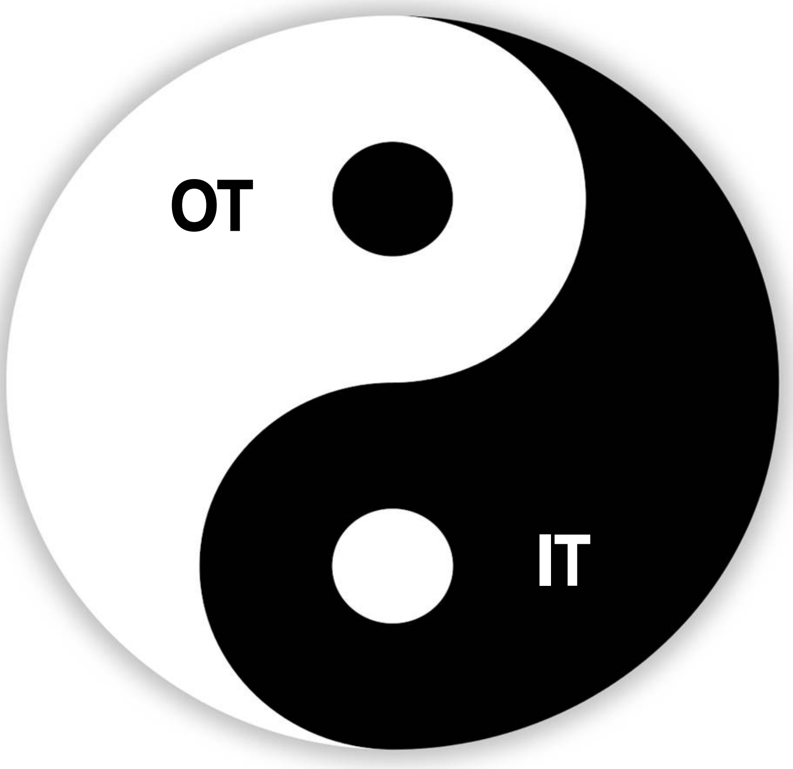
```
Mar 10 16:06:45 INFO Successful Snmp Set Request (Device: 192.168.1.130): hm2UserName =
"admin", hm2UserLockoutStatus = "0", hm2UserPassword = "********", hm2UserAccessRole =
"administrator", hm2UserSnmpEncType = "AES128", hm2UserStatus = "1".
```

Cyber Integrity Through Foundational Controls

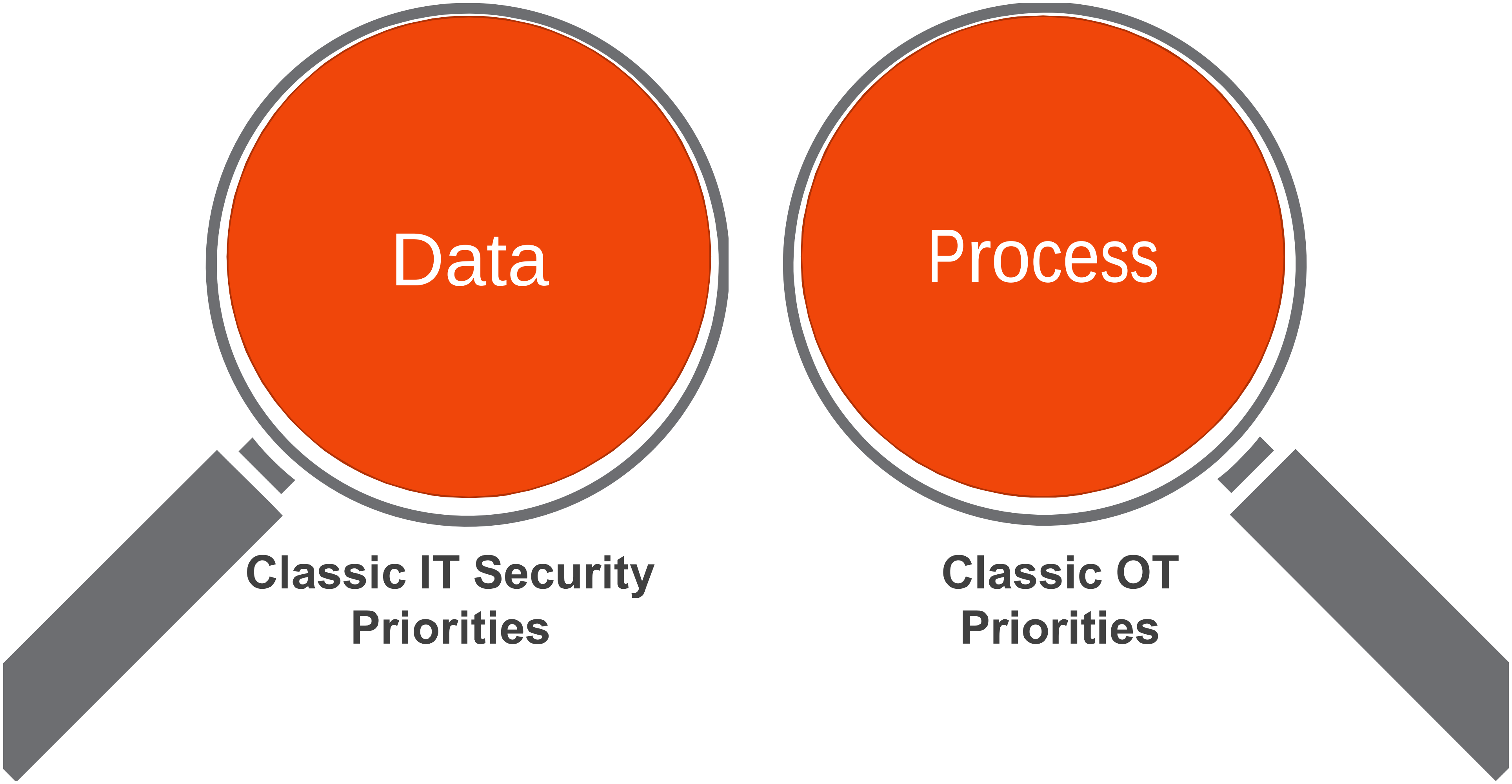
Pratap Mondal – RSM India & SAARC

IT-OT Convergence has long been in the works

- **Technology**
  - Networks
  - Systems
- **People**
  - Operations
  - Engineering
  - Cyber Security
- **Cyber Incidents**
  - Human/Operator Error
  - Equipment Failure
  - Malicious Activity



IT & OT: Same issues, different perspectives



Data

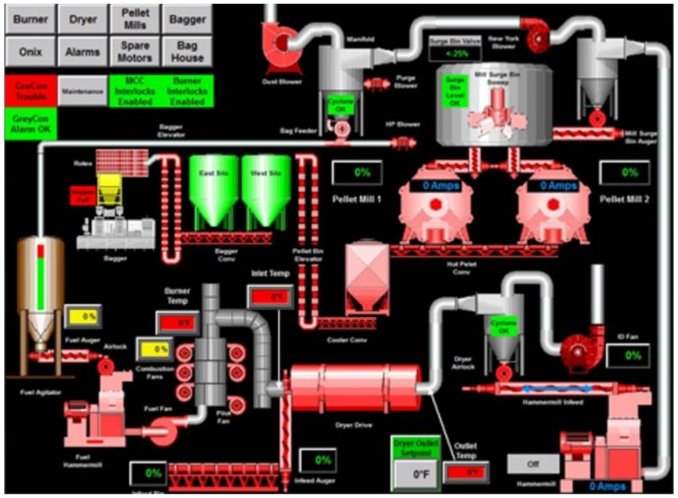
Process

Classic IT Security Priorities

Classic OT Priorities

Industrial Control Systems – Manage an Industrial Process

- **View**
  - Passive
  - Human interaction with process
- **Monitor**
  - Automated
  - Safety System
- **Control**
  - Changes driven through physical control of machinery



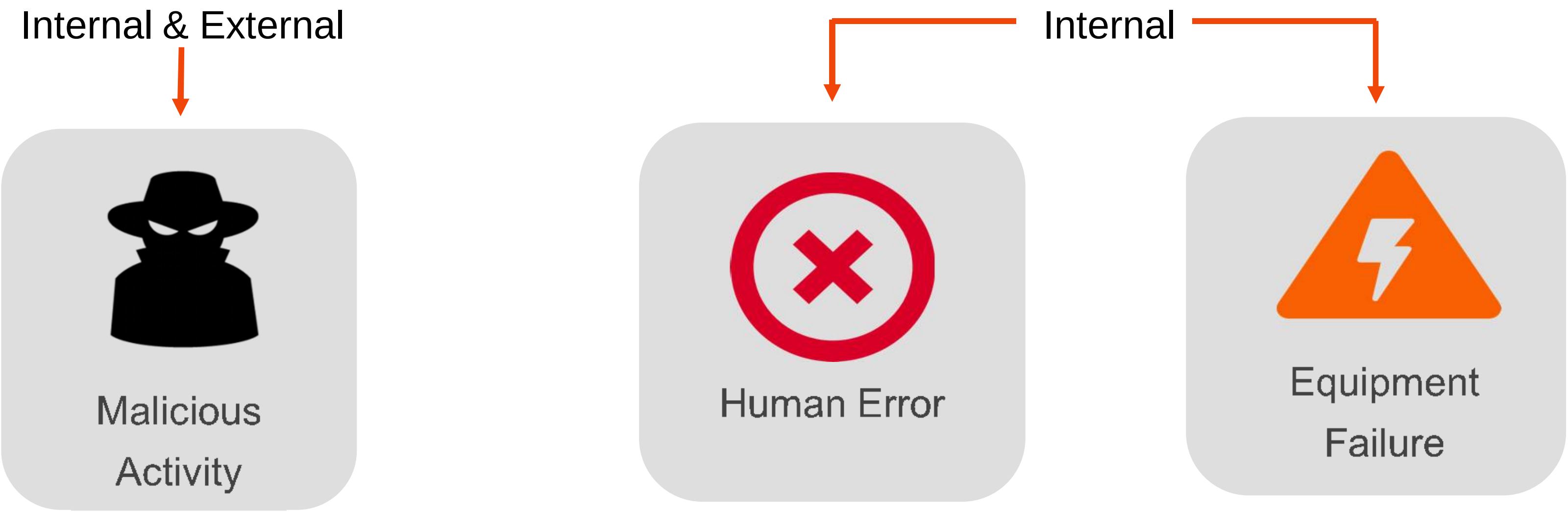
What is an Industrial Cyber Security Event?

- **Anything resulting in the loss, denial, or manipulation of the ability to:**
  - View
  - Monitor (Safety System)
  - Control
- **Which could detrimentally impact:**
  - Safety
  - Availability

What causes Industrial Cyber Security Events?

- **Human Error**
- **Equipment Failure**
- **Malicious Activity**
  - Disgruntled Employee
  - Hacker
  - Nation state
  - Ransomware
  - Malware

What causes an industrial cyber security event?



Internal & External

Internal

Malicious Activity

Human Error

Equipment Failure

Disgruntled employee, hacker, nation-state, ransomware, malware

Misconfiguration

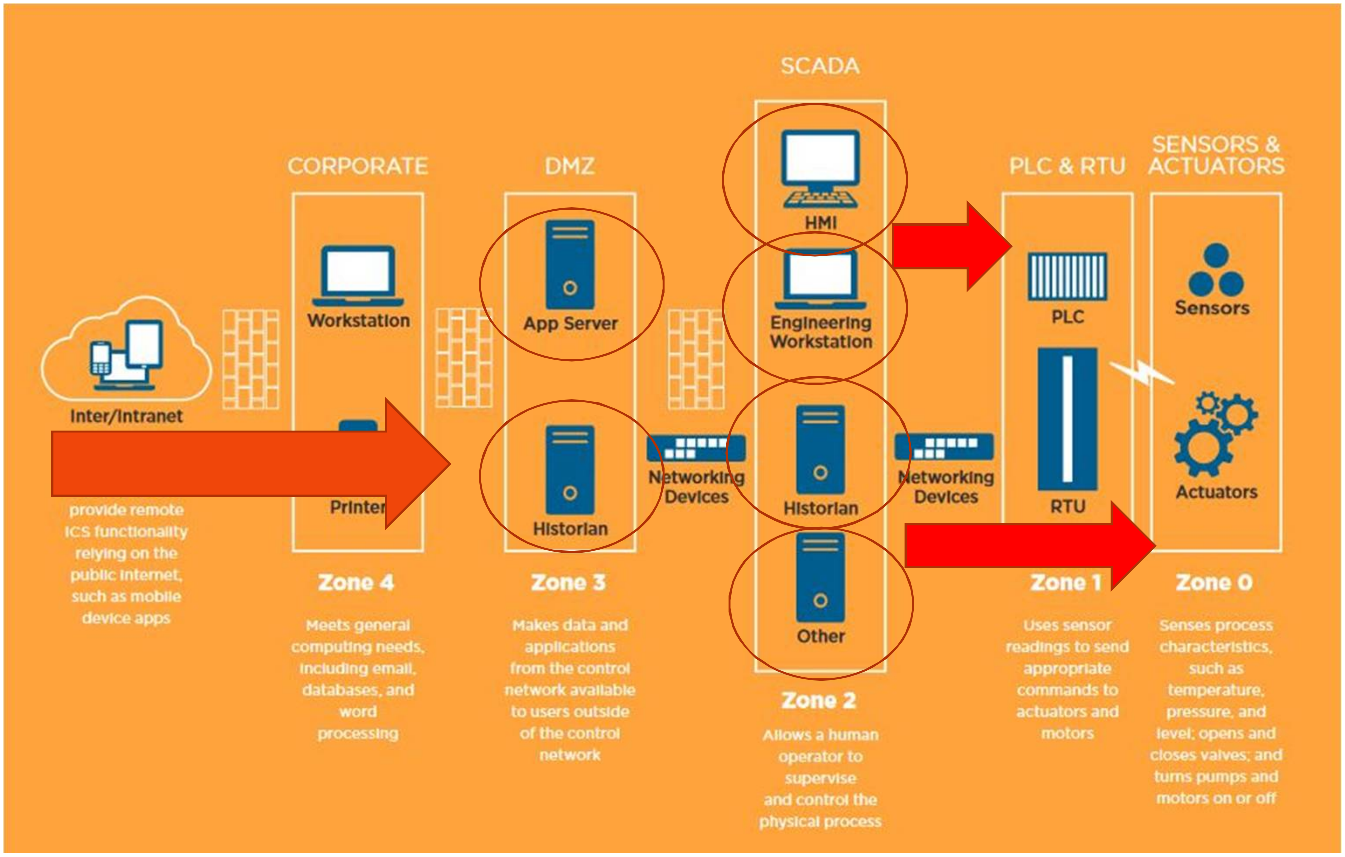
Not following process

Disk Drive

Power Supply

Faulty Cable

Where are the Hotspots for Cyber Security Events?



provide remote ICS functionality relying on the public internet, such as mobile device apps

Zone 4

Meets general computing needs, including email, databases, and word processing

Zone 3

Makes data and applications from the control network available to users outside of the control network

Zone 2

Allows a human operator to supervise and control the physical process

Zone 1

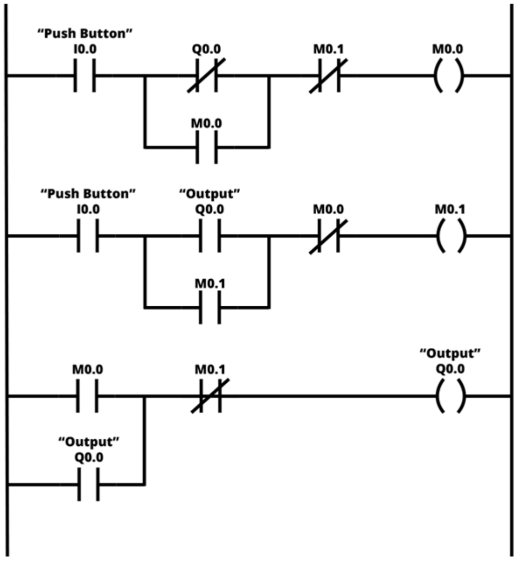
Uses sensor readings to send appropriate commands to actuators and motors

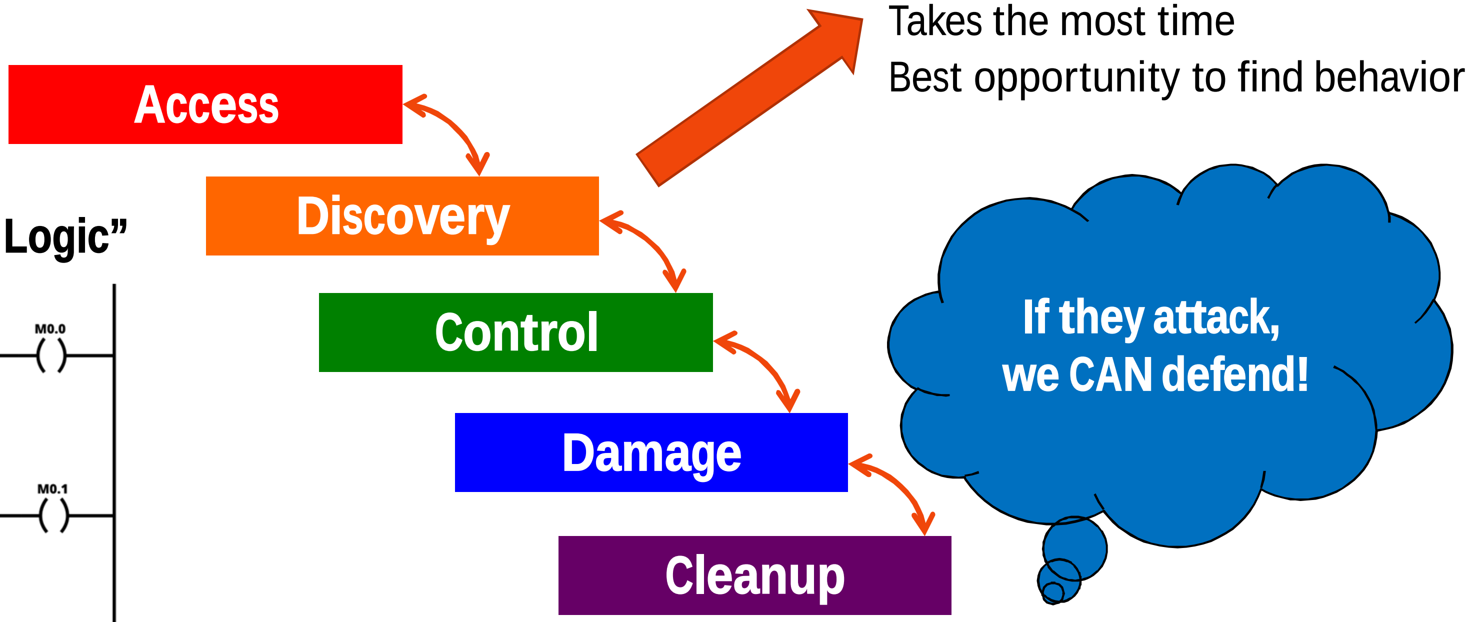
Zone 0

Senses process characteristics, such as temperature, pressure, and level; opens and closes valves; and turns pumps and motors on or off

We First Need to Understanding Attack Strategy

“Cyber Event Ladder Logic”





Access

Discovery

Control

Damage

Cleanup

Takes the most time
Best opportunity to find behavior.

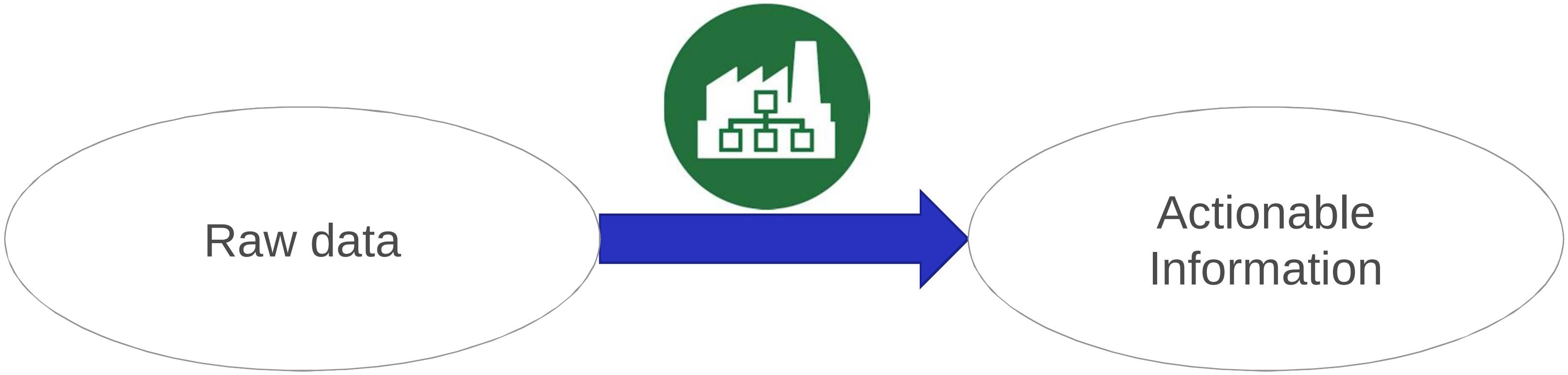
If they attack,
we CAN defend!

Data Gathering

Assessment/Detection Engine

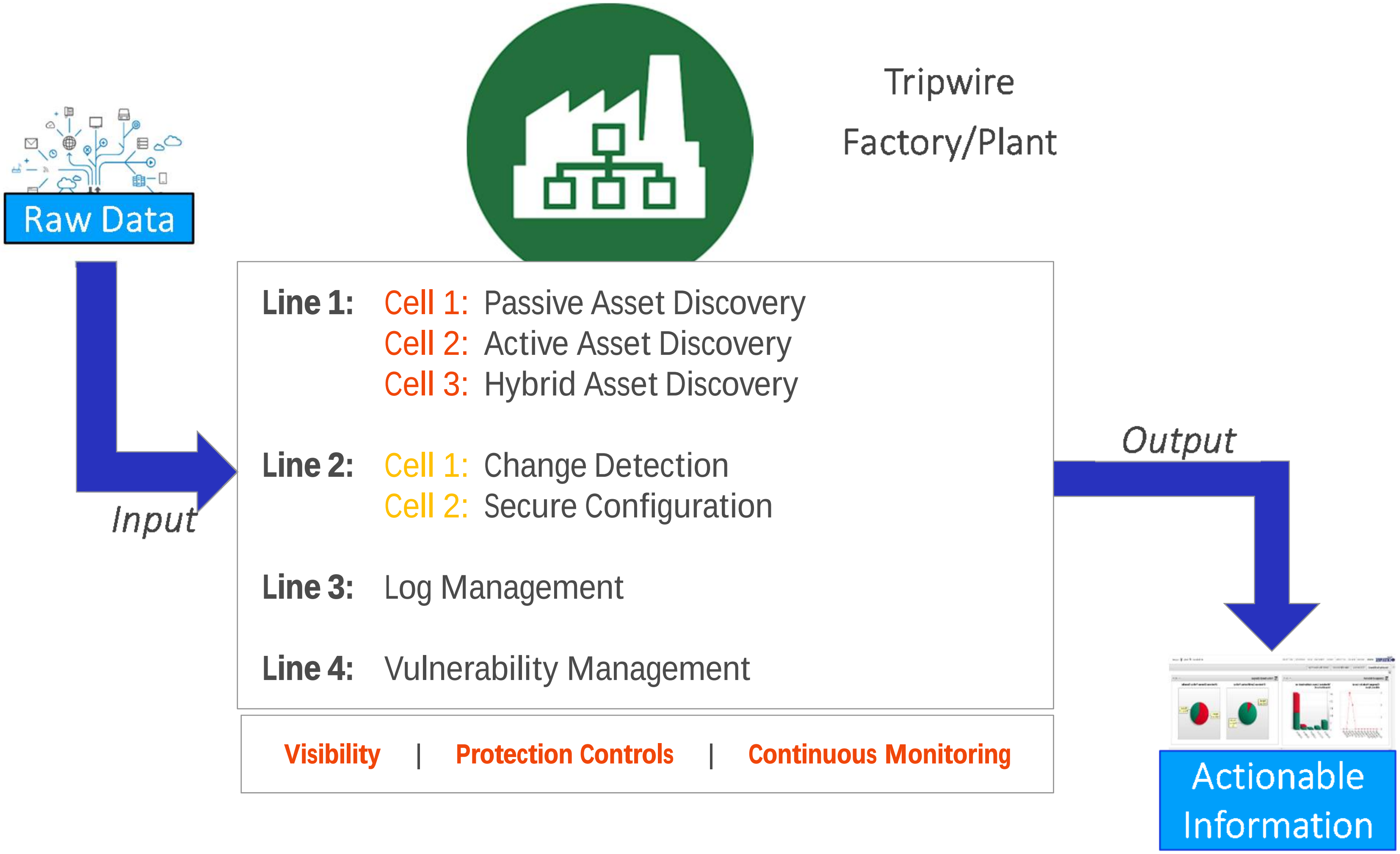
Actionable Results

Host/Device/Endpoint:
Server, workstation, database,
network device, applications,
third party systems,
integrations, etc.



Raw data

Actionable Information



Tripwire
Factory/Plant

Raw Data

Input

Line 1: Cell 1: Passive Asset Discovery
Cell 2: Active Asset Discovery
Cell 3: Hybrid Asset Discovery

Line 2: Cell 1: Change Detection
Cell 2: Secure Configuration

Line 3: Log Management

Line 4: Vulnerability Management

Visibility | **Protection Controls** | **Continuous Monitoring**

Output

Actionable
Information

Extending foundational controls into ICS environment

A layered approach to cyber resiliency

	BELDEN SENDING ALL THE RIGHT SIGNALS	tripwire			
Offering:	Network infrastructure	Log management	Vulnerability assessment	Change detection	Integrity monitoring
Security Level:	Integrated	Passive	Periodic	Continuous	
Capability Details:	• Network access control • Network segmentation • Zones and conduits	• Syslog data collection • Log filtering & management • Investigation analytics & reporting	• Security vulnerability & configuration assessment • Best practice & policy tests	• Real time change detection • Best practice assessment and remediation • Compliance analytics & reporting	
Benefit:	Access prevention	Centralized security data	No touch assessment	Whitelisting	Reduced MTTR

Key Industrial Relationships & Technology Integrations

RUMSEY

ANIXTER

EMERSON

Rockwell Automation
Solution Partner
Control • Process • Information

MDT SOFTWARE
Automation Change Management

ADVANTAGE
Industrial Automation

OVATION

OSI
powering the future

HIRSCHMANN
A BELDEN BRAND

kepware

McNAUGHTON-McKAY
ELECTRIC COMPANY

TOFINO SECURITY
A BELDEN BRAND

YOKOGAWA
Co-innovating tomorrow

monarch

FOXGUARD
SOLUTIONS

INS

GarrettCom
A BELDEN BRAND

Westinghouse

CLAROTY

NovaTech

SIGMAFLOW

MANDIANT
A FireEye Company

The Leader in Industrial Cyber Security Configuration Polices

IEC

IEC 62443

» *Global best practice framework for Industrial Automation and Control Systems Security*

NEI

NEI 08-09

» *Cyber Security Plan for Nuclear Power Reactors*

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST SP 800-82

» *Guide to Industrial Control Systems Security*

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

» *NERC Critical Infrastructure Protection*

- ***Many others, such as:***

ISO 27001

American Water Works Association

PCN Security Guidance

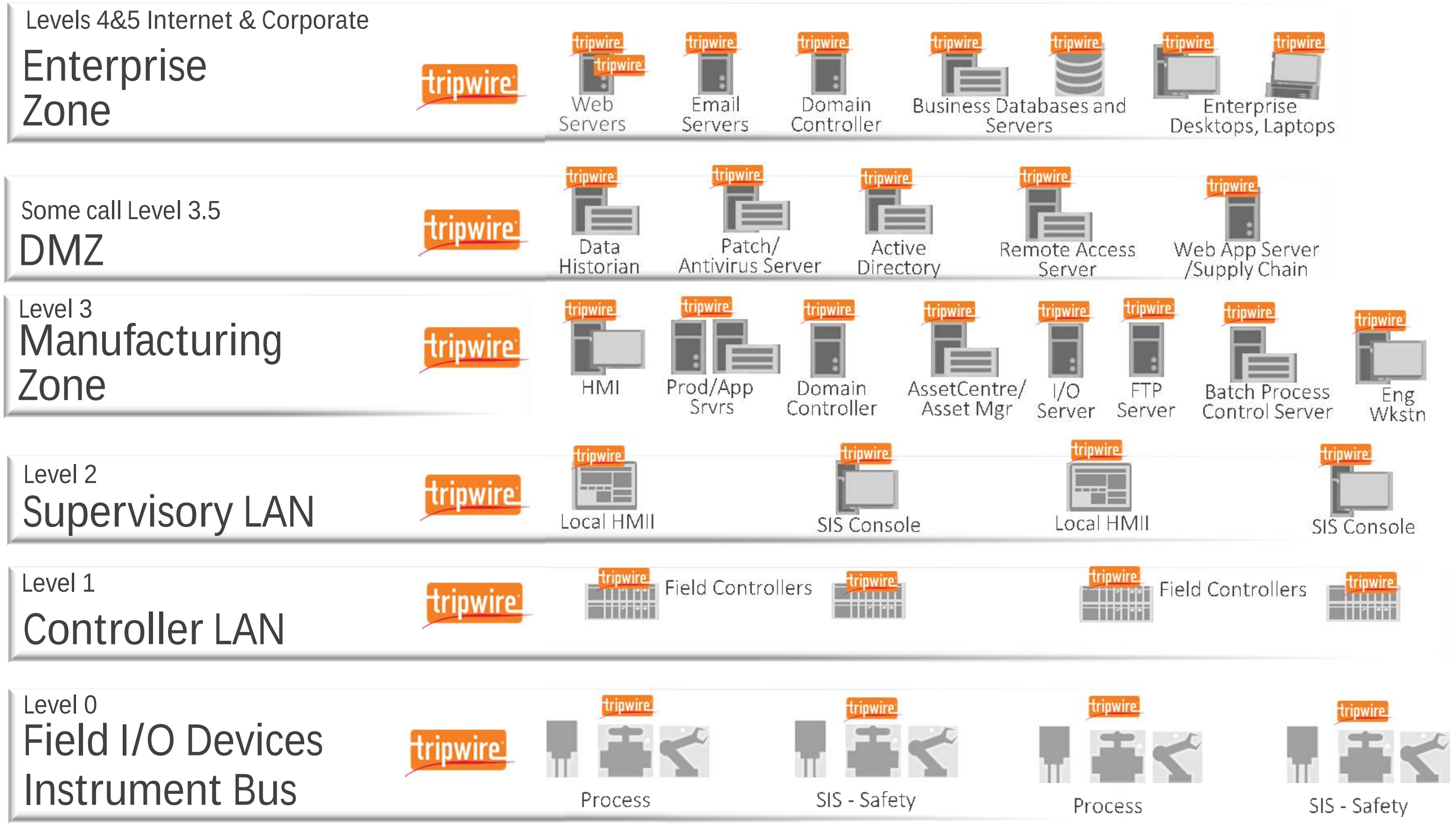
- ***Guide for Water Sector***

Tripwire Industrial Solutions

Level 5

to

Level 0



Levels 4&5 Internet & Corporate
Enterprise Zone
tripwire
Web Servers
Email Servers
Domain Controller
Business Databases and Servers
Enterprise Desktops, Laptops

Some call Level 3.5
DMZ
tripwire
Data Historian
Patch/ Antivirus Server
Active Directory
Remote Access Server
Web App Server /Supply Chain

Level 3
Manufacturing Zone
tripwire
HMI
Prod/App Srvrs
Domain Controller
AssetCentre/ Asset Mgr
I/O Server
FTP Server
Batch Process Control Server
Eng Wkstn

Level 2
Supervisory LAN
tripwire
Local HMII
SIS Console
Local HMII
SIS Console

Level 1
Controller LAN
tripwire
Field Controllers
Field Controllers

Level 0
Field I/O Devices Instrument Bus
tripwire
Process
SIS - Safety
Process
SIS - Safety

Case study: FedEx®

Pain point

Increasing e-commerce shipments—9M shipments/payments/day coupled with PCI compliance requirements

Answer

Tripwire Enterprise

Benefit

The breadth and depth of our file integrity monitoring capabilities helped FedEx better monitor and manage threats on their payment transactions

Case study:

Dominion

Pain point

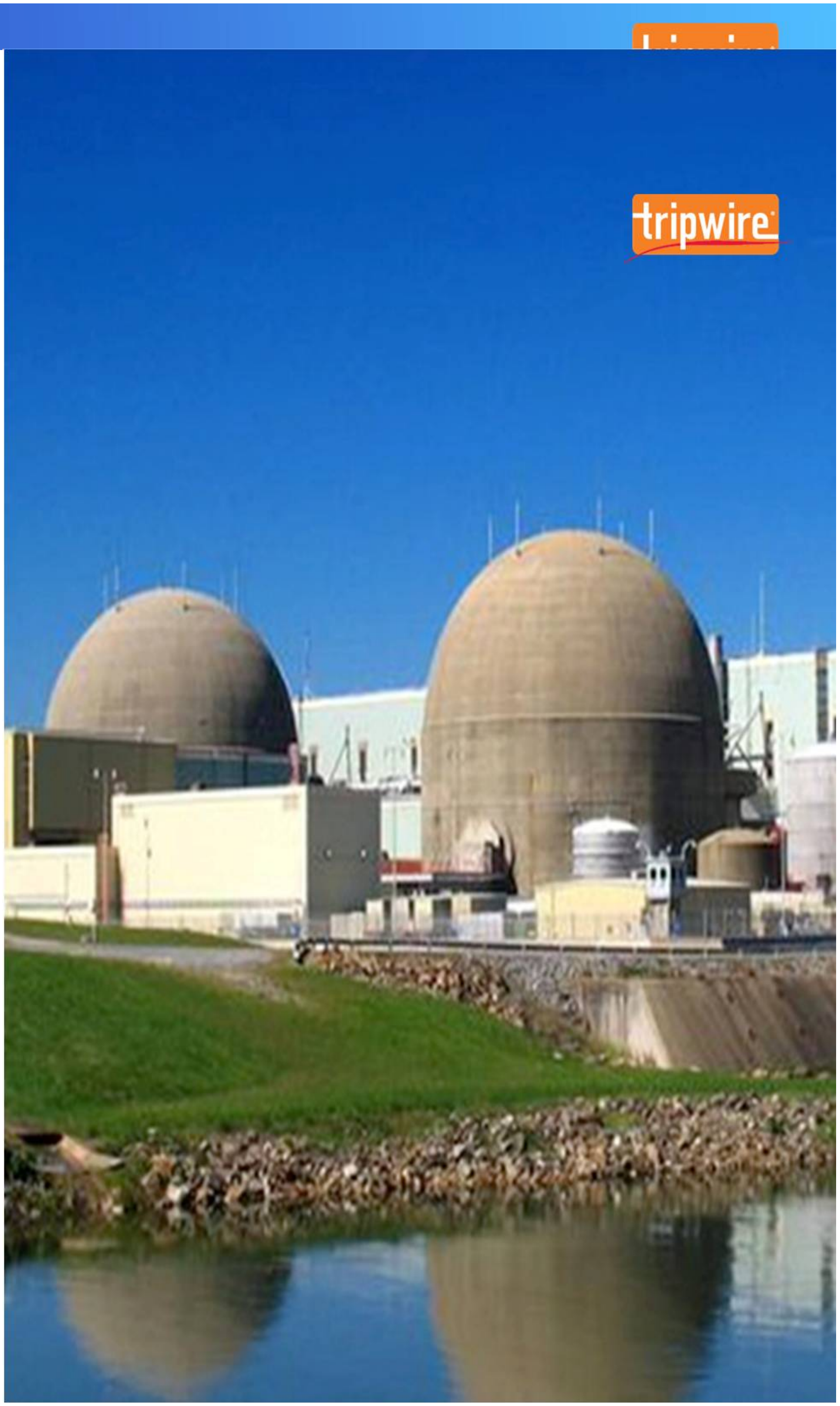
NERC compliance for their corporate environment, including a nuclear plant

Answer

Tripwire Enterprise and Tripwire IP360—including 20,000+ IPs

Benefit

Granular risk scoring enabled Dominion
to better track and measure security risks—
and address them more effectively



Case study: The Electric Company El Paso Electric

Pain point

Needed a solution to protect its entire attack surface, while simultaneously streamlining its NERC CIP compliance processes

Answer

Tripwire Enterprise and
Tripwire Professional Services

Benefit

Increased speed of detection, remediation and return to normal operations, automated multiple NERC CIP compliance processes, and enhanced alert accuracy and reduced overall complexity

Case study:

KISSIMMEE UTILITY AUTHORITY

Pain point

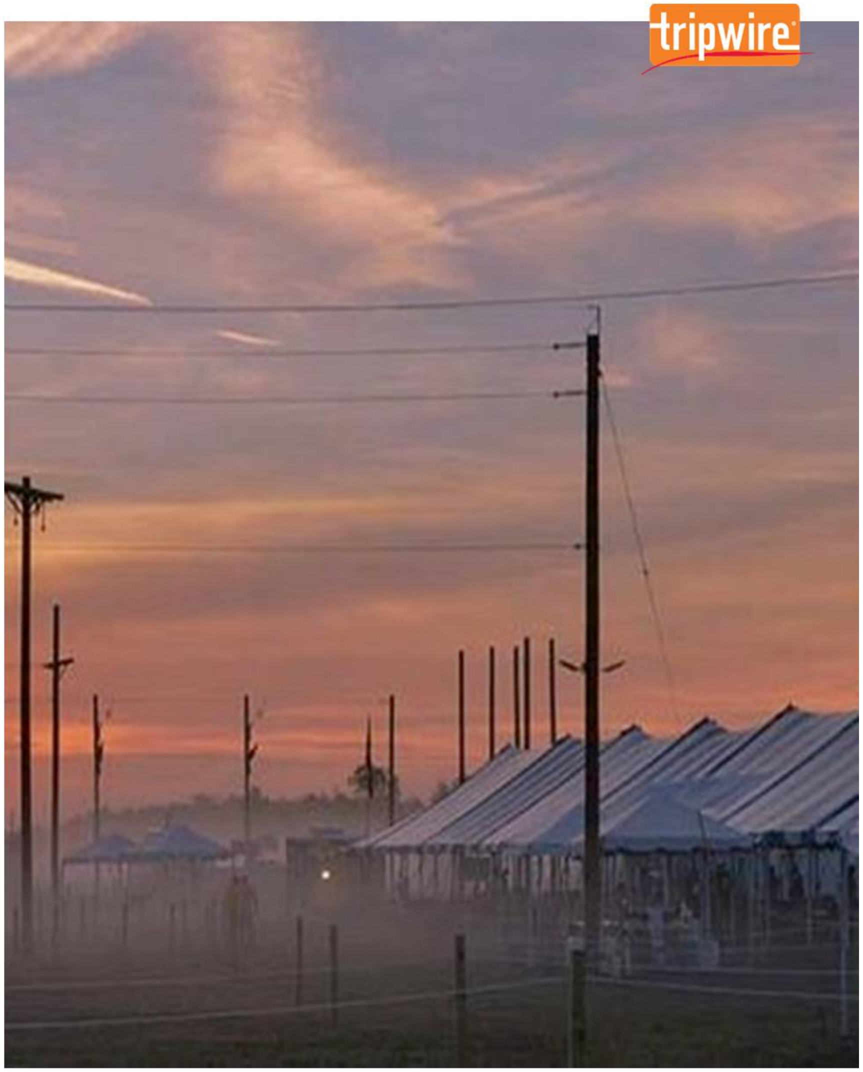
Wanted greater visibility into the IT environment for compliance with regulations

Answer

Tripwire Configuration Compliance Manager

Benefit

Gained a clear picture of system configurations and the compliance impact of configuration changes



Case study:

VERVE INDUSTRIAL PROTECTION

Pain point

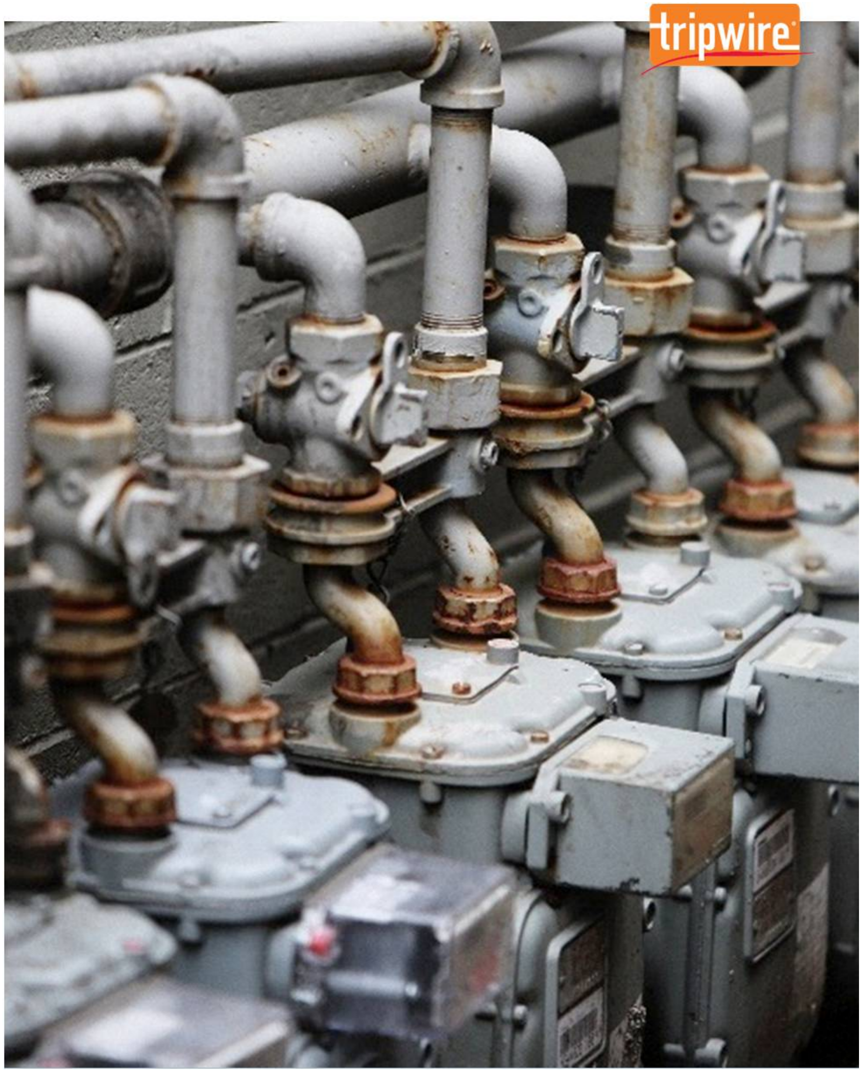
Develop a cybersecurity solution tailored to protect power generation that accommodates highly diverse legacy infrastructure components (including embedded and fragile endpoint devices) without requiring replacement of existing control system elements

Answer

Tripwire Enterprise

Benefit

Attained unprecedented visibility across the entire asset portfolio utilizing integrated dashboards for security and compliance, and obtained competitive differentiation by using best-in-class components



9,000 Customers Rely on Tripwire

50% of the Fortune 500

Financial Services & Insurance

First Gulf Bank
AVIVA
FannieMae.
MetaBank
Allstate
KeyBank
CIBC
ICBC
MEPCO
BAIDURI BANK
Capital One
KEMI
Resurance
OneWest Bank
IXE
ahlibank
AMALGAMATED BANK
InterBank
ahli united bank
QNB
HSBC
ANZ
BlueShield

Healthcare & Pharmaceuticals

INTEGRIS Health
Mylan
Aurora Health Care
BAYLOR
Tenet
UnitedHealthcare
KU Medical Center
Univita
Boston Medical
John Muir Health
Saint Luke's Health System
CMS
HealthPartners
Medtronic
Health Sciences Center
Hollister
American Psychological Association
emdeon
Oklahoma Heart Hospital
Roche
Alere
Otsuka
The University of Kansas Hospital
availity

Energy & Utilities

PSE Puget Sound Energy
Safaricom
ERCOT
PG&E
Duke Energy
APS
pjm
verizon wireless
elpaso
BC hydro
LCRA
Shell
SPP Southwest Power Pool
ONCOR
swisscom
GE
STC
SRP
Portland General Electric
aeso
noble energy
Dominion
IDAHO POWER
vodafone
KCP&L
Chevron
Batelco

Government

USDA
DCSA
GSA
CMS
DHCS
Saudi Post
Herefordshire Council
IRS
CERT
FEMA
USAID
City of Phoenix
City of London
U.S. Army
Ottawa

Media & Leisure

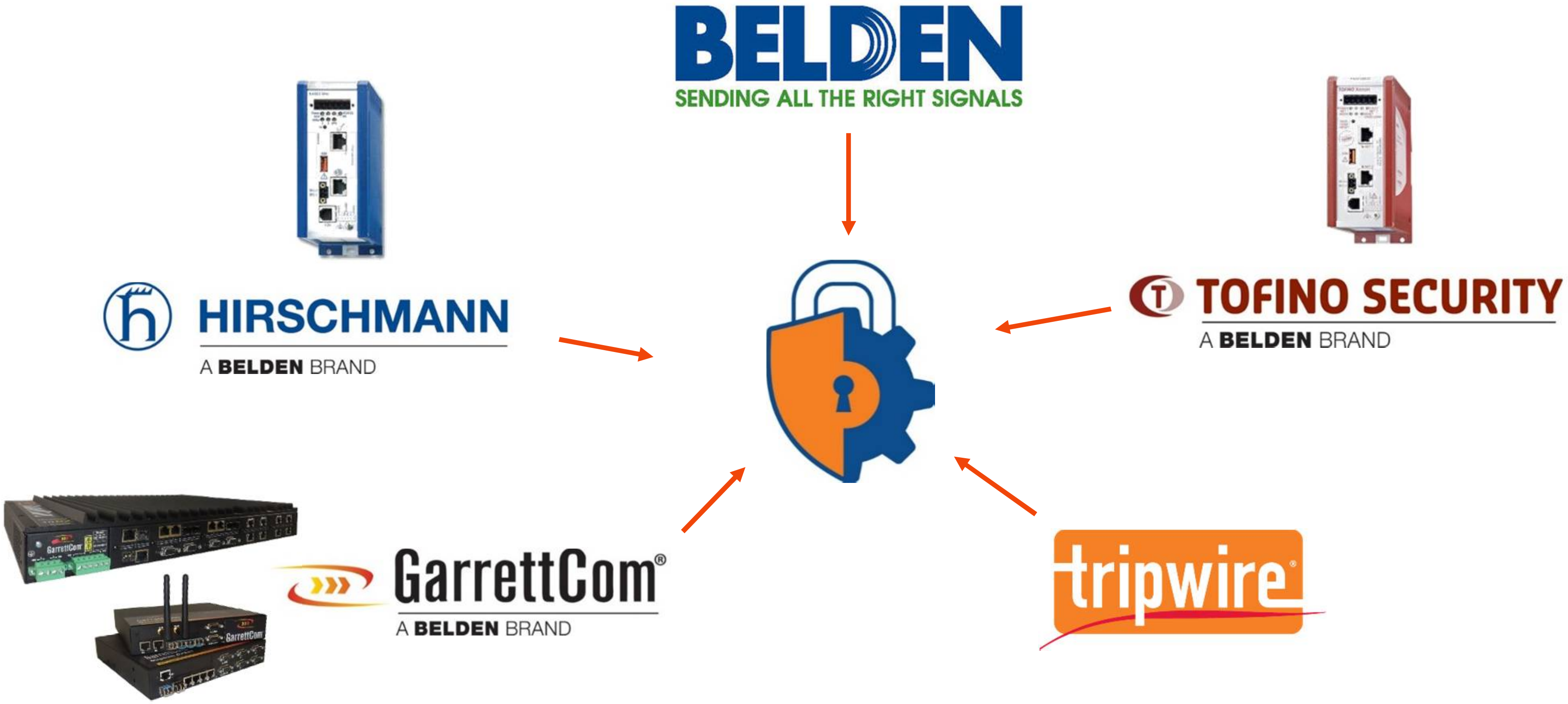
bwin
ACCOR
American Museum of Natural History
FANDANGO
Expedia.com
OLSON
denali
REGAL ENTERTAINMENT GROUP
facebook
comcast
SiriusXM
BOOKING.COM
PayPal
JWT
redbox.
SONY
zipcar
WYNDHAM HOTEL GROUP
Donaldson.
Jumeirah
Corus Entertainment
CARNIVAL CORPORATION & PLC
amc ENTERTAINMENT
DNC

Retail & Consumer Goods

hp
GENERAL MILLS
Armstrong
WHOLE FOODS MARKET
Kellogg's
Jean Coutu
FUJITSU
ABC Supply Co. Inc.
afni
Quiznos
HOWDENS
ADM
Starbucks Coffee
Liverpool
SIGNET JEWELERS
COSTCO WHOLESALE
Reitmans
The BRICK
DISCOUNT TIRE
TOYOTA
KOHLER
Walmart.com
KIRKLAND'S
REGIS CORPORATION
RadioShack
DELHAIZE GROUP
Payless
coles

Belden Industrial Cybersecurity

Hardware and Software Solutions for Complete Cybersecurity Coverage



BELDEN

SENDING ALL THE RIGHT SIGNALS

Belden.com | @BeldenInc