IoT Cybersecurity in a Connected World

June 2017

Sylvain Denoncourt GSEC, CISSP
IoT network architecture consultant
Cisco

Cybersecurity. “cyber”

… from the FBI’s standpoint. “**Cyber** is just another way by which malicious or bad people try to do bad things,”

Current threats come from five main areas, the most serious of which is the “big four” nation states (Russia, China, Iran and North Korea), followed by multinational criminal syndicates, insider threat (both intentional and unintentional), hacktivists and terrorists, who might currently lack the ability or capability to hack.

Source: SDM

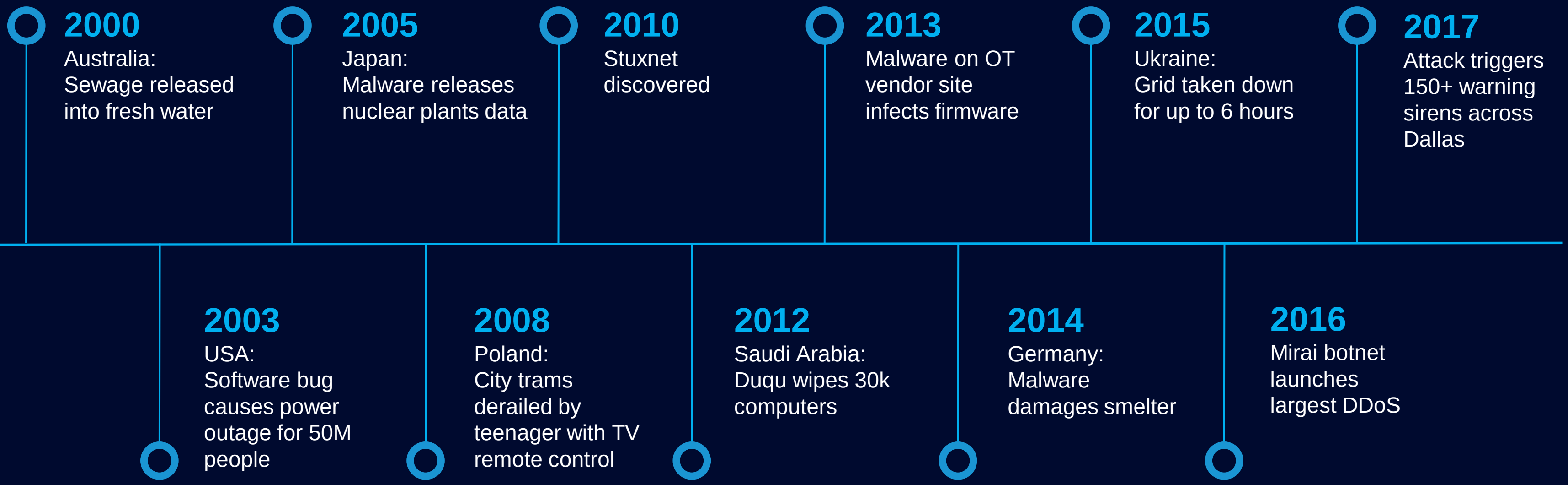
***Computer networks controlling the buildings and infrastructure architects design are regularly being hacked*.**

This tends to go under-reported, because it often involves private companies concerned for their public images, and untreated, because these systems are coordinated by various parties that have never been responsible for cyber security.

Source Architizer :

https://architizer.com/blog/hacking-architecture/

Escalating Attacks in IoT Domain



2000
Australia:
Sewage released into fresh water

2003
USA:
Software bug causes power outage for 50M people

2005
Japan:
Malware releases nuclear plants data

2008
Poland:
City trams derailed by teenager with TV remote control

2010
Stuxnet discovered

2012
Saudi Arabia:
Duqu wipes 30k computers

2013
Malware on OT vendor site infects firmware

2014
Germany:
Malware damages smelter

2015
Ukraine:
Grid taken down for up to 6 hours

2016
Mirai botnet launches largest DDoS

2017
Attack triggers 150+ warning sirens across Dallas

Source:

[1] Cyberattacks against critical manufacturers nearly doubled in 2015: Government report - The Washington Times in Jan 2016

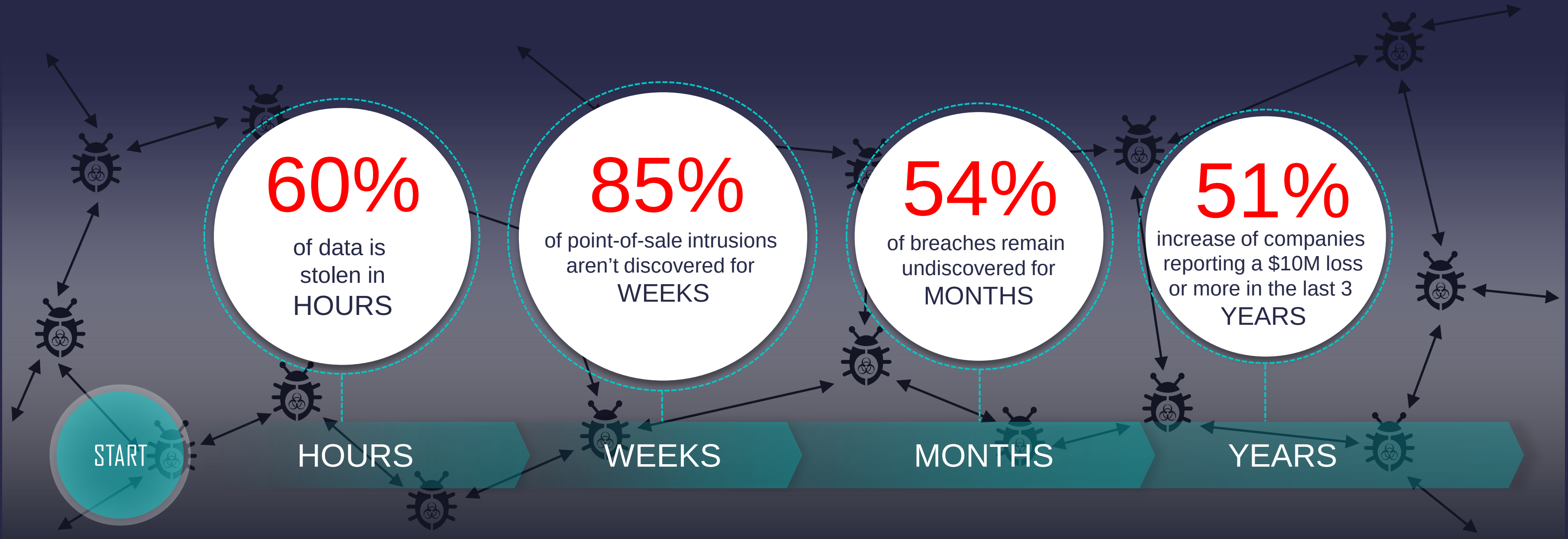
[1]"The FBI estimated that $400 billion of intellectual property is leaving the US each year because of cyberattacks" - Dark Reading 2016

Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation



60% of data is stolen in HOURS

85% of point-of-sale intrusions aren’t discovered for WEEKS

54% of breaches remain undiscovered for MONTHS

51% increase of companies reporting a $10M loss or more in the last 3 YEARS

START

HOURS

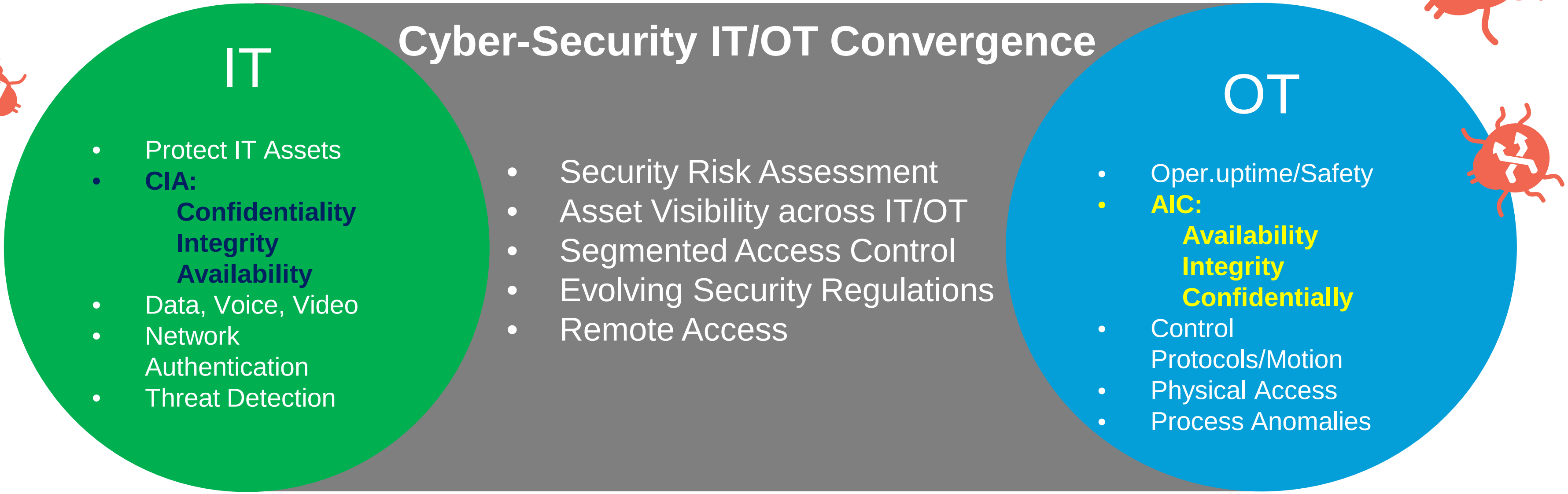
WEEKS

MONTHS

YEARS

Convergence of IT and OT

Information Technology vs Operation Technology



Cyber-Security IT/OT Convergence

IT

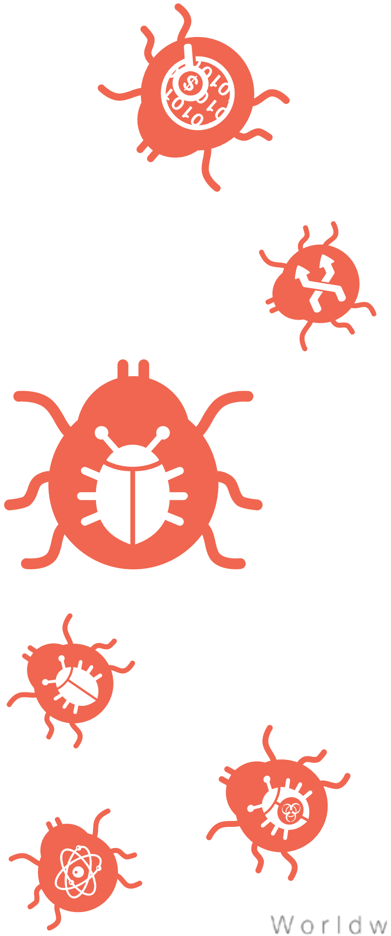
- Protect IT Assets
- **CIA:**
  Confidentiality
  Integrity
  Availability
- Data, Voice, Video
- Network Authentication
- Threat Detection

- Security Risk Assessment
- Asset Visibility across IT/OT
- Segmented Access Control
- Evolving Security Regulations
- Remote Access

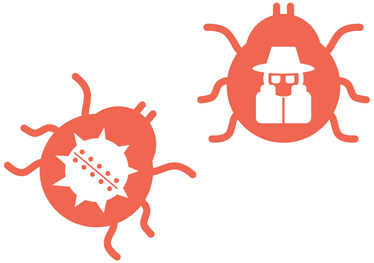
OT

- Oper.uptime/Safety
- **AIC:**
  Availability
  Integrity
  Confidentially
- Control Protocols/Motion
- Physical Access
- Process Anomalies

IOT Systems as Attack Surface



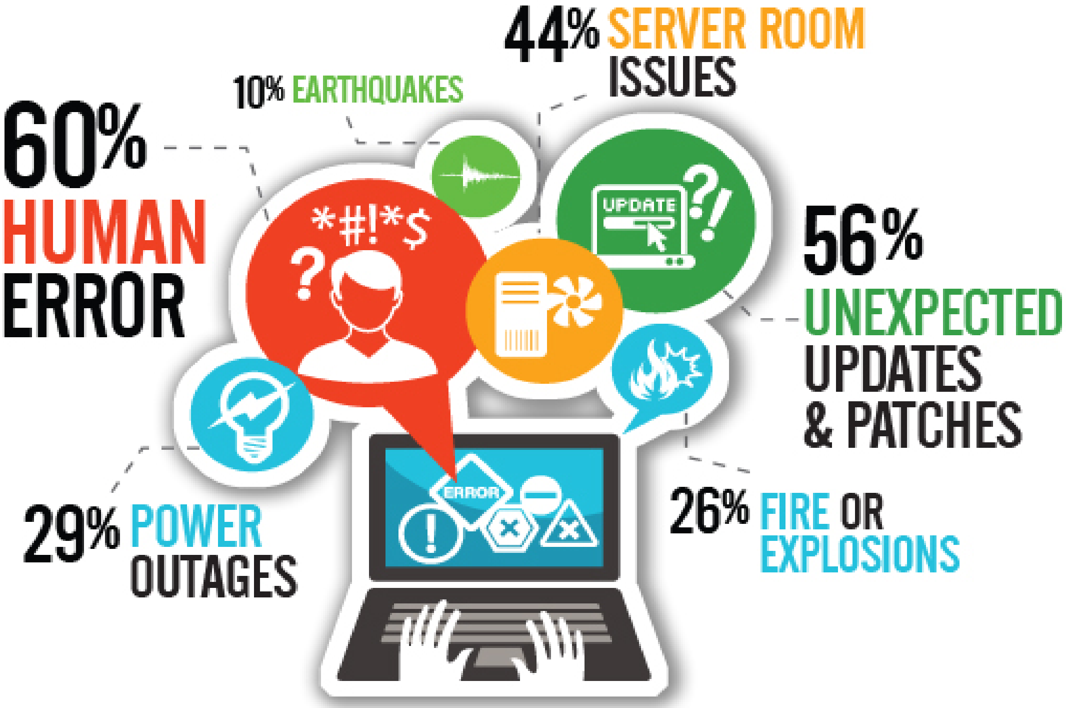
IoT devices and control systems are vulnerable



IOT Systems as Attack Surface

Customer IoT Security Concerns

Challenges are not always malicious



IoT Systems as Attack Surface

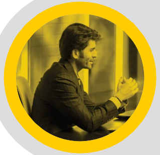
Vulnerabilities found in industrial systems rose 2400% from 2009 to 2015

Automation vendors still ship application updates on EOL Windows platforms

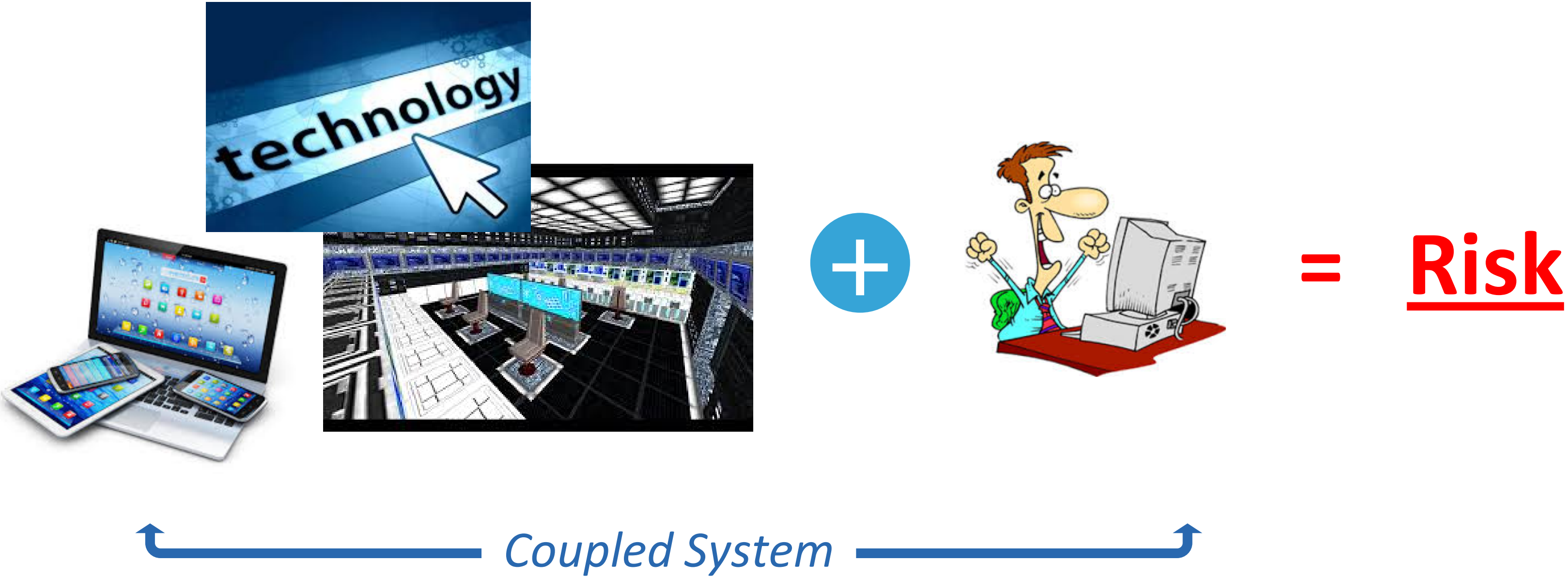
The most common Ethernet/IP based OT protocol lacked authentication till Fall of 2015

Yet Ethernet/IP in manufacturing grew 96% the three years before

Securing IT and OT Risks

	**HUMAN RESOURCES OPENING E-MAIL FROM APPLICANT**	Opening E-mail
	SALESMAN RESEARCHING NEW PRODUCTS	Outbound web access
	VIDEO SURVEILLANCE CAMERAS	IoT devices sending Alerts and Telemetry
	ENGINEER CONFIGURING OT SERVICE PROFILES REMOTELY	Accessing PLC Programmer

The human element is usually the path of least resistance



+

= **Risk**

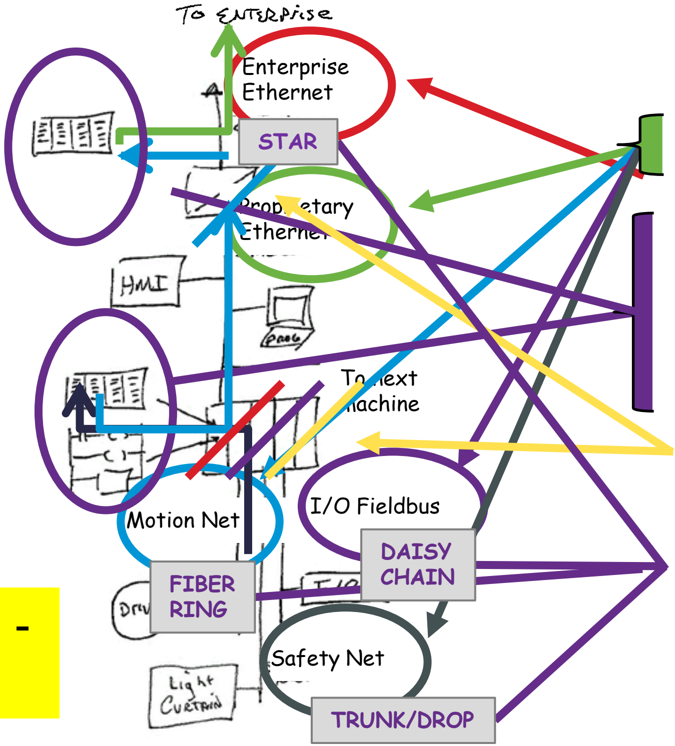
Coupled System

Network Design Concerns…

- A bad network design is as big a threat to security success as the lack of security.

- Better to know what you are missing than to think you are safe.

This does not mean that there was no architecture - It is likely that the architecture eroded over time.



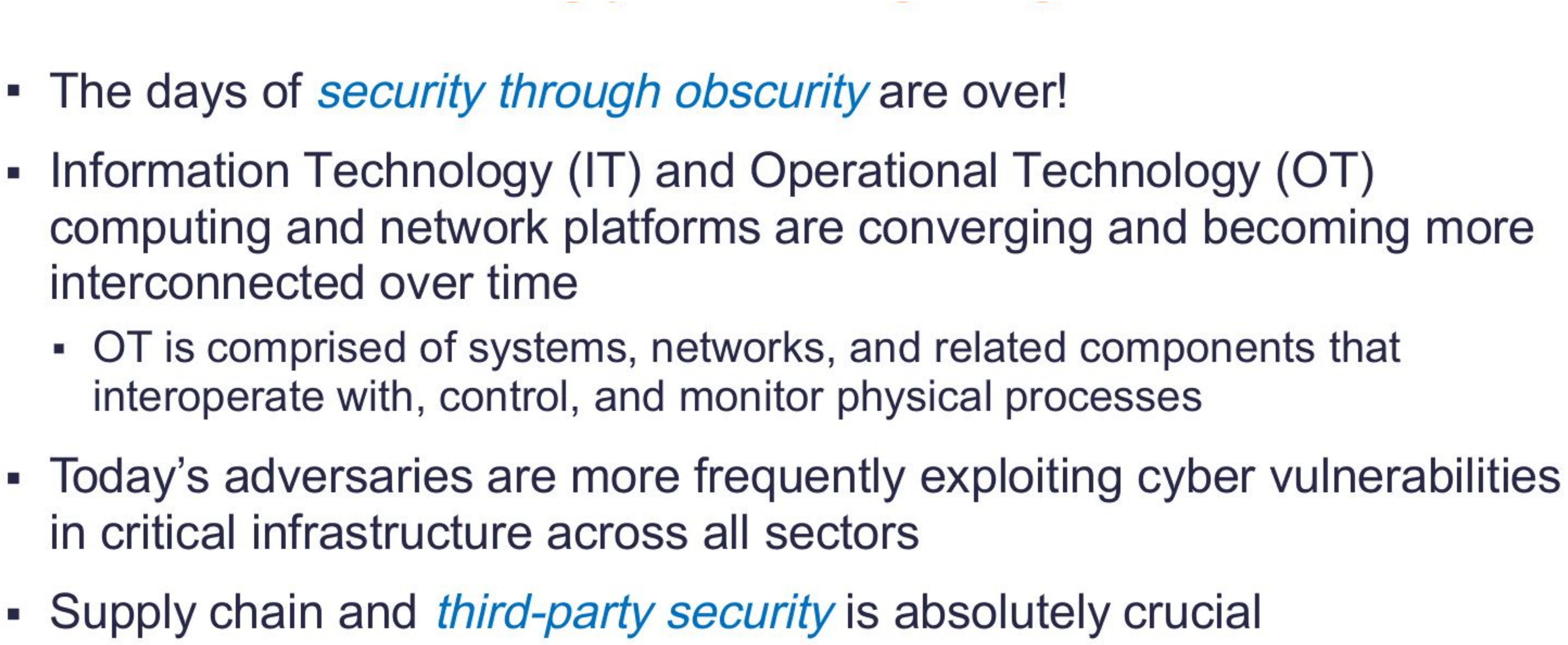
Adversary Capabilities are Rapidly Advancing

- Threat actors are *highly capable* and *very adaptable*
- Adversaries are extremely patient and willing to invest time and large sums of money to exploit their targets
- The expertise needed to exploit utility OT is no longer a “barrier to entry”
  - Specialized knowledge of control system and utility operations is moderate, i.e. vast information is freely and readily available
  - Exploits are sophisticated and becoming highly automated
- Traditional defensive measures are becoming *inadequate*

Common Pathways into OT Environments

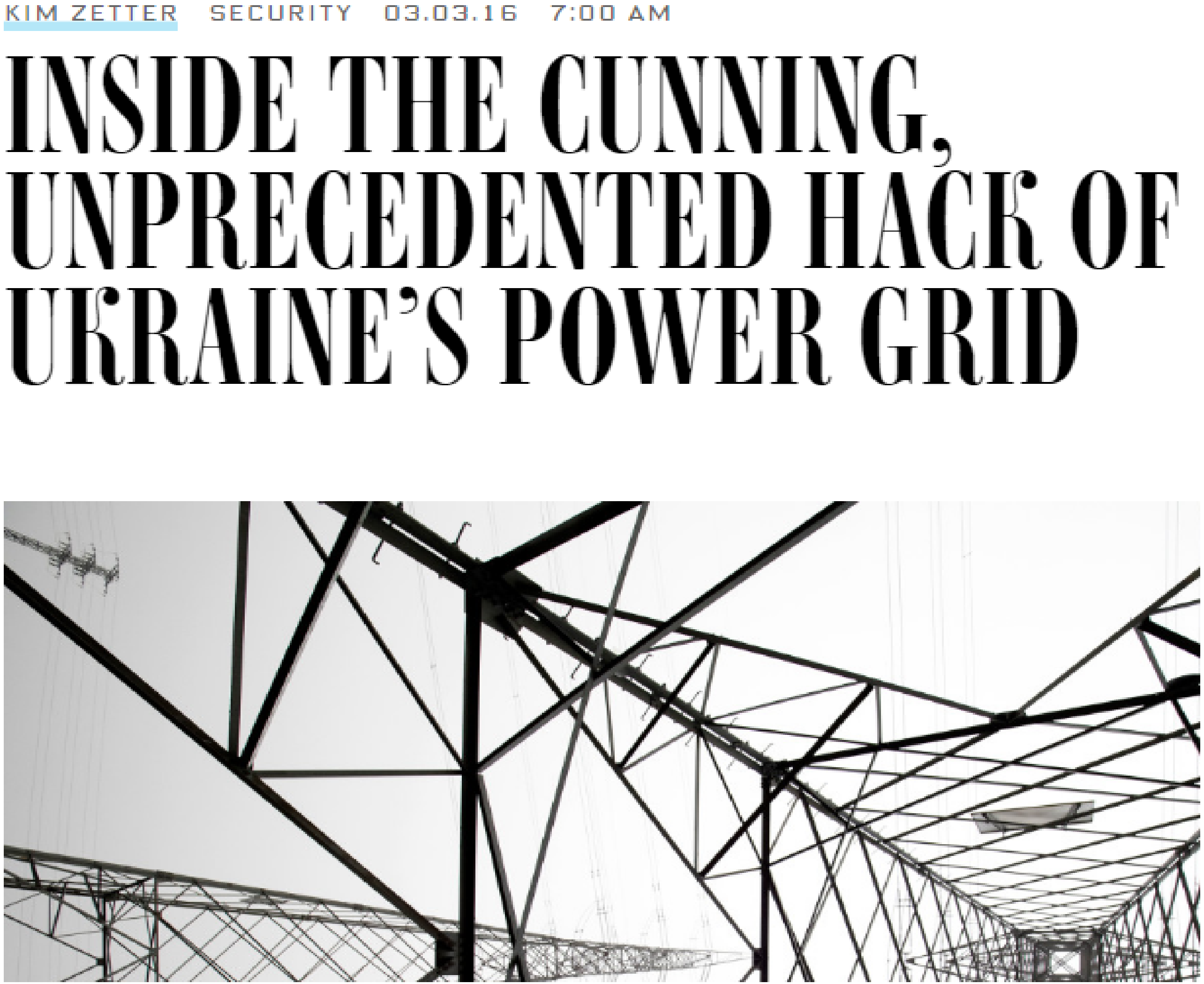
- Portable *media* such as USB drives and flash cards
- Laptops and other *portable computing devices* that have network interfaces and are capable of storing data
  - Stuxnet initially spread globally via infected *laptops* and *media*
- Trusted *third-party* vendor software installation and updates
- Network and dial-up *remote access* including VPN
- Inadequate network segmentation
- Poor system and device *password* or *authentication* practices

Organizations are increasingly Becoming Targets



- The days of *security through obscurity* are over!
- Information Technology (IT) and Operational Technology (OT) computing and network platforms are converging and becoming more interconnected over time
  - OT is comprised of systems, networks, and related components that interoperate with, control, and monitor physical processes
- Today's adversaries are more frequently exploiting cyber vulnerabilities in critical infrastructure across all sectors
- Supply chain and *third-party security* is absolutely crucial

Cybersecurity attacks



KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

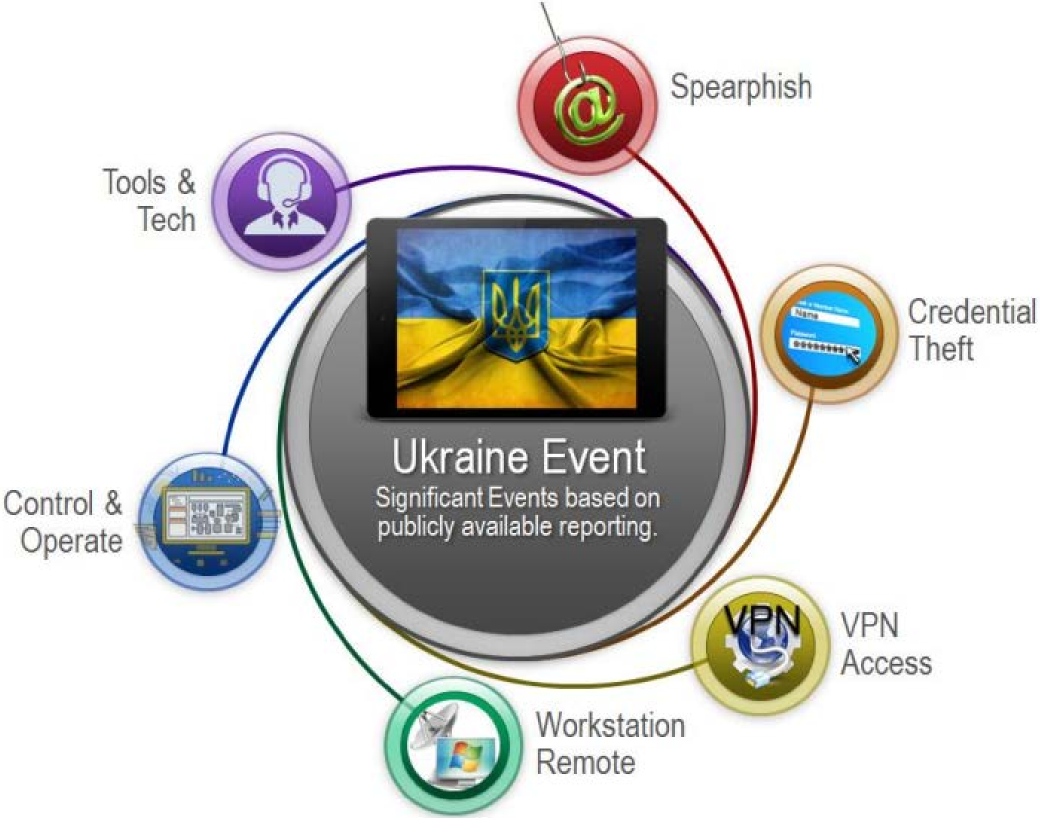
Impact in Ukraine 2015:

Aftermath of the Attack

1.8 M people
2-3 days of
lost power

Ukraine Utility Attack – Anatomy of an attack

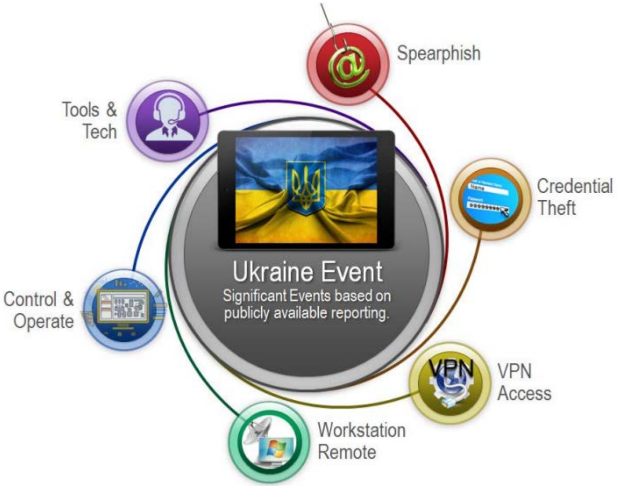
- Spear Fishing into IT
- BlackEnergy Malware Placed
- Credential Theft for Access
- VPN access from outside
- Remote management tools
- Firmware update / corruption
- UPS system disabled
- KillDisk anti-forensics wipe
- Telephone DDOS

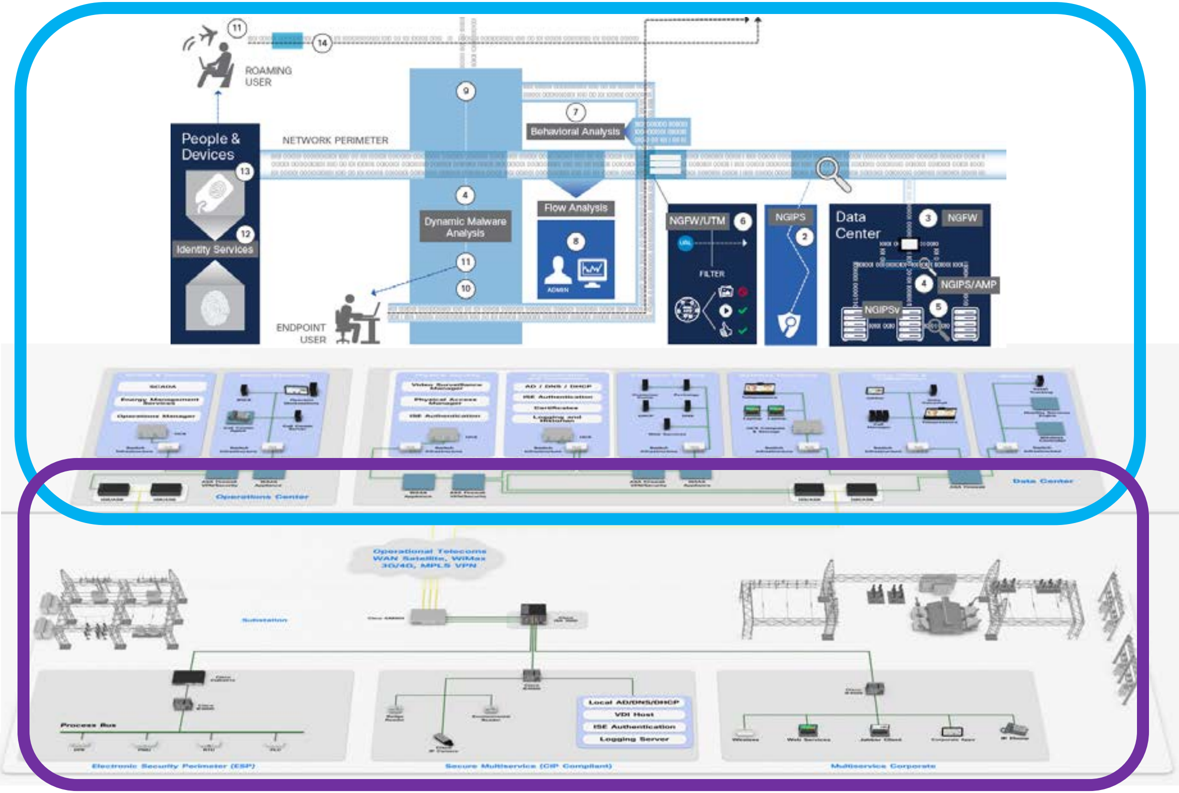


Kill Chain – ICS Variant

1

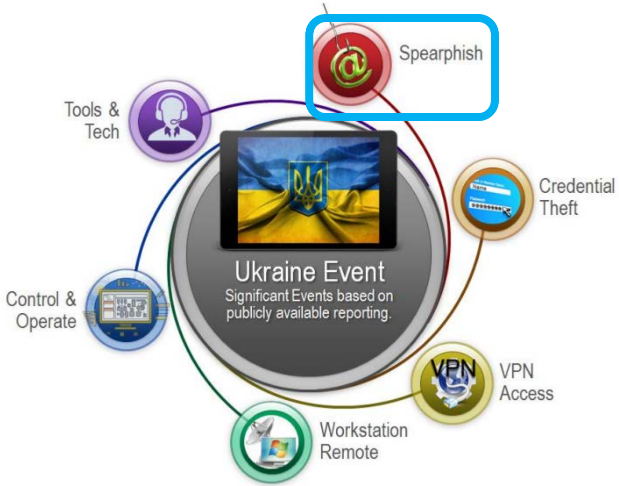
- Attacks start on IT side
- Work their way to OT

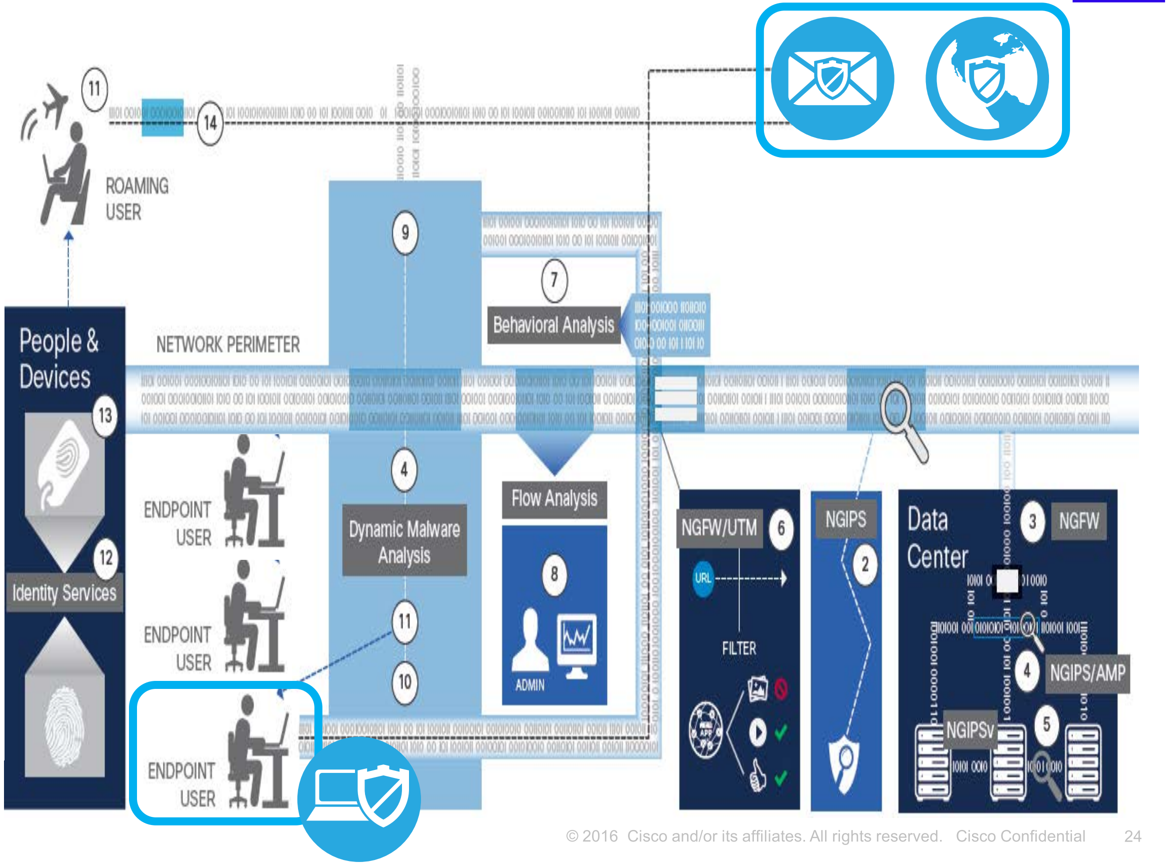




Initial Entry: Reconnaissance / Targeting

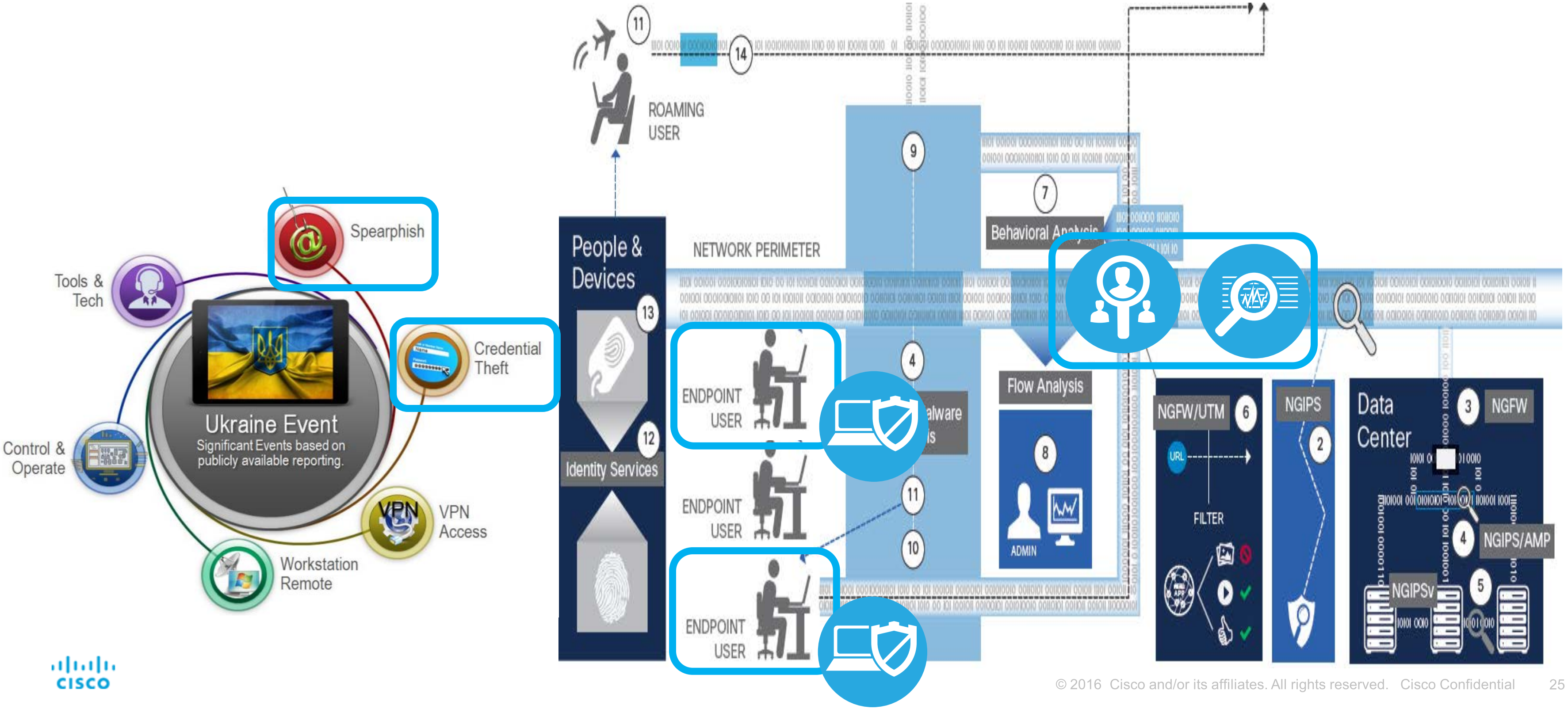
2





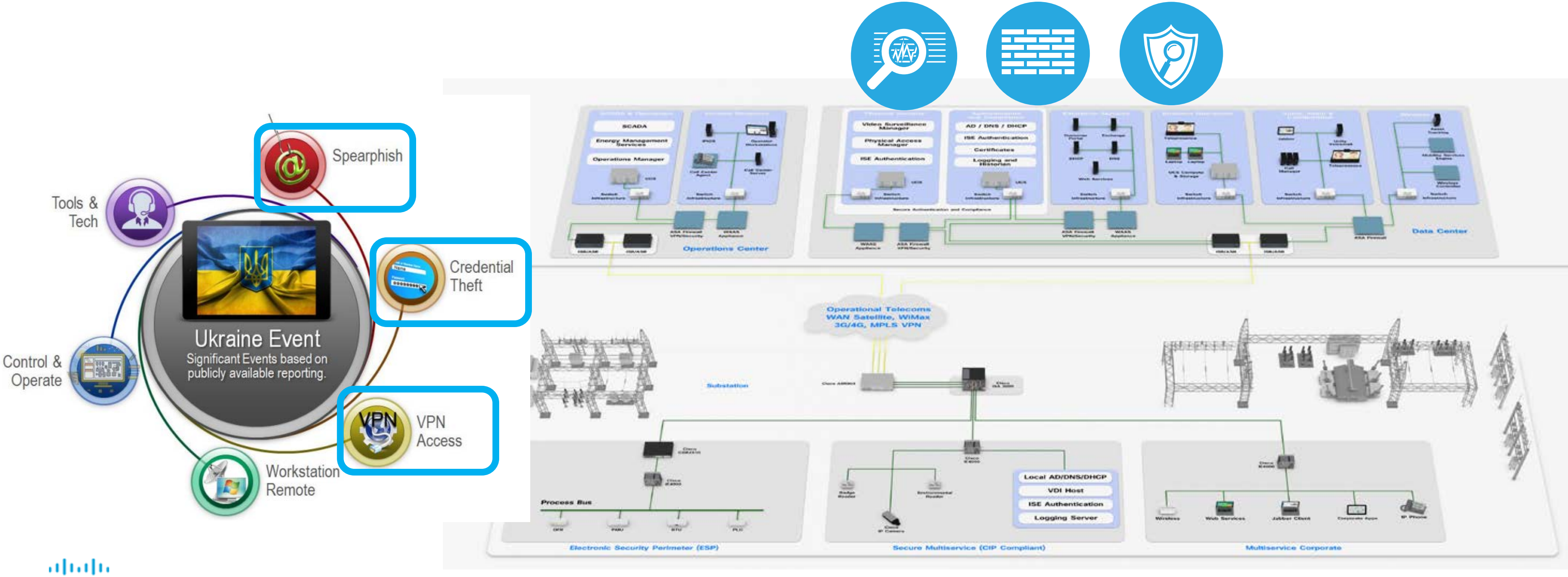
Traversal: Credential Theft

3



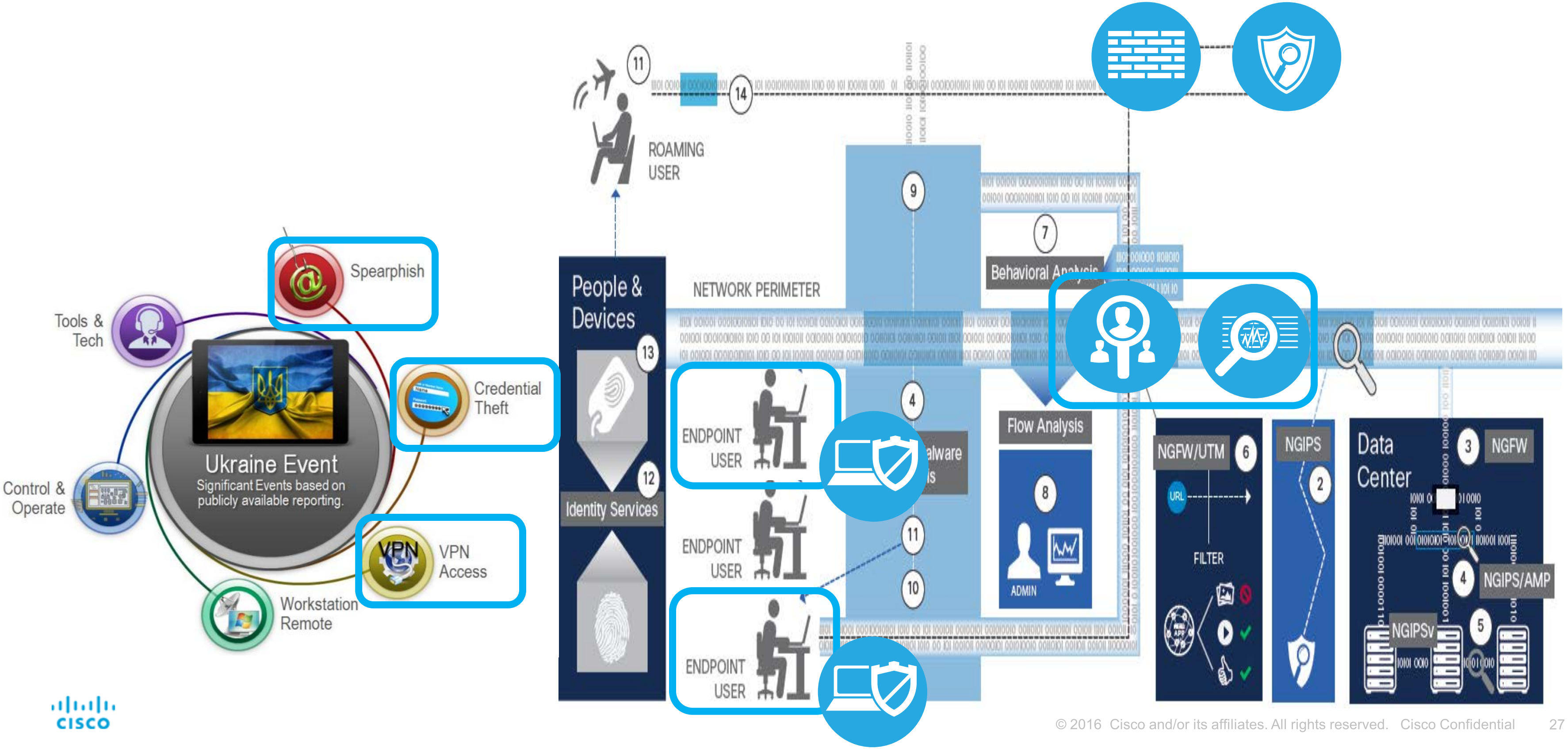
Command and Control: VPN Access (OT)

4



Command and Control: VPN Access (IT)

5

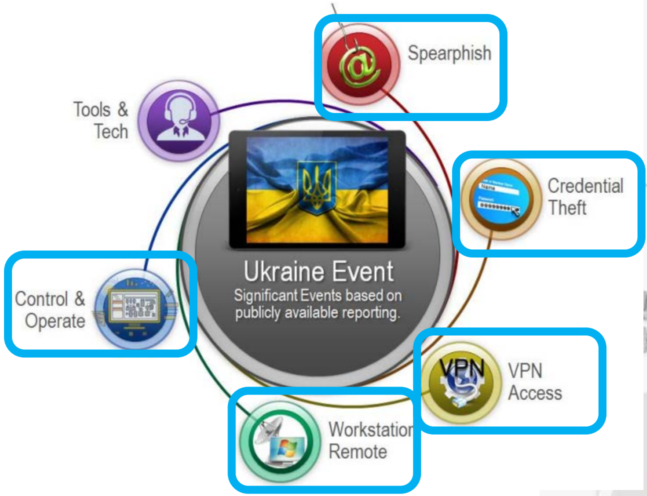


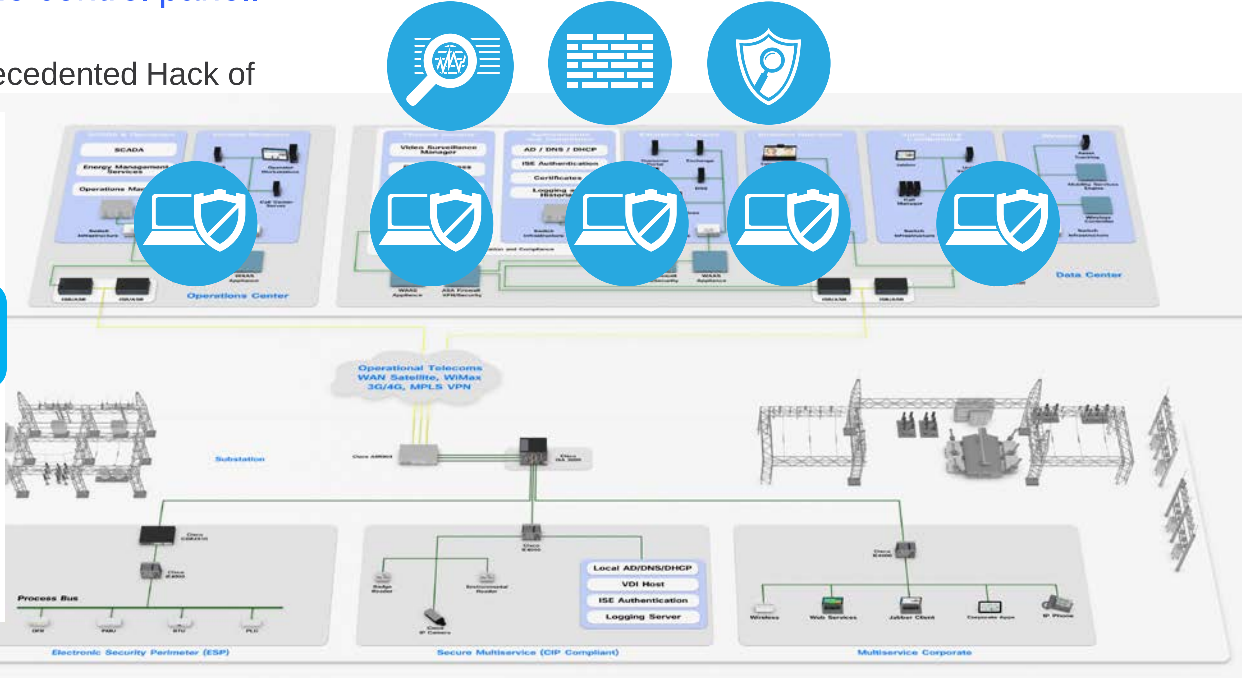
Attack: Remote Desktop / Control

6

"The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel."

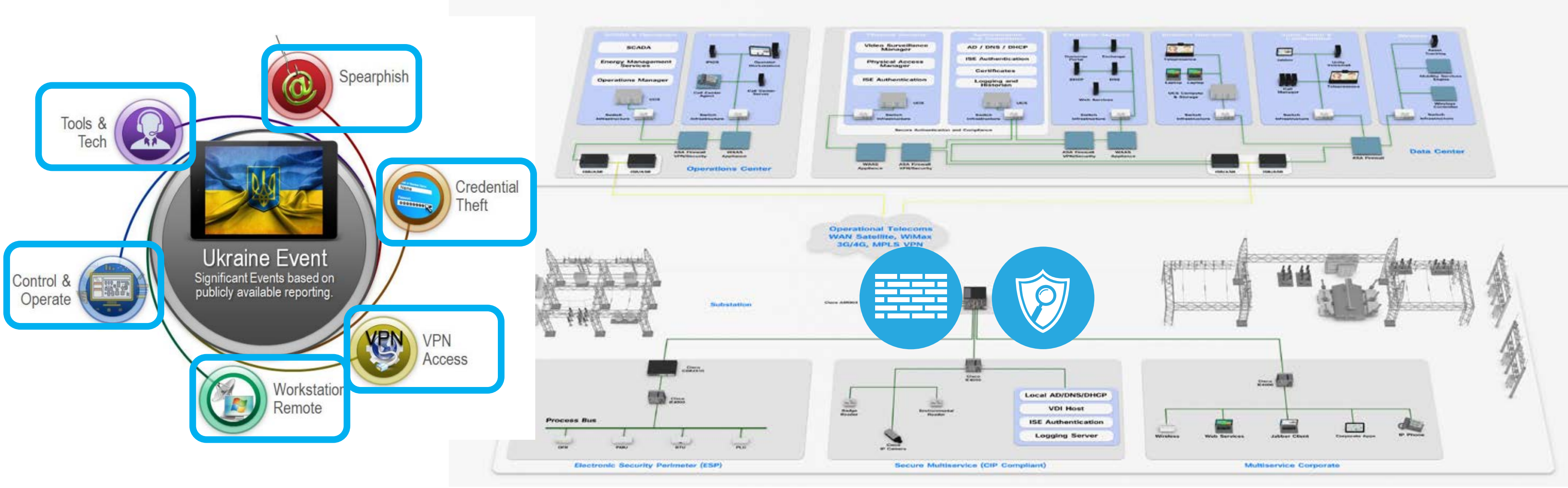
Wired Magazine – Inside The Cunning Unprecedented Hack of Ukraine's Power Grid



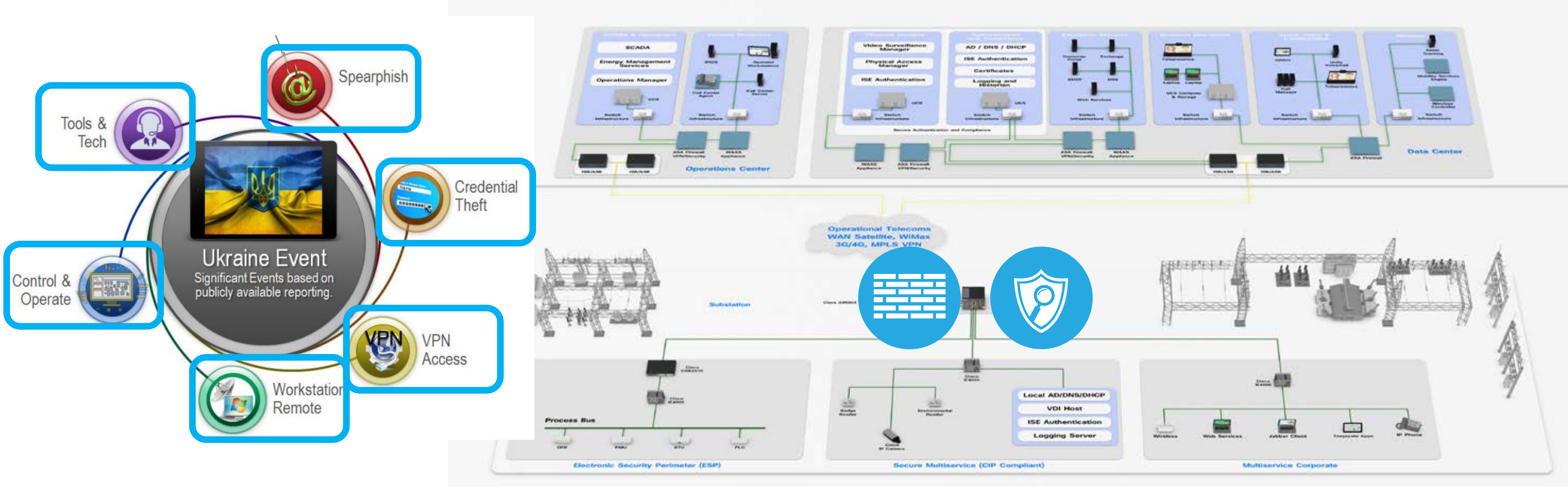

SCADA
Energy Management Services
Operations Center
Video Surveillance Manager
AD / DNS / DHCP
ISE Authentication
Certificates
Data Center
Operational Telecoms WAN Satellite, WiMax 3G/4G, MPLS VPN
Substation
Local AD/DNS/DHCP
VDI Host
ISE Authentication
Logging Server
Process Bus
Electronic Security Perimeter (ESP)
Secure Multiservice (CIP Compliant)
Multiservice Corporate

ICS Specific Attack: UPS Shutdown

7

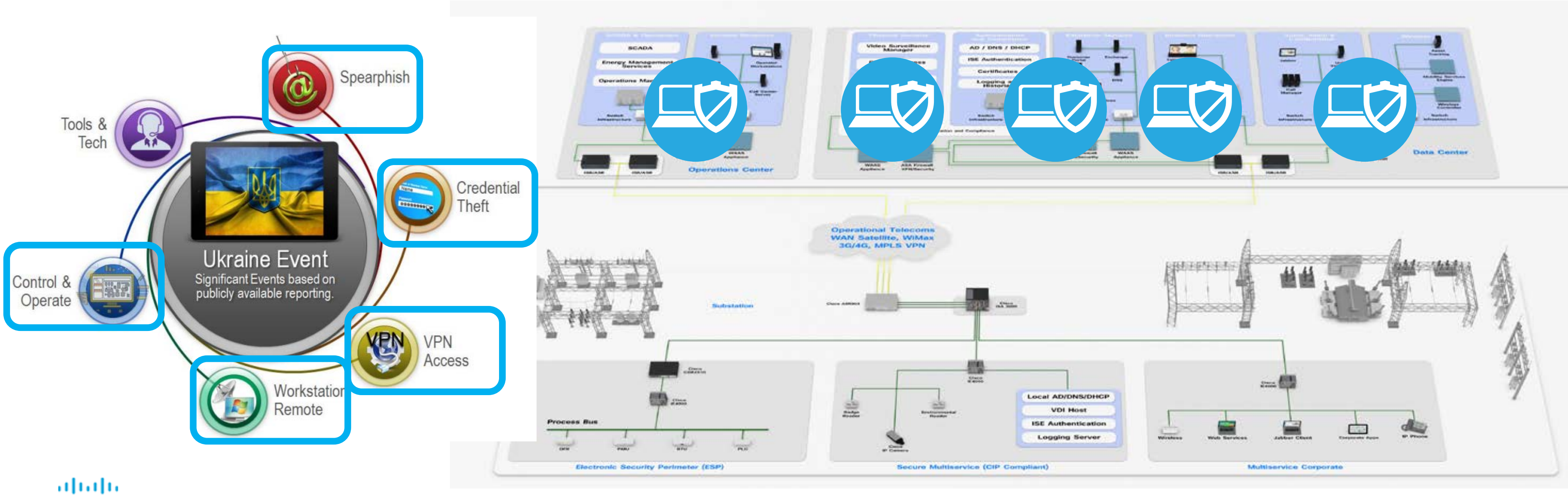


ICS Specific Attack: Bad Firmware Upgrade 8

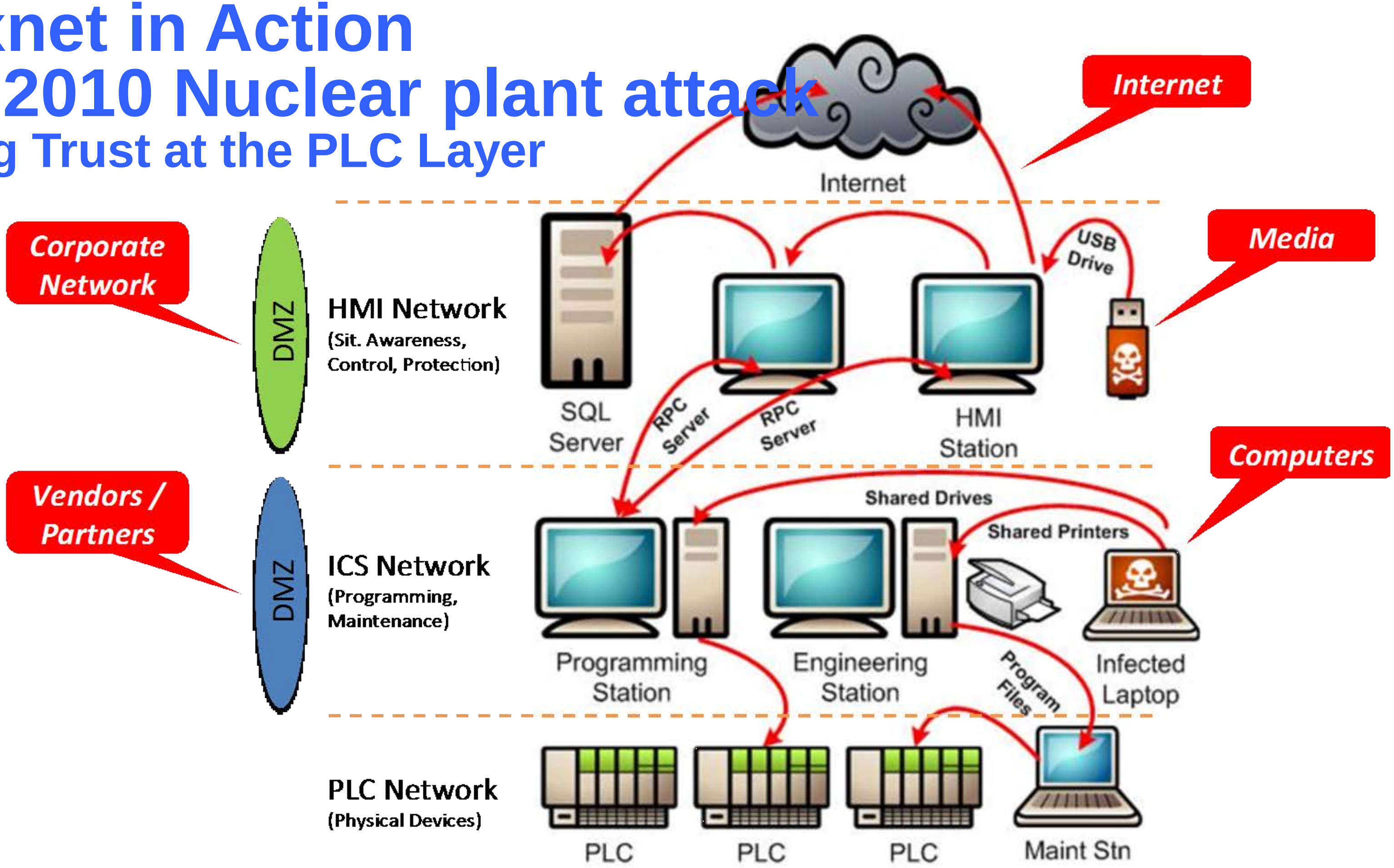


Attack: Anti-Forensics – Wiper Software

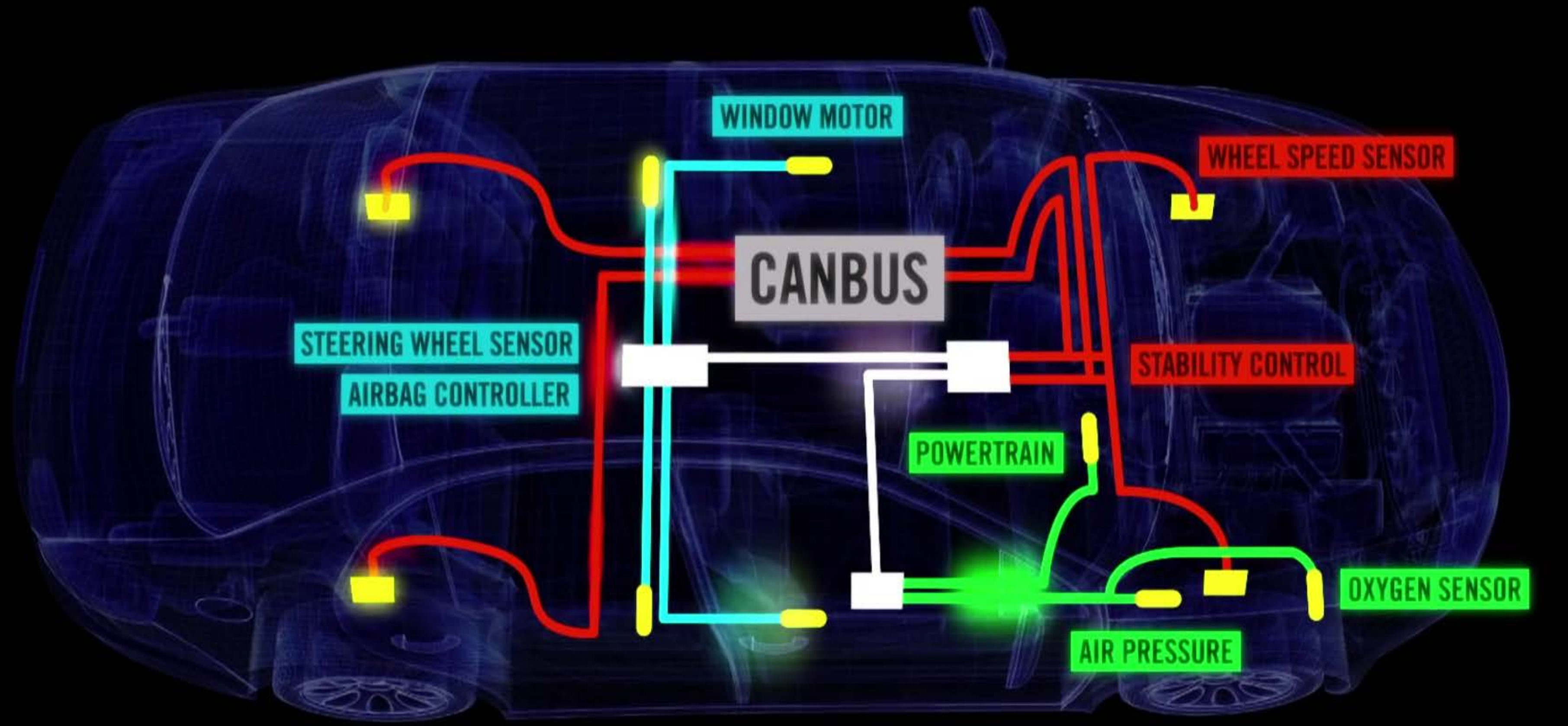
9



Stuxnet in Action
Iran 2010 Nuclear plant attack
Losing Trust at the PLC Layer



CANBus hacking

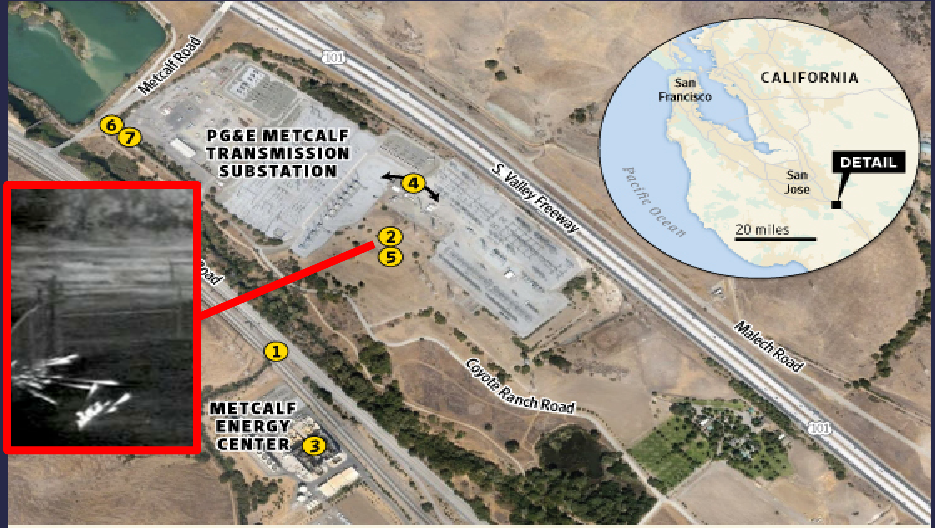


https://youtu.be/3jstaBeXgAs

PG&E Metcalf substation Attacks

Opportunities to Improve:

- Redundant Communication
- Gun Shot Detection
- Physical Access Control



Shots in the Dark

A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1	2	3	4	5	6	7
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can't enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

OT assets might include exploitable technologies like:

- Embedded Windows or Linux
- Web servers enabled
- FTP servers enabled
- Wi-Fi, Ethernet, Bluetooth or other non-serial ports enabled
- Network or dial-up remote access services enabled

Such assets must be configured, patched, and tested for security over their life cycle similar to IT assets

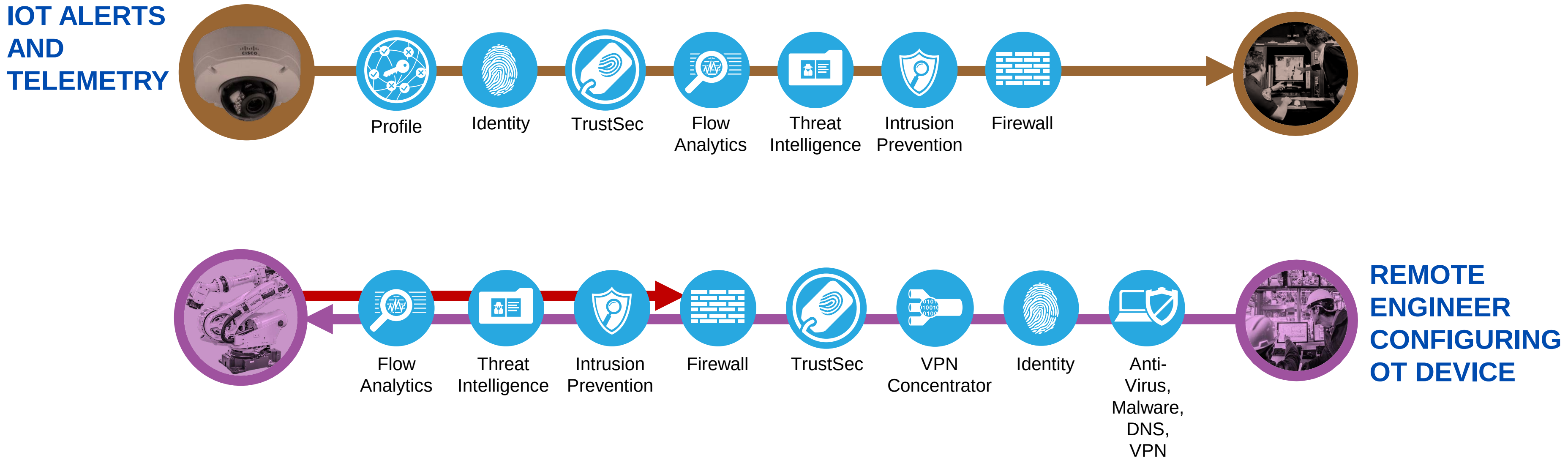
Substation Transformer

Security Architectures and solutions

Cybersecurity: Technology Areas and Key Use Cases

- Access Control
- Electronic Security Perimeter
- Threat Detection/Mitigation
- Secure Remote Access

Capabilities to Mitigate OT Risks



IOT ALERTS AND TELEMETRY

Profile

Identity

TrustSec

Flow Analytics

Threat Intelligence

Intrusion Prevention

Firewall

Flow Analytics

Threat Intelligence

Intrusion Prevention

Firewall

TrustSec

VPN Concentrator

Identity

Anti-Virus, Malware, DNS, VPN

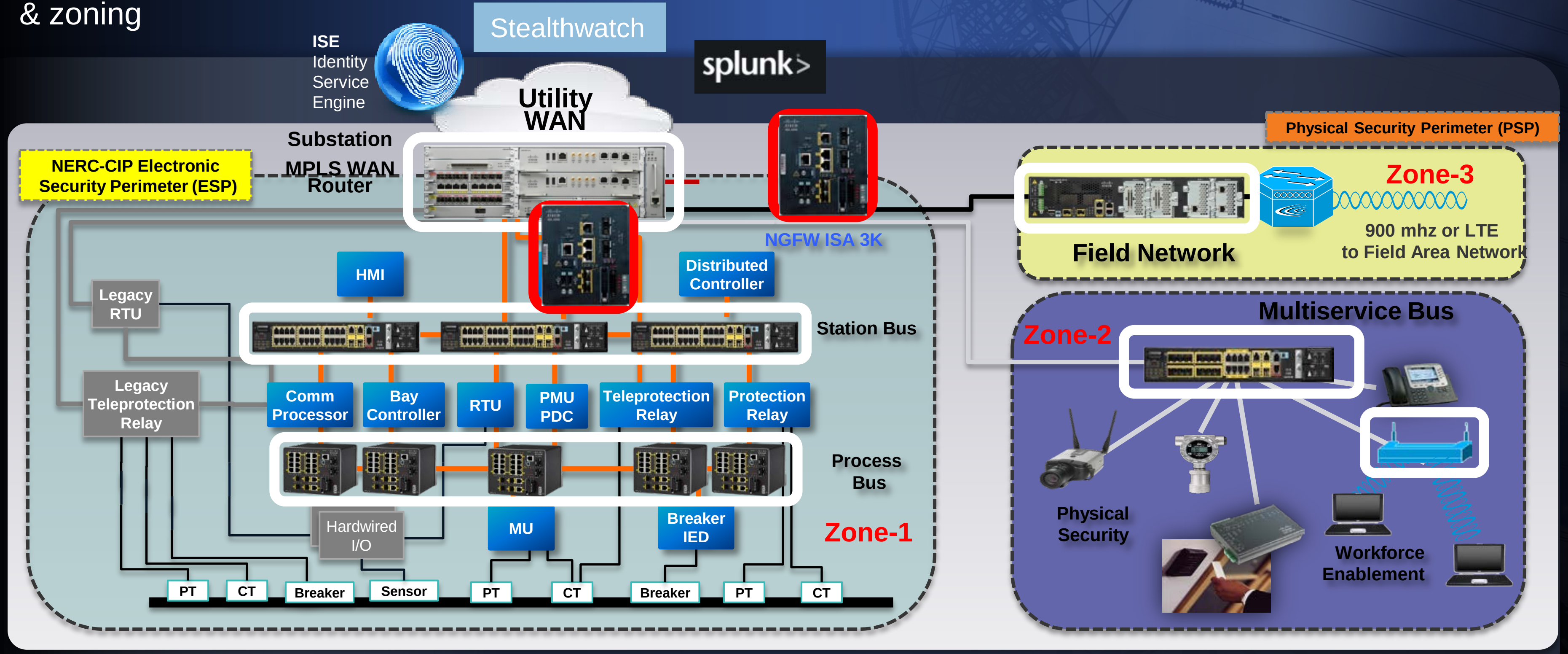
REMOTE ENGINEER CONFIGURING OT DEVICE

OT IoT Phased Security Architecture - Utilities substation use case

First Stage –
Secured Connectivity & zoning

Second Stage –
Secured Visibility & Control

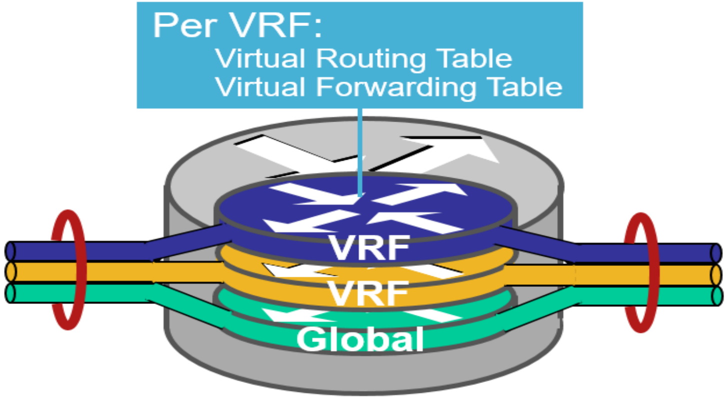
Third Stage –
Converged Security & Depth



Path Isolation

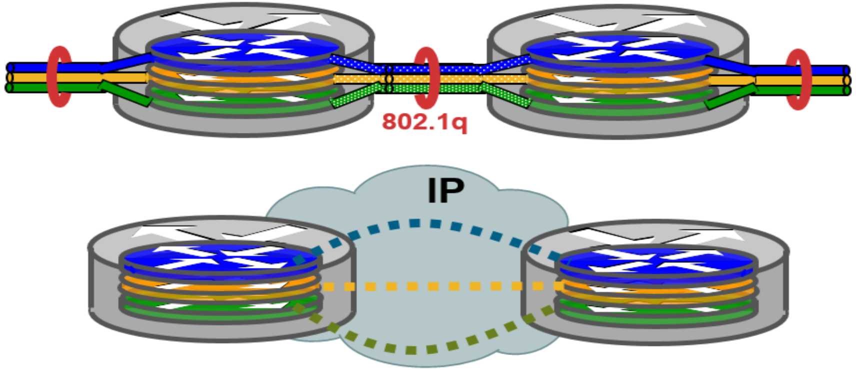
Functional Components

- Device virtualization
  - Control plane virtualization
  - Data plane virtualization
  - Services virtualization



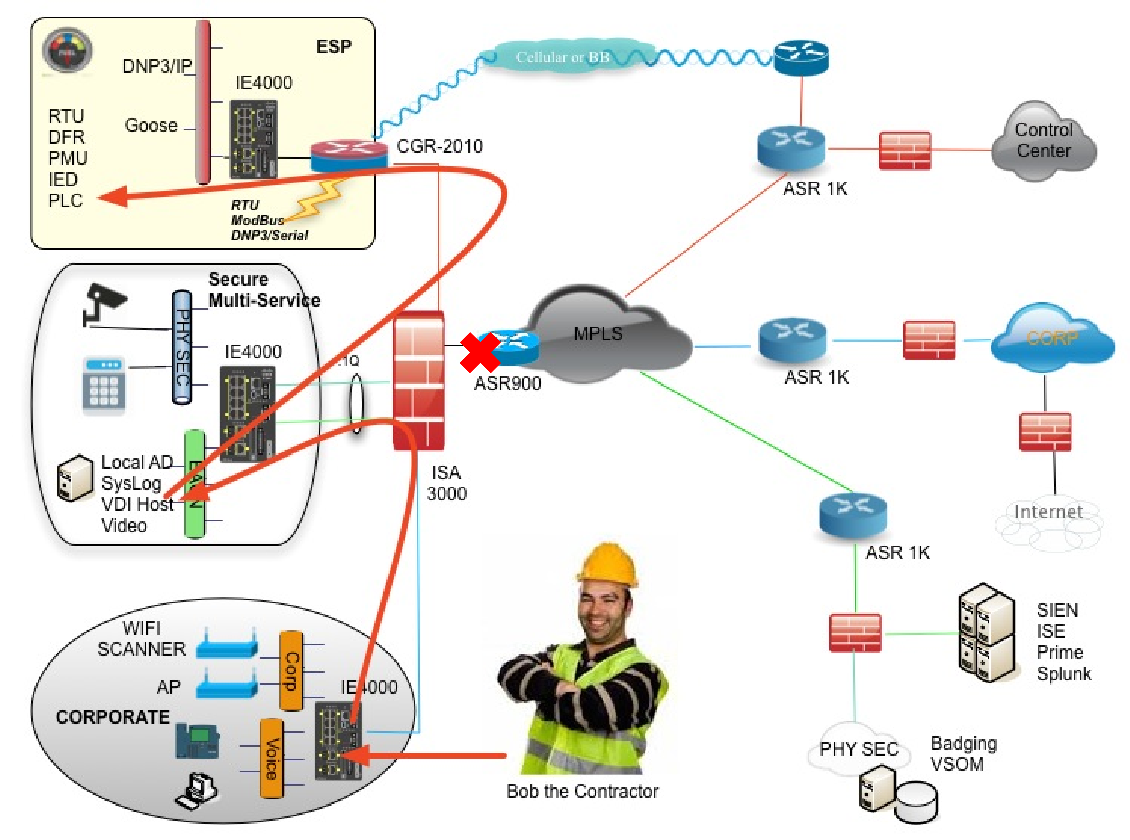
Per VRF:
Virtual Routing Table
Virtual Forwarding Table

- Data path virtualization
  - Single-hop
  - Multi-hop



VRF: Virtual Routing and Forwarding

Contractor Remote Access Control use case



Device is scanned and user authentication verified

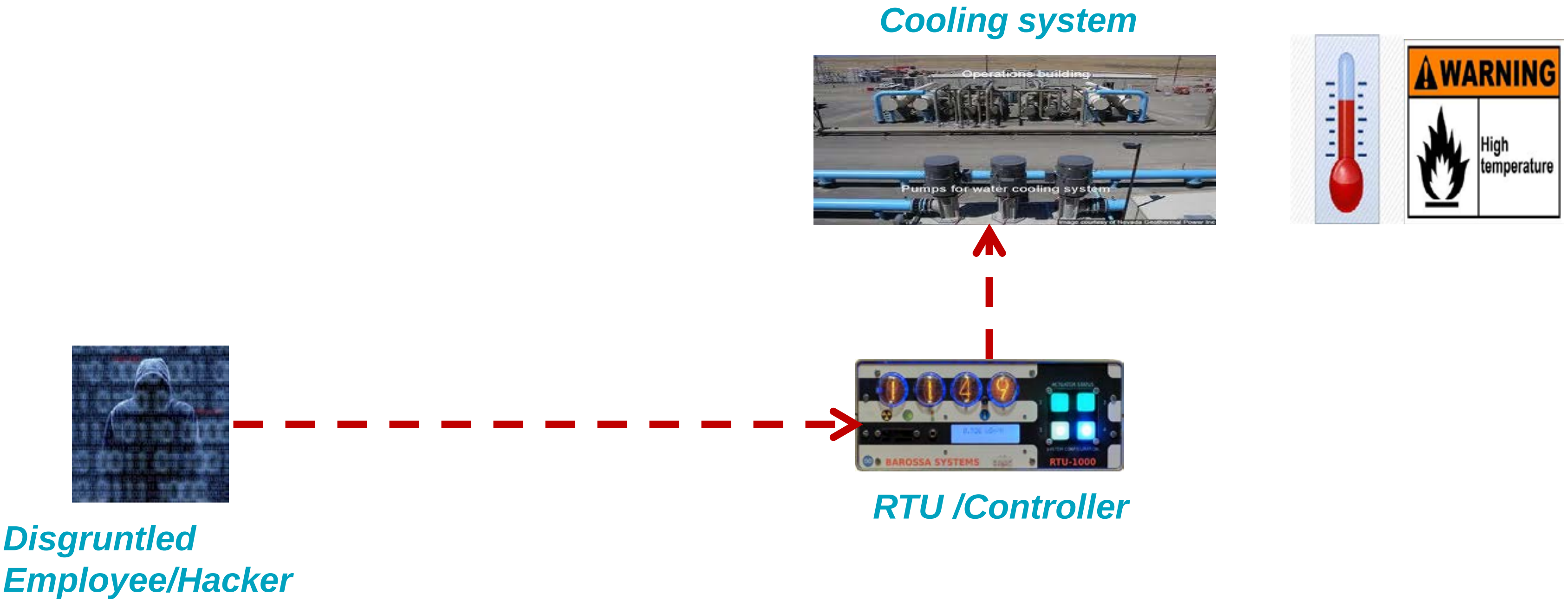
User profile applied and ISA 3K Sourcefire limit applications and path

VDI Host operates as a virtual air gap providing isolation to the ESP

Switch port security and Identity profiling control & monitor device

Centralized logging of events promotes accurate audits

Malicious Activity in the manufacturing Plant – Use case



Cooling system

RTU /Controller

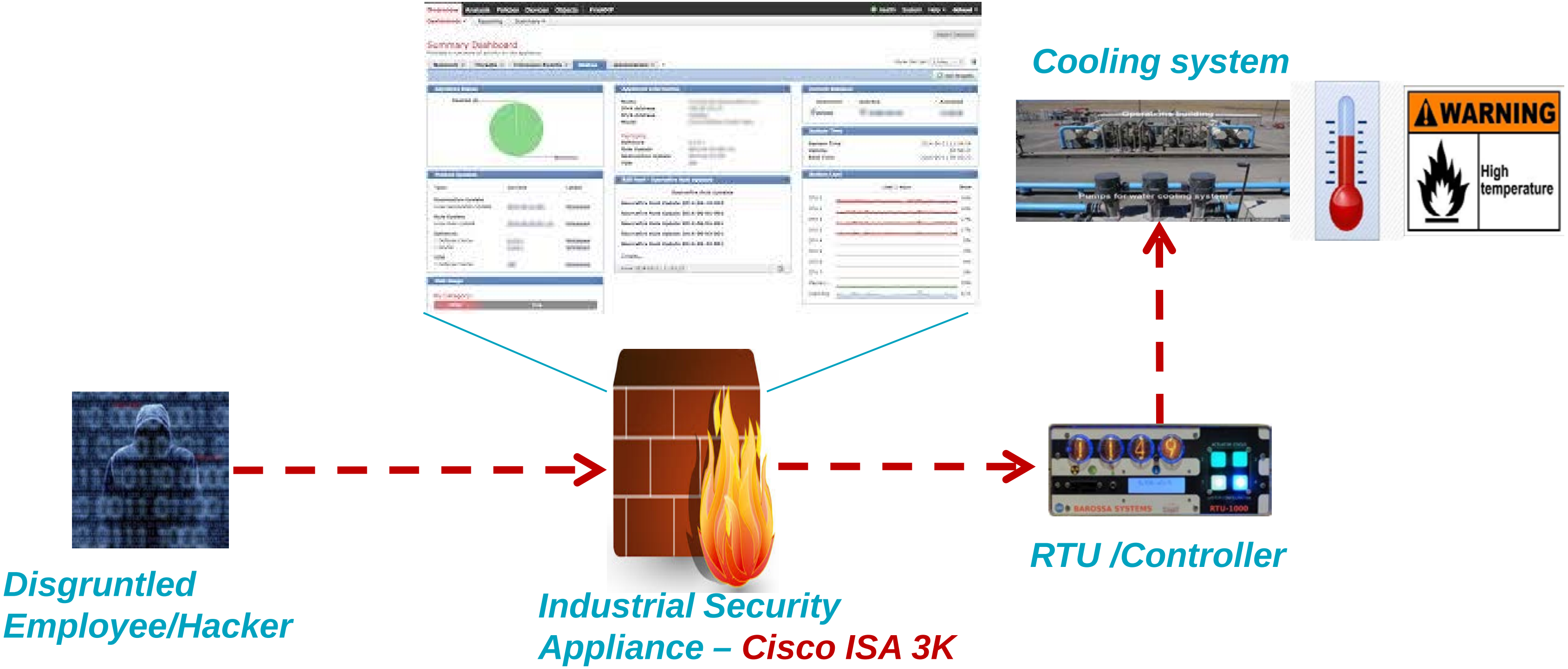
Disgruntled Employee/Hacker

Operations building
Pumps for water cooling system
Image courtesy of Nevada Geothermal Power Inc
WARNING
High temperature
BAROSSA SYSTEMS
RTU-1000

Plant Scenario – **Malicious Misconfiguration**
No Visibility, Minimal Controls

- Disgruntled Employee enters into the system shuts off the cooling functionality, changes password, locks RTU
- Alarms go off in the plant after temperature increases beyond threshold
- Cooling function could not be restored as RTU is locked

Malicious Activity in the Plant



Cooling system

RTU /Controller

Disgruntled Employee/Hacker

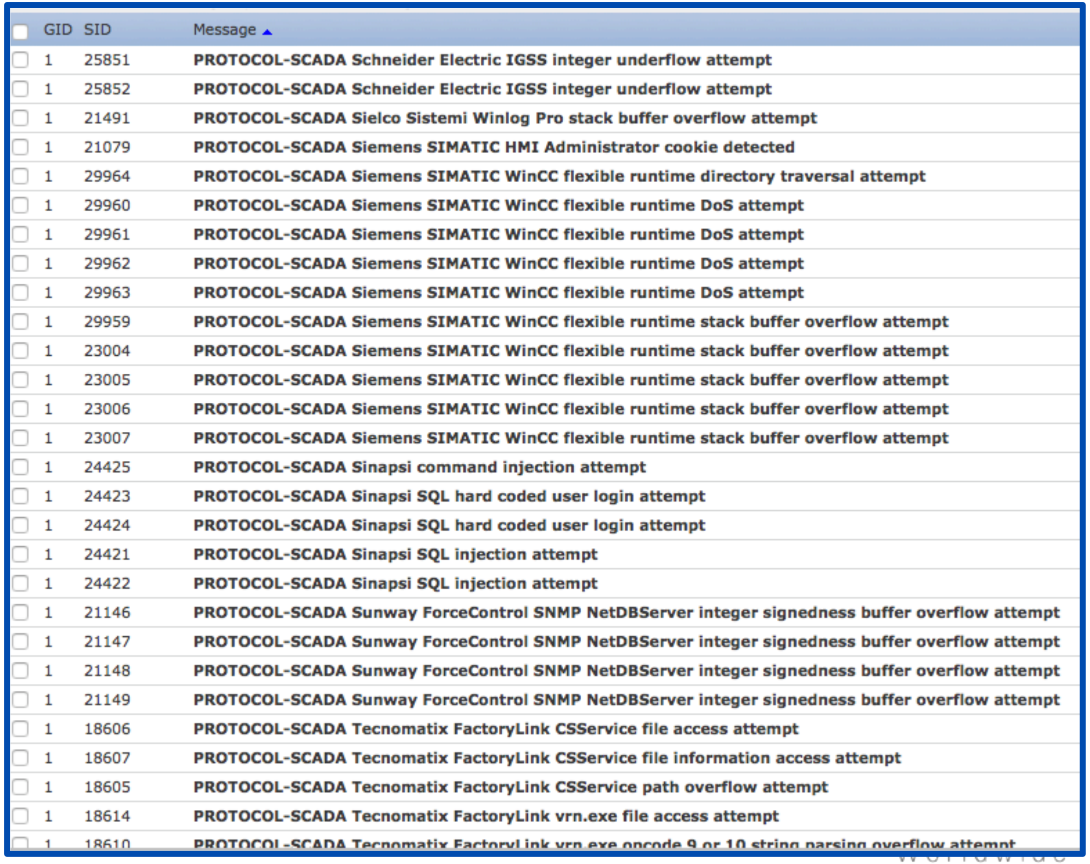
Industrial Security Appliance – Cisco ISA 3K

Plant Scenario – **Malicious Misconfiguration**
Full Visibility, Application Controls

- Disgruntled Employee enters into the system **ATTEMPTS** to shut off the cooling functionality, change password, lock RTU
- Cisco ISA in IPS mode, repeat the attack. No effect as ISA prevents the attack by dropping the packets

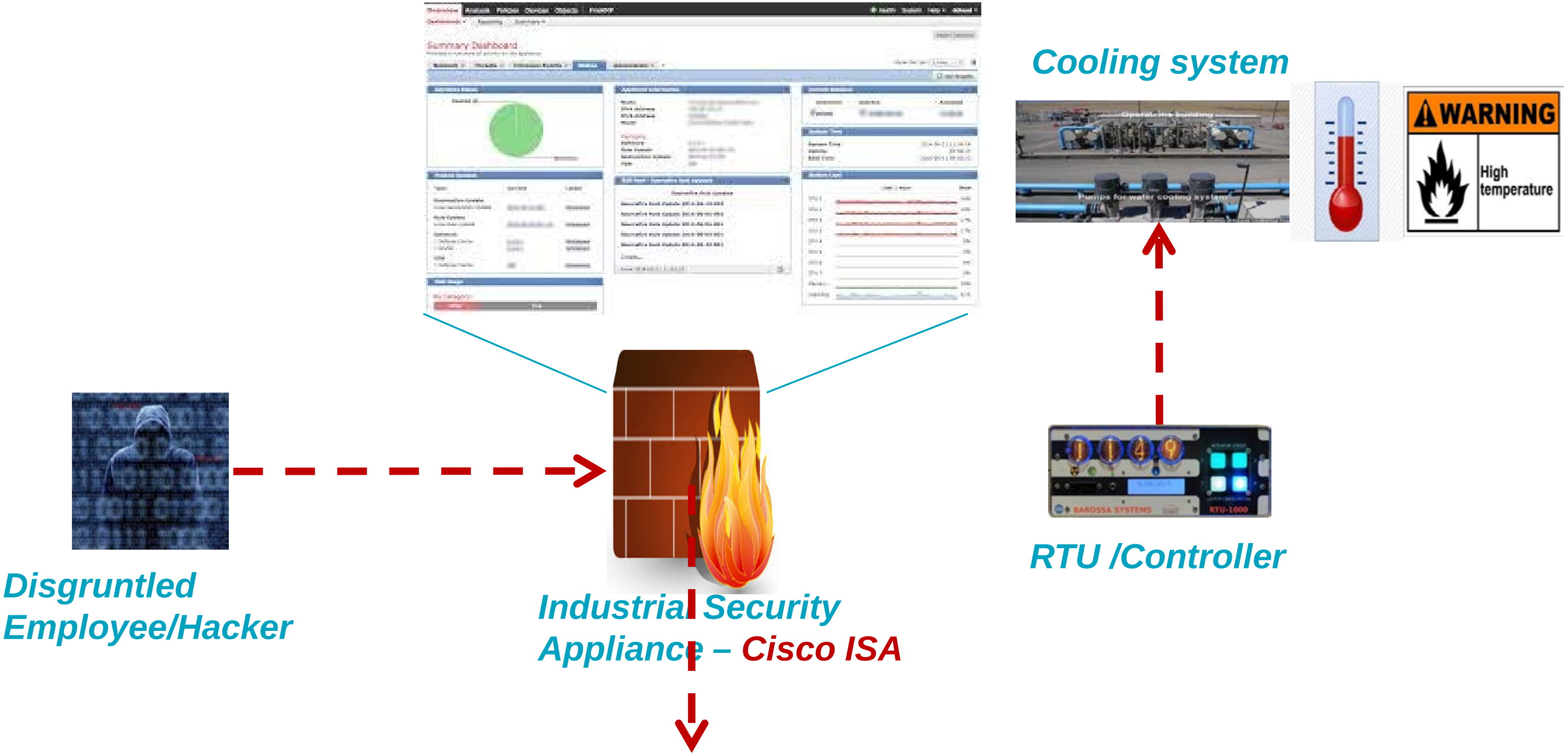
ISA 3000 industrial IPS signatures

- 300+ built-in Signatures for OT protocols and endpoints
- Based on Vulnerabilities discovered in protocols, devices
- Protection against Known/Unknown threats.
- Industrial Threat Signatures Updated regularly by Talos



□	GID	SID	Message ▲
□	1	25851	PROTOCOL-SCADA Schneider Electric IGSS integer underflow attempt
□	1	25852	PROTOCOL-SCADA Schneider Electric IGSS integer underflow attempt
□	1	21491	PROTOCOL-SCADA Sielco Sistemi Winlog Pro stack buffer overflow attempt
□	1	21079	PROTOCOL-SCADA Siemens SIMATIC HMI Administrator cookie detected
□	1	29964	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime directory traversal attempt
□	1	29960	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime DoS attempt
□	1	29961	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime DoS attempt
□	1	29962	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime DoS attempt
□	1	29963	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime DoS attempt
□	1	29959	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime stack buffer overflow attempt
□	1	23004	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime stack buffer overflow attempt
□	1	23005	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime stack buffer overflow attempt
□	1	23006	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime stack buffer overflow attempt
□	1	23007	PROTOCOL-SCADA Siemens SIMATIC WinCC flexible runtime stack buffer overflow attempt
□	1	24425	PROTOCOL-SCADA Sinapsi command injection attempt
□	1	24423	PROTOCOL-SCADA Sinapsi SQL hard coded user login attempt
□	1	24424	PROTOCOL-SCADA Sinapsi SQL hard coded user login attempt
□	1	24421	PROTOCOL-SCADA Sinapsi SQL injection attempt
□	1	24422	PROTOCOL-SCADA Sinapsi SQL injection attempt
□	1	21146	PROTOCOL-SCADA Sunway ForceControl SNMP NetDBServer integer signedness buffer overflow attempt
□	1	21147	PROTOCOL-SCADA Sunway ForceControl SNMP NetDBServer integer signedness buffer overflow attempt
□	1	21148	PROTOCOL-SCADA Sunway ForceControl SNMP NetDBServer integer signedness buffer overflow attempt
□	1	21149	PROTOCOL-SCADA Sunway ForceControl SNMP NetDBServer integer signedness buffer overflow attempt
□	1	18606	PROTOCOL-SCADA Tecnomatix FactoryLink CSService file access attempt
□	1	18607	PROTOCOL-SCADA Tecnomatix FactoryLink CSService file information access attempt
□	1	18605	PROTOCOL-SCADA Tecnomatix FactoryLink CSService path overflow attempt
□	1	18614	PROTOCOL-SCADA Tecnomatix FactoryLink vrn.exe file access attempt
□	1	18610	PROTOCOL-SCADA Tecnomatix FactoryLink vrn.exe opcode 9 or 10 string parsing overflow attempt

Malicious Activity in the Plant – Preventing the attack



Cooling system

RTU /Controller

Disgruntled Employee/Hacker

Industrial Security Appliance – Cisco ISA

Key Takeaways

- **The key takeaways from this demonstrations were:**
  - Understanding the needs for Security in OT networks (also IT vs OT Firewalls)
  - Both Intended and Un-intended actions leading to security risks
  - Industrial Security Appliance have the ability to Inspect Industrial Protocols and further take actions.

cisco