ISA Italy Section

Cyber security - why and how

Frankfurt, 14 June 2018

ACHEMA

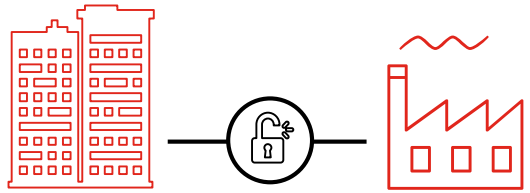
Industrial Cyber Security Program

Honeywell

THE POWER OF CONNECTED

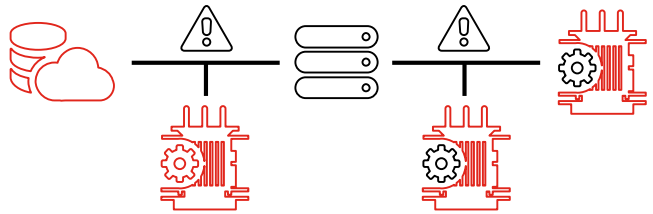
Konstantin Rogalas

Cyber Security Challenges – VoC Feedback



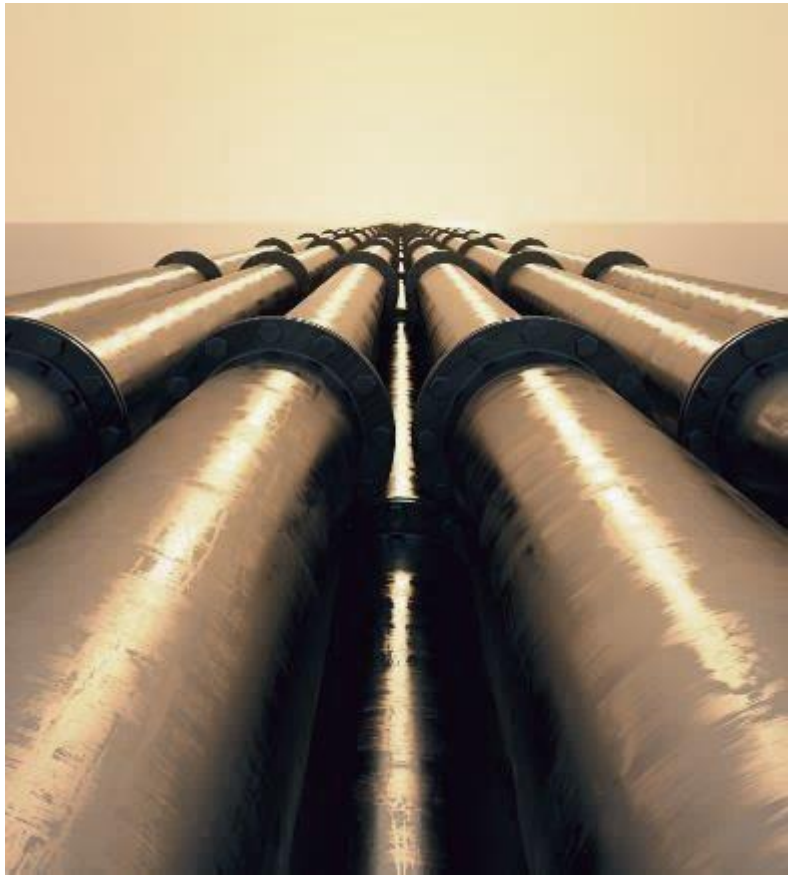
Don’t feel secure

- Attacks are increasing in frequency
- Limited compliance to standards and regulations (EU NIS Directive, NIST SP 800-82, ISA-62443, NERC CIP…)



Pressure to increase connectivity of field to center

+ Data-driven management and analytics. IOT, Industrie 4.0
+ Improvement of asset reliability & safety using remote access
- Increases the attack surface



Cyber Security Requires Proactive Management & Scientific Discipline

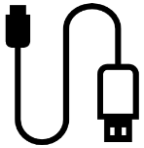
OT Cybersecurity Questions…

What's my company's exposure to the latest industrial cyber threat?

Are my plants compliant with our corporate cyber security directive?

50% of Board of Directors are not satisfied with Leaderships Cyber Issue Management

Are there "non-sanctioned" devices, like USBs, that have been added to plant process control networks?



What happens if I have a malware outbreak in my control network?

- Production impact?
- Operations staff SOP?
- How quick can I recover?

Agenda

- Who is the Honeywell Industrial Cyber Security (H-ICS) Organization?
- NIS Directive
- USB Protection – SMX Presentation & Demo
- ICS Shield Presentation & Demo
- Blueprint Methodology – Assessments & Consultancy Services – Automation Security Program Approach

Honeywell
THE POWER OF CONNECTED

Konstantin Rogalas MSc, MBA

Business Development for Honeywell Industrial Cyber Security - DACH, Central & South-East Europe

Konstantin.Rogalas@Honeywell.com

- 1989 – 1998 in Discrete Automation & Process Control;
- 1999 – 2012 in Telecommunications: Broadband-M2M/IoT;
- 2013 – Oil&Gas, Energy, Pharmaceuticals & Chemicals industry Certification study for ENISA in Industrial Cyber Security;
- 2014 – 2015 ICS Council with policy makers, asset owners and service providers;
- Member of the European ICS Stakeholders Group.
- Contributions: ENISA Reports, ICS3C, EC-JRC ERNCIP “European IACS Components Cyber-security Compliance & Certification Scheme” and “Thematic Network on Critical Energy Infrastructure Protection(TNCEIP)”

Cyber Security Specialist for ICS (OT)

220+
Certified Cyber Security Professionals

450+
Security assessments for Industrial Control Systems

600+
Remediation Projects

Global team

Cyber Security Services

Multi Vendor

Cyber Security Standard driven
IEC 62443 (ISA 99), ANSSI, BSI, CPNI

Numerous Partners

Cyber Security Products

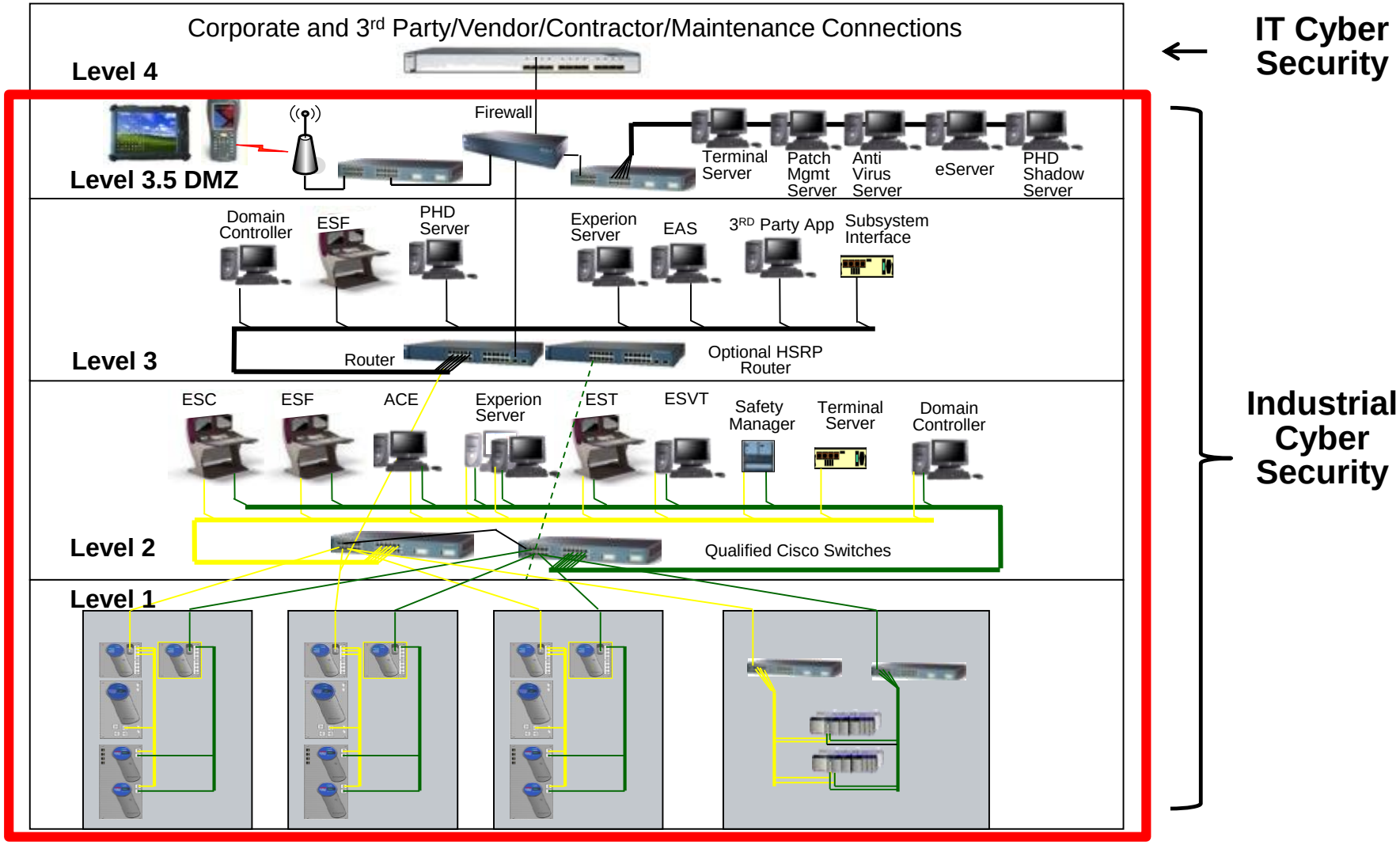
Embedded or Stand-alone

Cyber labs

450+
Managed Security Networks

Honeywell

Focus: Up to But Not Including Corporate and 3rd Party Networks



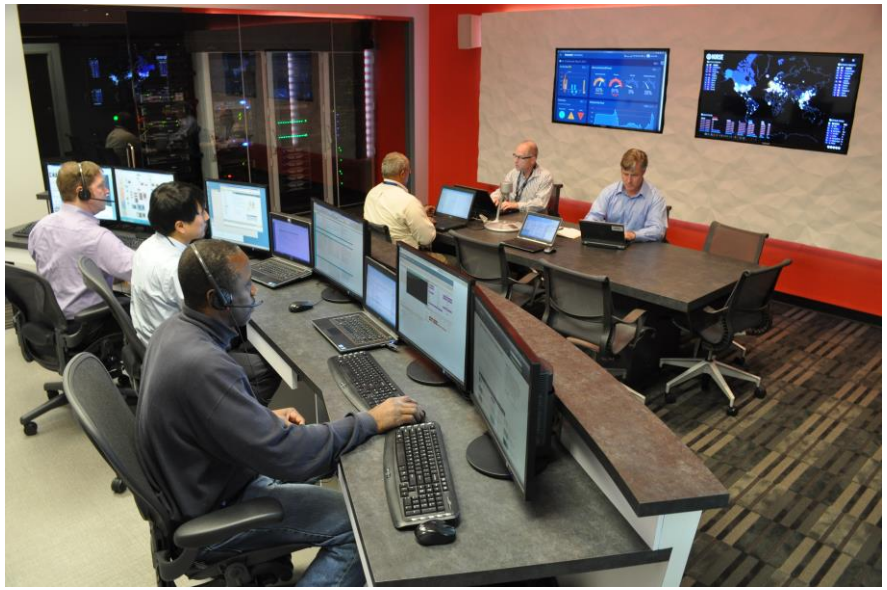
Honeywell

Industrial Cyber Security Solutions Lab

World-Class and Industry Leading Innovation Platform

Flexible model of a complete process control network up to the corporate network

- **Industrial Cyber Security solutions development and test**
- **Training Platform for Industrial Cyber Security Engineers**
- **Simulation lab for customers**
  - Simulate OT cyber attacks; demonstrate cyber security solutions



Atlanta, UAE, Singapore

Solutions Development

Training and Certification

Customer Demonstrations

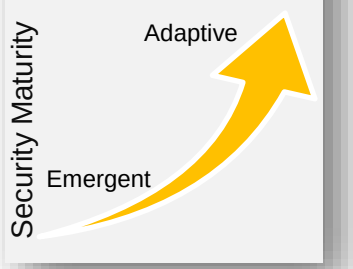
Honeywell
THE POWER OF CONNECTED

Honeywell ICS specialists background

- Unique combination of long time experience in process control, networks and cyber security
- Gain knowledge, demonstrate knowledge, and maintain knowledge
  - CISSP
  - CISM
  - CEH
  - CRISC
  - CCNA
  - CCNP
  - CCIE
  - CCSP
  - MCSE
  - MCSA
  - VCP
- Specialists with many backgrounds
  - Honeywell
  - Yokogawa
  - Emerson
  - Schneider
  - ABB
  - Siemens
  - …
  - Penetration testing
  - IT departments
  - Telecom providers
  - 14+ Languages

Honeywell Provides Full Solutions for Industrial Cybersecurity

INDUSTRIAL SECURITY CONSULTING



- Industrial security program development
- Assessment services
- Architecture and design
- Implementation and systems integration
- Operational service and support
- Compliance audit & reporting

INTEGRATED SECURITY TECHNOLOGY

- Whitelisting
- Antivirus
- Next-generation Firewall
- IDS/IPS
- Security Information & Event Management (SIEM)
- Threat Intelligence

MANAGED SECURITY SERVICES

- Secure remote access
- Continuous monitoring and alerting
- Automated patch & antivirus updates
- Incident response & recovery/ back up
- Security device co-management
- Hosting, management and operation of ICS Shield®
- OT SOC management & operations

CYBER SECURITY SOFTWARE

- ICS Shield® platform for cyber security operations
- Industrial Cybersecurity Risk Manager: Enterprise and Site
- Secure Media Exchange (SMX)
- Advanced Threat Intelligence Exchange (ATIX)
- Industrial assessment software & tools

Comprehensive, Proven and Trusted End-to-End Solutions

Agenda

- **Who is the Honeywell Industrial Cyber Security (H-ICS) Organization?**
- **NIS Directive**
- USB Protection – SMX Presentation & Demo
- ICS Shield Presentation & Demo
- Blueprint Methodology – Assessments & Consultancy Services – Automation Security Program Approach

Honeywell

Network and Information Security (NIS) Directive

- 18.12. 2015 - Final text was approved by the Member States (MS)
- Directive on Security of Network and Information Systems

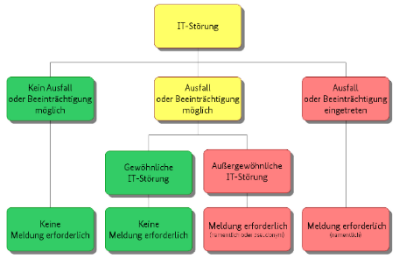
DEADLINES	entry into force + …	Milestone
August 2016	-	Entry into force
February 2017	6 months	Cooperation Group begins tasks, CSIRTs
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
May 2018	**21 months**	**Transposition into national law**
November 2018	**27 months**	**Member States to identify operators of essential services**
May 2019	33 months (i.e. 1 year after transposition)	Commission report assessing the consistency of Member States' identification of operators of essential services
May 2021	57 months (i.e. 3 years after transposition)	Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers

Honeywell

D – What must KRITIS-Operators comply with?

1. Appoint a contact point
   - KritisV Dealine: until 3. Nov 2016 to register at BSI (National Regulator)

2. Report Cybersecurity incidents
   - With concrete information flow:
   - 24x7 cybersecurity-org
   - Using appropriate technical controls
   - Within an cyber-aware, mature organization



<u>3. Certify all 730 KRITIS facilities with an Audit by latest May2018:</u>

- that they comply with the „state of the art“ norms/standards, such as
  - ISO/IEC 27001/62443

Honeywell

Other EU examples, all must follow

- **France**: 2 June 2006 identified the sectors of essential services
  - The associated law is
  - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id
  - The associated application decree:
    - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405967

- **Czech Republic**:
  - 1st January 2015 – Czech Cyber Security Act entered into force
  - 25th March 2015 – Several CII elements were determined
  - 26th June 2015 – Responsible authorities had to announce contact details
  - 25th March 2016 – The end of transitional period
  - 1st August 2017 – Implement NIS Directive – Identify operators of the following essential services

- Other countries following: EE, (UK), NL, SE, IT, BE, FI, AT, BG, HU, ES, IE, LV, LT, PL, PO, RO, SK, DK, GR etc.
- Deadline for all EU Member States transposition into national legislation was May 2018 as per initial slide on NIS Directive milestones

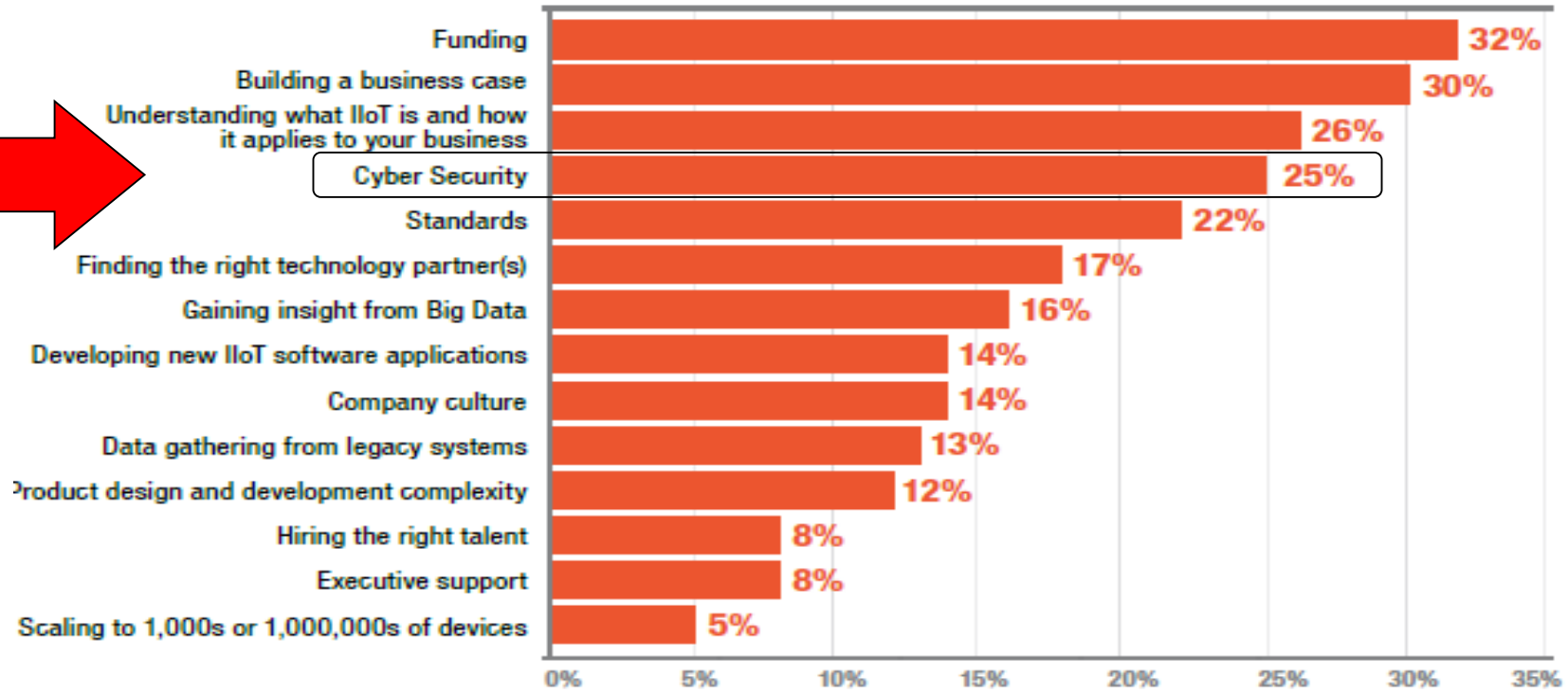
Honeywell

Agenda

- **Who is the Honeywell Industrial Cyber Security (H-ICS) Organization?**
- **NIS Directive**
- **USB Protection – SMX Presentation & Demo**
- ICS Shield Presentation & Demo
- Blueprint Methodology – Assessments & Consultancy Services – Automation Security Program Approach

Honeywell

Study: IIoT Challenges



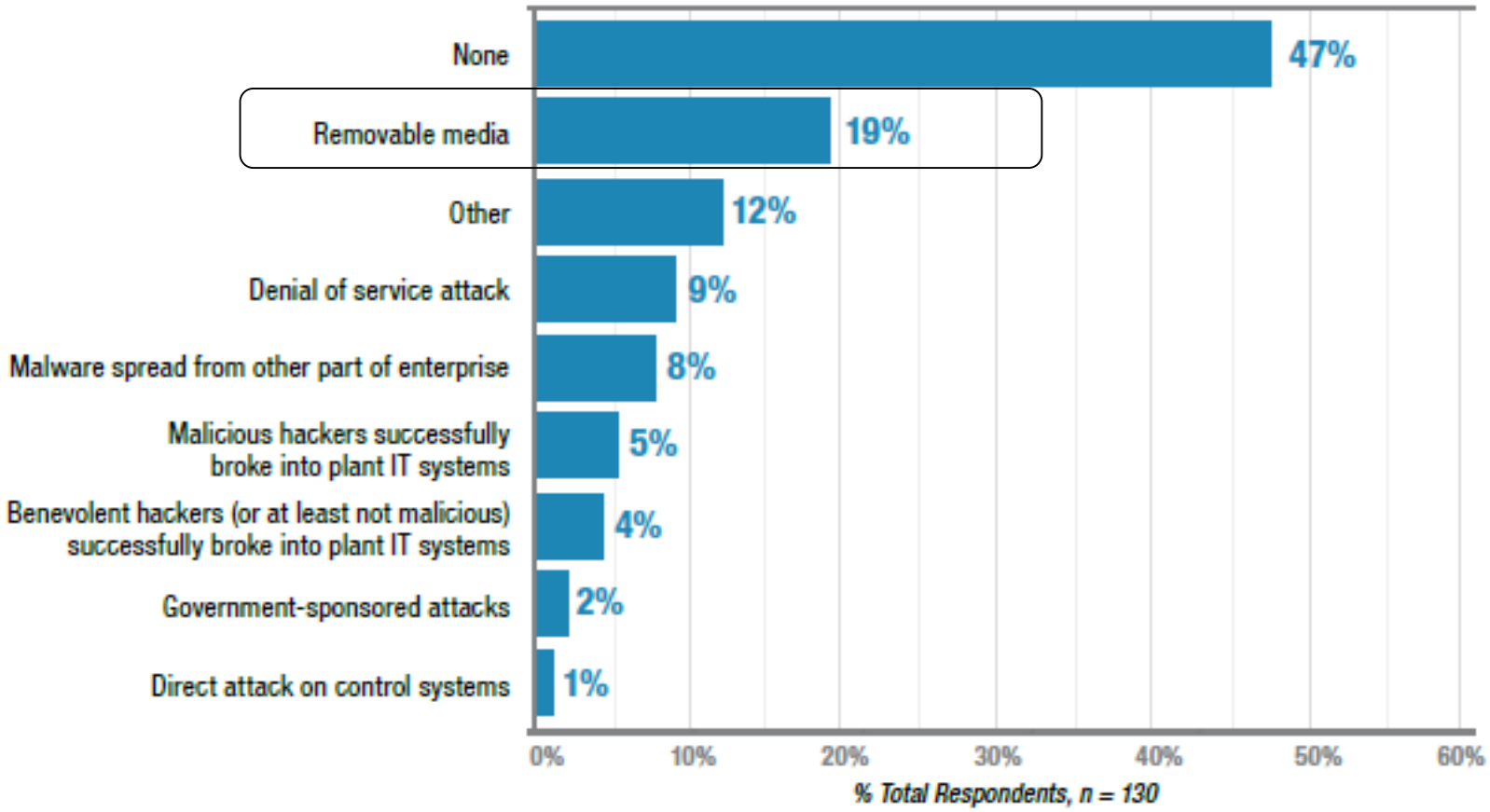
What are the top challenges your company faces in deploying IIoT technology?
(N=269, all respondents)

- Cyber Security: most important non-business Element for IIoT-Projects
- Security for IoT CAGR ~35%, 2017-22
  (Market-Research-Reports.com)

Source: Nov17; 'Putting ICS at the top of the CEO agenda'

Study: How frequent are industrial cyber security attacks?

What were the attack sources?



Source: Nov17; 'Putting ICS at the top of the CEO agenda'

Industrial USB Attacks are Increasing – Operation Copperfield

How this attack happened:

Another example of the need for SMX…the attack known as Operation Copperfield was caused by an operator watching a movie loaded from a USB during his shift

- On December 11, 2017 at 01:21 a.m., a night-shift employee working at a critical infrastructure facility in the Middle East inserted a USB drive into a shared workstation that dozens of employees use on a daily basis," said researchers at Nyotron.
- "The employee was watching the movie *La La Land* that he had recently downloaded to his USB."
- The employee did not realize that simple actions of inserting the USB drive initiated a sequence of events that had the potential to be disastrous for his organization.
- "Along with the movie, he had launched a well-crafted attack now known as Operation Copperfield"

Source: http://www.isssource.com/ics-alert-usb-malware-attack/

Other Industrial Examples:

Major Gas Company Hit by Virus Infection:

Office systems were unusable since the malware struck. Virus entered the systems via USB flash drive.

U.S. Electric Utility Virus Infection:

Virus infection discovered in a turbine control system at the power plant. A third-party technician used a USB drive that was infected with a variant of the Mariposa virus.

Steel Plant Infected with Conficker:

An investigation revealed Conficker virus infection in all machines of the ALSPA system. One possibility regarding how this virus spreads is through a USB drive as well as via network.

U.S. Power Plant Hit by USB-Based Malware:

Attacked through an infected USB stick used for software updates. Infected with two common malware & one with sophisticated malware

Honeywell
THE POWER OF CONNECTED

SMX Now Protects Against Advanced USB Threats

Increasing Threat Complexity

BadUSB

- Manipulation of USB firmware.
- USB device will act as – HID (Human Interface Device, like a keyboard) and can execute scripts.

Rubber Ducky

- A keystroke injection tool disguised as generic flash drive.
- Computer recognizes the USB as a typical keyboard and automatically executes the preprogrammed rubber ducky scripts.
- Execution speed around 1000 words per minute.

Bash Bunny

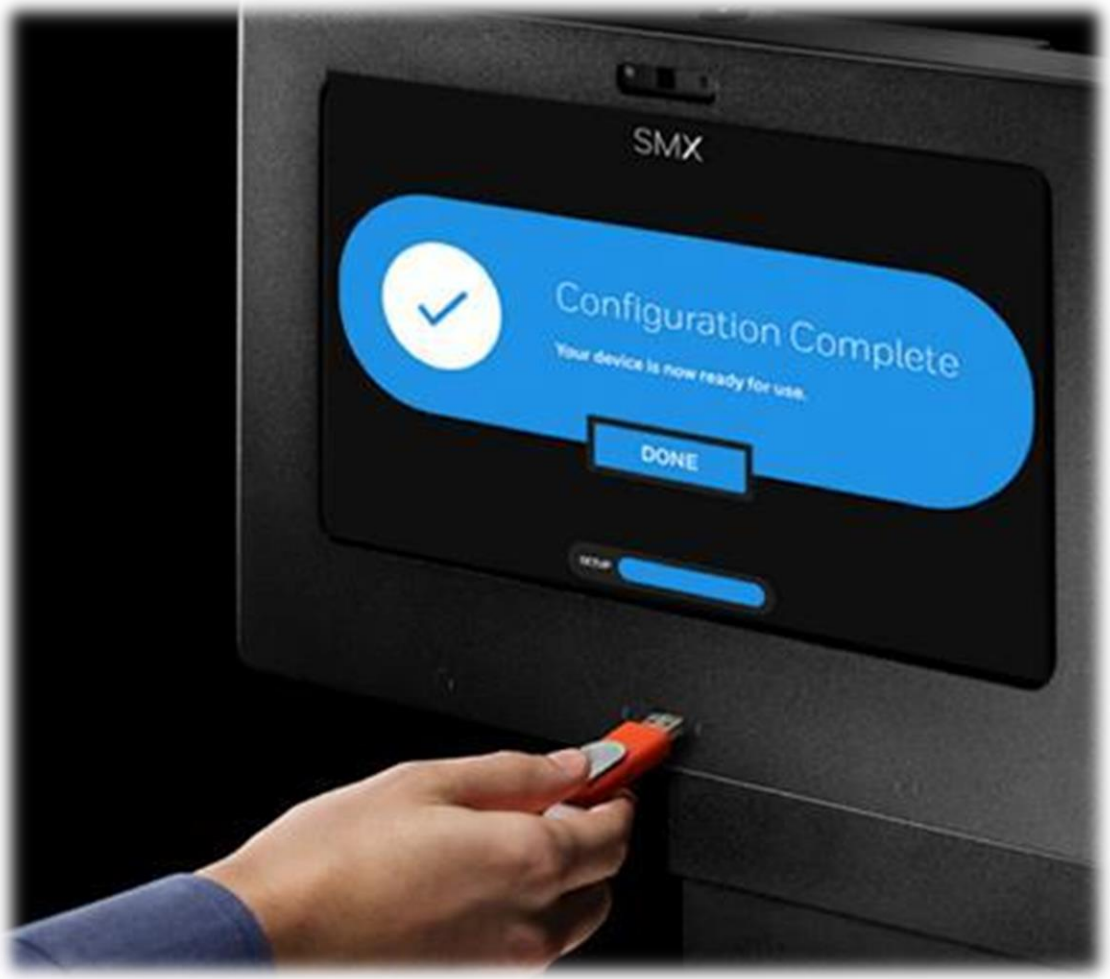
Ability to execute all Rubber ducky scripts, as well as more complex attacks:

- Ethernet over USB via RNDIS (Remote Network Driver Interface Specification) or Ethernet control model (ECM)
- Mass Storage Device
- A serial device
- Fully featured Linux computer

SMX Provides Protection from Attacks Others in the Industry Cannot

Unique Features

Value-For-Money



Why choose Honeywell's SMX?

1 Are your policies really enforced?

- Can USB scanning be bypassed?
- Can files be added/modified after initial check?

2 Traditional weak USB Protection security controls

- AV / Competing solutions only scan *files* for threats, not the USB device itself
- Will they catch malware that exists at root or firmware level on device?
- Can they protect against the latest threats like BadUSB or Rubber Ducky bypass attacks?

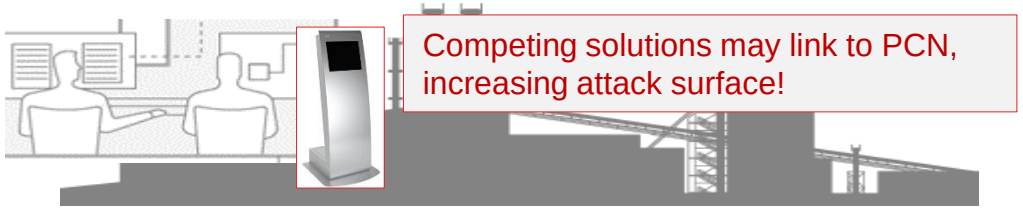
3 Traditional High life-cycle cost and effort because

- Competing solutions can require manual effort to update malware signatures
- Do you have the time and resources in place to keep things up to date?
  … or to add newer, more advanced detection solutions?

4 Is it really up-to-date?

- AV/Others are in practice updated every month, week or at best daily.
- Timely delays to the latest cyber threats create a serious security vulnerability.

Process Control Network



Honeywell's SMX:

Advanced Threat Intelligence Exchange (ATIX)

1 Enforces policies

- USB drive cannot be accessed unless checked-in
- SMX provides tamper resistance & digitally signs clean files

2 Strongest security controls

- SMX guards against new attacks where competing products are still vulnerable (e.g. BadUSB or Rubber Ducky bypass attacks)
- SMX uses Reputation & File-Code analysis in addition to AV by continuous feed from multiple detection engines/vendors.

3 Lower life-cycle cost and less effort to maintain

- SMX is a fully managed solution requiring no manual administration
- Cost savings through labor efficiencies and built-in threat detection offset cost of ownership

4 Auto-learning protection

- Honeywell's threat repository (ATIX) grows continuously as threats are identified globally
- Threat intelligence sources include Industrial and PCN updates, much more than off the shelf anti-virus scanning

SMX sits outside PCN so there is zero threat

Process Control Network

SMX Connection to ATIX Ensures Evergreen Cyber Threat Protection

SMX is an Award Winning Product

- Honeywell's Secure Media Exchange (SMX) has been named a Control Engineering's 2018 Engineers' Choice Awards winner
- The coveted Control Engineering Engineers' Choice Awards highlight some of the best new control, instrumentation and automation products as chosen by Control Engineering's print and online subscribers

SMX Won an Award from Control Engineering China Earlier in 2017

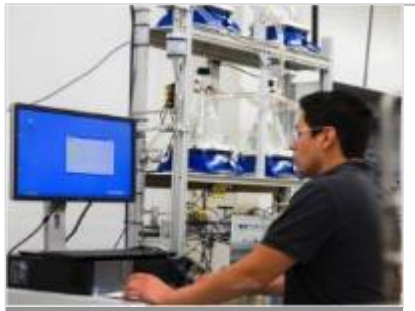
Recent Examples of SMX Customers

Refining

5 year subscription to SMX by major US refiner

Cement

5 year subscription to SMX by Asian cement producer



Oil and Gas

5 year subscription to SMX by major Indian oil and gas company

Natural Gas

5 year subscription to SMX by major natural gas company in the Middle East

Manufacturer

5 year subscription to SMX by industrial manufacturer in China

Chemicals

5 year subscription to SMX by major European chemical company

Growing Customer Base Strengthens ATIX's Cyber Threat Intelligence

Agenda

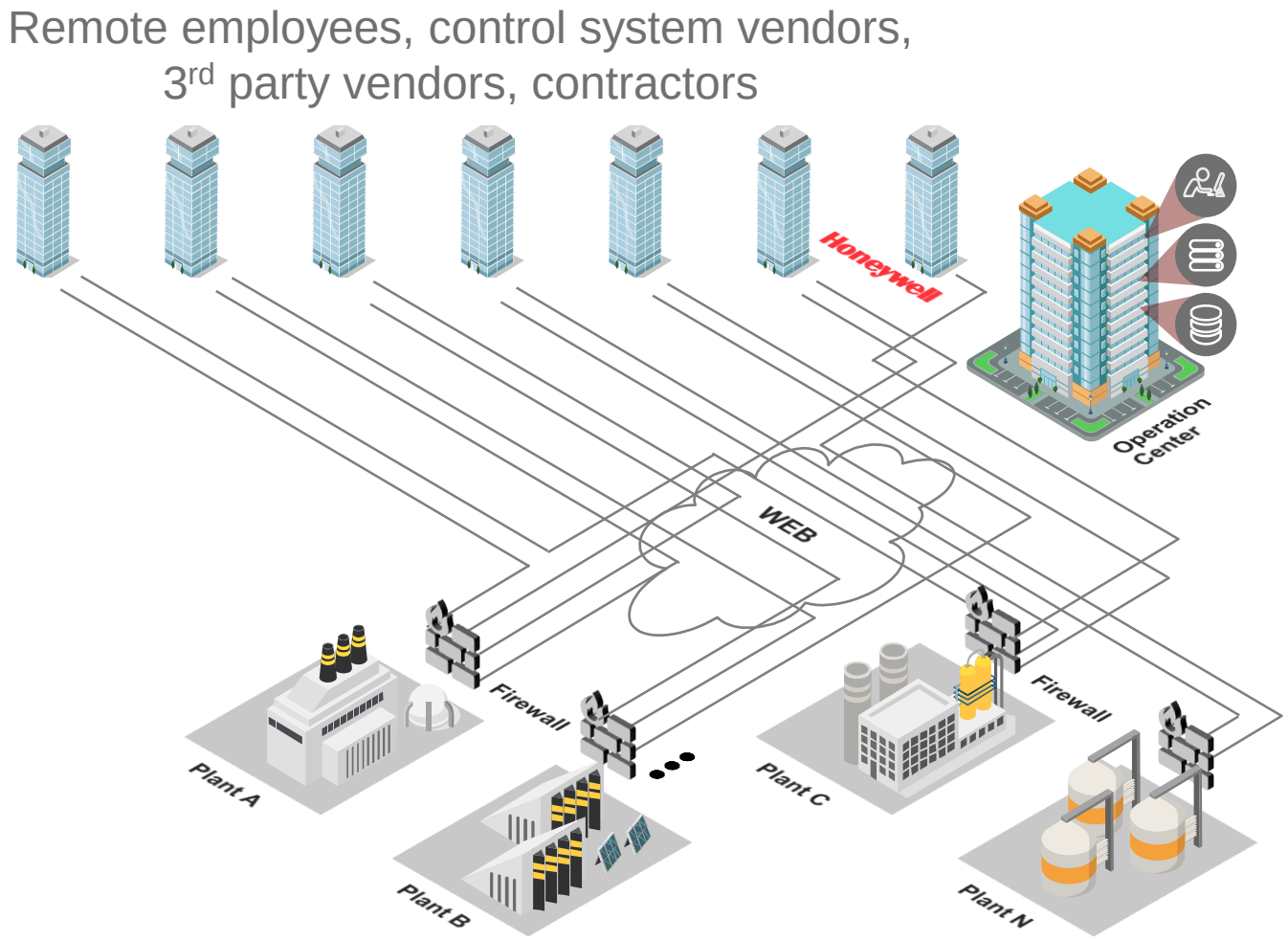
- Who is the Honeywell Industrial Cyber Security (H-ICS) Organization?
- NIS Directive
- USB Protection – SMX Presentation & Demo
- ICS Shield Presentation & Demo
- Blueprint Methodology – Assessments & Consultancy Services – Automation Security Program Approach

Honeywell

Grassroots-level OT Cyber Security Issues

Partial coverage of security essentials

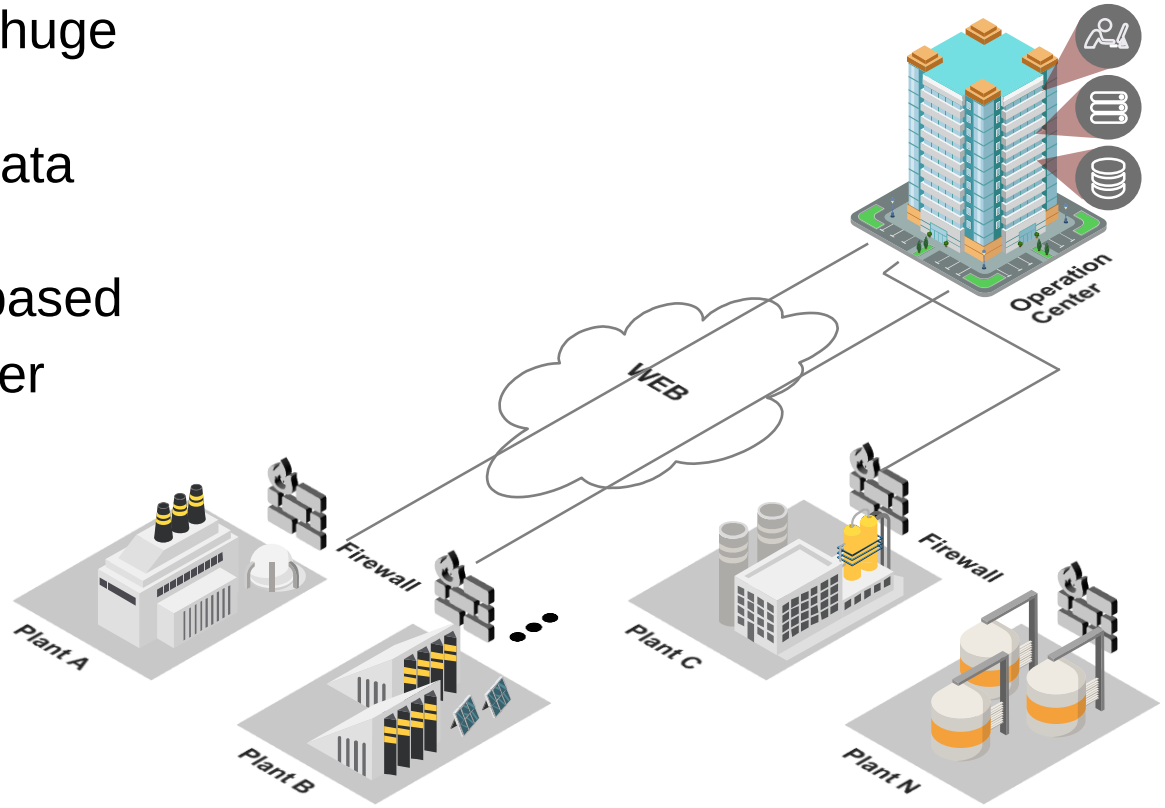
- Multiple access points
- Partial data on assets & events
- No proper hardening
- No proper monitoring
- No proper governance
- No proper planning & accountability



IIoT Security Management Challenge

Secure transfer of data to HQ or cloud

- IIoT devices (such as sensors) will generate huge amount of data
- Advanced analytics are needed to turn this data into strategic wisdom
- Analytics capabilities will be at HQ or cloud based
- Modern plants will require secure data transfer tunnel to cloud or HQ



Requires massive data transfer outside of the ICS network

Honeywell ICS Shield

Top-down OT security management

- Automates top-down integrated approach for deployment and enforcement of plant-wide security policies
- Based on proven technology acquired through Nextnine acquisition – over 6000 installs
- Delivers unrivaled visibility, reliability and compliance for industrial plant operations
- Enables security of remote field assets from a single operations center

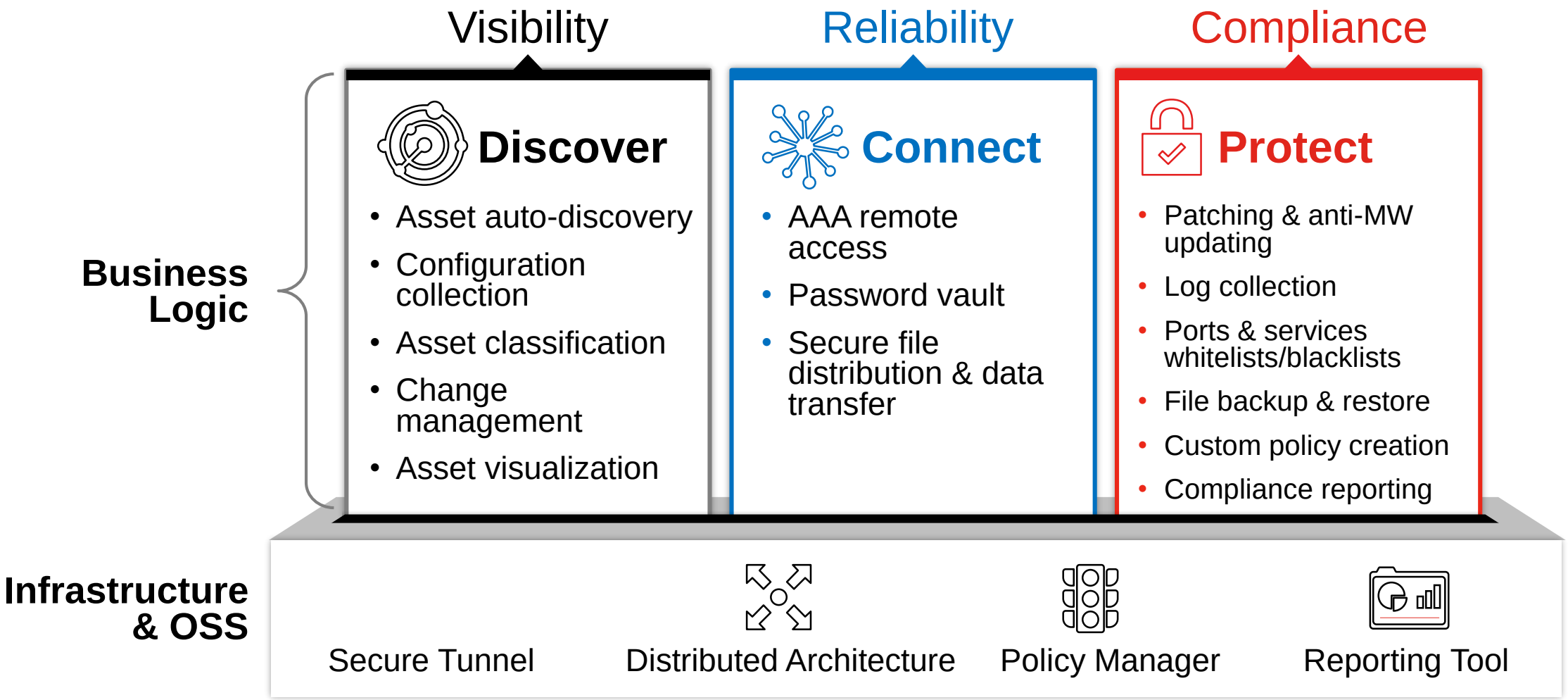
NEXTNINE
Connected ICS. Secured.

Key Features:

- Secure remote access
- Secure file transfer
- Automated patch and AV updates
- Asset discovery
- Performance/health monitoring
- Compliance reporting

Industry Standard Platform for Secure Remote Access – 6000+ Installs

ICS Shield: OT Security Management Platform

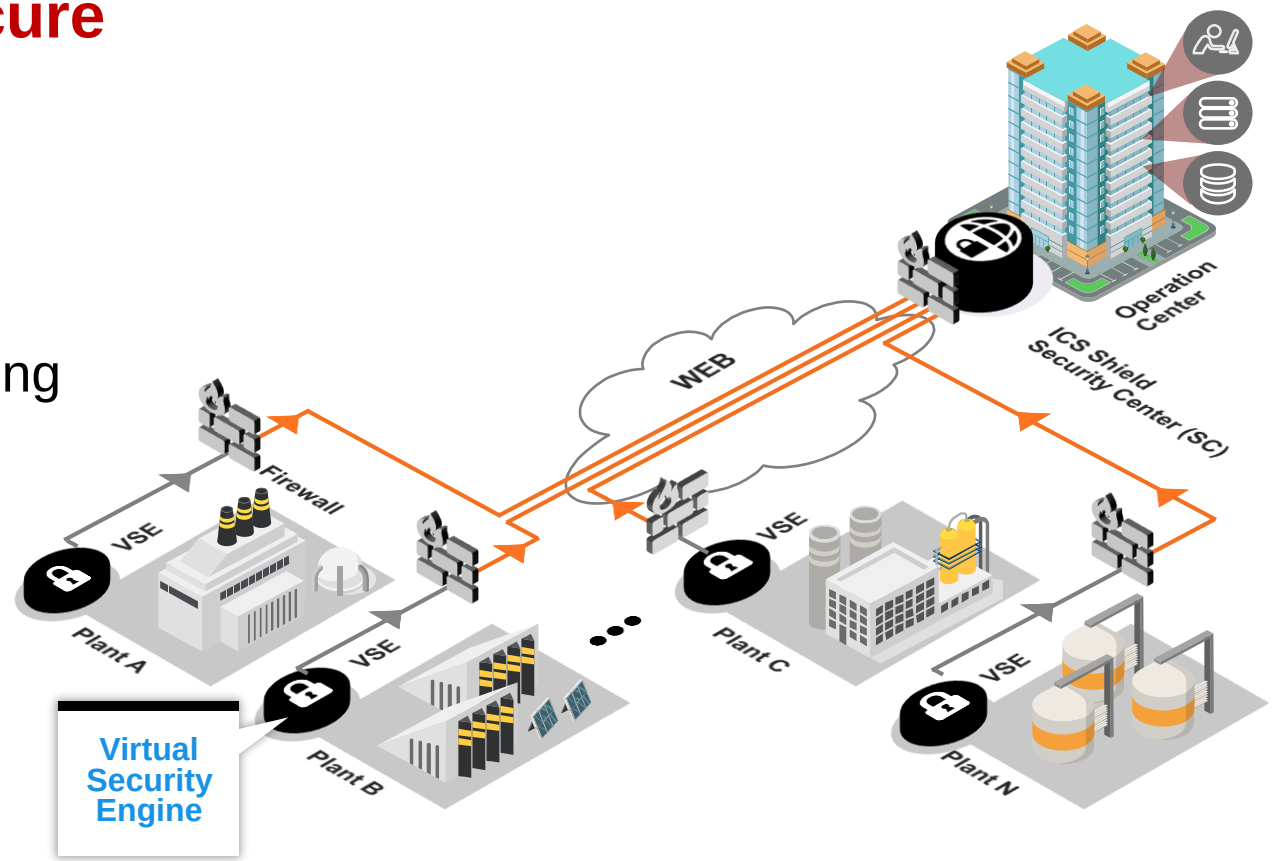


Honeywell
THE POWER OF CONNECTED

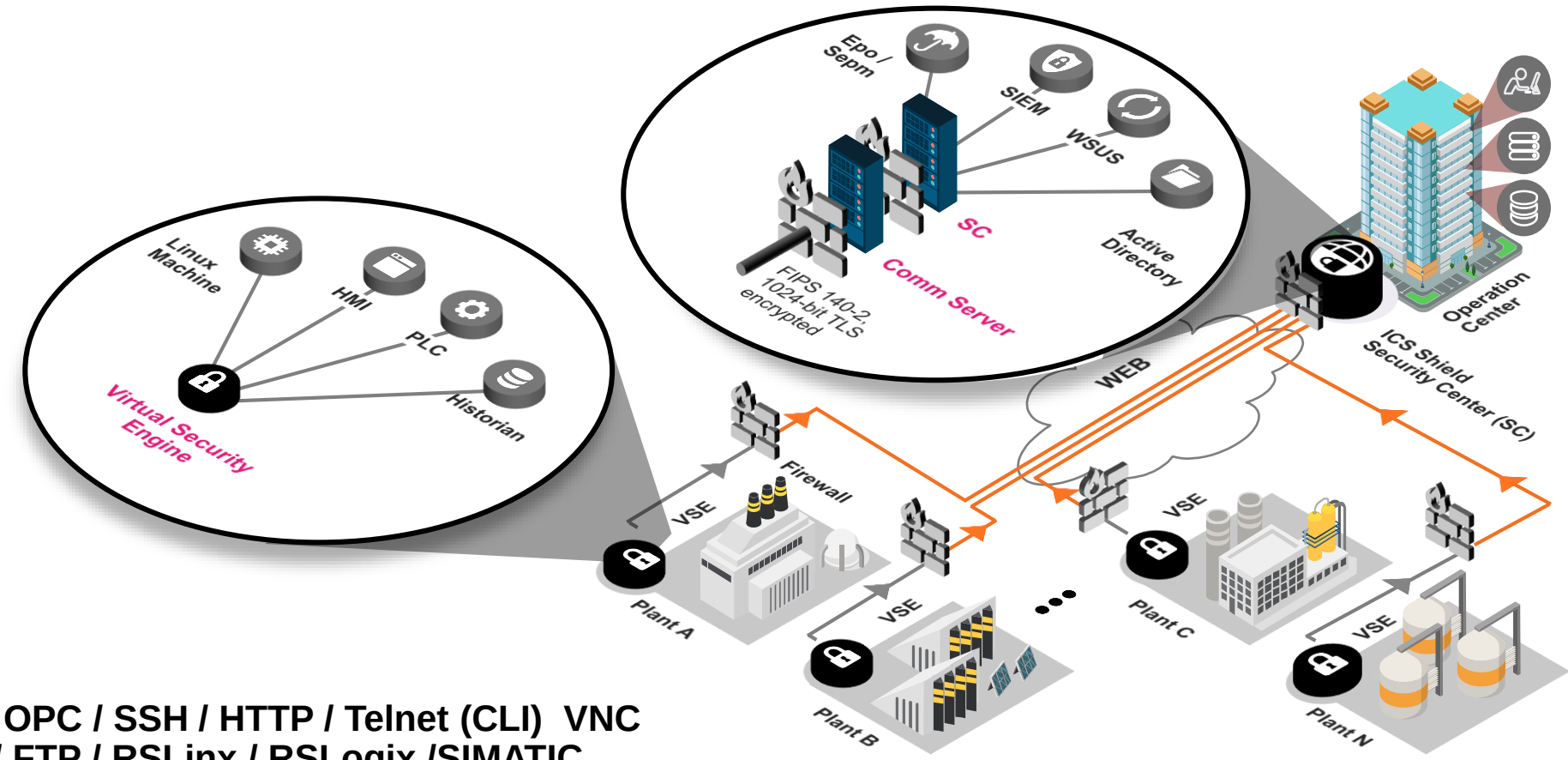
ICS Shield Deployment

Distributed architecture and secure tunnel from plants to center

- Install SC at the data center
- Install VSEs at each plant
- Establish a secure tunnel, outbound, using port 443, TLS encrypted
- One FW rule to manage all remote connections



ICS Shield System Architecture



WMI / SNMP / OPC / SSH / HTTP / Telnet (CLI) VNC / RDP / SFTP / FTP / RSLinx / RSLogix /SIMATIC

Any Proprietary TCP or UDP based protocols

Windows | Networking | Industrial

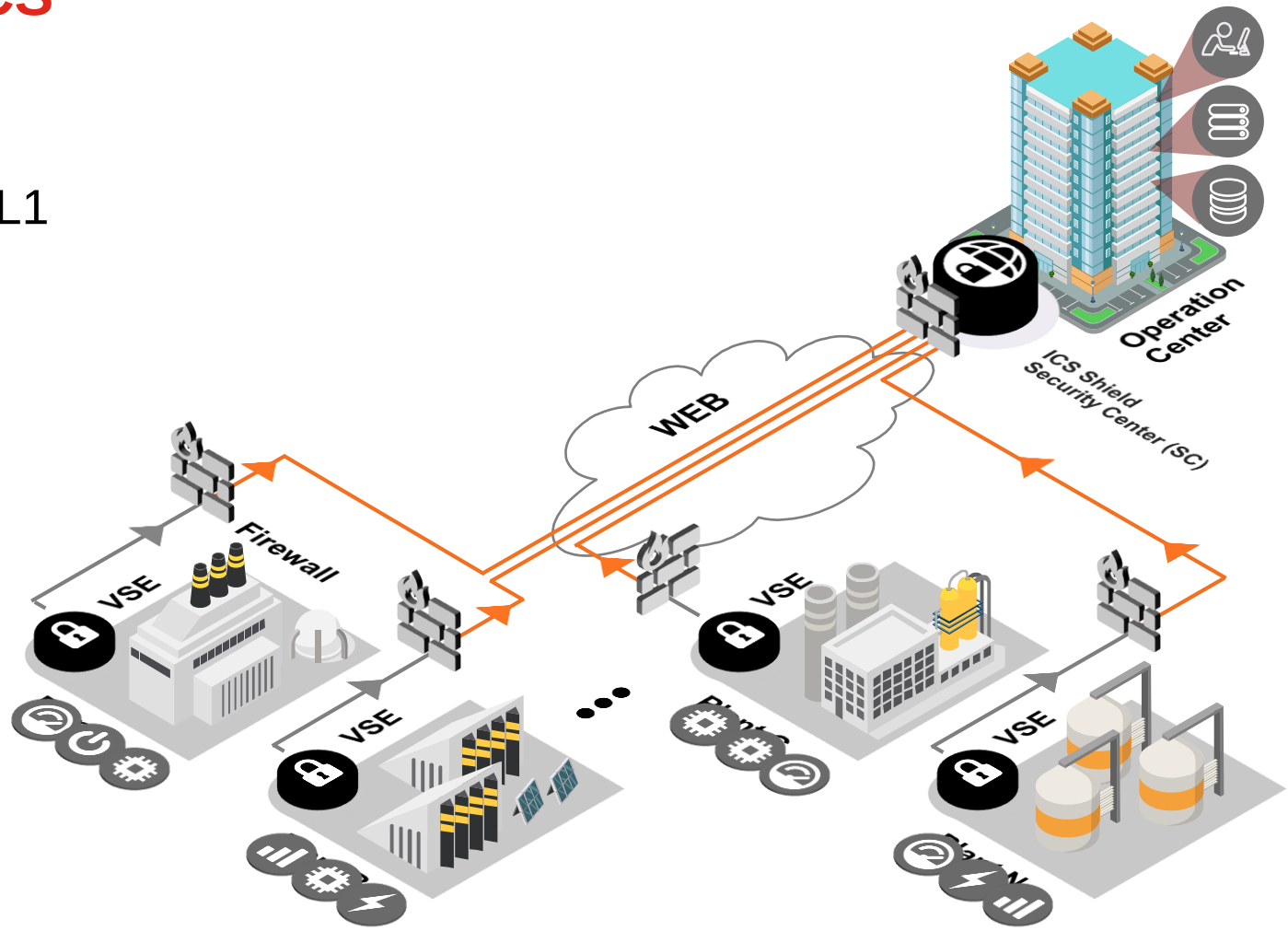
Honeywell

THE POWER OF CONNECTED

Discover – The Starting Point For A Secure ICS

End-to-end visibility into the ICS

- Passive and Active discovery
- Discovery down to L3, L2 and even L1
- Configuration collection
- Change monitoring
- Classification & labeling
- Visualization
- Assets labeling



NIST Cybersecurity Framework
ID.AM-2: Software platforms and applications within the organization are inventoried.

Honeywell
THE POWER OF CONNECTED

Connect – Expert To Asset, Fast And Secured

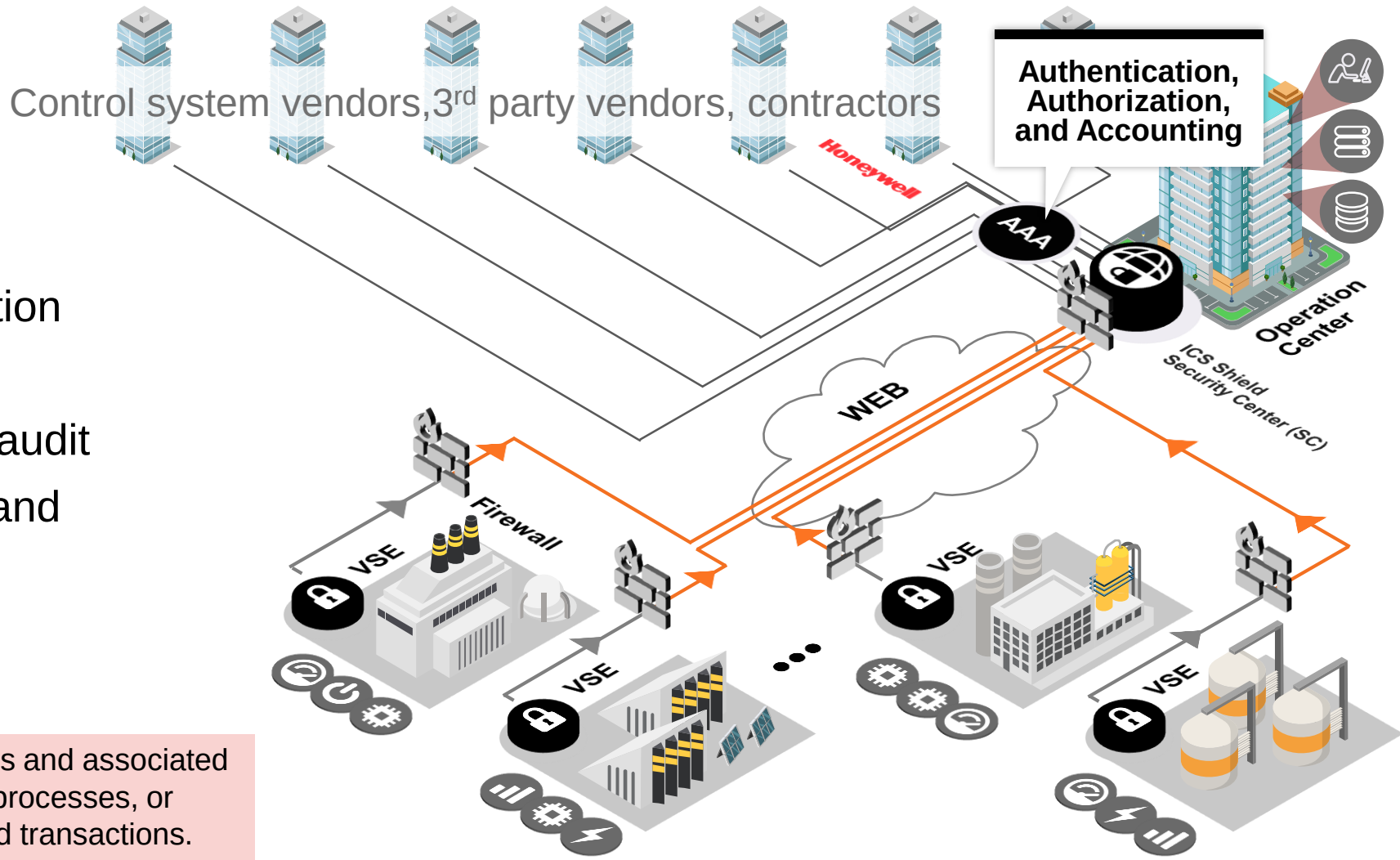
Improving assets reliability & safety

AAA Remote Access control

- Centralized authentication
- Granular privilege
- Accountability with full audit
- Real-time supervision and session termination
- Vault

- Files & Data transfer

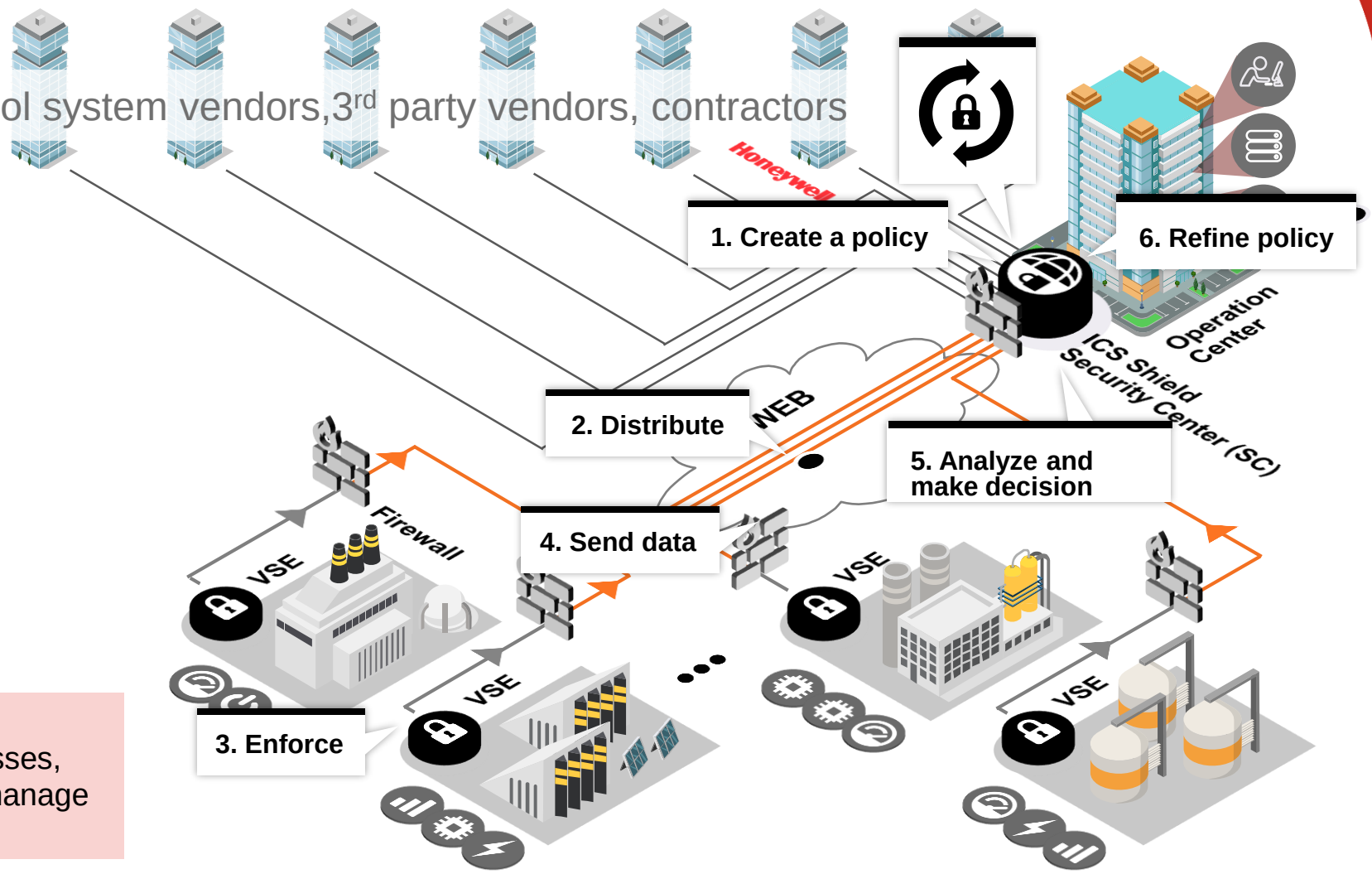
Access Control (AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.



Protect – Automate Plant-wide Security Policy

Minimize manual effort and human mistakes

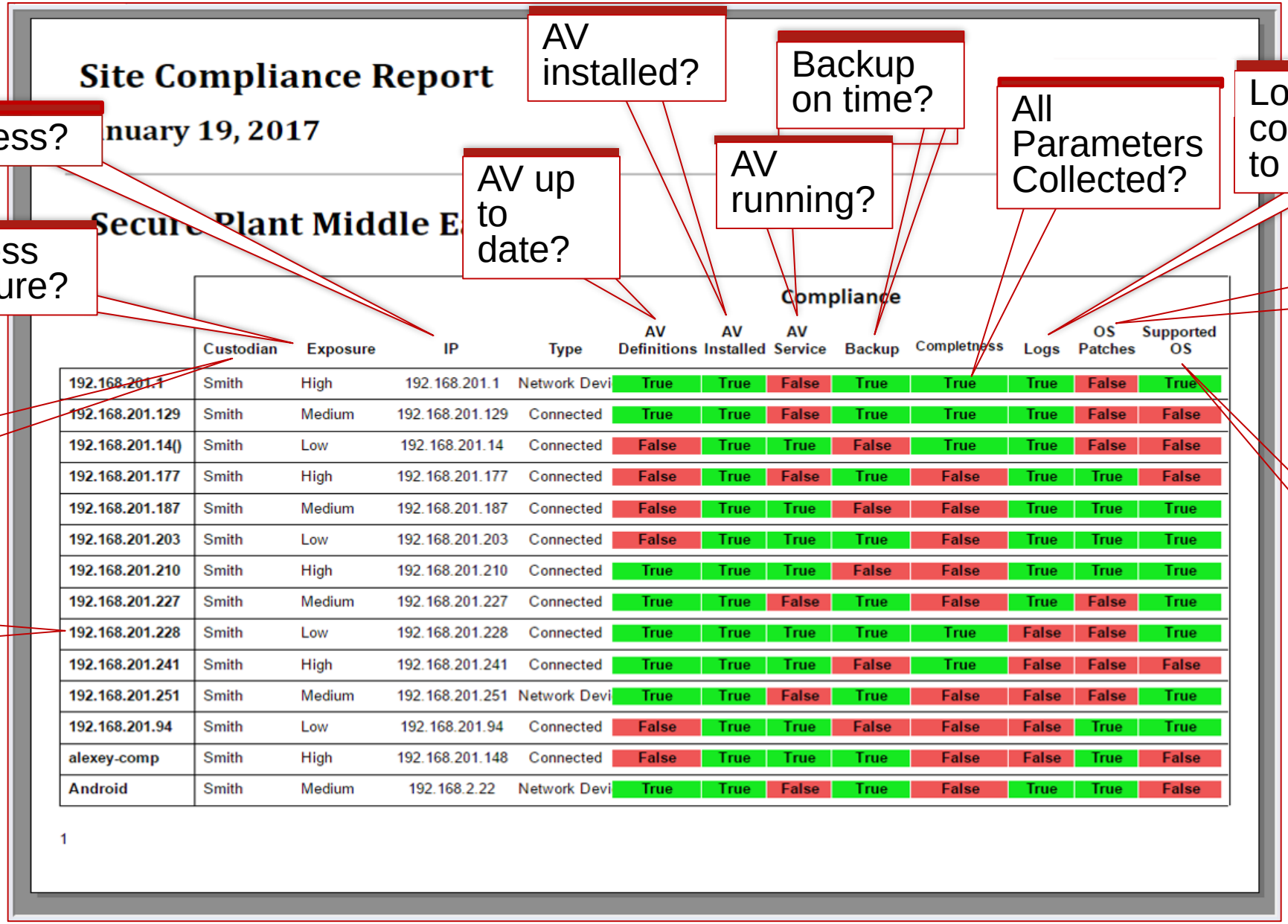
Improve security and compliance by standardizing on plant-wide policy



Information Protection Processes and Procedures (PR.IP): Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.

Honeywell
THE POWER OF CONNECTED

Plant Hardening Compliance Report



Site Compliance Report

nuary 19, 2017

Secur Plant Middle E

					Compliance							
	Custodian	Exposure	IP	Type	AV Definitions	AV Installed	AV Service	Backup	Completness	Logs	OS Patches	Supported OS
192.168.201.1	Smith	High	192.168.201.1	Network Devi	True	True	False	True	True	True	False	True
192.168.201.129	Smith	Medium	192.168.201.129	Connected	True	True	False	True	True	True	False	False
192.168.201.14()	Smith	Low	192.168.201.14	Connected	False	True	True	False	True	True	False	False
192.168.201.177	Smith	High	192.168.201.177	Connected	False	True	False	True	False	True	True	False
192.168.201.187	Smith	Medium	192.168.201.187	Connected	False	True	True	False	False	True	True	True
192.168.201.203	Smith	Low	192.168.201.203	Connected	False	True	True	True	False	True	True	True
192.168.201.210	Smith	High	192.168.201.210	Connected	True	True	True	False	False	True	True	True
192.168.201.227	Smith	Medium	192.168.201.227	Connected	True	True	False	True	False	True	False	True
192.168.201.228	Smith	Low	192.168.201.228	Connected	True	True	True	True	True	False	False	True
192.168.201.241	Smith	High	192.168.201.241	Connected	True	True	True	False	True	False	False	False
192.168.201.251	Smith	Medium	192.168.201.251	Network Devi	True	True	False	True	False	False	False	True
192.168.201.94	Smith	Low	192.168.201.94	Connected	False	True	True	False	False	False	True	True
alexey-comp	Smith	High	192.168.201.148	Connected	False	True	True	True	False	False	True	False
Android	Smith	Medium	192.168.2.22	Network Devi	True	True	False	True	False	True	True	False

1

Device IP address?

Device's business criticality/exposure?

Custodian?

Devices?

AV installed?

AV up to date?

Backup on time?

AV running?

All Parameters Collected?

Logs being collected and sent to the SIEM?

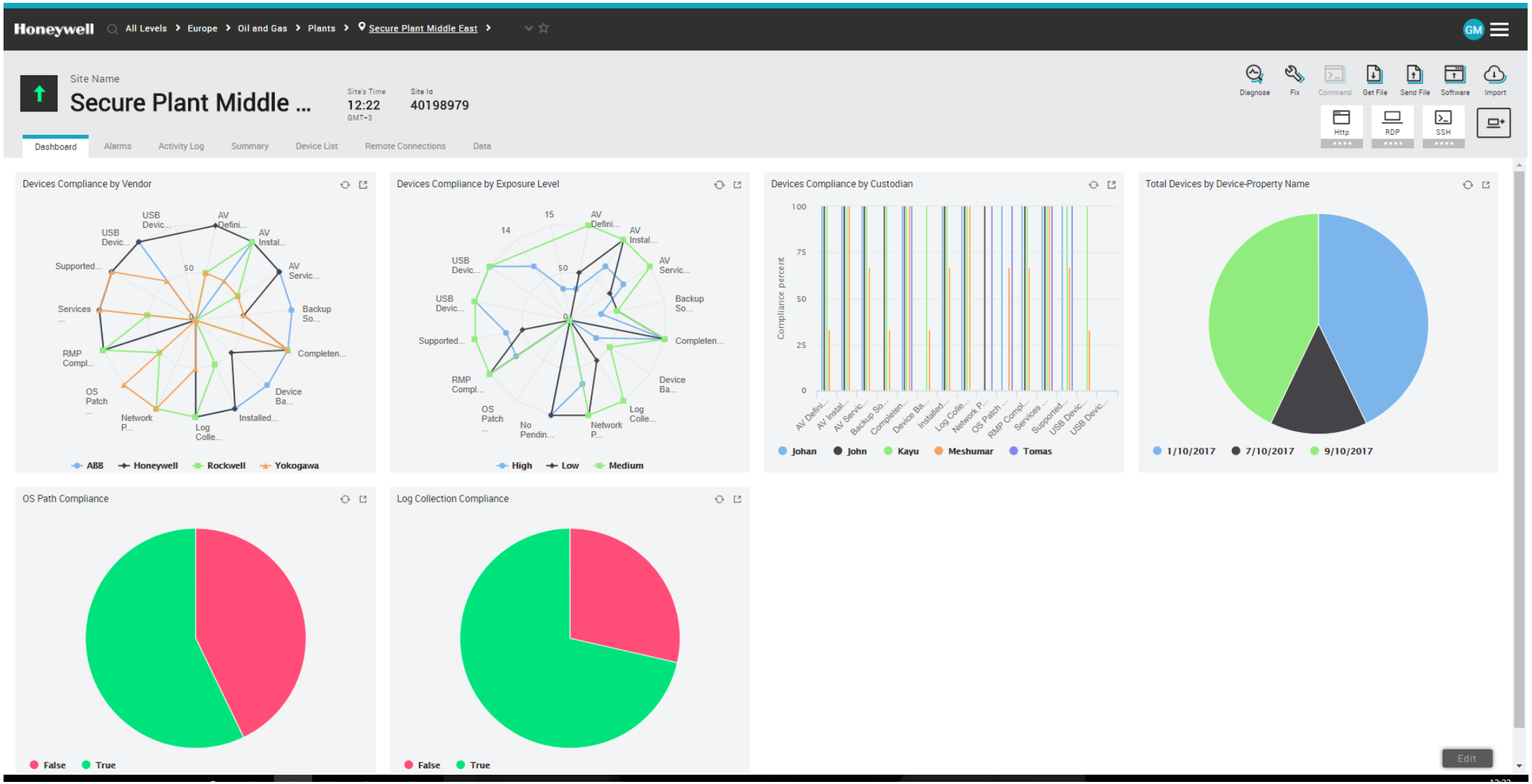
OS patches up to date?

OS still supported?

Honeywell

THE POWER OF CONNECTED

Compliance Dashboard

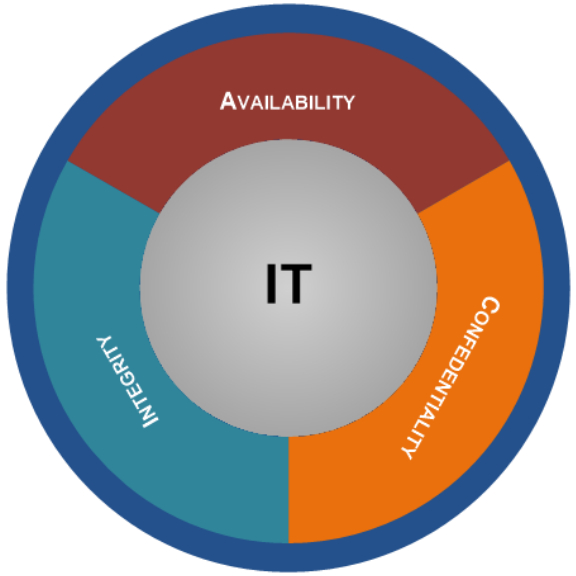


Agenda

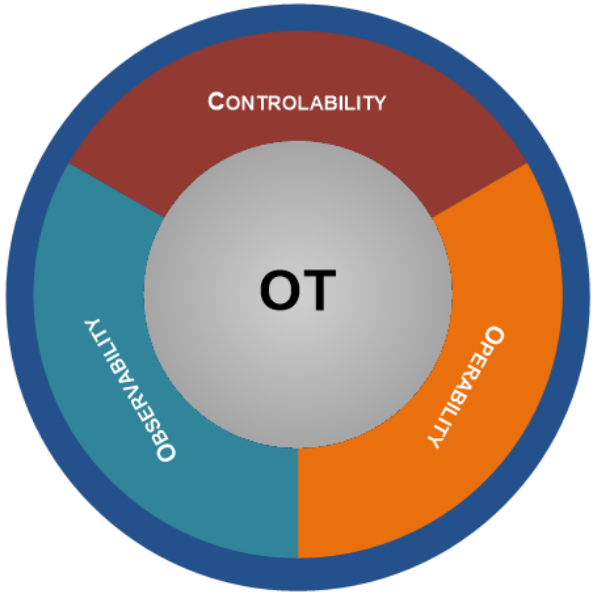
- Who is the Honeywell Industrial Cyber Security (H-ICS) Organization?
- NIS Directive
- USB Protection – SMX Presentation & Demo
- ICS Shield Presentation & Demo
- Blueprint Methodology – Assessments & Consultancy Services – Automation Security Program Approach

Honeywell

Industrial Cyber Security – A Custom Approach !



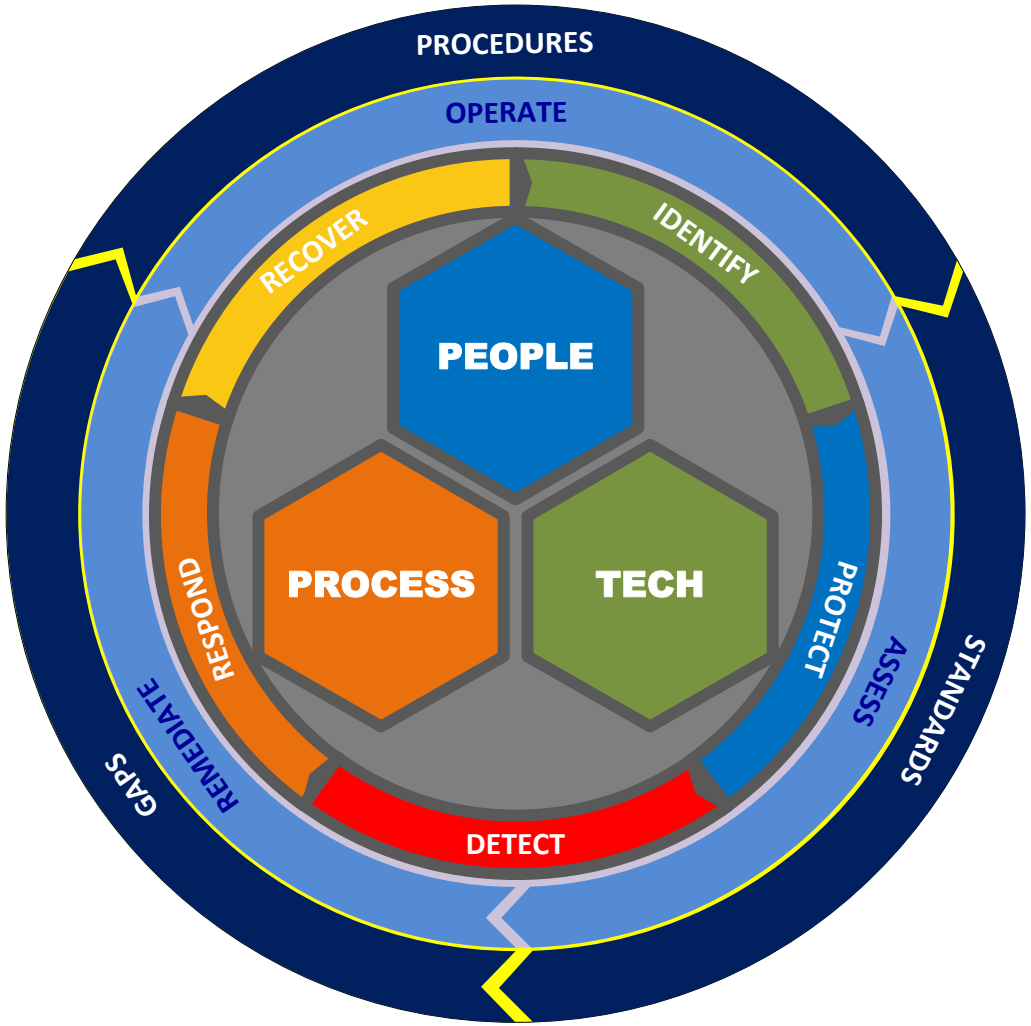
- IT Security is all about CIA triad.
- Failures result into Information Disclosure, Loss of Money, Intellectual Properties, Denial of access to Services,……etc.
- IT Systems are dynamic, continuously adopting newer and more secure cyber infrastructure
- Critical assets are concentrated in the network core (Server Farms)



- OT Security is concerned with Reliable and Safe operation of the Industrial Control Systems
- OT Cyber failures can result in **Injury**, Loss of **Life**, Loss of Property, Damaged Production, Damaged Equipment, Environmental Crisis, and Denial of access to **Critical Infrastructure**
- OT still uses legacy unsecured open protocols
- OT critical assets are distributed in the field (Logic Solvers – Control/Safety)

OT security builds on IT security technologies to ensure **SAFE, RELIABLE,** and **SECURE** operation of an ICS environment from Procurement to Retirement

Cyber Security Program Elements, Foundations, and Life Cycle



Elements

1- People
2- Technology
3- Process

Foundations

1- Identification
2- Protection
3- Detection
4- Response
5- Recovery

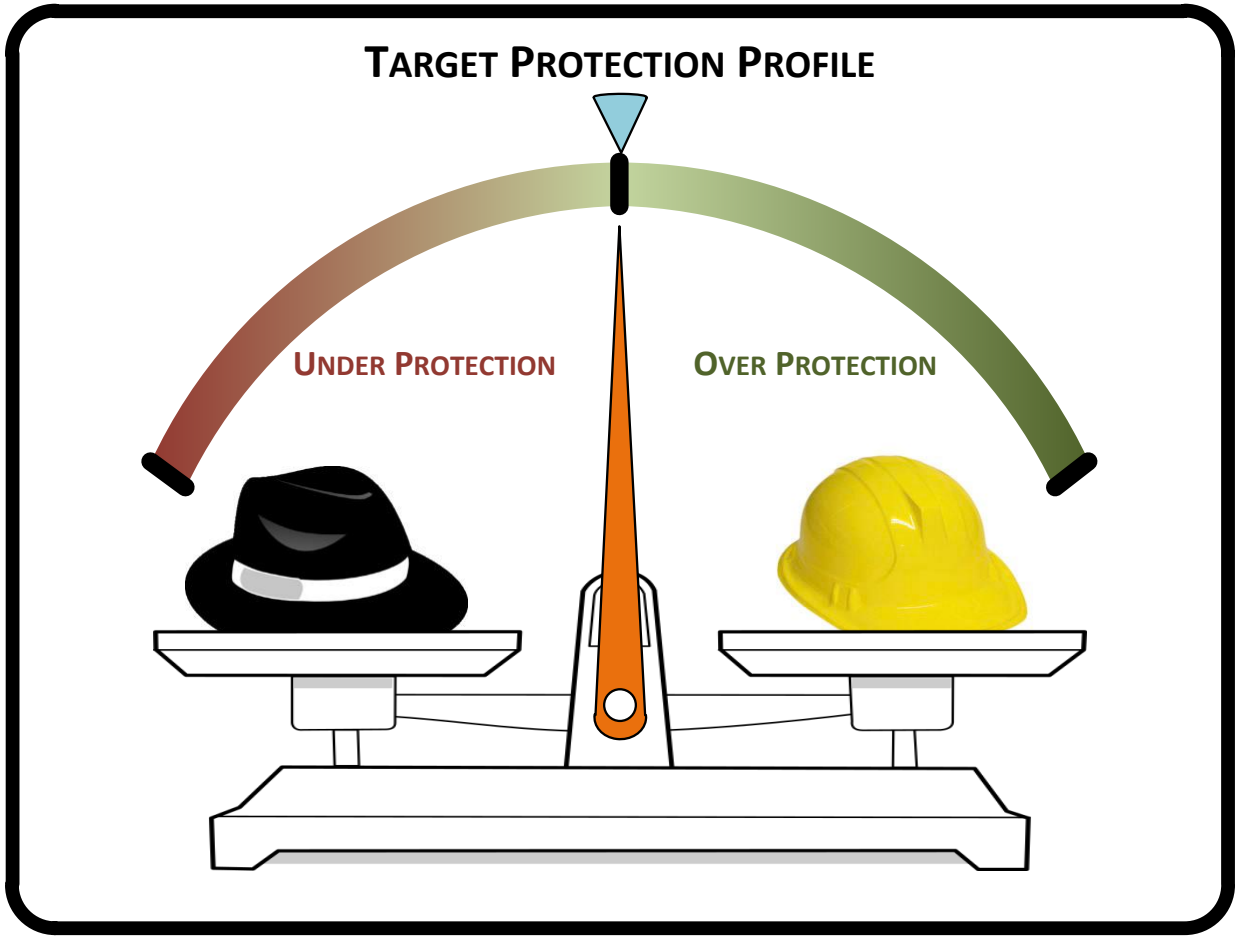
Life Cycle

1- Operate
2- Assess
3- Remediate

Honeywell
THE POWER OF CONNECTED

CYBER SECURITY FOUNDATIONS - IDENTIFICATION

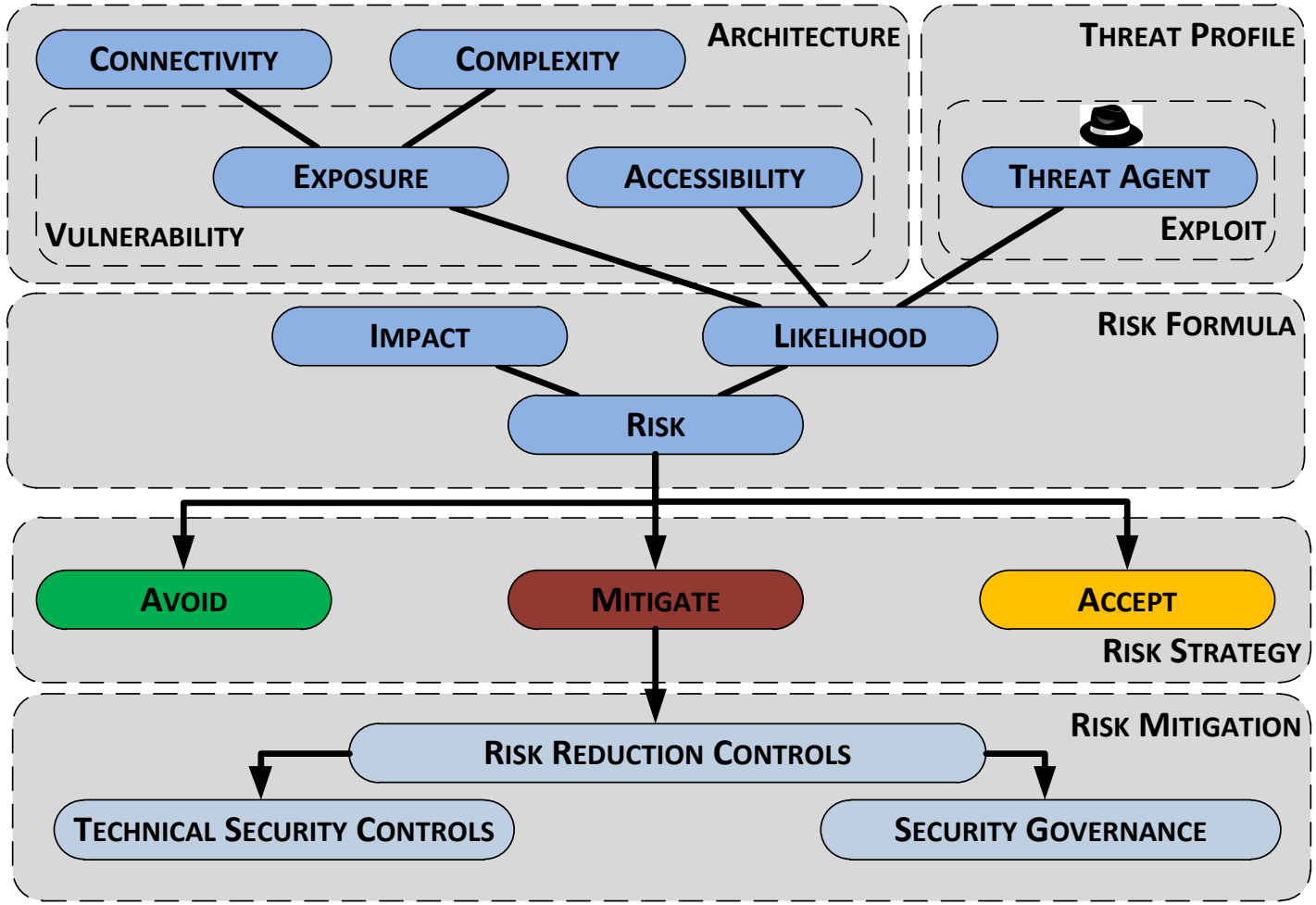
- The goal of the Identification is to identify the proper **TARGET PROTECTION PROFILE**



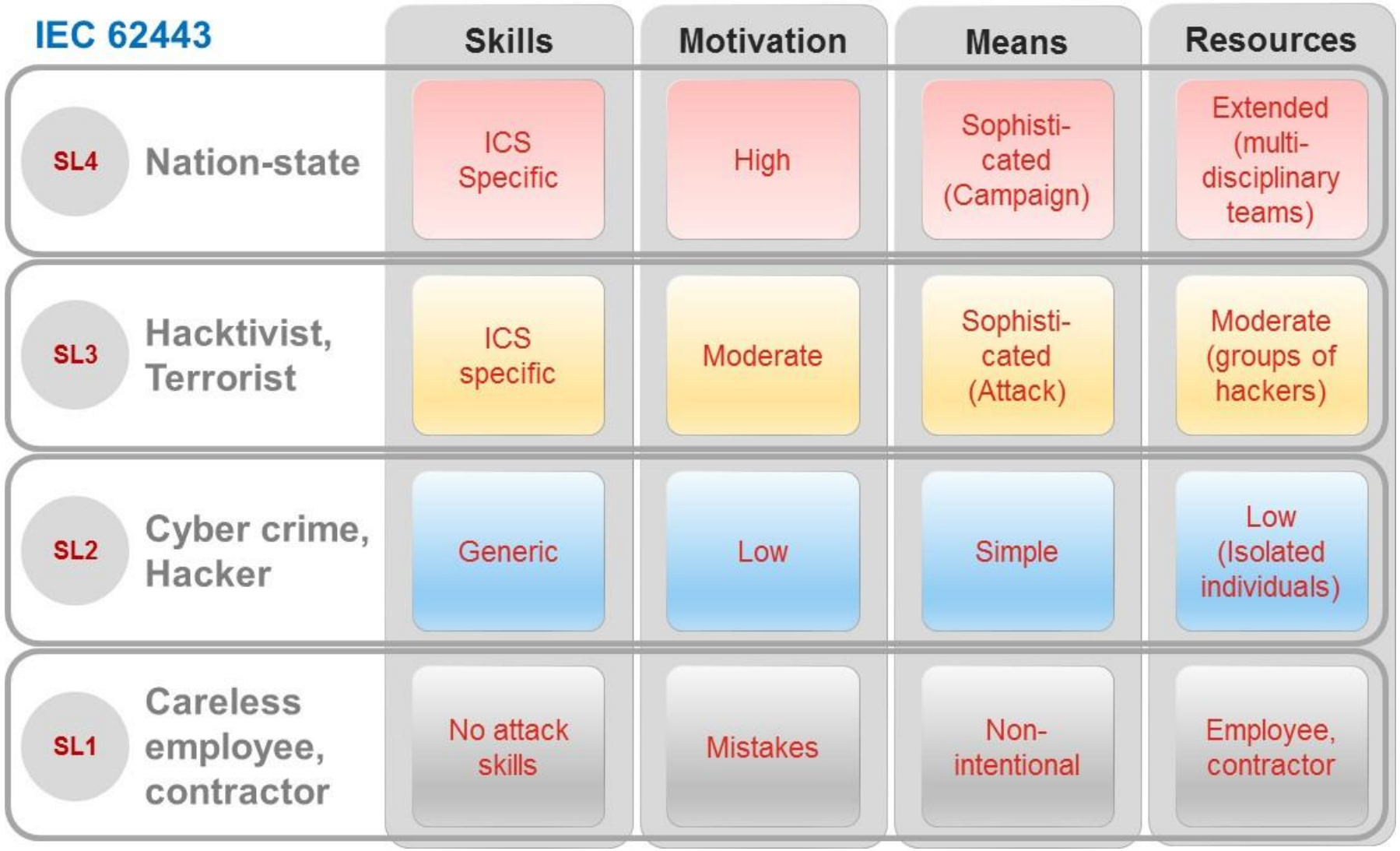
Honeywell
THE POWER OF CONNECTED

CYBER SECURITY FOUNDATIONS - IDENTIFICATION

- The **TARGET PROTECTION PROFILE** can be reached through the study of **RISK,** and through **Regulations**

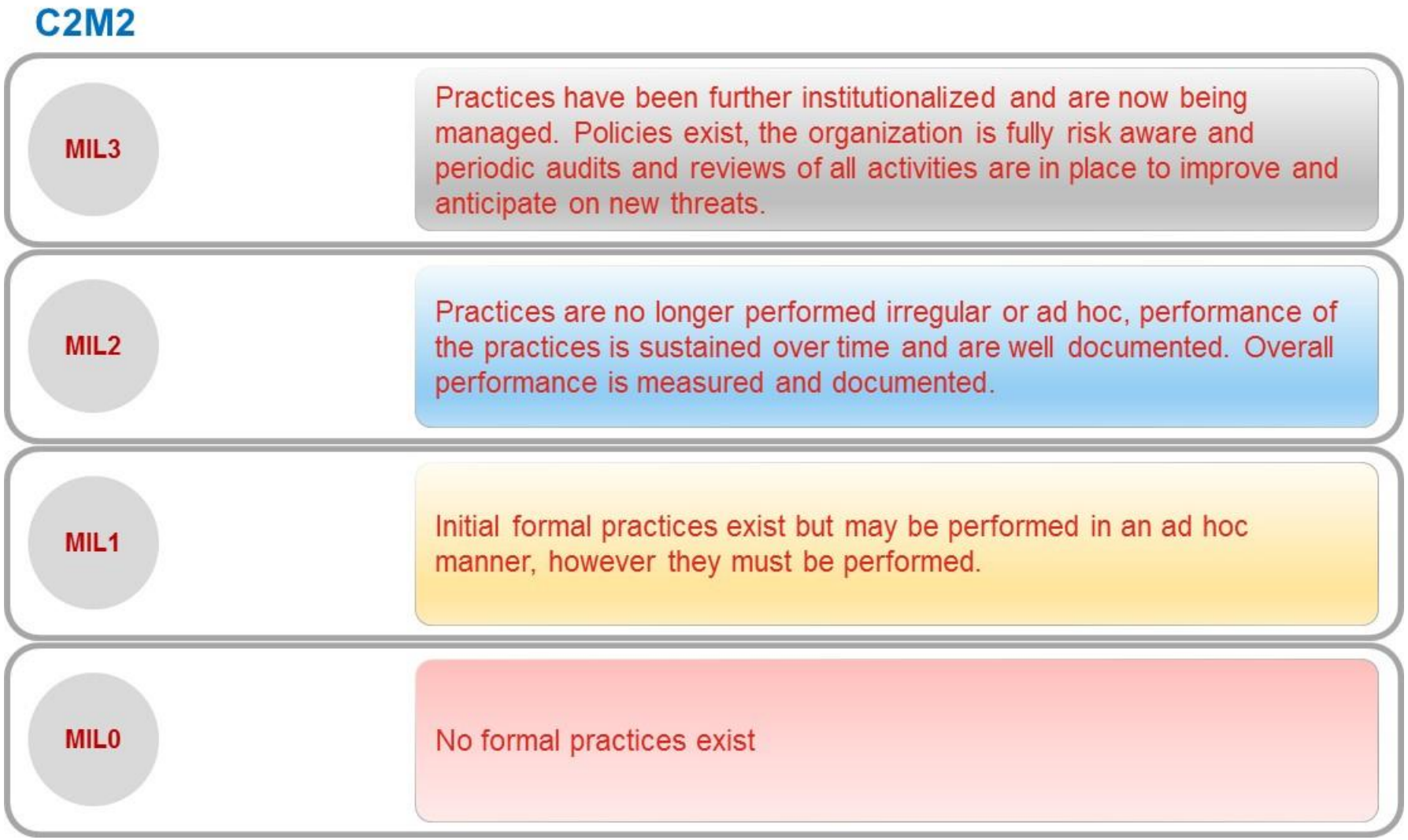


IEC 62443 Security Levels



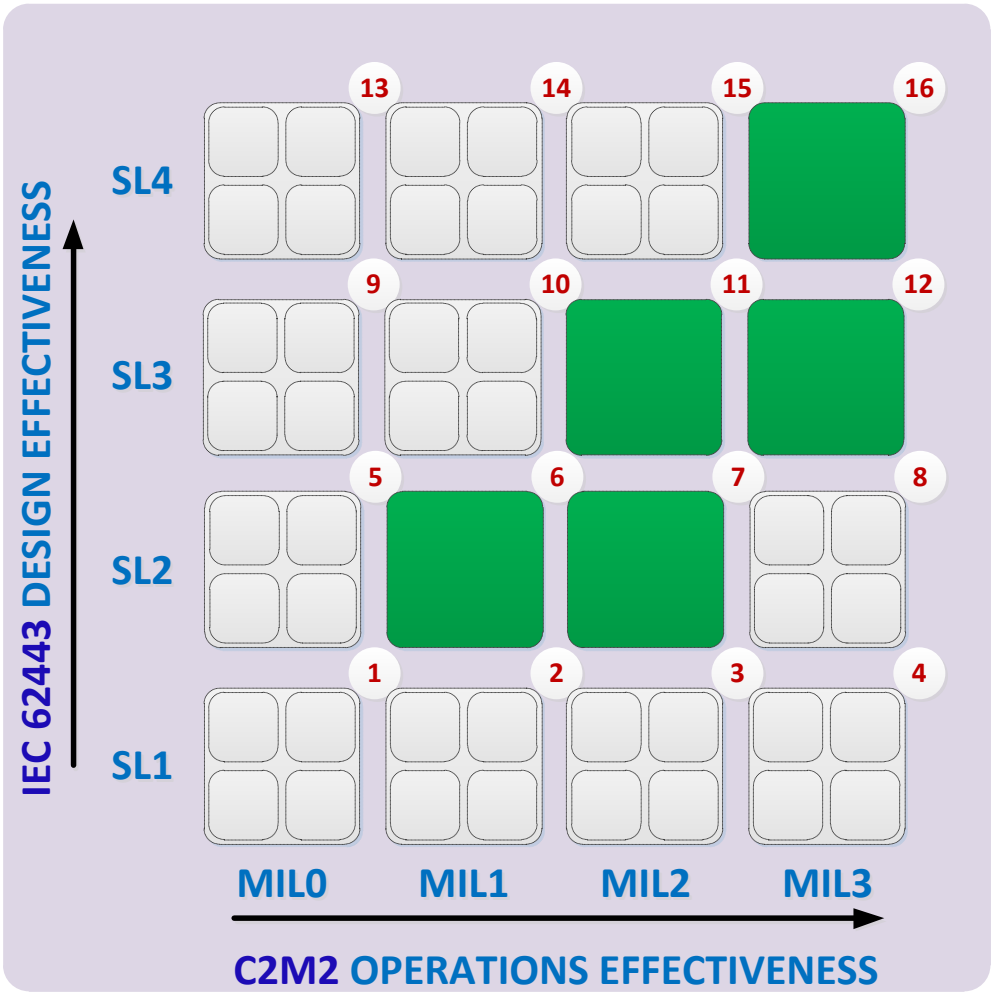
IEC 62443	Skills	Motivation	Means	Resources
SL4 Nation-state	ICS Specific	High	Sophisti-cated (Campaign)	Extended (multi-disciplinary teams)
SL3 Hacktivist, Terrorist	ICS specific	Moderate	Sophisti-cated (Attack)	Moderate (groups of hackers)
SL2 Cyber crime, Hacker	Generic	Low	Simple	Low (Isolated individuals)
SL1 Careless employee, contractor	No attack skills	Mistakes	Non-intentional	Employee, contractor

C2M2 Maturity Indicator Levels



Honeywell
THE POWER OF CONNECTED

PROTECTION PROFILE



Control Effectiveness = Design Effectiveness x Operations Effectiveness

Typical Protection Profile per Industry

Code	Market	SL1	SL2	SL3	SL4	MIL0	MIL1	MIL2	MIL3
1001	Refining process facilities		■	■				■	■
1102	O&G LNG terminals			■	■				■
1103	O&G processing			■					■
1104	O&G production – on-shore			■					■
1105	O&G production – off-shore			■					■
1108	O&G Marina – LNG IAS			■	■				■
1110	Gas To Liquid			■	■				■
1112	Production – Coal bed M		■	■				■	■
1114	Pipeline – Liquid		■	■				■	■
1115	Pipeline – Gas			■	■				■
1201	Pulp		■				■	■	
1202	Paper		■	■			■	■	■
1203	CWS		■				■	■	
1303	Utility Power			■	■			■	■
1401	Fertilizers		■	■				■	■
1403	Petrochemicals			■				■	■
1404	Plastics and fibers		■	■				■	■
1405	Specialty Chemicals			■	■			■	■
1406	Biofuels			■				■	■
1501	Alumina		■					■	
1502	Aluminum		■					■	
1503	Base materials		■	■				■	
1504	Cement		■				■		
1505	Coal & Coal Gasification		■	■				■	■
1506	Iron		■	■				■	
1509	Precious metals			■	■				■
1510	Steel making			■				■	■
1508	Other		■				■		

SL 2 REQUIREMENTS

SL 2 REQUIREMENTS

IAC																										
SR	1.1		1.2	1.3	1.4	1.5				1.6		1.7		1.8	1.9						1.10	1.11	1.12		1.13	
Capability	C1	C2	C5	C7	C9	C10	C11	C12	C13	C15	C16	C17	C18	C21	C22	C23	C24	C25	C26	C27	C29	C30	C31	C32	C33	C34
UC																										
SR	2.1			2.2	2.3			2.4			2.5	2.6	2.8									2.9	2.9	2.10	2.10	2.11
Capability	C35	C36	C37	C40	C42	C43	C44	C47	C48	C49	C51	C52	C54	C55	C56	C57	C58	C59	C60	C61	C62	C65	C66	C68	C69	C70
SI																										
SR	3.1	3.2	3.2	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9															
Capability	C75	C77	C78	C79	C81	C84	C86	C87	C88	C89	C93															
DC																										
SR	4.1	4.1	4.2	4.3																						
Capability	C95	C96	C98	C100																						
RDF																										
SR	5.1	5.1	5.1	5.2	5.2	5.3	5.4																			
Capability	C101	C102	C103	C106	C107	C110	C112																			
TRE																										
SR	6.1	6.2																								
Capability	C113	C115																								
RA																										
SR	7.1	7.1	7.2	7.3	7.3	7.4	7.5	7.6	7.7	7.8																
Capability	C116	C117	C119	C120	C121	C123	C124	C125	C127	C128																

SL2

Required Capabilities

SL 2 REQUIREMENTS

1. Architectural Design Requirements
   - Layered Network Architecture
     - Level 1.0 Real Time Control Network
     - Level 2.0 Supervisory Control Network
     - Level 2.5 Peer to Peer Supervisory control, and 3rd Party Supervisory control
     - Level 3.0 Advanced Control, and Infrastructure Management Network
     - Level 3.5 DMZ Network

SL 2 REQUIREMENTS

2. Technical Security Controls

- Use of Active Directory with Honeywell High Security Policy
- Malicious Code Protection Mechanism:
    1) Network based Firewalls
        - Level 1.0 to Level 2.0 boundary
        - Level 3.0 to Level 3.5 boundary
        - Level 3.5 to Level 4.0 boundary
    2) Intrusion Detection System at Level 2.5 to Level 3.0 boundary
    3) Access Control Lists at Level 2.5 to Level 3.0 boundary
    4) Host Based Firewalls
    5) Managed Antivirus deployment with continuous updates
    6) Patch Management Process / Mechanism
- Use of portable storage media protection mechanism
- Managed Backup and Recovery Mechanism
- Hardening of Network nodes and Networking Protocols
- Hardening of End Nodes

SL 2 REQUIREMENTS

3. Cyber Security Situational Awareness
   - Capability to continuously monitor all security mechanisms performance!
   - Honeywell Risk Manager:
     - Network Security (Detection of un authorized devices, un-shut interfaces,…etc)
     - End Node Security Monitoring (AV, Security Logs, …. Etc)
     - Patch Management Monitoring
     - Backup and Recovery

HONEYWELL SL 2 SOLUTIONS

Solutions for Mandatory Controls

1. Honeywell High Security Domain Policies
2. PaloAlto DMZ Firewall
3. McAfee IPS
4. McAfee ePO and Virus Scan Enterprise
5. Honeywell Secure Media Exchange (SMX)
6. Experion Backup and Recovery
7. Honeywell Risk Manager

Solutions for Optional Controls (Manage)

1. Honeywell Remote Managed Services:
    a. Secure Connect
    b. Antivirus Updates
    c. OS Patch Updates

SL 3 REQUIREMENTS

SL 3 Requirements

IAC																																
SR	1.1			1.2		1.3		1.4	1.5					1.6		1.7			1.8	1.9							1.10	1.11	1.12		1.13	
Cabability	C1	C2	C3	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31	C32	C33	C34

UC																																					
SR	2.1				2.2		2.3				2.4					2.5	2.6	2.7	2.8											2.9			2.10		2.11		2.12
Cabability	C35	C36	C37	C38	C40	C41	C42	C43	C44	C45	C46	C47	C48	C49	C50	C51	C52	C53	C54	C55	C56	C57	C58	C59	C60	C61	C62	C63	C64	C65	C66	C67	C68	C69	C70	C71	C73

SI																	
SR	3.1		3.2				3.3		3.4		3.5	3.6	3.7	3.8			3.9
Cabability	C75	C76	C77	C78	C79	C80	C81	C82	C84	C85	C86	C87	C88	C89	C90	C91	C93

DC					
SR	4.1		4.2		4.3
Cabability	C95	C96	C98	C99	C100

RDF											
SR	5.1				5.2				5.3		5.4
Cabability	C101	C102	C103	C104	C106	C107	C108	C109	C110	C111	C112

TRE			
SR	6.1		6.2
Cabability	C113	C114	C115

RA													
SR	7.1			7.2	7.3			7.4	7.5	7.6		7.7	7.8
Cabability	C116	C117	C118	C119	C120	C121	C122	C123	C124	C125	C126	C127	C128

SL3
Required Capabilities

SL3 requiems include all applicable SL2 requirements in addition to all SL3 Requirements Enhancements.

SL 3 REQUIREMENTS

1. Architectural Design Requirements
   - Additional Segmentation requirements:
     1) Use of security zones rather than functional network levels leading to a network level being segmented into multiple security zones and sub-zones
     2) Physical Segmentation of Process Controllers and Safety Controllers security zones
     3) Physical Segmentation of Critical and Not Critical control security zones
     4) Logical/Physical segmentation of Level 3 Automation, Infrastructure Management and Security Management security zones
     5) Logical/Physical segmentation of the DMZ Interfacing, Infrastructure Management, and Security Management security zones

SL 3 REQUIREMENTS

2. Technical Security Controls
   - Additional Malicious Code Protection Mechanisms:
     1) Next Generation Firewalls
        - Level 1.0 to Level 2.0 boundary
        - Level 2.5 to Level 3.0 boundary
        - Level 3.0 to Level 3.5 boundary
        - Level 3.5 to Level 4.0 boundary
     2) Intrusion Prevention System
        - Level 2.5 to Level 3.0 boundary
        - Level 3.0 to Level 3.5 boundary
     3) Application Whitelisting
   - Network Configuration Management
   - Performance Monitoring
   - Log Management and Storage (SIEM)
   - Security Events and Incidents Management (SIEM)
   - Two Factor Authentication for Remote Access
   - Active Directory Segregation

SL 3 REQUIREMENTS

3. Cyber Security Situational Awareness
   - Capability to continuously monitor all security mechanisms performance!
   - Honeywell Risk Manager:
     - Network Security (Detection of un authorized devices, un-shut interfaces,…etc)
     - End Node Security Monitoring (AV, Security Logs, …. Etc)
     - Patch Management Monitoring
     - Backup and Recovery
   - Periodic SL3 Security Auditing for Design and Implementation

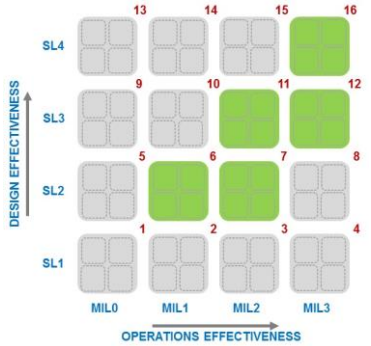
H-ICS Services & Assessments

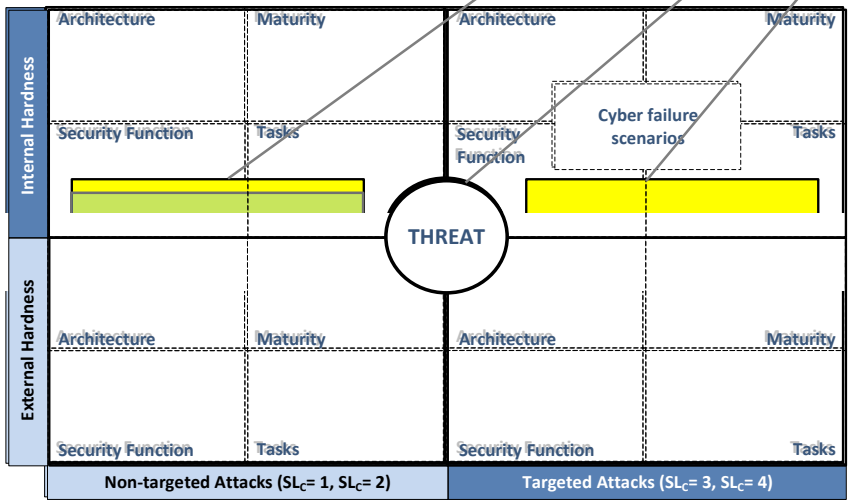
Security Assessment:

- Design check (Design gaps, technology gaps)
- Implementation check (Configuration gaps)
- Vulnerability check (Software gaps)
- Mitigation plan

Profiling:

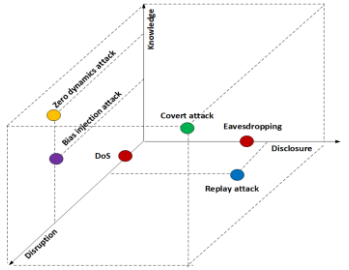
- Threat profile
- Maturity evaluation
- Design evaluation
- Create Z&C diagram
- Determine zone risk
- Mitigation steps
- Sets a common goal





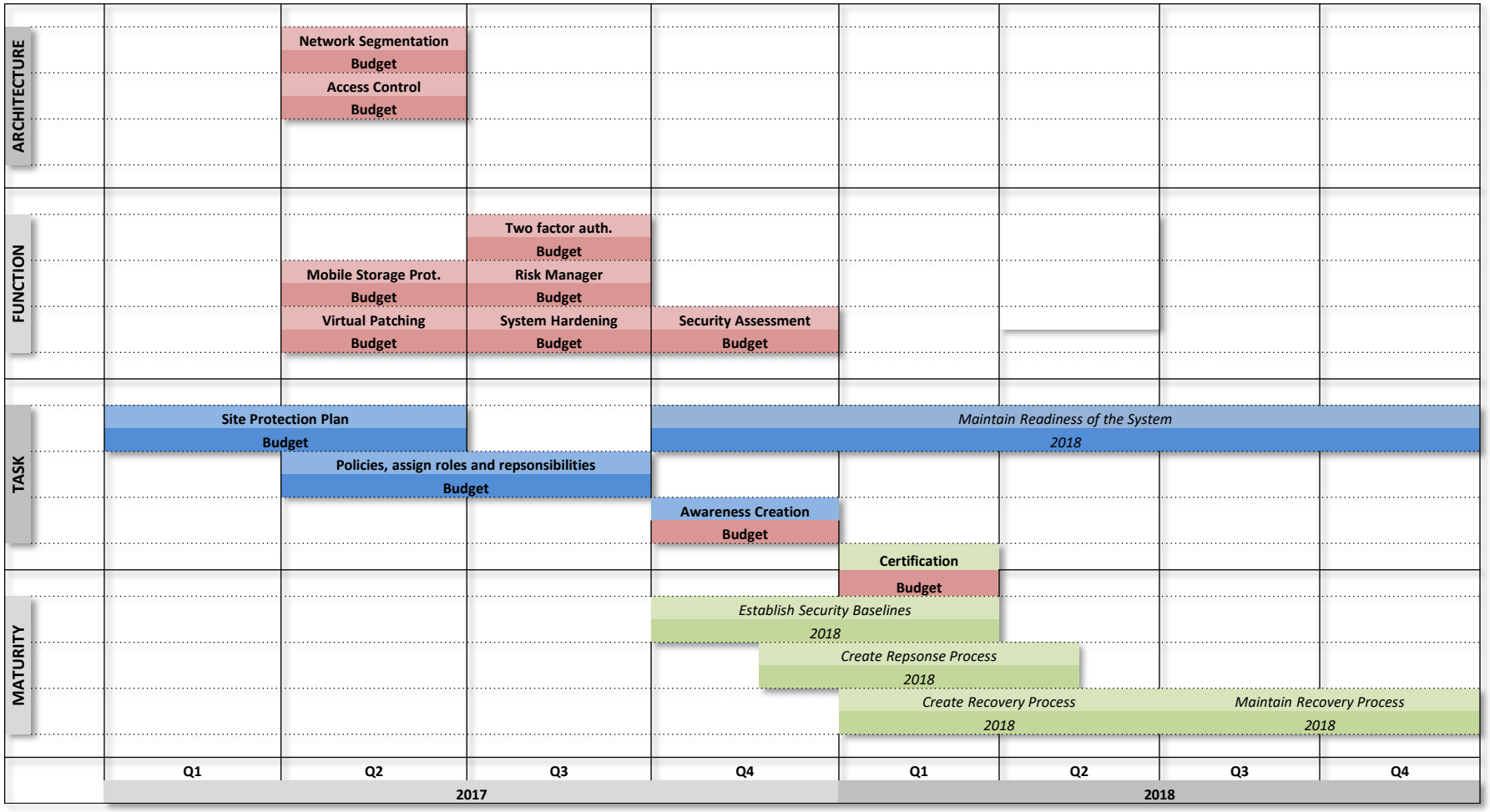
Threat Risk Assessment:

- Identification of cyber failure scenarios
- Construction of attack trees to accomplish scenario
- Analysis of functional separation
- Analysis of trust relationships
- Analysis of attack space (protection, detection)
- Determine risk per scenario for prioritization purposes
- Mitigation plan



Honeywell

Sample Automation Security Roadmap



Honeywell

Cybersecurity Roadmap Budget Breakdown

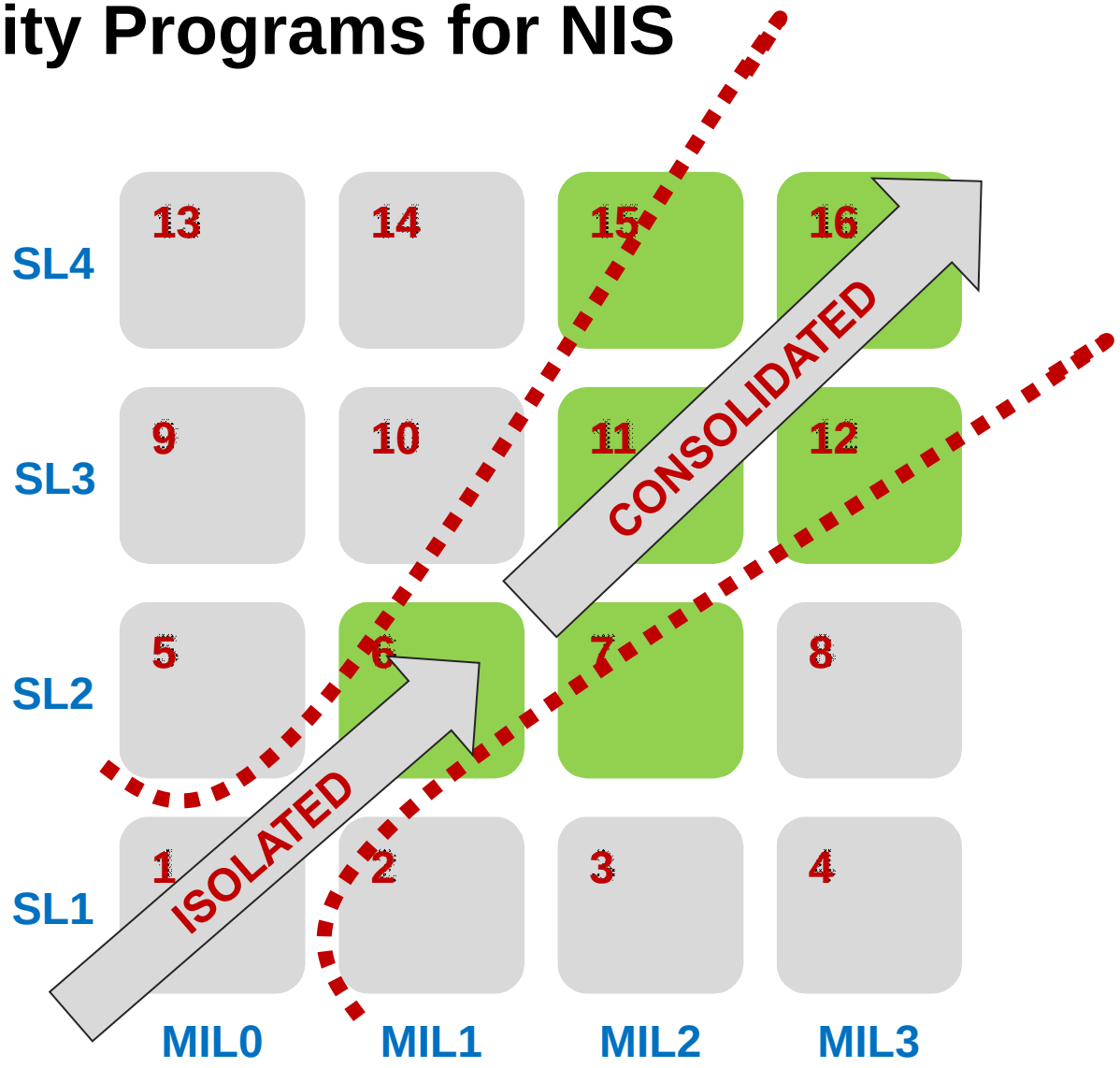
		Item Description	Q1	Q2	Q3	Q4
Step	0	Technical Project Management	X €	X €	X €	X €
Step	1	Site Protection Plan	Budget			
Step	2	Network Segmetnation & Access Ctrl		Budget		
Step	3	Mobile Storage Prot.		Budget		
Step	4	Virtual Patching		Budget		
Step	5	Two factor auth.			Budget	
Step	6	Risk Manager			Budget	
Step	7	Policies, assign roles and repsonsibilities			Budget	
Step	8	Awareness Creation				Budget
Step	9	System Hardening			Budget	
Step	10	Security Assessment				Budget
			Total Q1	Total Q2	Total Q3	Total Q4

Honeywell

Sample Tasks Framework

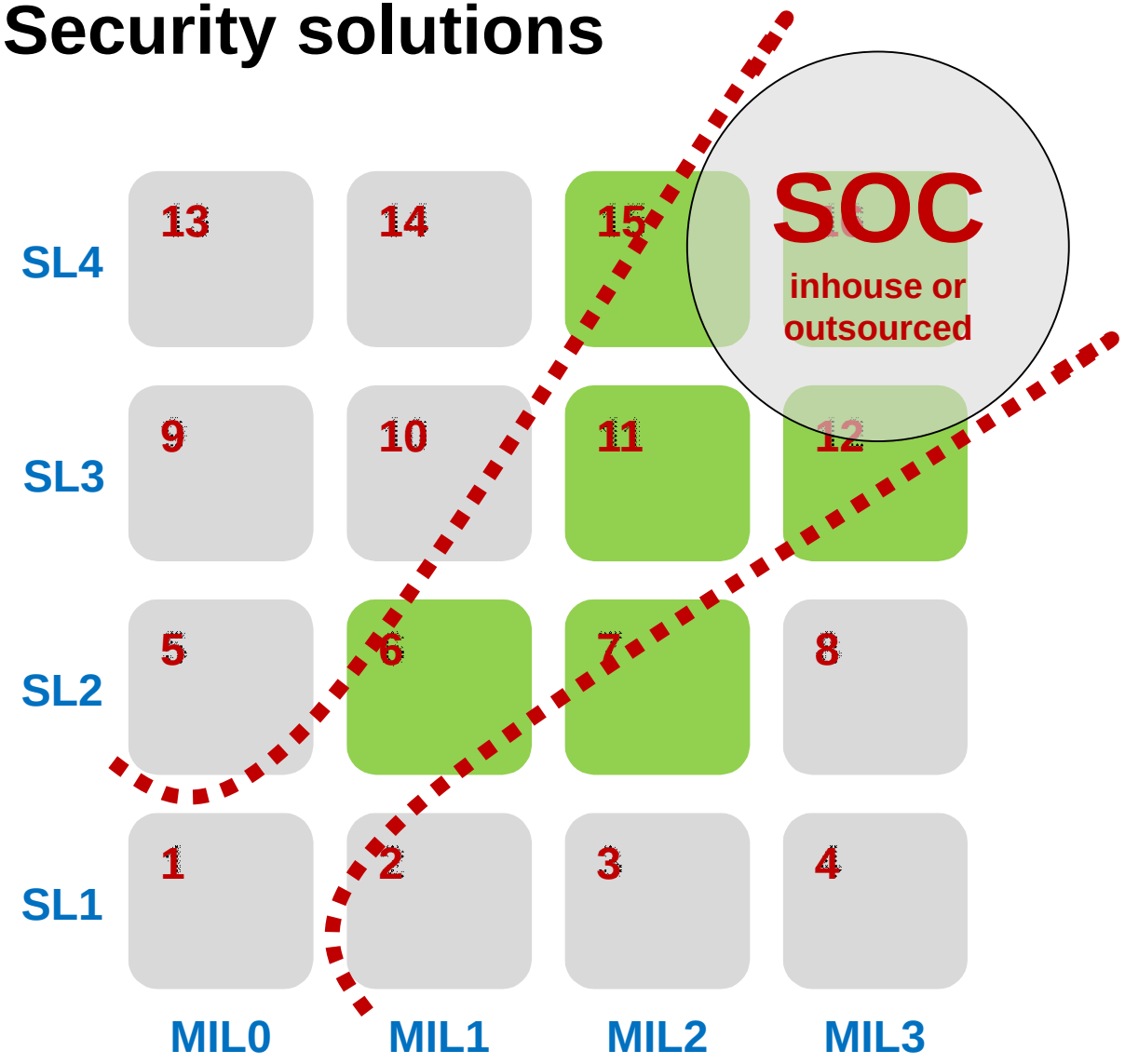
Identify	• Automated asset discovery and inventory (TRACE, Risk Manager) • Assessment Services	• Real-time multisite Risk Score (Risk Manager and Enterprise Risk Manager) • MSS/ICS Shield	
Protect	• Automated patch + AM delivery • SMX for Media • ATIX	• MSS/ICS Shield • ICS Shield for SOC • Endpoint Protection (AV, AWL) • Secure remote access & data transfer	
Detect	• Honeywell RM • SMX • Honeywell ERM • SIEM • Honeywell ATIX	• Monitor and log collection • Scan ports & services against whitelists/blacklists	• Compliance reporting • Risk based Reporting
Respond	• Consultancy services for Policies and procedures • Honeywell ICS Shield • Hosted SOC remotely or in Customer head office		
Recover	• Multi-site file transfer infrastructure for backup/restore • EBR • Disaster Recovery Program		

OT Cyber Security Programs for NIS



Manageability requires a S.M.A.R.T. and holistic approach

OT sustainable Security solutions



Manageability requires a S.M.A.R.T. and holistic approach

Takeaway Recommendations To Keep Secure

- Cyber Security will never be “SOLVED” but can & should be “MANAGED”
- Cyber Security now a scientific discipline
- Raise awareness in your organization

Benefits of Cyber Managed Program

1. Define a path forward
2. Assess your multi-year investment
3. Offer sustainable security
4. Benchmark your critical ICS

Honeywell
THE POWER OF CONNECTED

Honeywell is building a smarter, safer,
and more sustainable world

THAT'S THE POWER OF **CONNECTED**
THAT'S THE POWER OF **HONEYWELL**

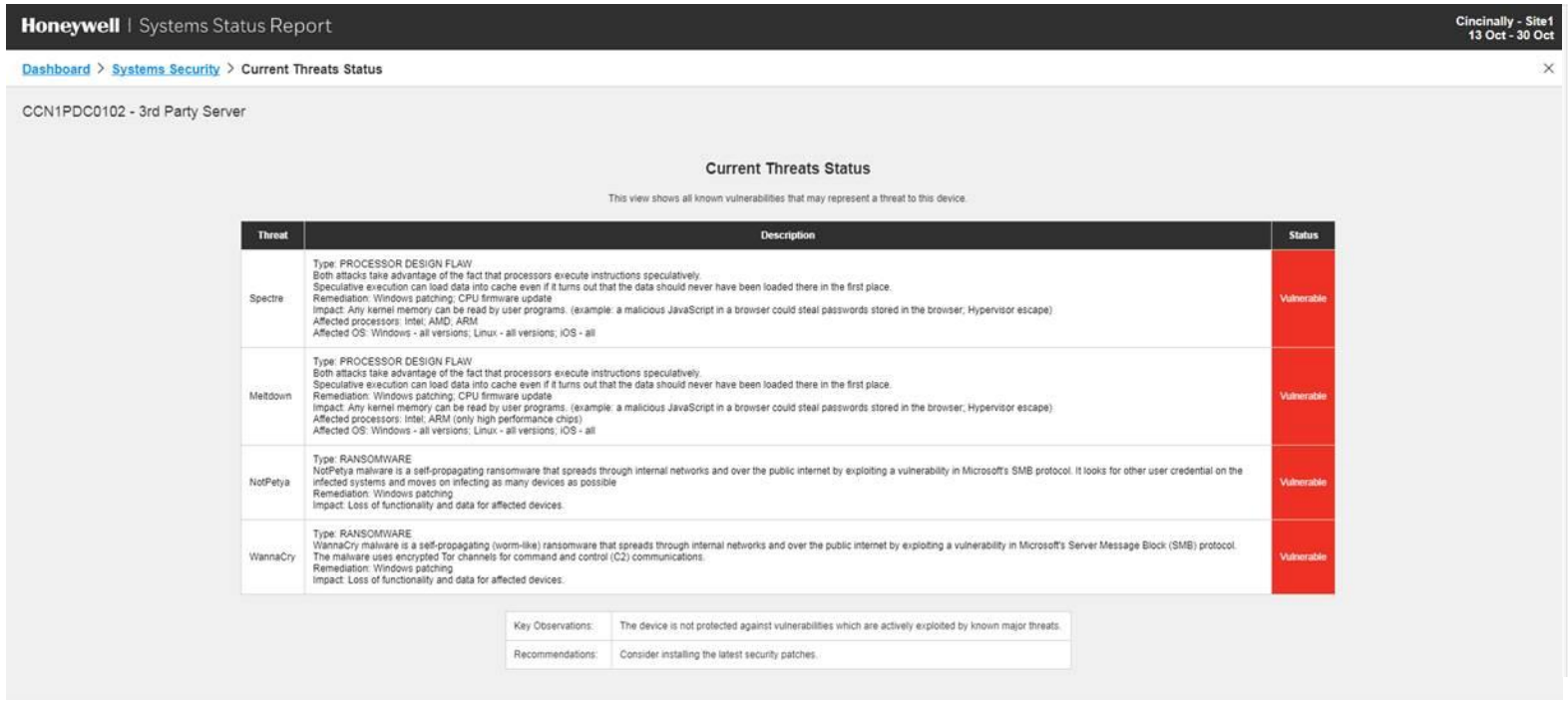
Connected Aircraft • Connected Automobile • Connected Home • Connected Building
Connected Plant • Connected Supply Chain • Connected Worker

Honeywell

THE POWER OF **CONNECTED**

Honeywell Recommendations & Statements

- Information about Vulnerabilities / Malware / Ransomware you can find under:
  https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx
- On Spectre & Meltdown - TRITON:
  - Application Whitelisting (AWL): provides best protection
    - Only the allowed „whitelisted“ Applications can execute
    - Potential Malware, which could exploit the vulnerabilities, are excluded in the first place.
  - MSS/HSSN Performance Report now includes „Current Treat Status“ – for each monitored device



Honeywell | Systems Status Report — Cincinally - Site1, 13 Oct - 30 Oct

Dashboard > Systems Security > Current Threats Status

CCN1PDC0102 - 3rd Party Server

Current Threats Status

This view shows all known vulnerabilities that may represent a threat to this device.

Threat	Description	Status
Spectre	Type: PROCESSOR DESIGN FLAW Both attacks take advantage of the fact that processors execute instructions speculatively. Speculative execution can load data into cache even if it turns out that the data should never have been loaded there in the first place. Remediation: Windows patching; CPU firmware update Impact: Any kernel memory can be read by user programs. (example: a malicious JavaScript in a browser could steal passwords stored in the browser; Hypervisor escape) Affected processors: Intel; AMD; ARM Affected OS: Windows - all versions; Linux - all versions; iOS - all	Vulnerable
Meltdown	Type: PROCESSOR DESIGN FLAW Both attacks take advantage of the fact that processors execute instructions speculatively. Speculative execution can load data into cache even if it turns out that the data should never have been loaded there in the first place. Remediation: Windows patching; CPU firmware update Impact: Any kernel memory can be read by user programs. (example: a malicious JavaScript in a browser could steal passwords stored in the browser; Hypervisor escape) Affected processors: Intel; ARM (only high performance chips) Affected OS: Windows - all versions; Linux - all versions; iOS - all	Vulnerable
NotPetya	Type: RANSOMWARE NotPetya malware is a self-propagating ransomware that spreads through internal networks and over the public internet by exploiting a vulnerability in Microsoft's SMB protocol. It looks for other user credential on the infected systems and moves on infecting as many devices as possible Remediation: Windows patching Impact: Loss of functionality and data for affected devices.	Vulnerable
WannaCry	Type: RANSOMWARE WannaCry malware is a self-propagating (worm-like) ransomware that spreads through internal networks and over the public internet by exploiting a vulnerability in Microsoft's Server Message Block (SMB) protocol. The malware uses encrypted Tor channels for command and control (C2) communications. Remediation: Windows patching Impact: Loss of functionality and data for affected devices.	Vulnerable

Key Observations:	The device is not protected against vulnerabilities which are actively exploited by known major threats.
Recommendations:	Consider installing the latest security patches.

Device	Model	Antivirus Software Compliance	Antivirus Definition Updates	Antivirus Errors	PC Login Alerts	USB Status	Guest Account Status	Current Threats Status	Security Patches	Non Security Patches	Experion Backup and Restore	Adobe Reader
CCN1ESC0105	ES-C	✓	✗	✓	✓	✓	✓	✗	✓	!	✓	
CCN1ESC0106	ES-C	✓	✗	✓	✓	✓	✓	✗		✗	✓	!
CCN1ESC0107	ES-C	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1ESC0108	ES-C	✓	✗	✓	✓	✓	✓	✗		✗	✓	!
CCN1ESC0109	ES-C	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1ECT0101	ES-CE	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1ECT0102	ES-CE	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	!
CCN1ECT0103	ES-CE	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1EST0101	ES-T	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1EST0102	ES-T	✓	✗	✓	✓	✓	✓	✓	!	✗	✓	!
CCN1EST0103	ES-T	✓	✗	✓	!	✓	✓	✓	!	✗	✓	!
CCN1EST0104	ES-T	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	!
CCN1EST0105	ES-T	✓	✗	✓	✓	✓	✓	!	!	✗	✓	!
CCN1EST0106	ES-T	✓	✗	✓	✓	✓	✓	✗				
CCN1EST0107	ES-T	✓	✗	✓	✓	✓	✓	✗				✓
CCN1EST0108	ES-T	✓	✗	✓	✓	✓	✓	✗				

Honeywell
THE POWER OF CONNECTED