



Cyber security - why and how

Frankfurt, 14 June 2018

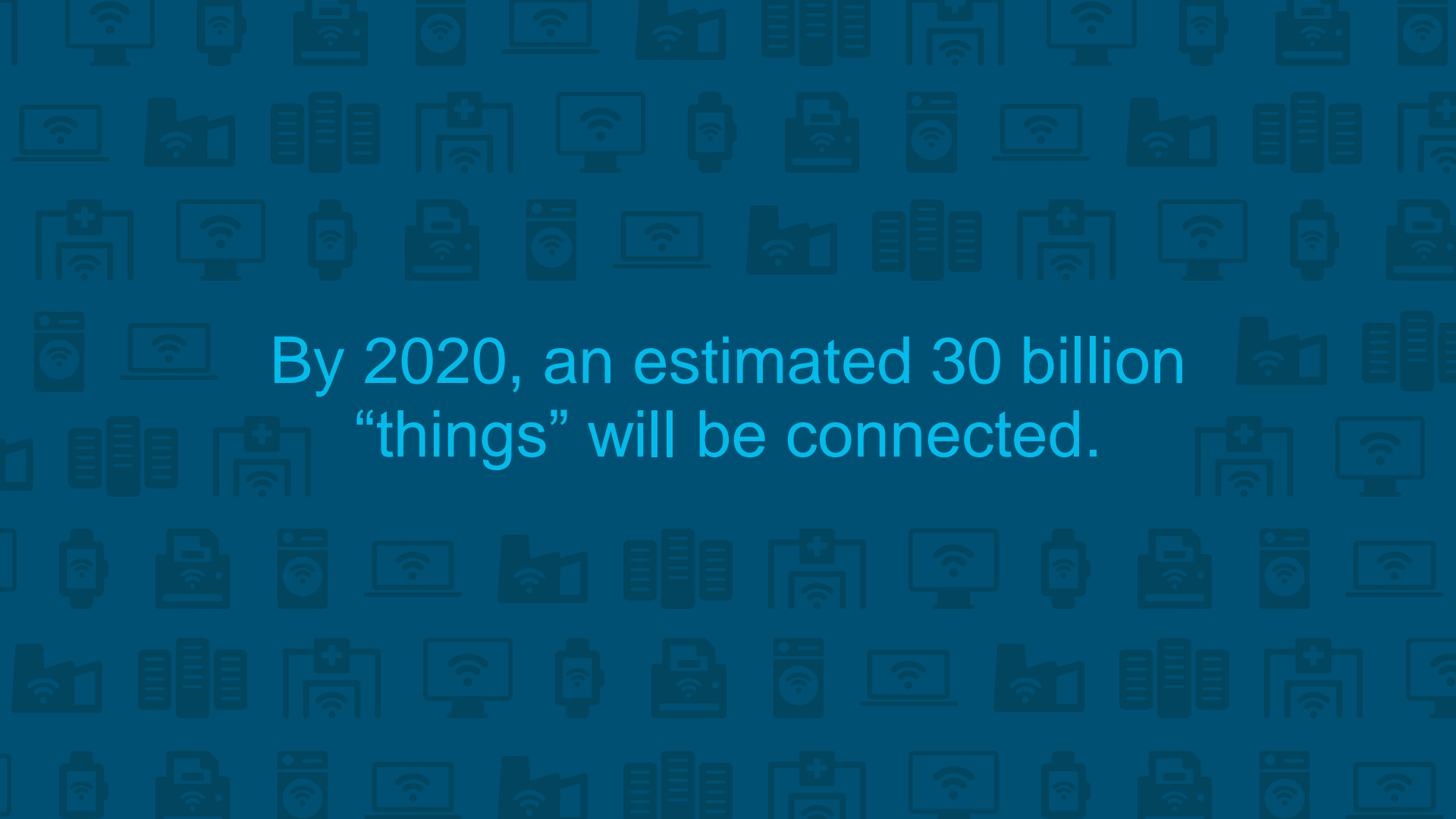
ACHEMA

Security between IT and OT Protecting the Promise of the Internet of Things

Disruption is happening everywhere.
Manufacturing

A photograph of a large industrial factory floor, overlaid with a semi-transparent blue filter. The scene is filled with complex machinery, including several large orange robotic arms (likely KUKA) positioned over workstations. In the foreground, there are conveyor belts with rollers. The background shows the high ceiling of the factory with a network of steel beams and lighting fixtures. The overall atmosphere is one of a busy, modern manufacturing environment.

**Operational Excellence
and Safety Are *Everything***

The background of the slide is a dark blue color with a repeating pattern of white icons representing various Internet of Things (IoT) devices. These icons include smartphones, laptops, desktop monitors, smart speakers, and other connected hardware, all arranged in a grid-like fashion.

By 2020, an estimated 30 billion
“things” will be connected.

Security challenges in the IoT



New to cybersecurity



Insufficient resources

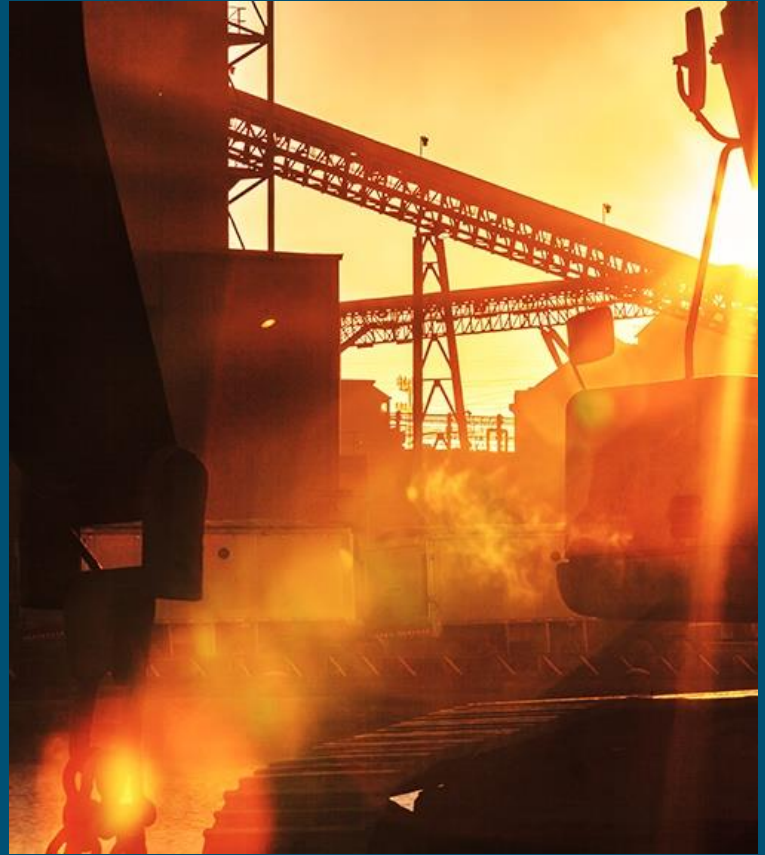


Market pressures

But what happens when
there's a breach?

BSI warns of cyber attacks
targeted towards German
power grid — tagesschau.de — 13
June 2018

Equipment damage



The simple fact is that enterprises are exposed now... we can't wait for others to build in cybersecurity.

Cisco has invented that solution

Cisco IoT Threat Defense



Visibility and
analysis



Segmentation



Remote access



Services

IoT Threat Defense



Visibility & Analysis

Detect anomalies, block threats,
identify compromised hosts

Umbrella
Stealthwatch
ISE/TrustSec
Cognitive Threat Analytics
Advanced Malware
Protection



Segmentation

Extensible, scalable
segmentation to protect IoT
devices

Identity Services
Engine/TrustSec
Next-Generation FW



Remote Access

Secure third-party access with
control and visibility

AnyConnect



Services

Reduce risk, design, deploy,
and respond to incidents while
protecting the business

Design
Assess risk
Incident response

Visibility and analysis

IoT Threat Defense also analyzes network traffic entering and exiting your organization to:



Detect anomalies



Block attacks



Identify
compromised hosts



Help prevent
user error

Context is everything



Poor context awareness

IP Address: 192.168.2.101

Unknown

Unknown

Unknown


Unknown

Unknown




Unknown

Rich context awareness

 Operator device

 Vendor

 Factory-A Floor-1 Zone-B

 10:30 AM EST on April 27

 Wireless / Ethernet / Zigbee

 No Threats / Vulnerabilities



Known

Extensible, scalable segmentation





Extensible - Scalable segmentation

Easily separate devices and data using the network

Assign role-based groups

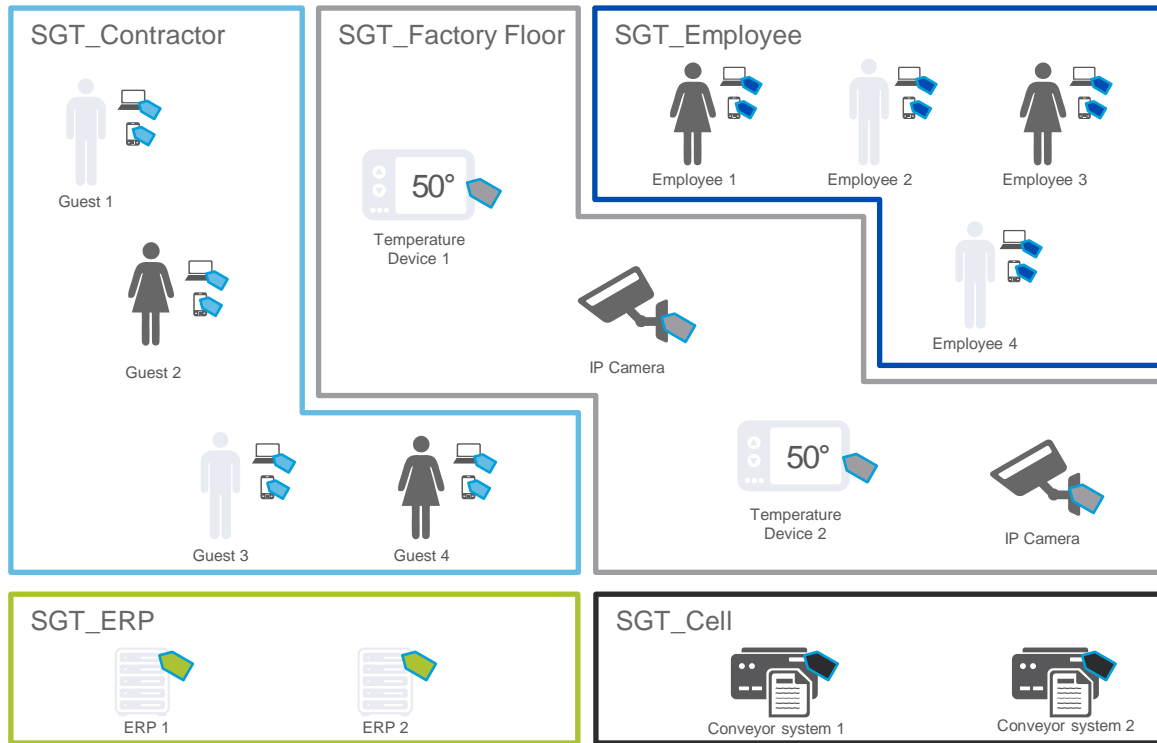
Assign business-based groupings to provide consistent policy and access independent of network topology

Get up and running quickly

Utilize ISE or another TrustSec-enabled controller to support group design

Establish context-aware groups

Leverage attributes such as location and device type to define group assignments



TrustSec policy management

Maintain agility with simple, dynamic policy updates



Sources	Destinations			
	Company Database	Public Cloud	External Partner	Internet
Cell Zone 1	Deny	Deny	Deny	Deny
Remote Access Contractor	Deny	Permit	Deny	Deny
Supervisor Workstation	Permit	Web Apps	Web Apps	Web Apps
Employee 01	Permit	Permit	Define Access	Permit

A context menu is open over the 'Remote Access Contractor' row, showing options: 'Permit' (checked), 'Deny', 'Web Apps', and '...'. A mouse cursor is pointing at the 'Permit' option.

Simplify role creation

Define access policies using plain language instead of complex ACLs and firewall rules

Apply rules automatically

Define segmentation based on logical groupings that are applied automatically

Maintain and scale dynamically

Defining policies with logical tags means that rules don't depend on individual IP addresses and can be dynamically and transparently changed no matter the group size

Secure remote access



Access based on
policy



Secure connectivity



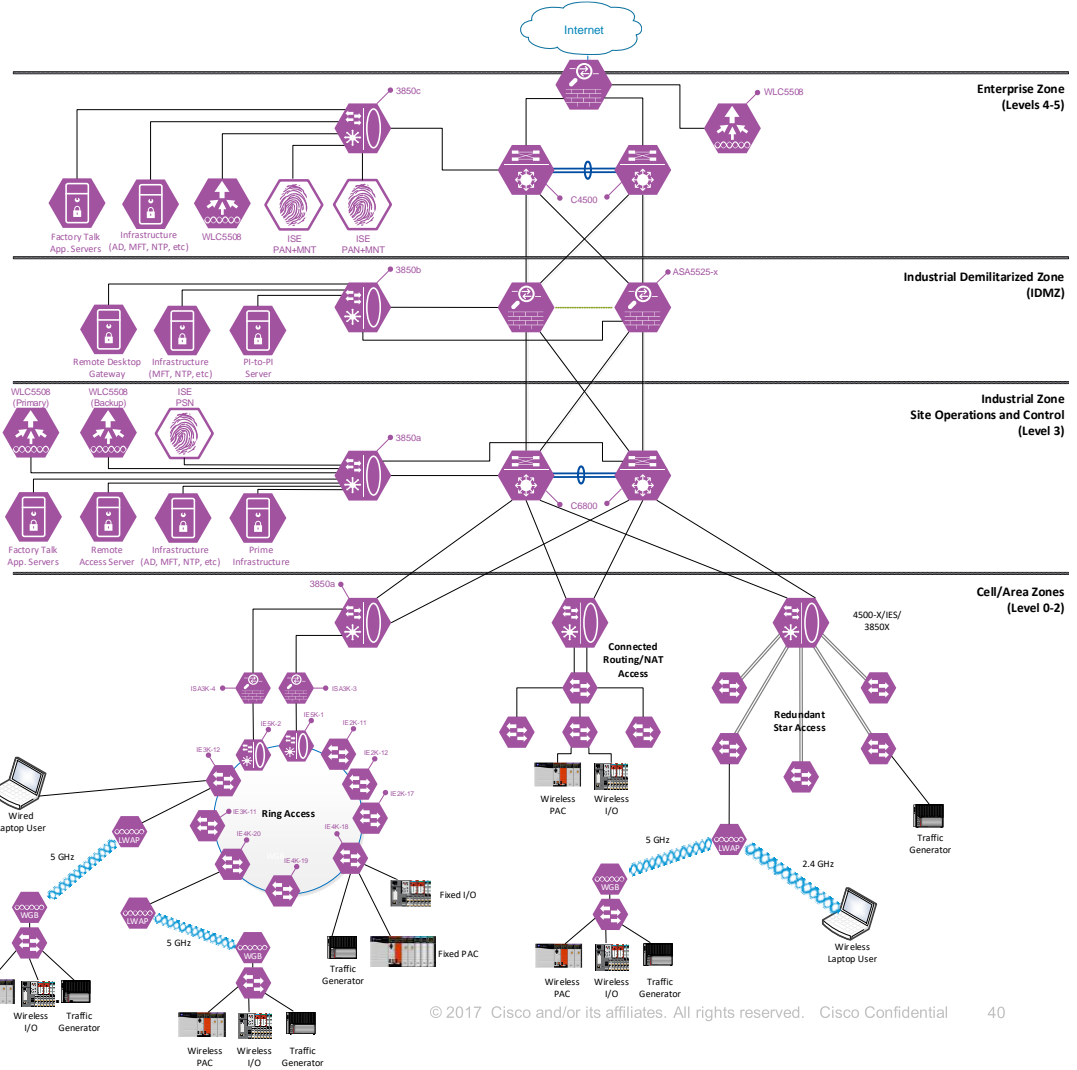
Visibility and control

Safe Validation Efforts



Connected Factory Lab for IoT

- Validation for CPwE
 - Ring Topology
 - Star Topology
 - Routed Topology
 - Industrial workflows
- Threat Defense Adds
 - Deploy StealthWatch
 - Implement PxGrid (ISE, FMC, SW)
 - TrustSec Segmentation
 - AMP4E on Access Servers
 - CTA for Enterprise Flows



Despite the technological advances
that the IoT represents...

The human
factor is the most
important.



Who better to help you
meet the challenge of
the IoT head on?



Services



People develop these technologies, and people are needed to secure IoT environments. Our people are highly-skilled experts who have decades of experience in helping our customers:



Assess risk



Design



Incident
response



Support

Cisco Security Services for IoT Threat Defense



Assess and Manage Risk


- Security Network Penetration Assessment
- Security Network Architecture Assessment
- Customized Network Penetration Testing
- Privacy impact assessments
- Automation & Control System Risk Assessment (for OT)
- Network Device Security Assessment

Readiness to Adopt IoT Threat Defense

- Security Segmentation Services
- Deployment Services for:
 - AMP for Endpoint
 - Firepower (NGFW)
 - Stealthwatch
 - ISE
- Incident Response Services

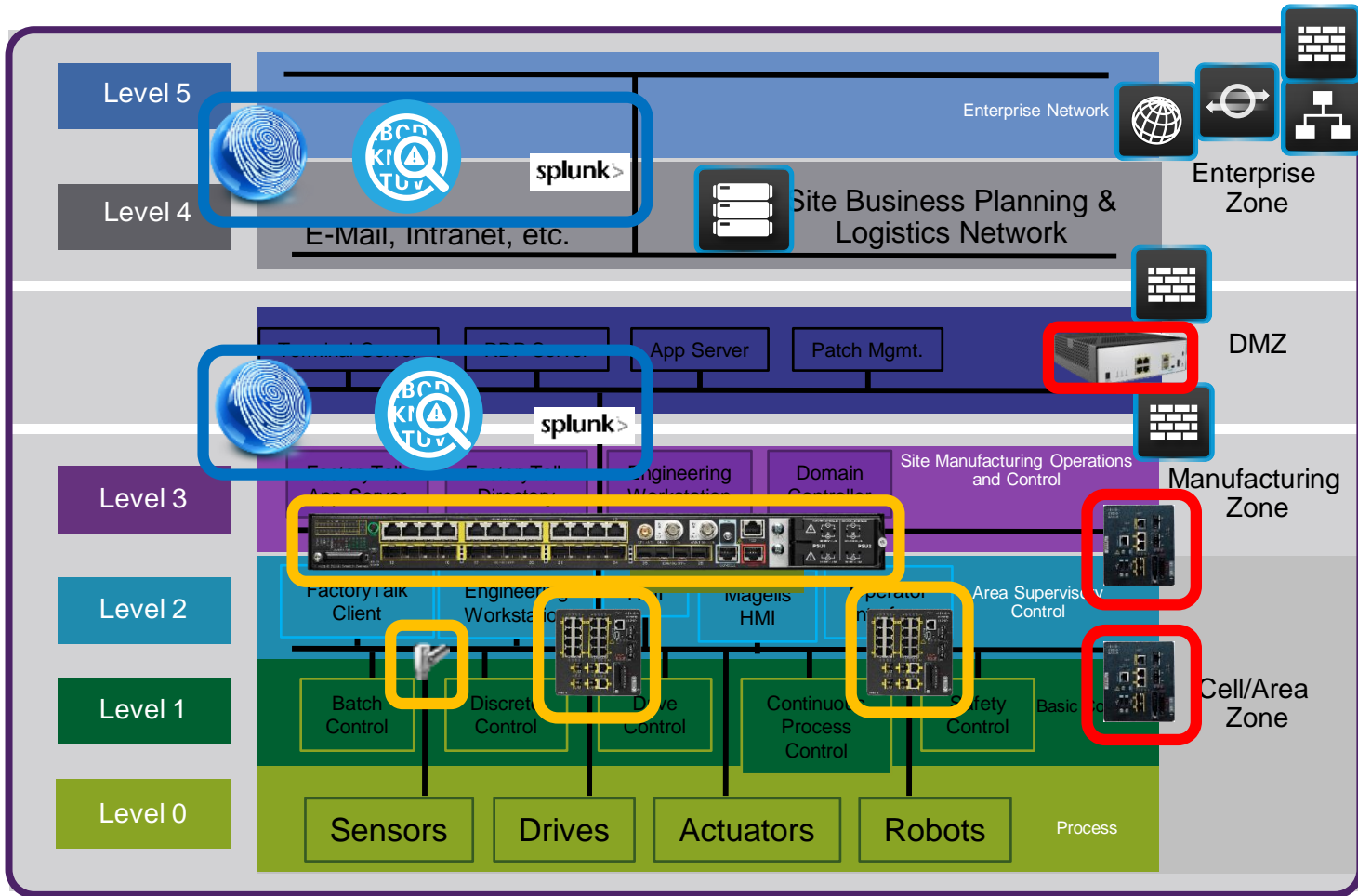
Improved Ability to Resolve Issues Quickly

- Cisco Solution Support for Network Security

- 
- Learning@Cisco for IoT training
 - SecureOps for industrial automation and control system environments



Evolve to Security: Phased Security Architecture



First Phase – Secured Connectivity

Zone Segmentation
Controlled Conduits

Second Phase – Secured Visibility & Control

Application Control
Threat Control

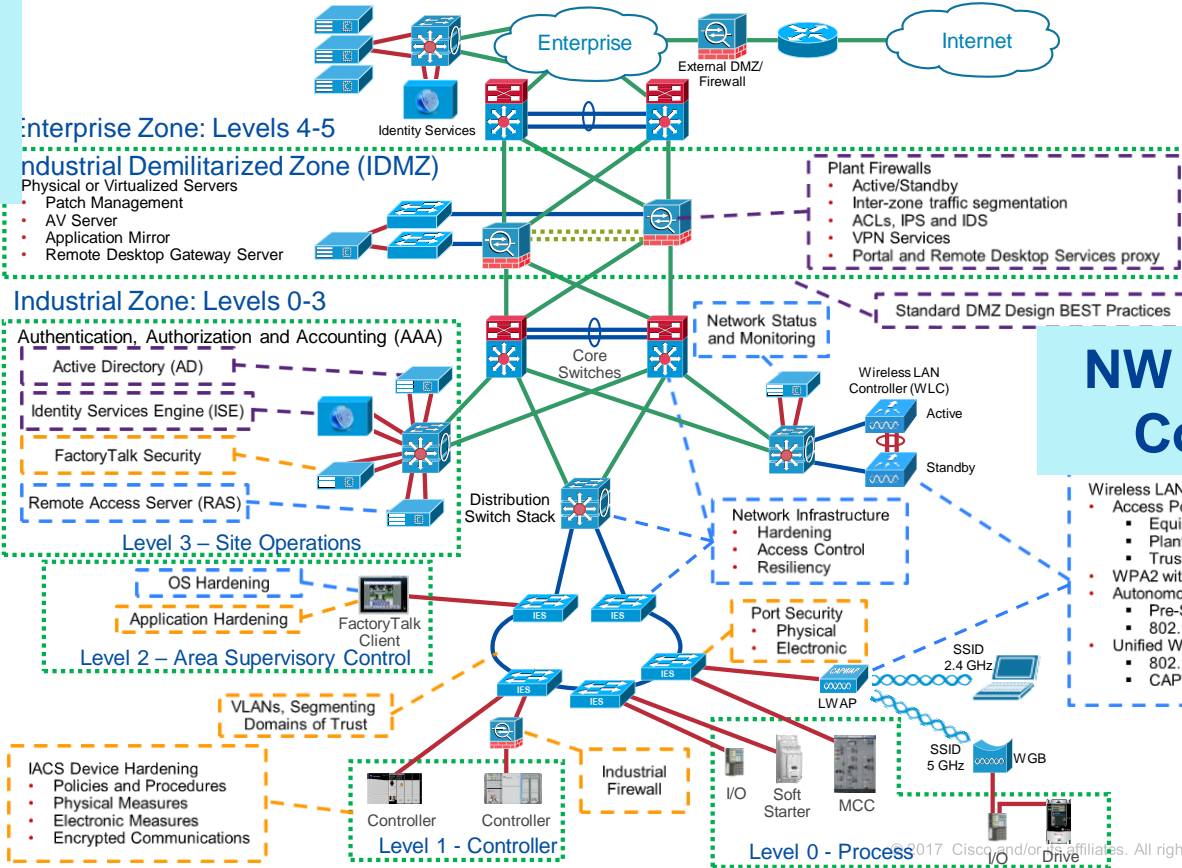
Third Phase – Converged Security & Depth

Policy Driven
Response
Deeper Vision /
Control

Start: Secured / Connected Modern Plant

Security Ready Networking

Access / Application Control



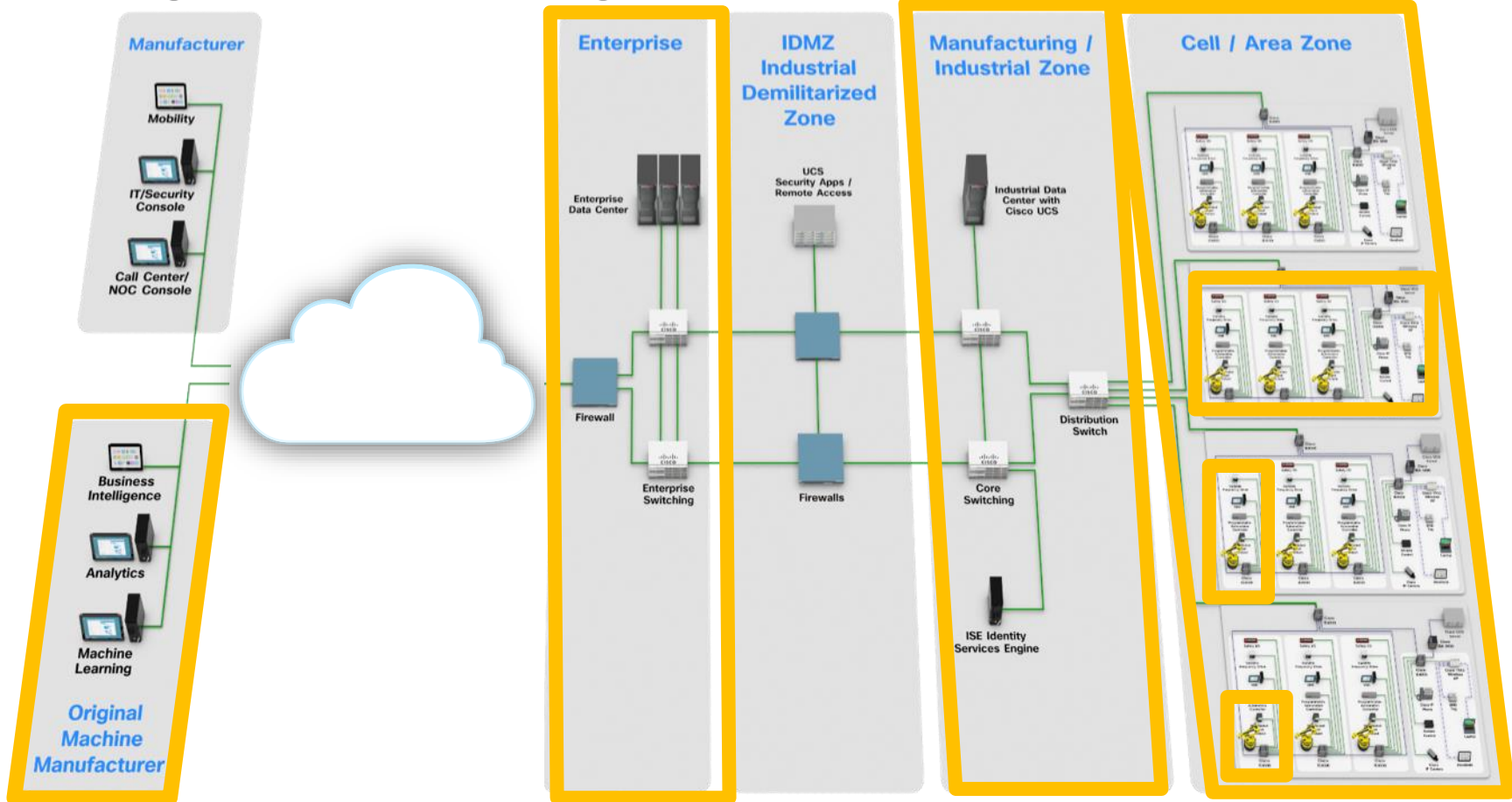
NW Access Control

- Control System Engineers
- Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
- IT Security Architects in Collaboration with Control Systems Engineers

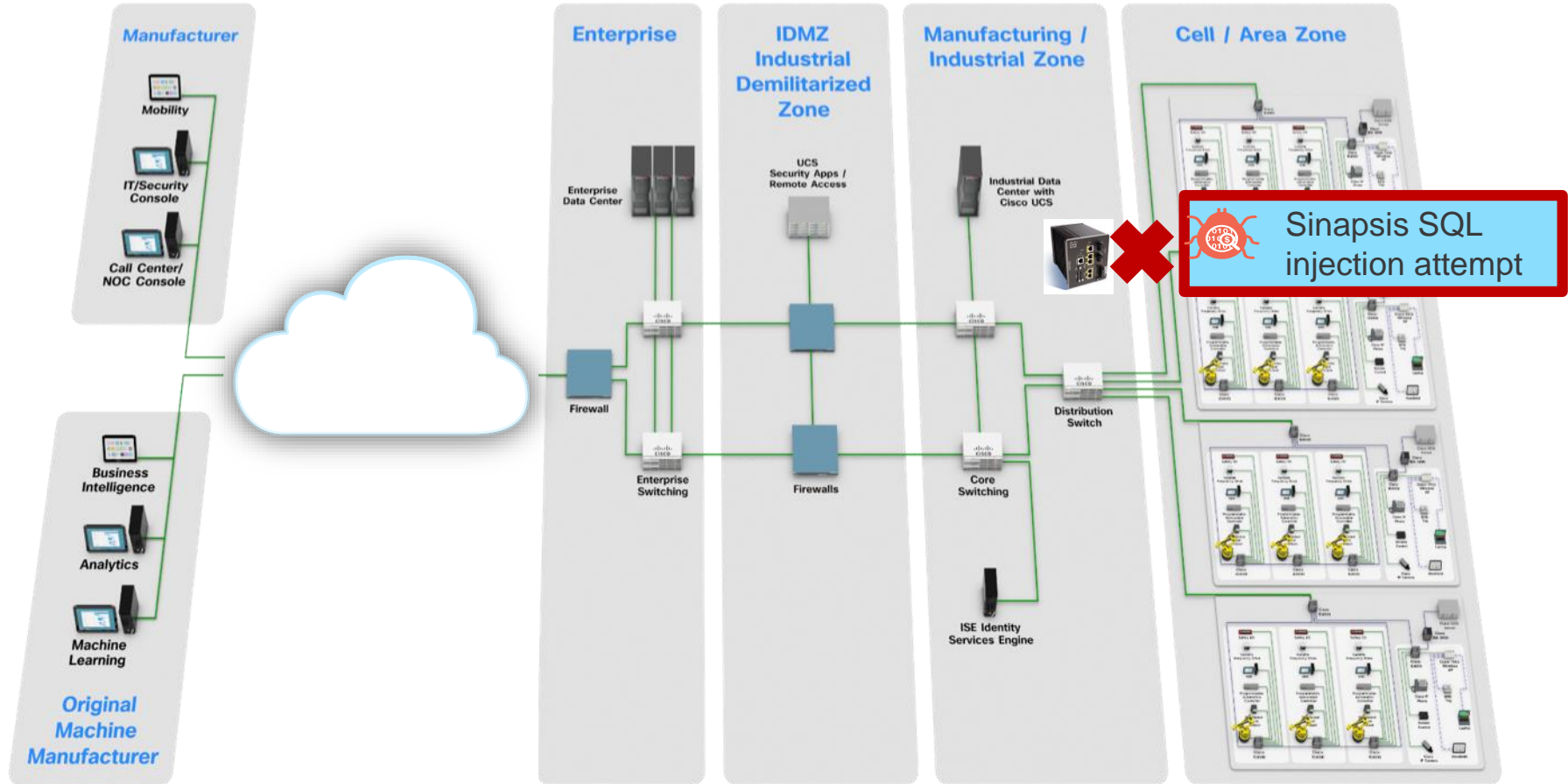
- Wireless LAN (WLAN)
 - Access Policy
 - Equipment SSID
 - Plant Personnel SSID
 - Trusted Partners SSID
 - WPA2 with AES Encryption
 - Autonomous WLAN
 - Pre-Shared Key
 - 802.1X - (EAP-FAST)
 - Unified WLAN
 - 802.1X - (EAP-TLS)
 - CAPWAP DTLS



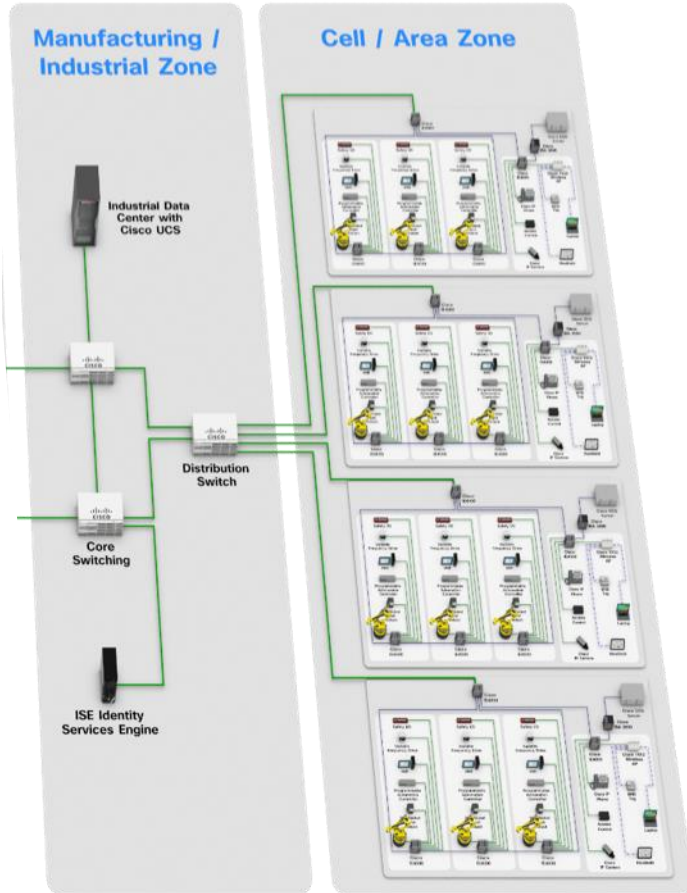
CPwE Use Case: Protect Critical Infrastructure: Through Network Segmentation – Zone Definition



CPwE Use Case: Protect Vulnerabilities



CPwE Use Case: Protect Critical Infrastructure – Safety Enforcement



Edit Rule 1:1000025:1 (View Documentation, Rule Comment)

Message:

Classification:

Action:

Protocol:

Direction:

Source IPs: Source Port:

Destination IPs: Destination Port:

Detection Options

flow

metadata

reference

modbus_unit

modbus_func

OT Pre-Processors – Modbus command inspection



Create New Rule

Message: Modbus Read Coils Command Detection Rule

Classification: scada

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

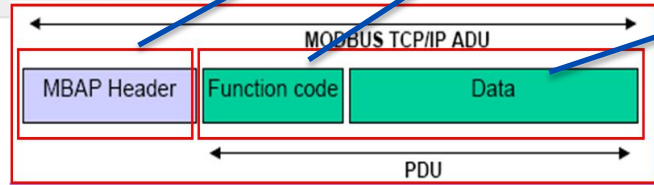
Destination IPs: any Destination Port: 502

Detection Options

ack Add Option Save As New

- metadata
- method_data
- modbus_data
- modbus_func
- modbus_unit

A Modbus rule to prevent a set point change
limit > 50 on
RTU-0122



Create New Rule

Message: Modbus Read Coils Command Detection Rule

Classification: scada

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

Destination IPs: any Destination Port: 502

Detection Options

modbus_unit: RTU-0122

modbus_func: write_single_register

modbus_data

byte_test: Bytes: 2, Offset: 16, Value: > 50, Number Type: Decimal String, Endian: Little Endian

byte_test Add Option Save As New

