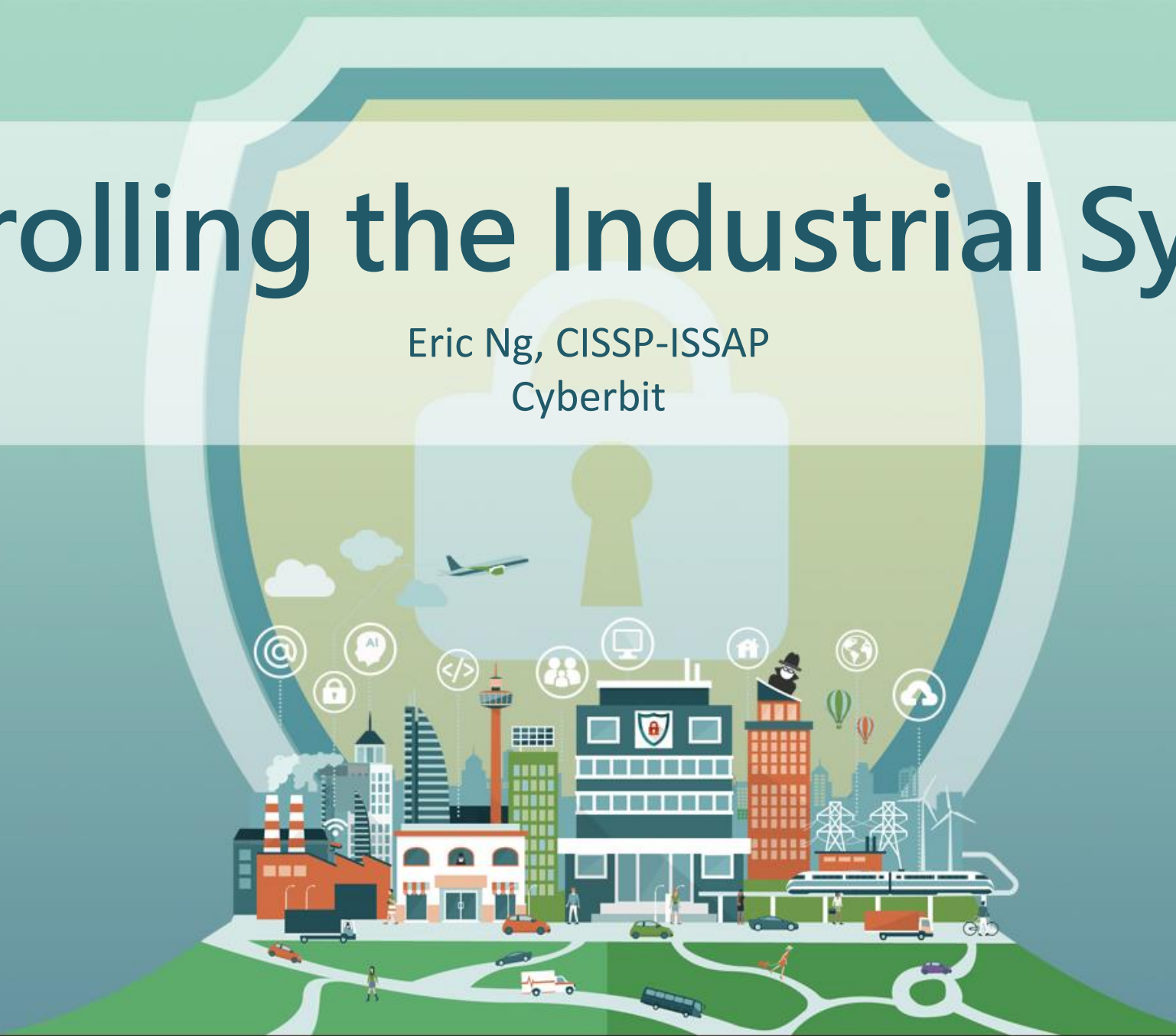


# Controlling the Industrial System

Eric Ng, CISSP-ISSAP  
Cyberbit



# PROTECTING ISRAEL'S CRITICAL INFRASTRUCTURE FOR OVER 8 YEARS

Electricity  
Grid



International  
Airport



Oil and Gas  
Storage &  
pipeline




Military and  
Airforce




Government Smart  
Buildings



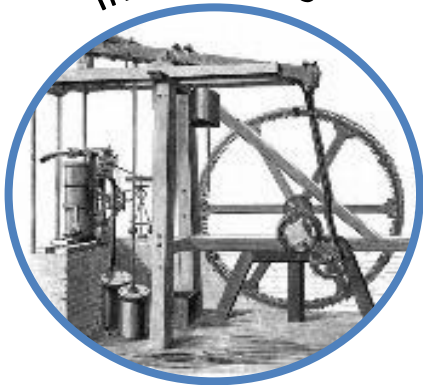


13:43:28

# Industry 4.0 – Connected Manufacturing



## Industry 1.0



1

End of 18<sup>th</sup> century

Use of **water and stream power** to run mechanical production facilities

## Industry 2.0



2

Beginning of 20<sup>th</sup>

Use of **electrical power** to enable work-sharing mass production

## Industry 3.0



3

Early 1970s

Use of **electronics and IT** to automate production

## Industry 4.0



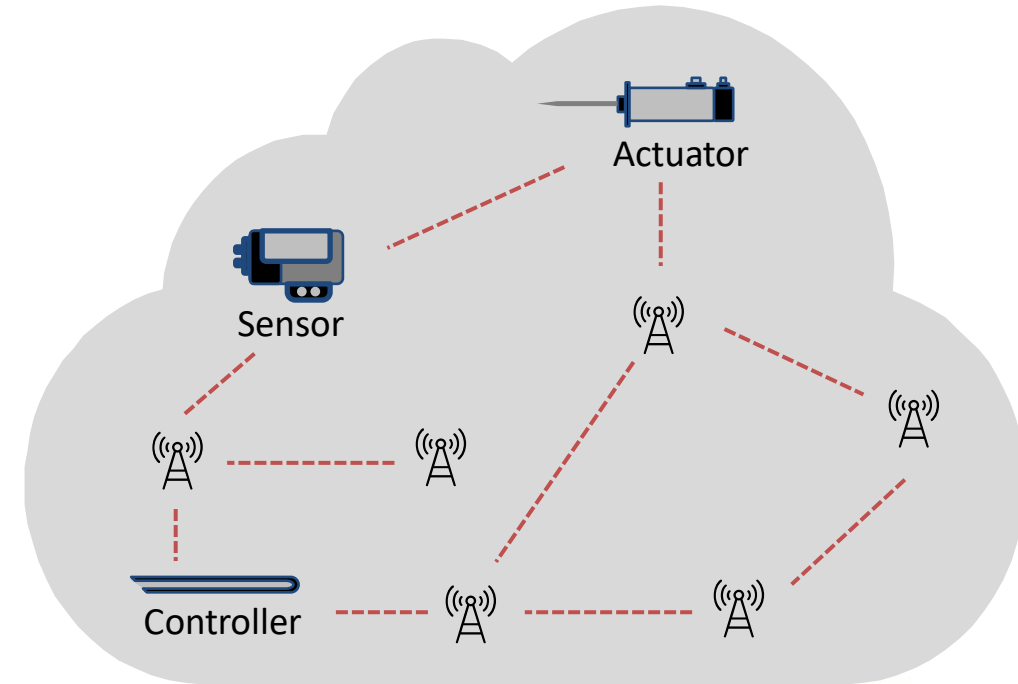
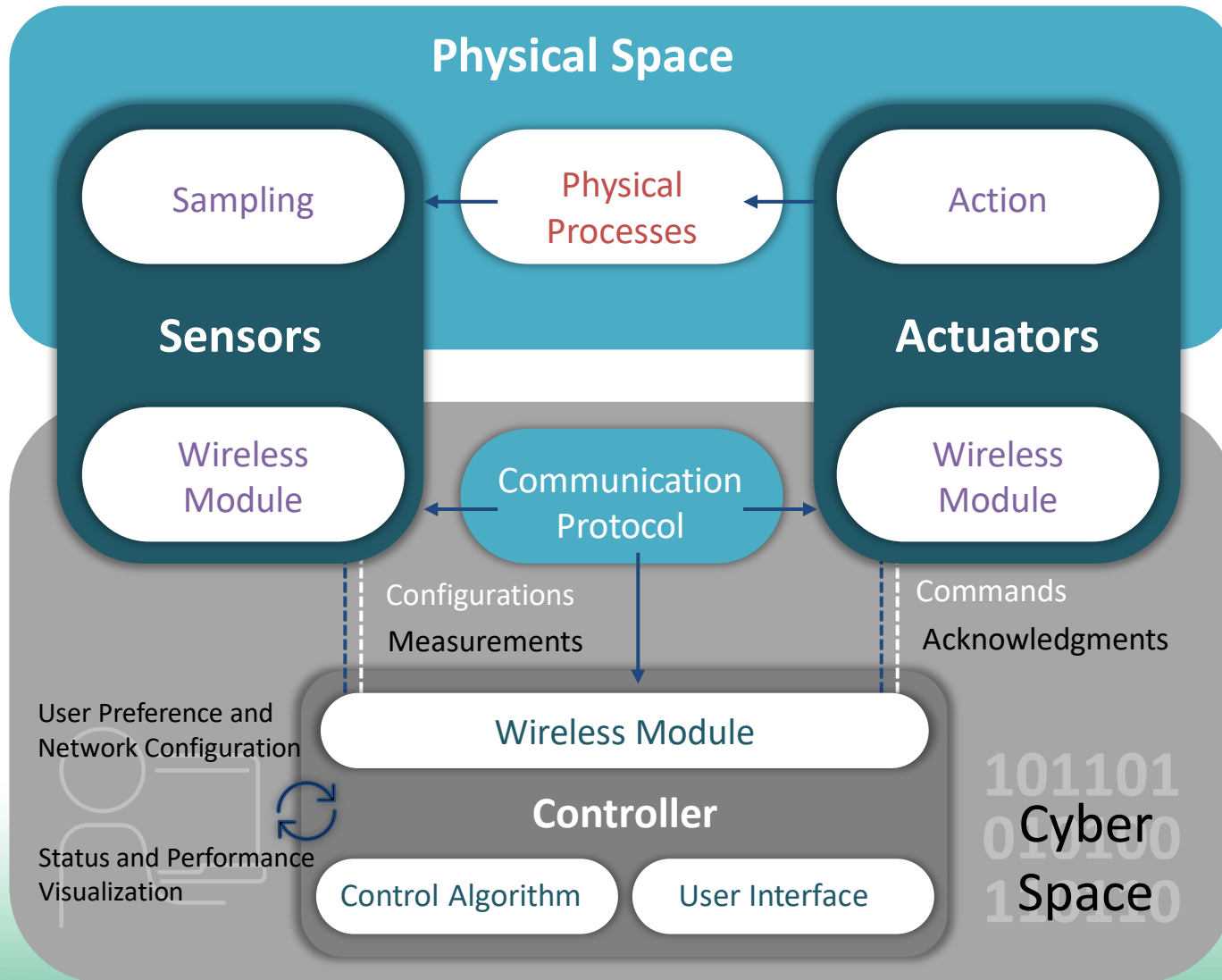
4

Today

Use of **Cyber-physical systems** to monitor, analyze, and automate business



# Cyber Physical Systems (IIoT)

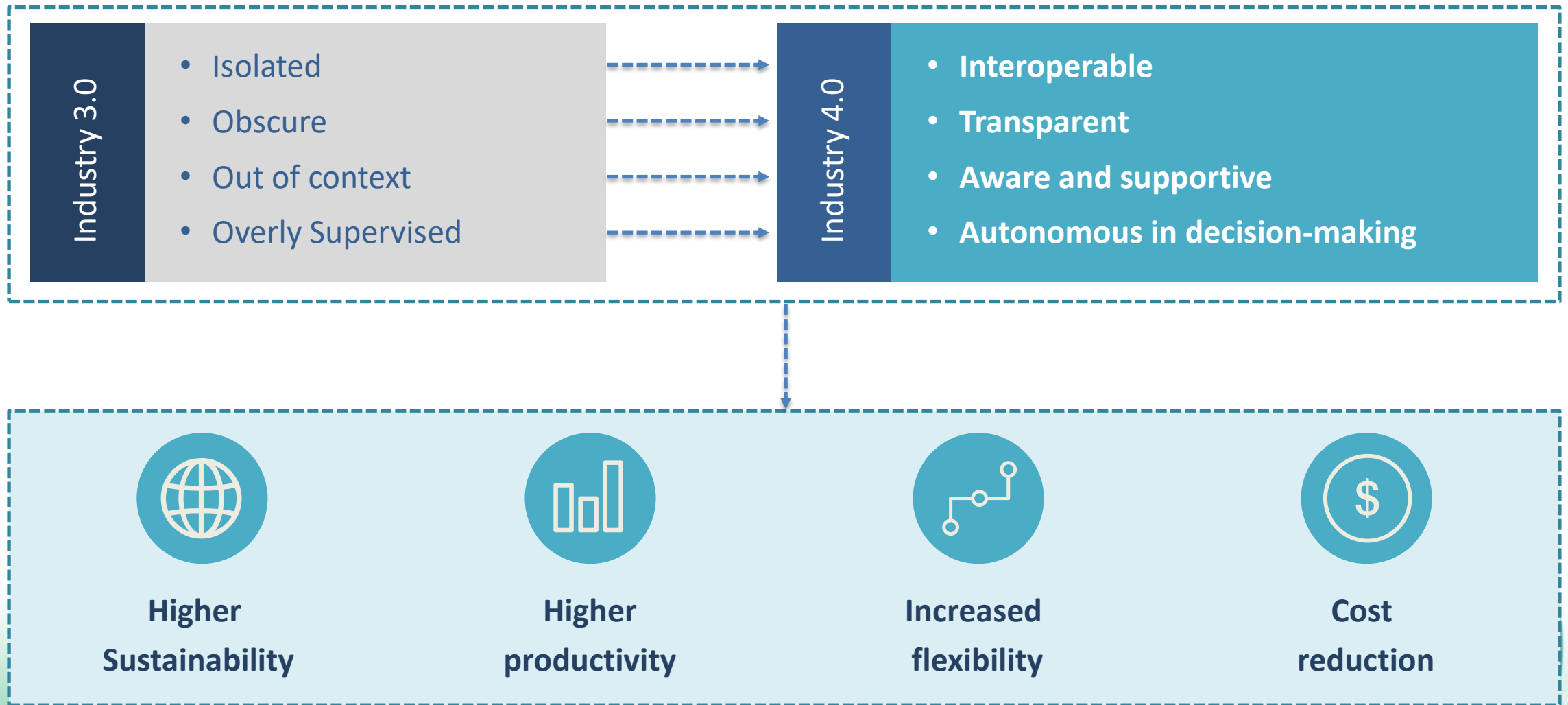


**Wireless Sensor Network**



## Wireless Communication

# Industrial environment is changing for (the) good.



# Expectations are skyrocketing



**60%** believe I4.0  
Will Increase Revenues



**55%** believe I4.0  
Will Lower Costs



**70%** believe I4.0  
Will increase efficiency

[IDC Survey](#)

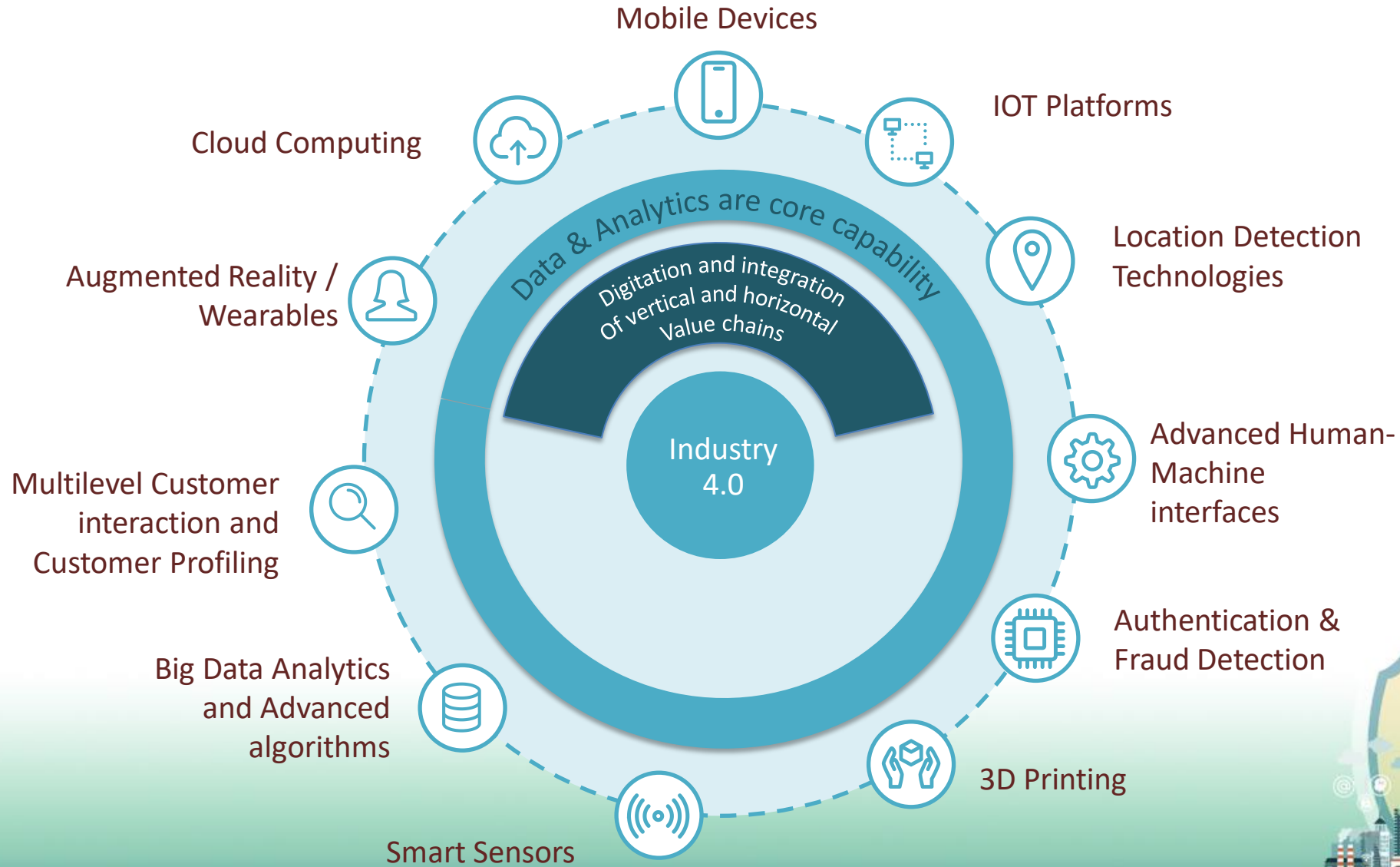


A person wearing a dark hoodie is shown from the chest up, holding a laptop. The background is a dark, textured surface with vertical columns of white binary code (0s and 1s) falling from the top, reminiscent of the 'Matrix' effect. A semi-transparent blue horizontal band is overlaid across the middle of the image, containing the text.

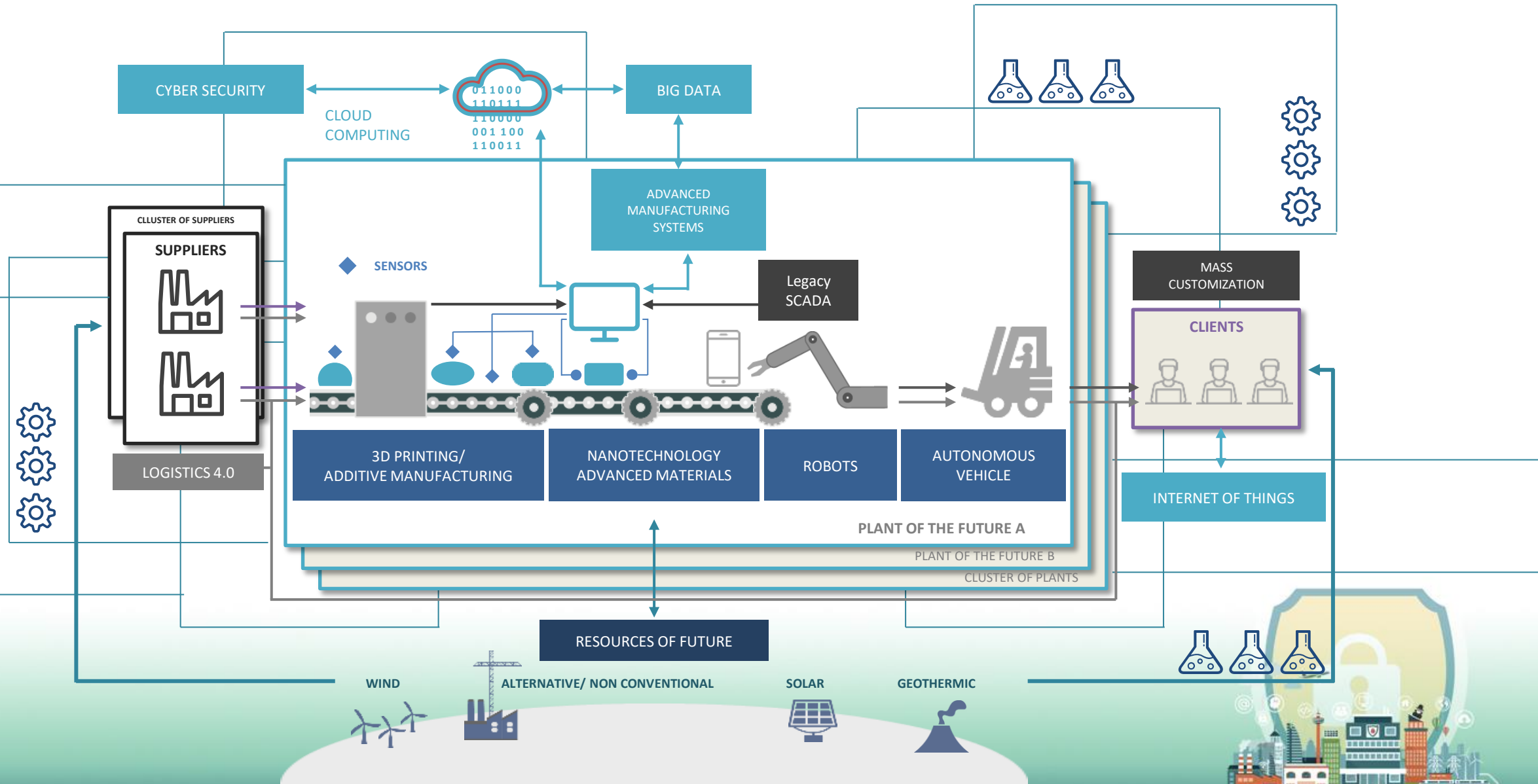
**But not all is bright....**



# We imagine industry 4.0 like this...



# But it looks more like this...



# Increasingly Exploiting the Growing Connectivity



**Ukraine**

**Power Grid Attack (2016)**



**German**

**Steel Mill Attack (2015)**



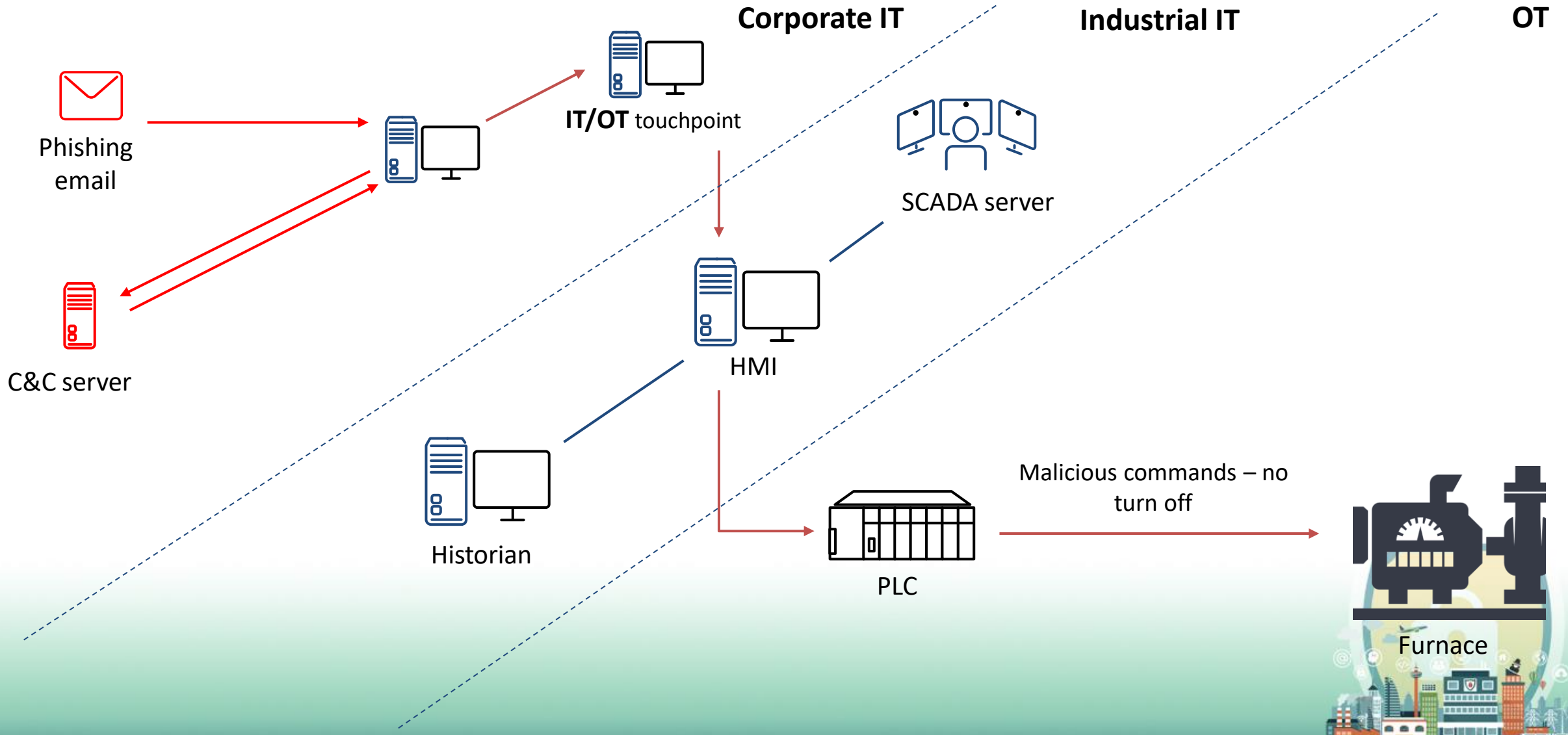
**Stuxnet**

**Nuclear Reactor Attack (2015)**

**And these are just the ones everybody's heard of**



# German Steel Mill Attack (2015)





## Industrial IT is not maintained properly

Remote accessed by multiple factors, unpatched, undocumented



## SCADA Protocols are vulnerable

Operational consideration triumph security considerations leading to severe vulnerabilities in the protocols



## Convergence between IT and OT

IT components are moving into the process environment (windows/Linux PLC's)



## Wide Attack surface

Wi-Fi, RF, Phishing, Remote Access, internal threats, Over 40,000 industrial components are already accessible online (shodan.io)



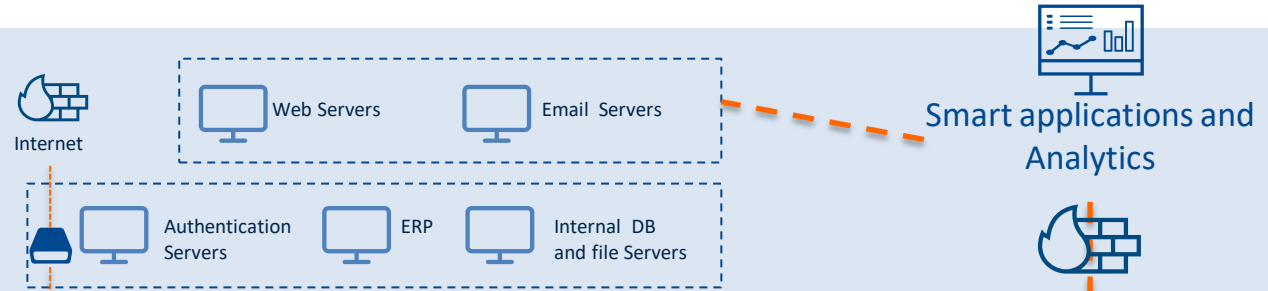
## Lack of SCADA security personnel

Most Cyber security personnel is focused on IT security rather than OT security



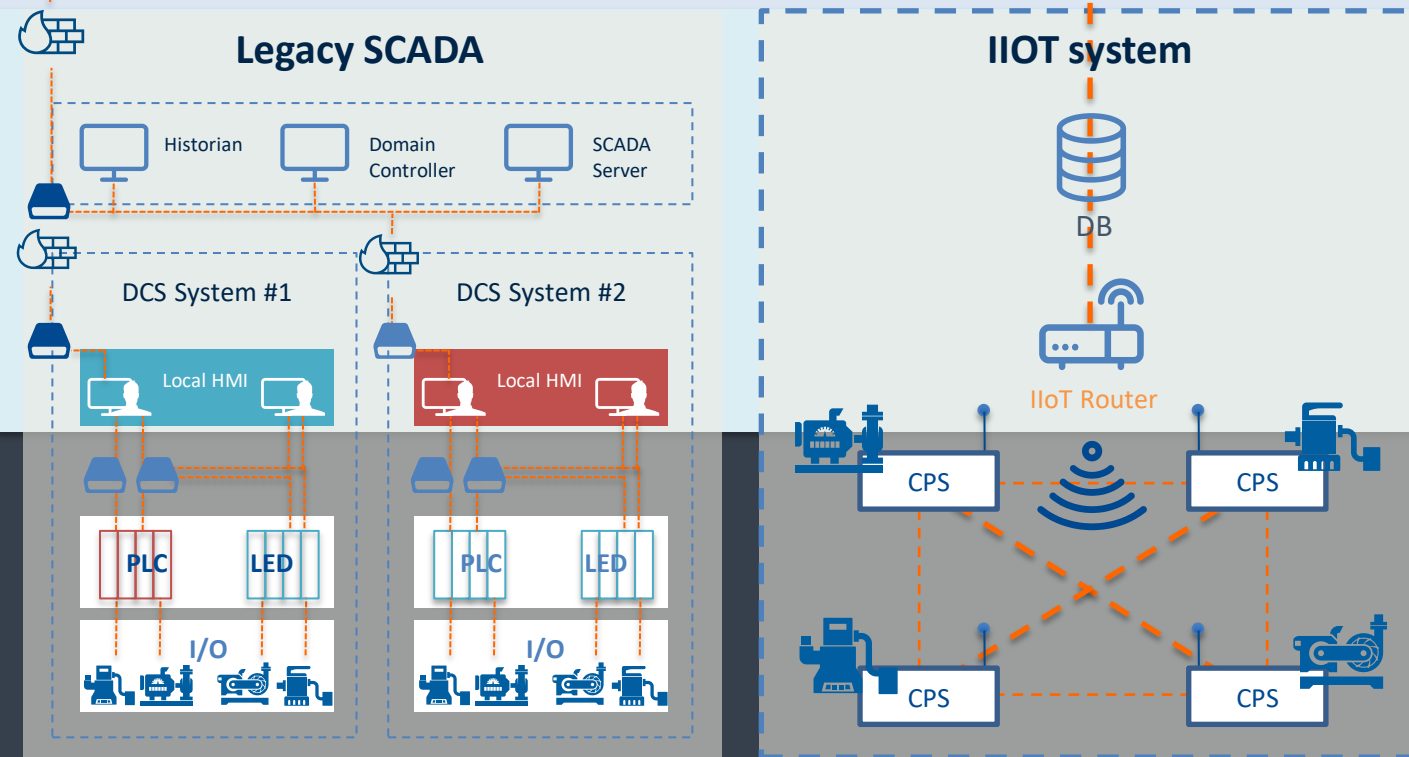
# Threat Stack

Corporate IT



**Malware**  
Spear phishing, External devices, Macros

Industrial IT



**MaIoT**  
Lateral movement, Remote access,

Industrial OT

**M2M attacks**  
MITM, Unauthorized devices





More than **60%** of organizations perceive the current cyber threat level to their ICS is high to severe

Over **70%** of organizations had at least 1 malicious event in the past year

Less than **25%** of organizations have a fully documented OT network



A black and white photograph of a control room. In the foreground, two people are seated at a desk with multiple computer monitors. The person on the left is using a keyboard, and the person on the right is using a mouse. The background features three large monitors mounted on the wall. The leftmost monitor displays a complex data interface with various charts and tables. The middle monitor shows a digital clock displaying '13:43:28' and several smaller data visualizations, including pie charts and bar graphs. The rightmost monitor displays a high-resolution, textured image, possibly a satellite or aerial view. A window with blinds is visible on the far right. A semi-transparent blue banner is overlaid across the middle of the image, containing the text 'Introducing Cyberbit SCADAshield' in white.

# Introducing Cyberbit SCADAshield



# The Challenge: SCADA networks are unprotected

## Insecure “by design” –

ICS systems are designed to maintain high availability, not security.

---

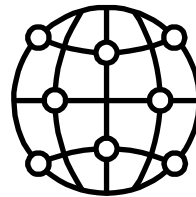


- Flat architecture
- No authentication
- Rarely patched

## High Connectivity –

modern ICS networks become more complex, and connected to the outside world

---



- Remote accesses
- IT/OT connectivity
- IIoT/ Industry 4.0

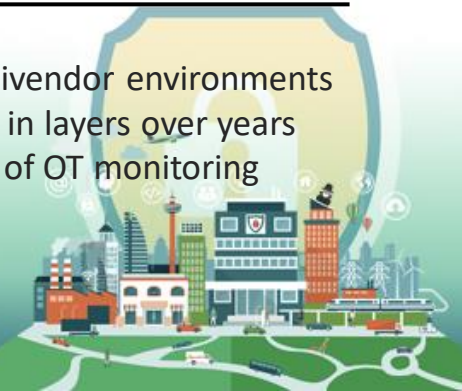
## Lack of visibility –

assets, commands and communications

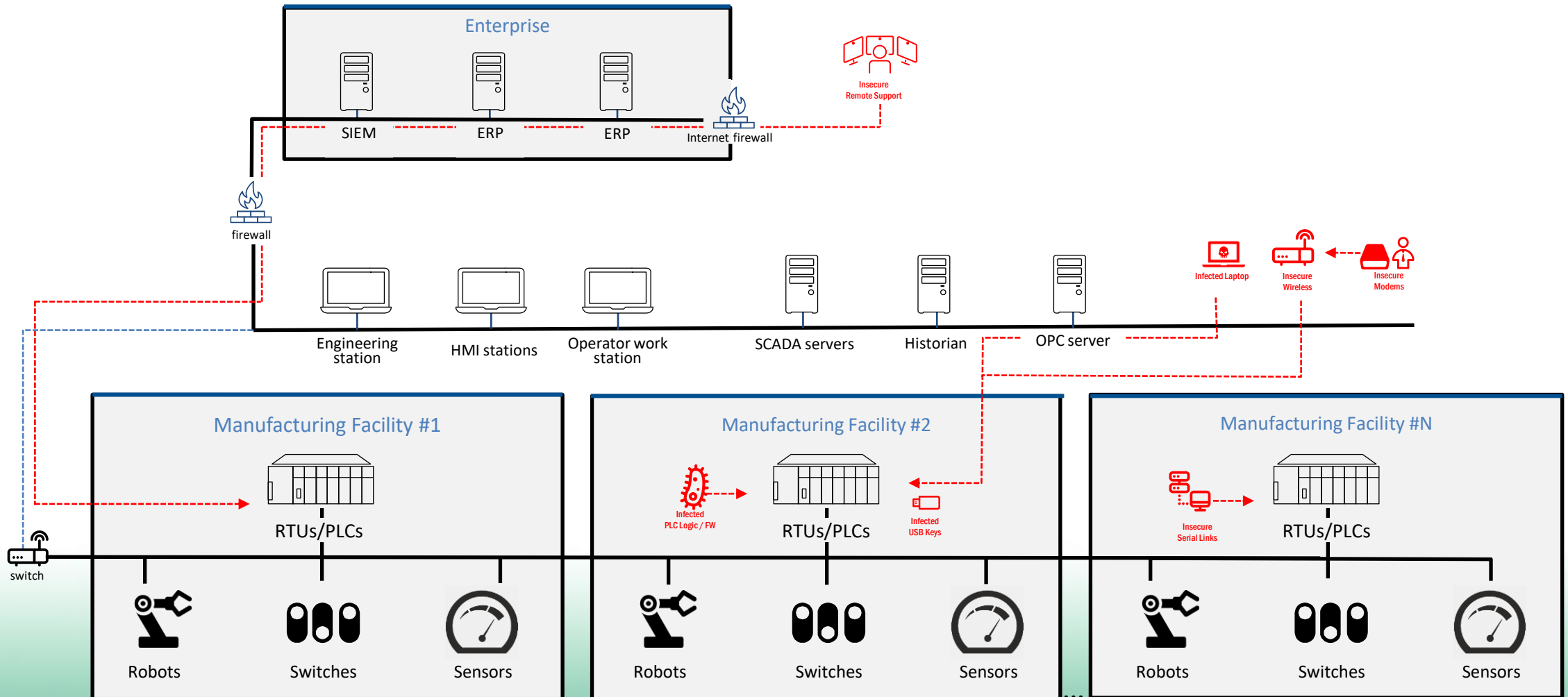
---



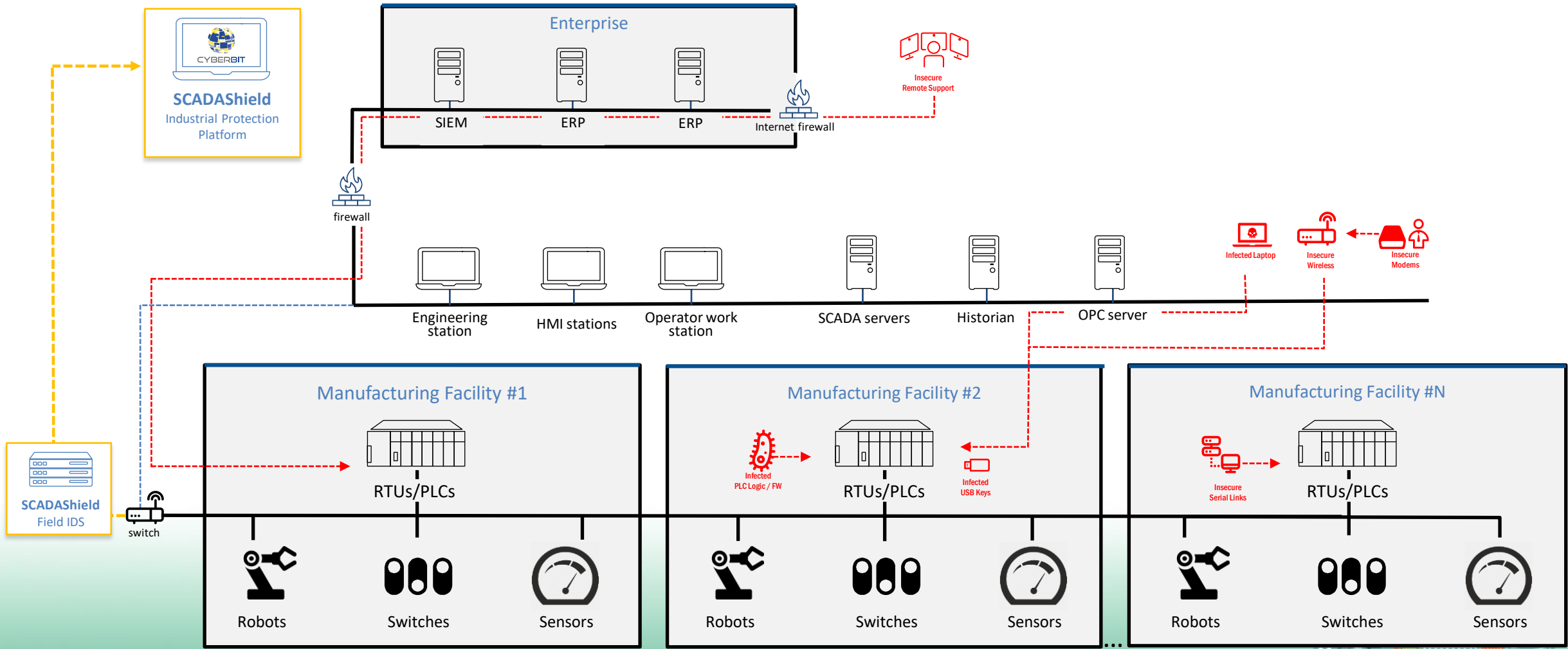
- Multivendor environments
- Built in layers over years
- Lack of OT monitoring



# Manufacturing Automation Systems are **Under High Risk**



# SCADAshield Allows You to Detect and Respond to Malicious Activities in Your Network



# SCADAshield Industrial Protection Platform



Network **Discovery & Visibility**



Detection of **known vulnerabilities** for SCADA and IT



Detection of **unknown industrial threats**



Detection of **Operational malfunction & misconfiguration**



# Network Discover

- Discover all network assets – IP and Non-IP (Fieldbus, serial) - automatically
- Have a clear view of your assets, their usage and activity
- Conduct Space/Time event analysis

Filters and investigation tools

NETP..AP

Search

**EVENTS**

- NORV SCADA LINK DOWN, 21/12/2017, 19:44:05  
Source: 168.254.0.1  
Target: 168.254.255.255
- NORV SCADA LINK DOWN, 21/12/2017, 15:22:05  
Source: 168.254.0.1  
Target: 168.254.255.255
- NORV SCADA LINK DOWN, 21/12/2017, 19:21:05  
Source: 192.168.242.131  
Target: 192.168.242.2
- NORV SCADA LINK DOWN, 21/12/2017, 15:21:05  
Source: 192.168.242.131  
Target: 65.55.165.20
- NORV SCADA LINK DOWN, 21/12/2017, 19:21:05

**FILTERING**

- Broadcast Multicast (18)
- unknown (230)
- Groups (0)
- Alerts (4)
- Scada (115)
- Non-Scada (129)

**ADVANCED FILTERING**

lec104\_s7comm\_p

ipv4

BBX 1 - BBX\_10.20

Groups

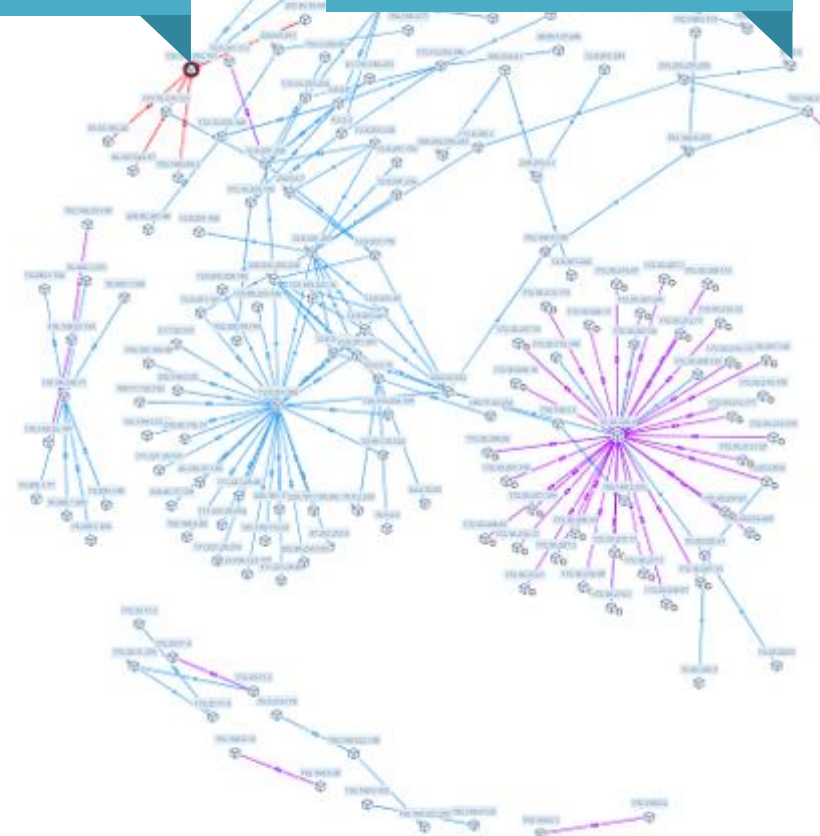
CLEAR APPLY

PROTOCOL COLORS

Layout: [Icons]

Netmap Alerts

Traffic color coding for SCADA and Non-SCADA



Asset details: IP, MAC, Vendor, Etc.

VMware, Inc.

IP Address: 192.168.242.131

Mac Address: 08:00:27:00:00:00

Vendor Name: VMware, Inc.

Detected By: BBX\_10.10.30.32



# Known Vulnerability

- Detect hundreds of SCADA and IT vulnerabilities in the network
- Provide guides and steps for vulnerability remediation
- Vulnerability severity analysis



**CYBERBIT SCADAshield**

**ALERTS**

8 Alerts [FILTER](#) [DELETE ALL](#)

2017/11/01 15:54:55:5455

Baseline Deviation

**Unknown Hosts** - 00:0c:29:51:58:be and 33:33:00:00:00:02

2017/11/01 15:54:48:5448

Policy Violation **BLACK**

**Non-Encrypted HTTP access to RTU** from EVE01 to RTU1

2017/11/01 15:54:45:5445

Baseline Deviation **WHITE**

**Unknown Host** - EVE01

2017/11/01 15:54:45:5445

CVE

**APPLICATION: Exploitation** from EVE01 to RTU1

2017/11/01 15:54:45:5445

Version 5.5.2.53

**Network components effected**

**EVE01**  
IP: 192.168.100.43  
MAC: 00:0c:29:51:58:be

BBX2

2 Events (2 Eps)

**RTU1**  
IP: 192.168.101.10  
MAC: 00:50:56:88:54:c3

**APPLICATION: Exploitation** **CRITICAL**

**BLACK**

CVE

⚠️ **Attempted Information Leak** ^  
(Signature ID: 1122) SERVER-WEBAPP /etc/passwd file access attempt

⚠️ **Web Application Attack** [CVE](#) ^  
(Signature ID: 5555003) Directory traversal attempt using GET

Device BBX2

First Event 2017/11/01 16:00:48:048

Last Event 2017/11/01 16:00:48:048

Protocol application

Status new

**COMMENT**

Enter Comment

[DELETE](#) [INVESTIGATE](#) [RESOLVE](#)

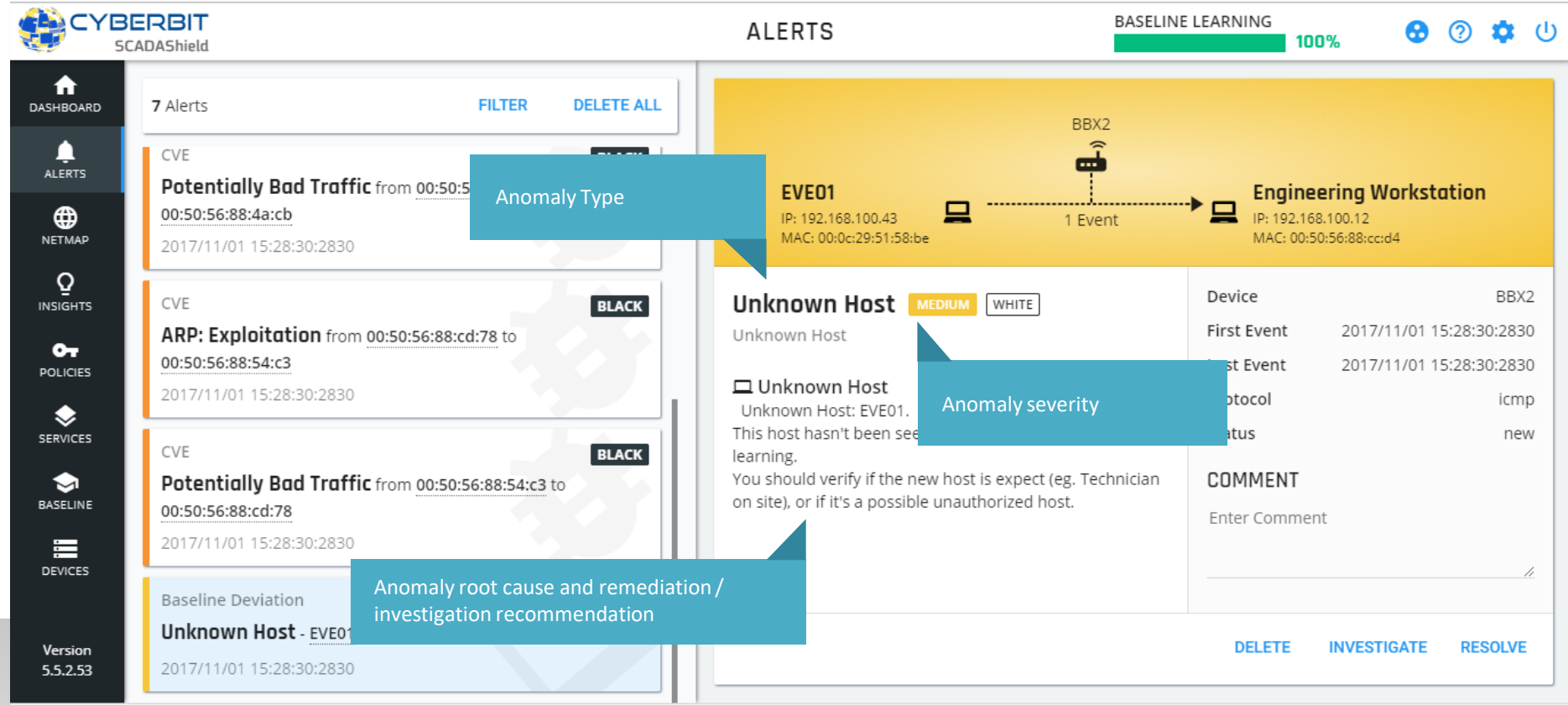
**Attack type and details**

**Link to CVE remediation details**



# Unknown Threat

- Detection of anomalous behaviors of SCADA and IT assets
- Based SCADAshield learning capabilities and auto-baselining
- Provides with anomaly response steps



**CYBERBIT SCADAshield** | **ALERTS** | BASELINE LEARNING 100%

7 Alerts | FILTER | DELETE ALL

**Alerts List:**

- CVE**  
Potentially Bad Traffic from 00:50:56:88:4a:cb to 00:50:56:88:54:c3  
2017/11/01 15:28:30:2830
- CVE** [BLACK]  
ARP: Exploitation from 00:50:56:88:cd:78 to 00:50:56:88:54:c3  
2017/11/01 15:28:30:2830
- CVE** [BLACK]  
Potentially Bad Traffic from 00:50:56:88:54:c3 to 00:50:56:88:cd:78  
2017/11/01 15:28:30:2830
- Baseline Deviation**  
Unknown Host - EVE01  
2017/11/01 15:28:30:2830

**Alert Detail: Unknown Host** [MEDIUM] [WHITE]

**Anomaly Type:** Unknown Host

**Anomaly severity:** MEDIUM

**Anomaly root cause and remediation / investigation recommendation:** This host hasn't been seen since baseline learning. You should verify if the new host is expect (eg. Technician on site), or if it's a possible unauthorized host.

**Event Details:** EVE01 (IP: 192.168.100.43, MAC: 00:0c:29:51:58:be) → Engineering Workstation (IP: 192.168.100.12, MAC: 00:50:56:88:ccd4) via BBX2 (1 Event)

**Device:** BBX2

**First Event:** 2017/11/01 15:28:30:2830

**Last Event:** 2017/11/01 15:28:30:2830

**Protocol:** icmp

**Status:** new

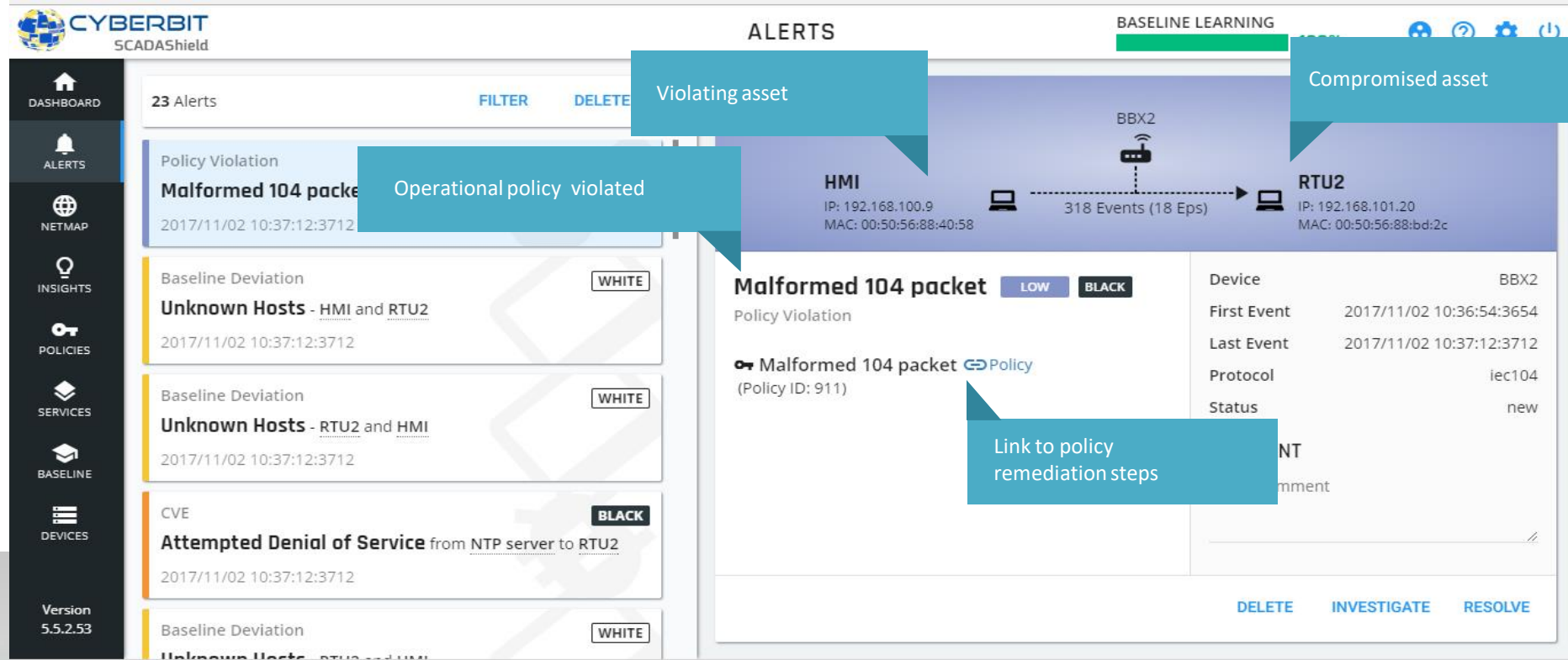
**COMMENT:** Enter Comment

DELETED | INVESTIGATE | RESOLVE



# Operational Anomalies

- Based on operational policies created by Cyberbit and the Operational team
- Detects possible system malfunctions and misconfigurations



**CYBERBIT SCADAShield**

**ALERTS** 23 Alerts [FILTER](#) [DELETE](#)

**BASELINE LEARNING**

**Violating asset** (HMI)

**Compromised asset** (RTU2)

**Operational policy violated** (Malformed 104 packet)

**Link to policy remediation steps** (Policy)

**Alert Details:**

- Malformed 104 packet** (Policy ID: 911)
- Severity: **LOW** **BLACK**
- Device: BBX2
- First Event: 2017/11/02 10:36:54:3654
- Last Event: 2017/11/02 10:37:12:3712
- Protocol: iec104
- Status: new

**Alert List:**

- Policy Violation: **Malformed 104 packet** (2017/11/02 10:37:12:3712)
- Baseline Deviation: **Unknown Hosts - HMI and RTU2** (2017/11/02 10:37:12:3712) [WHITE]
- Baseline Deviation: **Unknown Hosts - RTU2 and HMI** (2017/11/02 10:37:12:3712) [WHITE]
- CVE: **Attempted Denial of Service** from NTP server to RTU2 (2017/11/02 10:37:12:3712) [BLACK]
- Baseline Deviation: **Unknown Hosts - RTU2 and HMI** (2017/11/02 10:37:12:3712) [WHITE]

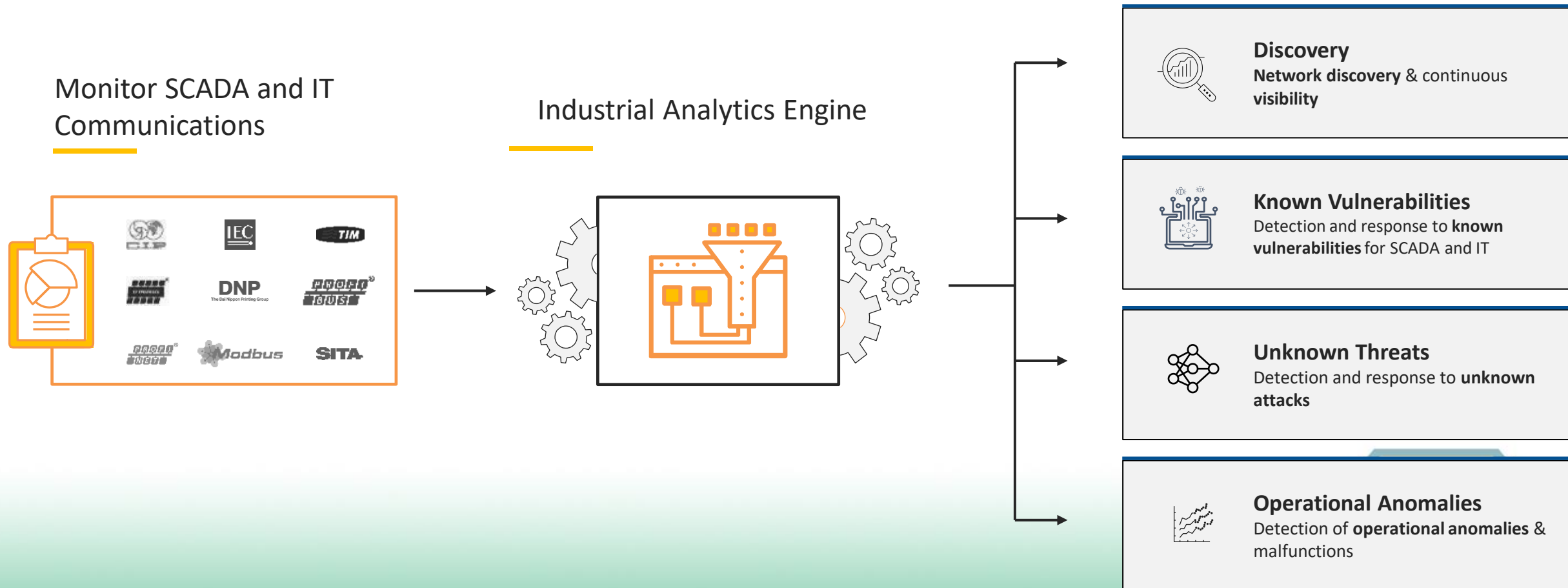
Version 5.5.2.53

[DELETE](#) [INVESTIGATE](#) [RESOLVE](#)





# SCADAshield Operational Flow

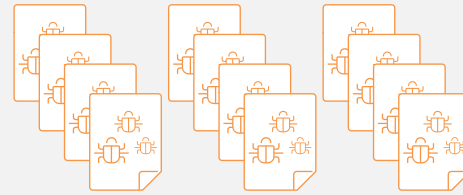


# Industrial **Analytics** Engine



## Unknown threats detection

Auto-learning based whitelisting




## Known CVE Database

Public and inhouse research CVE's




## Operational Policies

Monitoring operational standards violations and changes

 Detect anomalous malicious behavior in the network

 Detect vulnerability exploitation by the attacker

 Detect malfunctions and human errors

 Detect configuration changes



# Wide Vendor and Protocol Coverage

## Vendors



Honeywell

Rockwell  
Automation

SIEMENS

ABB



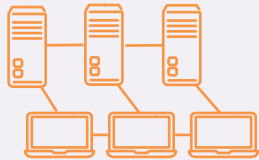
Schneider  
Electric

## Protocols







- CLNP
- COTP
- DCE RPC
- ENIP
- EtherNet/IP,
- IEEE 802.3
- LLC
- Ethercat
- BACNET
- BVLC
- CIP
- CIPCLS
- CIPCM
- DNP3
- MDLC
- MMS
- Modbus/TCP
- OMRON-FINS
- Profibus
- Profinet CM
- Profinet DCP
- Profinet IO
- Profinet PTCP,
- S7Comm
- SITA
- Goose
- IEC 60870-5
- IEC 61850, IEC101
- IEC104
- Kingfisher
- Serial Modbus
- NTP
- HTTP
- FTP
- SyncPhasor
- Teleperm XP
- TIM
- SNMP
- SSH
- SSL
- ARP
- **And many more....**







# Detection of Dozens of Attack Vectors

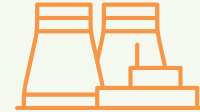


## IT






-  Known IT CVEs
-  ARP poisoning
-  Weak algorithms of SSL, SSH
-  Detecting of web-base attacks
-  Detecting new hosts
-  Detection of anomalous connections between hosts

## IT/OT

-  Detecting traffic to unusual host
-  Detecting Firmware and Logic updates from an unusual hosts
-  Unauthorized HTTP, SSH, FTP access
-  Setpoint alternation



## OT

-  Known SCADA CVE's
-  Field to Field attacks
-  Anomalous PLC behavior
-  Malformed packets
-  Out-of-range value commands to PLC/RTU

 Known vulnerabilities

 Unknown threats

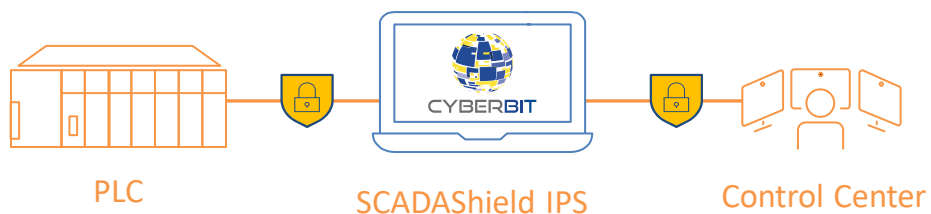
 Operational violations



# SCADAShield Advanced Capabilities

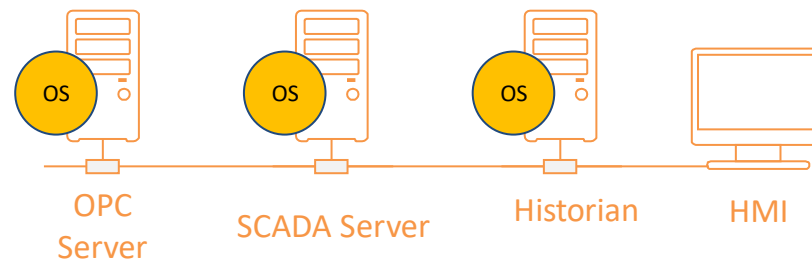
## SCADAShield IPS




Inline installation delivers IPS capabilities for attack prevention



## SCADAShield OS

Integration with Cyberbit EDR for advanced malware protection



-  Block malicious commands
-  Detect and respond to malware on HMI/SCADA server
-  Analyze and respond to IT/OT attacks



# Value for the organization



## Reduce Reputation Risk

Maintain quality standards by assuring process integrity and monitoring changes and errors



## Reduce downtime

Detect and respond to cyber attacks, human errors and system malfunctions



## Support compliance requirements

Support cyber security ISA/IEC and NERC CIP



**Thank You**

---



**CYBERBIT**  
PROTECTING A NEW DIMENSION