CYBERBIT
PROTECTING A NEW DIMENSION

Controlling the Industrial System

Eric Ng, CISSP-ISSAP
Cyberbit

SYSTEX A DATA COMPANY

PROTECTING ISRAEL'S CRITICAL INFRASTRUCTURE FOR OVER 8 YEARS

Electricity Grid

Israel Electric

International Airport

רשות שדות התעופה בישראל
ISRAEL AIRPORTS AUTHORITY

Oil and Gas Storage & pipeline

Delek

Military and Airforce

צבא ההגנה לישראל

Government Smart Buildings

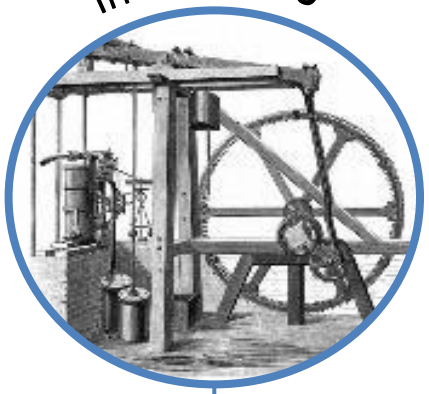
ישראל

SYSTEX A DATA COMPANY

Industry 4.0 – Connected Manufacturing

CYBERBIT

Industry *1.0*



1

End of 18th century

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

Industry *2.0*

2

Beginning of 20th

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

Industry *3.0*

3

Early 1970s

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

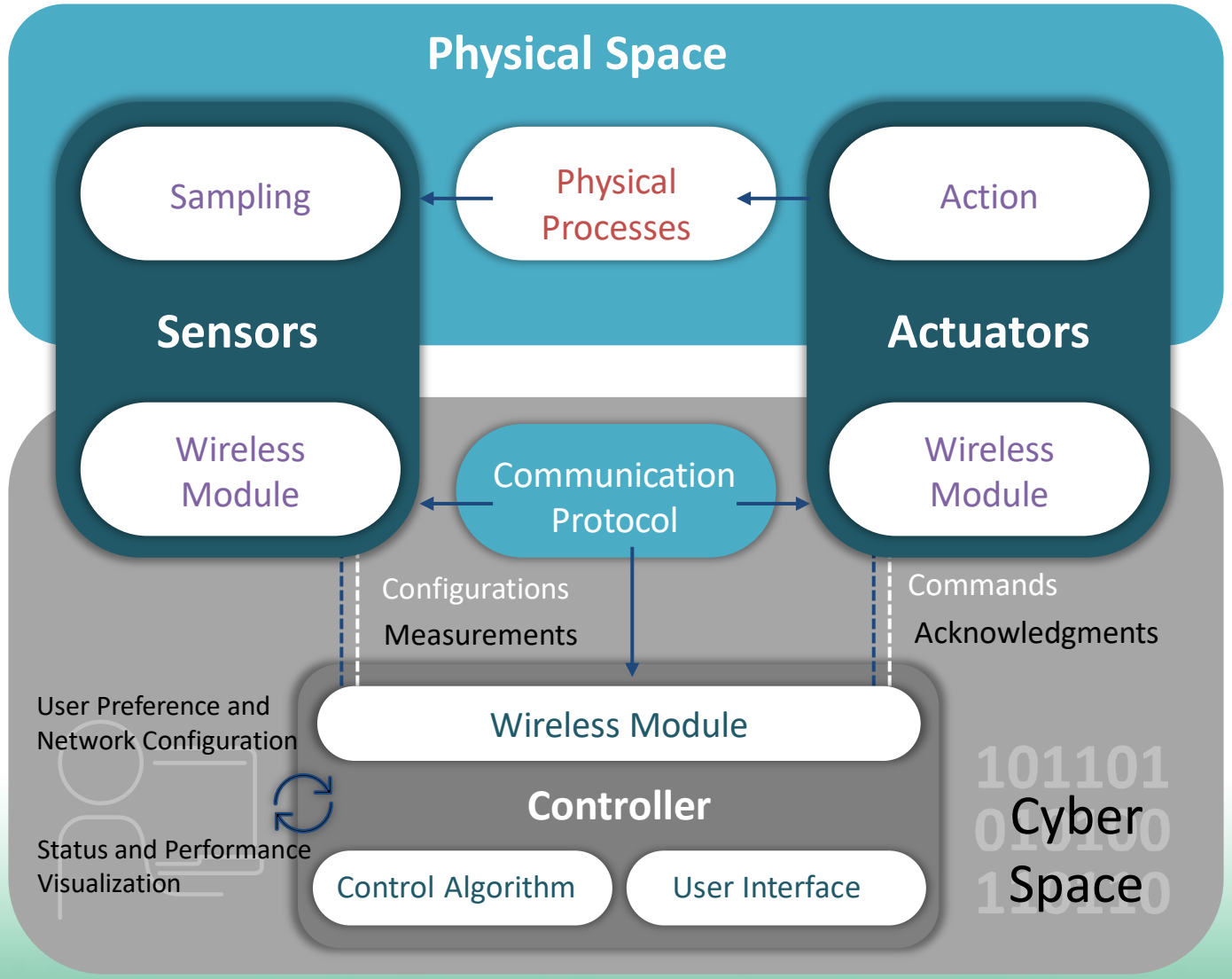
Industry *4.0*

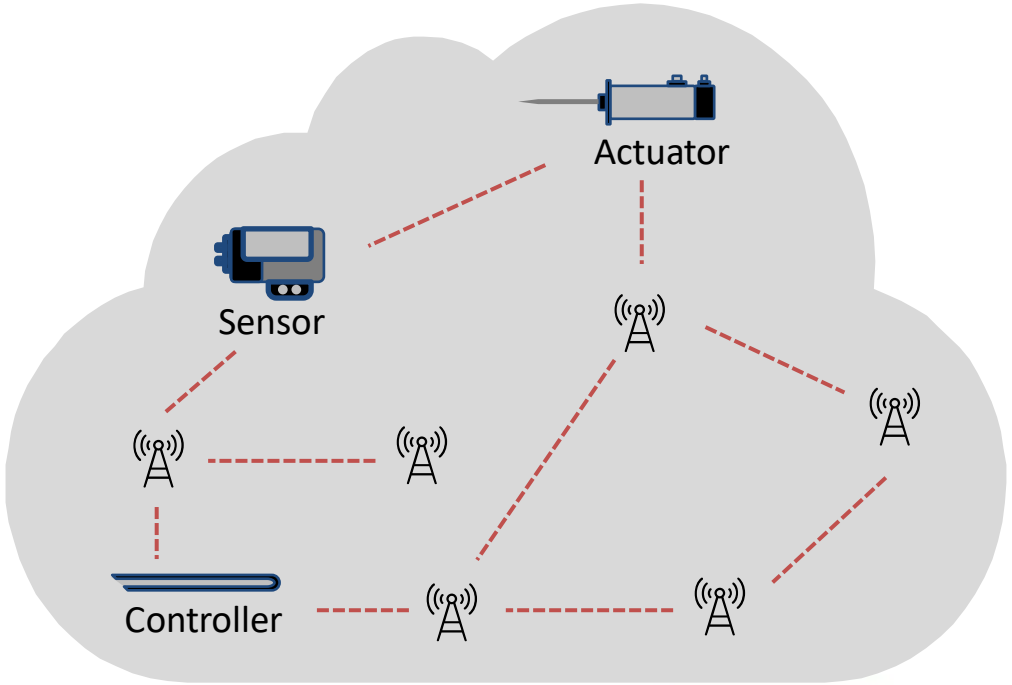
4

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.

Industry 3.0

- Isolated
- Obscure
- Out of context
- Overly Supervised

Industry 4.0

- **Interoperable**
- **Transparent**
- **Aware and supportive**
- **Autonomous in decision-making**

Higher Sustainability

Higher productivity

Increased flexibility

Cost reduction

Expectations are skyrocketing

60% believe I4.0

Will Increase Revenues

55% believe I4.0

Will Lower Costs

70% believe I4.0

Will increase efficiency

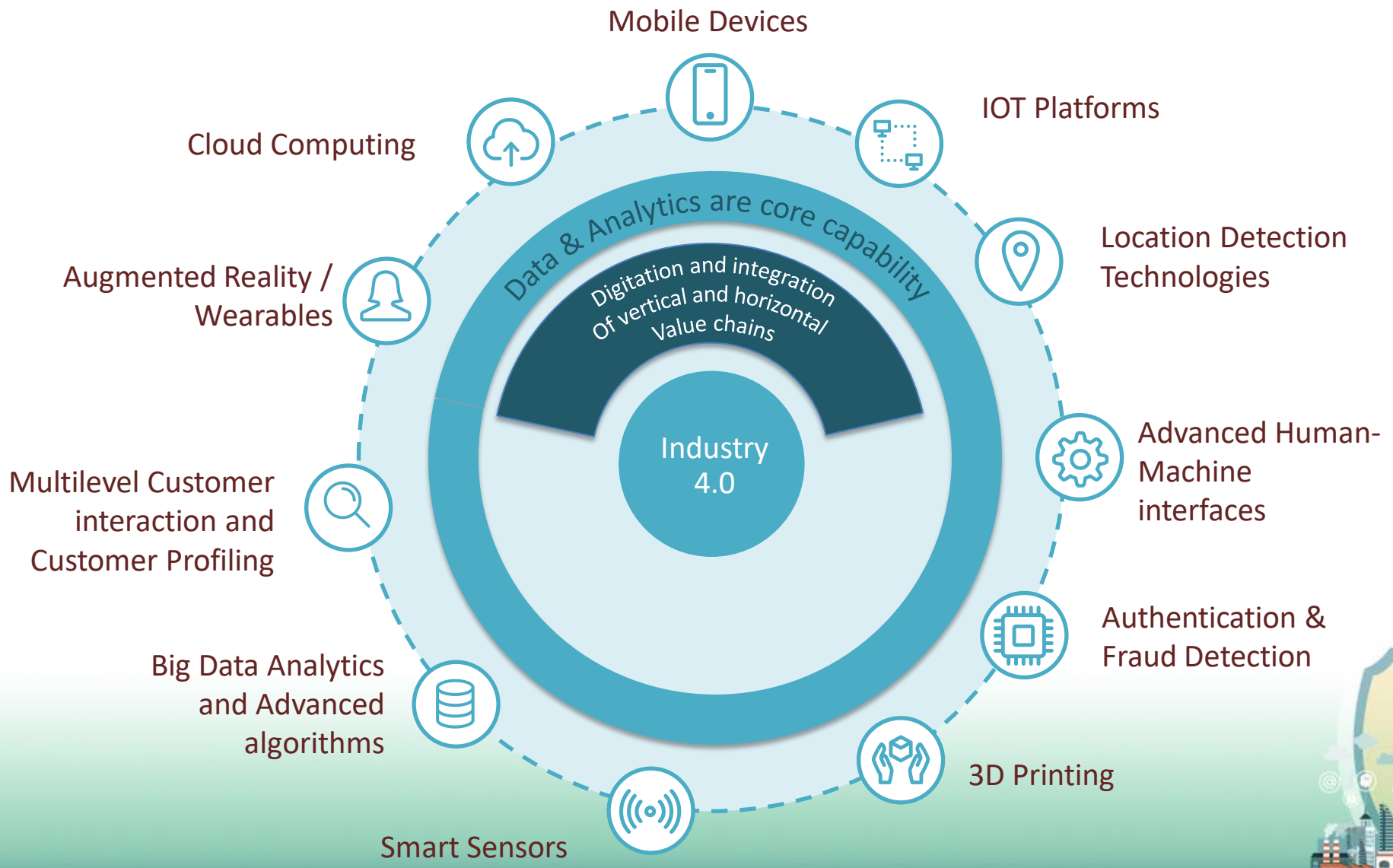
IDC Survey

SYSTEX A DATA COMPANY

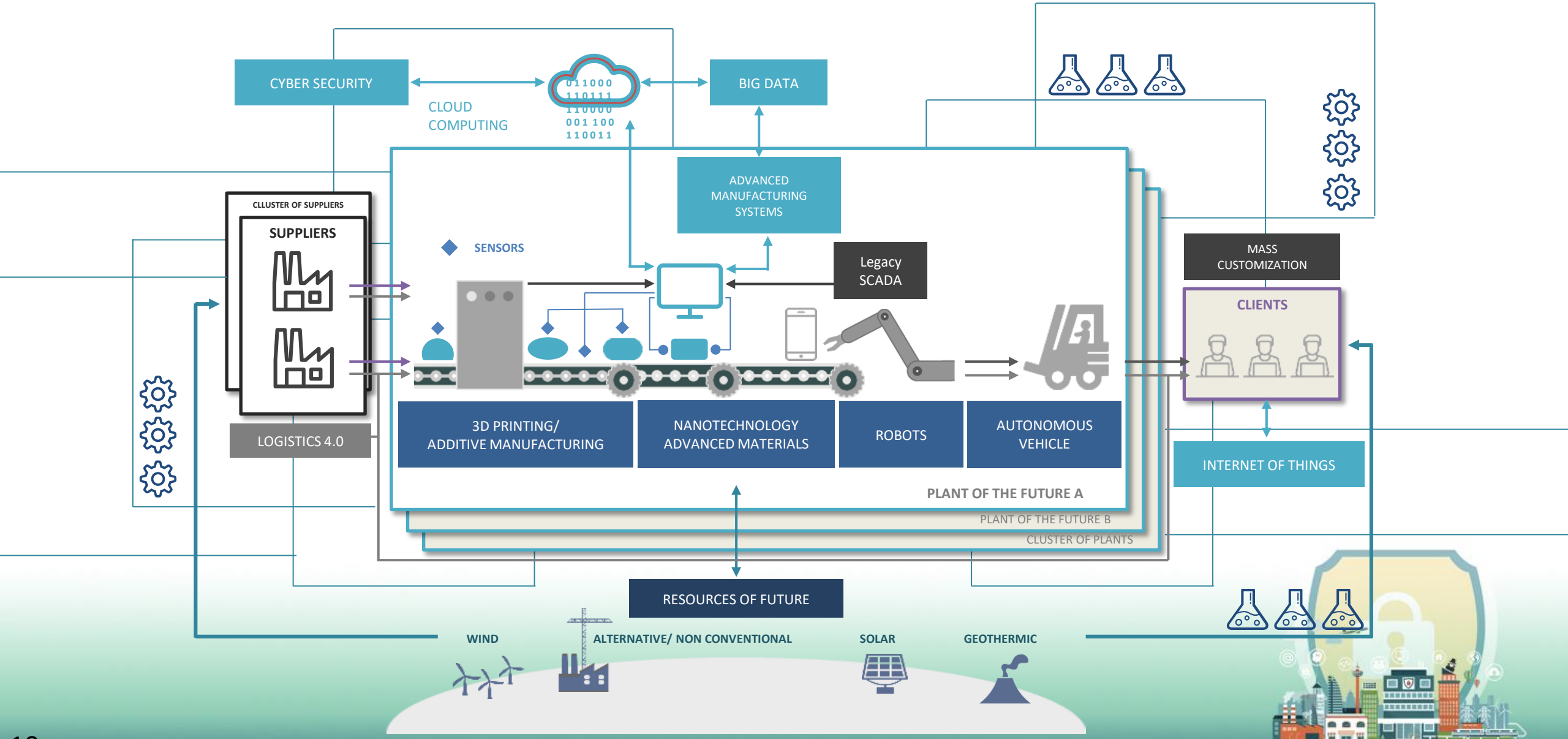
But not all is bright….

CYBERBIT

We imagine industry 4.0 like this….



But it looks more like this…



Increasingly Exploiting the Growing Connectivity

Ukraine

Power Grid Attack (2016)

German

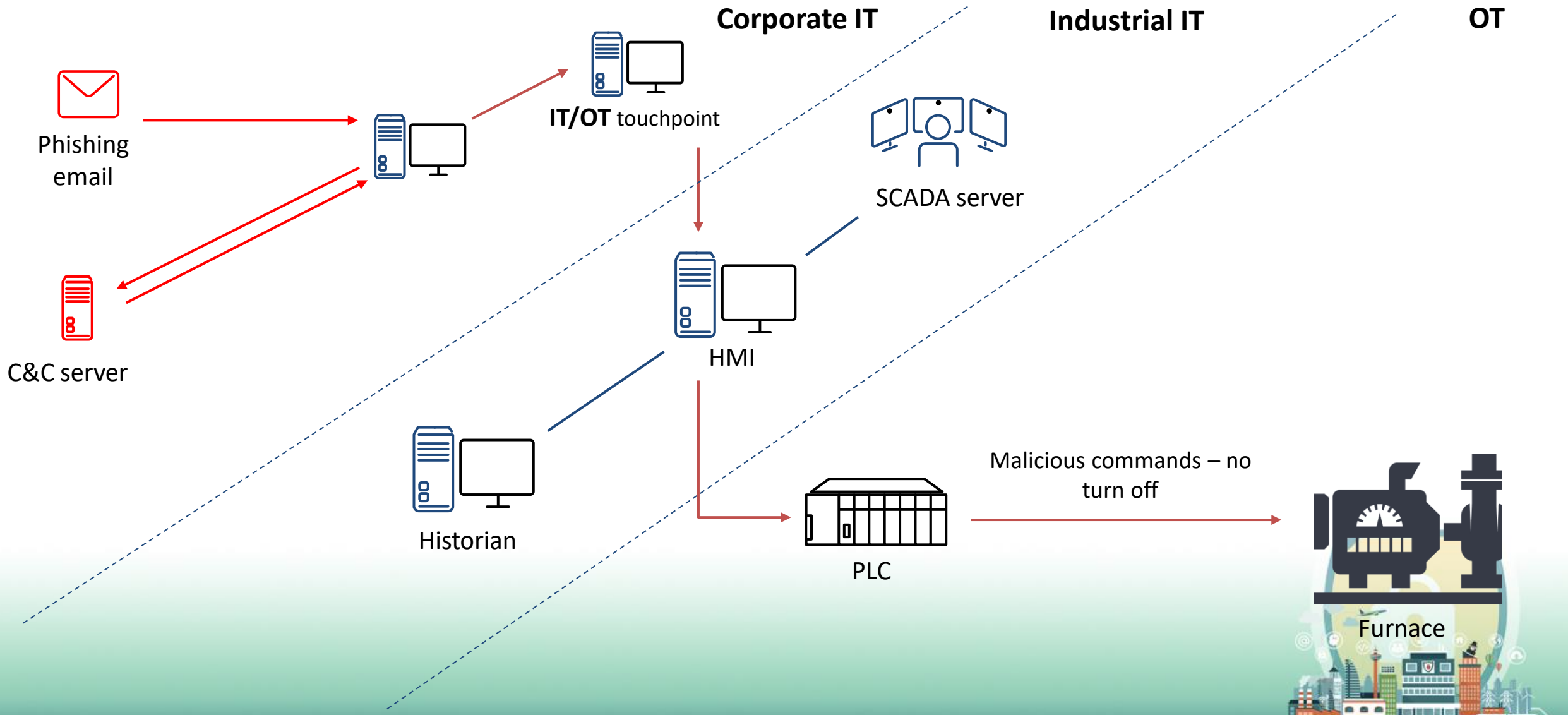
Steel Mill Attack (2015)

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)

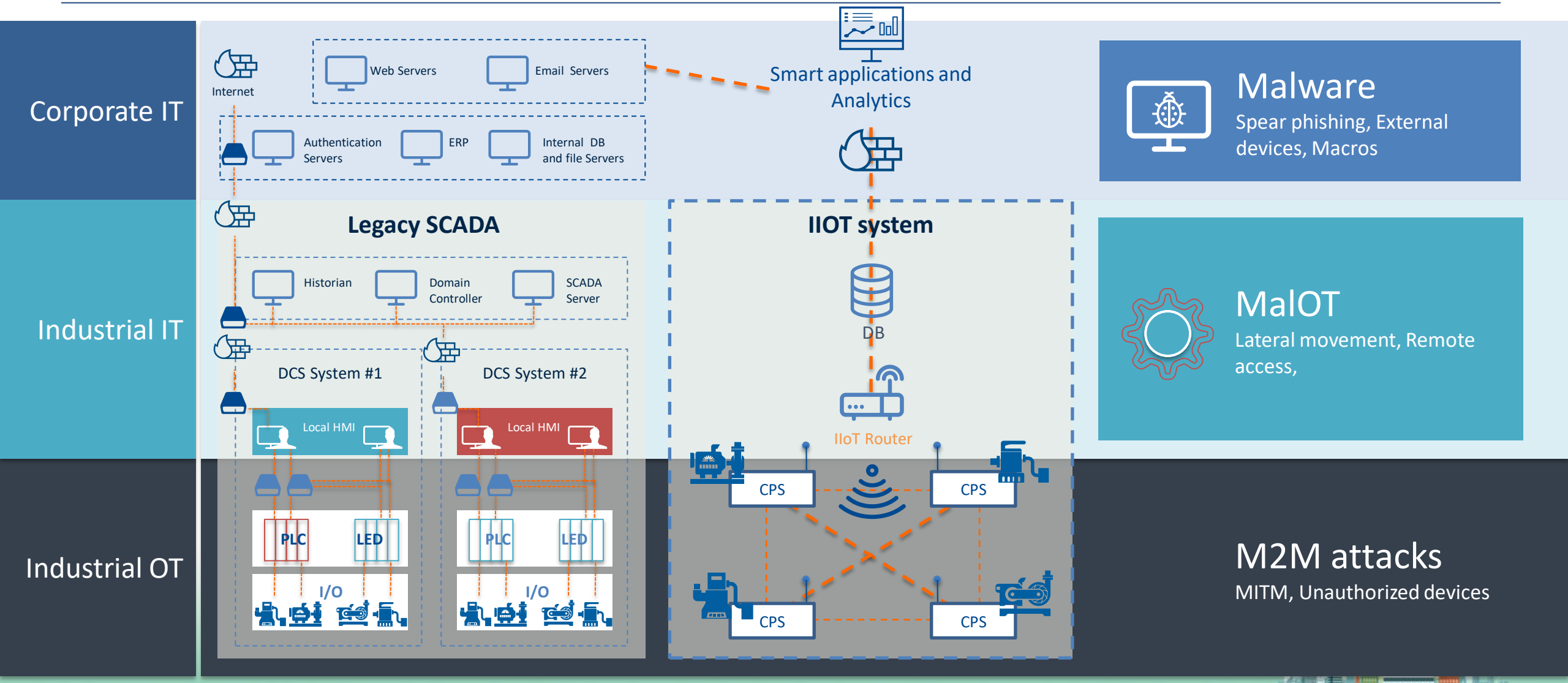
Wide Attack surface

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



101101
010100
110110

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

SANS 2016 State of ICS Security Survey

Introducing Cyberbit SCADAshield

CYBERBIT

The Challenge: SCADA networks are unprotected

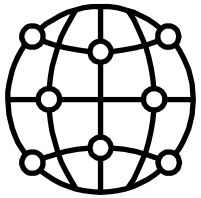
Insecure "by design" –

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

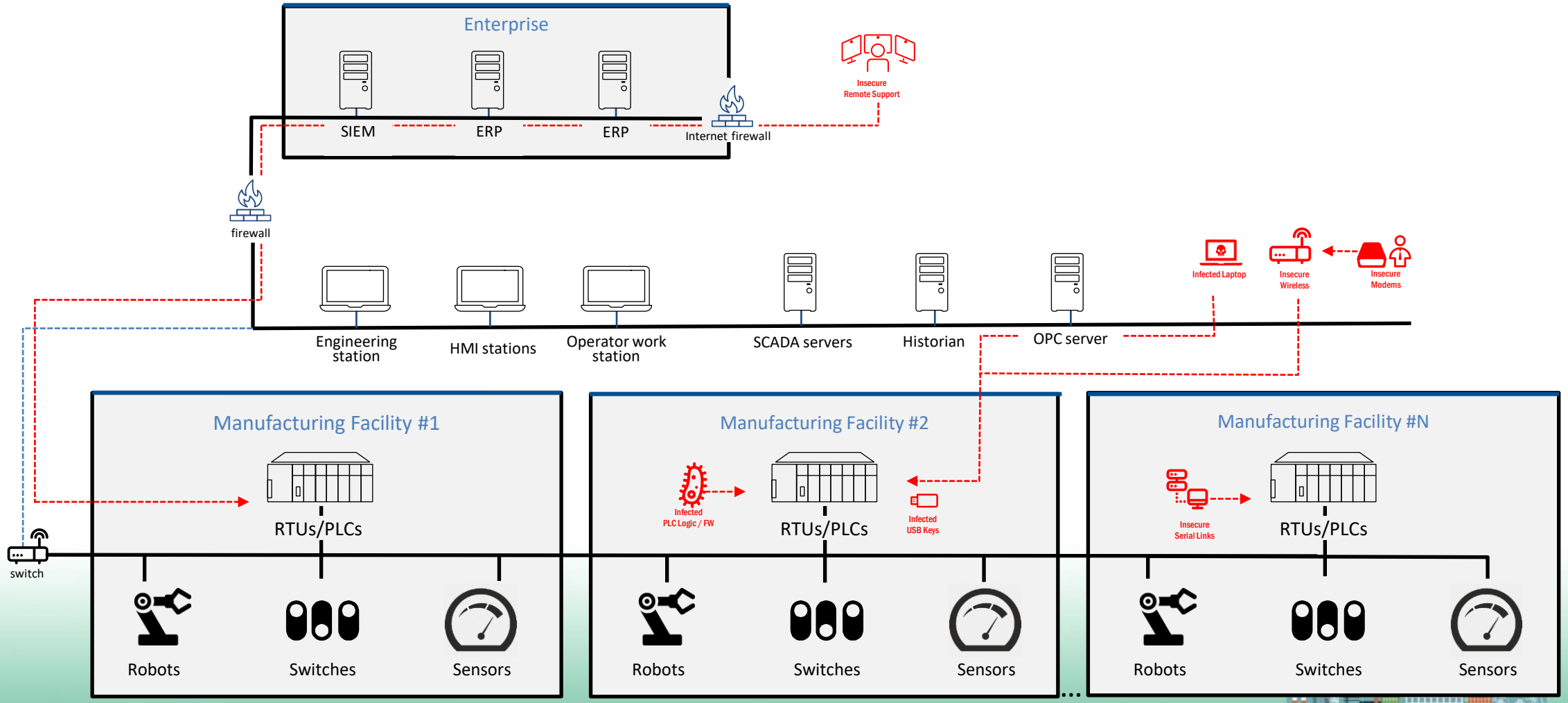
Lack of visibility –

assets, commands and communications

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

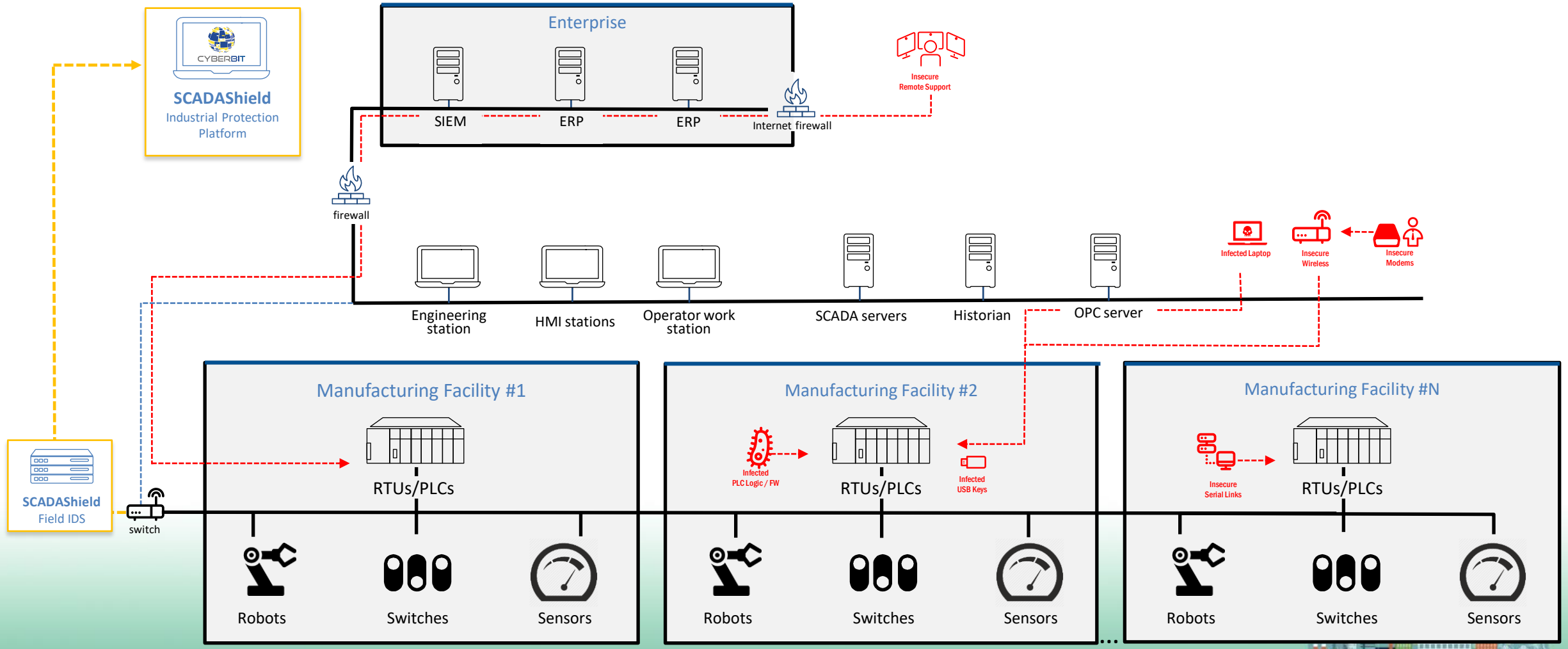
SYSTEX A DATA COMPANY

Manufacturing Automation Systems are Under High Risk



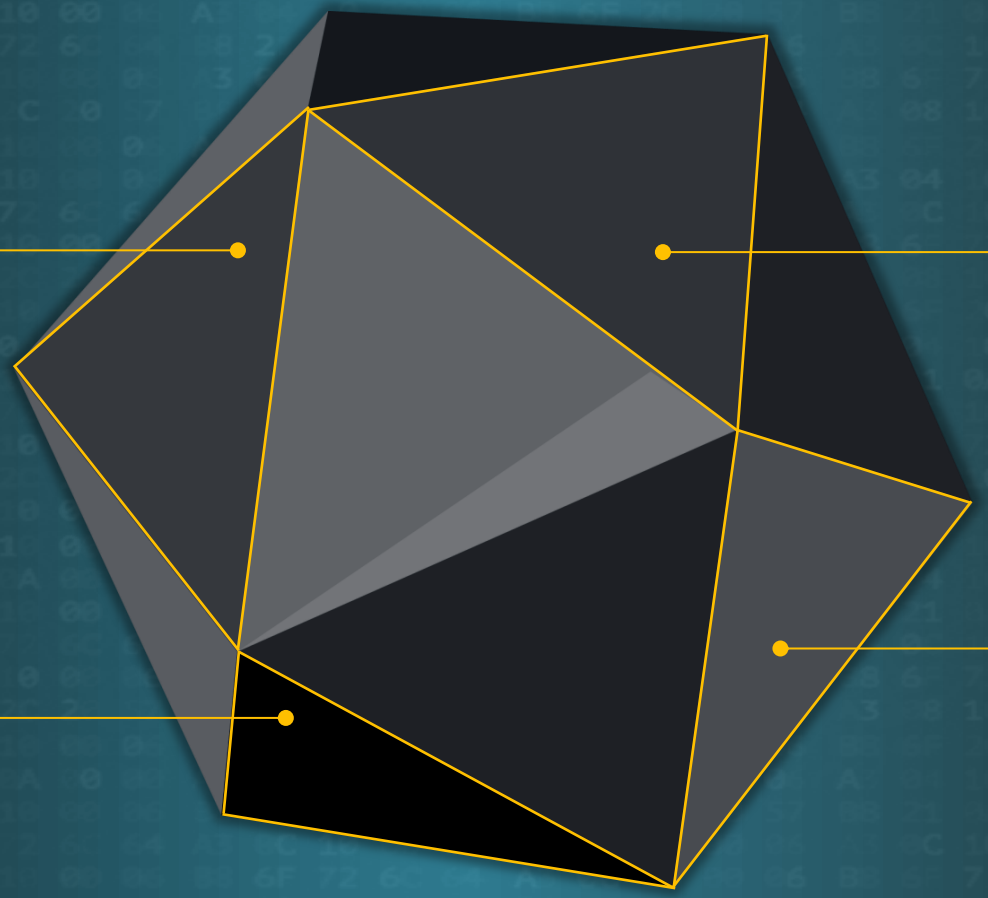
SYSTEX A DATA COMPANY

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



SYSTEX A DATA COMPANY

SCADAShield Industrial Protection Platform



Network **Discovery & Visibility**

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

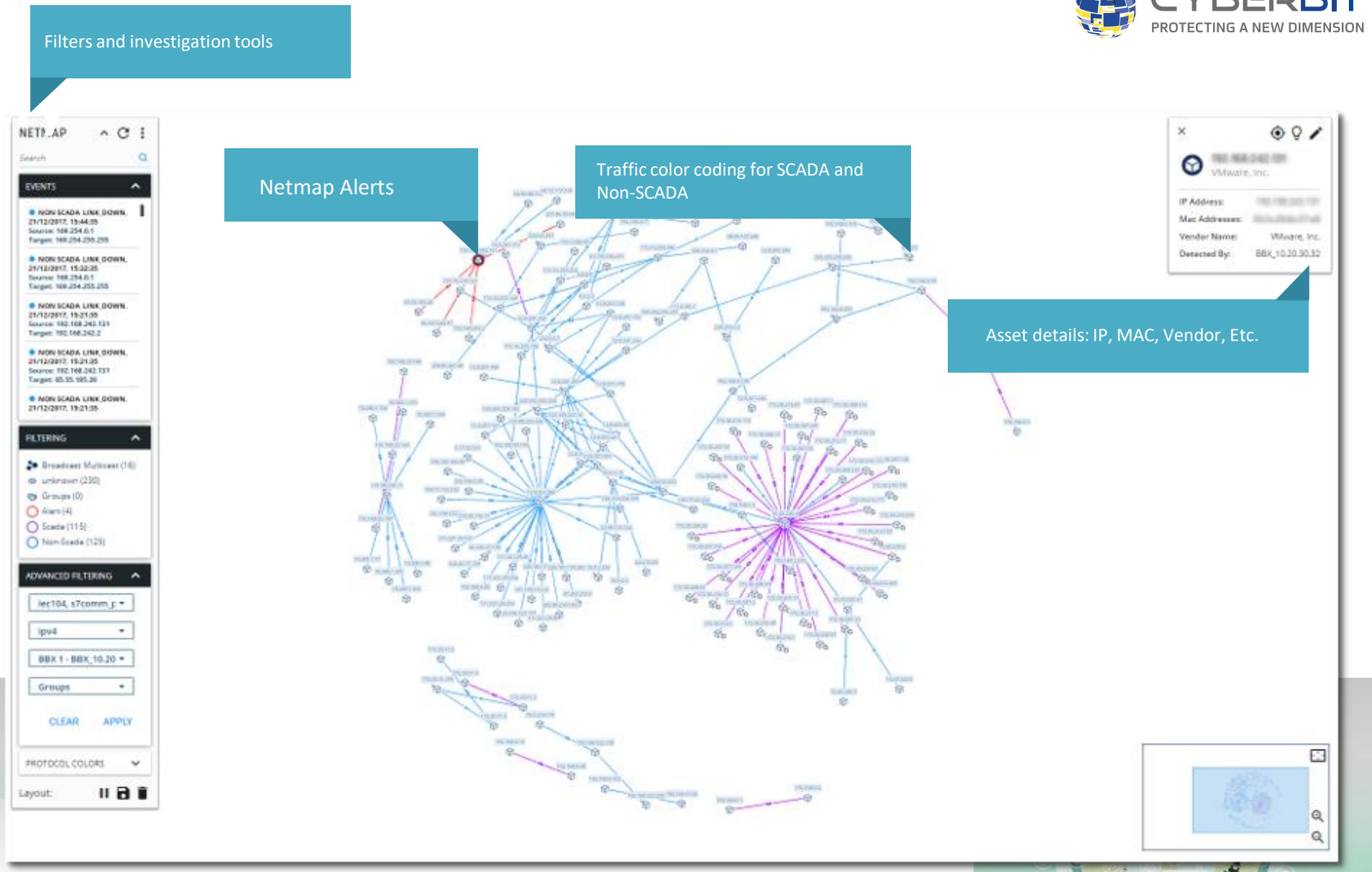
Detection of **unknown industrial threats**

Detection of **Operational malfunction & misconfiguration**

SYSTEX A DATA COMPANY

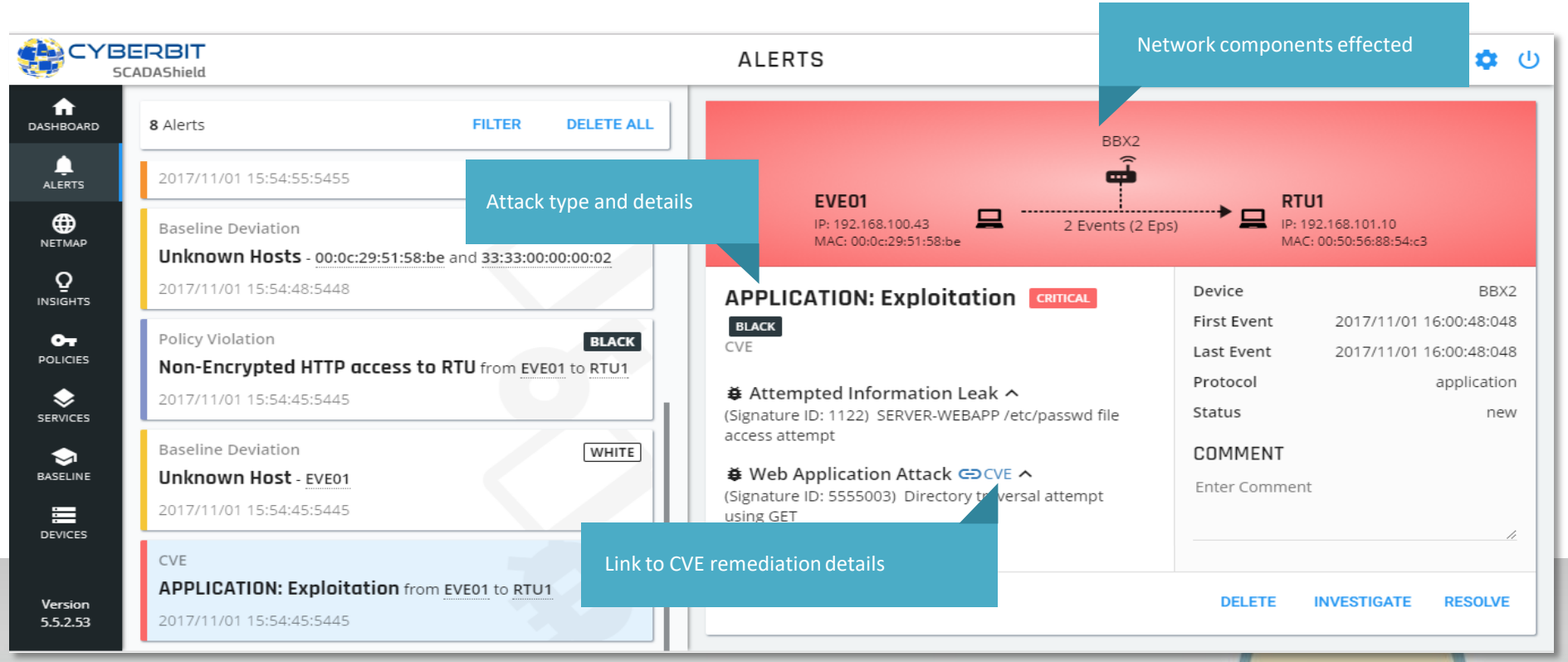
Network Discov

- 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



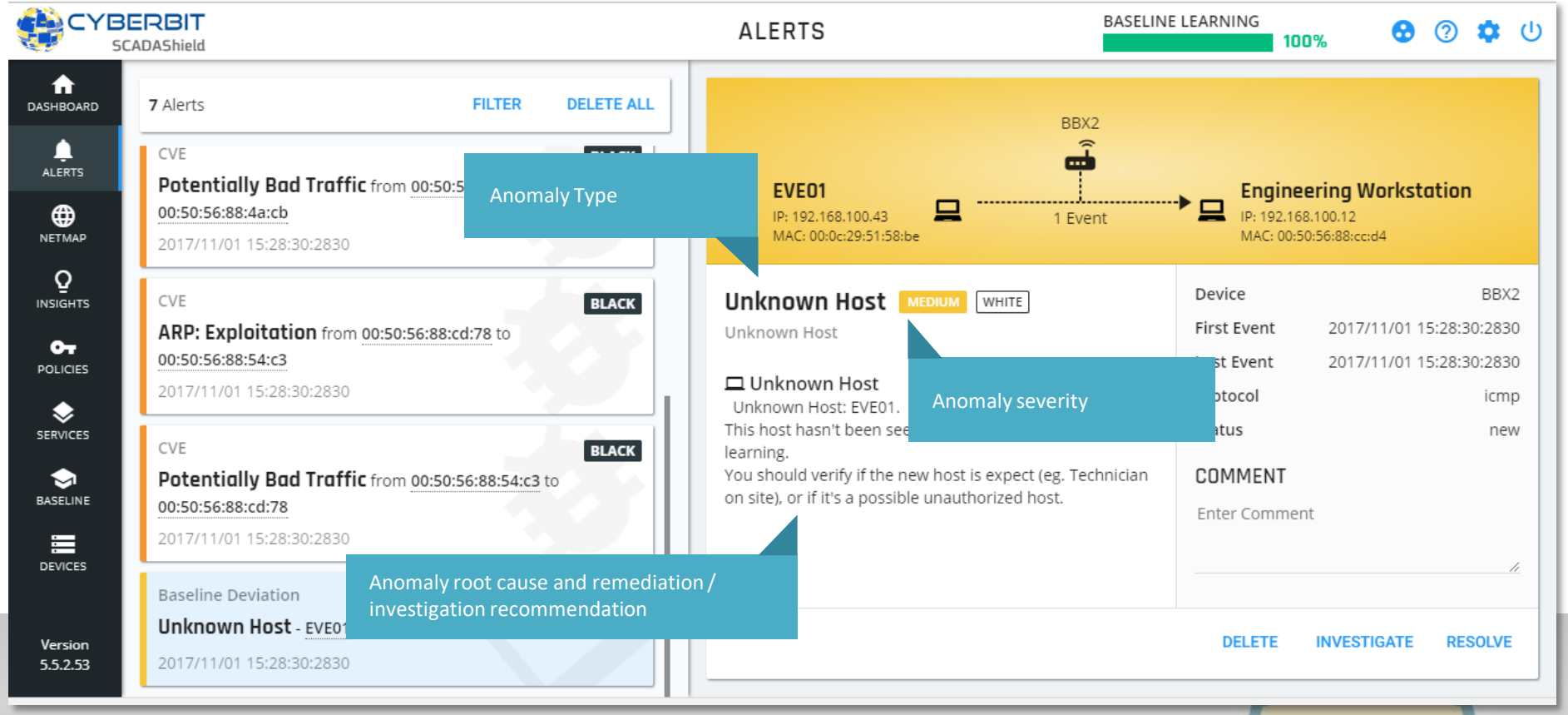
Known Vulnerability

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



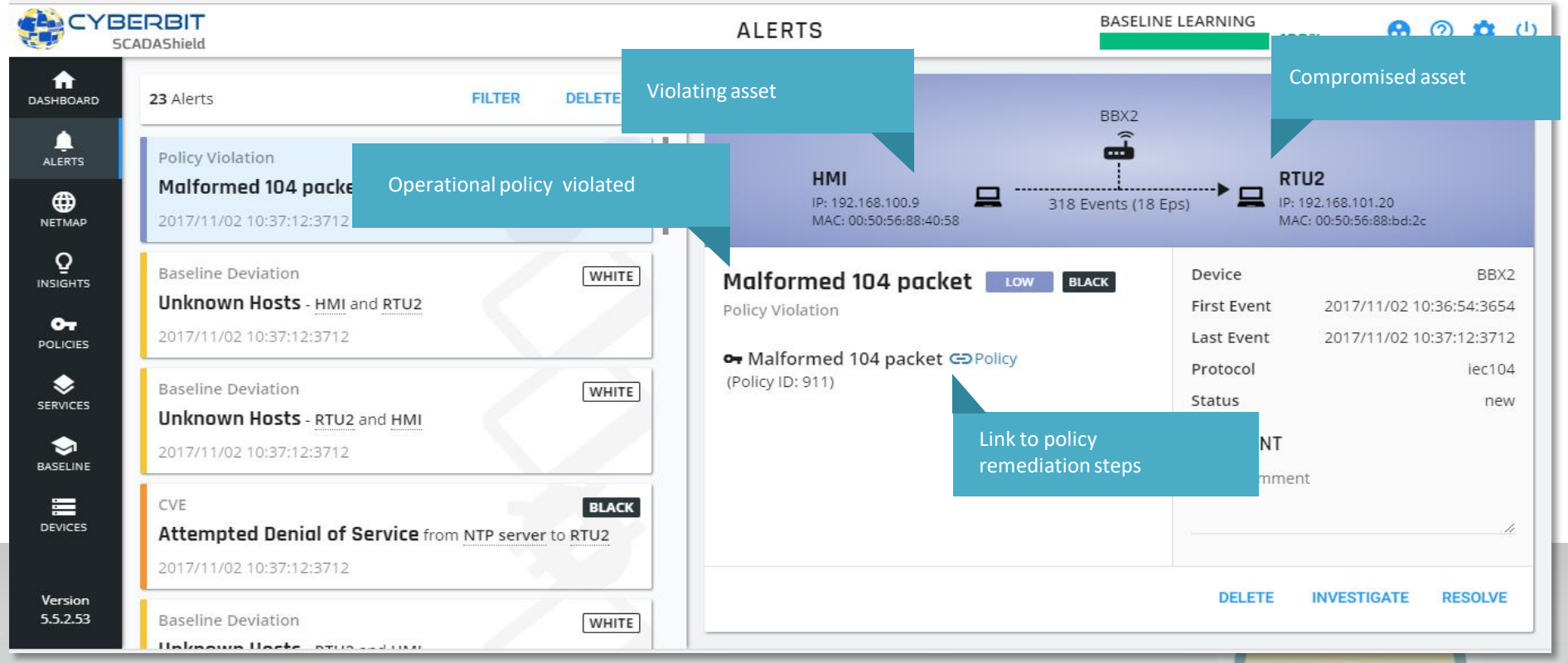
Unknown Threa

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



Operational Anomalies

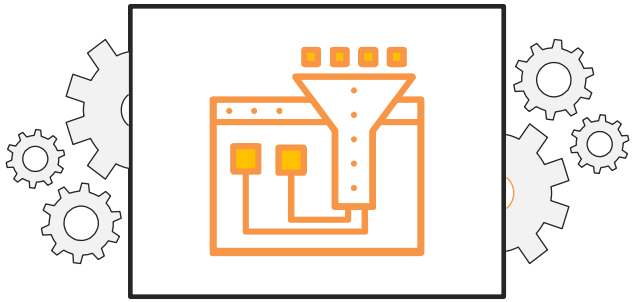
- Based on operational policies created by Cyberbit and the Operational team
- Detects possible system malfunctions and misconfigurations



SCADAShield Operational Flow

Monitor SCADA and IT Communications

Industrial Analytics Engine



Discovery
Network discovery & continuous **visibility**

Known Vulnerabilities
Detection and response to **known vulnerabilities** for SCADA and IT

Unknown Threats
Detection and response to **unknown attacks**

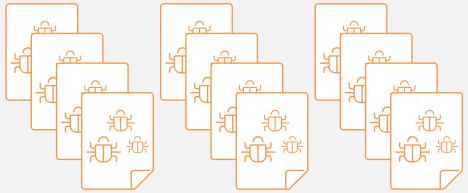
Operational Anomalies
Detection of **operational anomalies** & malfunctions

SYSTEX A DATA COMPANY

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

SYSTEX A DATA COMPANY

Wide Vendor and Protocol Coverage

Vendors

MITSUBISHI
General Electric
Honeywell
Rockwell Automation
SIEMENS
ABB
EMERSON
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

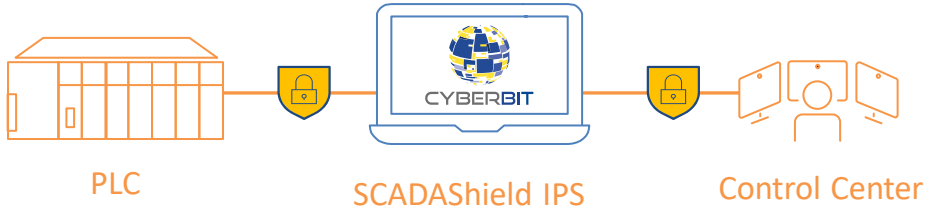
- Known SCADA CVE's
- Field to Field attacks
- Anomalous PLC behavior
- Malformed packets
- Out-of-range value commands to PLC/RTU

Known vulnerabilities **Unknown threats** **Operational violations**

SCADAShield Advanced Capabilities

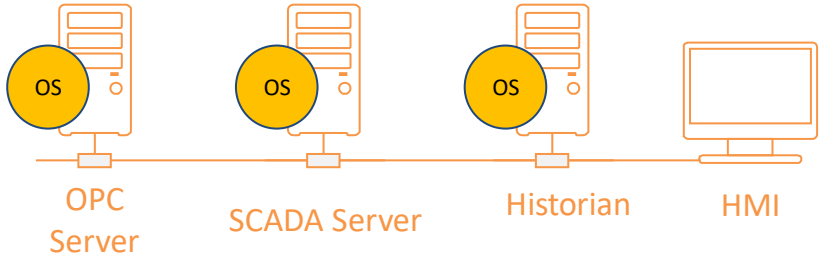
SCADAShield IPS

Inline installation delivers IPS capabilities for attack prevention



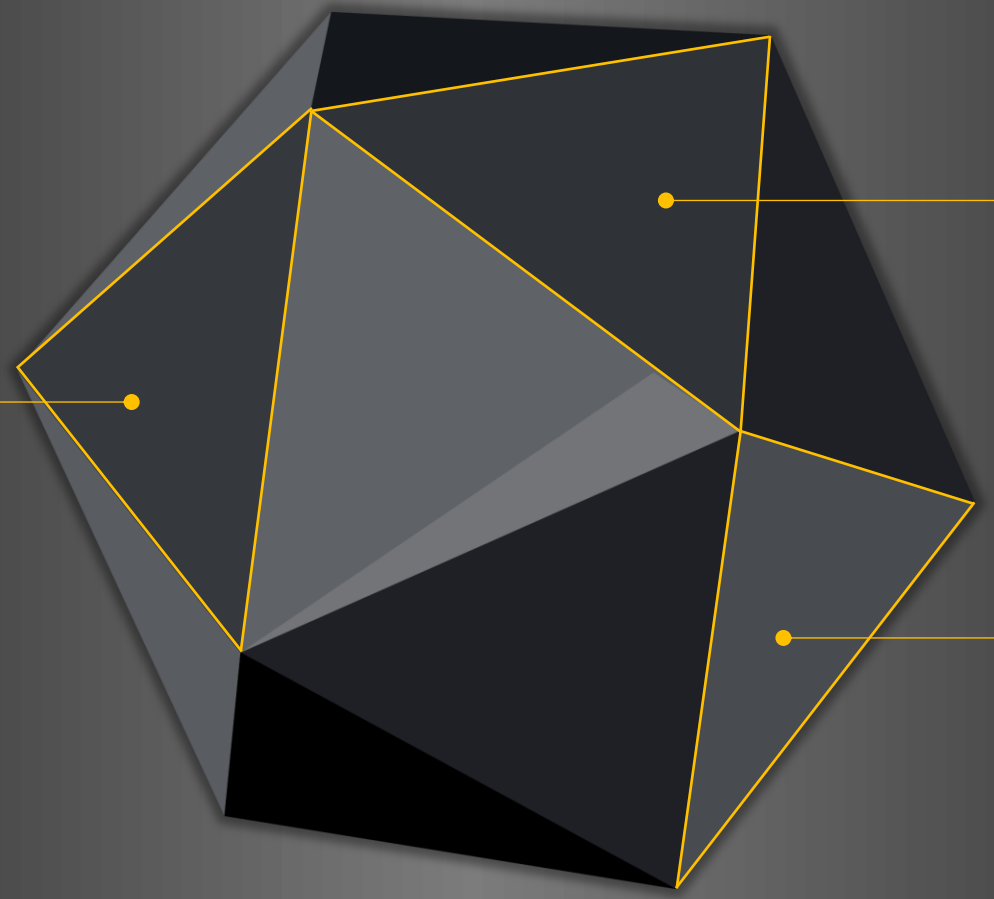
SCADAShield OS

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 downtime

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

Reduce Reputation Risk

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

Support compliance requirements

Support cyber security ISA/IEC and NERC CIP

Thank You

CYBERBIT
PROTECTING A NEW DIMENSION