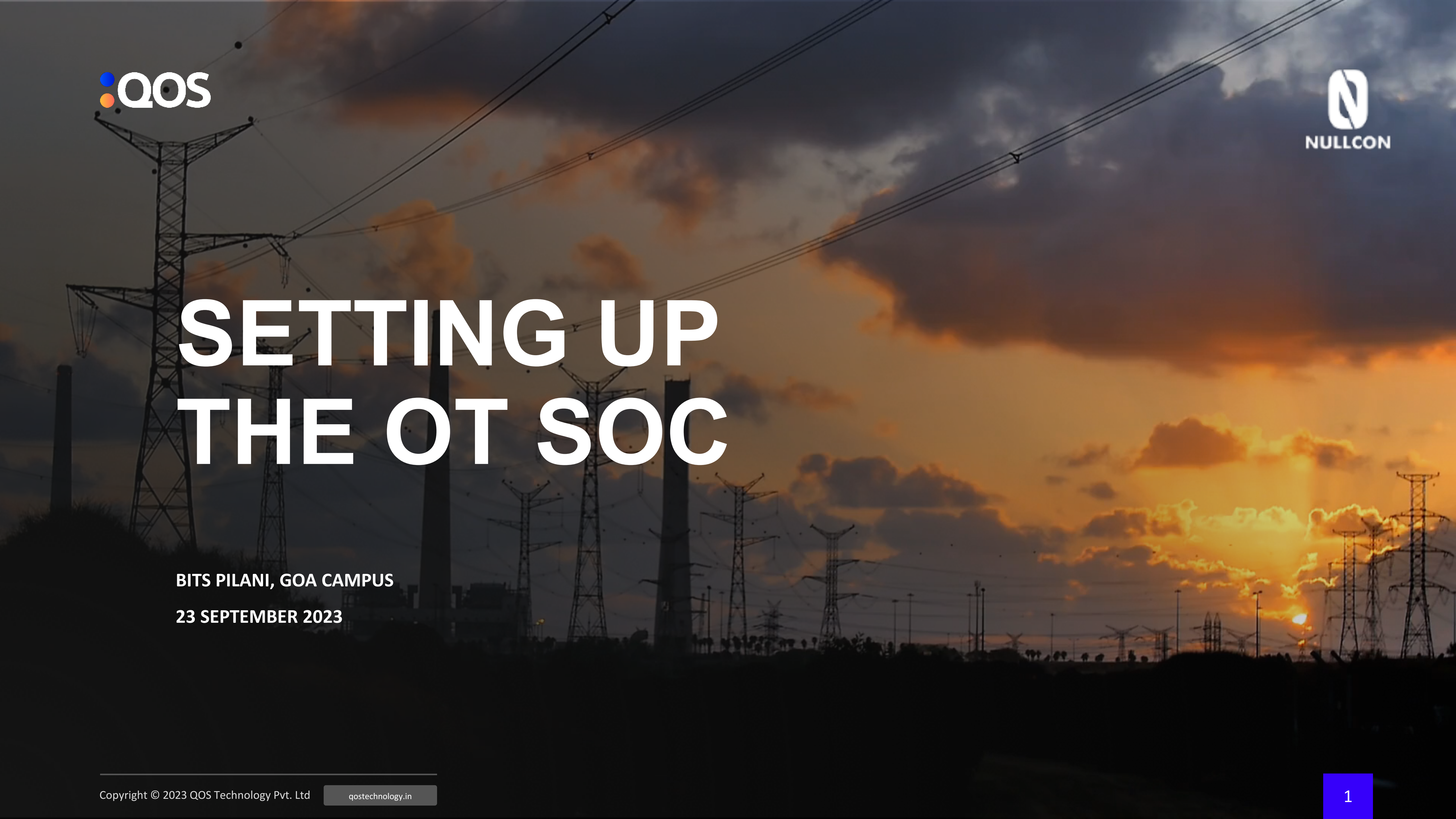


SETTING UP THE OT SOC

BITS PILANI, GOA CAMPUS

23 SEPTEMBER 2023

QOS

- 25 Years Cybersecurity Experience in both, IT and OT Networks
- B.E in 1997 (SLIET); Executive MBA in 2016 (The Wharton School, UPENN)
- Previously worked in Check Point Software Technologies and HCL Technologies
- Carved another Cybersecurity Company with a focus on Product Development & Trainings – PurpleSynapz Labs™

Ramandeep Singh

CEO - QOS Technology

LinkedIn linkedin.com/in/ramanqos

IT BUILDING BLOCKS

- SAP/R3
- MAIL
- CLOUD
- WEBSITE
- API/ SDK
- ERP
- MOBILE APPS
- E-COMMERCE
- CONTAINERS
- PORTAL
- USER EXPERIENCE
- TEAMS’ COLLABORATION APPS
- DATA MINING AND ANALYTICS

OT BUILDING BLOCKS

- SCADA
- PLC
- DCS
- IPC
- IOT
- Historian
- ICS
- RTU/FRTU
- Engineering Workstation
- IED
- Operators’ Console (HMI)

INDUSTRY 4.0

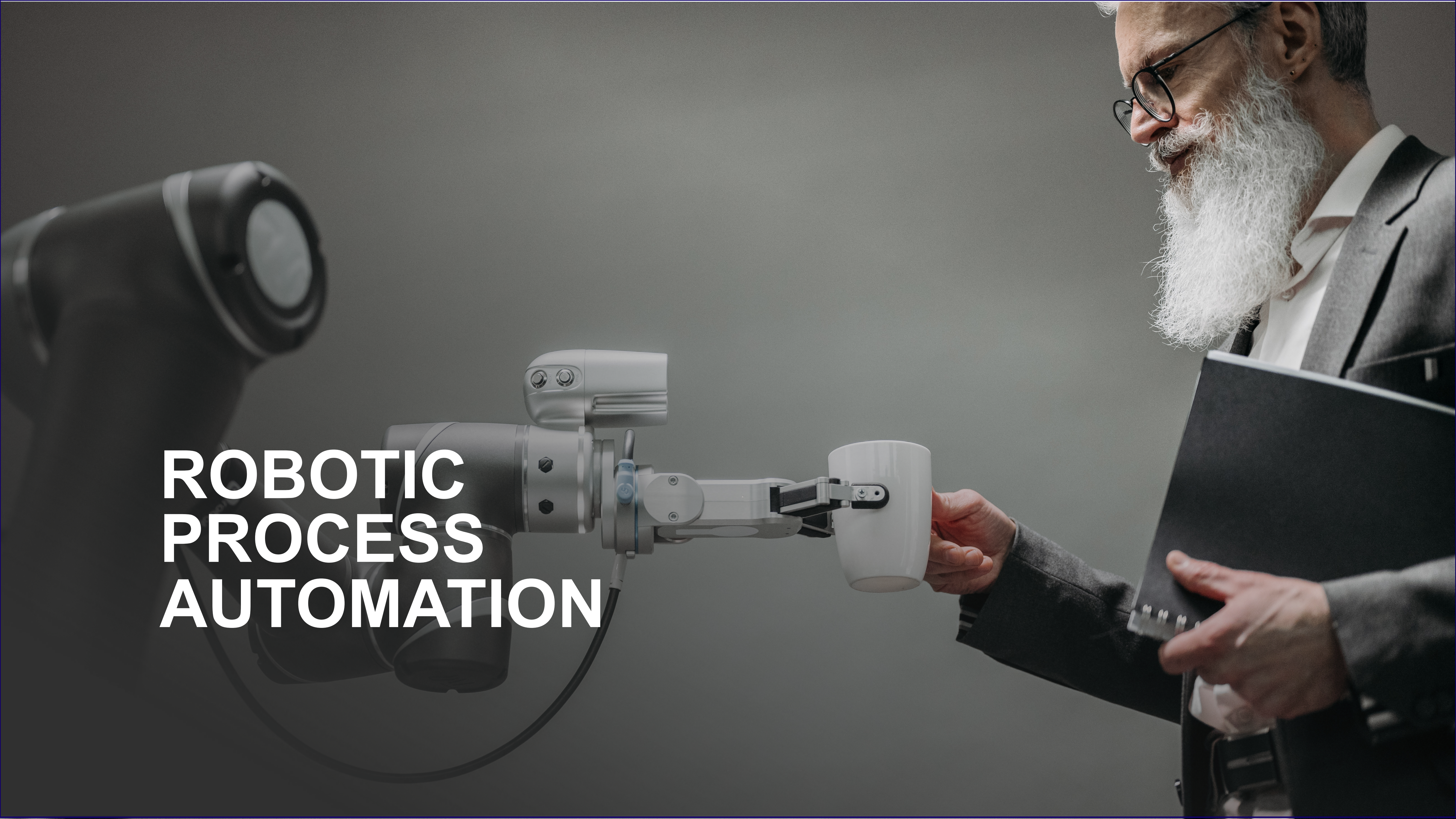
MANUFACTURING 4.0

DIGITAL TRANSFORMATION

INDUSTRIAL METAVERSE

SMART FACTORY

ROBOTIC PROCESS AUTOMATION



VISION SYSTEMS

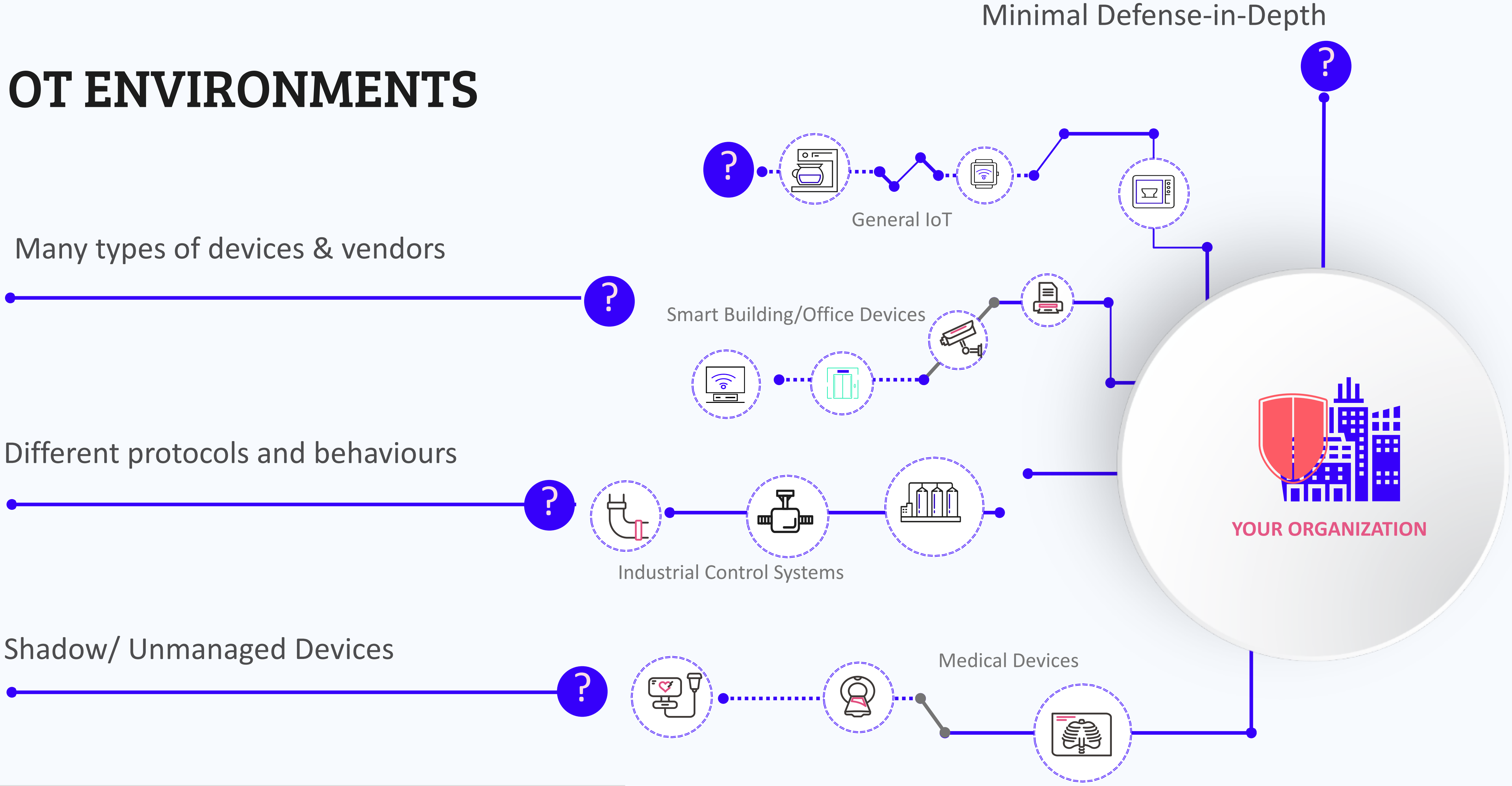
PREDICTIVE MACHINE MAINTENANCE

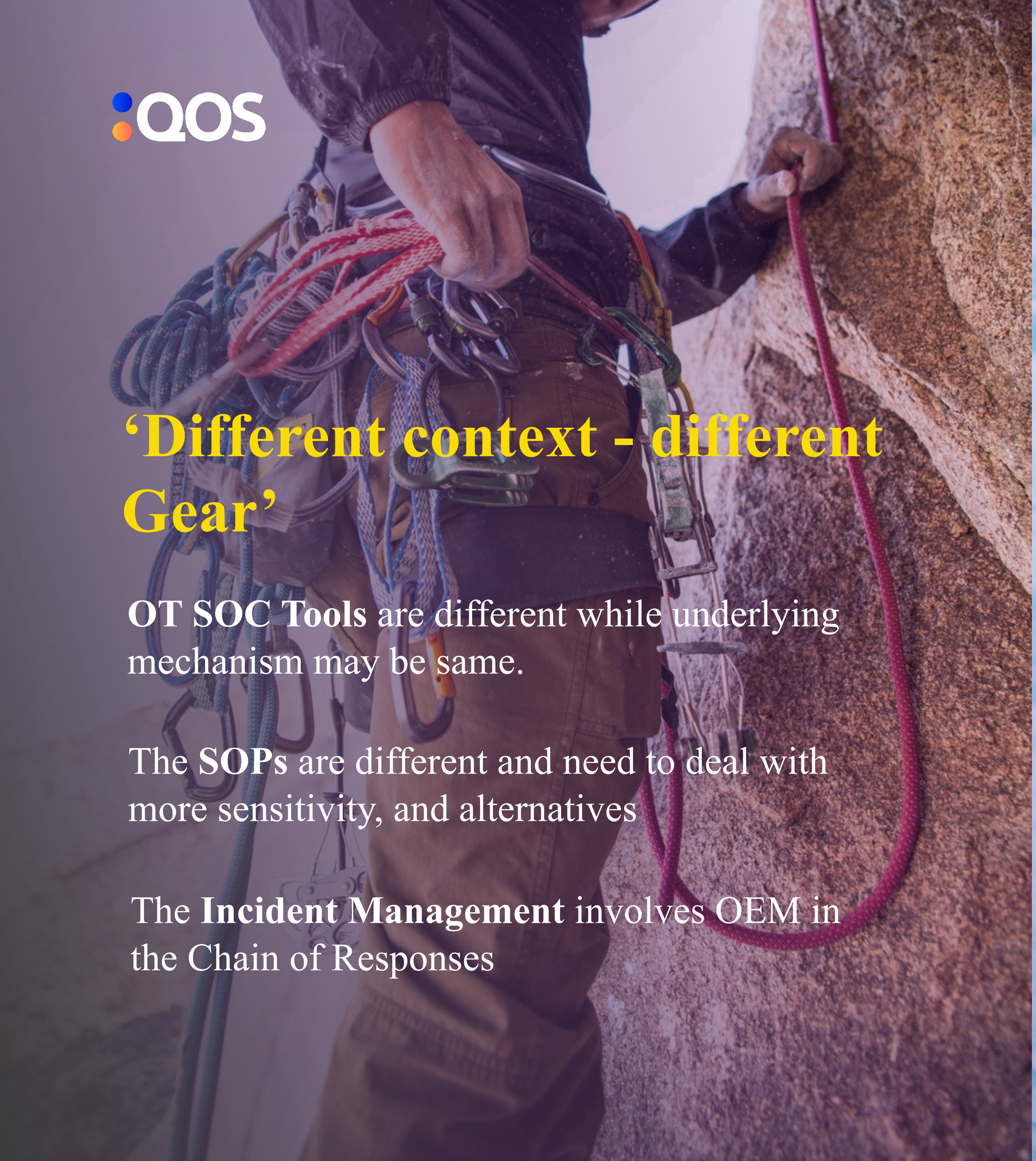
SUSTAINABILITY GOALS

DIGITAL TWINS

LET US SETUP OT SOC

OT ENVIRONMENTS


Minimal Defense-in-Depth
?
?
General IoT
Many types of devices & vendors
?
Smart Building/Office Devices
Different protocols and behaviours
?
Industrial Control Systems
YOUR ORGANIZATION
Shadow/ Unmanaged Devices
?
Medical Devices



‘Different context - different Gear’

OT SOC Tools are different while underlying mechanism may be same.

The **SOPs** are different and need to deal with more sensitivity, and alternatives

The **Incident Management** involves OEM in the Chain of Responses

DESIRED STATE OF SECURITY OPS

OT Network Situational Awareness

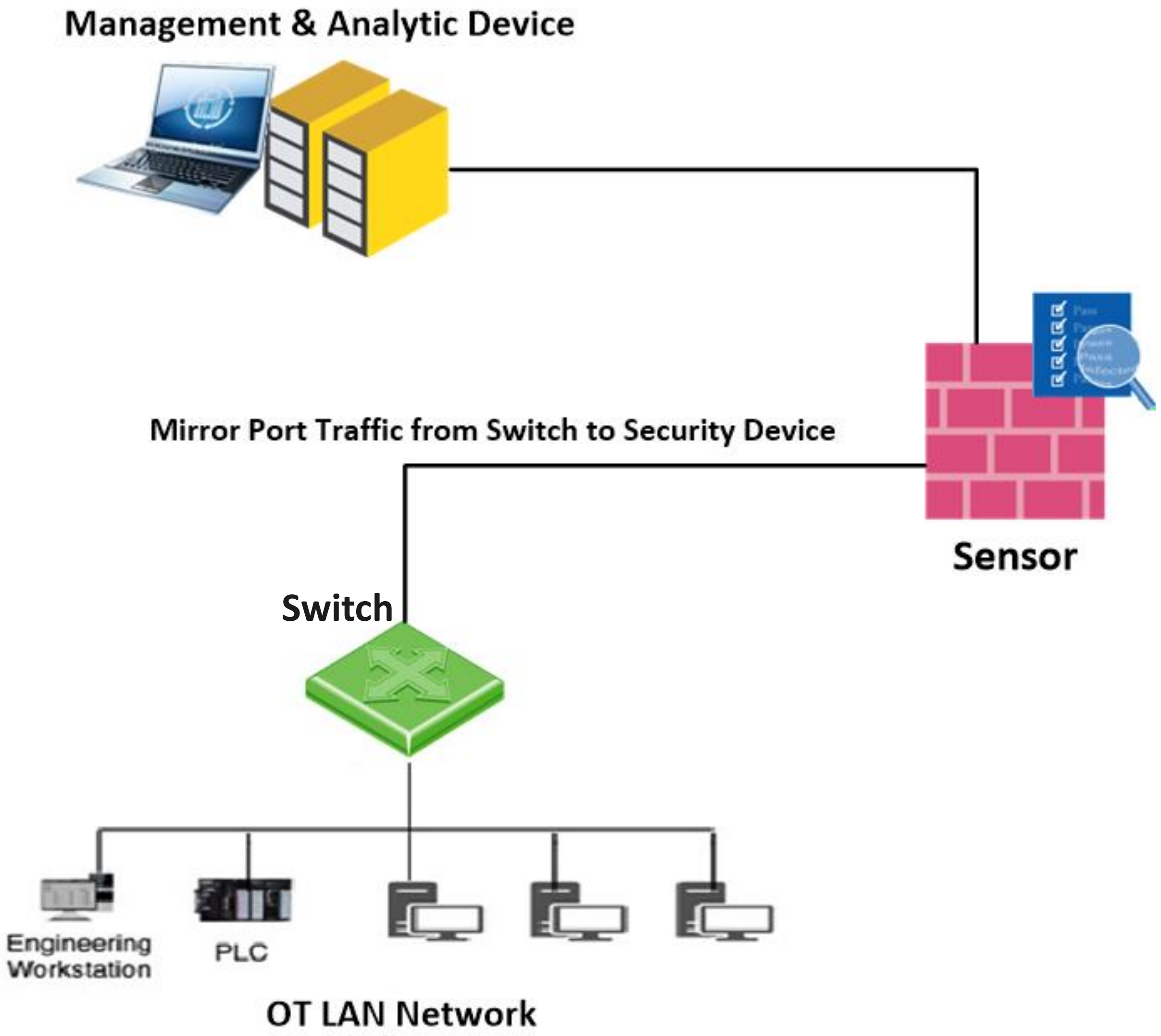
- Real Time Visibility for IT-OT, OT Networks.
- Real Time Visibility for IIoT, Edge Components, and Cloud Instances
- **OT Sensors:** Passive Scanning of Assets for Known Vulnerabilities in OT, IT-OT, and IIoT
- **OT Security Analytics:** Threats Management for the OT and IIoT Networks:-
    - Malicious Activity Detection & Prevention,
    - Risk Assessment {V, P = f(events), I = f(asset value)}
    - OT, IIoT Best Practices' Violations
    - OT, IIoT Process Variable Anomaly Detection

OT Security Operations Centre (SOC)

- 24x7 OT Network Situation Awareness
- Deploy SIEM or Forward OT Network Situation Awareness logs to IT SIEM
- Correlation of IT events with OT Alerts (Out of Box, and Advanced with Yara/Snort Signatures detection)
- Standard Operating Procedures (SOPs)**
- Threat Intelligence Integration
- Threat Hunting (Research Based, Hypothesis, Internal, Ext, OT Specific, Spray-Pray, Red Team based)
- Adversarial Simulations
    - VAPT, or
    - Digital Twin for Red Teaming in OT, or
    - Both

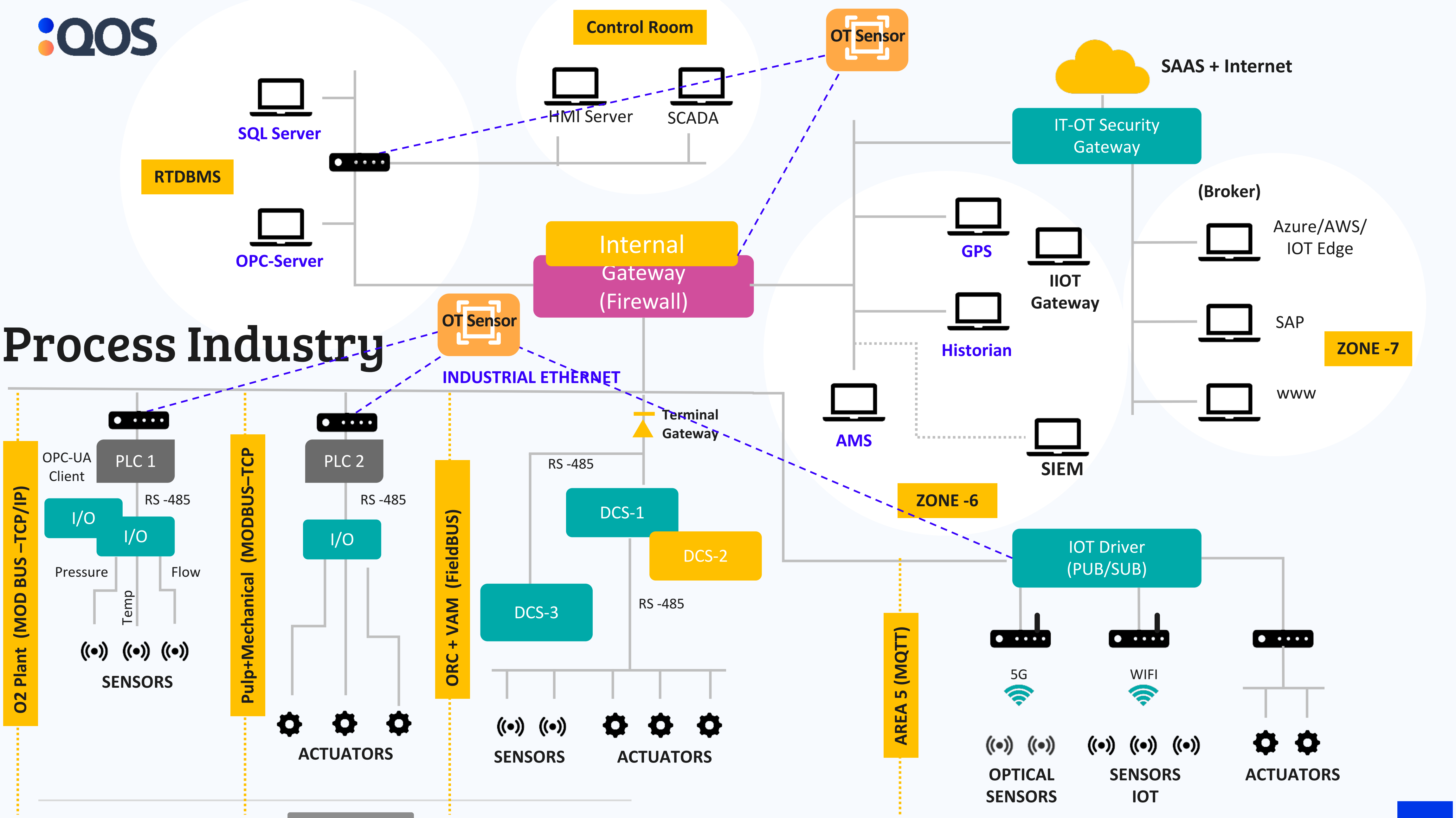
** OT Context is not same as IT

OT NETWORK SITUATION AWARENESS


Management & Analytic Device
Mirror Port Traffic from Switch to Security Device
Sensor
Switch
Engineering Workstation
PLC
OT LAN Network

QOS

Process Industry



Control Room

HMI Server

SCADA

OT Sensor

SQL Server

RTDBMS

OPC-Server

SAAS + Internet

IT-OT Security Gateway

(Broker)

Azure/AWS/ IOT Edge

SAP

www

ZONE -7

Internal Gateway (Firewall)

GPS

IIOT Gateway

Historian

AMS

SIEM

ZONE -6

OT Sensor

INDUSTRIAL ETHERNET

Terminal Gateway

O2 Plant (MOD BUS –TCP/IP)

OPC-UA Client

PLC 1

RS -485

I/O

I/O

Pressure

Temp

Flow

SENSORS

Pulp+Mechanical (MODBUS–TCP

PLC 2

RS -485

I/O

ACTUATORS

ORC + VAM (FieldBUS)

RS -485

DCS-1

DCS-2

DCS-3

RS -485

SENSORS

ACTUATORS

AREA 5 (MQTT)

IOT Driver (PUB/SUB)

5G

WIFI

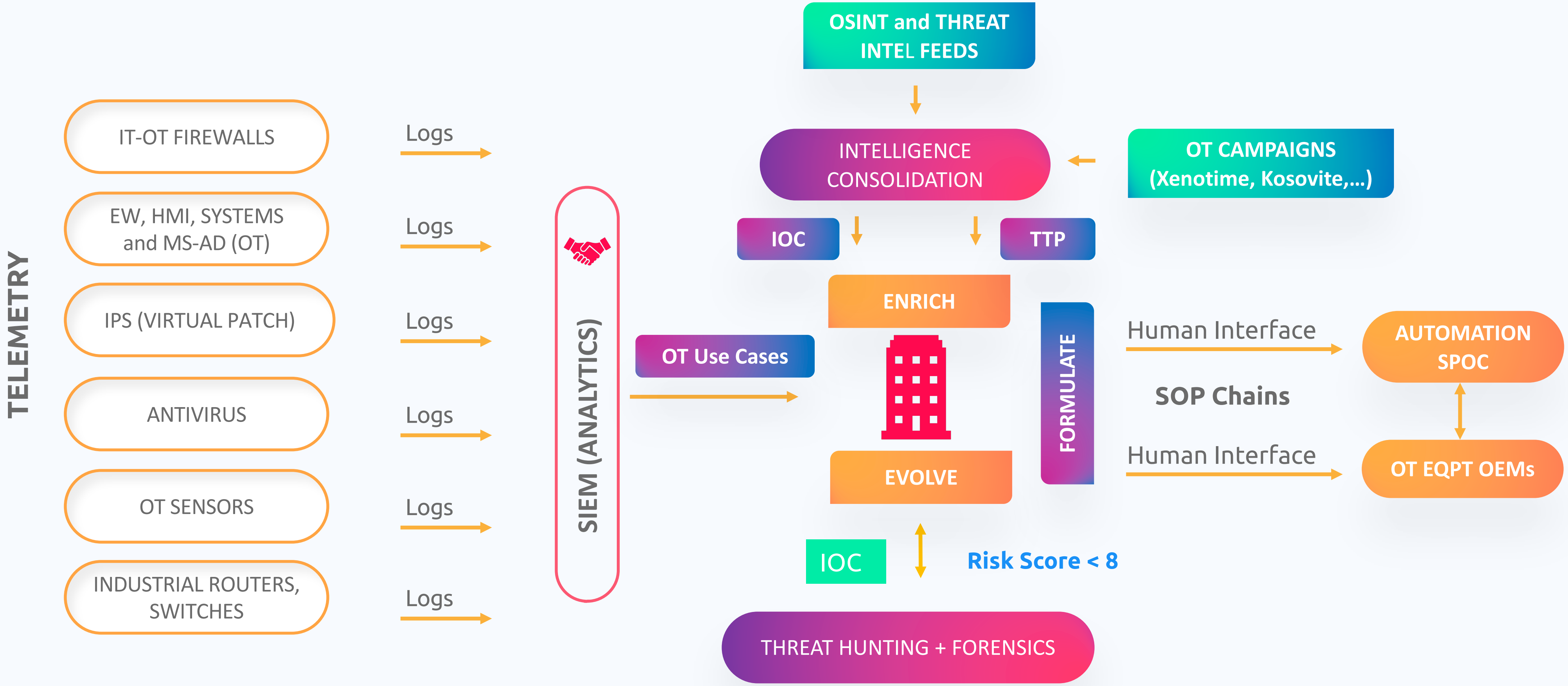
OPTICAL SENSORS

SENSORS IOT

ACTUATORS

RESPONSE & REMEDIATION

SIEM + Managed Detection & Response



TELEMETRY

IT-OT FIREWALLS

EW, HMI, SYSTEMS and MS-AD (OT)

IPS (VIRTUAL PATCH)

ANTIVIRUS

OT SENSORS

INDUSTRIAL ROUTERS, SWITCHES

Logs

Logs

Logs

Logs

Logs

Logs

SIEM (ANALYTICS)

OT Use Cases

OSINT and THREAT INTEL FEEDS

INTELLIGENCE CONSOLIDATION

OT CAMPAIGNS (Xenotime, Kosovite,...)

IOC

TTP

ENRICH

EVOLVE

FORMULATE

IOC

Risk Score < 8

THREAT HUNTING + FORENSICS

Human Interface

SOP Chains

Human Interface

AUTOMATION SPOC

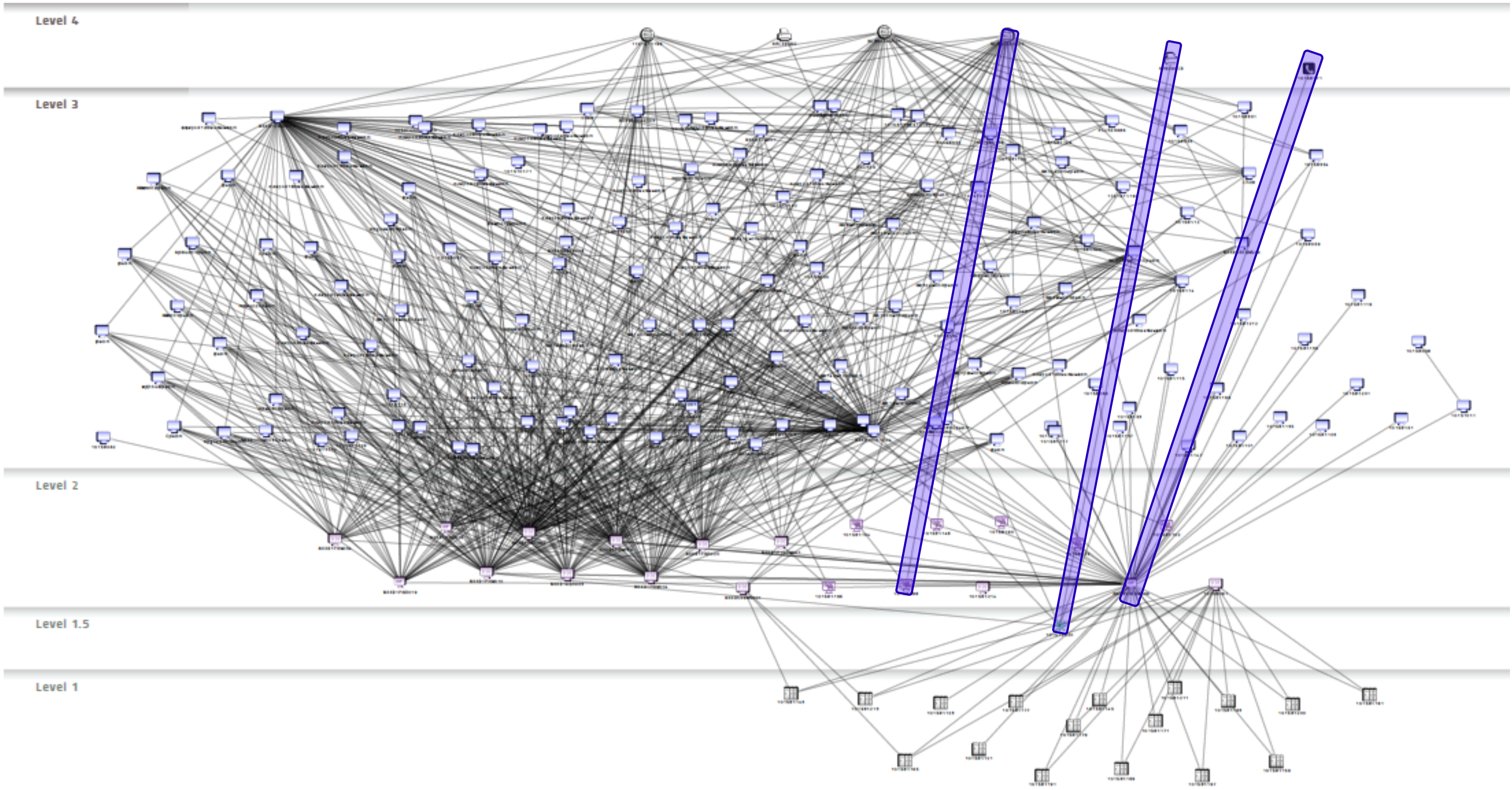
OT EQPT OEMs

OT SOC IS NOT JUST OPERATIONS

IT-OT Firewall	Review and fine-tune config, In IT SOC it’s device management team job. Check for Execution/Coverage
Key IT Systems (SCADA)	Crown Jewel Analysis, Logs Retention, Digital Twins for Testing
Virtual Patch	Compensatory Control, Detection Personas for SIEM
OT Sensors	No. of Assets, Choke Point Selection, Ethernet Switches Mirroring, Serial Networks – Asset/Risk Information
OT SOC Use Cases	IT-OT Specific, IEC 62443 Violations, specific to OT Protocols in use, Process Variables’ Anomalies
Threat Intel Feeds	Very few OT specific, Need to go for curated than straight forward push/pull
Threat Informed Defenses	Enhance the Detection & Response Persona with Adversary Simulations (Tabletop and Digital Twin)

CORE SOC OPERATIONS

GRAPH BASED ANOMALIES



BASICS OF OPS USE CASES

01

Ext IP Communications

If OT Assets from the shop floor or OT DMZ directly communicate with the Ext IPs or DNS Hosts in Internet, then this poses a cyber risk

02

Assets End of Life

End of Life for any asset is when the OEM of the respective asset stops doing any further development on model/make/version of the asset that poses cyber risk

03

Weak/Default Passwords

OT and IT-OT Assets may be configured with the vendor's default or weak passwords that may be guessed easily by the Brute Force tools. Using strong passwords is desired

04

Controllers Data-Acquisition

The data-acquisition write privileges from operators on Controllers (PLC, RTU, DCS, SCS) shall generate alert as this may be an attack

05

Vulnerable Protocols

It is important to note that protocols like SMBv1, Telnet, SNMPv1 have inert vulnerabilities that may be exploited easily. It is imp to limit the usage of these

06

USB Connectivity

As the USB drives may introduce the Malware in the network or the USB Dongle may connect asset to Internet so any usage shall be notified

07

High Risk Incidents

IEC 62443 cybersecurity framework for the OT and IT-Assets defines the network in Purdue model and any asset shall communicate with alternate layer assets

08

Remote Admin

Remote Administration using the protocols like SSH, VNC, RDP may be exploited by the Hackers. RDP is one of the most common vector of the OT/ICS attacks in recent times

09

SNMP Activity

SNMP is a common application to track the current state of the assets. SNMPv1 queries responses may expose network info

10

Multihomed Assets

A Multi-homed Assets has more than one Network Ports and hence it may interconnect plant and control networks hence, it is imp to have visibility on this

OPS PLAYBOOKS

BREACH SIMULATIONS

Validating the technical, process and legal response and recovery frameworks based on the current setup and SOPs

PURPLE TEAM SIMULATIONS

This is Penetration Testing across sample site or subsystem IT-OT intersection including BMS/Safety/MQTT along with Purple Team (Adversarial) Simulations

Risk Assessment Reports and Security Blueprint

STUDY THE GOVERNANCE MODEL

Understand the current Compliance and Policy frameworks. Also, need to understand the Nodal Bodies to whom current Biz needs to report a Breach

MANUAL ASSESSMENT

Visit the site or Discuss with the diagrams to understand the high level protocols and ISA 95 layout in ISA99 expectations (functional knowledge is key)

TOOLS BASED ASSESSMENT

IT Audits, Assessments & OT Assets Identification, Protocols Assessment, ISA-95 Map of Devices, Communications Map, Missing Patches (sample sites)

XENOTIME SIMULATION

	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0008	TA0009	TA0011
	Initial Access	Execution	Persistence	Priviledge Escalation	Defense Evasion	Credential Access	Lateral Movement	Collection	Command and Control
	T1133	T1059.001	T1133	T1546.012	T1070.004	T1003.001	T1021.001	T1074.001	T1571
Red	External Remote Services	Powershell	External Remote Services	Image File Execution Options Injection	File Deletion	LSASS Memory	Remote Desktop Protocol	Local Data Staging	Non-Standard Port
Blue	1) Multi-factor Authentication 2) Traffic Inspection 3) Use VPN with Traffic Inspection 4) Dedicated Landing Zone	1) Anti-Virus 2) Restricted User Access for using Powershell 3) Powershell Logging	1) Multi-factor Authentication 2) Use VPN with Traffic Inspection 3) Jump Server - Reverse Connection Monitor	1) Process Control in EndPoint 2) End Point Application Whitelisting	1) Enable Auditing of Files and Folders (from AD) and monitor events 2) Logging of every action in the system (Forensics)	1) Process Control in EndPoint 2) End Point Application Whitelisting 3) AV	1) Two-factor Authentication 2) Password Policy 3) Block RDP Traffic to Systems using Firewall	1) Process Control in EndPoint 2) End Point Application Whitelisting 3) Restrict the File extensions that can be used 4) Restrict File Transfer to Internet using Firewall	1) IPS Traffic Monitoring 2) Allow specific ports for outbound traffic across FW
	T1078	T1053.005	T1078	T1053.005	T1070.006		T1021.004		
Red	Valid Accounts	Scheduled Task	Valid Accounts	Scheduled Task	Timestamp		SSH		
Blue	1) Multi-factor Authentication 2) Password Policy 3) Check for Multi-system Login from a Single User	1) Restricted User Access 2) OS Policy to restrict Scheduled Task to run as User and not System 3) Windows Event Monitoring	1) Multi-factor Authentication 2) Password Policy 3) Check for Multi-system Login from a Single User	1) Restricted User Access 2) OS Policy to restrict Scheduled Task to run as User and not System 3) Windows Event Monitoring	1) Enable Auditing of Files and Folders (from AD) and monitor events 2) Logging of every action in the system (Forensics)		1) Two-factor Authentication 2) Password Policy 3) Block SSH Traffic to Systems using Firewall		
			T1546.012	**T1078**	**T1036.005**				
Red			**Image File Execution Optic**	**Valid Accounts**	**Matach Legitiate Name or Location**				
Blue			1) Process Control in EndPoint 2) End Point Application Whitelisting	1) Multi-factor Authentication 2) Password Policy 3) Check for Multi-system Login from a Single User	1) Enable Auditing of Files and Folders (from AD) and monitor events 2) Logging of every action in the system (Forensics)				
			T1053.005		**T1027.005**				
Red			**Scheduled Task**		**Indicator Removal from Tools**				
Blue			1) Restricted User Access 2) OS Policy to restrict Scheduled Task to run as User and not System 3) Windows Event Monitoring		1) Enable Auditing of Files and Folders (from AD) and monitor events 2) Logging of every action in the system (Forensics) 3) AV and IPS				
			T1505.003						
Red			**Web Shell**						
			1) Process Control in EndPoint						

THANK YOU