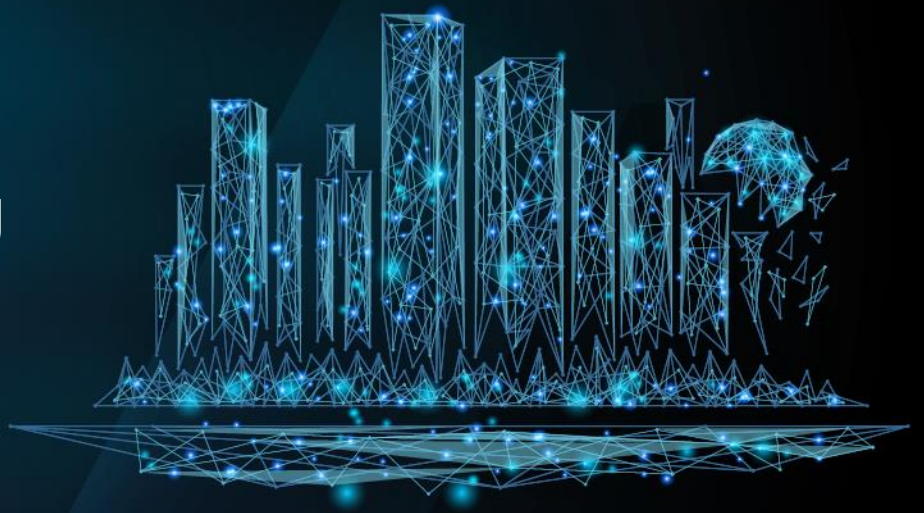
THALES
Building a future we can all trust

# Best Practices for securing IT/OT Convergence



Soultana ELLINIDOU, Cyber Security Manager
Grégoire GRISON, Senior Cyber Security Engineer

INDUSTRIAL CYBERSEC FORUM

*February 2023*

OPEN

# Planning

- Introduction
- Reality of NIS2
- Challenges & Approaches
- Case study - Best Practices  (Integrated IT/OT services & systems)

# Introduction

85%

…of organizations in the chemical and production process sectors **deploy IoT solutions**.

83%

…of tech decision makers in manufacturing companies feel there is still **insufficient knowledge** about the connection **between IT, OT** and its **security**.

Source: Thales IT/OT Cybersecurity Whitepaper

OPEN

# Introduction


« The convergence and integration between IT and OT is by no means a new phenomenon. […]
The trend is fully fledged, but **the ramifications are still emerging** in domains such as **cybersecurity** risk management.
Although the benefits of such integration are appealing, there are risks that need to be managed if business are to **protect their assets from cyberattacks**. »

# History of Cyber Threats affecting industrial sectors

**1950s – 1960s**
First computers set up by governments, military and some large organizations

**1980s**
Computers arrive in schools, companies, factories and to the private individuals

**1999**
The whole world connects to Internet

**2010s**
Development of cloud computing usages

**2020s**
Internet of Things (IoT), Autonomous and Intelligent Systems, Artificial Intelligence, Big Data

**Digital processing of information** | **Digital connectivity** | **Digital automation**

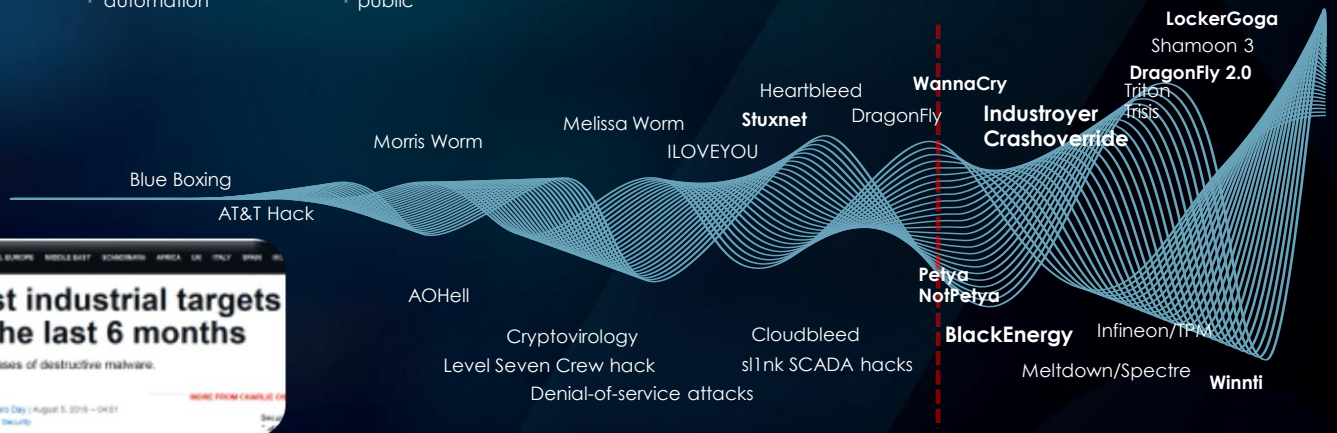
**1970s**
Launch of the first personal computer

**1990s**
Numerical improvements of the electrification and the automation

**1991**
Internet (World Wide Web) available for the public

**2000s**
Development of mobile usages

**2020s**
Industry 4.0

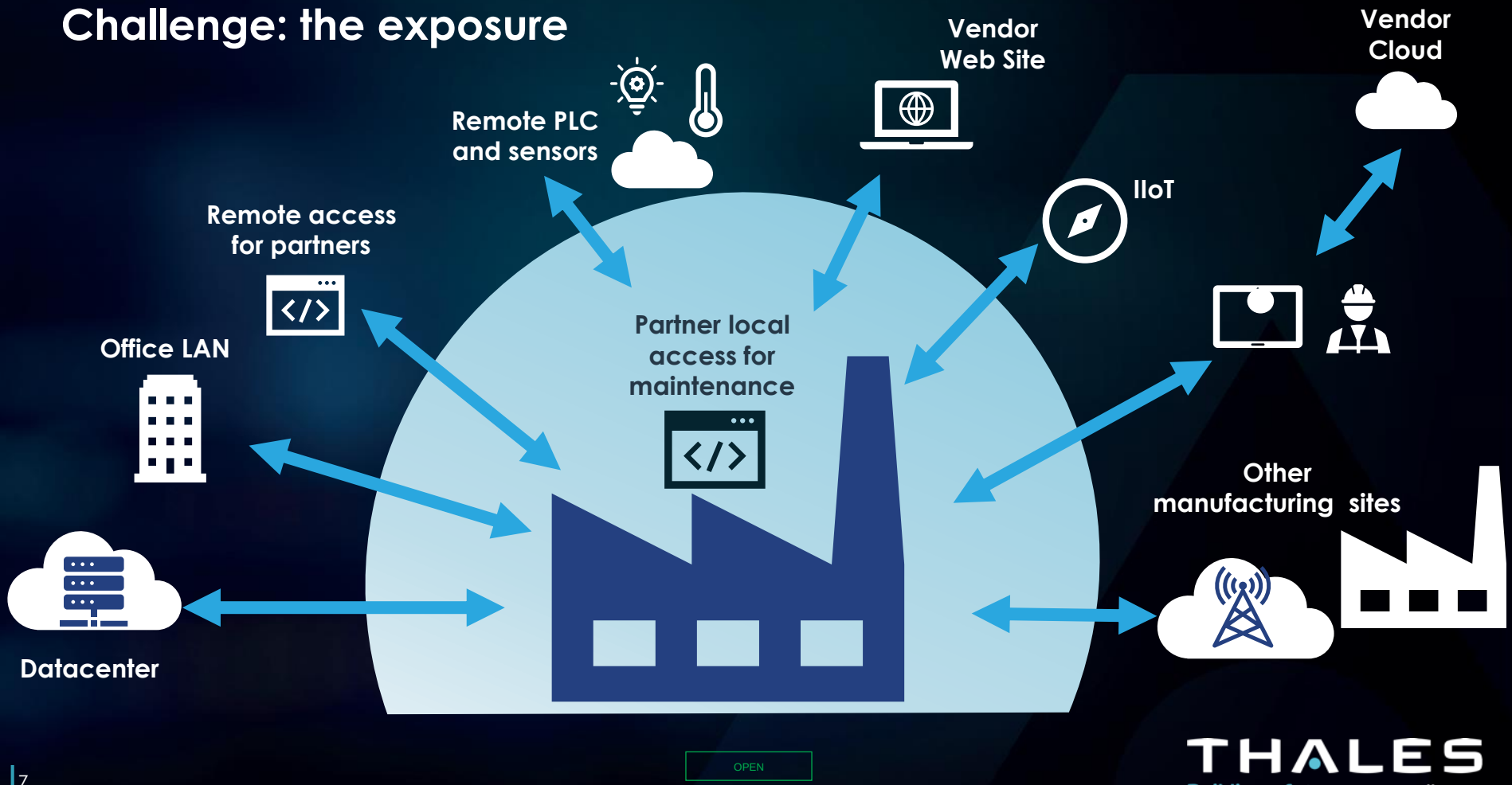

**Motivations : Sabotage/Terrorism, Profit, Vengeance, Cyber Warfare - APT**

# Legislation

**NIS2:** Directive adopted on 28th November. National law translation by September 2024.

> **Much more** entities concerned.
> Stricter incident-reporting deadline.
> Application of cyber risk-management measures.
> High fines for non-compliance.
> On-site inspections, audits.
> C-level staff with new cyber responsibilities.
> C-level executives temporary suspensions or prohibitions.

# Challenge: the exposure




OPEN



THALES
Building a future we can all trust

# SECURE INDUSTRIAL ENVIRONMENT
## CHALLENGES OT SECURITY TEAMS ARE FACING

**Low visibility** on infrastructure
No comprehensive documentation

Low cybersecurity **Awareness**

Priority on **Process** and **Safety**

No **pre-production** site

Long equipment **life cycle**

**Silo** of IT an OT **Organizations**

**Accreditation** requirement

**Security** (was) not a **Requirement**

**Limited partnership with IS teams** in manuf. environment

**ALL THESE CHALLENGES MAKE HARDENING DIFFICULT IN A SHORT TIMEFRAME** (EVEN MIDDLE OR LONG TIMEFRAME)
**AT LEAST WE NEED TO KNOW WHAT IS GOING ON!**

# OK … I CANNOT HARDEN EVERYTHING, LET'S GET AT LEAST VISIBILITY !

## Visibility on Infrastructure

- Cartography and Inventory
- Communication Flows
- Vulnerabilities detection

## Detection & Alerting

- Unexpected behaviors
- Unexpected Communication Flows
- Malicious files

# BUT NOW … HOW CAN I DO THAT?

Approach #1

**Apply to OT Manufacturing the principles applied in IT environment. Collect the logs from assets which compose the manufacturing environment.**

Main challenges with this approach :

- ✓ Not always possible to modify asset configuration
- ✓ Logs do not exist or poor quality
- ✓ Does not answer cartography challenges
- ✓ Risk of project tunnel effect -> Monitoring will not start before a while!

**This strategy can be applied to IT parts of OT environment and security devices (Eg: Windows Server and Firewall).**

# BUT NOW … HOW CAN I DO THAT?

**Approach #2**

## Non invasive approach by listening the network.

Most relevant approach as per specific OT challenges :

- ✓ Just **listening** the network: no need to modify any asset
- ✓ Leverage **non encrypted** flows opportunities
- ✓ **Fast** deployment
- ✓ **Foster adhesion** of operational team providing them immediate value: probe raising information related to process

**First results can be obtained in a short timeframe, within couple of days.**

# OT Cybersecurity Maturity Journey

- **INCREASE your security maturity to empower you** to withstand cyber attacks and **ensure business continuity** *(Ability to **RECOVER** from incidents)*

- **PROVIDE Visibility** over your **entire** OT estate, **Enhancing accuracy of your risk-posture** regarding cyber incidents *(Ability to **IDENTIFY** your posture)*


Recover

Identify

Detect

Respond

Protect

- **Proactive monitoring** and **incident response to cyber threats** in your OT estate *(Ability to **DETECT and RESPOND**)*

- **IMPLEMENT cost effective mitigations** preventing cyber-incidents from impacting the **availability** or **safety** of your critical systems *(Ability to **PROTECT** your systems)*


OPEN

# Case Study

**Goal: to develop OT Protective Monitoring solutions for plants operating in highly safety critical environments for one of our client in Energy sector.**

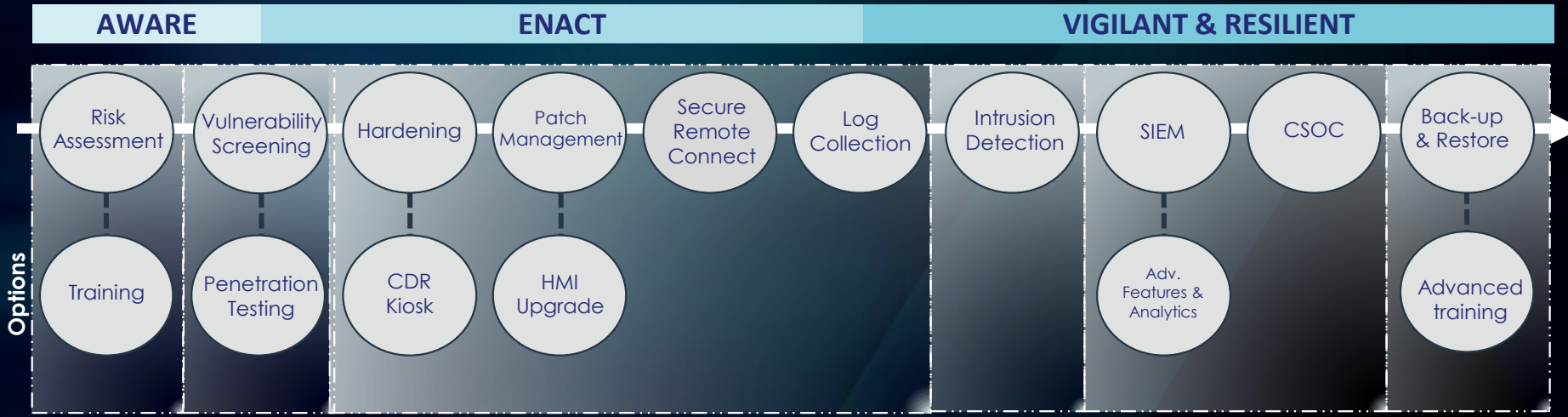

**ENSURING COMPLIANCE**
Establishment of a Governance regime which included the creation of an ISO27000-compliant ISMS, following the industrial control security standards of IEC62443 and the compliance with the provision of NIS2 directive.

**ASSESSING RISK**
Risk Assessments conducted against the IT/OT architecture and systems using the ISF IRAM methodology in order to identify the potential risks and threats and develop a plan in order to mitigate them.

**ASSURING PROTECTION**
Development of state of the art, OT-focussed monitoring solutions which can be integrated into existing Security Incident and Event Monitoring solutions, providing real-time visibility of extremely complex manufacturing environments.

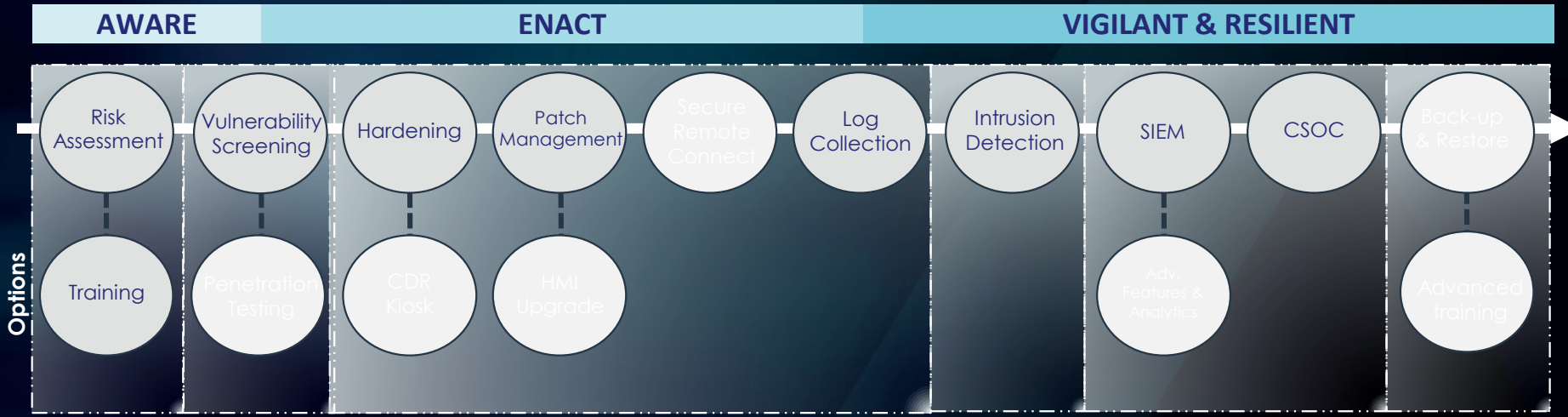
OPEN


# Seamless, contextualized security from the domain experts…




## …that can be integrated in any cyber (IT&OT) defense plan


# Seamless, contextualized security from the domain experts…




## …that can be integrated in any cyber (IT&OT) defense plan

# Training

**Cybersecurity Training Sessions**

**Cybersecurity Demonstration with Physical equpment**

**Cybersecurity Exercices:**
-ICS Attack/Defense Scenarios
-Red/Blue Team
-Purple Team


OPEN



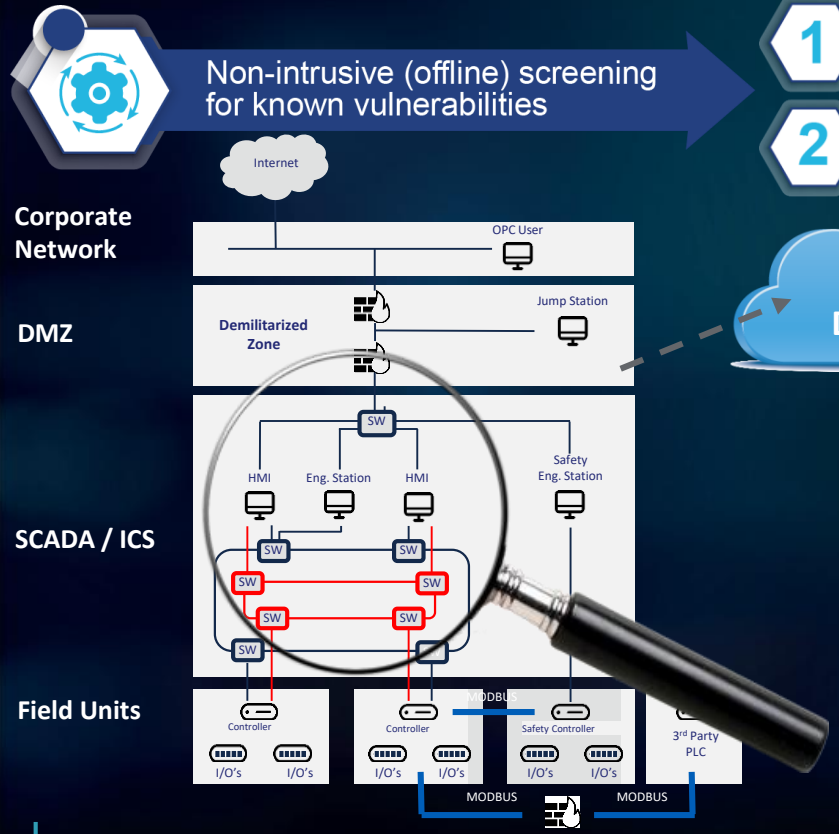
**Cybels Range**
**Powered by DIATEAM**

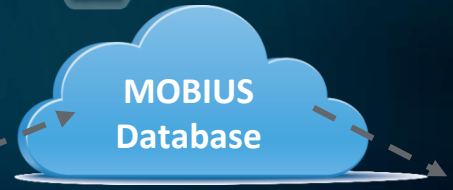
THALES
Building a future we can all trust

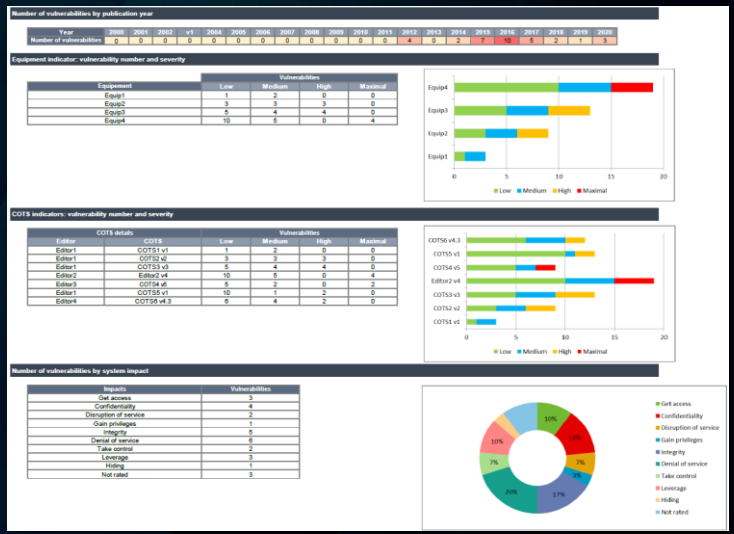
# Vulnerability Screening

Non-intrusive (offline) screening for known vulnerabilities

1. Offline Screening of pre-mapped network
2. Compare with Thales Database
3. Report with vulnerabilities and criticality based on Network components & use of equipment



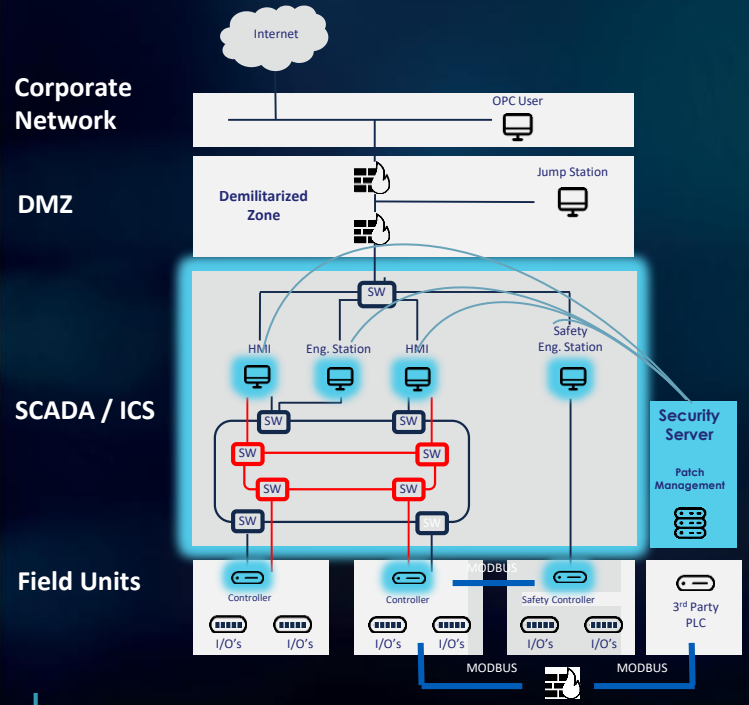

OPEN



THALES
Building a future we can all trust

# Hardening & Patch Management

Close known hardware & network vulnerabilities




## Hardening

- Physical/logical port blocking and SW updates of controllers
- Configure operator / engineering stations, controllers , servers and Network devices
- Configure Network settings (e.g. MAC address filtering)
- Add Firewalls, e.g. in MODBUS connection or 3rd party equipment

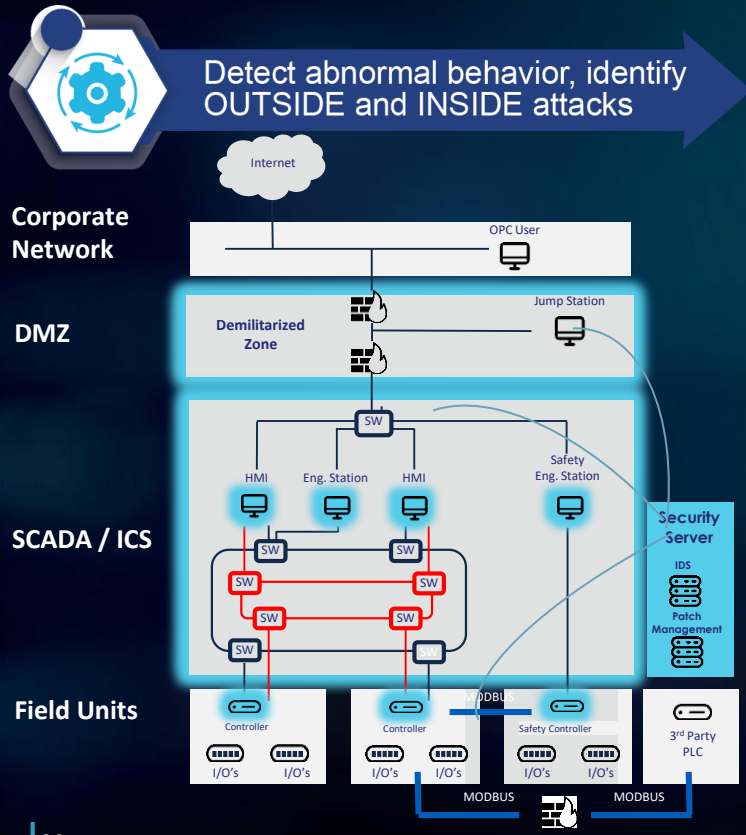
## Patch Management

- Never miss a security related Windows patch / update
- validated / tested patches: No risks of unintended consequences as a result of a software modification
- Patch Management station with automated deployment and reporting for know regulations(e.g. NERC-CIP)

OPEN

# Intrusion Detections System

Detect abnormal behavior, identify OUTSIDE and INSIDE attacks




## Intrusion Detection System (IDS)*

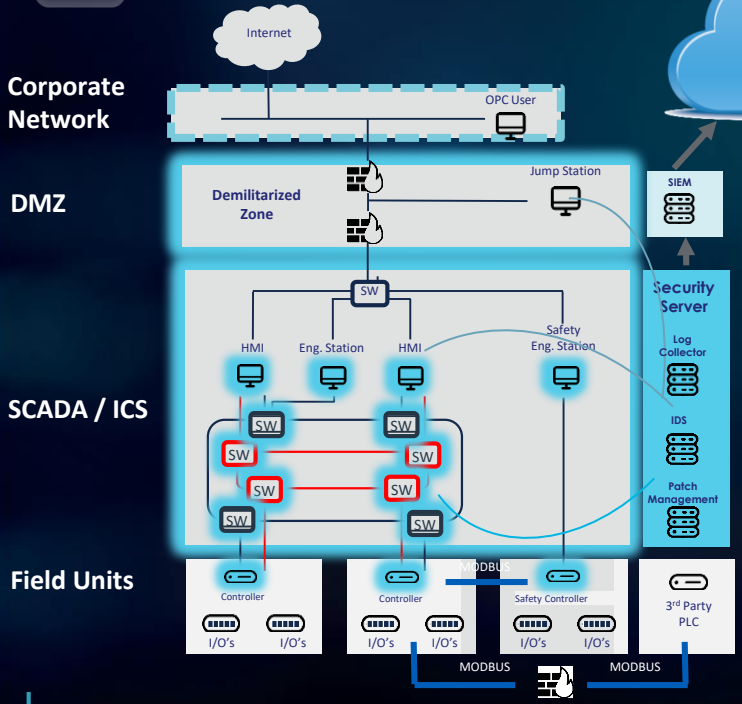
- Real time Networks Scans of: SCADA + DMZ + MODBUS Networks
- Optimized with Deep Package Inspection on propitiatory protocols
- Uses signature scans for known attacks
- Behavioral scans for unknown attacks
- Alarms if changes in the system occur

OPEN

* This solution offered with Partners

# Cyber Security Operations Center

Consolidate ALL Cyber Events: Monitor locally (SIEM), Action Remotely (CSOC)




**CSOC**
**in the cloud service**
Up to 24/7
Monitoring & Response

## SIEM (Security Information & Event Management)

- Centrally collect all events from Logs Collector and IDS
- Connects the data and runs analytics (Thales CYBEL Product)
- Easily displays results (Cyber Dashboard)
- Can be monitored locally or via a CSOC

Data Integration, Correlation and Enrichment

External Thread intelligence feeds providing info on Attack Patterns

## CSOC (Cyber Security Operations Center)

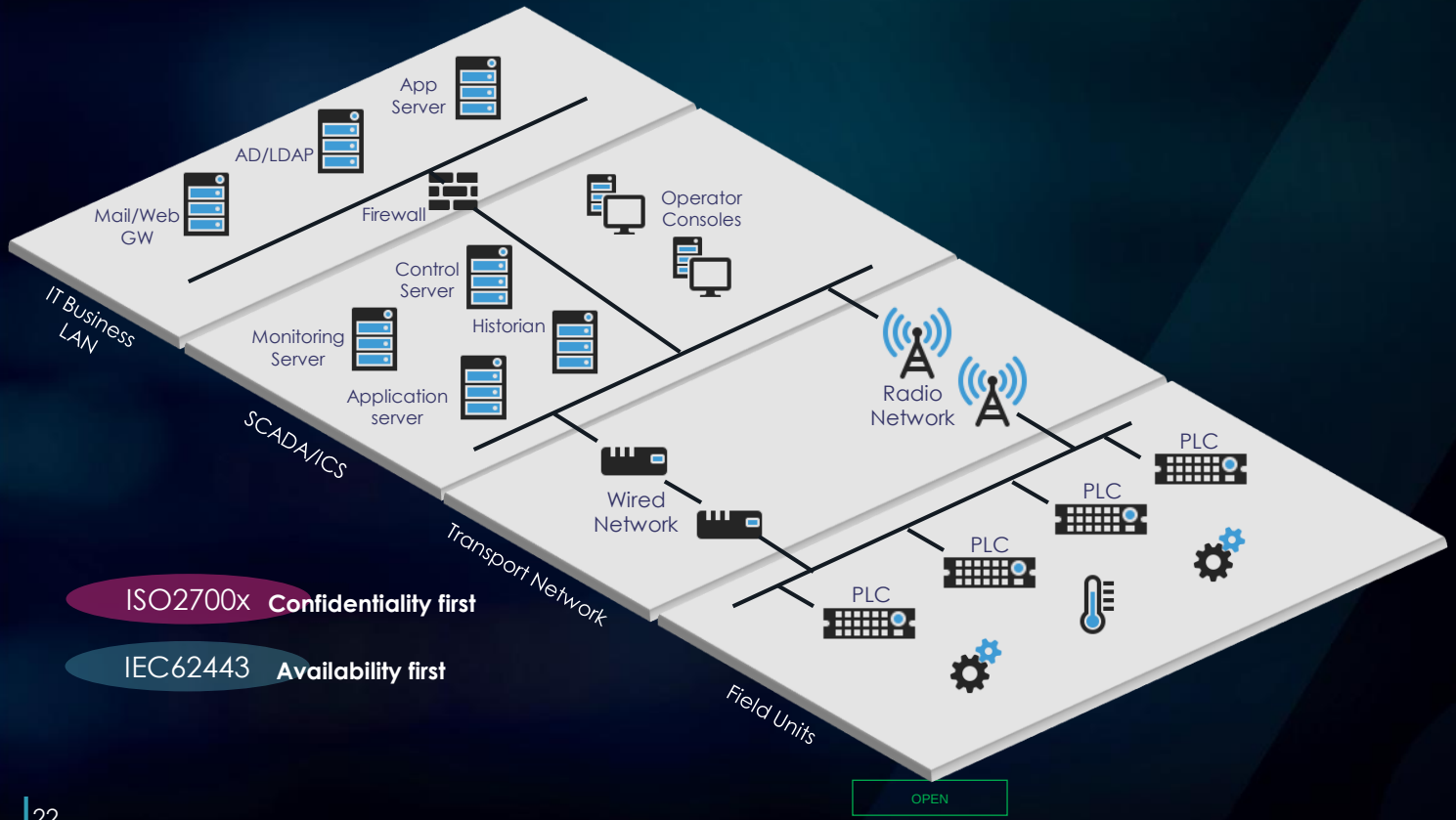
- Customer Internal CSOC
- Remotely Operated CSOC owned by customer operated by Thales
- CSOC as a Service. Cloud solution operated in Thales premise 24/7 or 8/5 operation services
- Capacity to extend the monitoring for fully integrated vision over IT/OT/IIoT Cyber Events

OPEN



THALES
Building a future we can all trust

# Cybersecurity for IT/OT environments




ISO2700x **Confidentiality first**

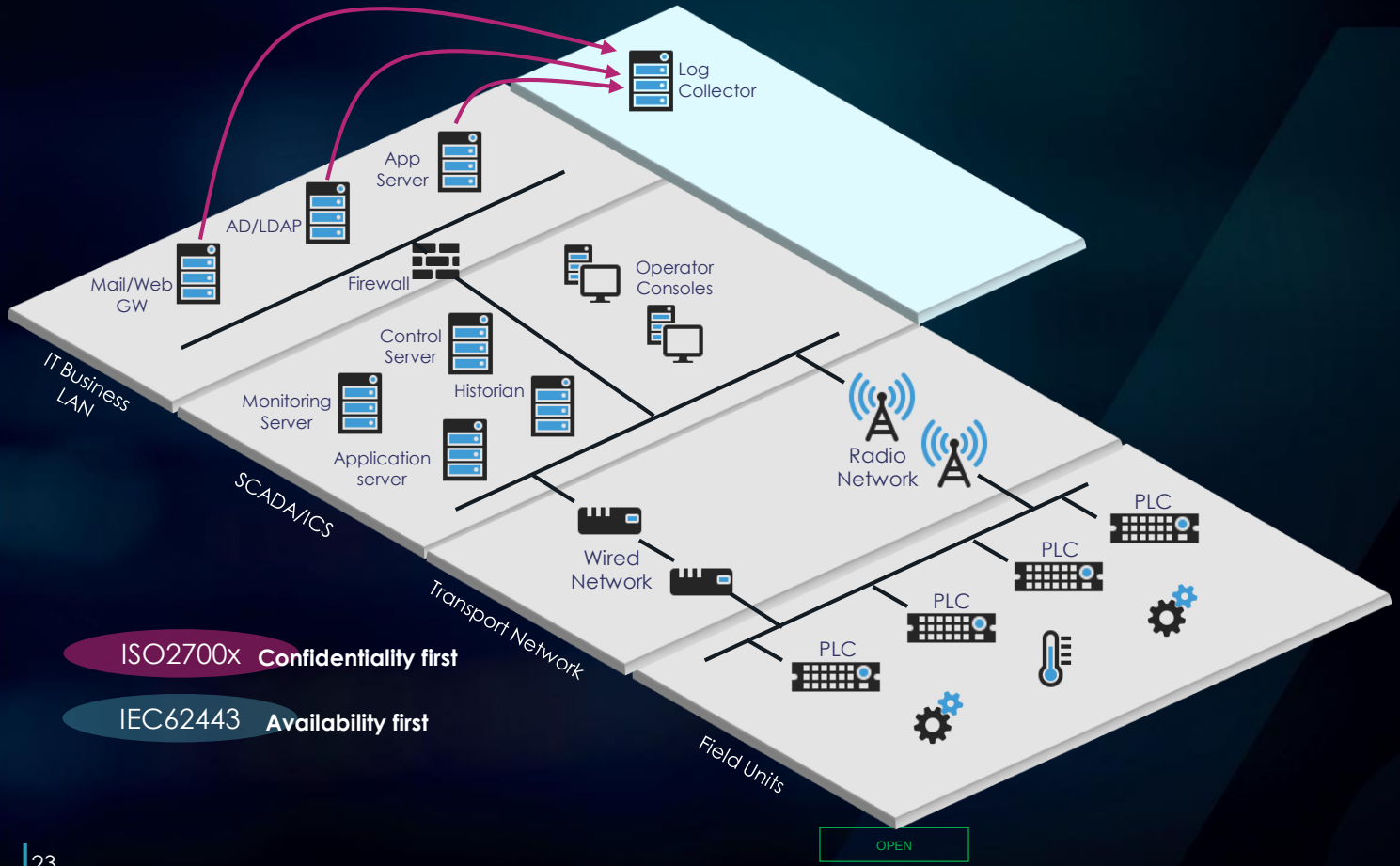
IEC62443 **Availability first**



THALES
Building a future we can all trust

# Cybersecurity for IT/OT environments

**IT services logs**




ISO2700x **Confidentiality first**

IEC62443 **Availability first**



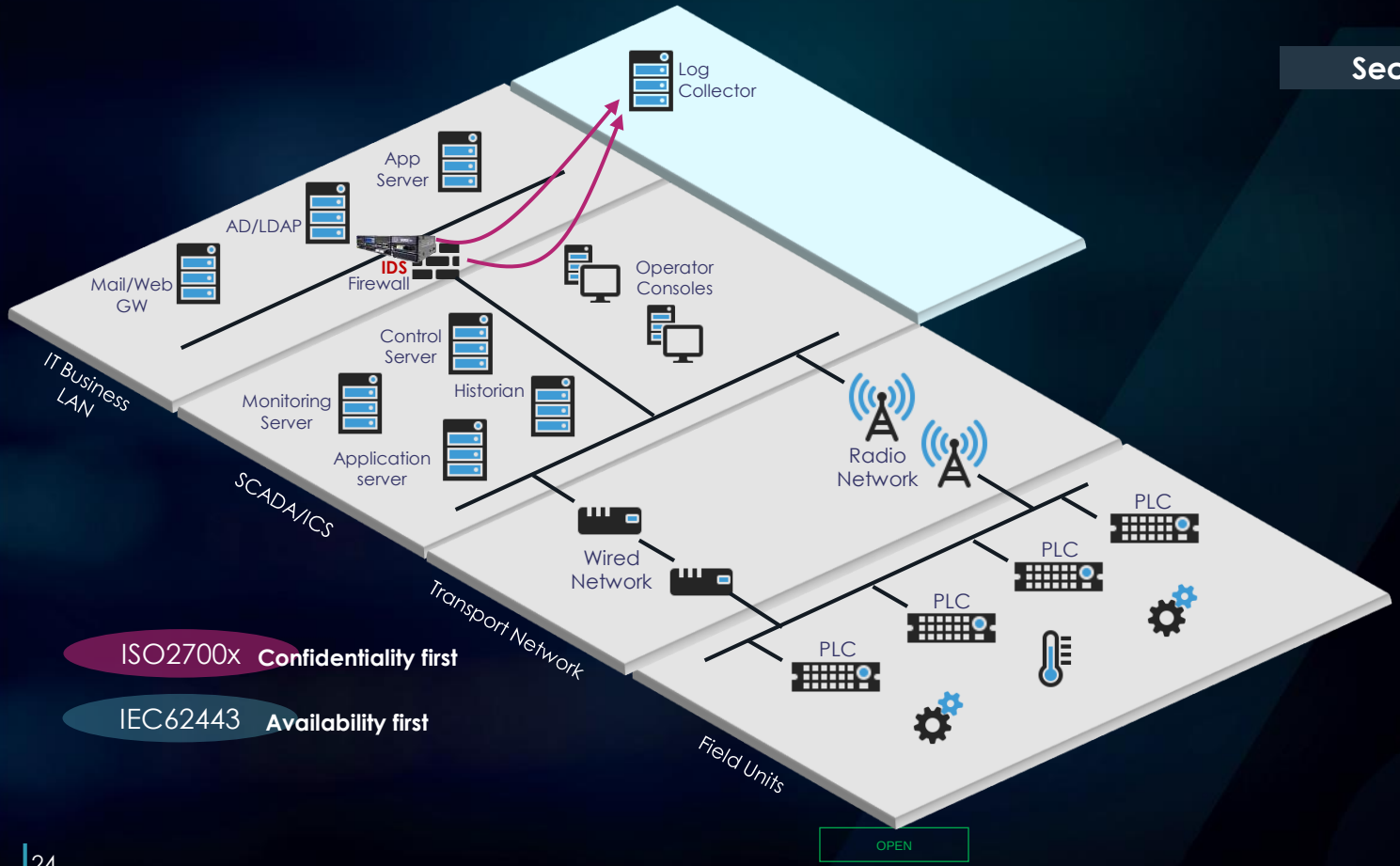
THALES
Building a future we can all trust

# Cybersecurity for IT/OT environments

IT services logs

+

Security devices logs




ISO2700x **Confidentiality first**

IEC62443 **Availability first**



THALES
Building a future we can all trust

# Cybersecurity for OT environments

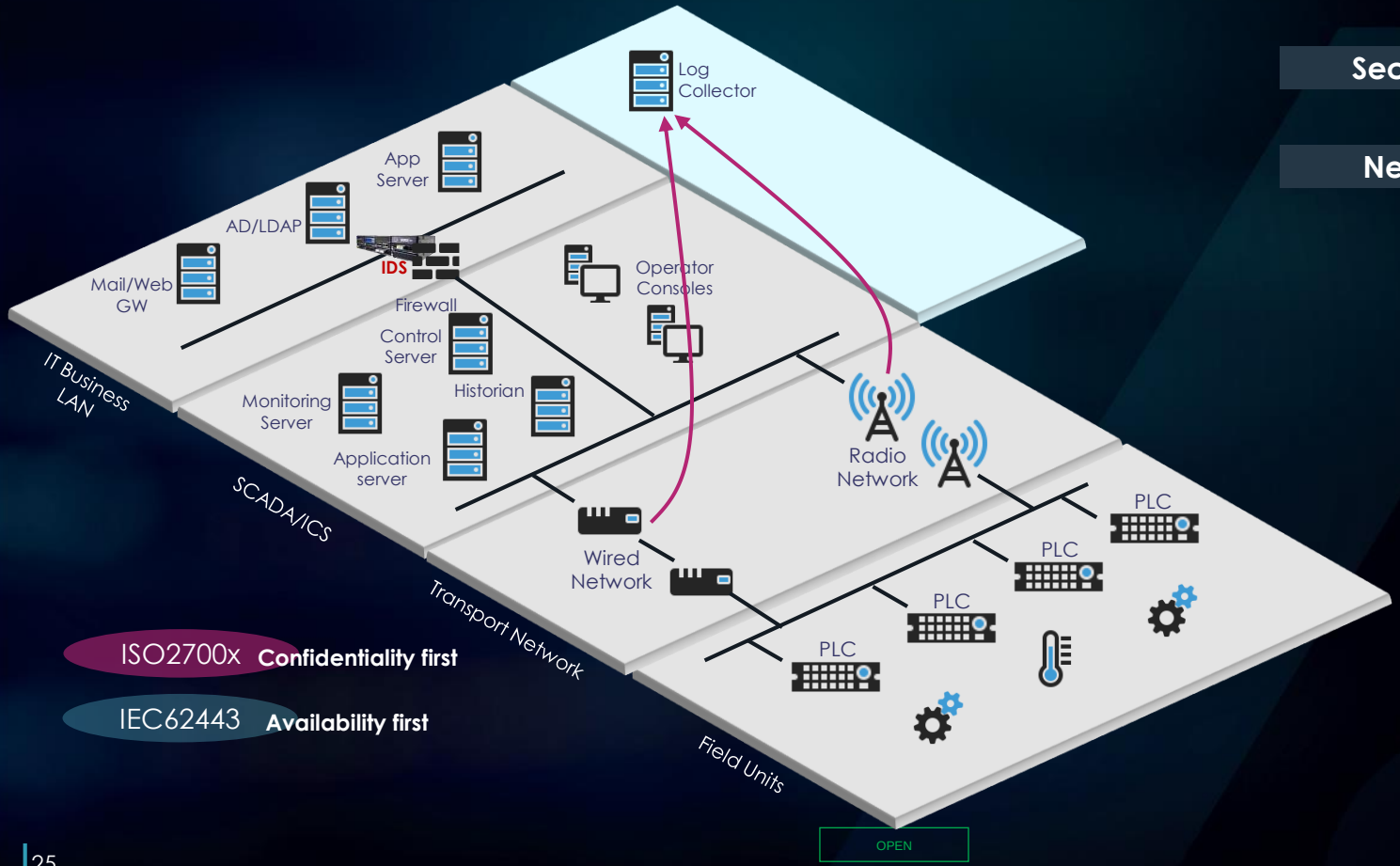
IT services logs

+

Security devices logs

+

Network assets logs



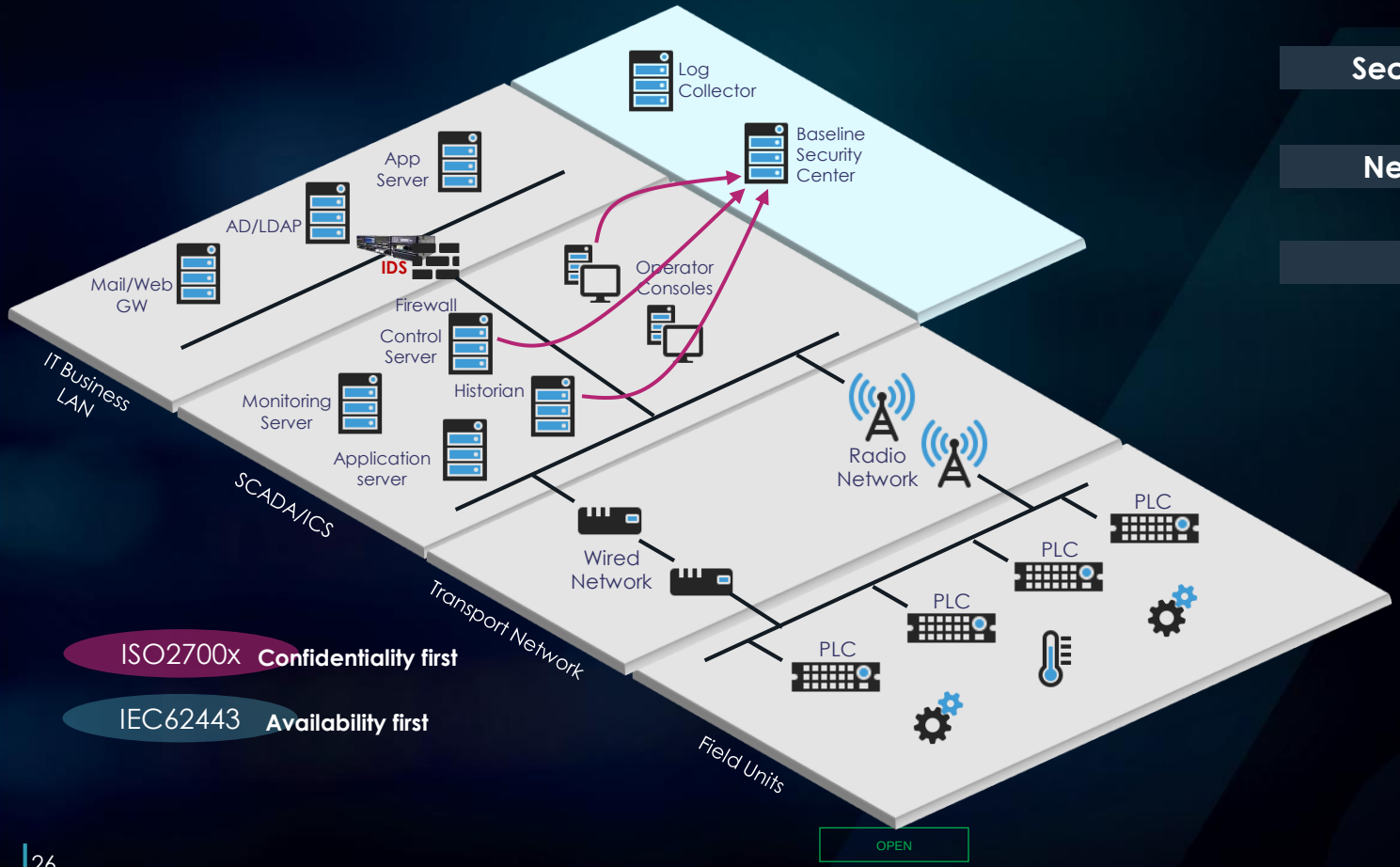

ISO2700x **Confidentiality first**

IEC62443 **Availability first**



THALES
Building a future we can all trust

# Cybersecurity for OT environments




IT services logs

+

Security devices logs

+

Network assets logs

+

OT assets logs

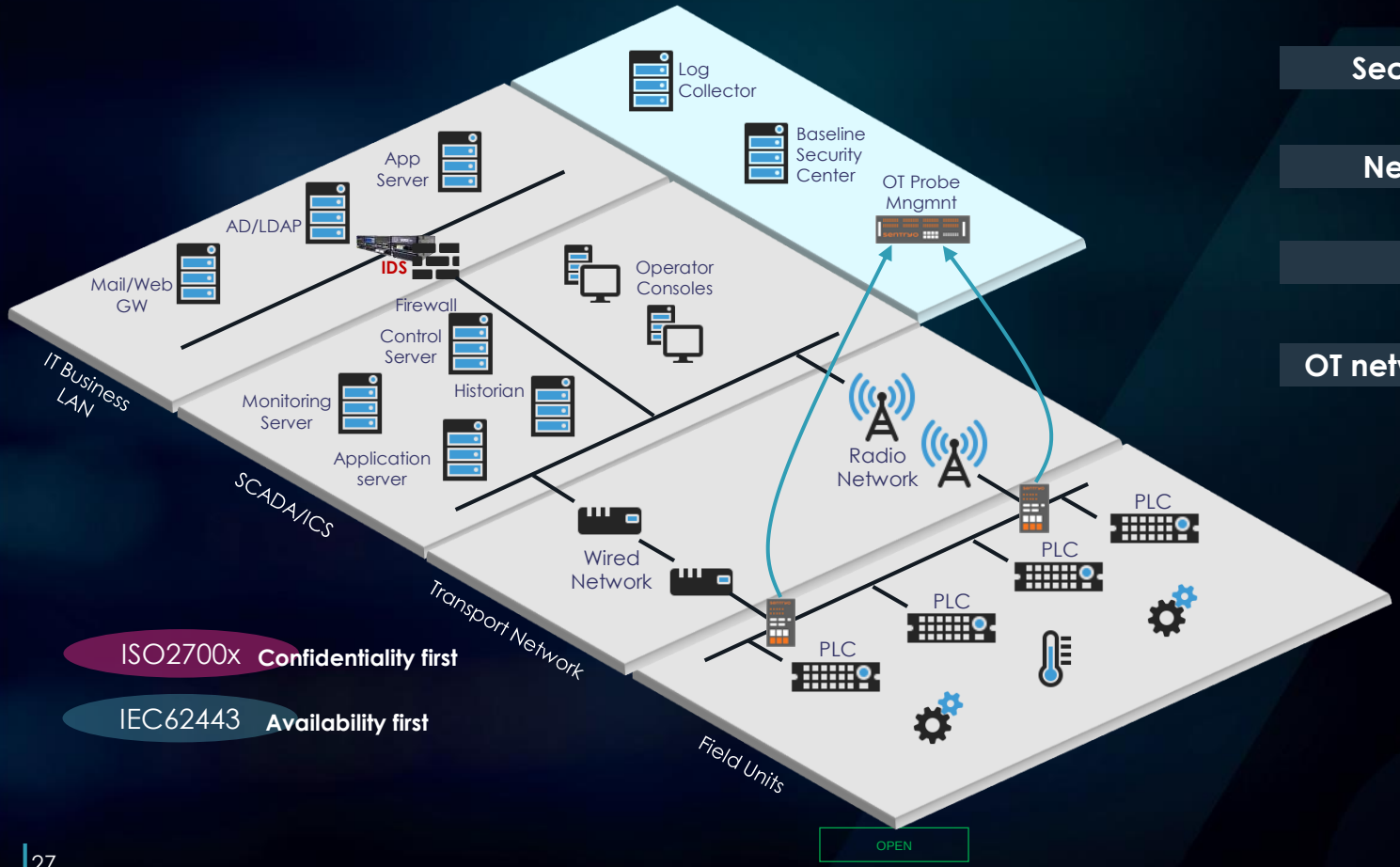
ISO2700x **Confidentiality first**

IEC62443 **Availability first**



THALES
Building a future we can all trust

# Cybersecurity for OT environments




- IT services logs
- Security devices logs
- Network assets logs
- OT assets logs
- OT network supervision logs

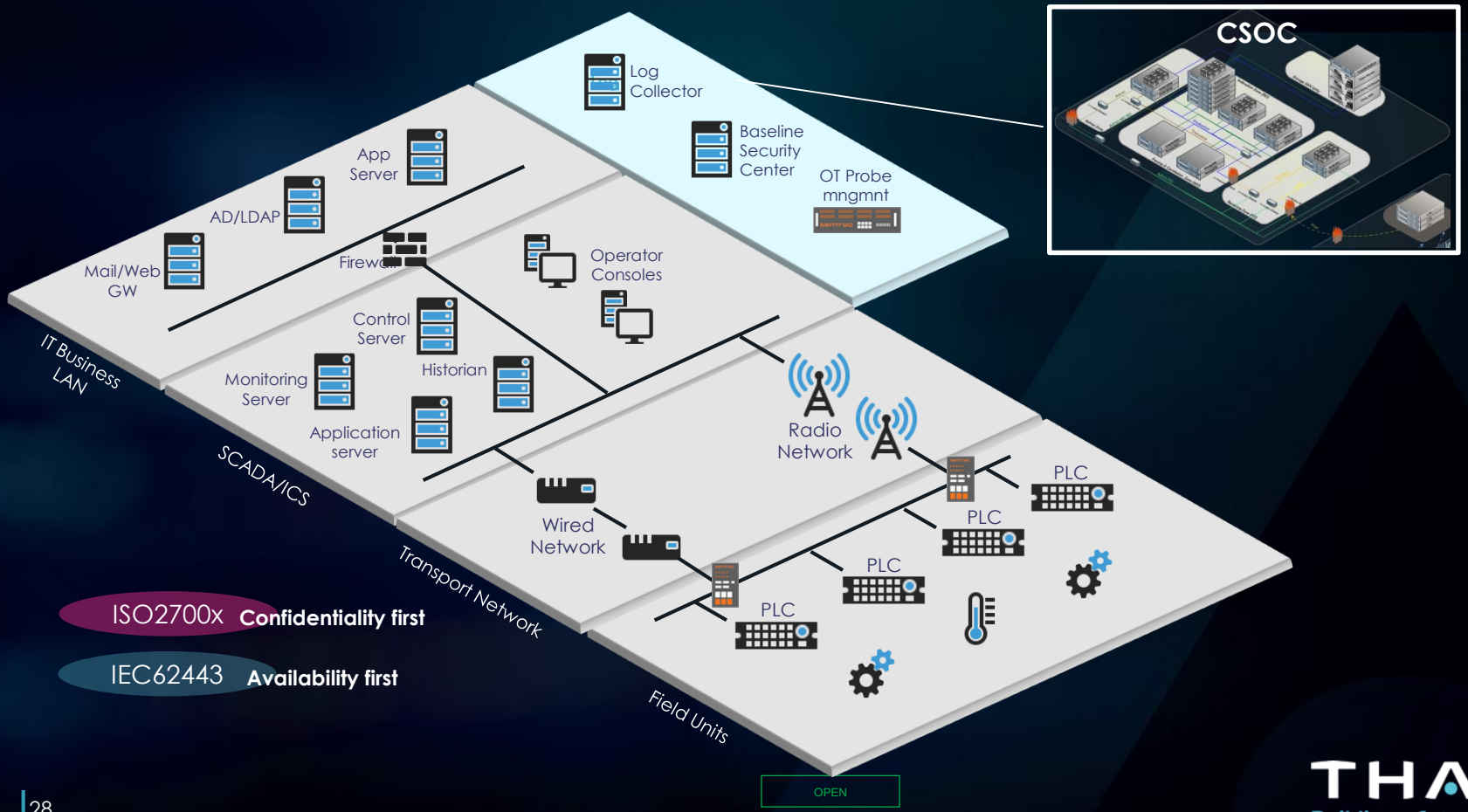
ISO2700x **Confidentiality first**

IEC62443 **Availability first**



THALES
Building a future we can all trust

# Cybersecurity for IT/OT environments



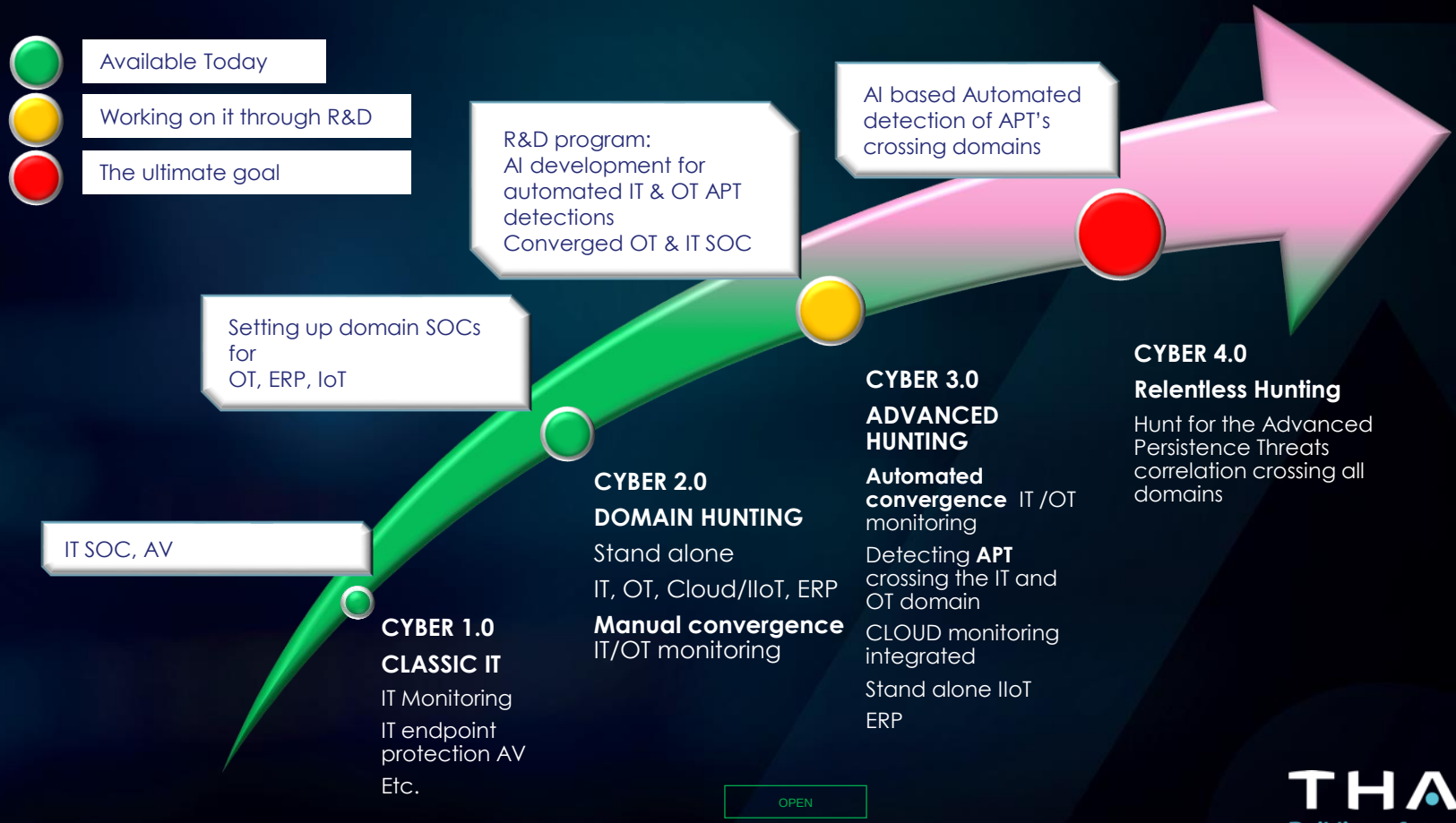

ISO2700x **Confidentiality first**

IEC62443 **Availability first**



THALES
Building a future we can all trust

# Focus on converged IT/OT monitoring roadmap



THALES
Building a future we can all trust

# Thank you!

## Questions ?

OPEN

Cybels