INFRABEL

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

EUROPEAN
UNION
AGENCY
FOR RAILWAYS

A « Railway » CyberSOC

(Episode 2)

5th ENISA-ERA Conference on Cybersecurity
in Railway – Tallinn

Cédric Cecotti

Cédric Cecotti

Chief Cyber-Resilience Architect

from 2025 to 2045

> Security is
> always too much
> until the day
> it is not enough

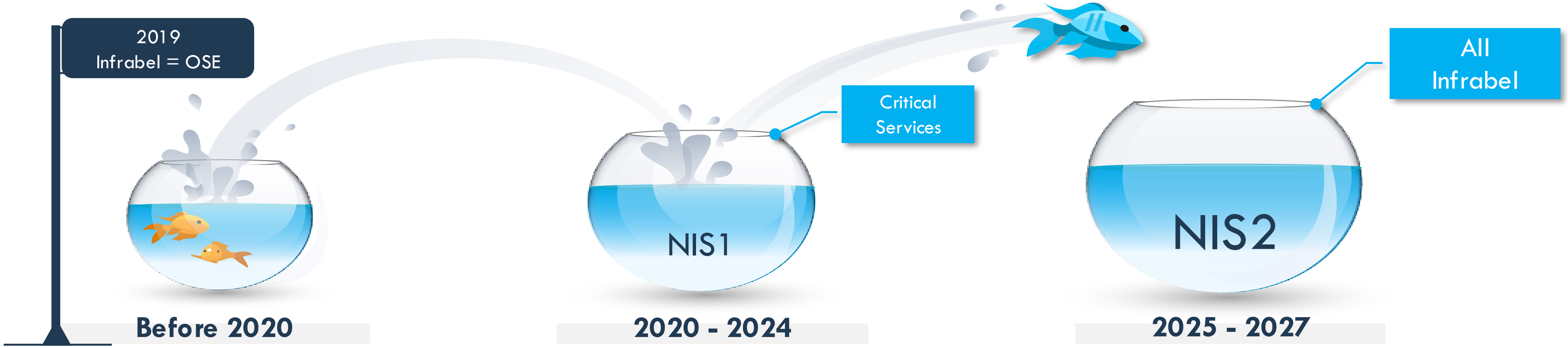
William H. Webster, Former FBI Director

Yes, we crazy enough to build a « Railway » CyberSOC !

Our journey so far…

1 Our context

More requirements to meet our legal obligations



Before 2020

Cyber Security Management with Due Care and Diligence

+

2020 - 2024

Critical Services Protection Measures

Dedicated Cyber-Security team

Risk analyses

Annual internal audits and an external audit in 2022

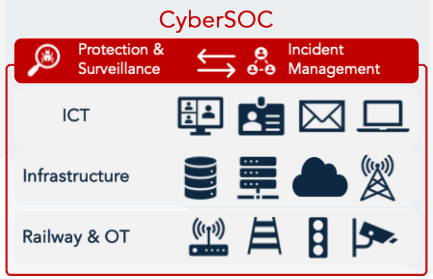
+

2025 - 2027

Focus on NIS2 Certification

A division to manage "Cyber Resilience"

Training program for all employees



Maturity

Since 2020, the level of maturity of cybersecurity management has been progressing year on year, enabling Infrabel to control its risks and meet its legal obligations (NIS).

Our action plan

Five main objectives to meet NIS2 requirements

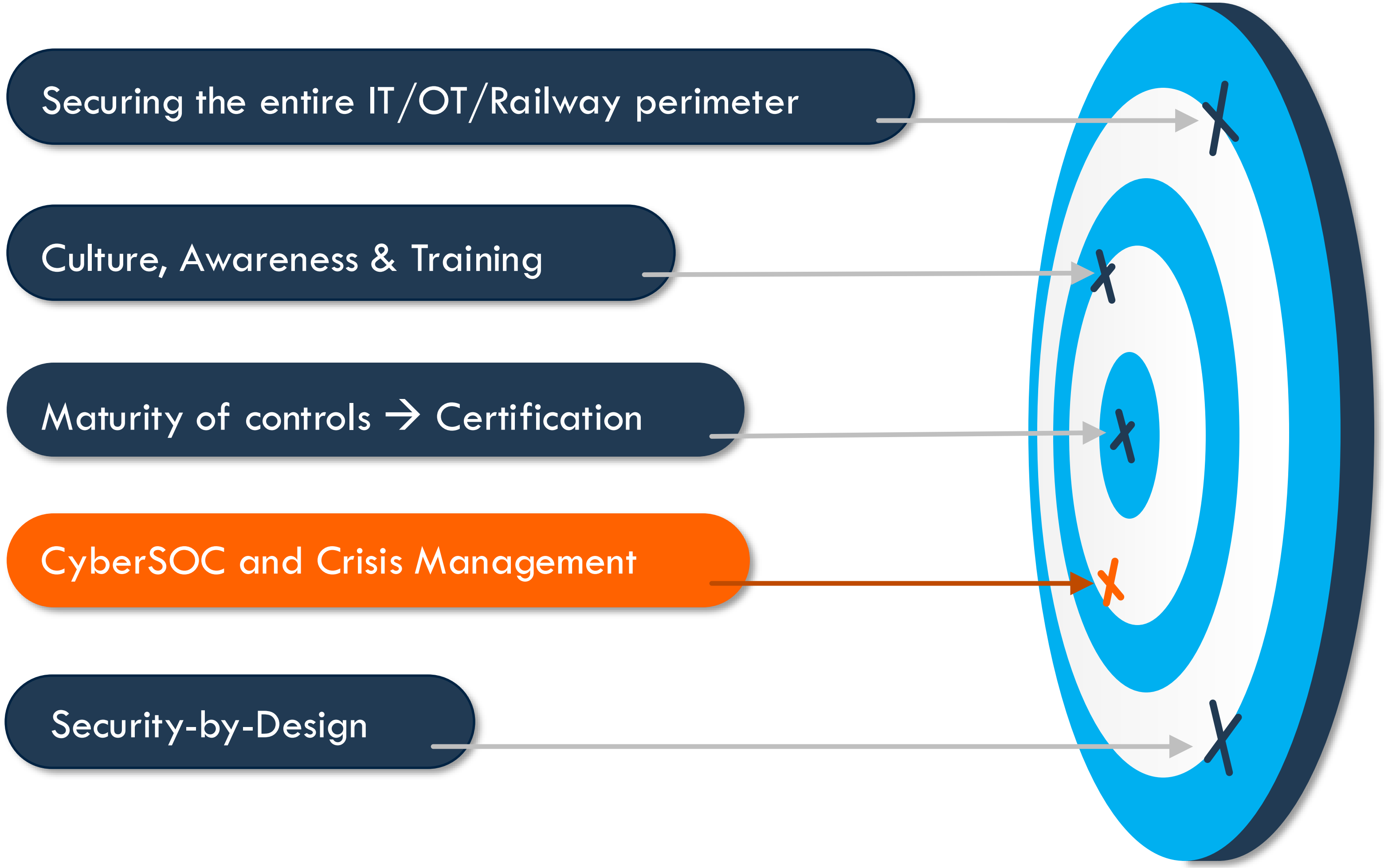
STRATEGIE DE CYBERSECURITE ET PLAN D'ACTION 2024 - 2027

Faire d'Infrabel une entreprise plus sûre et plus résiliente aux risques grâce à une culture forte de la cybersécurité

GOVERN
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
// CONTEXT

Cédric Cecotti
I-CISO

INFRABEL

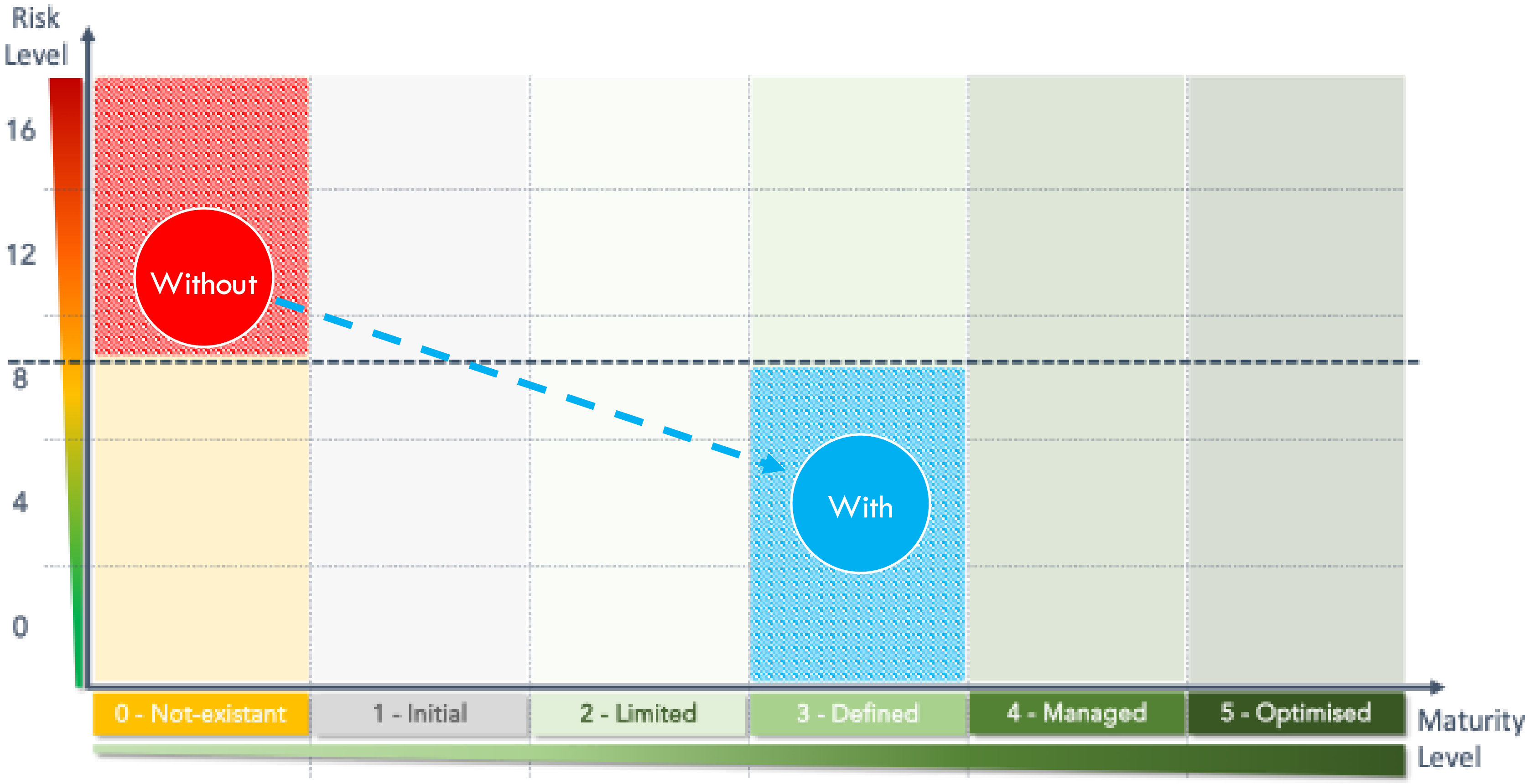


- Securing the entire IT/OT/Railway perimeter
- Culture, Awareness & Training
- Maturity of controls → Certification
- CyberSOC and Crisis Management
- Security-by-Design

3

Risks vs Maturity

Risk and Maturity Assessment to meet NIS2 requirements

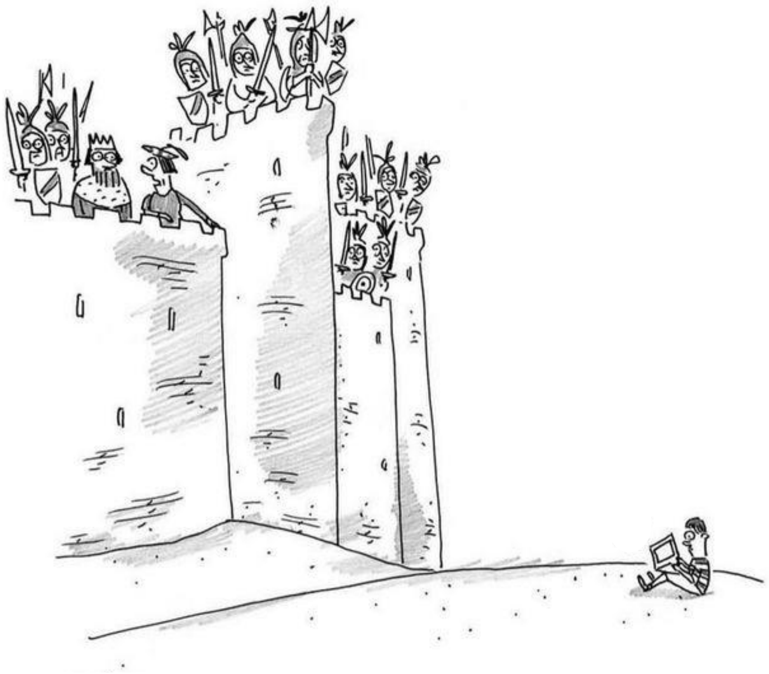


The implementation of our CyberSOC contributes significantly (but not exclusively) to improving Infrabel's maturity and reducing potential incident impact.

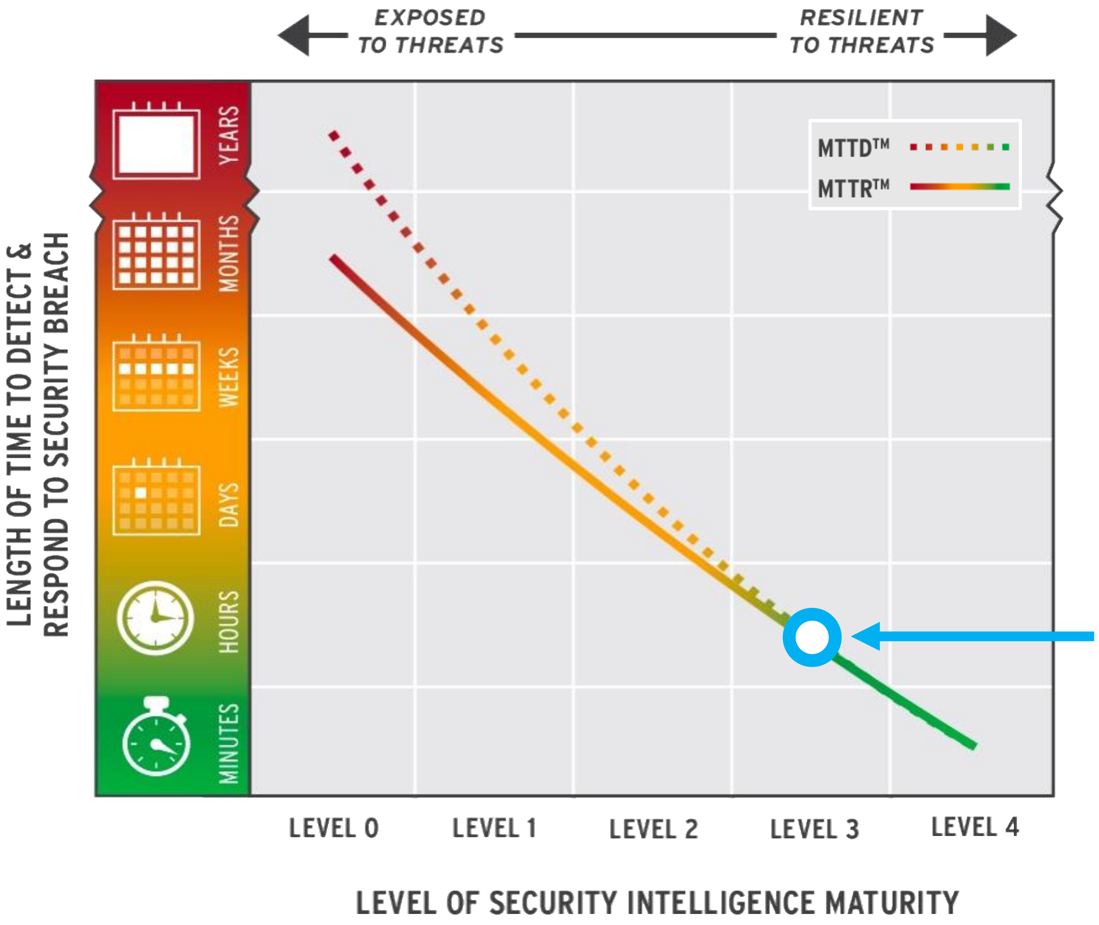
4

Incident Response Target

Detect attack attempts and respond as quickly as possible



« Bad news, Your Majesty – it's a cyberattack! »



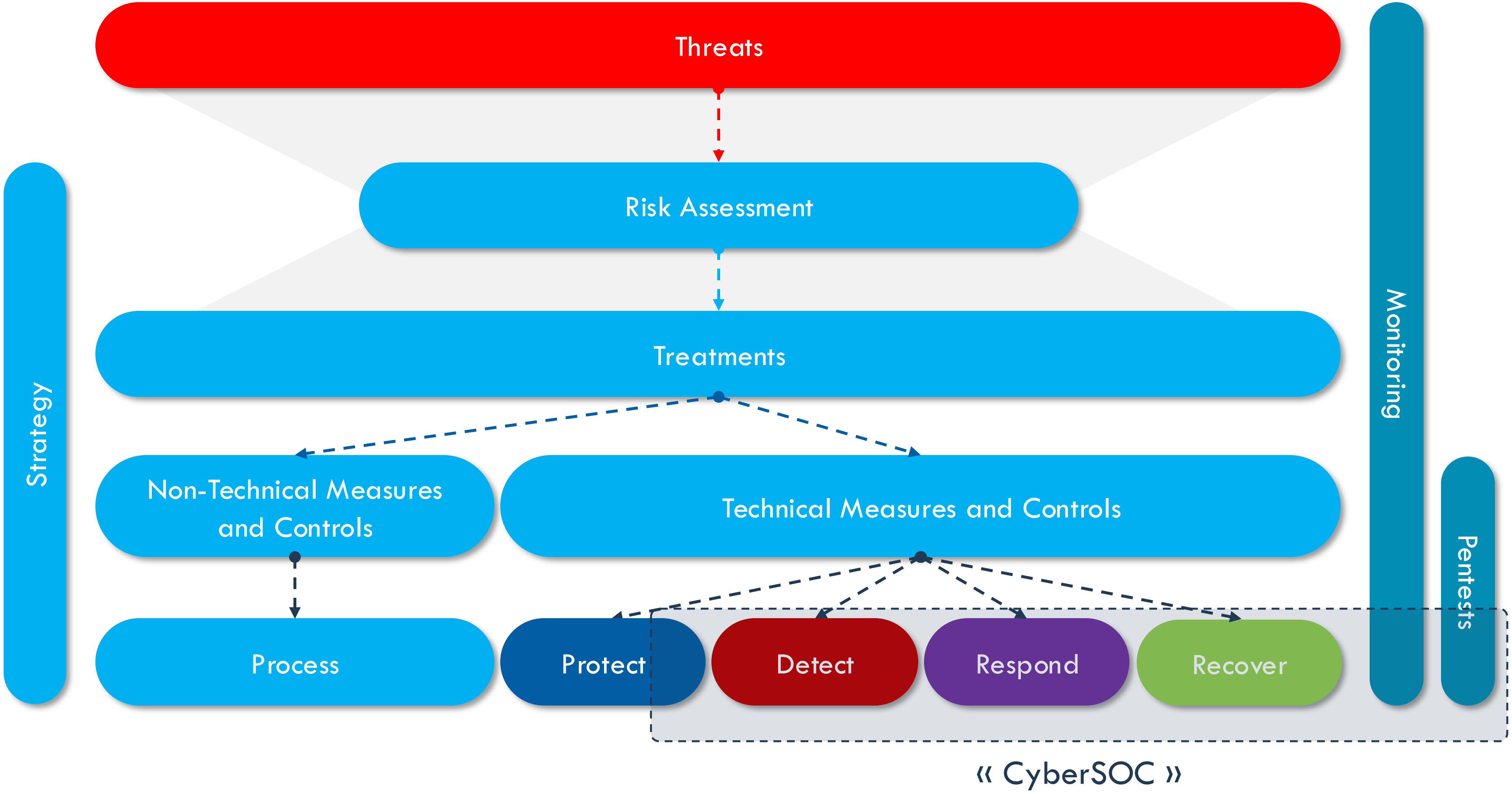
Our target

MEAN TIME TO DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

MEAN TIME TO RESPOND (MTTR)
The average time it takes to respond and ultimately resolve the incident

5 Risk Based Approach

Our CyberSOC strategy is guided by Risk Management



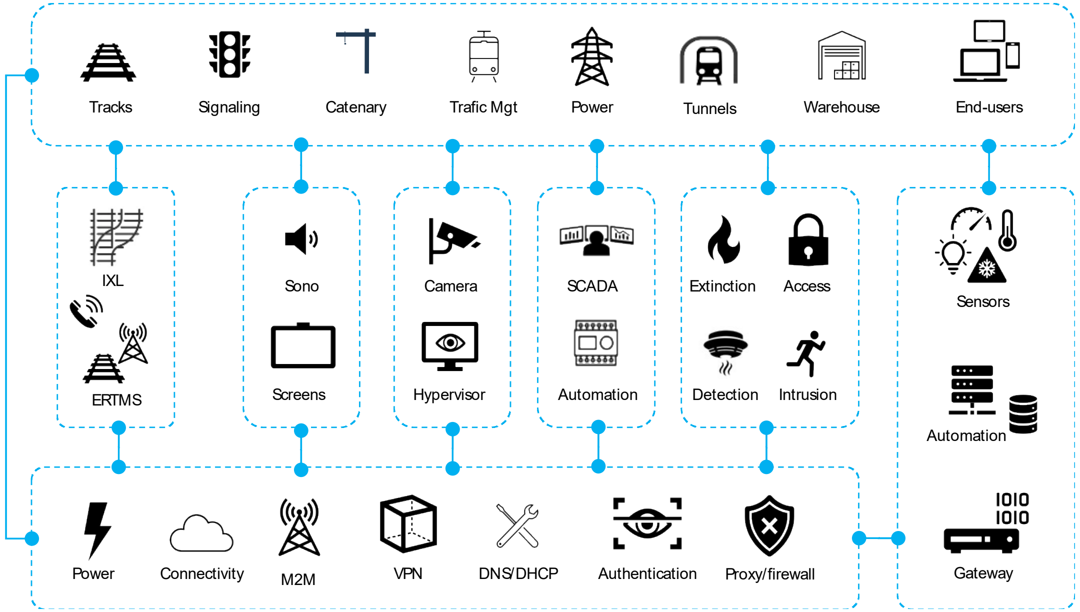
6

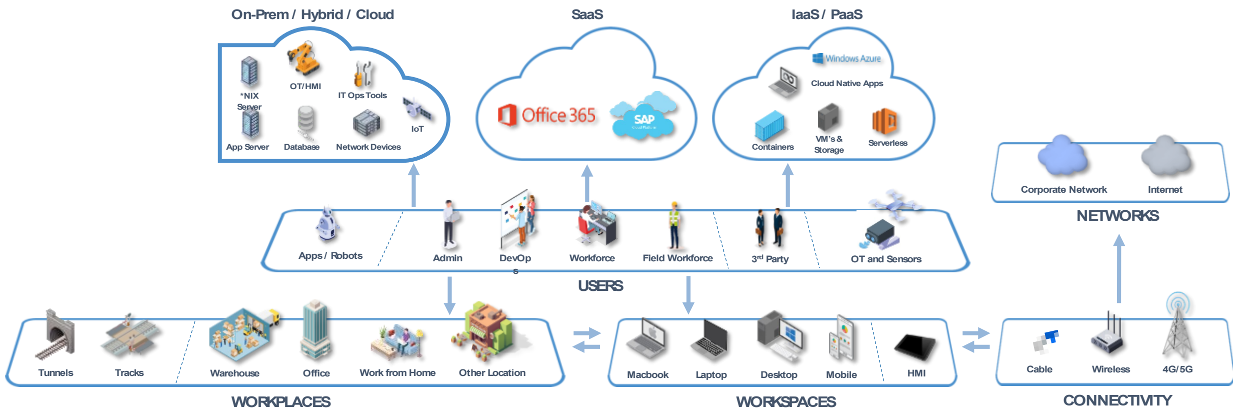
Defense in Depth

Defense of our entire IT and OT/Railway perimeter

24/7 Monitoring and Incident Response

End-to-End Defense in Depth





7

CyberSOC Objectives

Surveillance of our entire IT and OT/Railway perimeter

To achieve a sufficient level of cyber resilience, Infrabel has chosen to set up a CyberSOC with a Managed Services contract in which the partner supports Infrabel in reducing its risks across its entire scope and increasing its overall maturity.

THALES
Thales Cyber Solutions Belgium

Security Posture

The CyberSOC's mission is to strengthen our security posture so that we are sufficiently resilient in the event of cyberattacks.

Surveillance

The CyberSOC is responsible for monitoring our perimeter to detect signs of cyber threats, such as suspicious network activity or intrusion attempts.

Prevention

CyberSOC also strives to prevent cyberattacks by implementing security controls and best practices in cybersecurity.

Incident Response

In the event of a cyberattack, the CyberSOC is responsible for responding to the incident and taking measures to limit the damage and restore the affected systems.

Continuous Improvement

The CyberSOC works with our internal teams and external partners to investigate the incident, determine its root cause, and correct it.

8

CyberSOC Services

CybserSOC helps to consolidate the measures taken in each area.

GOVERN	Internal action plan and with suppliers → Resources + Budgets + Reporting ITSM process → ICC + RIOC + Suppliers → Change Management + Reporting	
IDENTIFY	Asset Management + Reporting Asset and application approval Automated connectivity provisioning	Risk Analysis
PROTECT	Security Posture Management Network Segmentation Patch Management + Reporting	
DETECT	Threat Hunting Collecte des logs → Big Data → CyberSOC Use Cases CyberSOC	Vulneralibity Management Technical Security Assessments Audits
RESPOND	CSIRT + 3rd Lines with Suppliers Incident Management + Reporting DRP + Testing	Incident Response Playbooks Crisis Management + NIS2 Notification Risk Treatment Plan
RECOVER	Backup/Restore + Tests	Root Cause Analysis

Provided by CyberSOC

9

Definition of a Use Case

The CyberSOC project is driven by the implementation of Use Cases

A « Use case » is defined as a security monitoring scenario aimed at identifying cyber threats.

It includes strategic, tactical and operational elements, describing the manifestations of these threats from the highest level (cybercriminals' modus operandi) to the lowest level (security events, logs) within the monitored infrastructure.

- A Use Case also includes incident response actions via playbooks and is linked to operational factors (impacts).
- It also defines how a system is configured to detect threats.

- For each detection, an incident is created and a playbook describes in detail the actions to be taken and by whom until the incident is resolved.
- The Use Cases are regularly reviewed in line with changes in the scope of Infrabel and its partners, threats and risks.

10

High Level Use Cases

Use cases must be specified and adapted to the Infrabel context

« Prevention » Use Cases

1. Compliance to NIS2
2. Compliance to IEC 62443
3. Compliance for Asset Inventory
4. Compliance for Identity and Access
5. Compliance for System Hardening
6. Compliance for Removable Media
7. Compliance for External Hardware
8. Compliance for Network Access
9. Compliance for Network Segmentation
10. Compliance for Firewall Rules
11. Compliance for Endpoint Configuration
12. Compliance for Secure Remote Access
13. Compliance for Internet Connections
14. Compliance for DevSecOps
15. …

« Detection » Use Cases

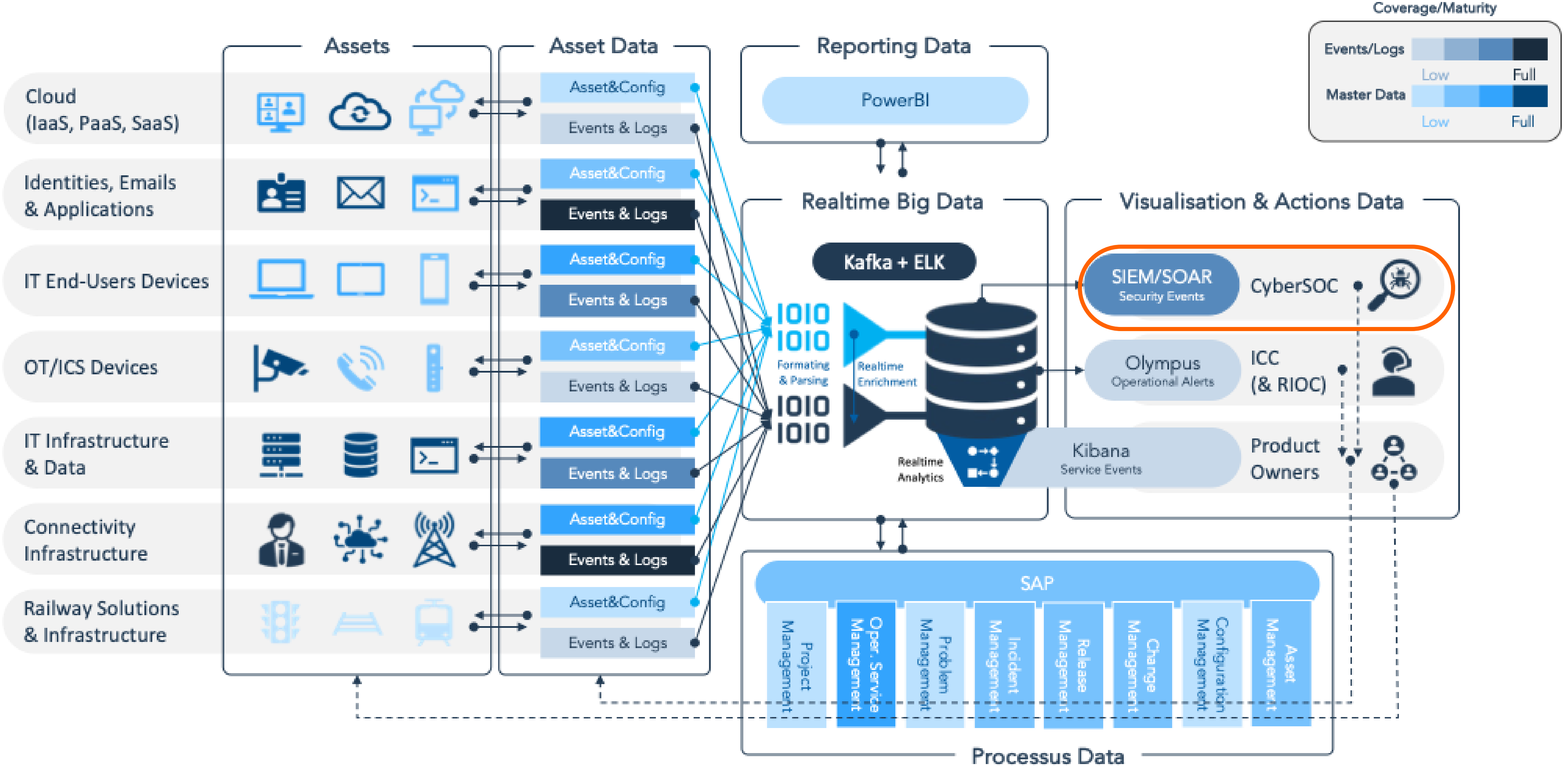
1. Unkown/Rogue Asset detection
2. Vulnerability Attacks detection
3. System Changes detection
4. Network Scan detection
5. Unkown (Remote) Access detection
6. Malware/Ransomware Infection attacks detection
7. Phishing and Social Engineering attacks detection
8. Supply Chain attacks detection
9. (D)DoS attacks detection
10. Man-in-the-middle attacks detection
11. Data Breach/Loss attacks detection
12. Compromised User Credentials detection
13. Unusual behavior on privileged accounts detection
14. Physical attacks detection
15. …

1st challenge: collecting data

11

Data Integration

CyberSOC is part of our overall Data strategy



Coverage/Maturity

Events/Logs: Low – Full

Master Data: Low – Full

Assets

Asset Data

Cloud (IaaS, PaaS, SaaS) – Asset&Config, Events & Logs

Identities, Emails & Applications – Asset&Config, Events & Logs

IT End-Users Devices – Asset&Config, Events & Logs

OT/ICS Devices – Asset&Config, Events & Logs

IT Infrastructure & Data – Asset&Config, Events & Logs

Connectivity Infrastructure – Asset&Config, Events & Logs

Railway Solutions & Infrastructure – Asset&Config, Events & Logs

Reporting Data

PowerBI

Realtime Big Data

Kafka + ELK

1010 1010

Formating & Parsing

Realtime Enrichment

Realtime Analytics

Visualisation & Actions Data

SIEM/SOAR Security Events – CyberSOC

Olympus Operational Alerts – ICC (& RIOC)

Kibana Service Events – Product Owners

SAP

Project Management

Oper. Service Management

Problem Management

Incident Management

Release Management

Change Management

Configuration Management

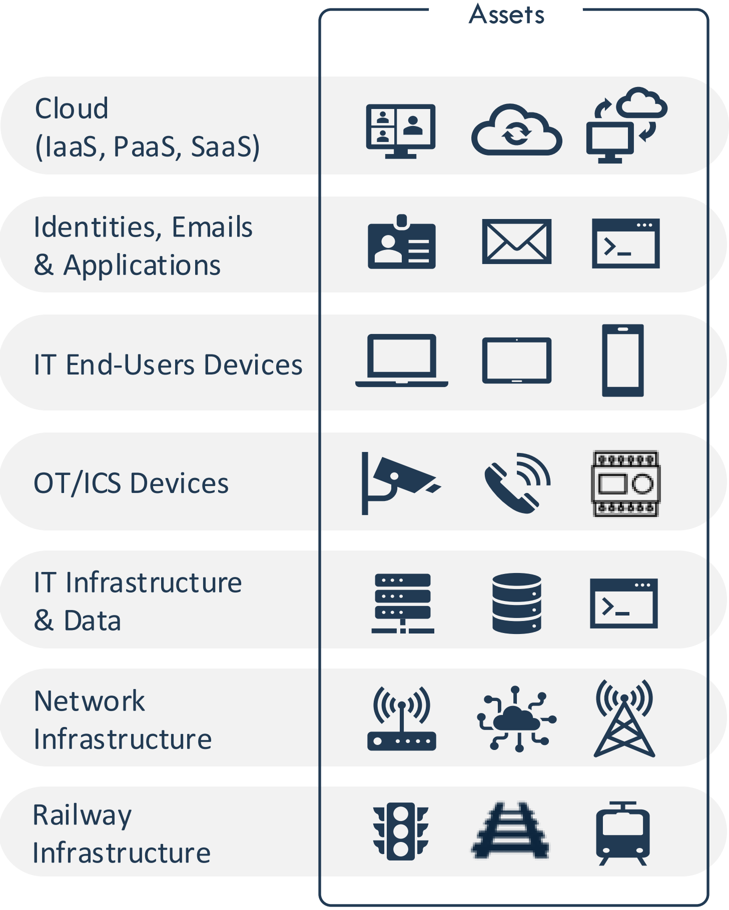
Asset Management

Processus Data

12

Assets by Numbers

A lot of Assets to integrate



+50	Log sources	2+1	Datacenters		
80.000	Identities	10.000	Emails	700	Applications
8.000	PC	5.000	Smartphones		
10.000	Cameras	5	Tunnels	5000	Buildings/Shelters
3.000	Servers	1.000	Databases		
10.000	Networks Devices	100.000	IP Addresses		
3.600 km	Tracks	700 BTS	GSM-R		
32 RBC	ETCS L2	800	Level Crossings	10.000	Signals

13

Our (Big) Data by numbers

Cybersecurity represent +60% of logs data

Assets

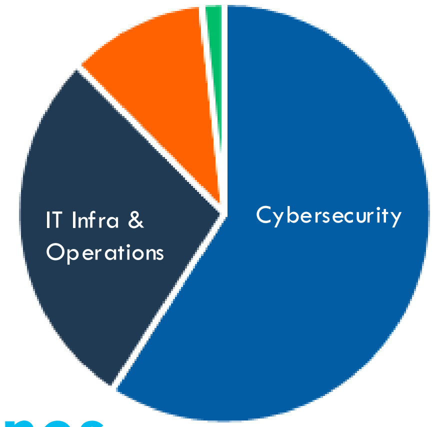
- Cloud (IaaS, PaaS, SaaS)
- Identities, Emails & Applications
- IT End-Users Devices
- OT/ICS Devices
- IT Infrastructure & Data
- Network Infrastructure
- Railway Infrastructure

+700 billion

More than 700 billion logs indexed (yearly)

+600 pipelines

Set up of more than 640 data ingestion pipelines



+900 TB

Over 900 TB of data

+70 Kibana spaces

+70 used last month

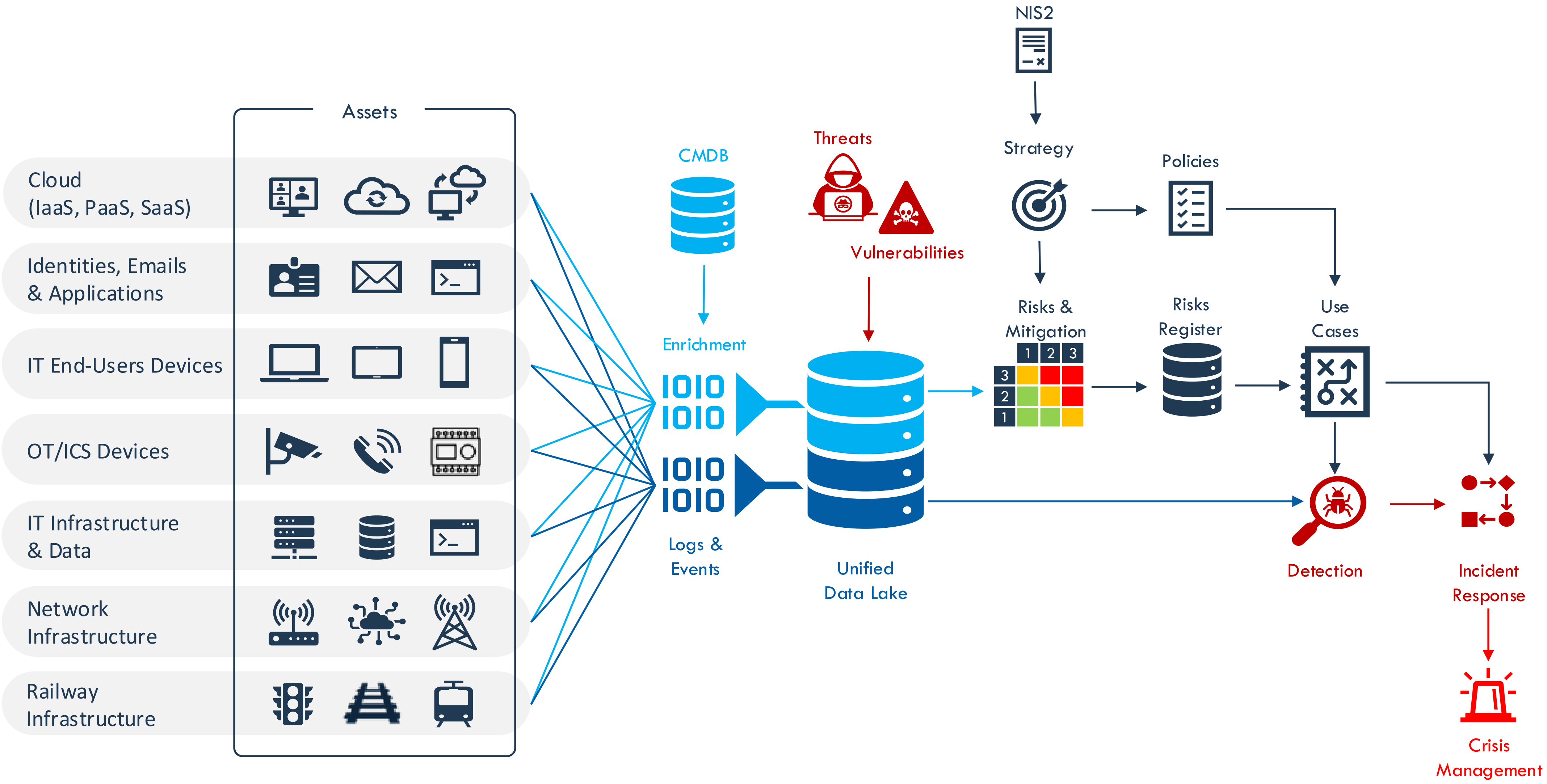
+200 unique users

on Kibana last month

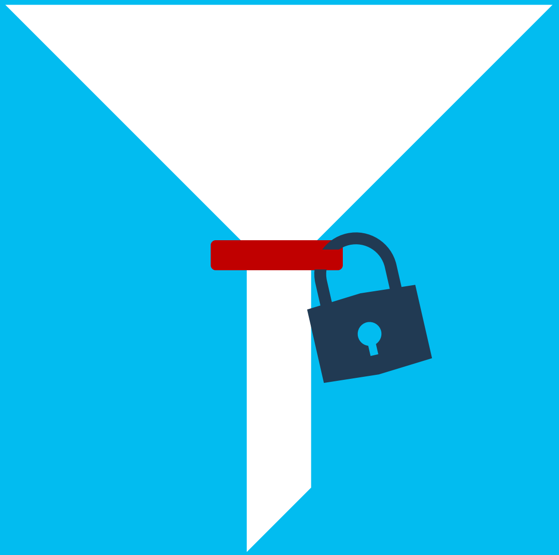
14

CyberSOC Data Flows

From Logs to Incident Response



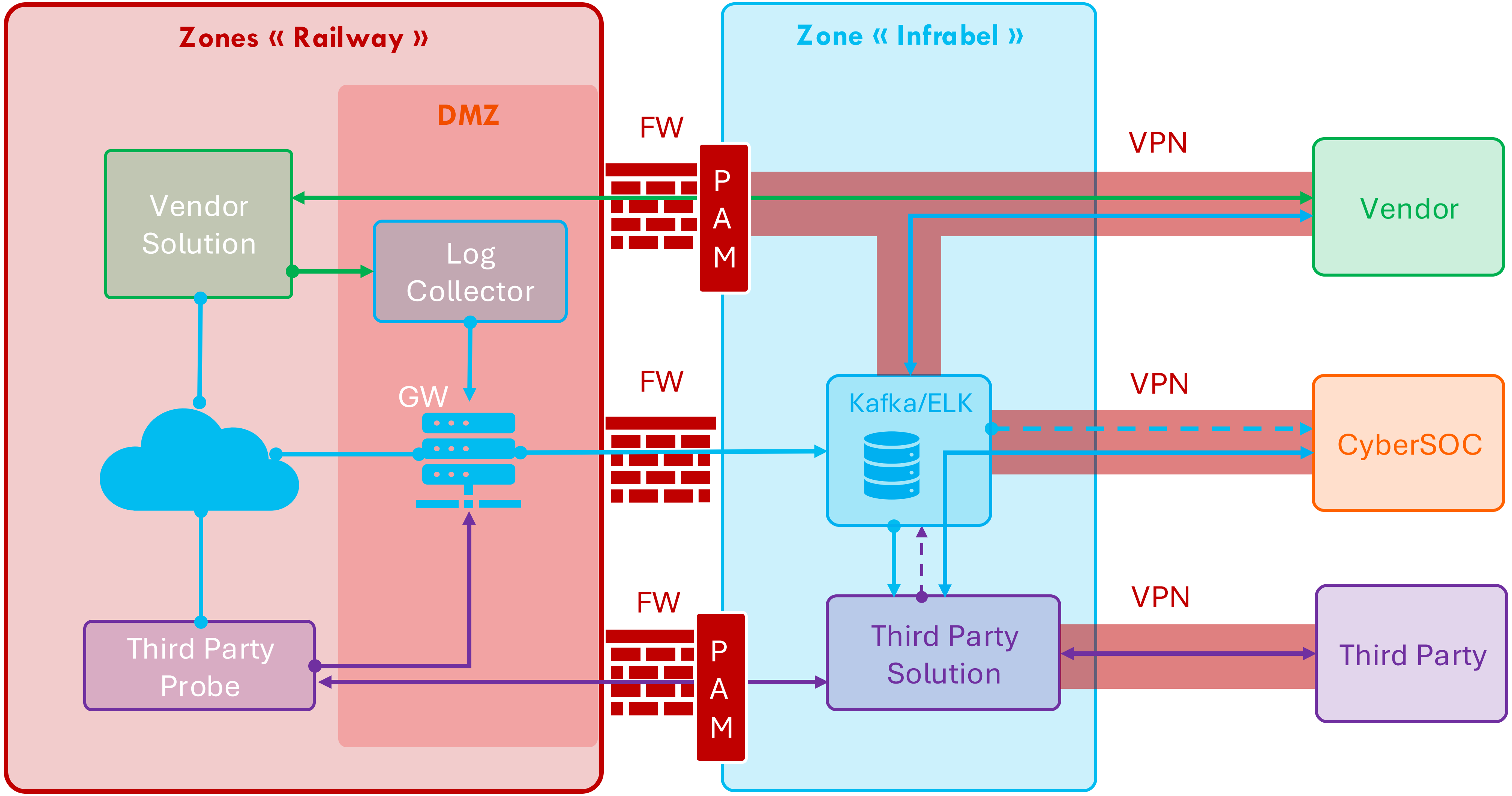
2nd challenge: collecting data on OT and Railway



15

Security Architecture

All interconnections and data flows are secured by design

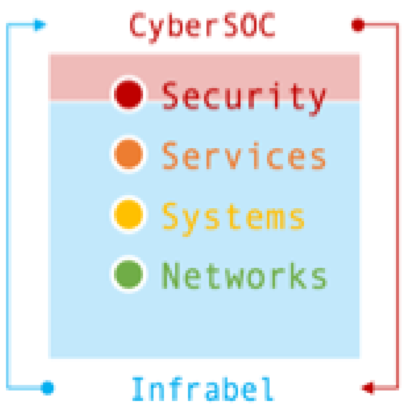


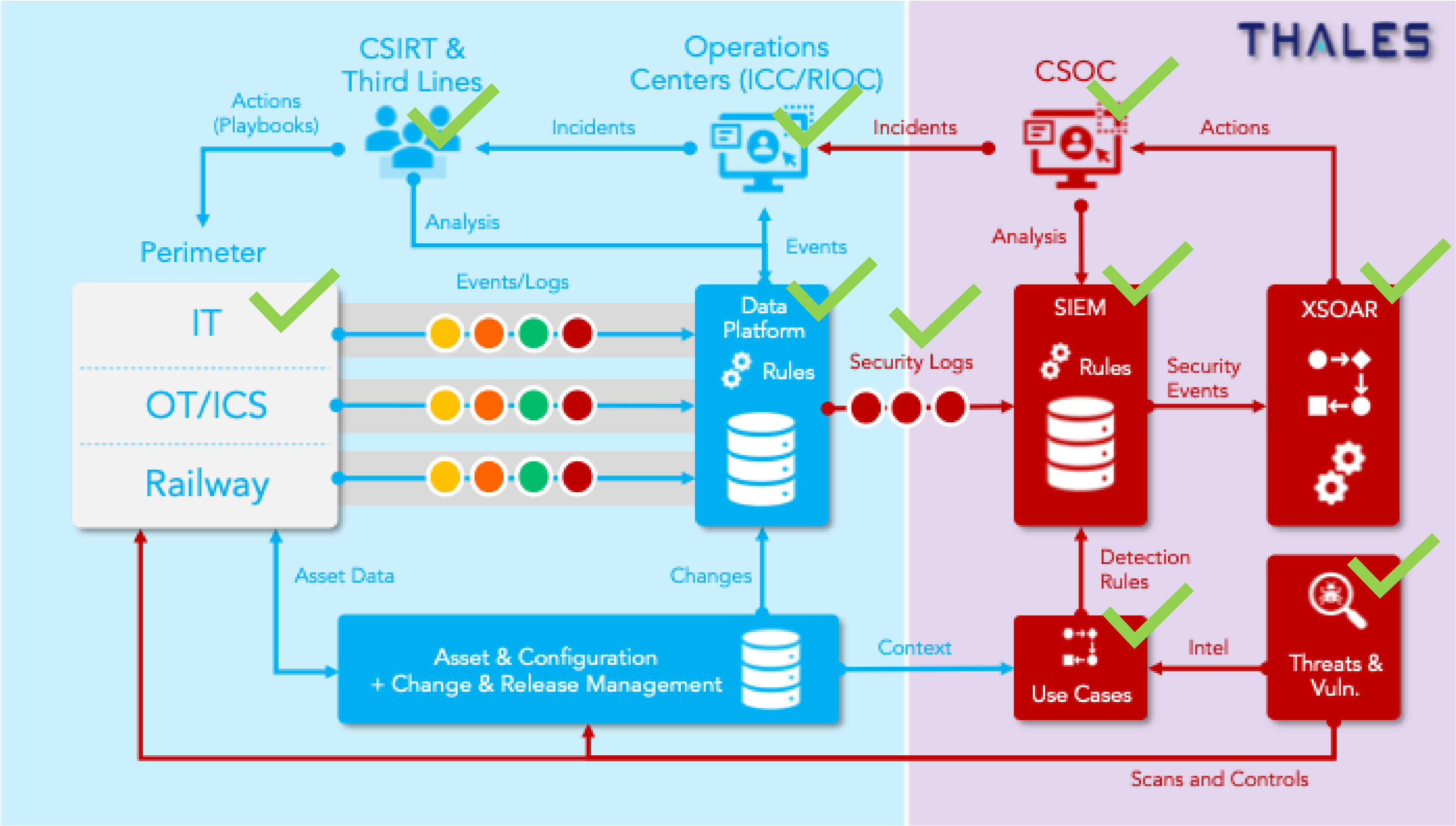
Results

16

Integration

The CyberSOC is integrated with Infrabel

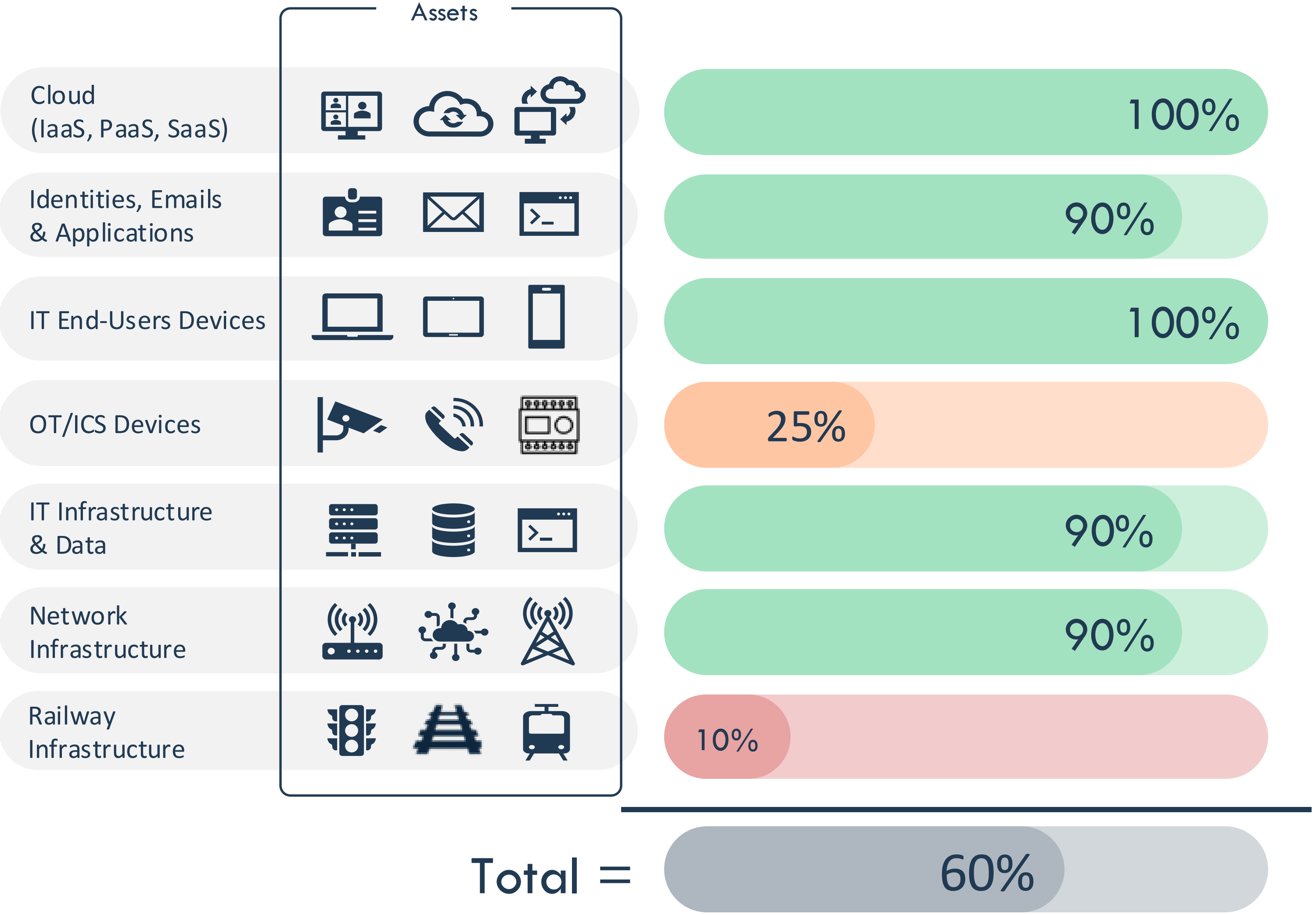




Done

Use Cases Coverage

We didn't achieve 100% coverage…



Extension of Logs collection to OT systems…

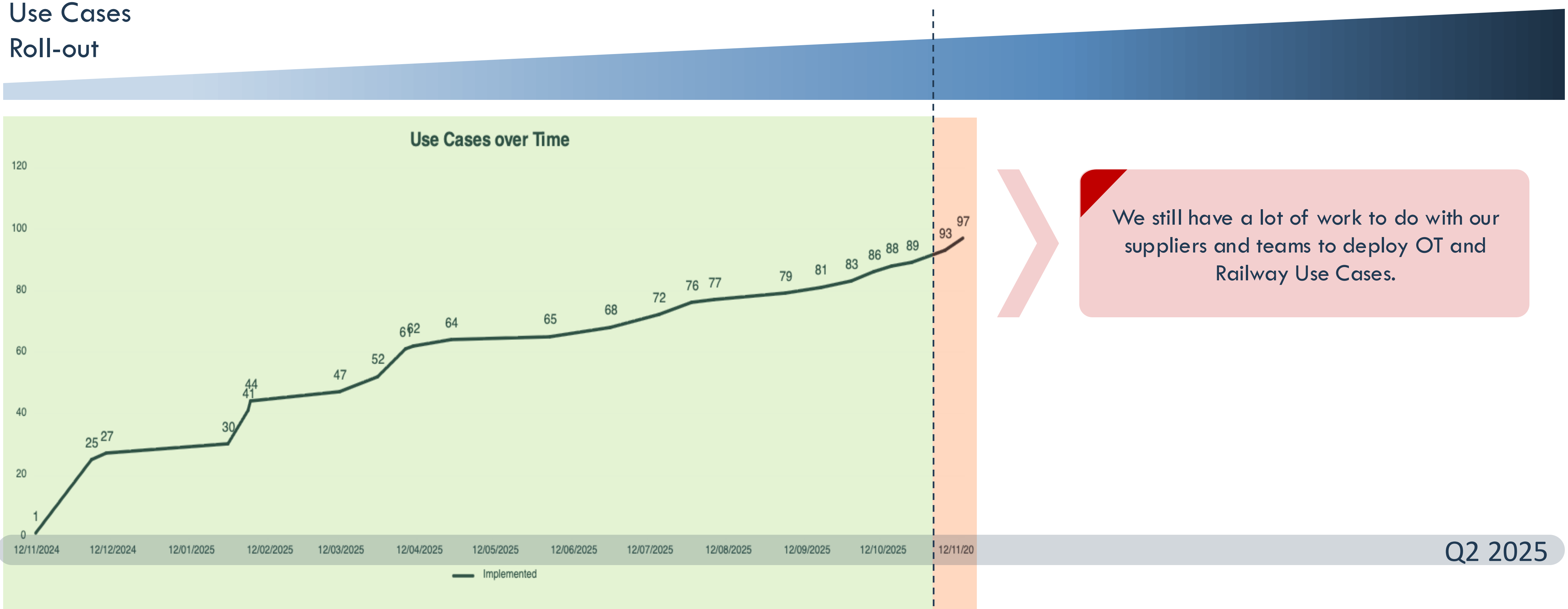
Need to be restarted from the beginning with our suppliers…

18

Use Cases Roll-out

Use cases are built and deployed sequentially

We are here → 60%



We still have a lot of work to do with our suppliers and teams to deploy OT and Railway Use Cases.

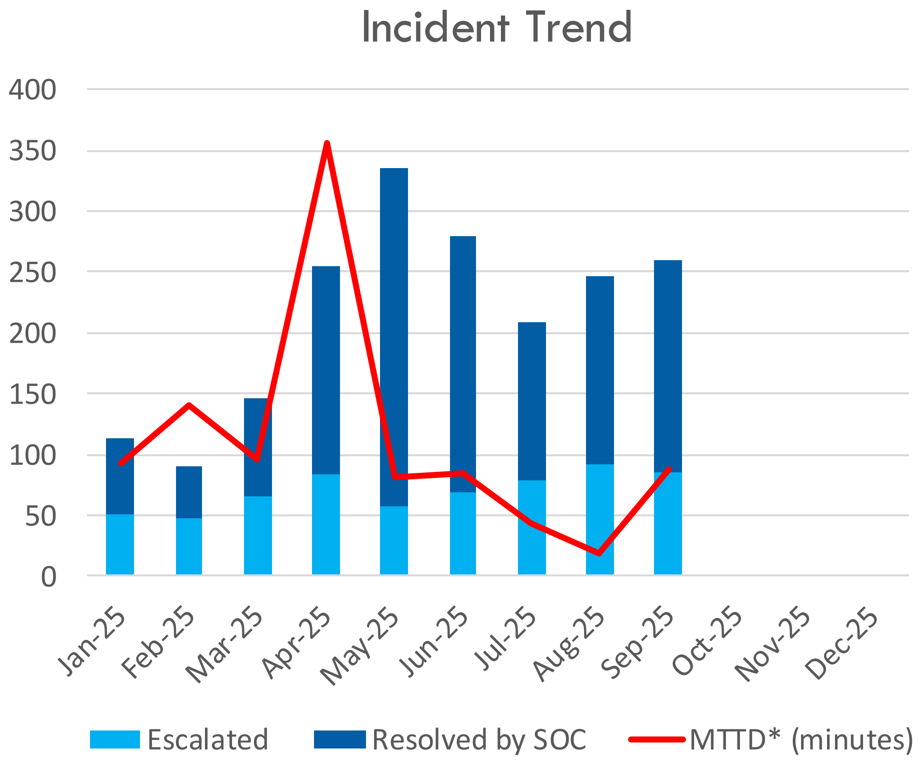
19

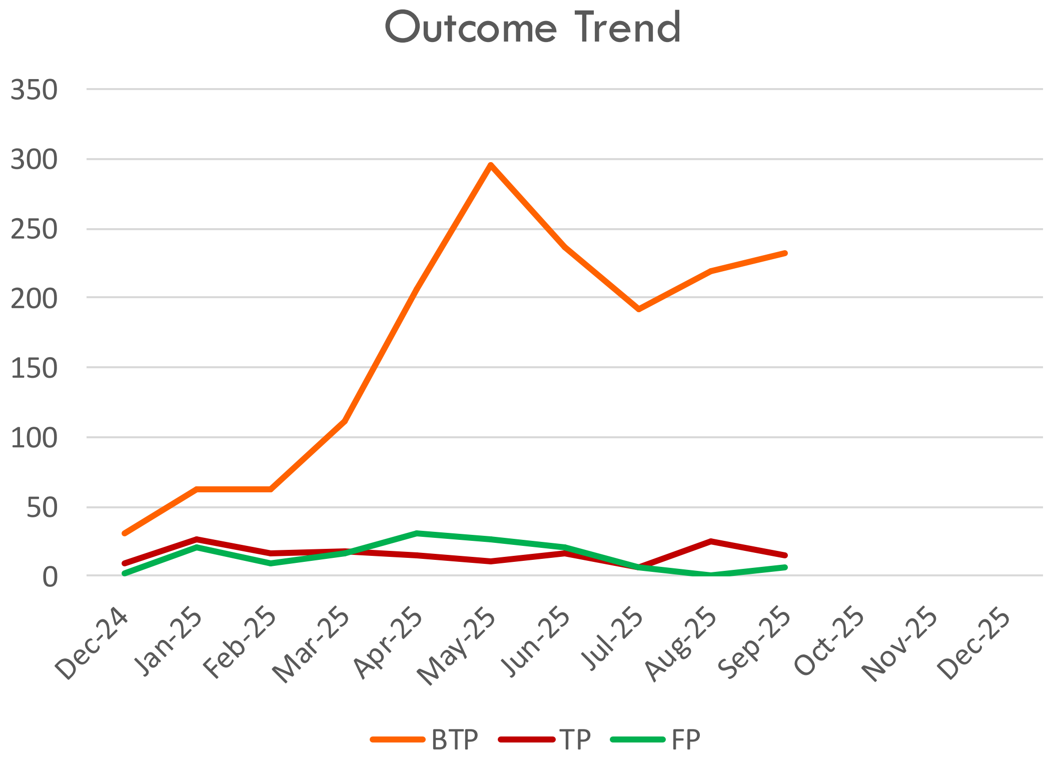
Incident Overview

The CyberSOC project aims to cover the entire scope of Infrabel

715 Incidents in Q3 2025

36% Incidents escalated in Q3 2025

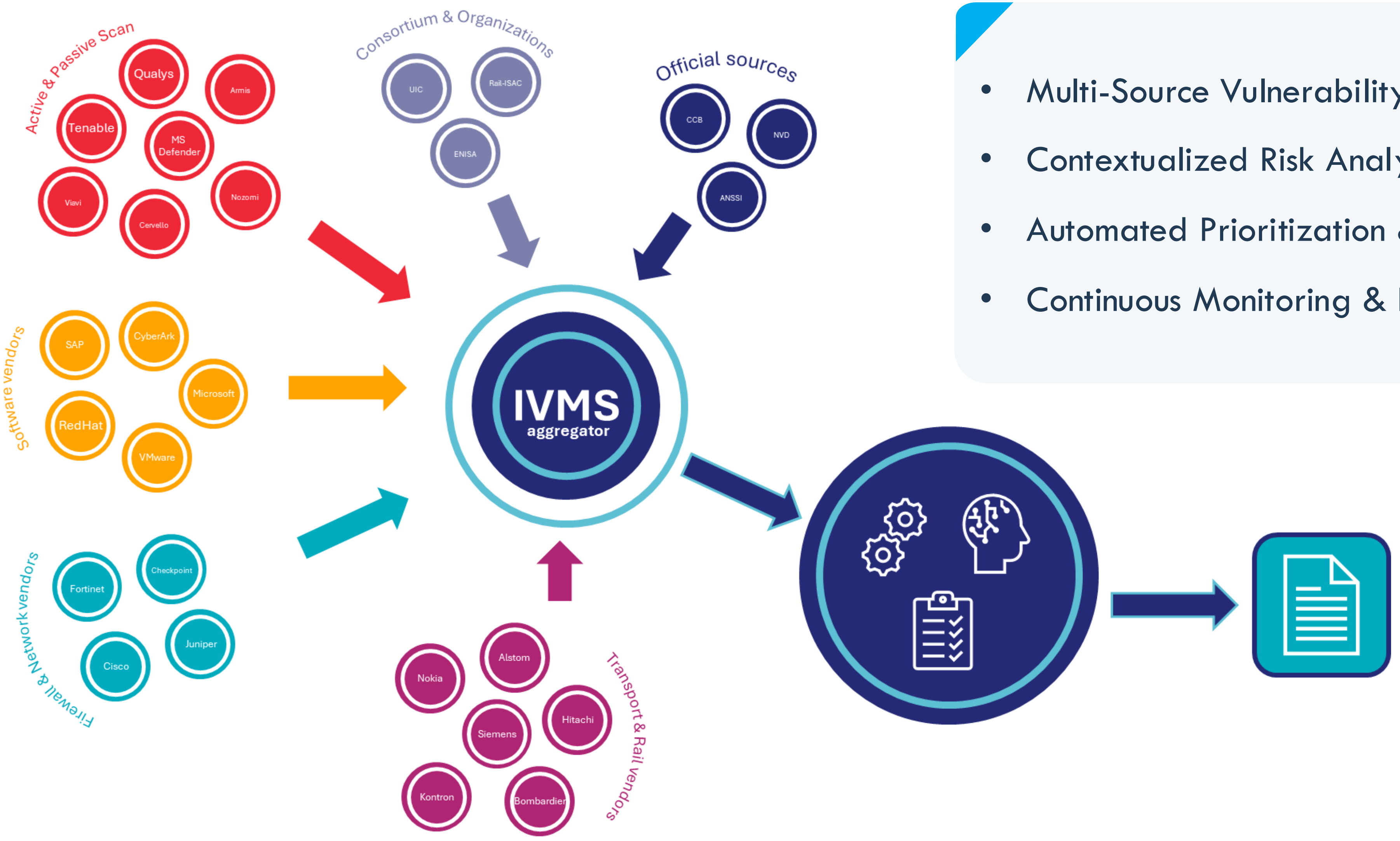




20

Vulnerability Management

IVMS = Integrated Vulnerability Management Service



- Multi-Source Vulnerability Aggregation
- Contextualized Risk Analysis
- Automated Prioritization & Remediation Guidance
- Continuous Monitoring & Reporting

Take Aways

21

Take aways

Summary of key points to remember

1. Collaboration between Infrabel and Thales
2. Improved visibility on our systems and our architectures
3. Improved Root Cause Analysis
4. Raising Awareness/Knowledge through incident feedback
5. Not easy journey, but the path is more important

22

Lessons Learned…

On building an OT and Railway CyberSOC

1. Raise Knowledge before starting → Project Team
2. Maturity in Risk Assessment → Use Cases on OT/Railway
3. Do not overlook the difficulty of collecting quality logs
4. Don’t deploy systems and only if this is really necessary
5. Yours suppliers are keys, but…

"I THINK HE MAY HAVE MISUNDERSTOOD WHEN I SUGGESTED USING A SOCKS PROXY TO BYPASS THE FIREWALL."

Tänan !