INFRABEL

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN UNION AGENCY FOR RAILWAYS

A CyberSOC, why and how

A very short introduction

Cybersecurity in Railways

3rd ERA – ENISA Conference, Athens November 2023

Cédric Cecotti

I-CISO

The Context


LIVE
11
FAKE
BREAKING NEWS
CYBER ATTACK ON BELGIAN RAILWAYS
08:57
ALL TRAINS STOP DUE TO CYBERATTACK ON SIGNALING SYSTEMS

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

William H. Webster, Former FBI Director

Our journey so far

Current Threat Level

Today

Short Term

Who are the Threat Actors ?

Individuals (Internal or External)

Satisfaction

Motive = Financial Gain or Revenge
Targets = Your Data or Network

Criminal Organisations

Profit

Motive = Profit, Financial Gain
Targets = People, Bank, Institution

Nation States

Geopolitical

Motive = Economic or Military
Targets = Infrastructures

Hackers/Hacktivists

Ideological

Motive = Publicity, Watch it burn
Targets = Anything and Everything

Terrorists/Extremists

Ideological Violence

Motive = Cause Support
Targets = Highly Visible Targets

Risk-Based Strategy

Cyber Resilience

Business Continuity

The European NIS Directive

NIS2 Directive is already there

The NIS Act of 7 April 2019 transposes European Directive (EU) 2016/1148 on measures to ensure a common high level of network and information system security in the Union

INFRABEL

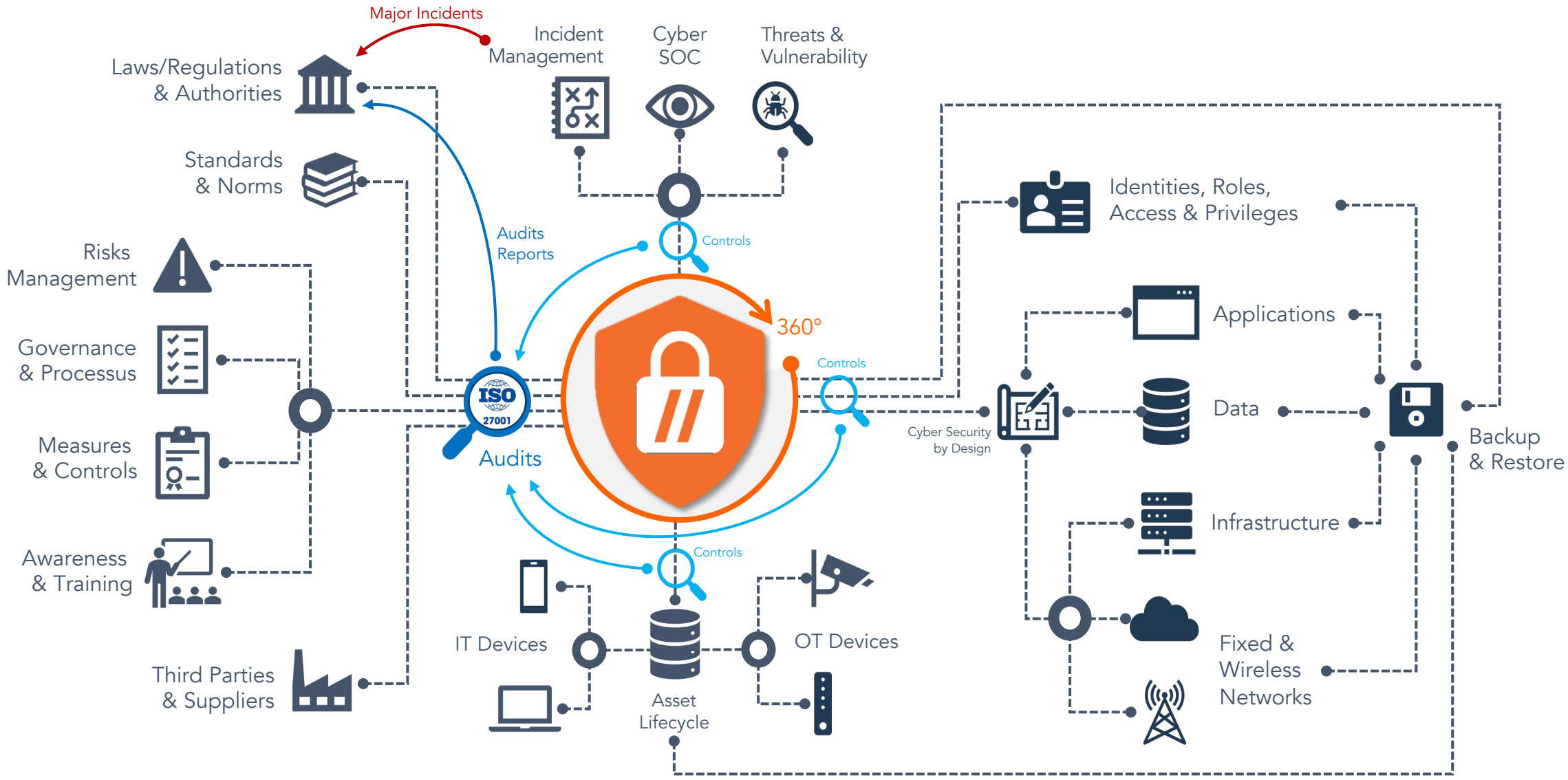
« Essential Services Operator »

- The adoption and implementation, within a timetable defined by the legislator, of the technical and organisational measures (I) necessary and proportionate (II) to manage the risks that threaten the security of networks and information systems, it being understood that these measures must guarantee a level of physical and logical security appropriate to the existing risks (III), taking into account the state of technical knowledge (IV).
- The notification and management of incidents having a significant impact on the security of networks and information systems linked to essential services;
- Regular internal and external audits of the networks and information systems supporting essential services.

Yearly

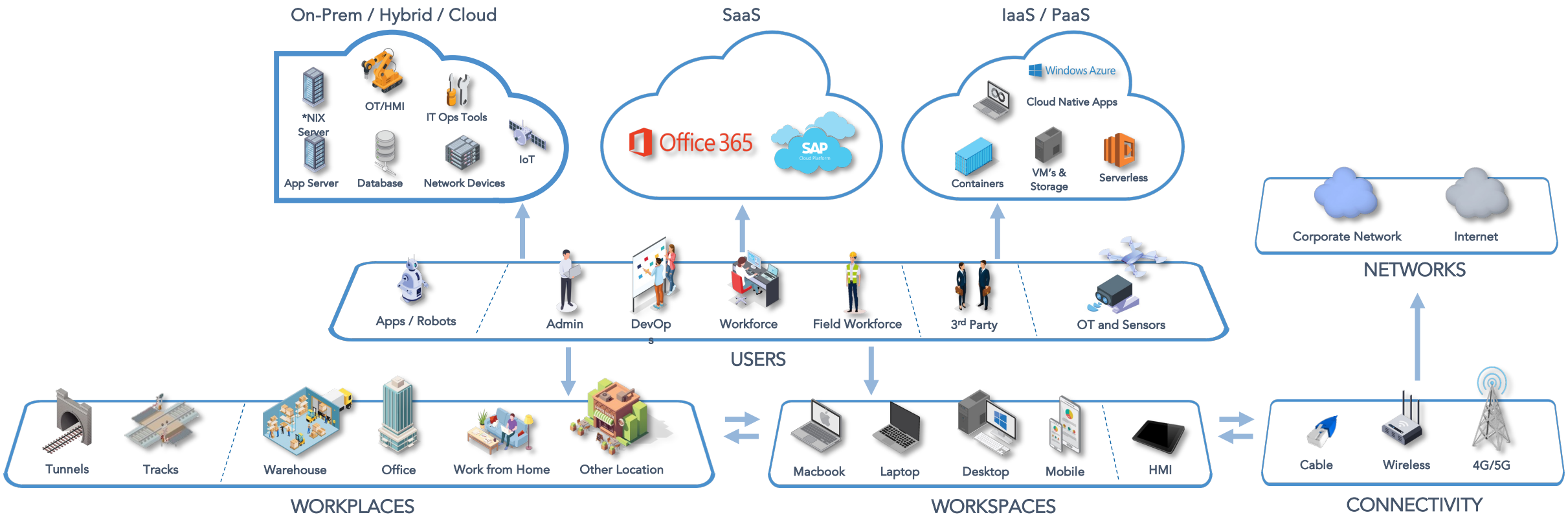
Every 3 years

We adopt an holistic approach



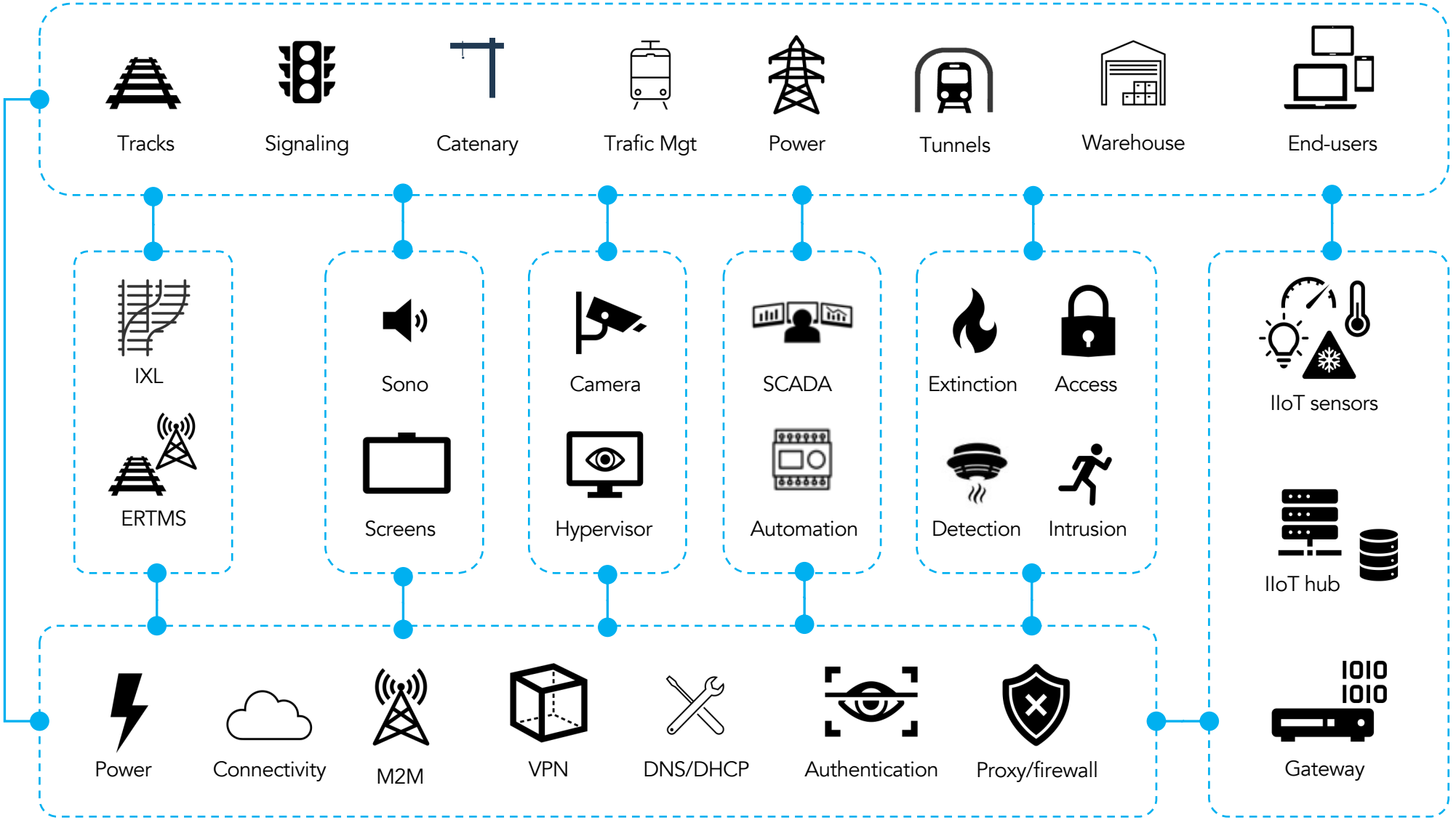
ICT Landscape

Our ICT Landscape becomes more and more complex and exposed



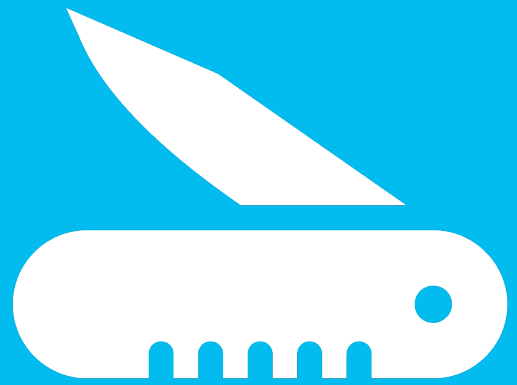
OT and Railway Landscape

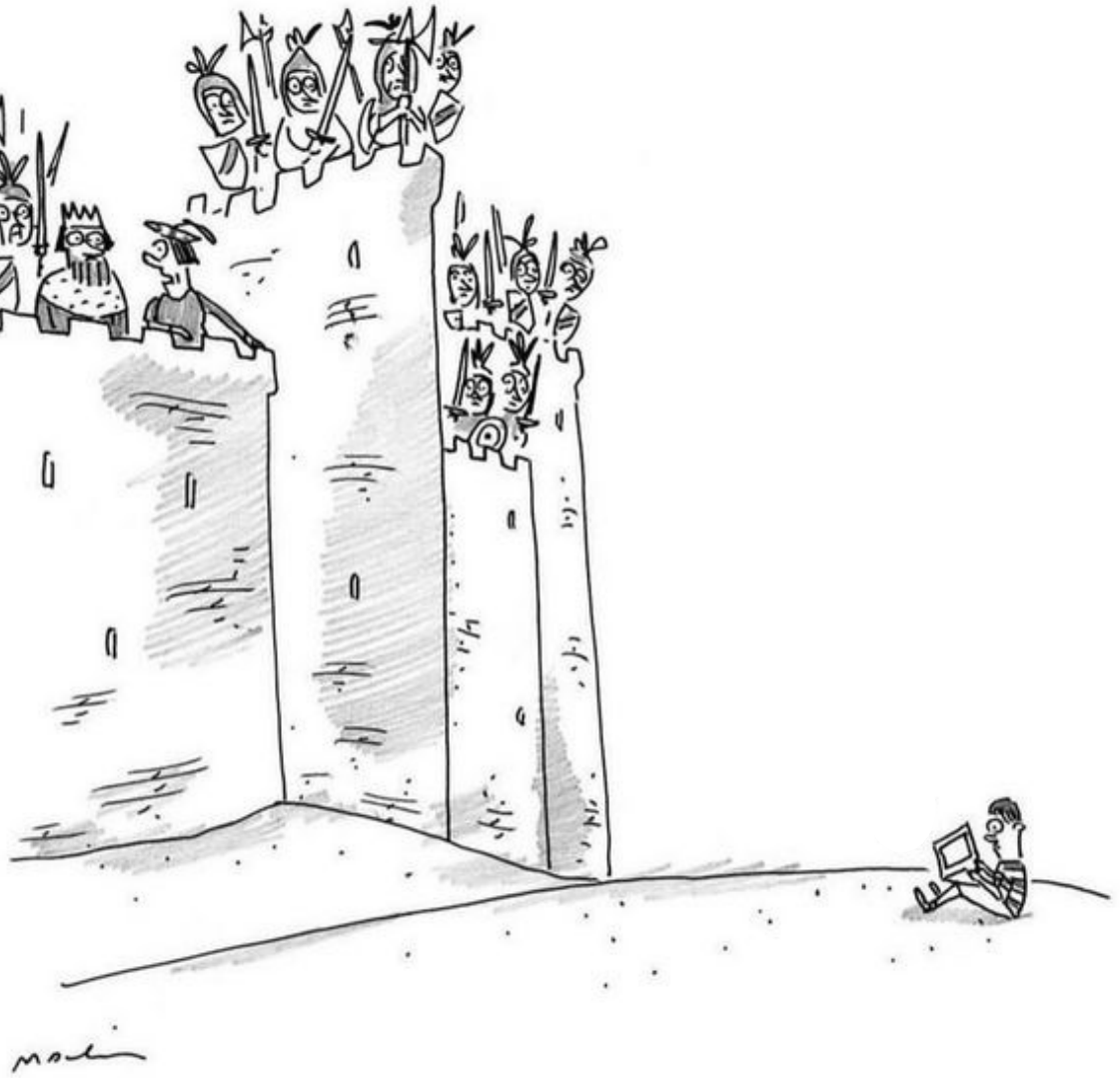
Our OT and Railway Landscape becomes also more and more complex and exposed



It's all about balance

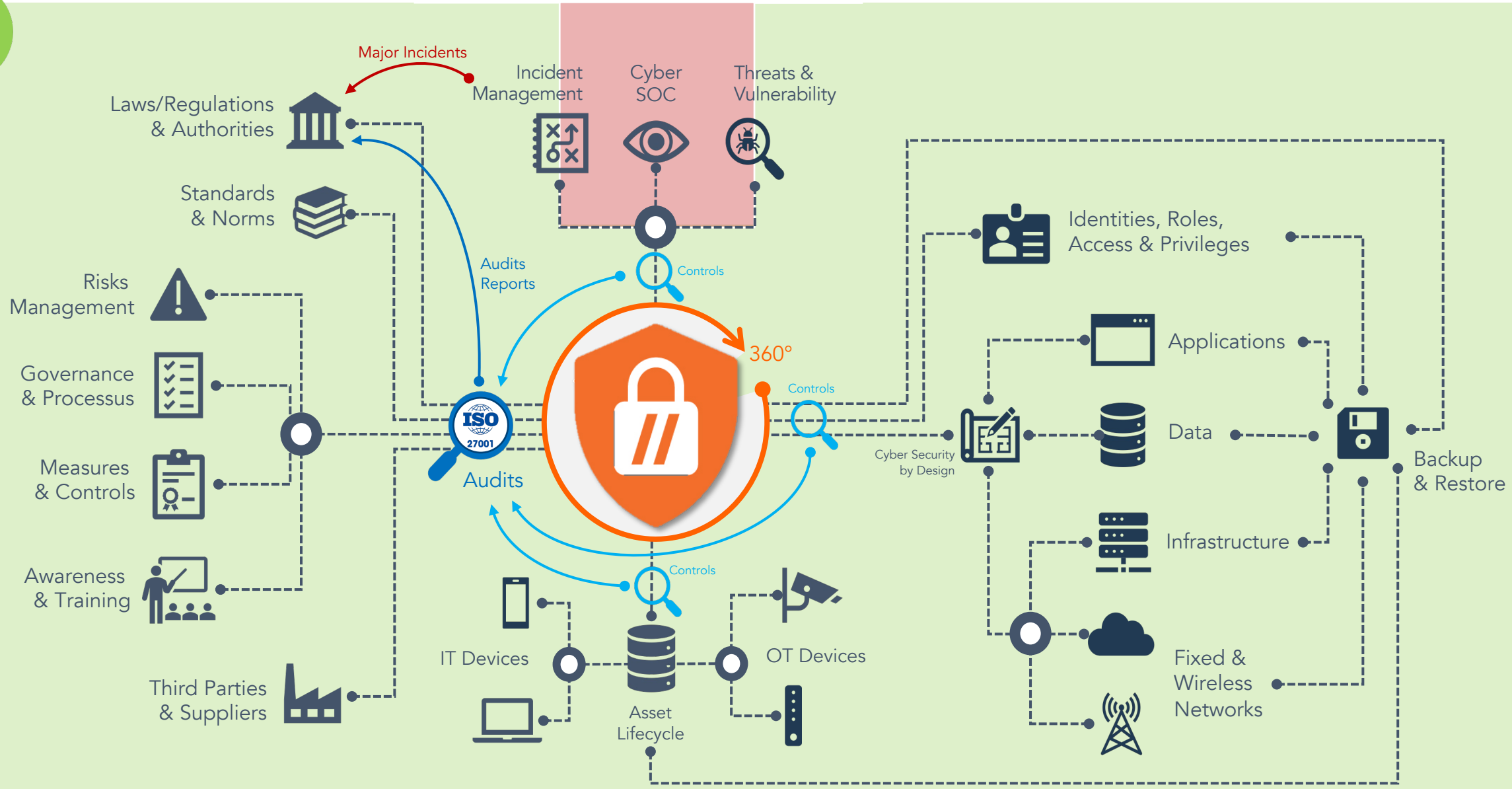
Why do we need a CyberSOC ?





"Bad news, Your Majesty—it's a cyberattack."

Why a CyberSOC ?

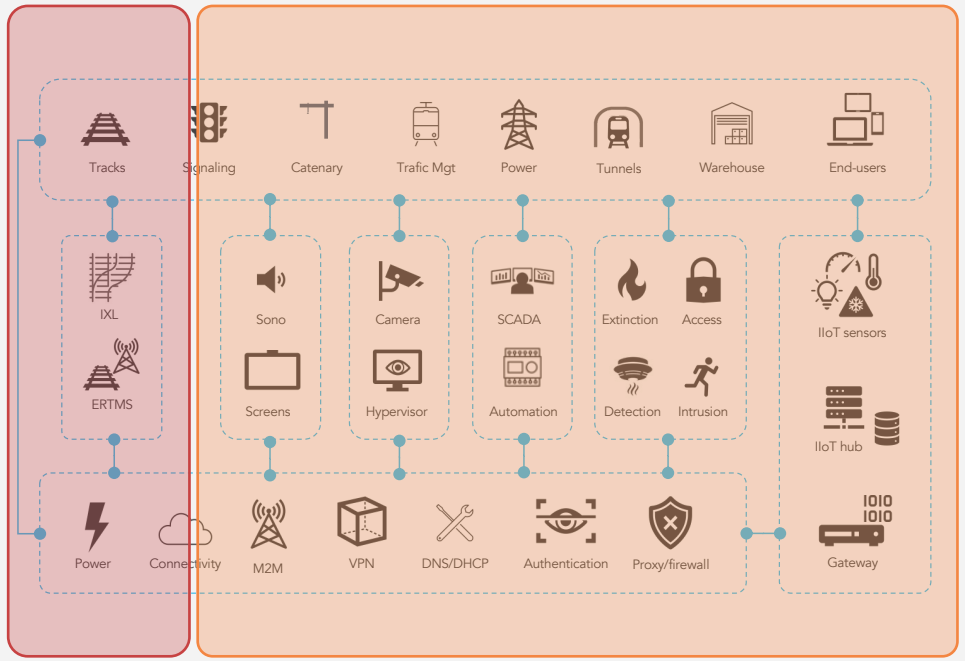


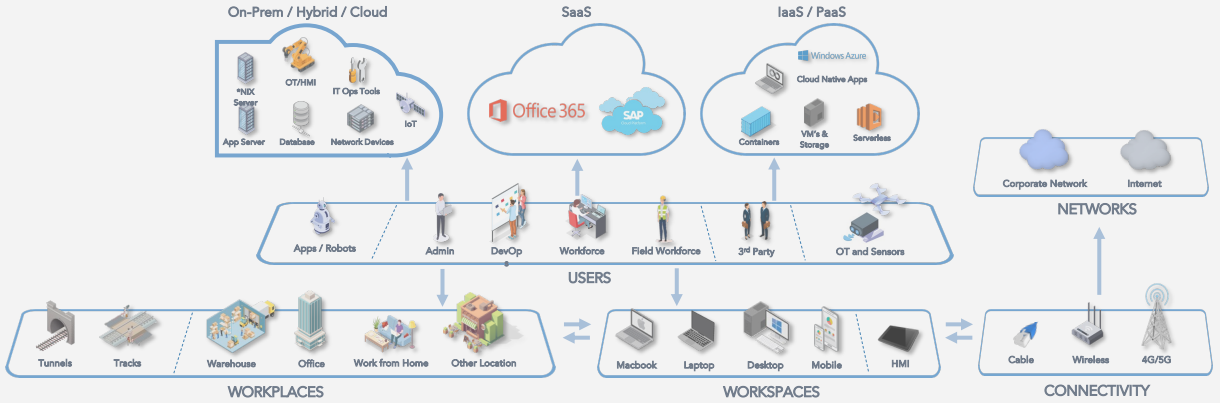
Why a CyberSOC ?

24/7 Surveillance

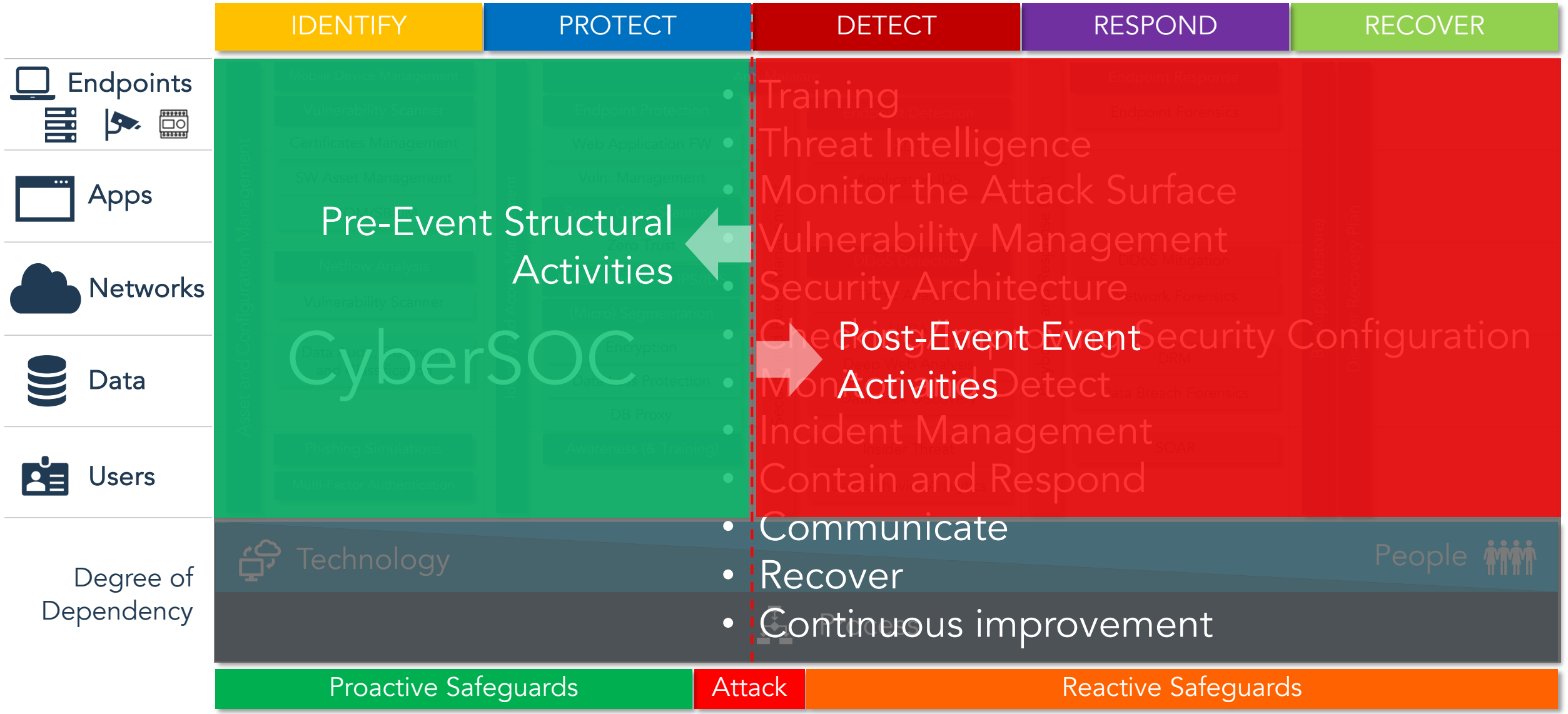
End-to-End Defense in Depth

Critical Systems



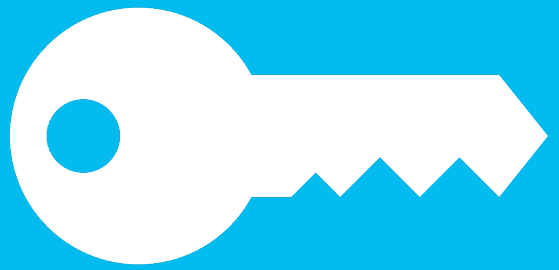


Why a CyberSOC ?



Implemented Not yet implemented

Key Challenges



Key Challenges

Choose your Strategy

We have opted for a global approach and to build our CyberSOC with an MSSP

Identify All Assets

Identifying all assets is the hardest essential prerequisite

Project Management

Solid project plan and organisation before getting started

Key Challenges

Design and Build Right

The design phase is crucial to build the correct solution at the right price

Involving The Organisation

Don't forget to involve the organisation in close collaboration

Third Parties Management

Third parties must also be involved from the beginning

Key Challenges

Tests & Validation

Test, test, test before putting each part in production and test again

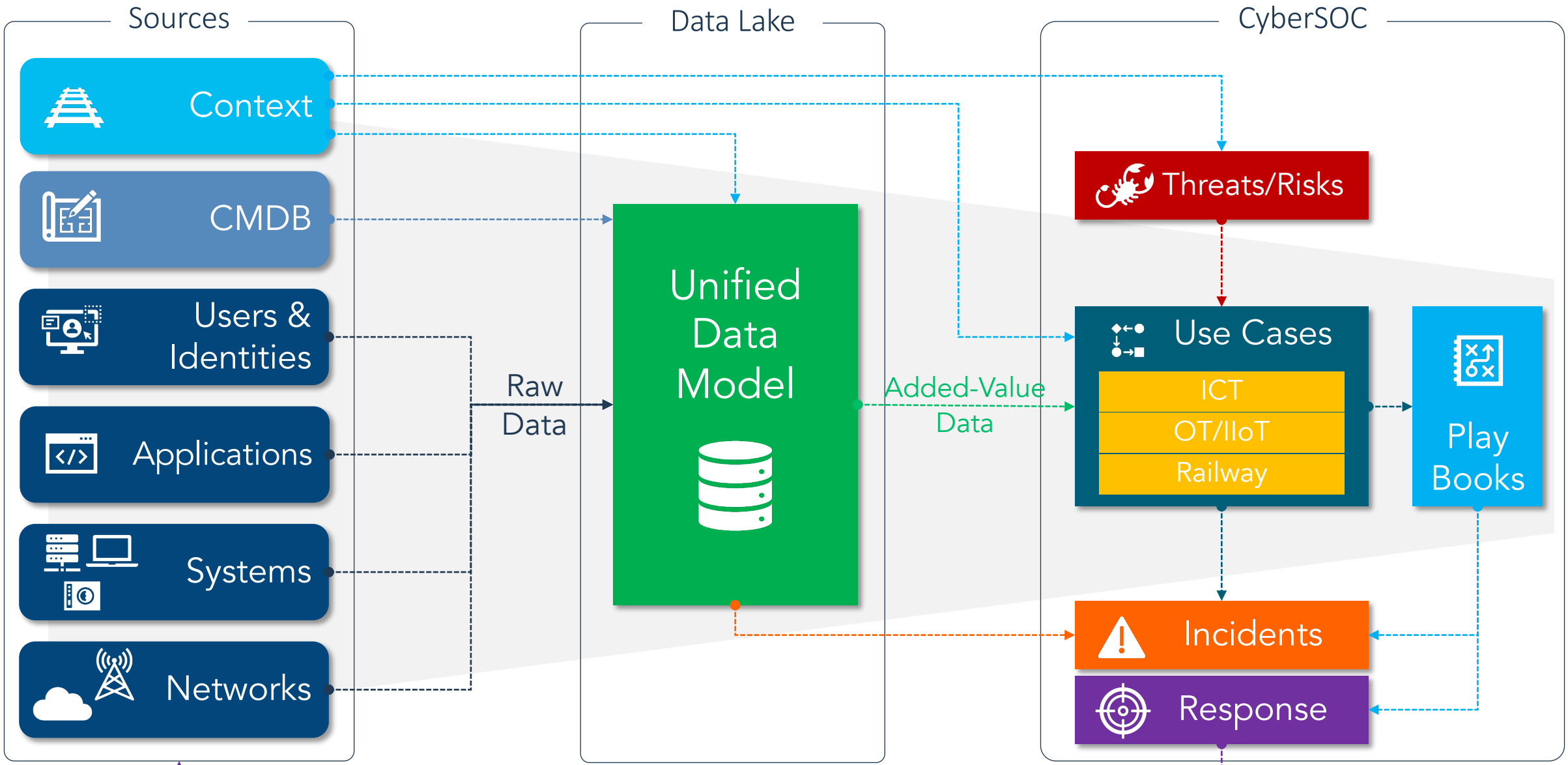
Use Cases Lifecycle

Use cases are key and must evolve according to context, threats and risks

Data Collection

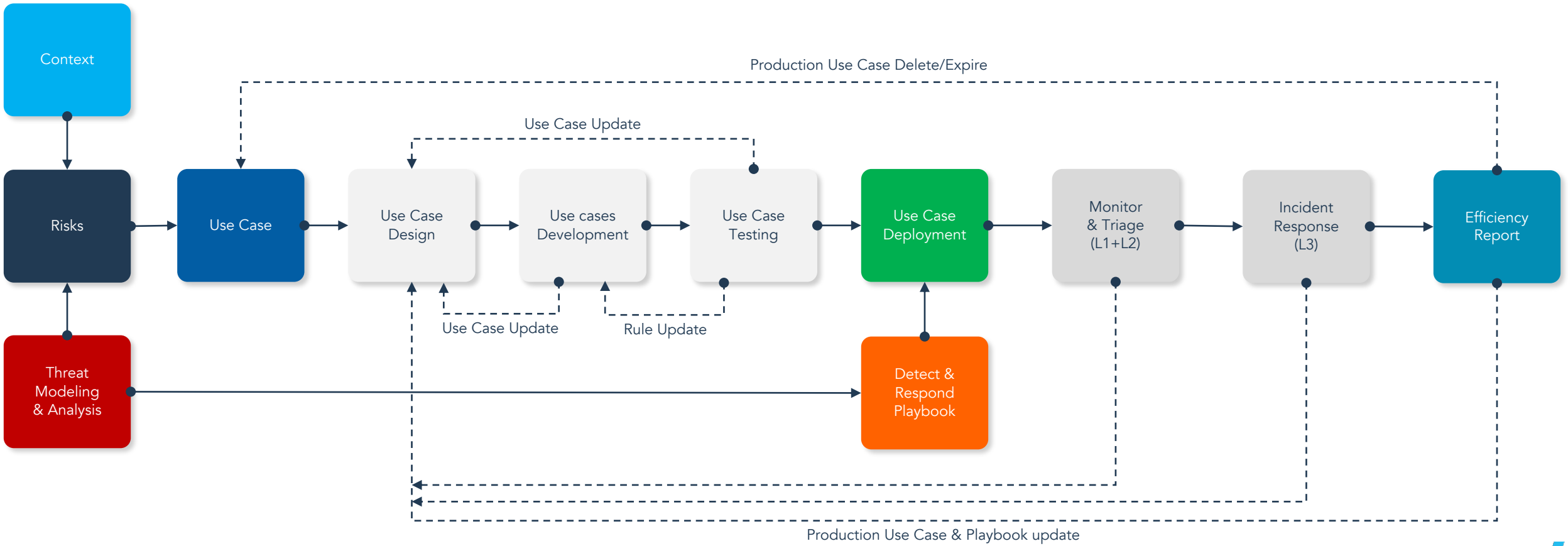
Without reliable and complete data, there can be no CyberSOC

Conceptual Architecture

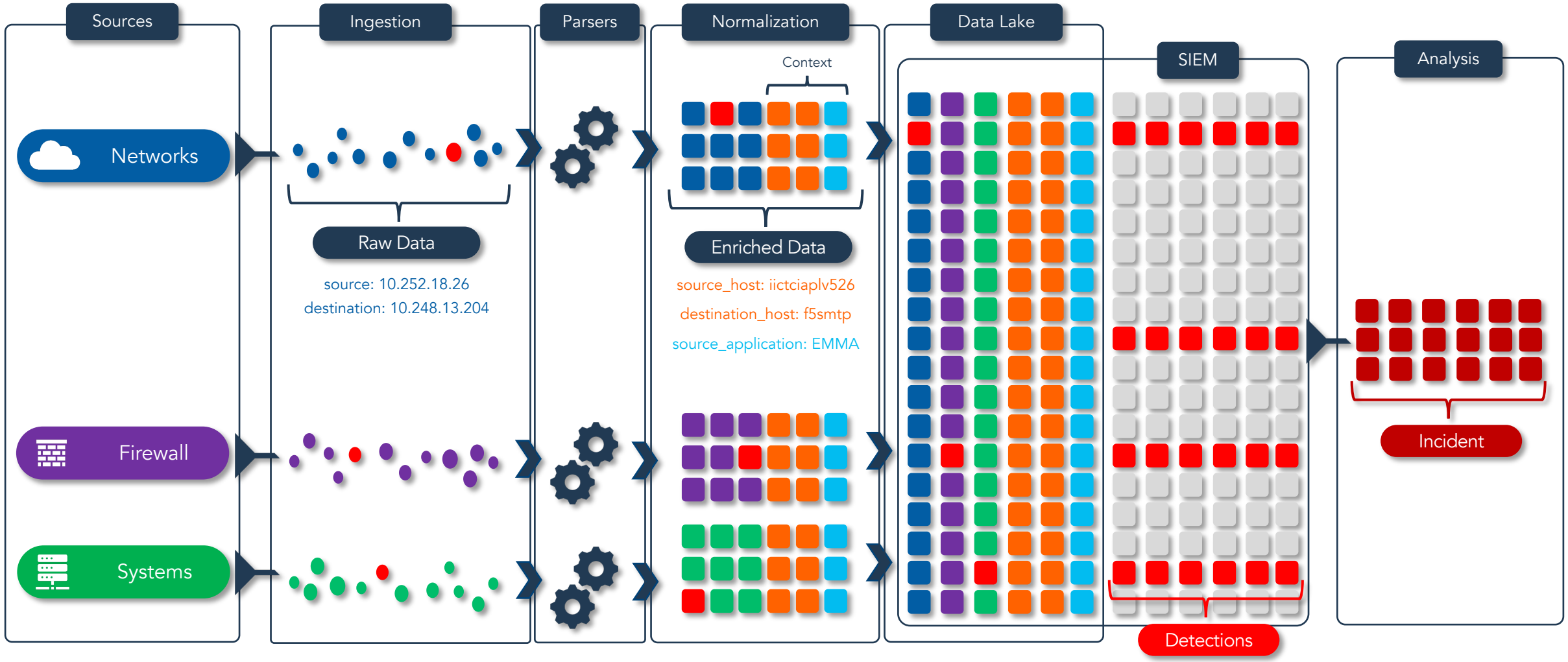


Use Cases Lifecycle

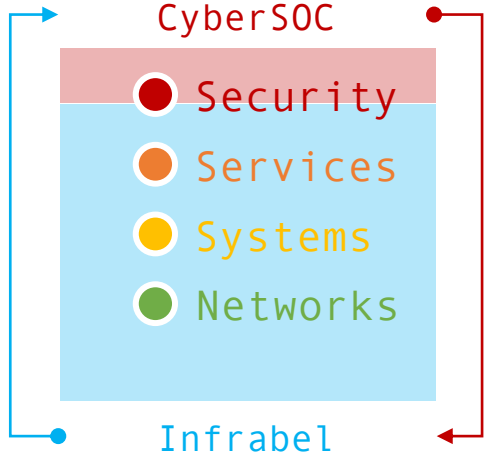
A "Use Case" refers to a specific scenario regarding risks and is designed to help identify, detect, and respond to various types of cyber threats or attacks.

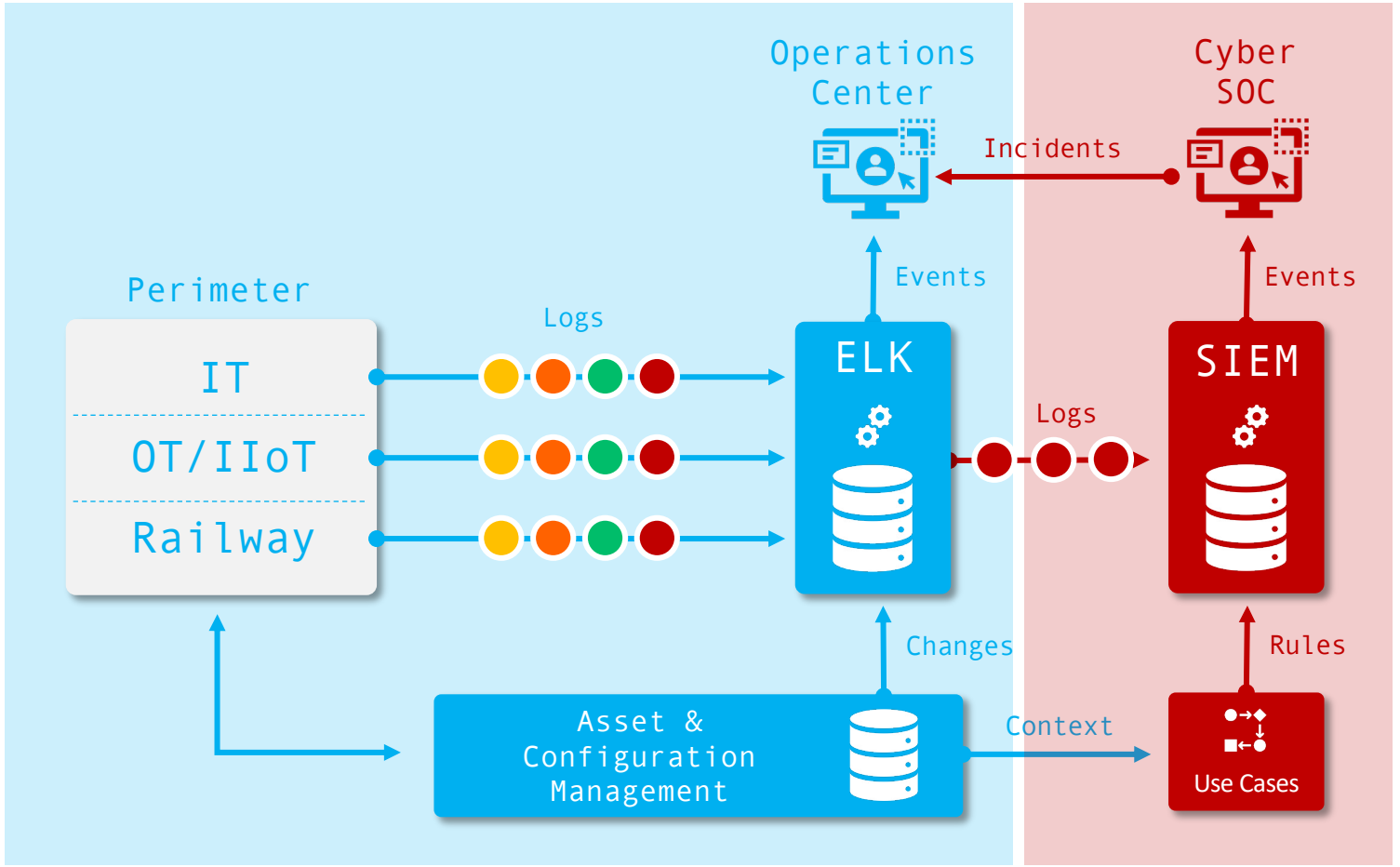


Data are the key

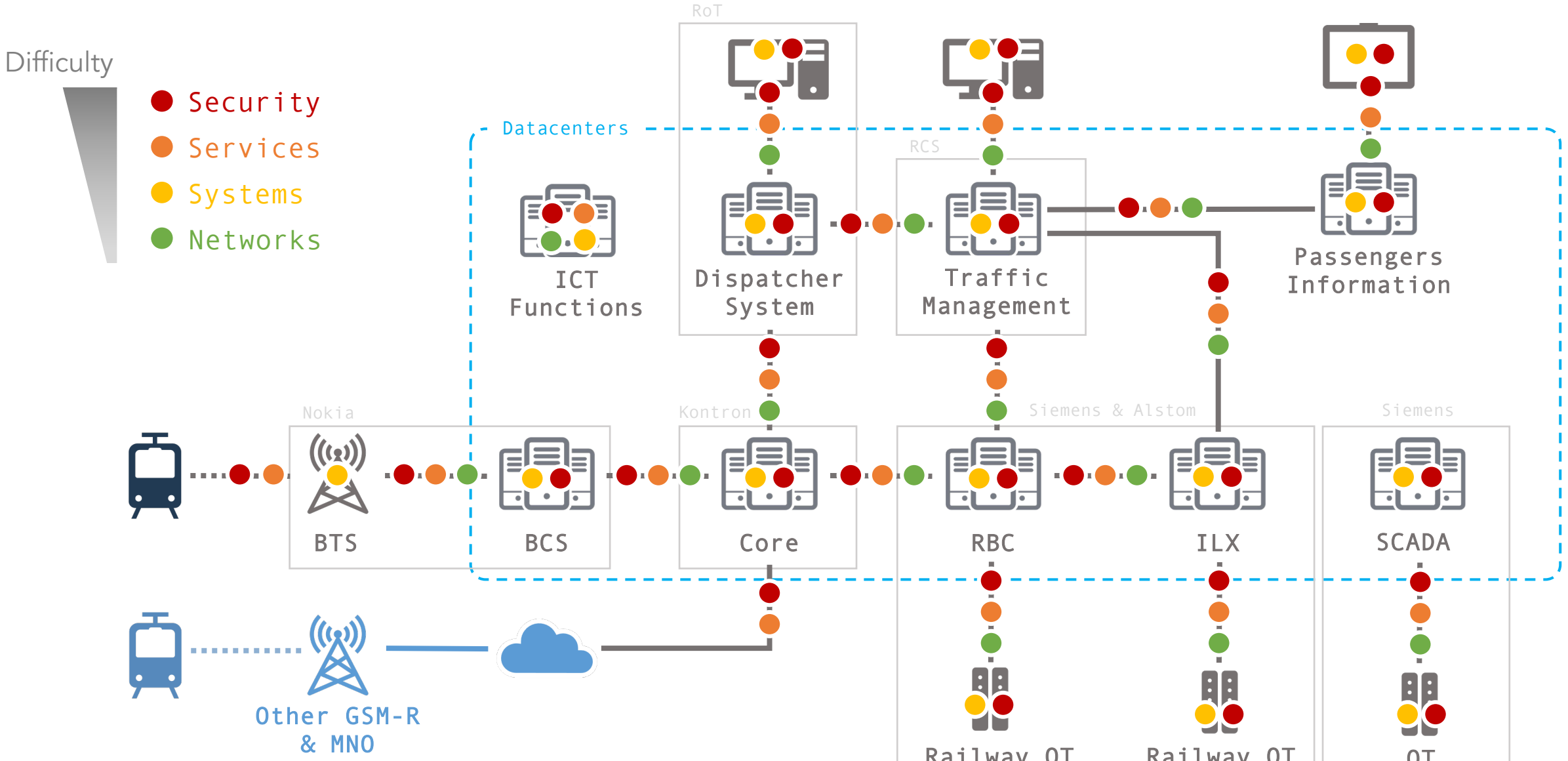


Data Collection and Analysis



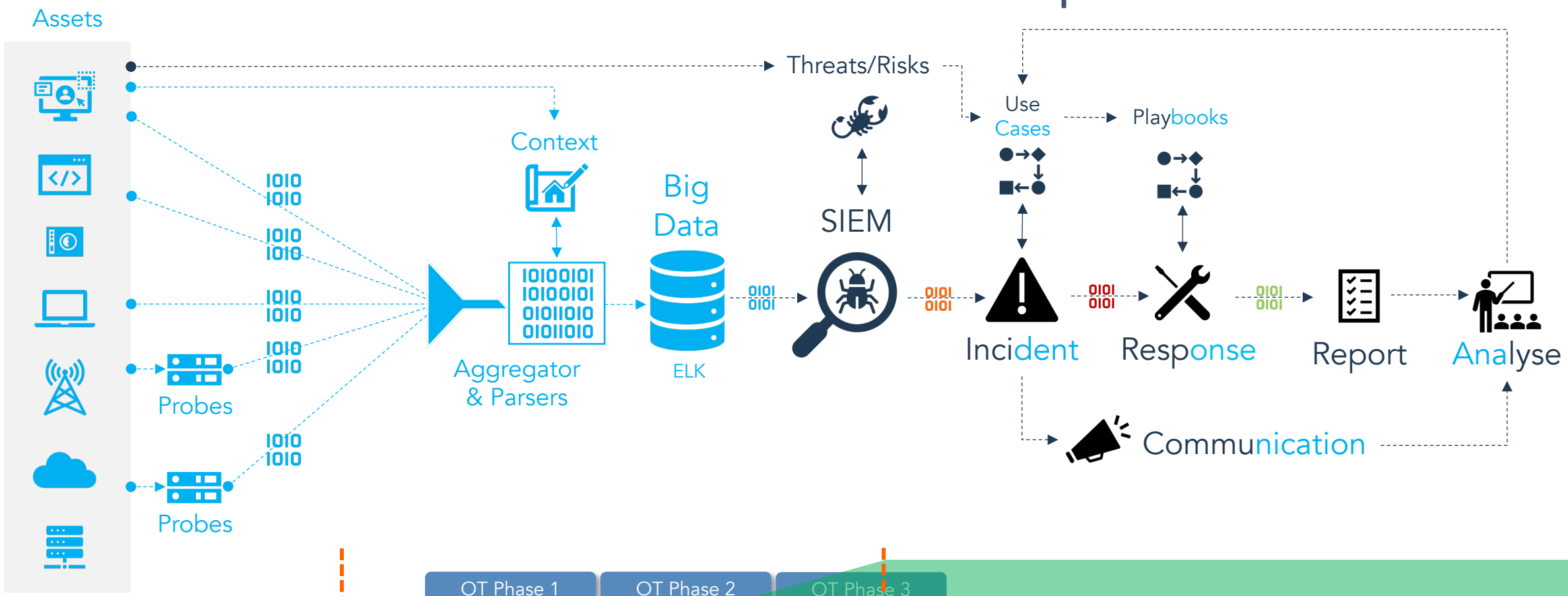


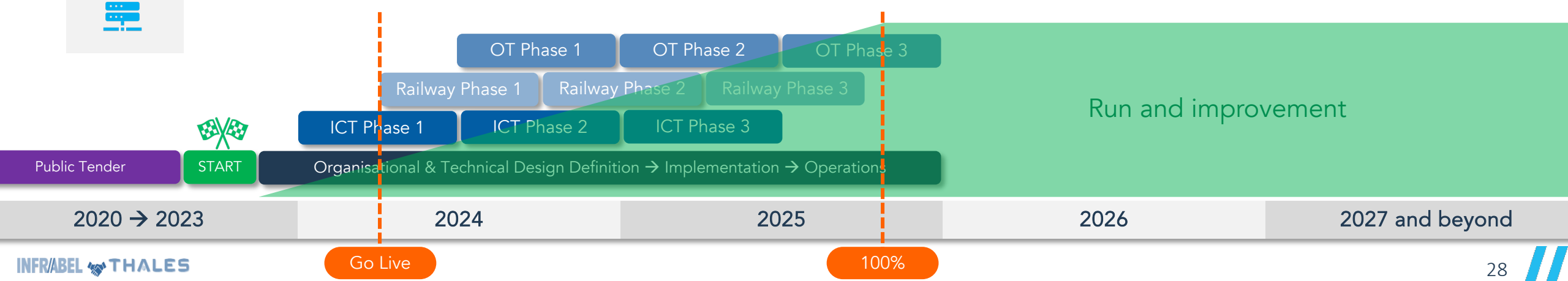
Data Collection for Railway Systems



Use Cases Roadmap

Thales Infrabel





Take Aways

Take Aways

Misunderstanding of CyberSOC	Many think having a CyberSOC means we're completely secure, but that's not true
First Protect Your Castle	While a CyberSOC adds security controls, core assets must be clearly known and maintained to keep them strong
Use Cases & Data are key	Building a CyberSOC on Use Cases and Quality Data is the best strategy to avoid to miss the essential and to control the output
Maintenance and improvement	Even the CyberSOC needs attention. If we don't keep it in good shape, our defenses weaken, and our assets become easy targets

Thank you