Detection/Response solution for railway systems

Fabien Pornet

Technical Manager
Airbus Cybersecurity

Airbus CyberSecurity

Airbus Defence and Space

Connected Intelligence

Airbus CyberSecurity

Detection for railway system: the challenges

1

Continuous monitoring during system operational time

- Intervention level definition
- Incident response strategy
- Need for handover after a fix period

2

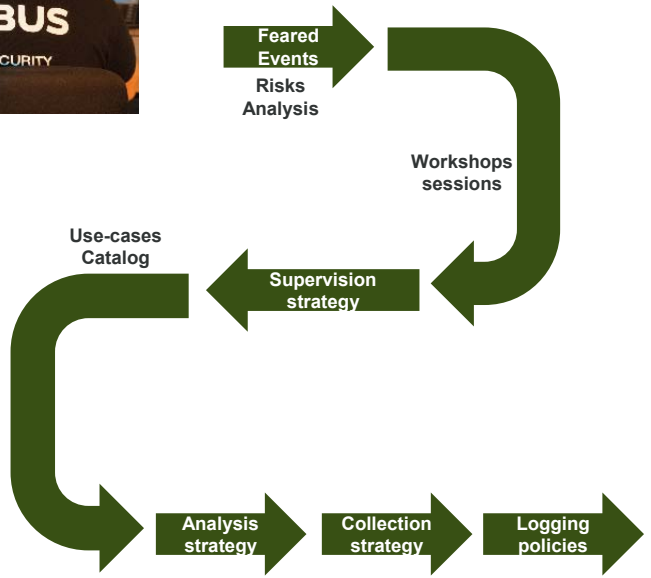
Railway systems not natively in Airbus Portfolio

- Partner identification for Design and Build
- Incremental Integration in sub-systems then global system
- Validation and test

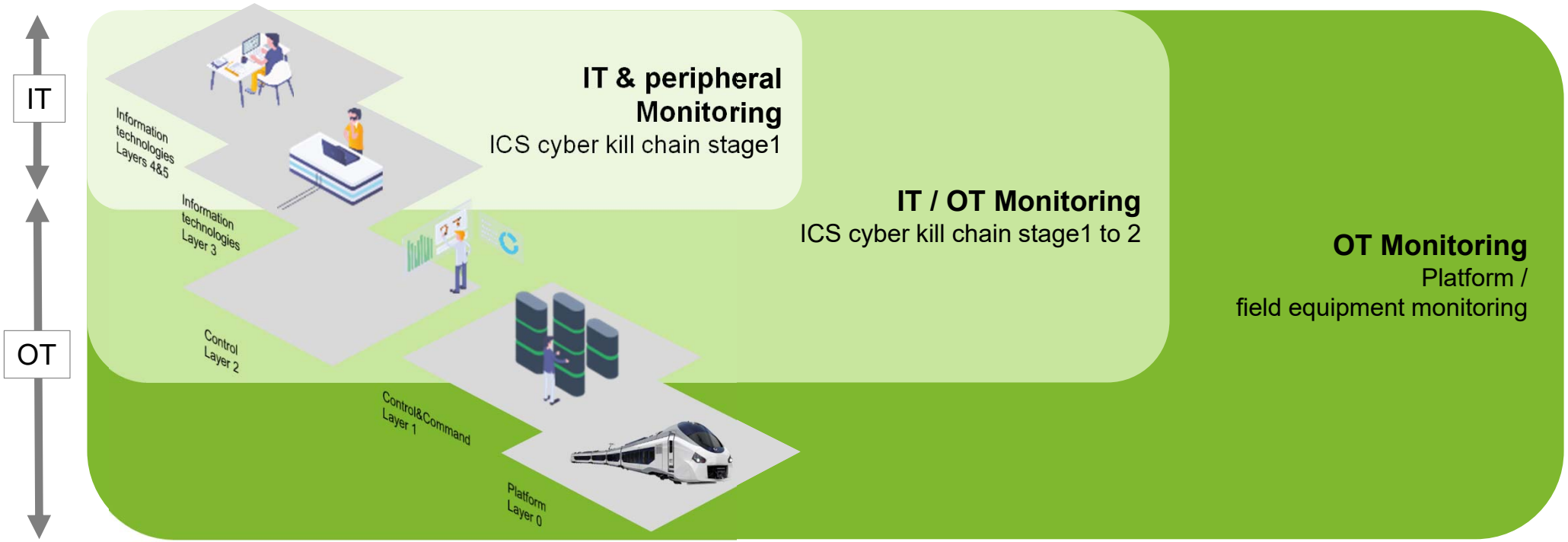
3

Heterogeneity of equipment and logging capabilities

- Identify key assets
- Build relevant use cases



Several supervision strategies



Key feedbacks

1

Foster a step-by-step approach

To master specific railway projects
(very long V-Cycle, risk analysis, vocabulary, sub-system split)

2

Include cybersecurity early in conception

Collection Strategy
Definition of Auditing Policy (Logs)

3

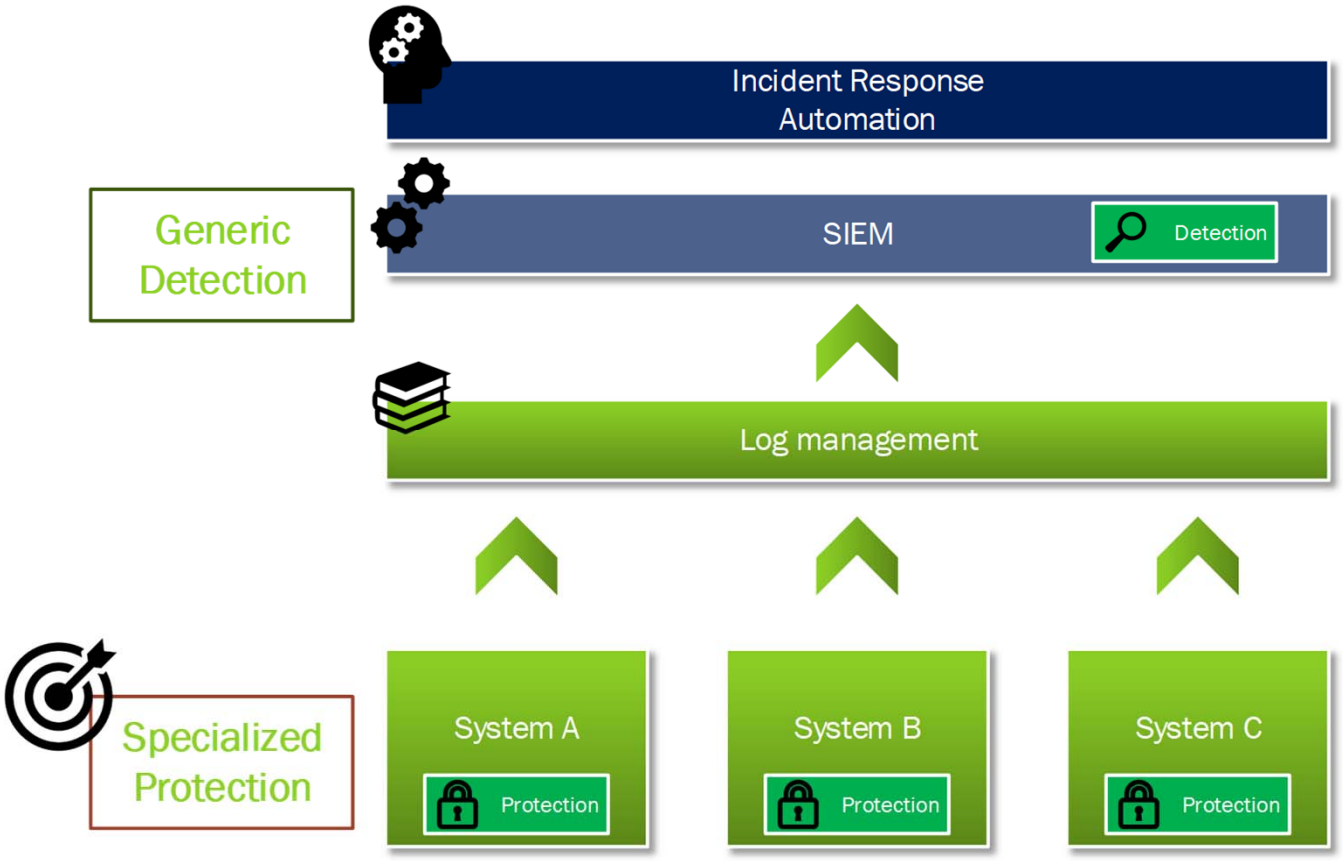
Elaborate a realistic detection strategy

Detailed attack scenarii identification & likelihood
Priorization of asset to secure according to criticity
Extension of Risks scope over time

Current technical detection solution

All SIEM Architecture

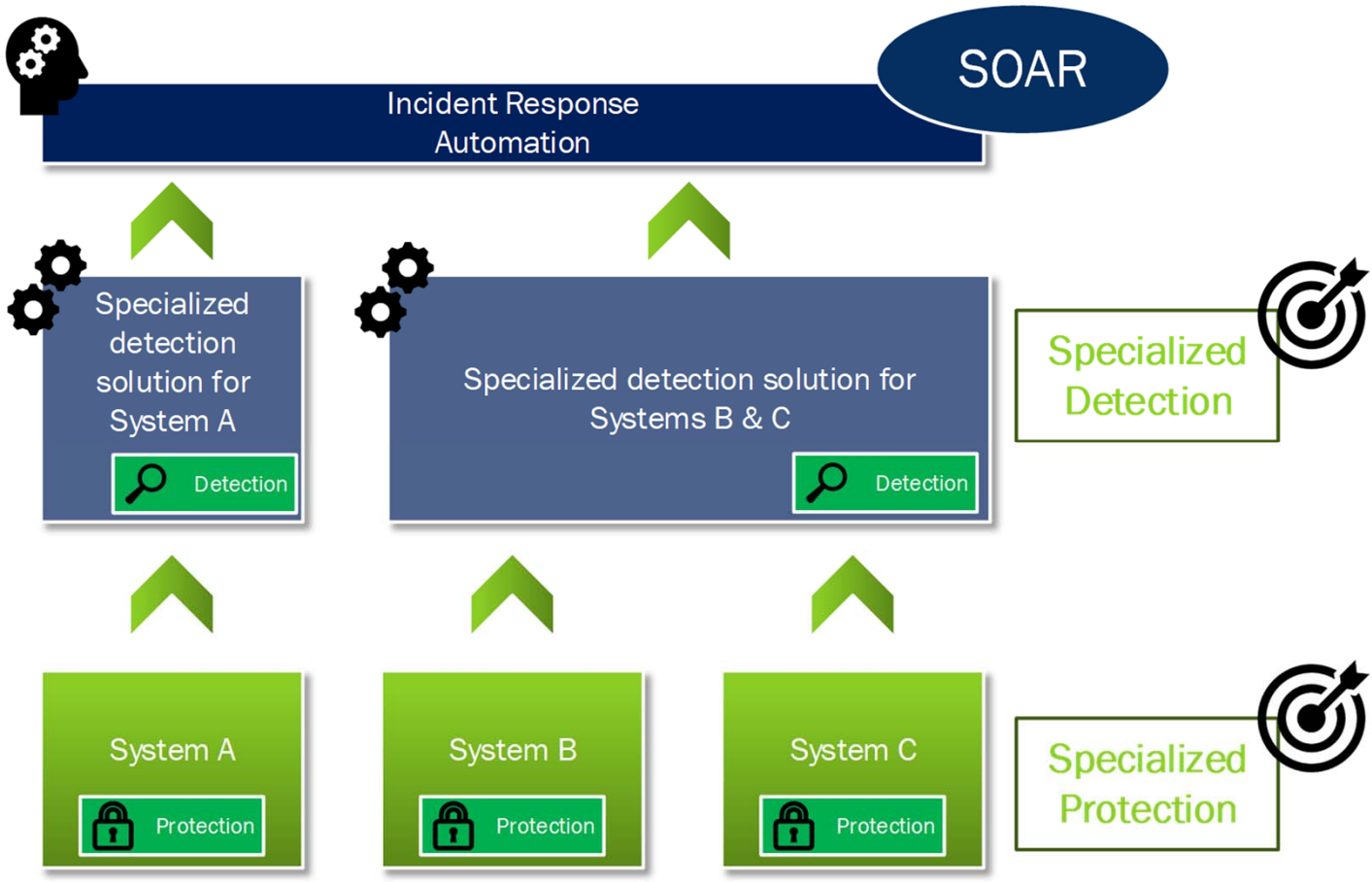
- SIEM agglomerates all logs
- **One tool fit all** systems…
- … so one security team has to master every system
- Usually limited to some systems because of **cost**
  - ➢ Attacks are becoming faster
  - ➢ We need a view on all attack surface…
  - ➢ … at every step of the attack



A new technical paradigm for Detection & Response

SOAR Architecture

- **Specialized** detection
  - Relying on editors' operational knowledge
- SOAR is a **360° Security** view on all IS
- Easier integration of **Remediation** tools
- Increase **Analysts' insight**
- SIEM still a solution along with :
  - EDR
  - NDR
  - DLP
  - Vulnerability management
  - Cloud solutions
  - …




Smart and
Sustainable
Mobility
for all.
its
EUROPEAN
CONGRESS
TOULOUSE
30 May - 1 June 2022

Thank you!