CyberSecurity

Securing Critical Business

# OT SOC Use Case Development – A Specific Example at AIRBUS

IMI, 19th of November 2019

Mirko Haustein & Joerg Schuler

AIRBUS

# An Airbus takes off or lands every 1.4 seconds.

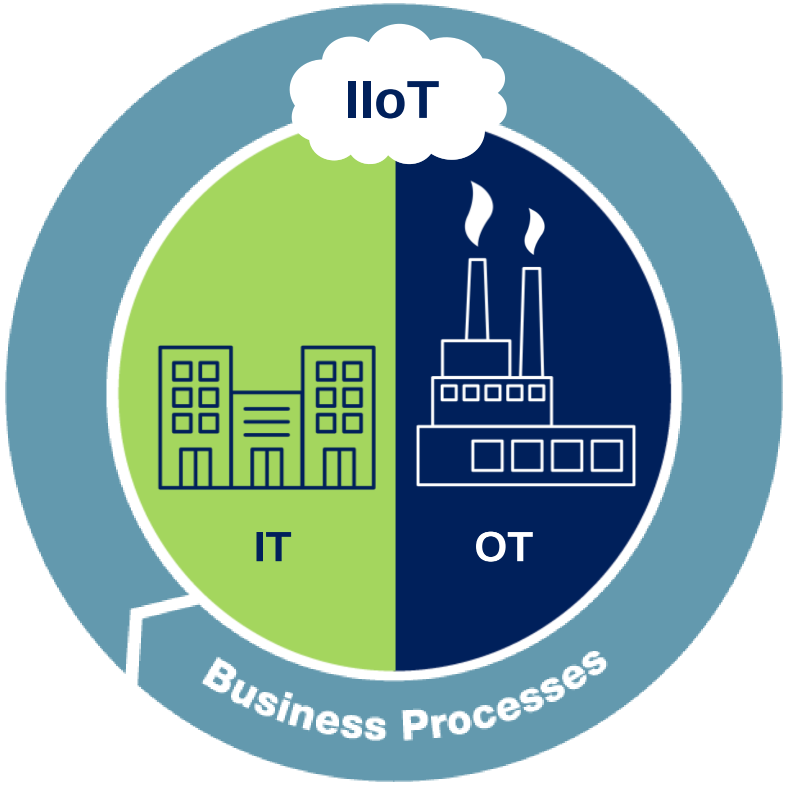
- **19,282**
  Aircraft sold
- **60**
  Produced monthly
- **25,000+**
  Daily flights
- **11,925**
  Delivered
  End March 2019

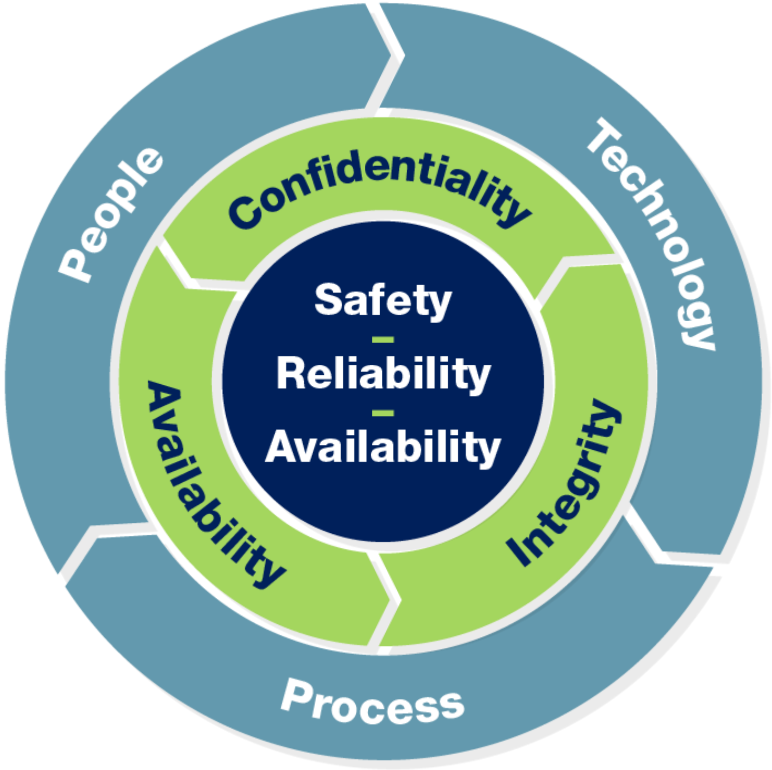
## Industrial Cyber Security

Enables the IT/OT Convergence for Industrial Process Automation @ Shop Floors

# Our Mission: Protecting Critical Industrial Processes

## along the full value chain

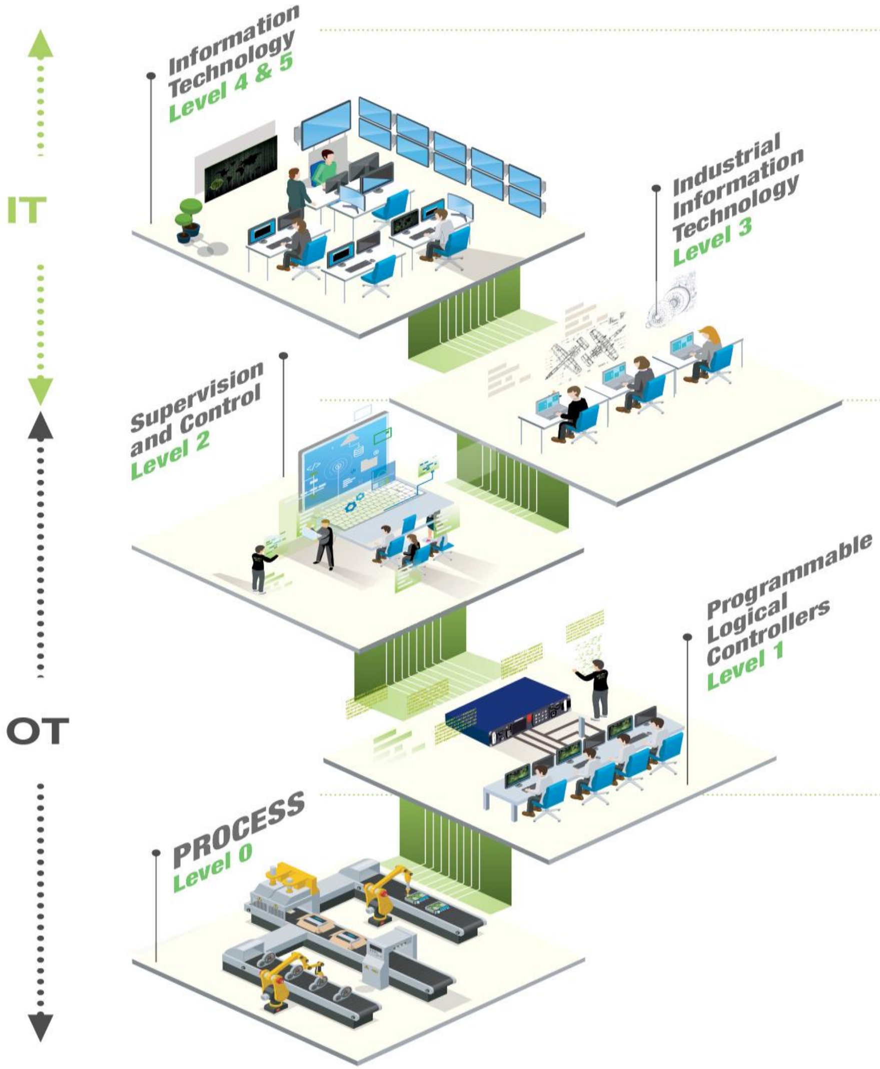




by considering all dimensions!

# Airbus Critical OT/ICS Security Monitoring

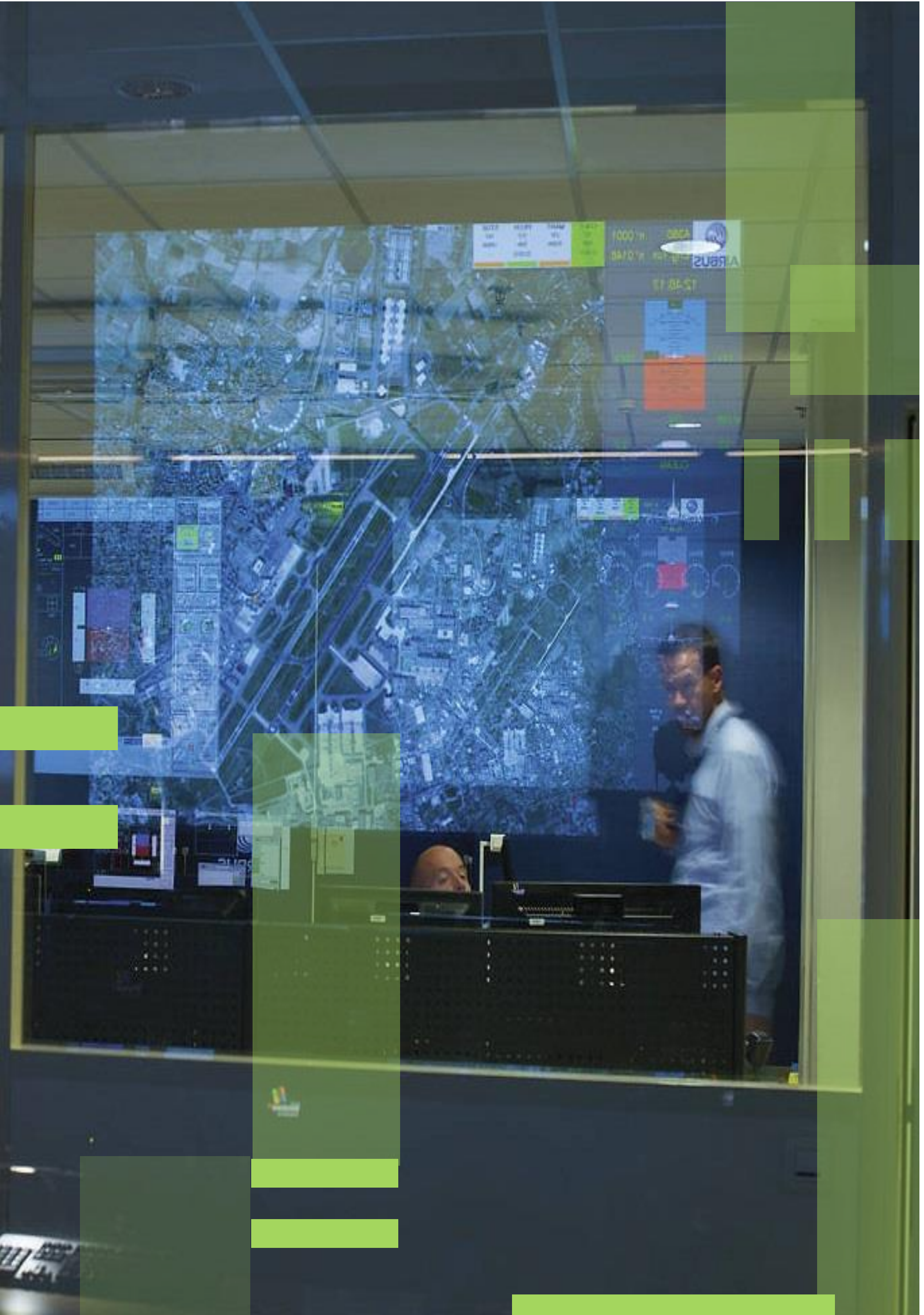
## by extending the SOC to OT


IT
OT
Information Technology Level 4 & 5
Industrial Information Technology Level 3
Supervision and Control Level 2
Programmable Logical Controllers Level 1
PROCESS Level 0

Detection of IT Perimeter

Detection of Industrial Zone

In-depth Detection of Industrial and ICS Zone



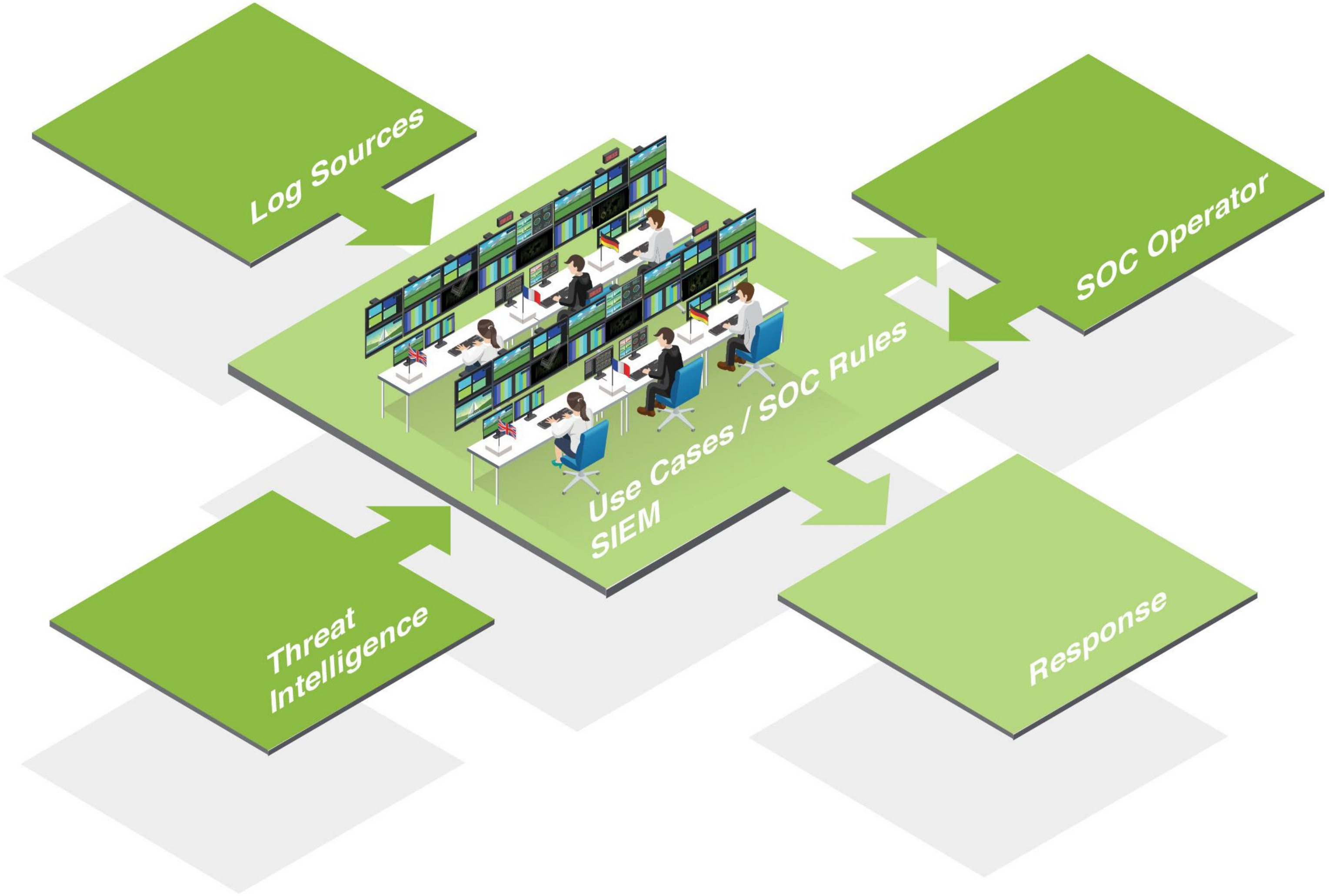
# OT SOC Use Case Development

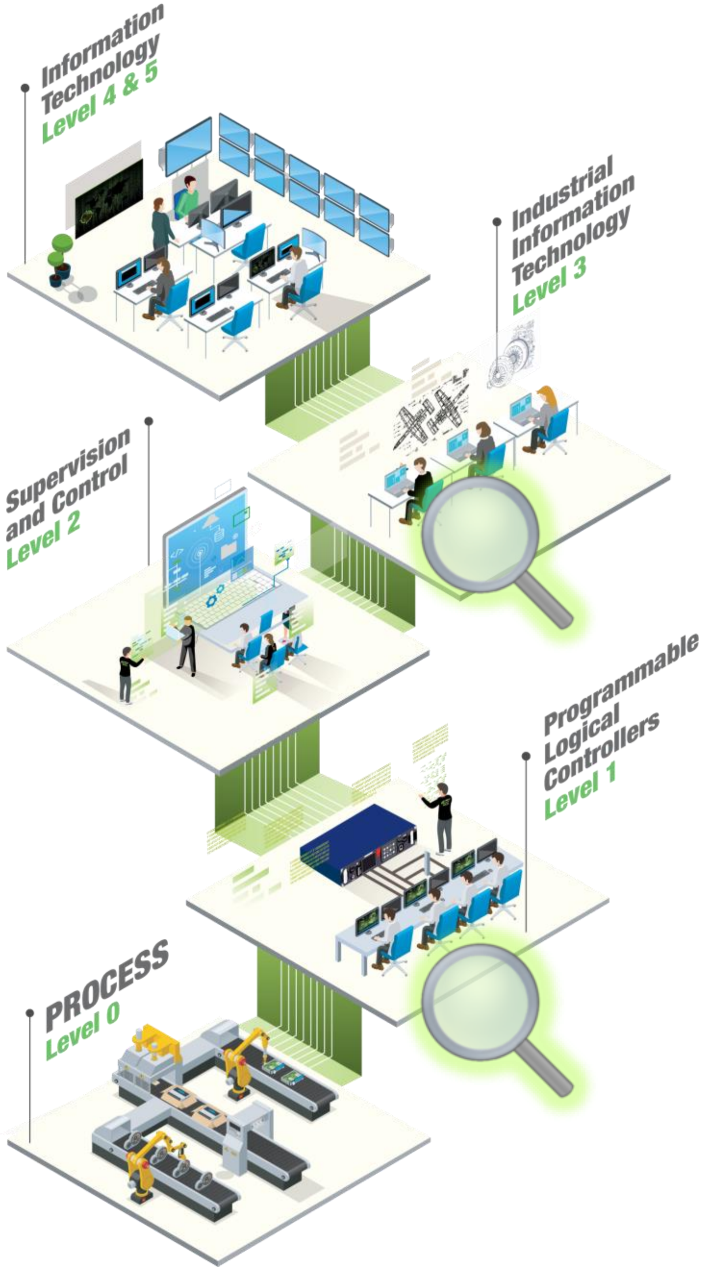
CyberSecurity

# SOC => SOC 4.0

# OT SOC (SOC 4.0)

## The key dimensions for the SOC extension to OT




Information Technology Level 4 & 5
Industrial Information Technology Level 3
Supervision and Control Level 2
Programmable Logical Controllers Level 1
PROCESS Level 0

# OT SOC (SOC 4.0)

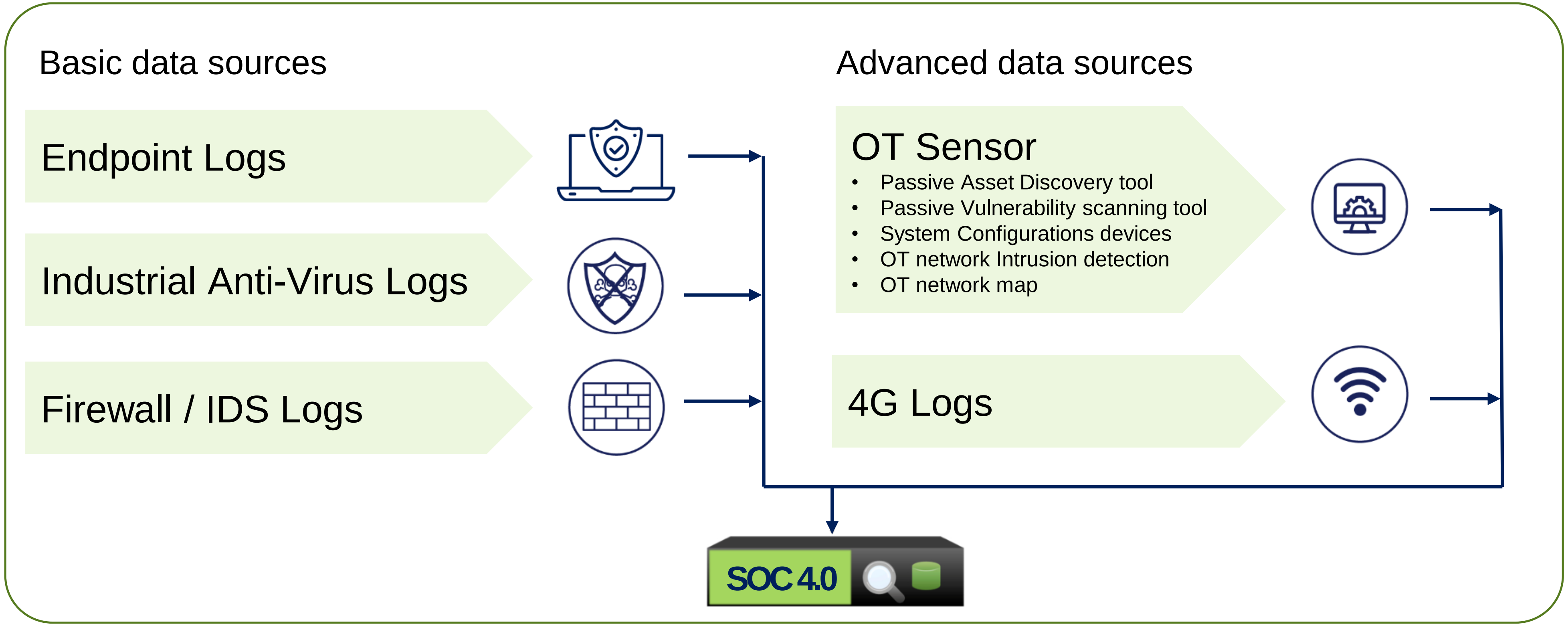
➢ Basic data sources:

- Endpoint Logs
- Industrial Anti-Virus Logs
- Firewall / IDS Logs

➢ Advanced data sources:

- OT Sensor Logs
- 4G Logs

# OT SOC (SOC 4.0)



Basic data sources

Endpoint Logs

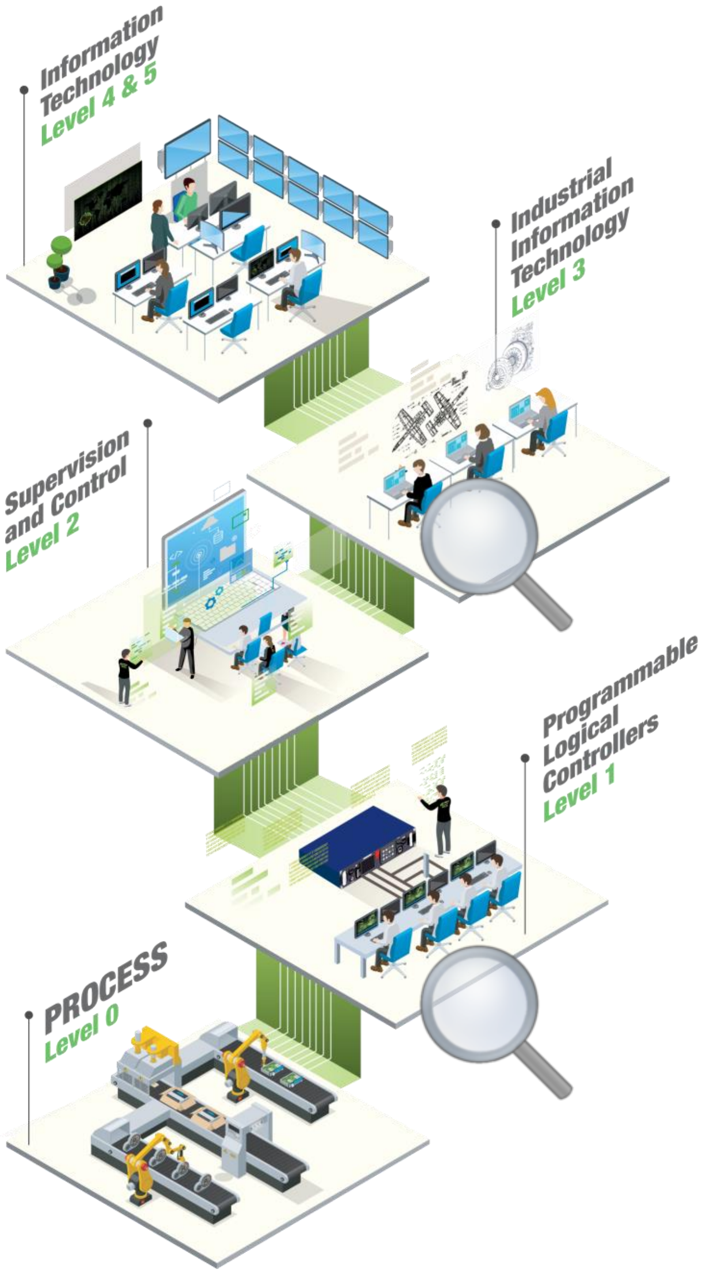
Industrial Anti-Virus Logs

Firewall / IDS Logs

Advanced data sources

OT Sensor
- Passive Asset Discovery tool
- Passive Vulnerability scanning tool
- System Configurations devices
- OT network Intrusion detection
- OT network map

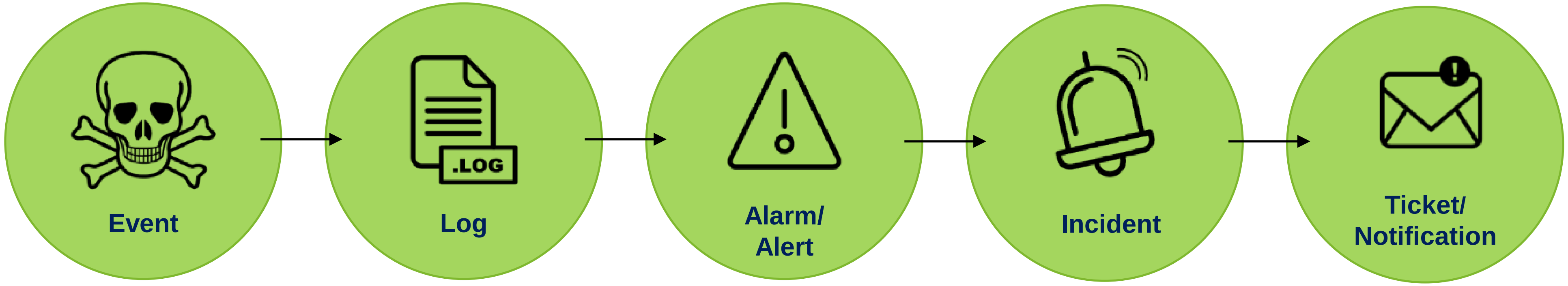
4G Logs


Information Technology Level 4 & 5
Industrial Information Technology Level 3
Supervision and Control Level 2
Programmable Logical Controllers Level 1
PROCESS Level 0

# OT SOC (SOC 4.0)

- ➢ Infrastructure for log collection required
- ➢ Involvement of machine owners necessary
- ➢ Specialised OT incident response process

# OT SOC Use Case



Event

Log

Alarm/
Alert

Incident

Ticket/
Notification

“Something
Happened”

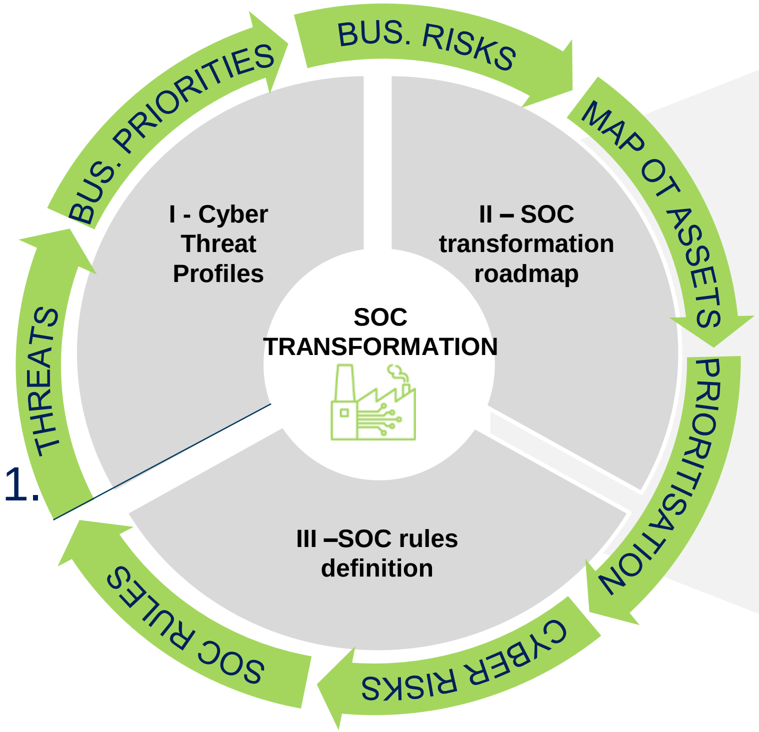
“We saw
something
Happening”

“We *think* we
have seen
something bad”

“We *know* this is
a bad thing”

“We have found this…
and here is how to
solve it”

# OT SOC Use Case Development



1 THREAT PROFILE

2 BUSINESS PRIORITIES

3 BUSINESS RISKS ASSESSMENT

4 MAPPING WITH OT ASSETS

5 PRIORITISATION

6 CYBER RISKS ASSESSMENT

7 SOC RULES

FROM BUSINESS UNDERSTANDING…

… TO CYBER RISKS MANAGEMENT

# OT SOC Use Case Development – Example

| MITRE ID | MITRE Technique | Use Case Title | Log Sources | SOC CIM |
|---|---|---|---|---|
| T1046 | Network Service Scanning | Port Scanning | Network IDS, OT-Specific Network Sensors | Intrusion Detection |
| T1078 | Valid Accounts | Default Credential Logon | Application, OT-Specific Network Sensors | Authentication |
| T1082 | System Information Discovery | OT System Discovery | OT-Specific Network Sensors | Intrusion Detection |
| T1109 | Component Firmware | Modification in Logic of Controllers | MES Server, Application, OT-Specific Network Sensors | Change |
| T1110 | Brute Force | Brute Force attempt detected | Windows, Application / Appliance | Authentication |
| T1133 | External Remote Services | Unknown Remote Maintenance Connection | Remote Maintenance Solution | Network Sessions |
| T1204 | User Execution | Malware on Endpoint | AntiVirus Application | Malware |

# OT SOC Use Case Development – Example

| MITRE ID | MITRE Technique | Use Case Title | Log Sources | SOC CIM |
|---|---|---|---|---|
| T1046 | Network Service Scanning | Port Scanning | Network IDS, OT-Specific Network Sensors | Intrusion Detection |
| T1078 | Valid Accounts | Default Credential Logon | Application, OT-Specific Network Sensors | Authentication |
| T1082 | System Information Discovery | OT System Discovery | OT-Specific Network Sensors | Intrusion Detection |
| T1109 | Component Firmware | Modification in Logic of Controllers | MES Server, Application, OT-Specific Network Sensors | Change |
| T1110 | Brute Force | Brute Force attempt detected | Windows, Application / Appliance | Authentication |
| T1133 | External Remote Services | Unknown Remote Maintenance Connection | Remote Maintenance Solution | Network Sessions |
| T1204 | User Execution | Malware on Endpoint | AntiVirus Application | Malware |

# OT SOC Use Case Development – Example

**MITRE Technique: T1046 – Network Service Scanning** (https://attack.mitre.org/techniques/T1046/)

**Description:** Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

**MITRE Tactic:** Discovery

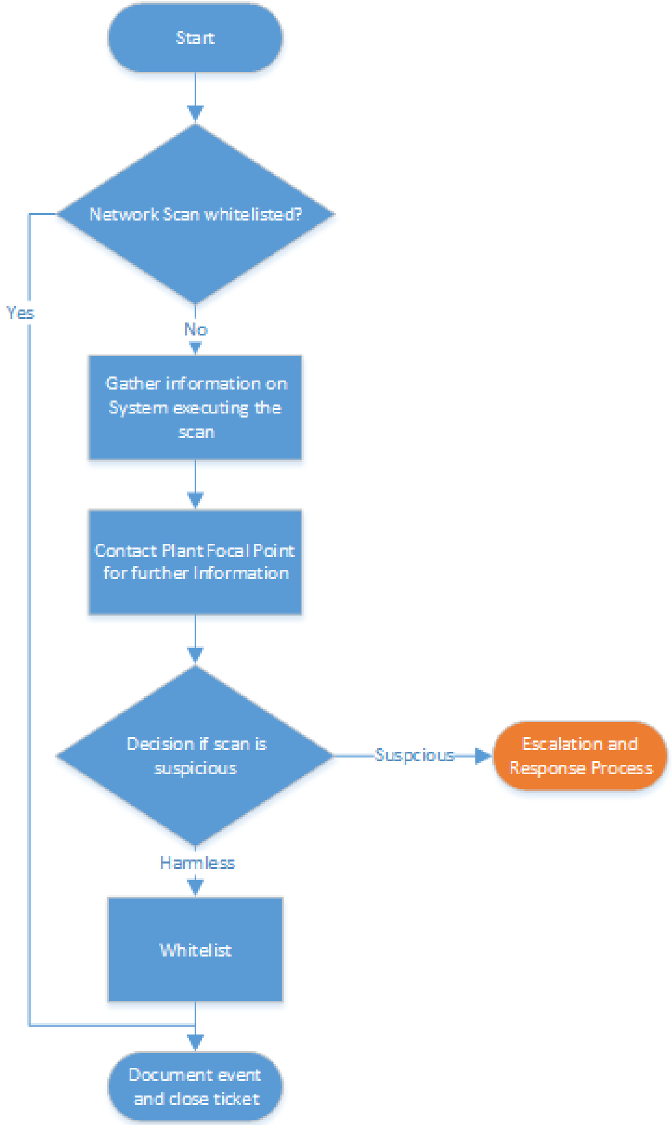
**Criticality:** Medium

**Detection:** Alerts by Network IDS and firewalls

**Business Risk:** Discovery of vulnerabilities via network reconnaissance

**Constraints:**

- Maintenance tasks that might trigger False-Positives are not synchronized with IT CAB and executed by non-IT staff or external suppliers
- Enclave structure limits investigation possibilities


Start
Network Scan whitelisted?
Yes
No
Gather information on System executing the scan
Contact Plant Focal Point for further Information
Decision if scan is suspicious
Suspcious
Escalation and Response Process
Harmless
Whitelist
Document event and close ticket

# Conclusion

## for an efficient OT SOC Use Case Development

01 Understand assets, risks and get relevant data

02 Create the right use cases (people, process, technology)

03 Manage & improve

# CyberResilience for Tomorrow

## Enabling IT/OT Convergence for industrial processes with an holistic and sustainable approach

**Want to find out more?**

www.airbus-cyber-security.com

contact.cybersecurity@airbus.com