The Missing Ingredient

Importance of combining aviation business intelligence with cyber intelligence via the case study of Aviation SOC

6th of December 2018

Murtaza Nisar, SITA Cybersecurity Lead - Americas

SITA

OUR “2018 CYBERSECURITY INSIGHTS REPORT”

SITA

2018 AIR TRANSPORT CYBERSECURITY INSIGHTS

OF CYBERSECURITY BUT EXISTING

ed to grow and spending is evention.

but Cybersecurity teams d positioning at C-level.

SITA RECOMMENDATIONS

Air transport industry stakeholders must empower their Cybersecurity teams and provide necessary resources to initiate concrete and actionable

CYBERSECURITY | Cyber Spend & Challenges

CYBERSECURITY BUDGETS ARE GROWING AND IS SHIFTING TOW DETECTION AND PREVENTION

% of IT budget spent on Cybersecurity

© SITA 2018 Air Transport CYBERSECURITY INSIGHTS

investments during the past three years. Security spending is expected to shift towards detection and response in the coming years.

EMPLOYEE AWARENESS IS CONSIDERED THE MOST IMPORTANT COMPONENT IN THE DEFENCE AGAINST CYBER RISK

No. 1 investment priority

Employee awareness & training 76%

% of respondents who communicate their Security Policies to employees

% of respondents with a formal Cybersecurity training program for employees

SITA

ANALYSIS

Employees are the weakest link in the fight against cyber attacks, and the very first topic to address. Air transport industry security experts accept that employees need to be part of their core security arsenal in the defence against risk.

SITA's Air Transport Cybersecurity Insights survey shows that 'Employee awareness & training' is the number one priority for Cyber-security (76%).

With Ransomware and Phishing at the top of the risk agenda, it is good to see such a high proportion of organizations placing employees at the top of Cybersecurity best practice. Over three quarters (77%) of aviation organizations communicate their security policies to their employees, while 69% have a formal training program in place.

© SITA 2018 Air Transport CYBERSECURITY INSIGHTS

SITA CyberSecurity survey 2018

- Most comprehensive study investigating Cybersecurity trends within the air transport industry
- Answers from 59 senior decision makers at major airlines & airports globally (CEO, CIO, CISO, etc.)

KEY OUTPUTS

- High Awareness of the importance of CyberSecurity but **existing challenges are delaying progress**
- Majority of Airlines & Airports have put core safeguards in place and **are ready to advance to the next level**
- Leading CyberSecurity driver is shifting from compliance to **proactive protection with focus on detection** of external threats and prevention of disruption
- **One in two organizations will implement a “Security Operation Center”** in the next 3 years to ramp up protection

Available here: https://www.sita.aero/resources/type/surveys-reports/air-transport-cybersecurity-insights-2018

AIRPORT CYBERSECURITY CHALLENGES

PEOPLE & GOVERNANCE

- Limited tone from the top/ Reactive vs proactive/ No Chief Information Security Officer
- Insufficient budget/competing priorities
- Lack of ATI-specific knowledge within security vendors

PROCESS

- Limited understanding of business impact
- Lack of asset visibility & difficulties to define the asset criticality
- Extensive and complex supply chain involving several different stakeholders

TECHNOLOGIES

- Complex and evolving technology landscape
- IT/OT convergence, physically accessible to 1,000's of people
- Growing threats targeting Airports

SITA CyberSecurity **INSIGHT**

Key CyberSecurity implementation challenges in the ATI

1. Limited resources, budget & staff training
2. Visibility of IT Assets & Data Protection
3. Securing Cloud usage & Operational technologies

Source: SITA CyberSecurity survey (2018)

What is a SOC?

A security operations center (SOC) is a facility that houses a cyber security team responsible for monitoring and analyzing an organization’s security posture and responding to incidents on an ongoing basis.

TRIVIA QUESTION

What is the number of days from first evidence of compromise that an attacker is present before detection i.e. Dwell Time

A. 5
B. 32
C. 66
D. 101

101

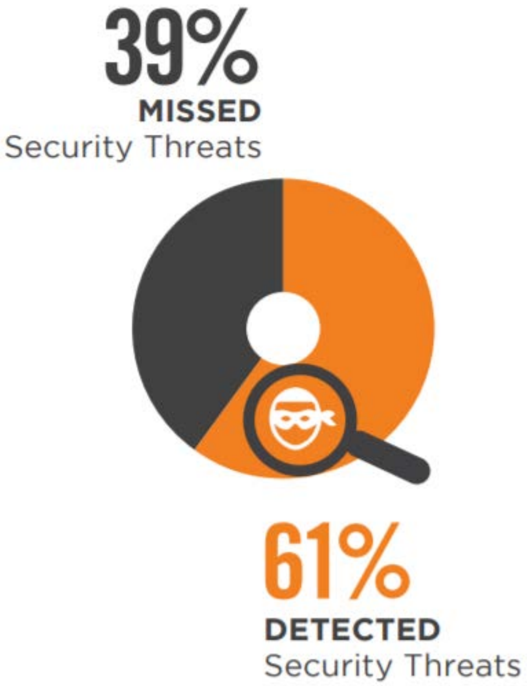
DAYS

Source: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

TRIVIA QUESTION

On average, what is the percentage of threats missed by a SOC

A. 4%
B. 10%
C. 39%
D. 65%



Source: https://www.alertlogic.com/assets/industry-reports/2018-Threat-Hunting-Report-Alert-Logic.pdf

AIRPORT SECURITY OPERATIONS CENTER CHALLENGES

GAP IN DETECTON COVERAGE

MISALIGNEMENT WITH BUSINESS RISKS, INFORMATION SYSTEMS IN PLACE & SCOPE TO COVER

"I am **not aware** of what my **SOC is covering**"

LACK OF DETECTION EFFICIENCY

A LOT OF FALSE POSITIVE, WITH NO CONTEXTUALIZATION INFORMATION

"My current SOC **generates 1 000 alerts a day**"

DIFFICULTIES IN ALERTS PRIORITIZATION

HIGH WORKLOAD TO PROPERLY A SECURITY INCIDENT, DEFINE A SEVERITY AND ASSIGN TICKETS

"I have **too many alerts** that I **don't know which are real incidents"**

37% of SOC teams faced more than 1,000 daily alerts, with **52% of them being false positives**
Ponemon Institute, 2016

SITA CyberSecurity **INSIGHT**

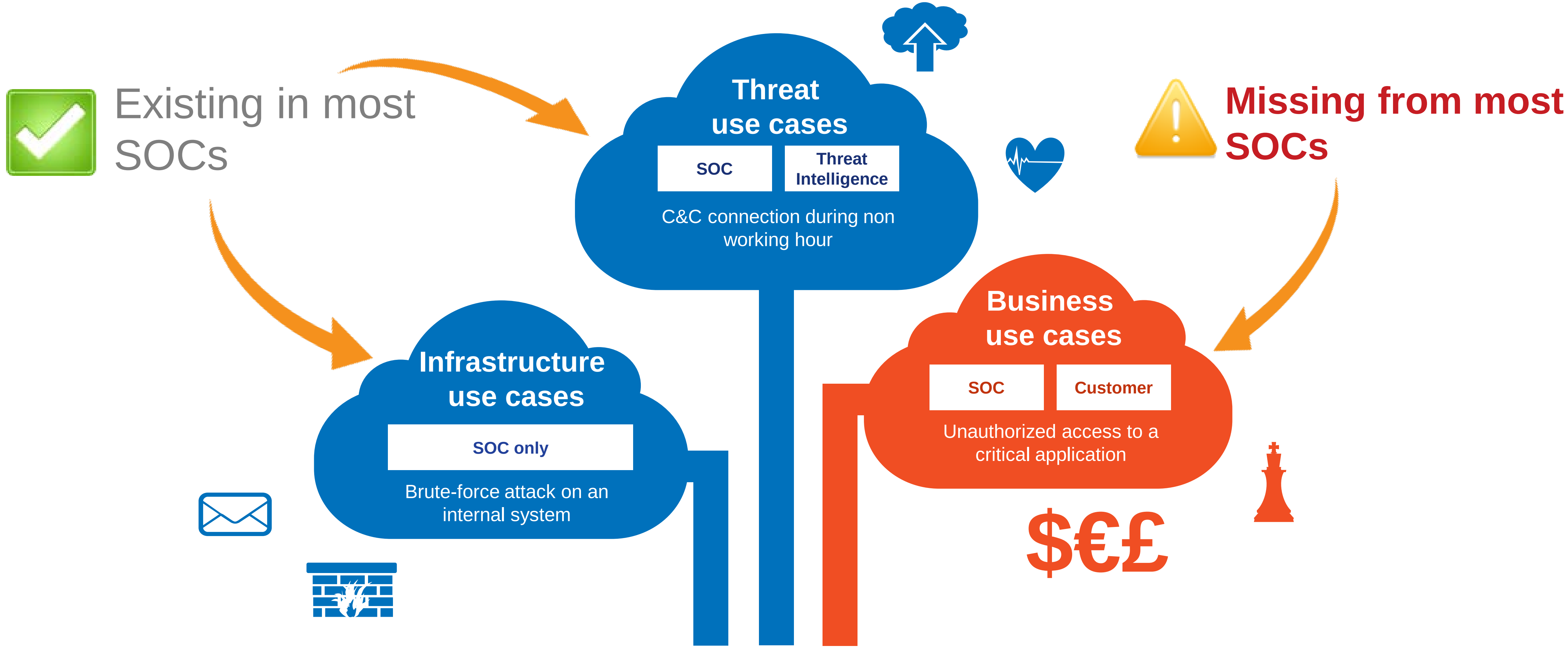
DO YOU HAVE A SOC IMPLEMENTED?

7%	*Yes, fully managed in-house*
26%	*Yes, outsourced*
47%	*Plan to have one by end of 2021*
21%	*No and no plan*

Source: SITA CyberSecurity survey (2018)

SITA

Business contextualization - The missing ingredient



Existing in most SOCs

Missing from most SOCs

Threat use cases

SOC	Threat Intelligence

C&C connection during non working hour

Infrastructure use cases

SOC only

Brute-force attack on an internal system

Business use cases

SOC	Customer

Unauthorized access to a critical application

The SOC must be able to **detect all these use cases**

The main challenge for SOCs is to know how to build business use cases

RETURN OF EXPERIENCE ON 4 EUROPEAN AIRPORTS

CONTEXT

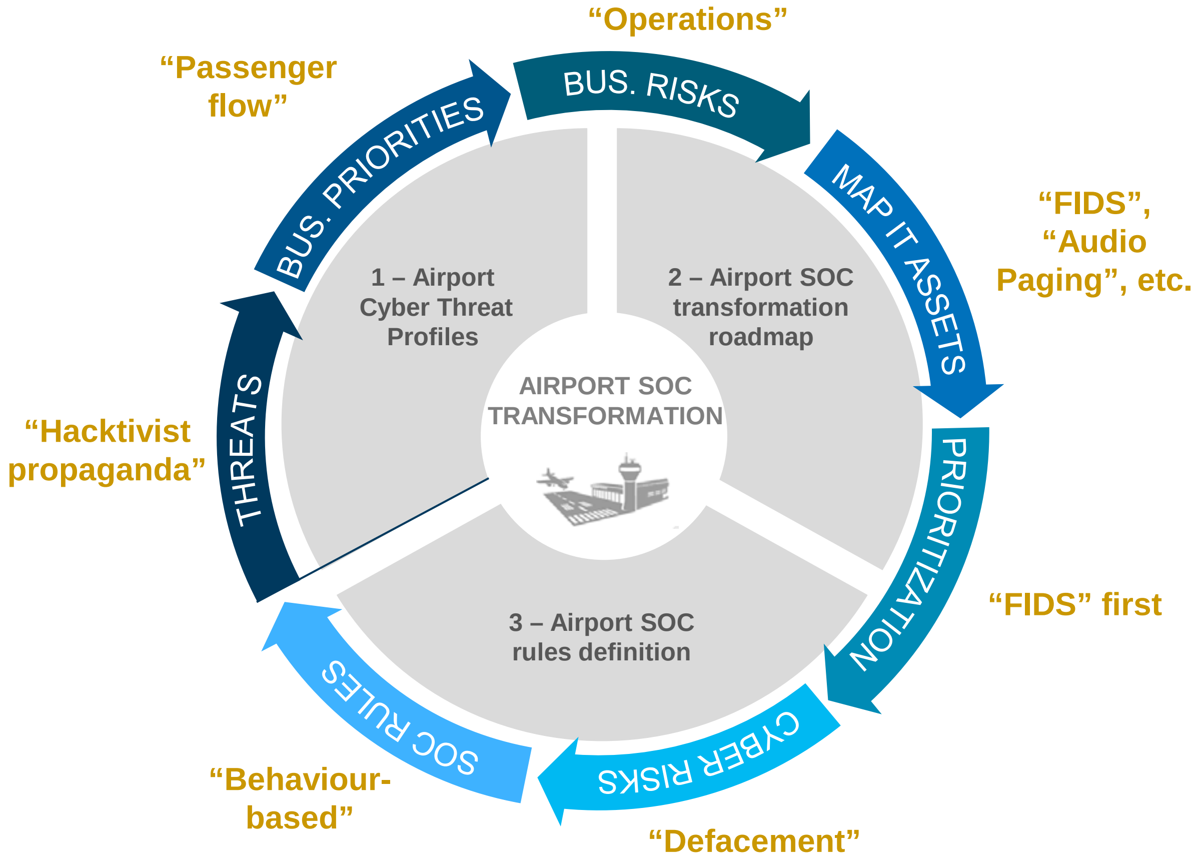
SCOPE: Design, build and run of 24/7 SOC services for 3 years, covering 850 devices and 4000 EPS

KEY DRIVERS

- 24/7 service delivered by SOC provider with proven expertise and experience
- SIEM technology licenses and maintenance
- Advanced detection (use cases) and threat intelligence
- Incident management and customised reporting
- Cyber On-demand Service (Catalogue)
- Provider with capability to deliver future requirements
- **Strong ROI**

RETURN OF EXPERIENCE ON 4 EUROPEAN AIRPORTS

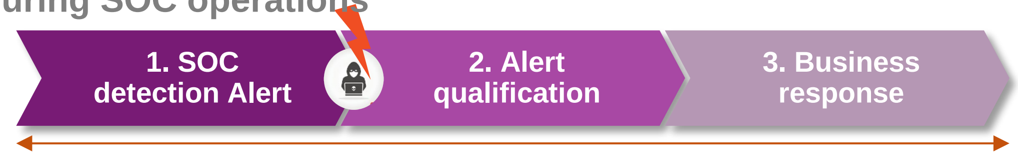
ENSURE A DETECTION ALIGNED WITH BUSINESS



FROM BUSINESS UNDERSTANDING…

… TO CYBER RISKS MANAGEMENT

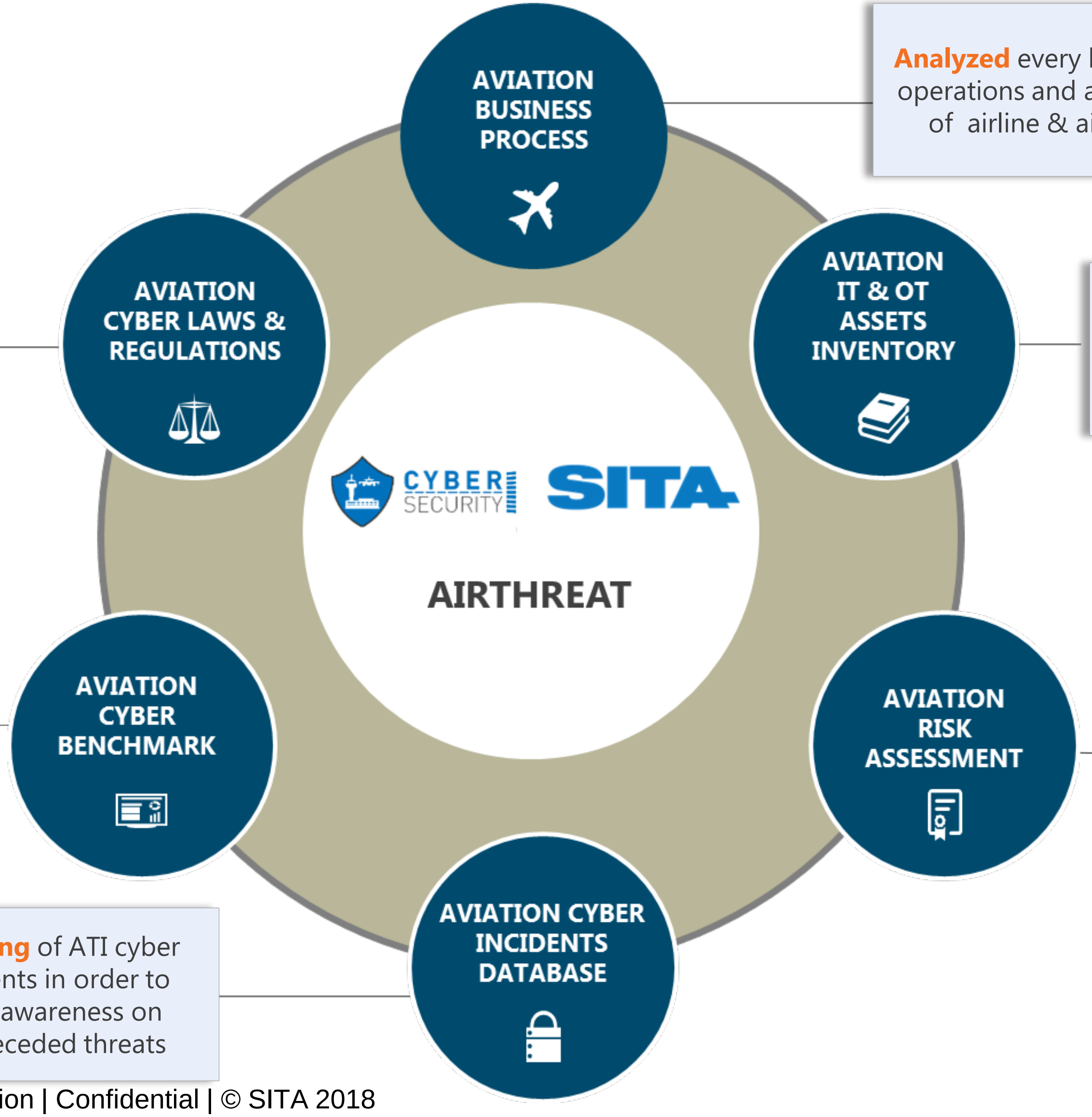
During SOC operations



BUSINESS CONTEXT OF THE ALERT

Our Aviation-Specific Approach and tools

We concentrated **70 years** of business expertise into one single Aviation specific cyber security **toolkit**.



CYBER SECURITY
SITA
AIRTHREAT
AVIATION BUSINESS PROCESS
AVIATION IT & OT ASSETS INVENTORY
AVIATION RISK ASSESSMENT
AVIATION CYBER INCIDENTS DATABASE
AVIATION CYBER BENCHMARK
AVIATION CYBER LAWS & REGULATIONS

Analyzed every business operations and activities of airline & airport

Listed all IT & OT assets of airlines & airports

Audited every IT & OT assets and generated risk assessments

Tracking of ATI cyber incidents in order to raise awareness on unpreceded threats

Creating an aviation cyber specific survey

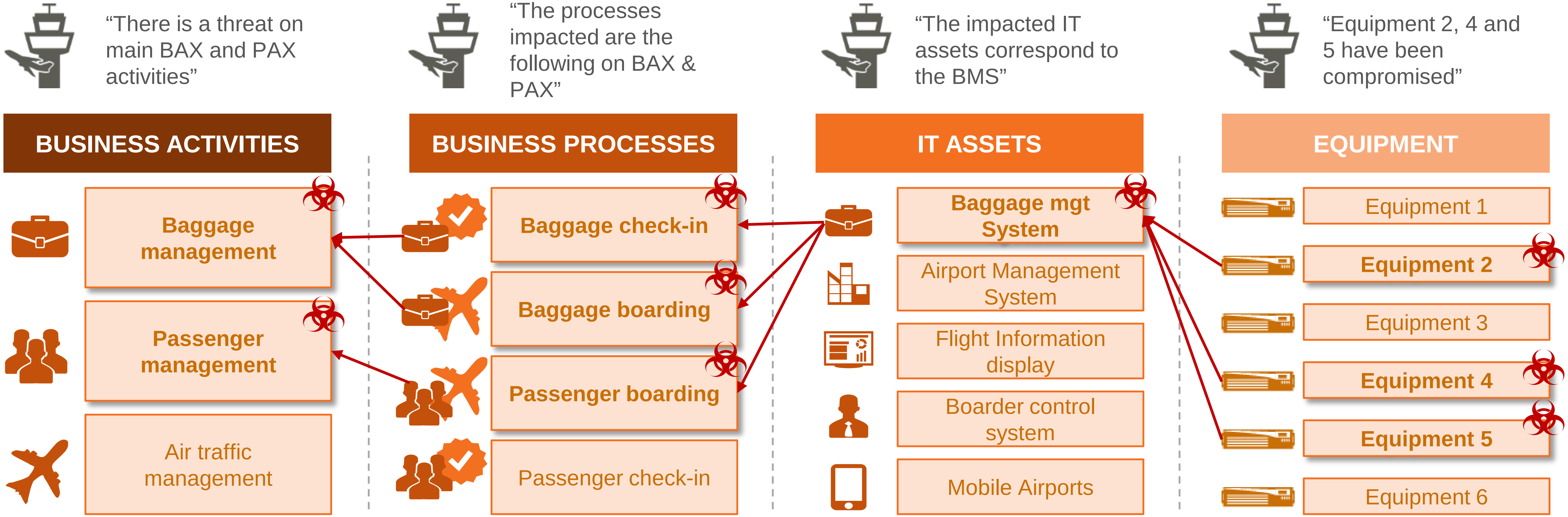
Mapped every cyber & aviation specific regulations and standards

Example: Aviation SOC

A Detection service Tailored to the Aviation industry

Detection of servers compromised

Ex. "Wannacry" ransomware attack



"There is a threat on main BAX and PAX activities"

"The processes impacted are the following on BAX & PAX"

"The impacted IT assets correspond to the BMS"

"Equipment 2, 4 and 5 have been compromised"

BUSINESS ACTIVITIES

- **Baggage management**
- **Passenger management**
- Air traffic management

BUSINESS PROCESSES

- **Baggage check-in**
- **Baggage boarding**
- **Passenger boarding**
- Passenger check-in

IT ASSETS

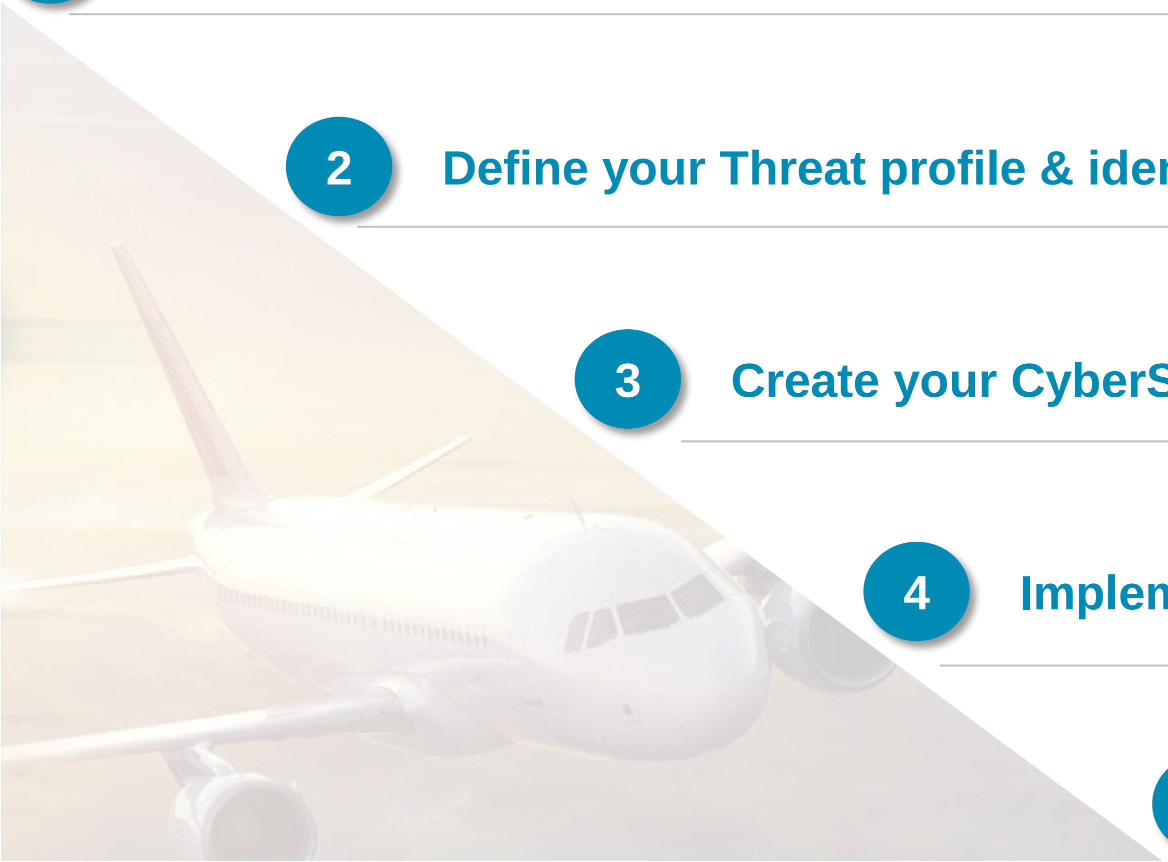
- **Baggage mgt System**
- Airport Management System
- Flight Information display
- Boarder control system
- Mobile Airports

EQUIPMENT

- Equipment 1
- **Equipment 2**
- Equipment 3
- **Equipment 4**
- **Equipment 5**
- Equipment 6

OUR RECOMMENDATIONS FOR AIRPORTS

WHERE TO START?



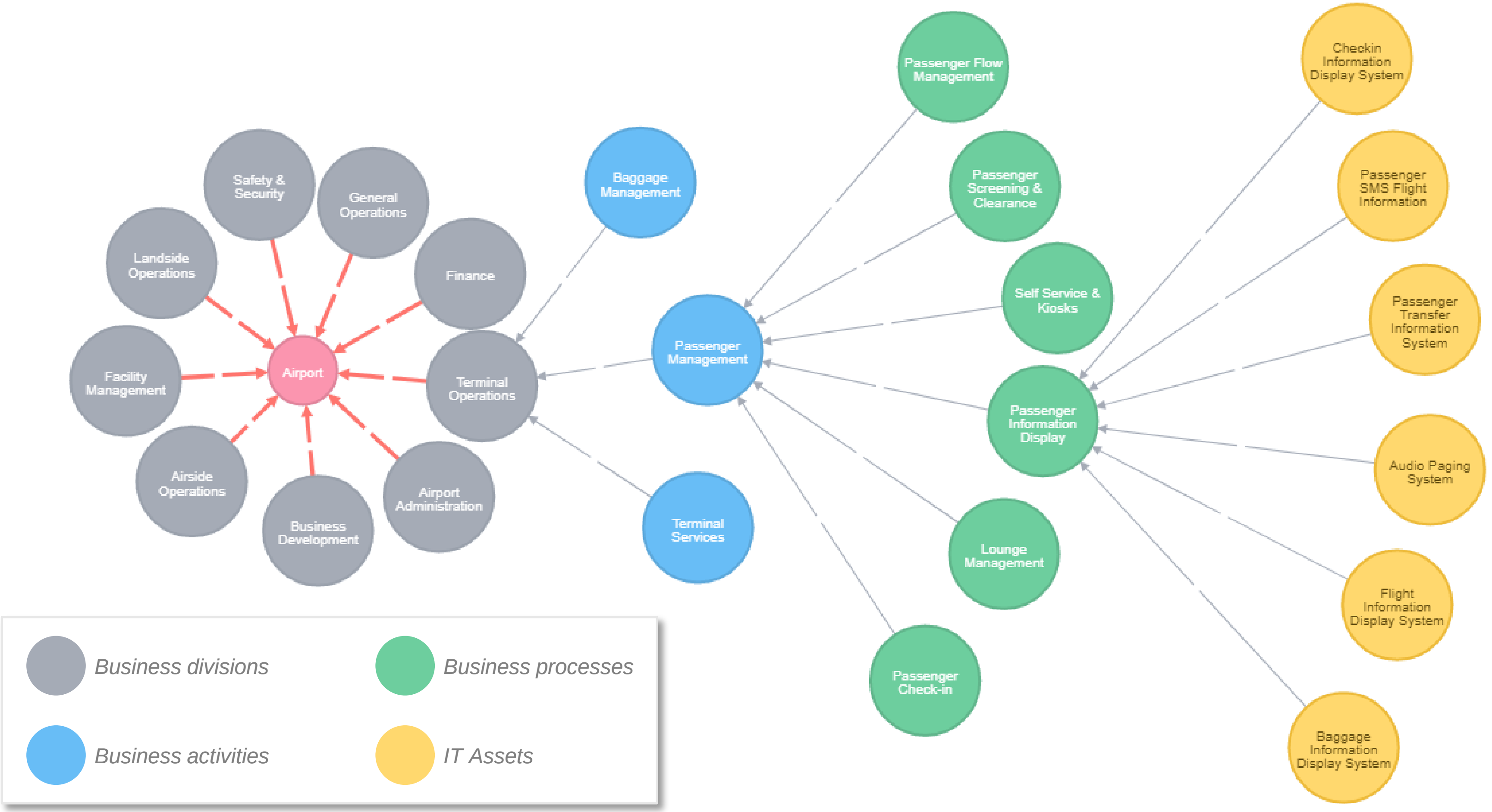
1. **Onboard your management by defining a CyberSecurity Sponsor**
2. **Define your Threat profile & identify your critical activities and assets**
3. **Create your CyberSecurity Program with a 3 to 5 years roadmap**
4. **Implement the CyberSecurity foundations**
5. **Report & communicate key improvements**

Our Aviation-Specific Approach

Illustration: Aviation business processes ↔ IT Assets

SITA CyberSecurity **AVIATION CONTEXT**

BUSINESS ACTIVITIES ←→ **IT ASSETS**



MORE THAN 240 IT ASSETS IDENTIFIED FOR AIRPORTS

For each of them, we identified the following information:

- **Business impact levels** *(safety, operations, financials, reputations and legal)*
- **Business activities impacted** *(flight departure, police operations, passenger check-in, etc.)*
- **Cyber criteria to handle** *(confidentiality, availability or integrity)*
- **Potential interconnections with other IT Assets**
- Other information: providers, reports / standards in the industry, etc.