Security of Mission Critical Network & evolution of the European cyber security landscape

PSCE 2019 – Lancaster UK

DEFENCE AND SPACE

Christophe Calvez – Head of Security - Airbus DS SLC - v1

AIRBUS

Introduction

Mastering collaboration solutions for critical communications.

- Secure Land Communications (SLC), a business unit of Airbus, offers advanced communication and collaboration solutions for Public Safety, Defence and Transport, Utility and Industry (TUI).

- The portfolio, based on TETRA, Tetrapol and LTE technologies, includes infrastructures, devices, professional apps and associated services.

AIRBUS

Agenda

Mission Critical Networks security

- TETRA overview / reminder
- Security of the Mission Critical Service

Evolution of the threat landscape

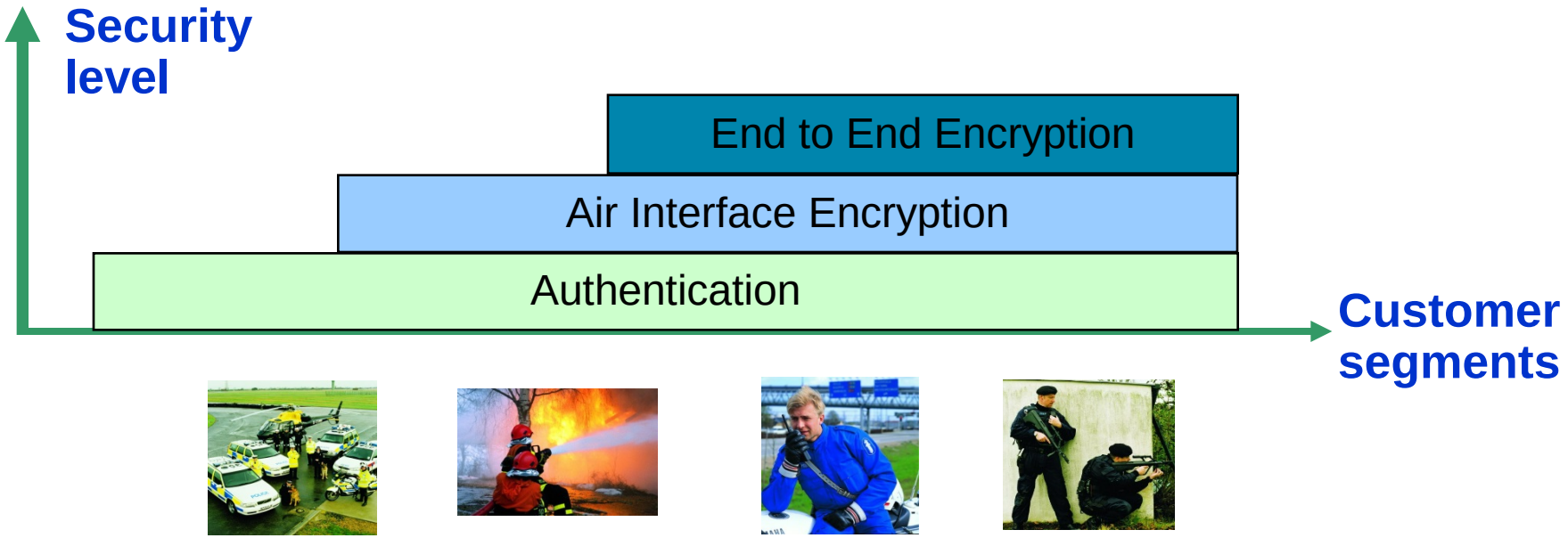
Security policy and risk management

New legislation Framework

TETRA security

AIRBUS

Overview - TETRA Security features



- TETRA security features are modular to fulfil the requirements of different customer segments.
- Specified in EN-300-392-7 and TCCA SFPG

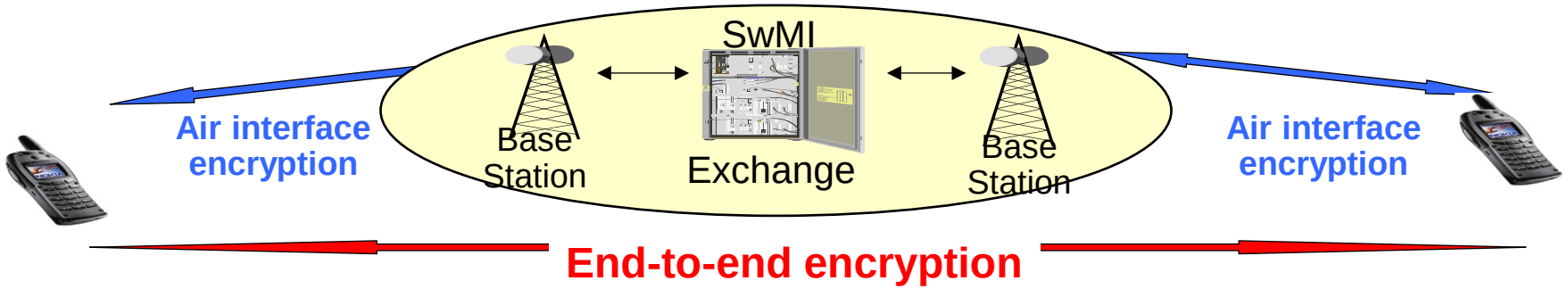
Overview - Encryption solutions

Air Interface Encryption (AIE) :

- *Encrypts data between MS and Network*
- *Encrypts <u>user data</u> and <u>signalling</u>*
- *Traffic is in plain form in the network*
- *TETRA standards Algorithms*
- *Standardized by ETSI*

End-to-End Encryption (E2EE) :

- *Encrypts data between MS*
- *Encrypts <u>user data</u>*
- *Traffic is encrypted from point-to-point*
- *Algorithms chosen by the customers*
- *Specified by SFPG recommendations for IOP*



AIRBUS

Mission Critical Services security

AIRBUS

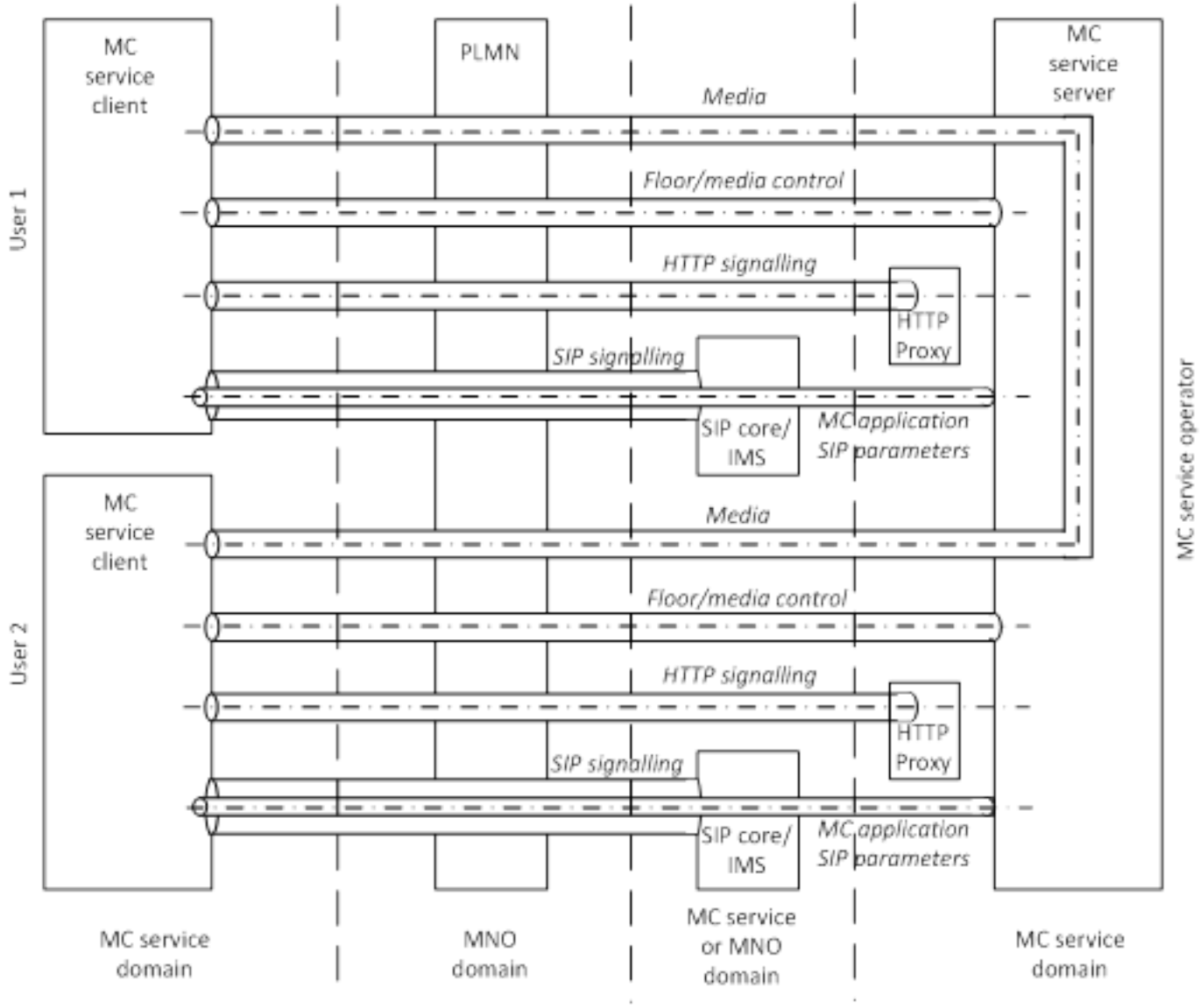
3GPP TS 33.180 V15.4.0 (2019-03)
Technical Specification

Security of the Mission Critical Service

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security of the mission critical service;
(Release 15)

- Specified in 3GPP TS 33.180
- Application layer overlay providing mission critical speech, video and data service
- Running over a 3GPP specified 4G or later network
- Independent from the underlying 3GPP (or other IP) network
- Confidentiality provided by MC application layer (eg not dependent on the MNO)
- Mobile Network Operator needs to be sufficiently trusted to provide the necessary service availability
- MC services also provide protection against traffic analysis
- The MC application layer security mechanisms include
  - Authentication and authorization of the Mission Critical user
  - End to end protection of media exchanged between users and within groups
  - Signalling security
  - Off-network security
  - Key management
- TCCA SFPG Recommendations 15 and 16 address “Secure implementation of mission critical systems”

Application level security



AIRBUS

Mission Critical Networks security

MCX, 4G, 5G bring new security challenges

- New architecture (*network slicing, virtualisation, …)*
- More open, services, integration, interconnection, interoperability, complexity,…

Threat and surface attack evolution

Evolution of the threat landscape

AIRBUS

Increasing cyber threats

- Stuxnet, Duqu, Locky, WannyCry, RobbinHood, Triton…

Increasingly vulnerable infrastructure

- IoT, Digitalization, Industry 4.0…

Countries react

- Cyber warfare, national security agencies, new laws

Hundreds of commercial aircraft – including Airbus and Boeing planes – vulnerable to hacking

bility Office (GAO) reported that "significant"
al Aviation Administration (FAA) are
ure the safe and uninterrupted operation of

GAO

s –

leaving them open to hacking from on

Attacks against critical infrastructure are increasing

Threat Landscape *(ENISA Report 2018)*

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/

AIRBUS

APT definition & principles

ADVANCED PERSISTENT THREAT

"ADVANCED"

The uses of **sophisticated techniques** exploiting **vulnerabilities** in systems

"PERSISTENT"

Continuously try to **introduce into networks** and steal data from a specific target while removing their tracks to stay **undetected as long as possible**

"THREAT"

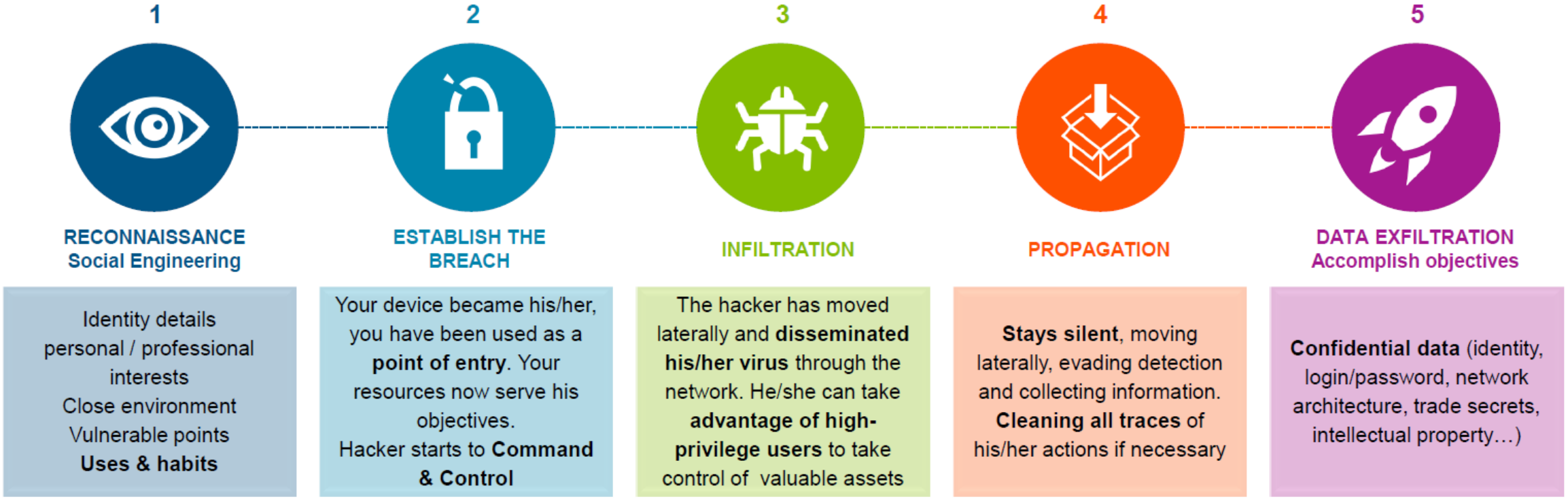
Based on **Human factors**, cyber criminals use ad**vanced technics, influence** and the art of **persuasion** to **manipulate** individuals to get **entry point**.

AIRBUS

APT simplified methodology

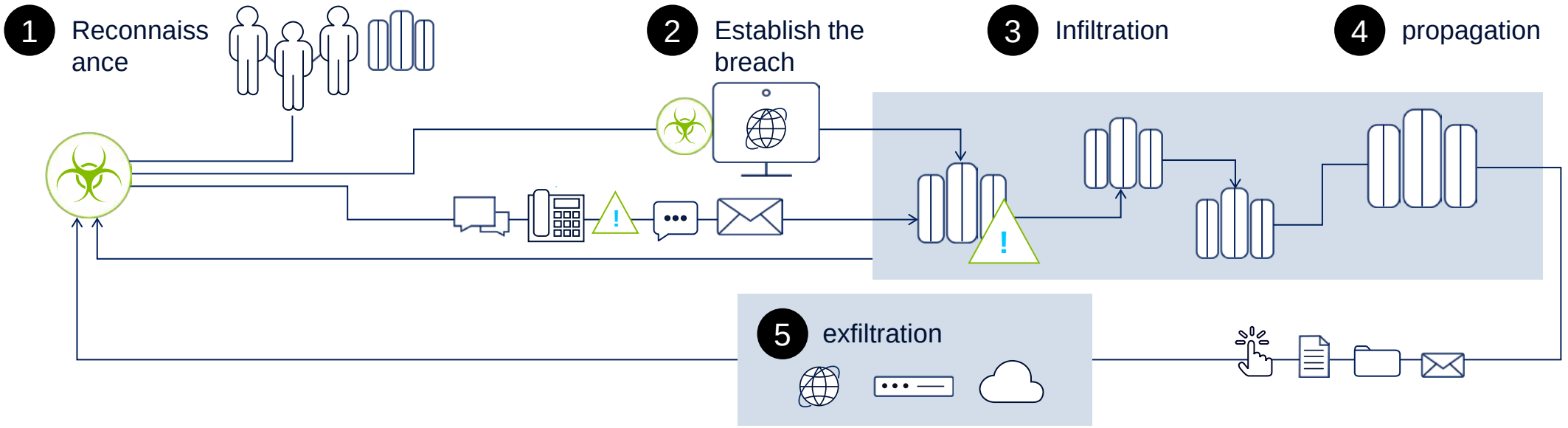
The lifecycle of an APT is much longer and more complex than other kinds of attacks.

Attackers executing APTs typically take the following sequential approach to gain and maintain ongoing access to a target.



AIRBUS

Stages of an APT attack



Security policy and risk management

AIRBUS

Security policy and risk management

To define a comprehensive system security and maintain it over time, it is important to address security as a whole taking into account all the equipment, operations and services offered.

Security policy & Risk Management Regime is central to organisation’s overall cyber security strategy

- Detailed asset inventory
- Classification of the data
- Cyber Threat Intelligence

The devil is in the details

Exemple from NCSC but similar exists from ANSSI, BSI, …

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

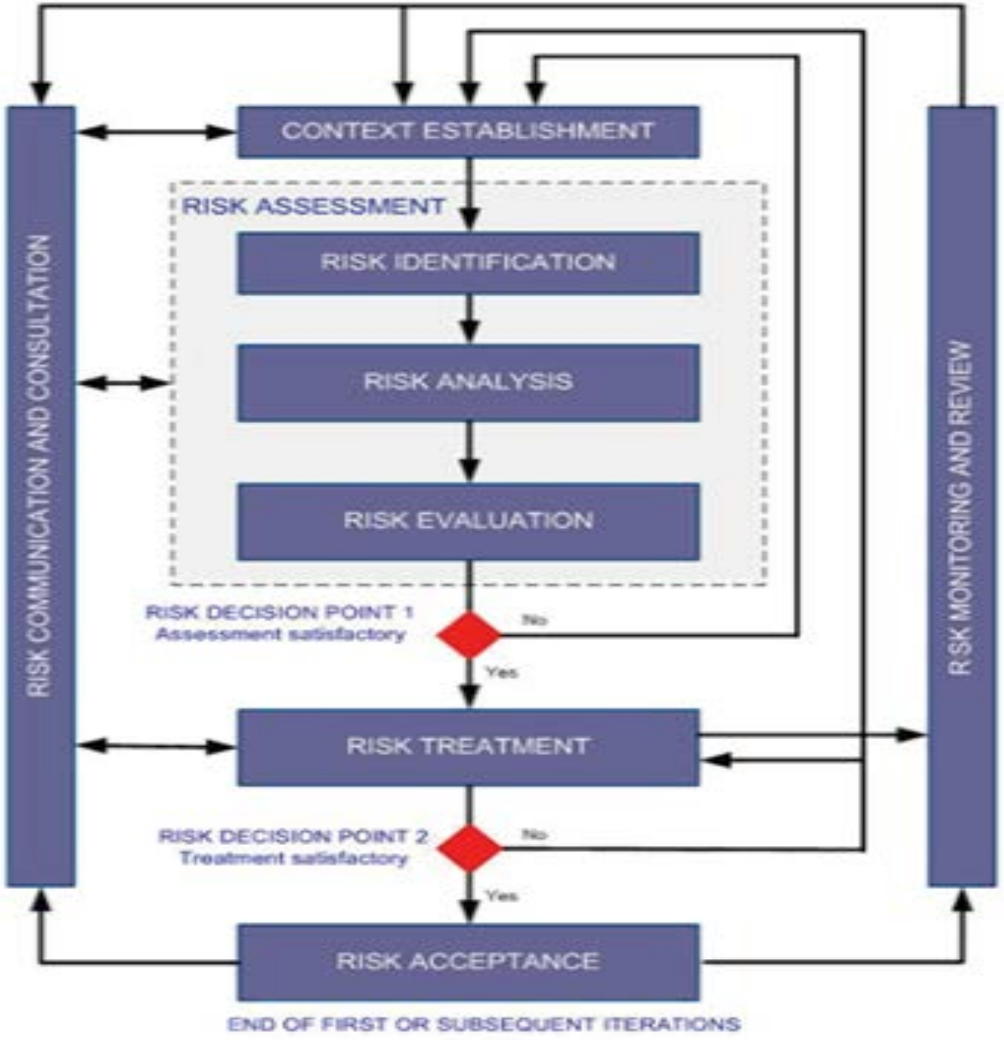
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

Security methodology and risk management



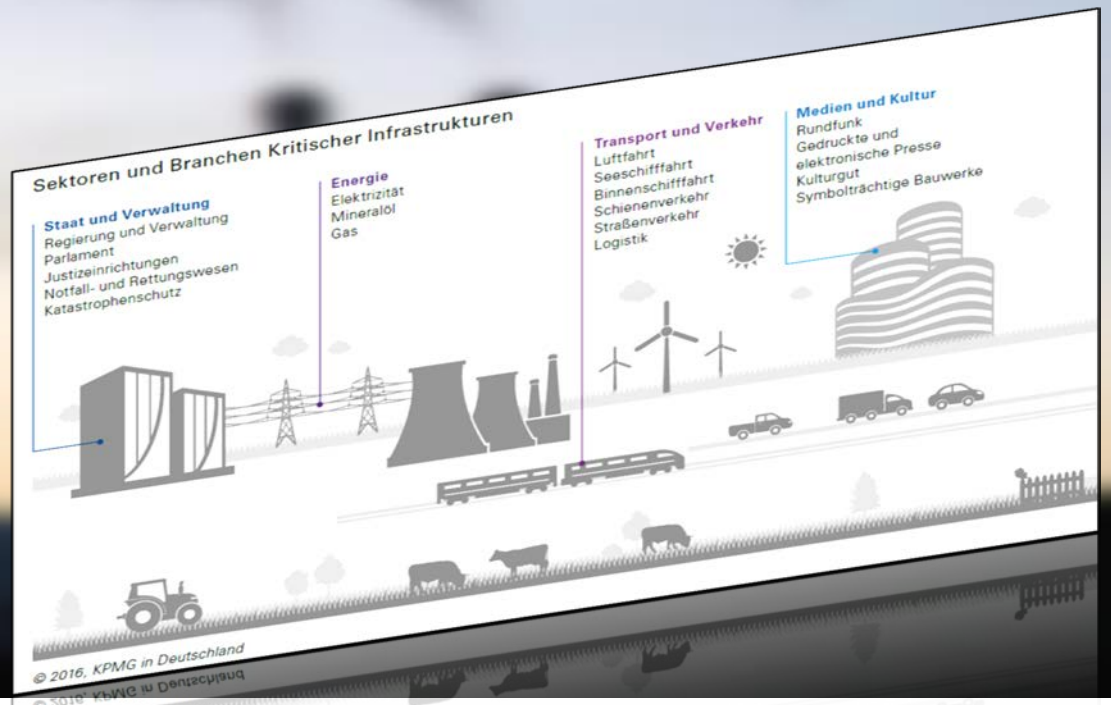
Source ISO 27005

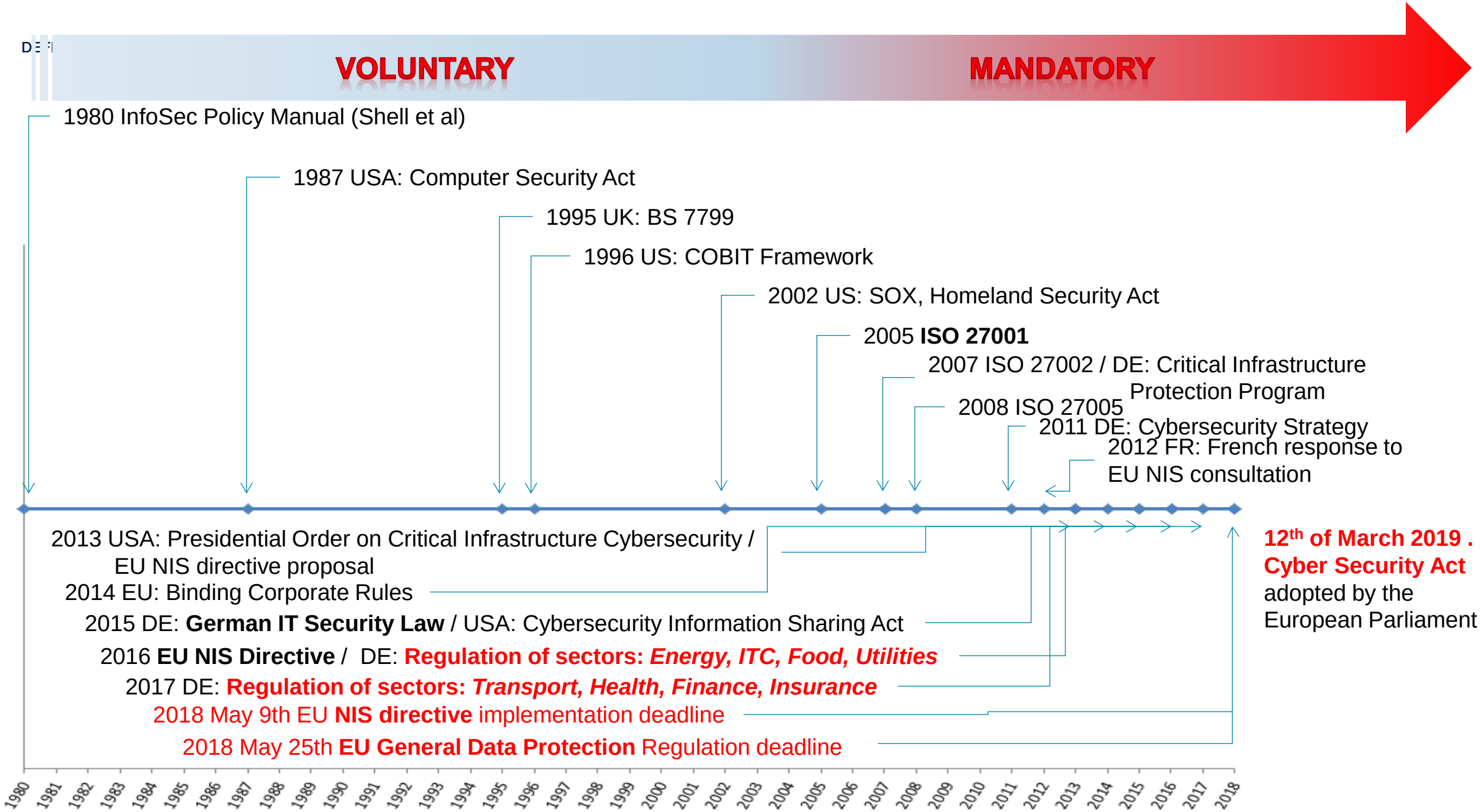
New legislation

AIRBUS

New regulation

- EU directive 2016/1148: NIS-directive
- EU GDPD: General Data Protection Regulation
- Cyber Security Act (EU) 526/2013




VOLUNTARY
MANDATORY
1980 InfoSec Policy Manual (Shell et al)
1987 USA: Computer Security Act
1995 UK: BS 7799
1996 US: COBIT Framework
2002 US: SOX, Homeland Security Act
2005 ISO 27001
2007 ISO 27002 / DE: Critical Infrastructure Protection Program
2008 ISO 27005
2011 DE: Cybersecurity Strategy
2012 FR: French response to EU NIS consultation
2013 USA: Presidential Order on Critical Infrastructure Cybersecurity / EU NIS directive proposal
2014 EU: Binding Corporate Rules
2015 DE: German IT Security Law / USA: Cybersecurity Information Sharing Act
2016 EU NIS Directive / DE: Regulation of sectors: Energy, ITC, Food, Utilities
2017 DE: Regulation of sectors: Transport, Health, Finance, Insurance
2018 May 9th EU NIS directive implementation deadline
2018 May 25th EU General Data Protection Regulation deadline
12th of March 2019 . Cyber Security Act adopted by the European Parliament
1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

AIRBUS

Cyber Security Act

- gives ENISA, the European Union Agency for Cybersecurity, a permanent mandate
- enhancing its role in supporting EU to achieve a common and high level cybersecurity.
- establishes the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in Europe.

AIRBUS

Food for tough

- National security agencies as well as ENISA provides good recommandations.
  - NCSC – www.ncsc.gov.uk
  - ANSSI www.ssi.gouv.fr
  - BSI https://www.bsi.bund.de
  - …
  - ENISA https://www.enisa.europa.eu/

DEFENCE AND SPACE

Thank you

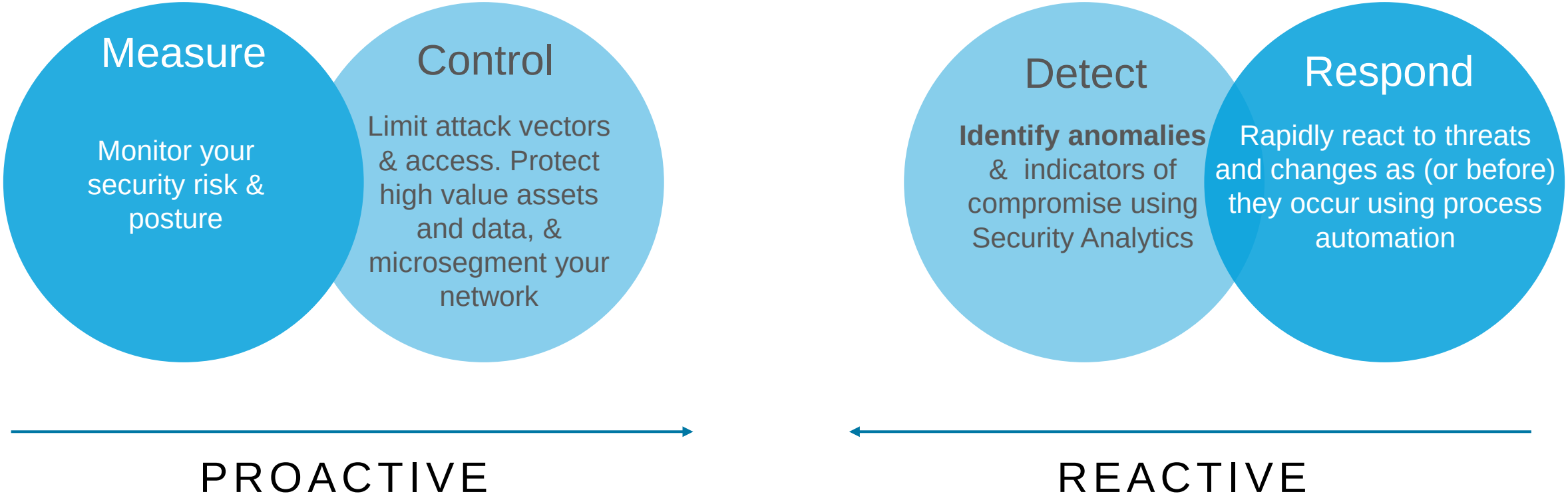
www.securelandcommunications.com

AIRBUS

Backup

AIRBUS

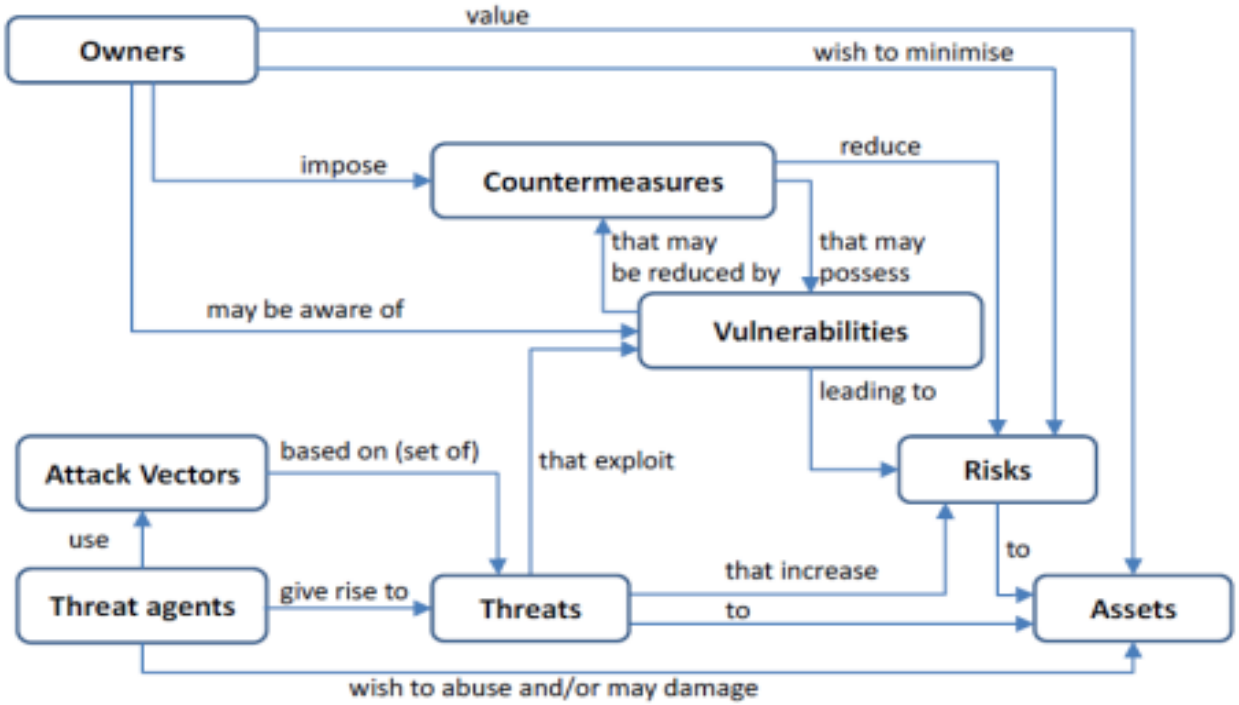
Balanced security



Risks

Source : ENISA

Asset (*Vulnerabilities, Controls*), **Threat** (*Threat Agent Profile, Likelihood*) and **Impact**.



Risk : Threats abuse vulnerabilities of assets to generate harm for the organisation
Vulnerability = weakness of an asset or group of assets that can be exploited by one or more threats