Anticipation of Cyber Crisis: Governance and Best Practices

Telecom Valley – Sophia Security camp

Robert Breedstraet / Jérôme Brognier
Amadeus CISO Office

amadeus

Agenda

01 Amadeus in a few words

02 One Strategy / Seven Security Pillars

03 Amadeus ISMS

04 Security Processes

Amadeus in a few words

- We are the leading technology company dedicated to the global travel industry
- We are present in 190+ countries and employ more than 16,000 people worldwide
- Our solutions enrich travel for billions of people every year
- We work together with our customers, partners and other players in the industry to improve business performance and power better journeys through travel technology

One of the world's leading software companies

690+ million
Passengers boarded in 2020 with Amadeus and Navitaire solutions

646+ million
Total bookings processed in 2019 using the Amadeus distribution platform

9th consecutive year included in the DJSI. Recognized as world leader in the Software & Services industry sector in the Dow Jones Sustainability Index in 2020

Our customers

travel agencies, online travel agencies, tour operators and corporations worldwide

474 airlines

132 airport operators

133 ground handlers

1M+ hotel properties

90 rail operators

69 mobility providers

21 insurance provider groups

29 cruise and ferry lines

Attack Surface Management

60K
Devices

2K
Domains

112K
IPs

11
ASN

104K
Hosts

5K
SSL Certs

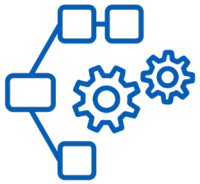
One Strategy, Seven Security Pillars

Risk-Based Approach

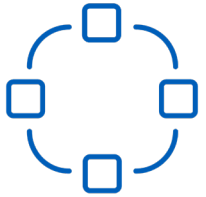
Visibility

Security in Suppliers

Security By Design



Security Resilience



People Security

Secure Cloud Solutions

Information Security Management System (ISMS)

Key Components

Amadeus Security Frameworks

Provide a structure to organize controls to ensure they are complete and cohesive
(ISO27001)

Security Controls Catalogs

A set of controls to start with & to build our security controls catalogue/model on top
(ISO27002, PCI-DSS, CIS, …)

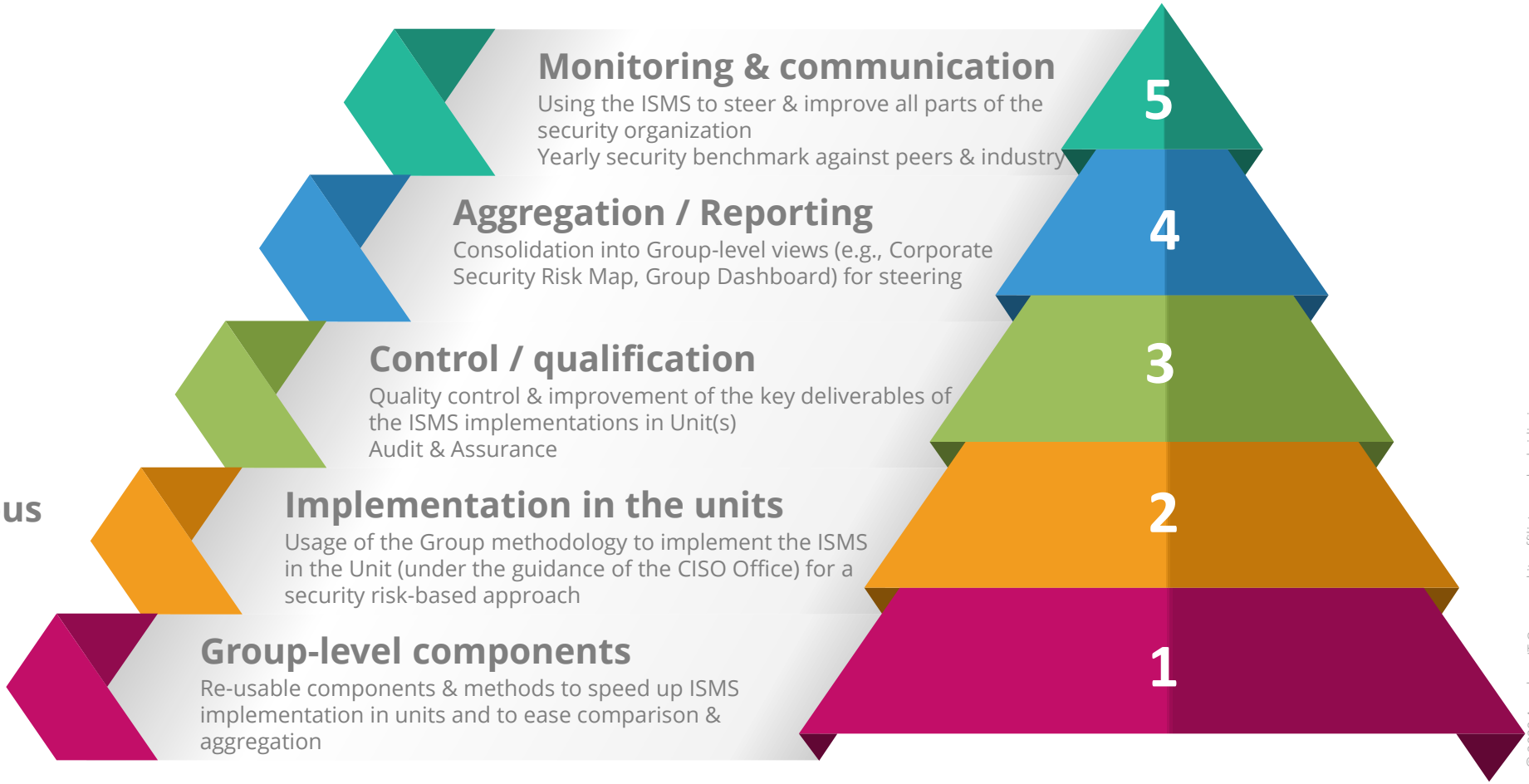
Security Processes

Mandatory or discretional operational actions executed to meet security control
(e.g. Security Governance, Security Management Policy, Security Awareness, Identity and Access Management, Vulnerability Management and Incident Management)

Source: Gartner

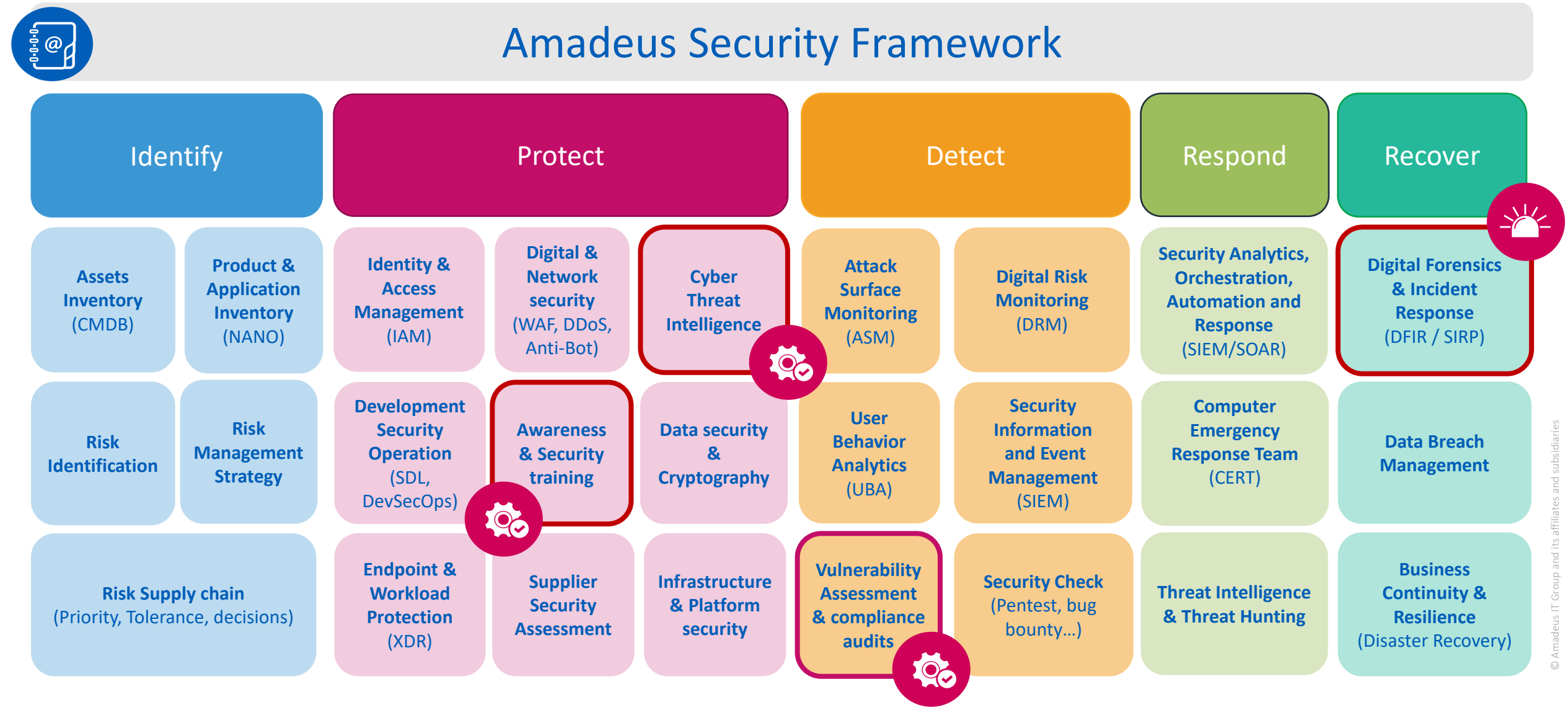
ISMS Governance at Amadeus

Maintenance & continuous improvement

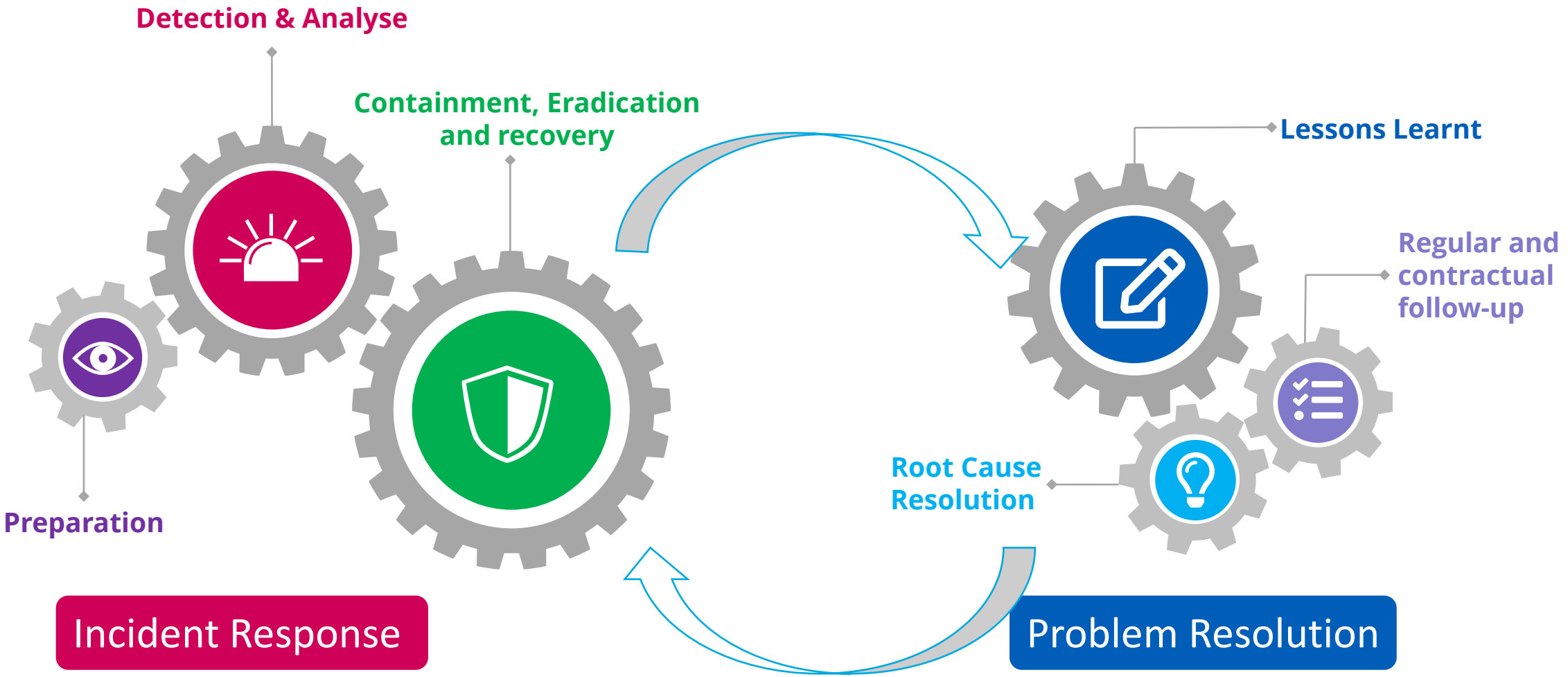


From Theory to Practice

Amadeus Security Framework



Security Incident Response Plan



[1]aligned to NIST SP 800-61 about " computer security incident handling"

Cyber Threat Intelligence

& other commercial sources

Global & Community Intelligence Feeds (80+)

Threat intel platform

Most Relevant IOC pushed to SIEM

Aggregation & De-duplication

Scoring & Expiration

Enrichment & Contextualization

Export & Push

Network & Endpoint Sensors

High Score IOC pushed to sensors for action

Incident Response Planning

IOC pushed to TIP at case closure

Case Management

IOC Management

SIEM

Continuous Monitoring

Threat Hunting

Alerting

Focus on Aviation ISAC

- Focused, actionable intelligence
- Trusted environment for anonymized information sharing and collaboration
- Shared situational awareness
- Global engagement
- Greater responsiveness and resilience
- Reduced business risk

Members & Partners
(Public & Private sector / Vendors)

32 Airlines are member today

Threat Intel Feeds

*Aviation Information Sharing and Analysis Center
https://www.a-isac.com/

Cybersecurity Awareness and Training program

Trainings

- Generic training for all staff, from a yearly mandatory training to mandatory monthly short trainings, dedicated trainings for administrators and priviledge account owners and dedicated trainings for security experts:
- CISM, CISSP, SANS,…

Phantom attacks

- Run internal fake phishing attacks

Perform cyber attacks simulation exercises

- Perfom cyber attacks exercices: could be table top exercices, Industry crisis exercices (with ENISA), cyber attack simulation… At different hierarchy levels : CCMT and ECMT:
- ANSSI guide: https://www.ssi.gouv.fr/uploads/2020/10/anssi-guide-organiser-un-exercice-de-gestion-de-crise-cyber-v1.0.pdf
- Perform restores tests from offline backups

Vulnerability & IT Compliance Management

Identify assets

Asset inventory: make sure you know your assets location, identify owners, solutions and data criticality,….

Internal scans to identify vulnerabilities

Use dedicated internal vulnerabilty scanners, track and verify updates (Nessus, Qualys)

External scans to measure our security posture

Use exernal scanners to verify our digital footprint. Business ecosystems also want to monitor and assess the security maturity of their partners (RiskIQ, Security Scorecards, Bitsight,…)

Firewall controls

Perform reviews of network cartography, firewall vulnerabilities and consistance of firewall rules

Thank you