Security Governance
Master of Science in Cyber Security

AA 2022/2023

HOW TO SUPPORT THE INCIDENT MANAGEMENT: SOC AND CERT

Security Operation Centre (SOC)

A Security Operations Centre (SOC) can be defined as a centralized security organization that assists companies with identifying, managing and remediating distributed security attacks.

Depending on the capabilities required from a SOC by the enterprise or client, a SOC can also be responsible for the management of technical controls.

The end-goal of a SOC is to improve the security posture of an organization by detecting and responding to threats and attacks before they have an impact on the business

https://www.agendadigitale.eu/sicurezza/soc-security-operation-center-e-cert-definizioni-differenze-e-sinergie-per-una-migliore-sicurezza/

Services provided by SOCs

Main fundamental services

- Log Management
- Security Monitoring and Alerting
- Security Incident Management

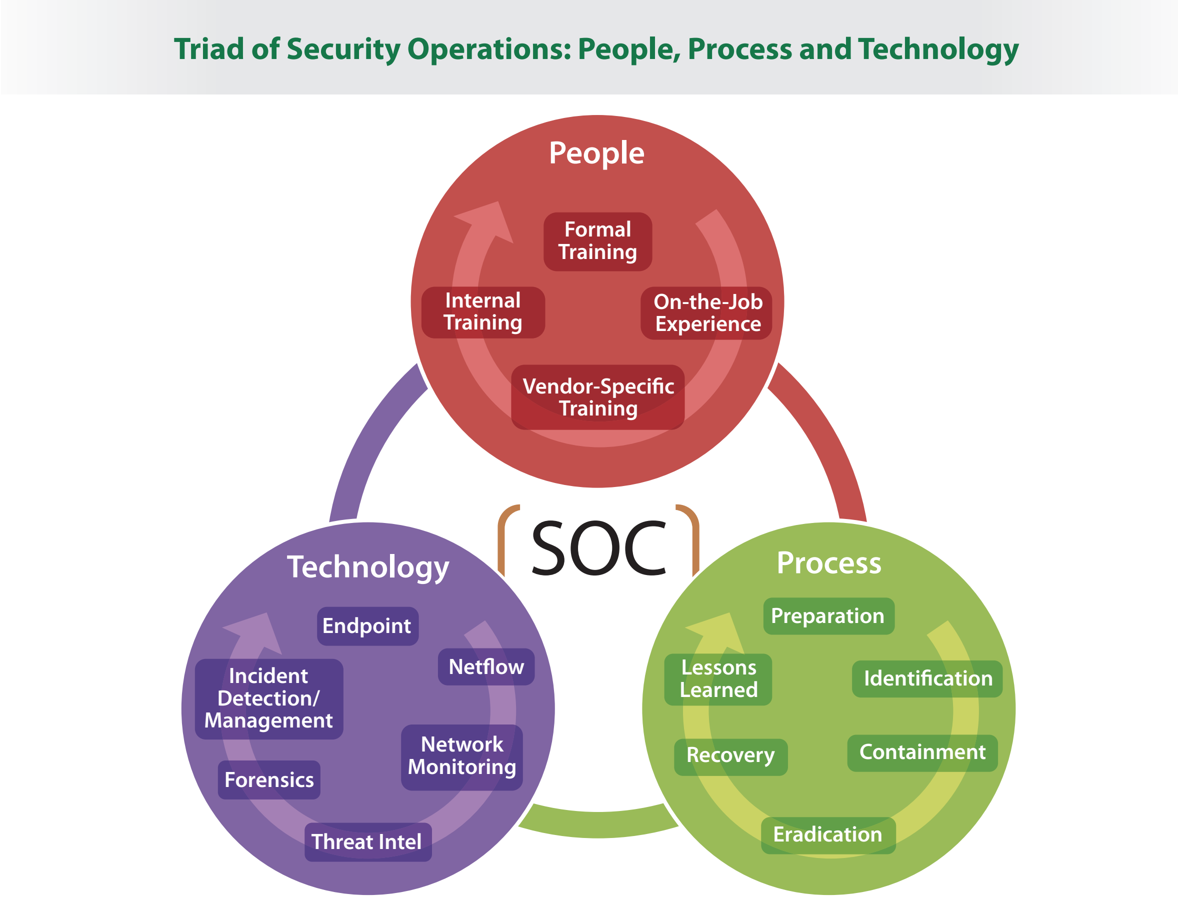
Additional Service

- Security Operation Management
- Vulnerability Assessment

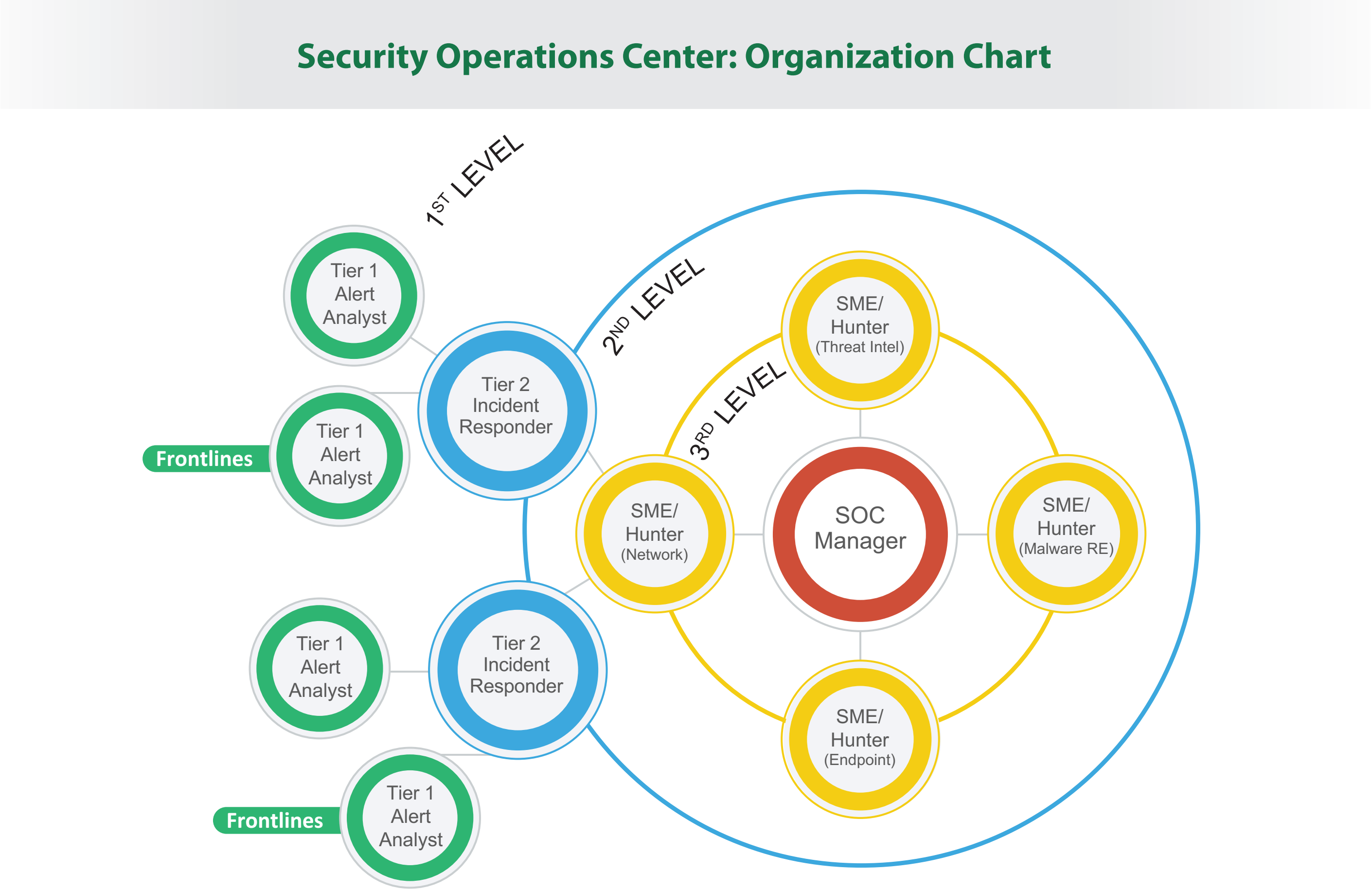
Evolved SOCs

- Service security assessment
- security analytics starting from data collected from SIEM
- threat intelligence (in partial overlapping with CERTs)

Building Blocks of a SOC



Organization of the SOC



When you should adopt a SOC

When it is good to have a SOC?

1. in presence of critical or "sensitive" data or processes (in terms of business and/or regulatory compliance)

2. when there is a growing trend of the company and an internal information security function (not structured and/or strongly unbalanced on the work of an outsourcer) can no longer "keep up" (creating bottlenecks between outsourcers and internal contacts, undersized outsourcing, etc.)

3. There is the need to equip themselves with "pushed" monitoring and technical response capacities to information security events.

Computer Emergency Response Team (CERT)

A computer emergency response team (CERT) is a group of experts who respond to cybersecurity incidents

The term CERT (Computer Emergency Response Team) was used first in 1989 by what is now the CERT Coordination Center (CERT/CC)

CERT/CC is hosted by Carnegie-Mellon University, USA

CERT functions

Over the years CERTs have extended their areas of action and intervention

- Shift from a pure reaction force to (in some cases) real security providers

Their main functions are

- Providing preventive services (such as alerts on cyber security attacks)
- Providing security bulletins (advisory)
- Training
- Providing management of security services (function in overlap with a SOC)

Computer Security Incident Response Team (CSIRT)

A capability set up for the purpose of assisting in responding to computer security-related incidents

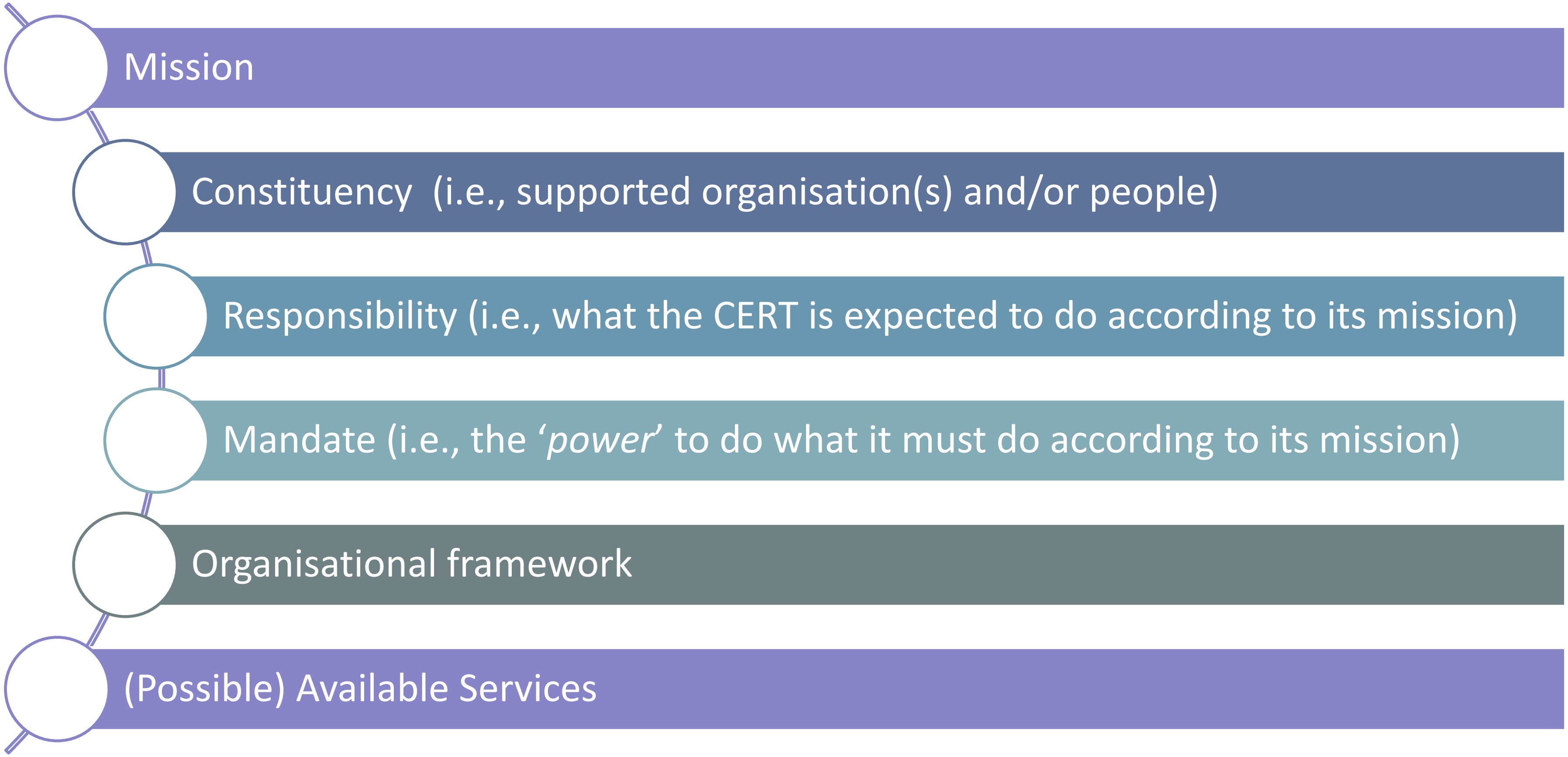
also called

- Computer Incident Response Team (CIRT) or
- Computer Incident Response Centre, Computer Incident Response Capability (CIRC)

Currently, CERT and CSIRT are used as synonyms

A framework for building up a successful CERT/CSIRT

The foundations of a CERT are



- Mission
- Constituency (i.e., supported organisation(s) and/or people)
- Responsibility (i.e., what the CERT is expected to do according to its mission)
- Mandate (i.e., the ‘*power*’ to do what it must do according to its mission)
- Organisational framework
- (Possible) Available Services

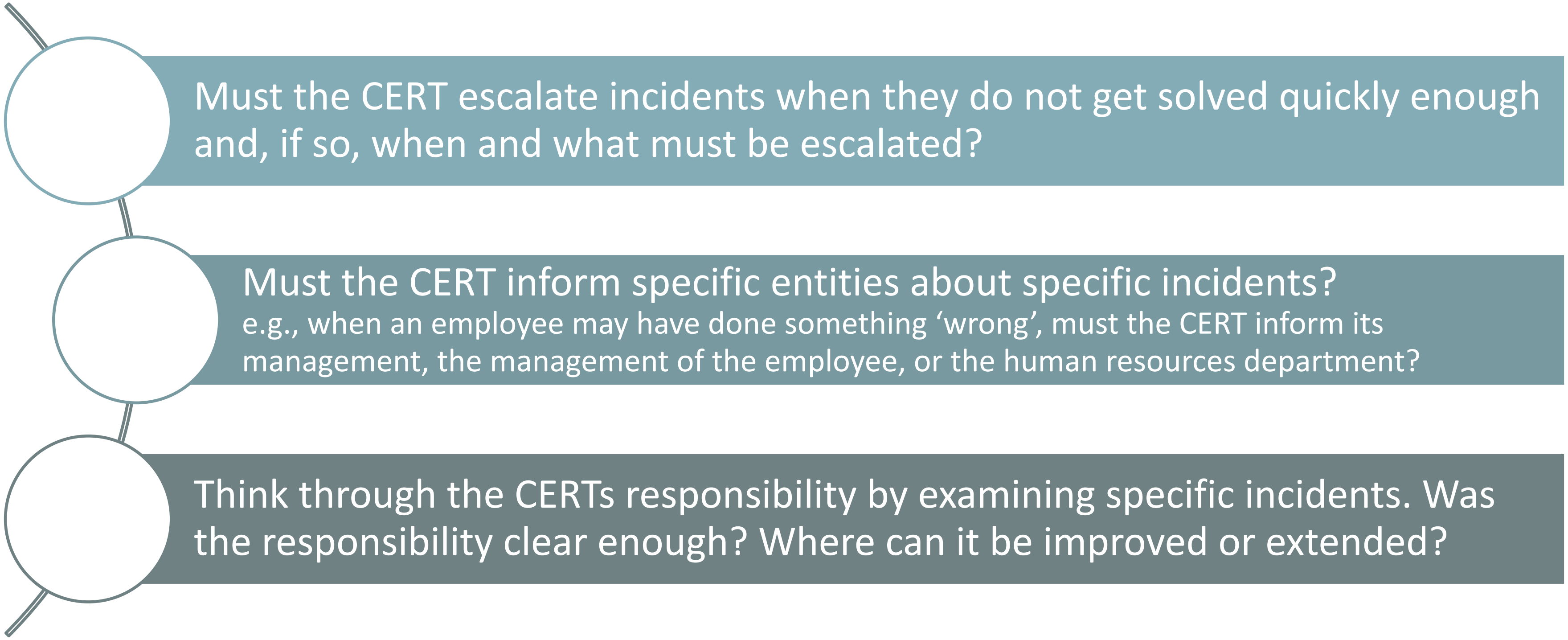
CERT: Responsibility

When defining responsibility, the following practical questions should be taken into account:

- Which type of incidents must be handled by the CERT and with what priorities?
- Must the CERT keep track of incident resolution and, in the end, close it? Or is it sufficient to notify constituents?
- Is the CERT obliged to actively solve an incident – which goes one step beyond guarding? Or should it notify and give advice?

CERT: Responsibility

When defining responsibility, the following practical questions should be taken into account:



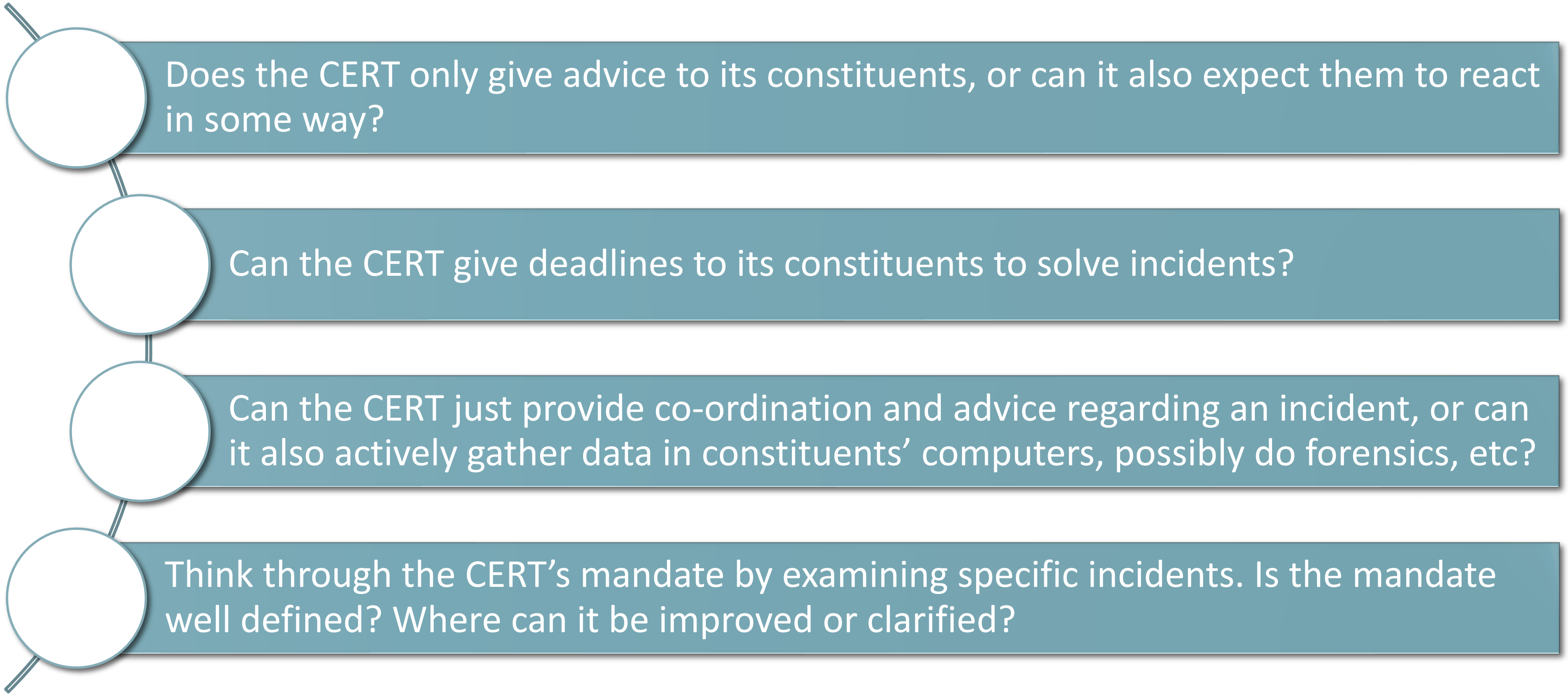
Must the CERT escalate incidents when they do not get solved quickly enough and, if so, when and what must be escalated?

Must the CERT inform specific entities about specific incidents?
e.g., when an employee may have done something ‘wrong’, must the CERT inform its management, the management of the employee, or the human resources department?

Think through the CERTs responsibility by examining specific incidents. Was the responsibility clear enough? Where can it be improved or extended?

CERT: Mandate

When defining the mandate, the following practical questions should be considered:



Does the CERT only give advice to its constituents, or can it also expect them to react in some way?

Can the CERT give deadlines to its constituents to solve incidents?

Can the CERT just provide co-ordination and advice regarding an incident, or can it also actively gather data in constituents’ computers, possibly do forensics, etc?

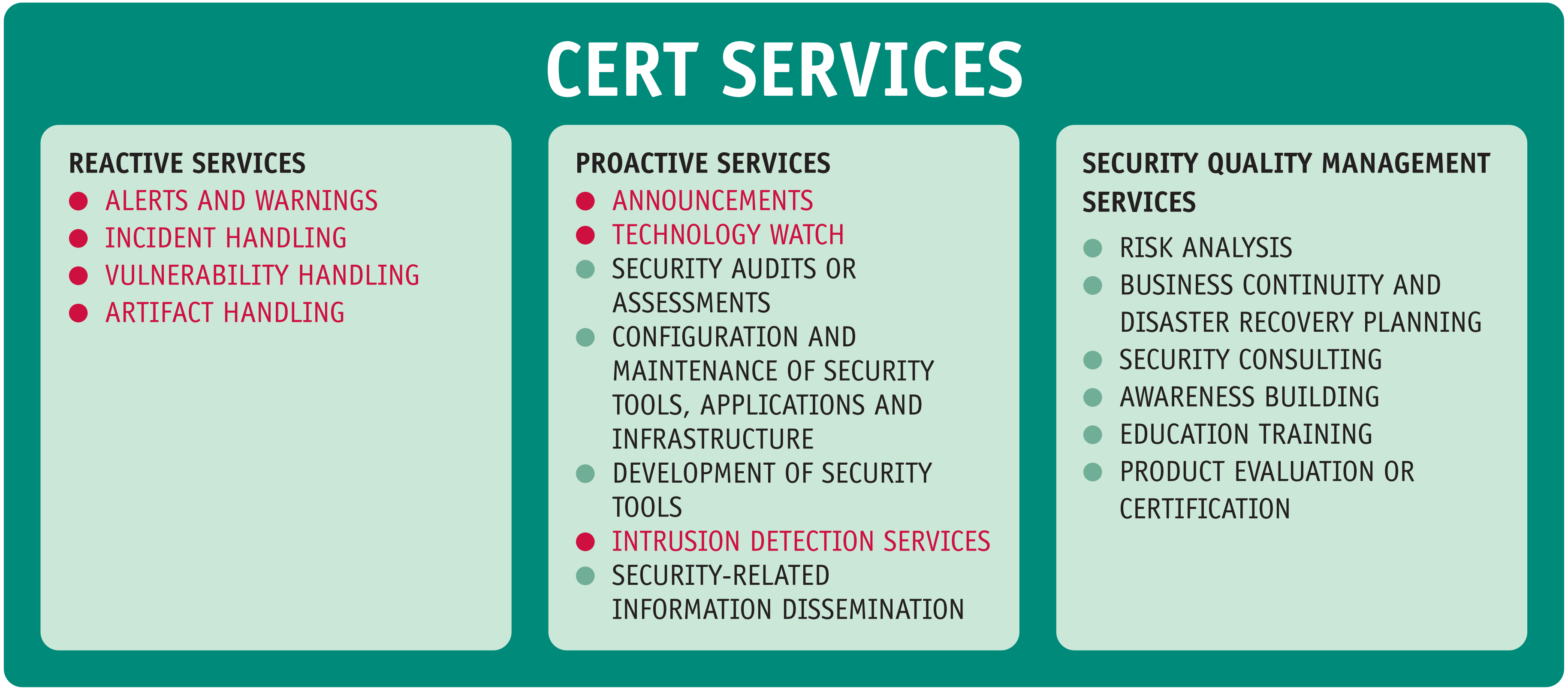
Think through the CERT’s mandate by examining specific incidents. Is the mandate well defined? Where can it be improved or clarified?

CERT: Organisational Framework

Some aspects of governance are essential for a good incident management and need to be thoroughly considered and clearly defined

- Escalation
- Relationship with CISO and CIO
- Relationship with Crisis Management inside organisation

CERT: Services



CERT SERVICES

REACTIVE SERVICES

- ALERTS AND WARNINGS
- INCIDENT HANDLING
- VULNERABILITY HANDLING
- ARTIFACT HANDLING

PROACTIVE SERVICES

- ANNOUNCEMENTS
- TECHNOLOGY WATCH
- SECURITY AUDITS OR ASSESSMENTS
- CONFIGURATION AND MAINTENANCE OF SECURITY TOOLS, APPLICATIONS AND INFRASTRUCTURE
- DEVELOPMENT OF SECURITY TOOLS
- INTRUSION DETECTION SERVICES
- SECURITY-RELATED INFORMATION DISSEMINATION

SECURITY QUALITY MANAGEMENT SERVICES

- RISK ANALYSIS
- BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING
- SECURITY CONSULTING
- AWARENESS BUILDING
- EDUCATION TRAINING
- PRODUCT EVALUATION OR CERTIFICATION

CERT: Roles

The mandatory roles are:

- Duty officer
    - She/he has to take care of all in-coming requests as well as carry out periodic or ad hoc activities dedicated to this role
- Triage officer
    - She/he has to deal with all incidents that are reported to or by the team.
    - She/he needs to decide whether it is an incident that is to be handled by the team, when to handle it and who is going to be the incident handler according to the triage process.
    - She/he needs to be up to date with all the latest trends, attack vectors and methods used by miscreants. In many cases the duty officers are also the triage officers.

CERT: Roles

The mandatory roles are:

- Incident handler
  - This is a crucial role in the incident handling team.
  - She/he deals with the incidents – analysing data, creating workarounds, resolving the incident and communicating clearly about the progress he has made to his incident manager and to and with the appropriate constituent(s).
- Incident manager
  - She/he is responsible for the coordination of all incident handling activities. He represents the incident handling team outside his team.

CERT: Roles

The following roles are optional…

- Public relations officer
- Legal officer
- Team manager
- Hotline operator

… However, in many cases part or all of the tasks that would fit the roles have to be undertaken in some way

IM Workflows

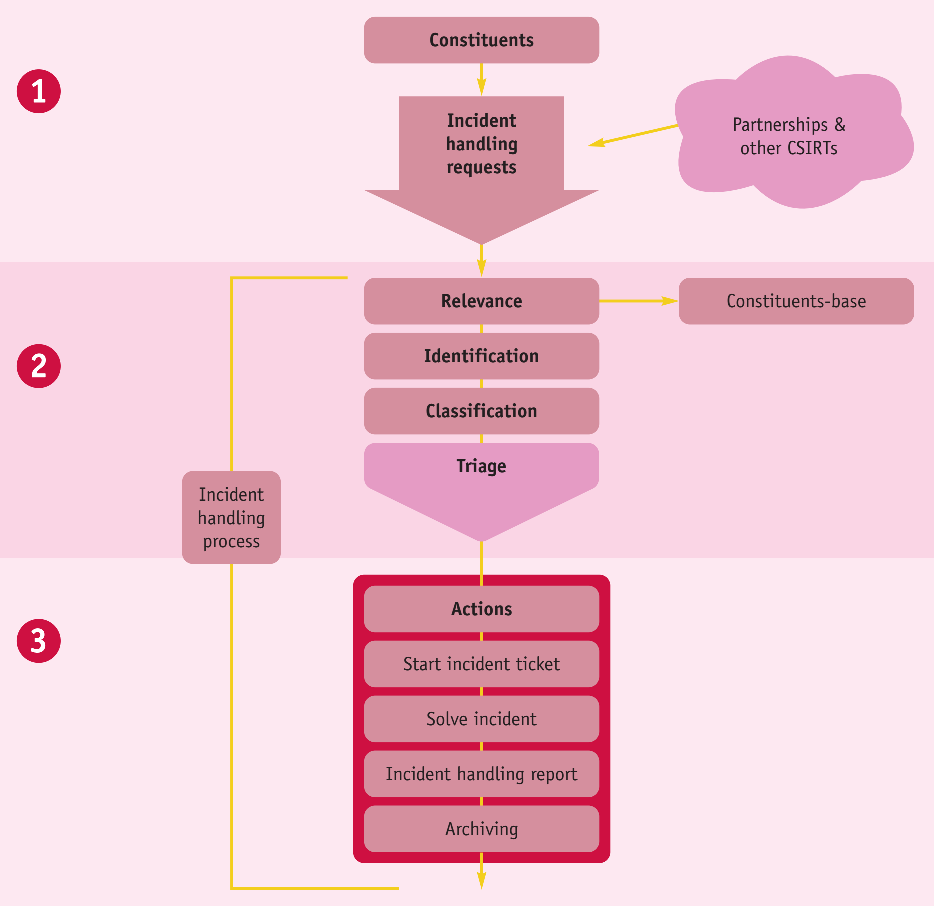


Figure 4 – Incident handling process flow

Source: ENISA – Good Proactice Guide for Incident Management
https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

IM Workflows

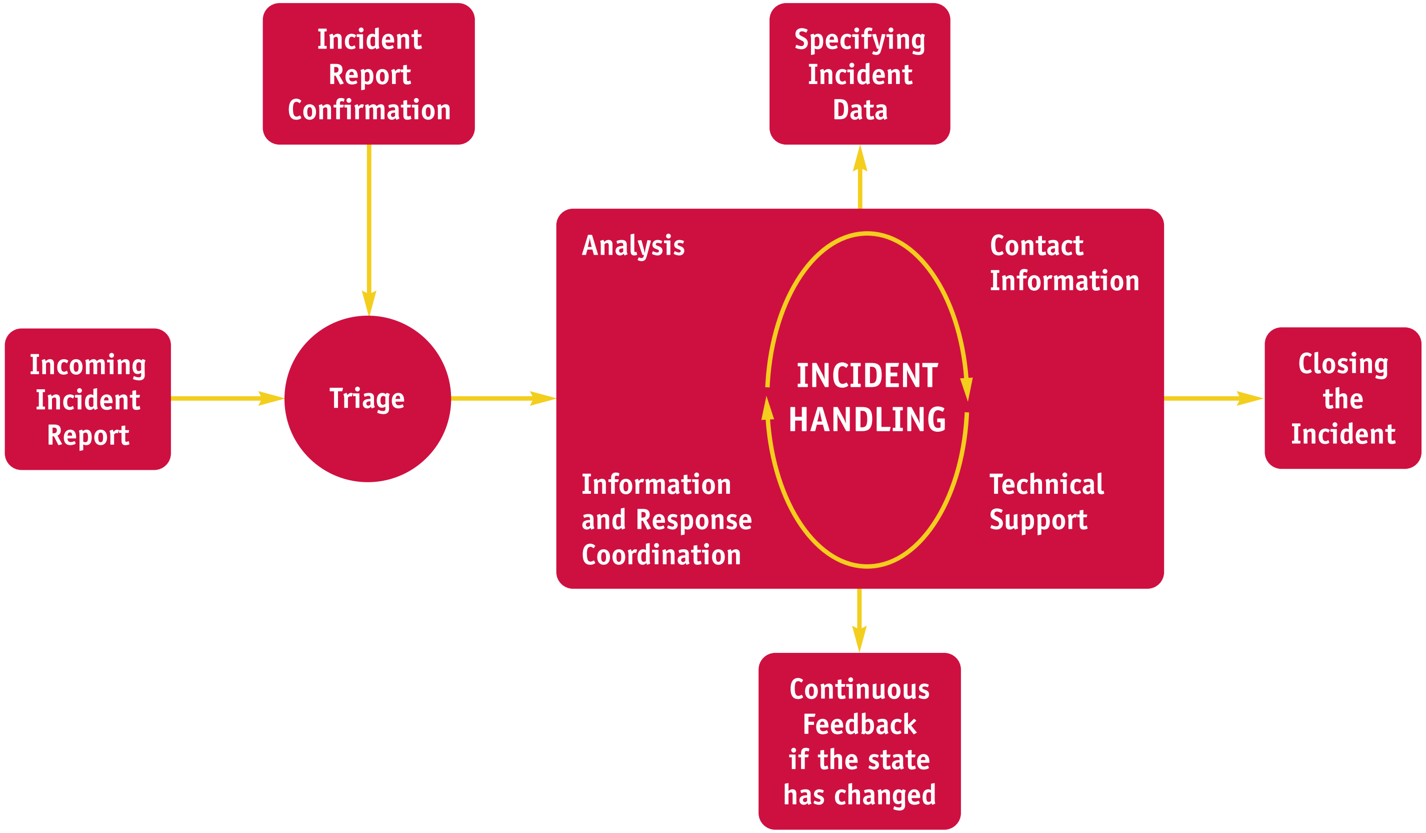


Figure 5 - Incident handling process flow (CERT Hungary example)

Source: ENISA – Good Proactice Guide for Incident Management
https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

IM Workflows

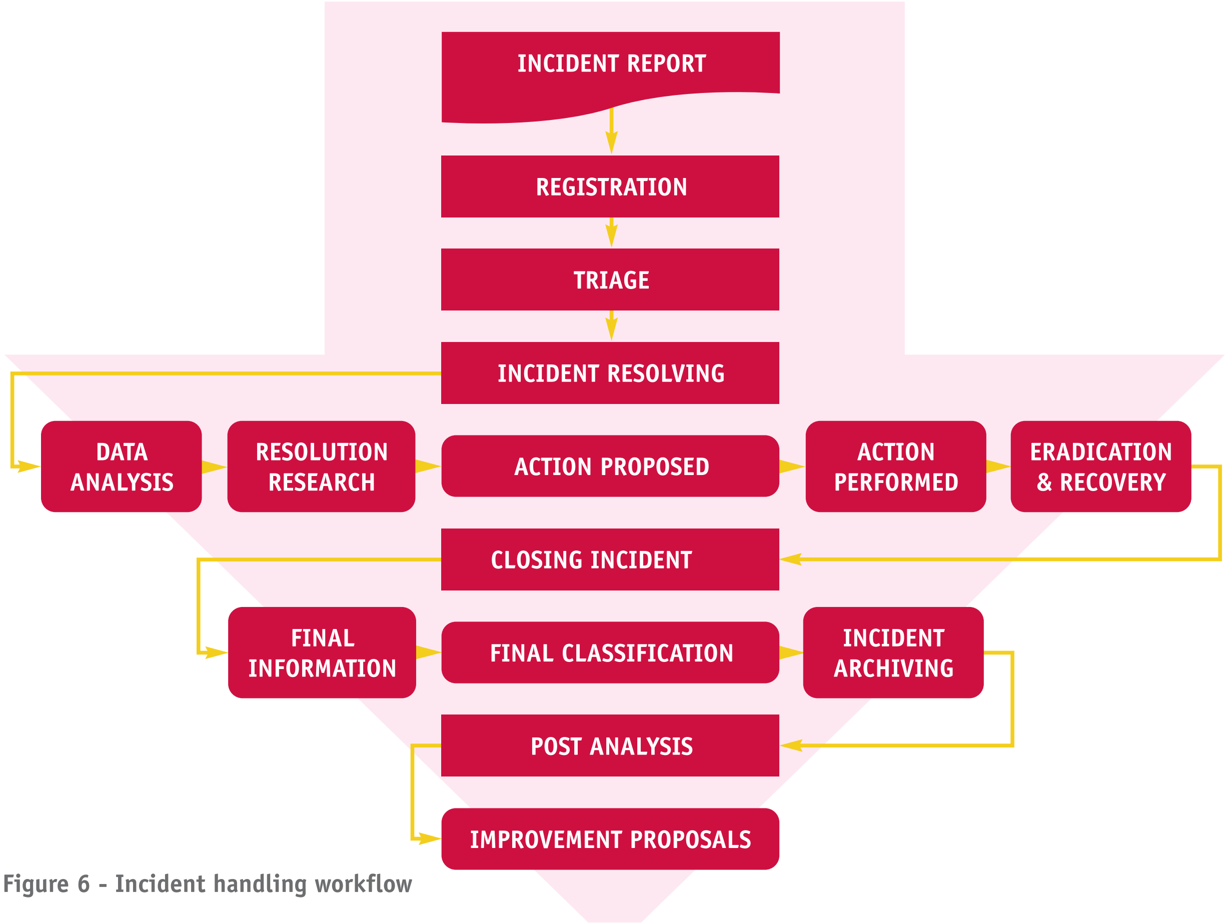
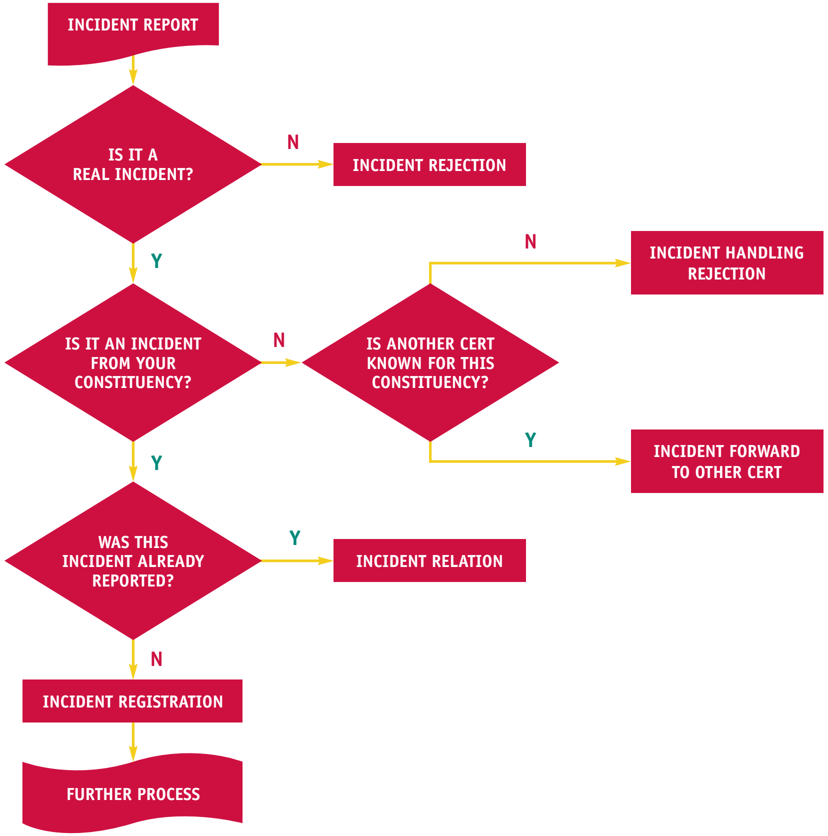


Figure 6 - Incident handling workflow

Source: ENISA – Good Proactice Guide for Incident Management
https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

IM Workflows

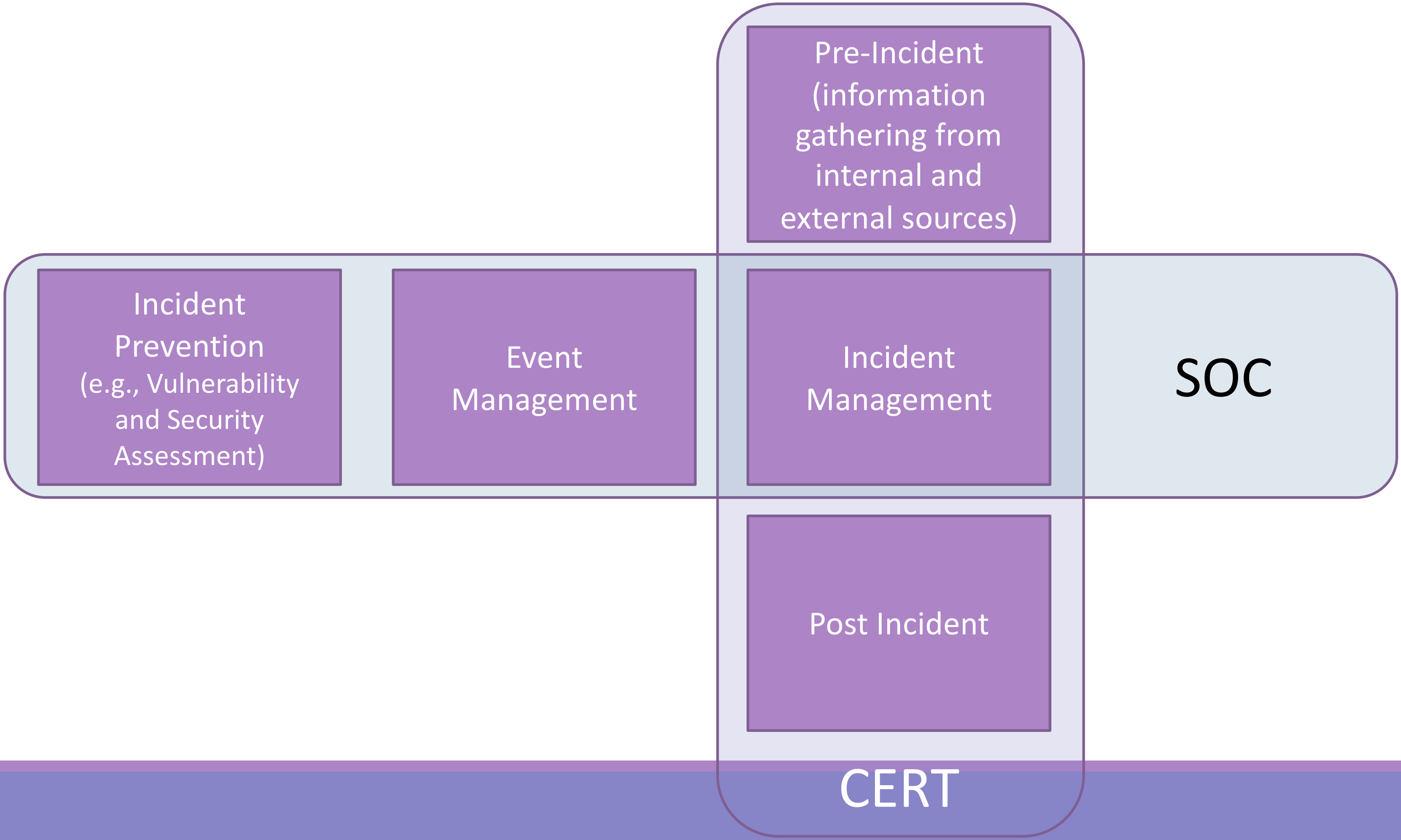


INCIDENT REPORT
IS IT A REAL INCIDENT?
N
INCIDENT REJECTION
Y
N
INCIDENT HANDLING REJECTION
IS IT AN INCIDENT FROM YOUR CONSTITUENCY?
N
IS ANOTHER CERT KNOWN FOR THIS CONSTITUENCY?
Y
INCIDENT FORWARD TO OTHER CERT
Y
WAS THIS INCIDENT ALREADY REPORTED?
Y
INCIDENT RELATION
N
INCIDENT REGISTRATION
FURTHER PROCESS

Figure 7 - Part of a detailed incident handling workflow – graphical approach

Source: ENISA – Good Proactice Guide for Incident Management
https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Relationships between SOC and CERT



Pre-Incident (information gathering from internal and external sources)
Incident Prevention
(e.g., Vulnerability and Security Assessment)
Event Management
Incident Management
SOC
Post Incident
CERT

References

1. SANS white paper - SANS: Building a World-Class Security Operations Center: A Roadmap
2. ENISA – Good Proactice Guide for Incident Management https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
3. SOC (Security operation center) e CERT: definizioni e sinergie per la sicurezza informatica - https://www.agendadigitale.eu/sicurezza/soc-security-operation-center-e-cert-definizioni-differenze-e-sinergie-per-una-migliore-sicurezza/