Security Governance
Master of Science in Cyber Security

AA 2024/2025

HOW TO SUPPORT THE INCIDENT MANAGEMENT: SOC AND CERT

Security Operation Centre (SOC)

A Security Operations Center (SOC) is a centralized security hub that helps organizations detect, manage, and mitigate distributed security threats

The responsibilities of a Security Operations Center (SOC) may extend to managing technical controls, depending on the specific capabilities required by the enterprise or client

The primary goal of a SOC is to strengthen an organization's security posture by proactively detecting and responding to threats and attacks, minimizing their potential impact on business operations

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

Services provided by SOCs

Core fundamental services

- **Log Management**. Collecting, storing, analyzing, and monitoring log data from various systems to support security, troubleshooting, and compliance
- **Security Monitoring and Alerting**. Continuous process of observing an organization’s IT environment for potential threats or anomalies and generating prioritized alerts to enable rapid detection and response
- **Security Incident Management**. The process of identifying, responding to, and resolving security incidents to minimize their impact on the organization

still SOC

Additional Services

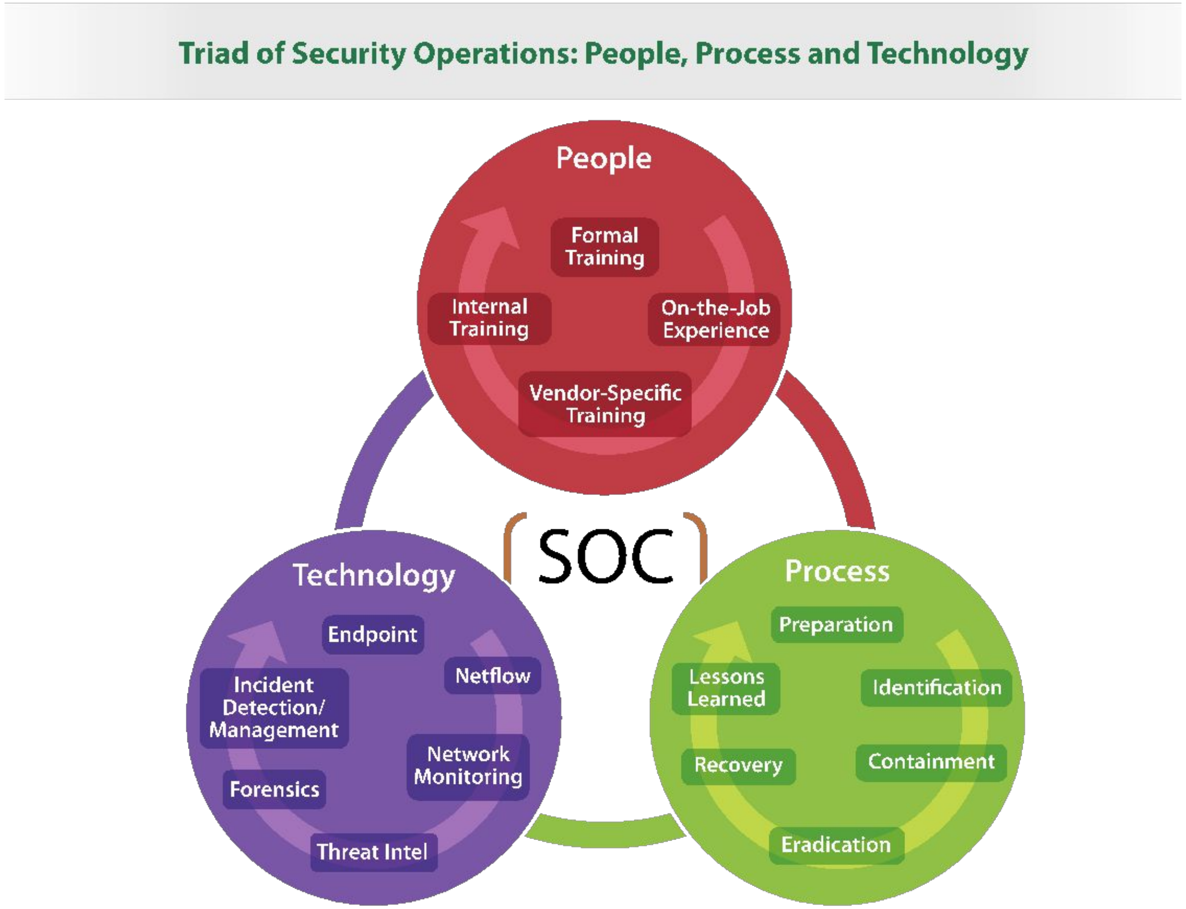
- **Security Operation Management** . Overseeing and coordinating security processes, tools, and teams to protect an organization’s IT infrastructure and respond to threats effectively
- **Vulnerability Assessment** . Identifying, evaluating, and prioritizing security weaknesses in the organization’s systems, networks, and applications

Advanced SOCs

- **Service security assessment** . It evaluates the security measures and risks associated with a specific service to ensure it meets organizational and compliance standards
- **Security analytics starting from data collected from SIEM** . Analyzes collected security event data to identify patterns, detect threats, and enhance incident response
- **Threat intelligence** (in partial overlapping with CERTs). Involves gathering, analyzing, and sharing information about cyber threats to enhance organizational defence and response capabilities

AI enhanced

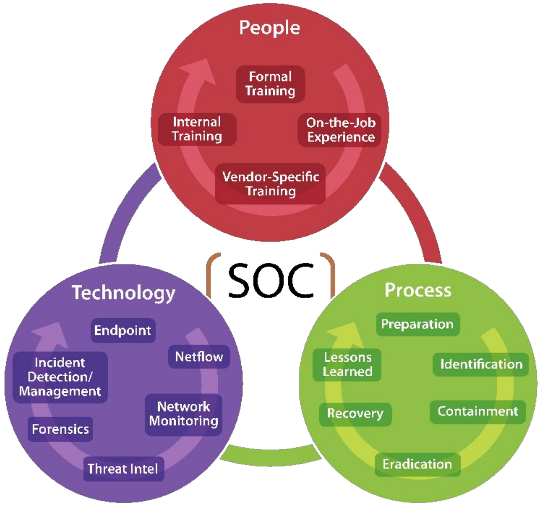
Building Blocks of a SOC



Overview of the Triad

The Triad of Security Operations is foundational to effective security in a SOC. It consists of three key elements:

- ❑ **People**: Skilled personnel and training
- ❑ **Process**: Structured protocols for incident management
- ❑ **Technology**: Tools and systems supporting operations



People: Key Elements

- ❑Formal Training: Certifications and structured learning
- ❑Internal Training: Organization-specific onboarding
- ❑On-the-Job Experience: Practical daily learning
- ❑Vendor-Specific Training: Tool-specific expertise

Process: Key Phases

- Preparation: Planning and readiness activities

- Identification: Recognizing threats or incidents

- Containment: Mitigating the impact of incidents

- Eradication: Removing threats from the environment

- Recovery: Restoring operations to normal

- Lessons Learned: Improving future responses

Technology: Key Components

- Endpoint: Device security (e.g., laptops, servers)

- Netflow: Monitoring network traffic for anomalies

- Network Monitoring: Observing and identifying threats

- Incident Detection/Management: Systems for responding to threats

- Forensics: Tools for analyzing security events

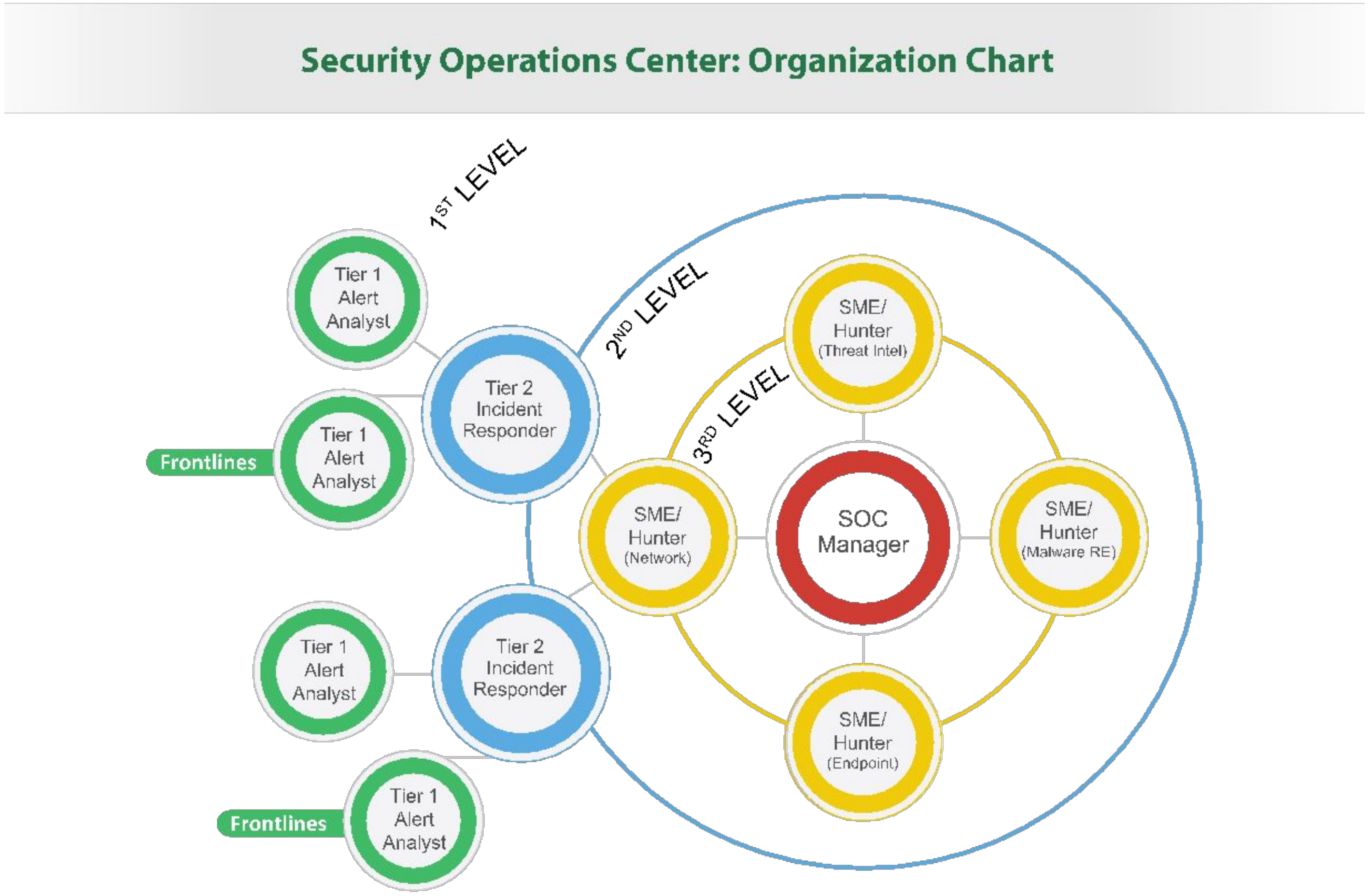
- Threat Intel: Insights into current and emerging threats

Integration in SOC

The three elements (People, Process, Technology) work together to form the core of a Security Operations Center (SOC). This integration ensures that:

- ❑Skilled personnel are supported by processes and technology
- ❑Robust processes guide effective incident management
- ❑Advanced technology enables efficient threat detection and response

Organization of the SOC


Security Operations Center: Organization Chart

Breakdown of the Organizational Chart

Frontlines (First Level)
Tier 1 Alert Analysts (Green)

Serve as the first line of defense in the SOC. Responsible for

1. Monitoring security alerts and identifying potential threats
2. Performing initial triage and determining if an alert requires escalation
3. Documenting and categorizing incidents

These analysts handle high volumes of alerts and provide rapid responses to known, low-complexity incidents

Incident Response (Second Level)
Tier 2 Incident Responders (Blue)

Handle escalated incidents from Tier 1 analysts. Responsible for:

1. Investigating and analyzing potential security breaches in greater detail
2. Coordinating the response to confirmed incidents
3. Communicating findings to higher-level teams or external stakeholders if needed

They act as the intermediate layer, bridging front-line analysts and Subject Matter Experts (SMEs)

Breakdown of the Organizational Chart 2

Subject Matter Experts (SMEs)/Hunters (Third Level)
Specialized experts who provide advanced insights and strategies for threat management. Roles include

- **Threat Intelligence SME**
  - Gathers, analyzes, and disseminates information on emerging threats
  - Provides insights to proactively defend against potential attacks
- **Network SME**
  - Focuses on network-related security issues and ensures secure network architecture
  - Detects and mitigates advanced network-based threats
- **Malware Reverse Engineer (Malware RE) SME**
  - Analyzes malware to understand its behavior, origin, and mitigation techniques
  - Assists in developing defense strategies against malware attacks
- **Endpoint SME**
  - Ensures the security of endpoint devices (e.g., desktops, laptops, servers)
  - Handles endpoint detection and response (EDR) solutions

Breakdown of the Organizational Chart 3

SOC Manager (Core Role)
Positioned at the center of the SOC structure, overseeing all operations.
Responsibilities:

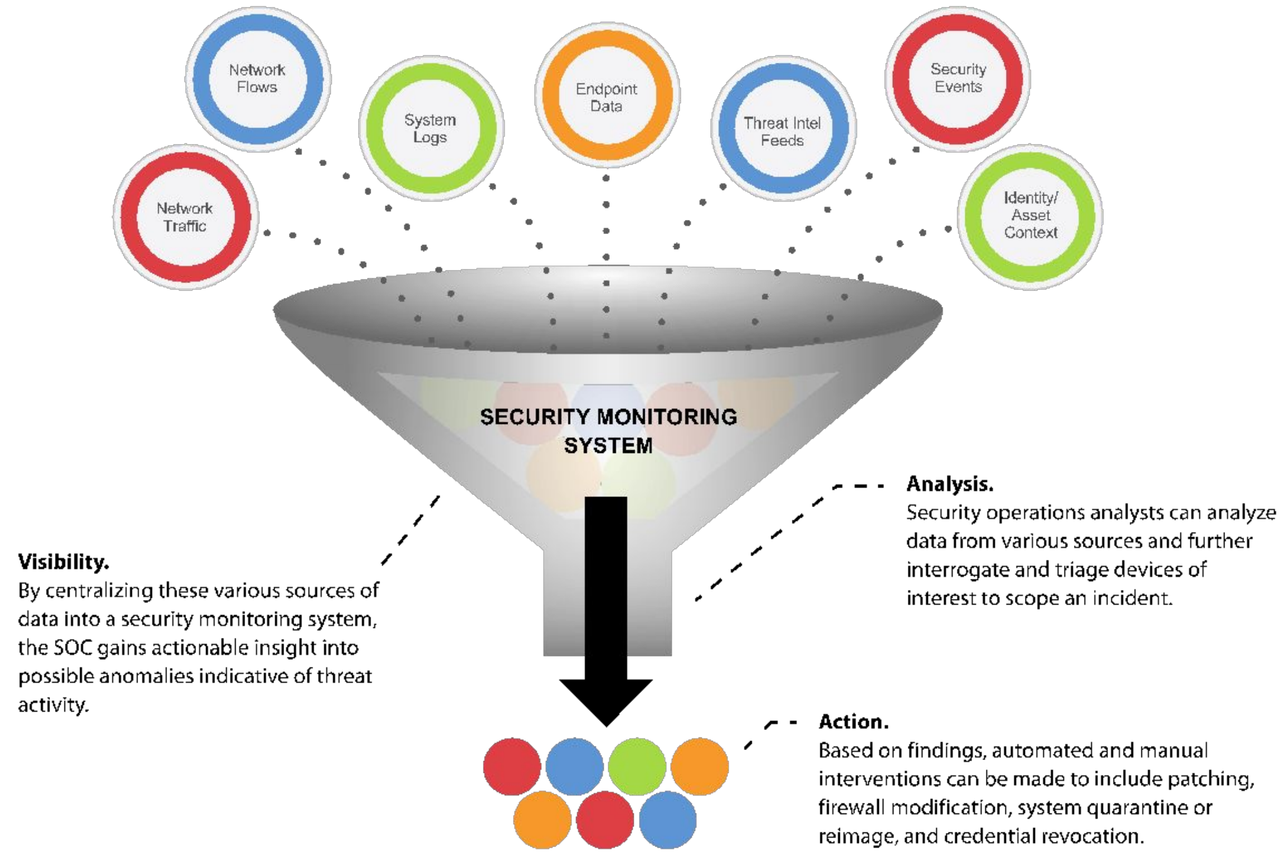
- Managing the SOC team and ensuring efficient workflows
- Ensuring incidents are handled in a timely and effective manner
- Coordinating with external stakeholders and other departments
- Strategic planning to improve SOC capabilities and address new security challenges

Levels of Responsibility

- First Level (Tier 1): Rapid, front-line alert monitoring and triage
- Second Level (Tier 2): Detailed incident investigation and escalation
- Third Level (SMEs/Hunters): Specialized expertise for complex and advanced threats

Purpose
This structure ensures a layered approach to cybersecurity, enabling efficient handling of threats from detection to resolution. Each role contributes to a cohesive SOC workflow, enhancing the organization’s overall security posture

Data Aggregation for Improved Incident Handling



Visibility.
By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

Analysis.
Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Action.
Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

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.

A SOC is critical for organizations dealing with high-risk data, experiencing growth that outpaces their existing security infrastructure, or requiring enhanced monitoring and response capabilities to safeguard against evolving cyber threats. It ensures a proactive and structured approach to information security

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

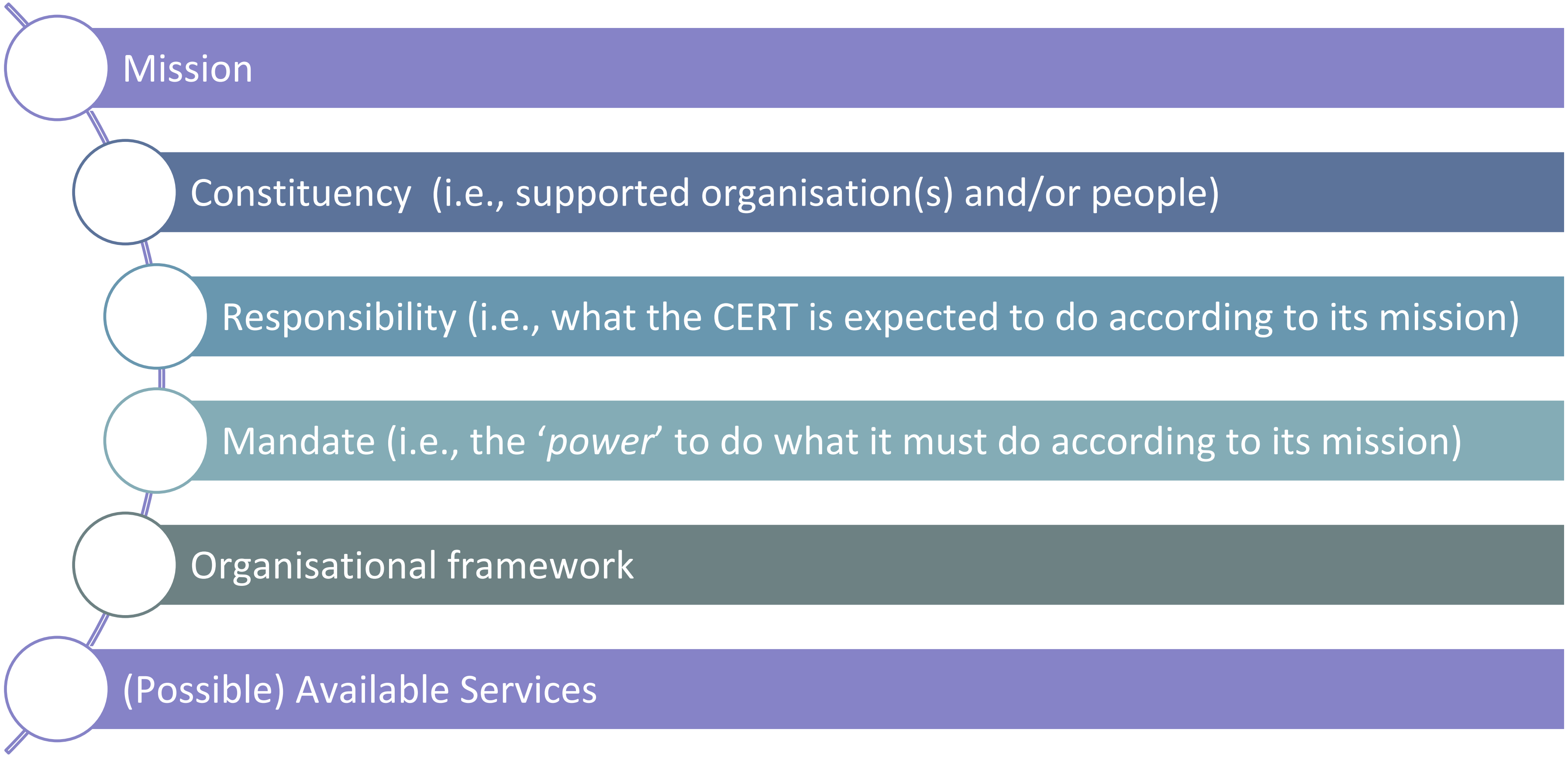
also called

- 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

Mission of a CERT

It focuses on enhancing security and resilience against cybersecurity threats.

1) Incident Response and Management: Mitigate and contain cybersecurity incidents.
2) Vulnerability Analysis and Coordination: Identify and address software vulnerabilities.
3) Threat Intelligence and Information Sharing: Provide actionable information on threats.
4) Proactive Security Support: Promote best practices and security preparedness.
5) Collaboration and Coordination: Foster partnerships with stakeholders to strengthen defenses.
6) Research and Development: Advance tools and methods to combat cyber threats.

Core Goal: Enable organizations to anticipate, withstand, and recover from cyber incidents.

Constituency of a CERT

The constituency of a CERT refers to the group or entities it serves in cybersecurity matters. This defines the scope and responsibilities of the CERT.

1. **National CERTs**: Serve governments and public infrastructure.

2. **Sector-Specific CERTs**: Focus on industries like finance or healthcare.

3. **Organizational CERTs**: Support individual organizations or corporations.

4. **Regional CERTs**: Serve a geographic region or multiple countries.

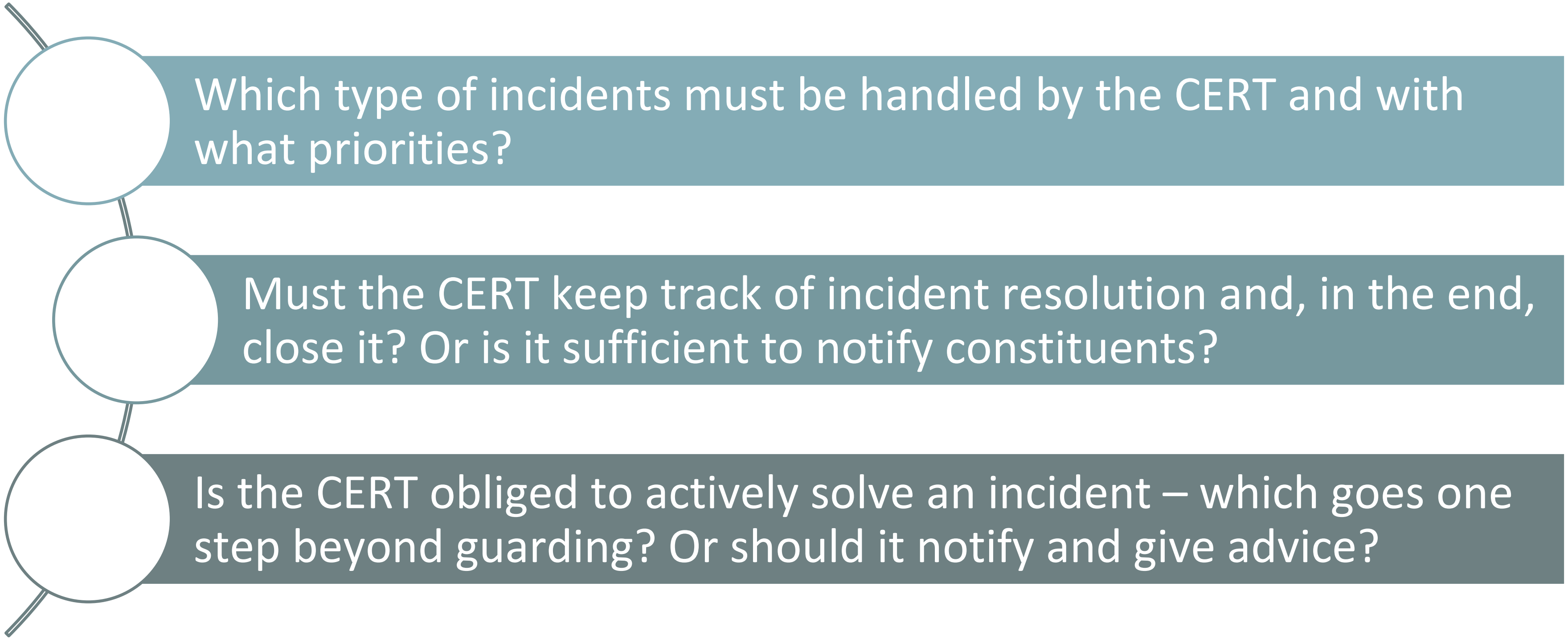
5. **Academic CERTs**: Focus on universities and research institutions.

6. **Military CERTs**: Serve defense and armed forces organizations.

7. **Specialized CERTs**: Focus on niche areas like malware or threat intelligence.

CERT: Responsibility

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



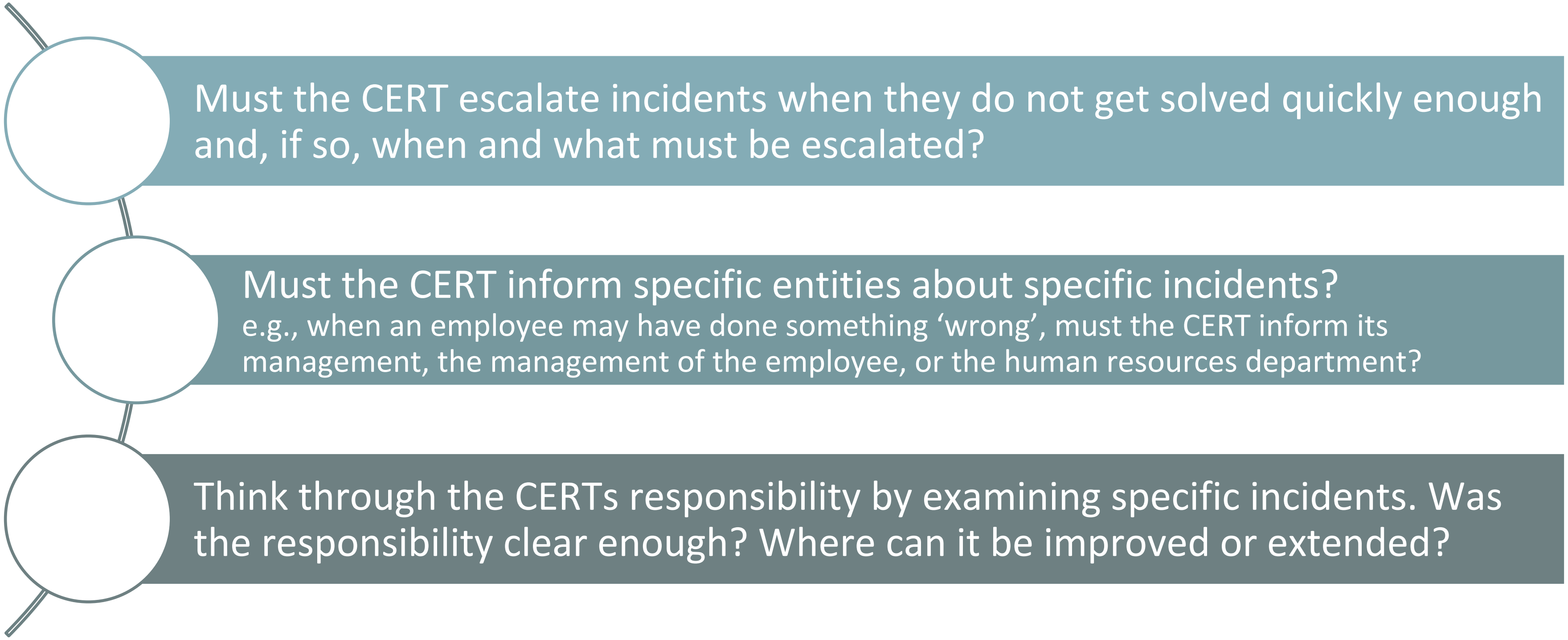
Which type of incidents must be handled by the CERT and with what priorities?

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:



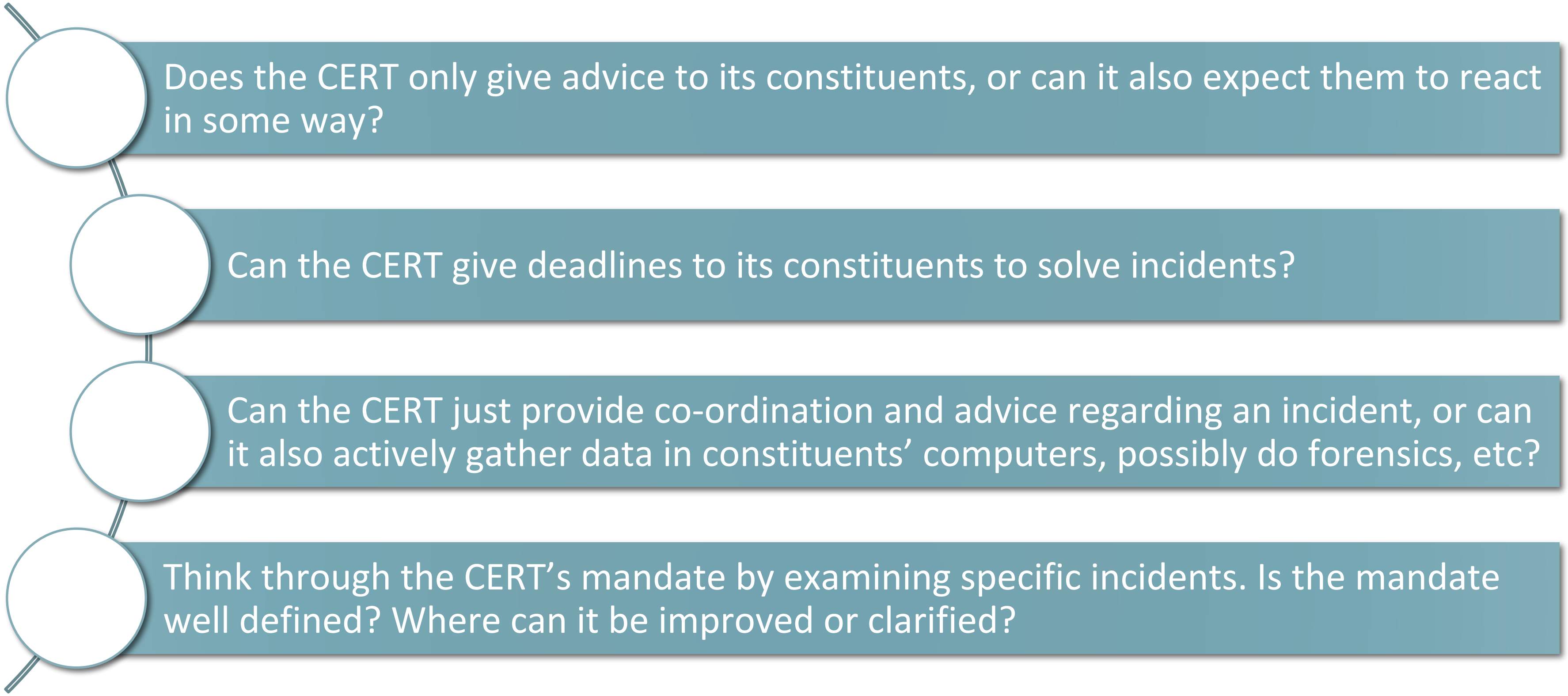
Must the CERT escalate incidents when they do not get solved quickly enough and, if so, when and what must be escalated?

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:



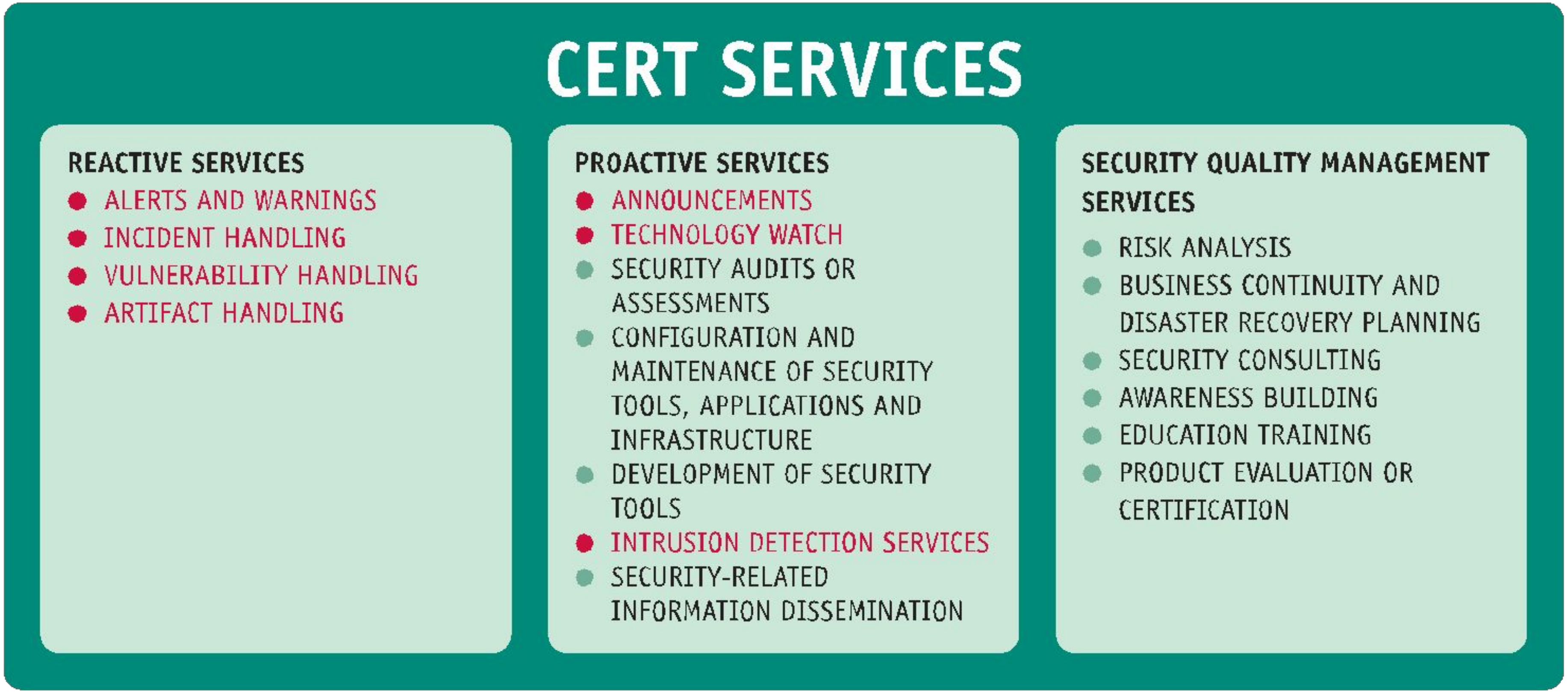
- Does the CERT only give advice to its constituents, or can it also expect them to react in some way?
- Can the CERT give deadlines to its constituents to solve incidents?
- Can the CERT just provide co-ordination and advice regarding an incident, or can it also actively gather data in constituents’ 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

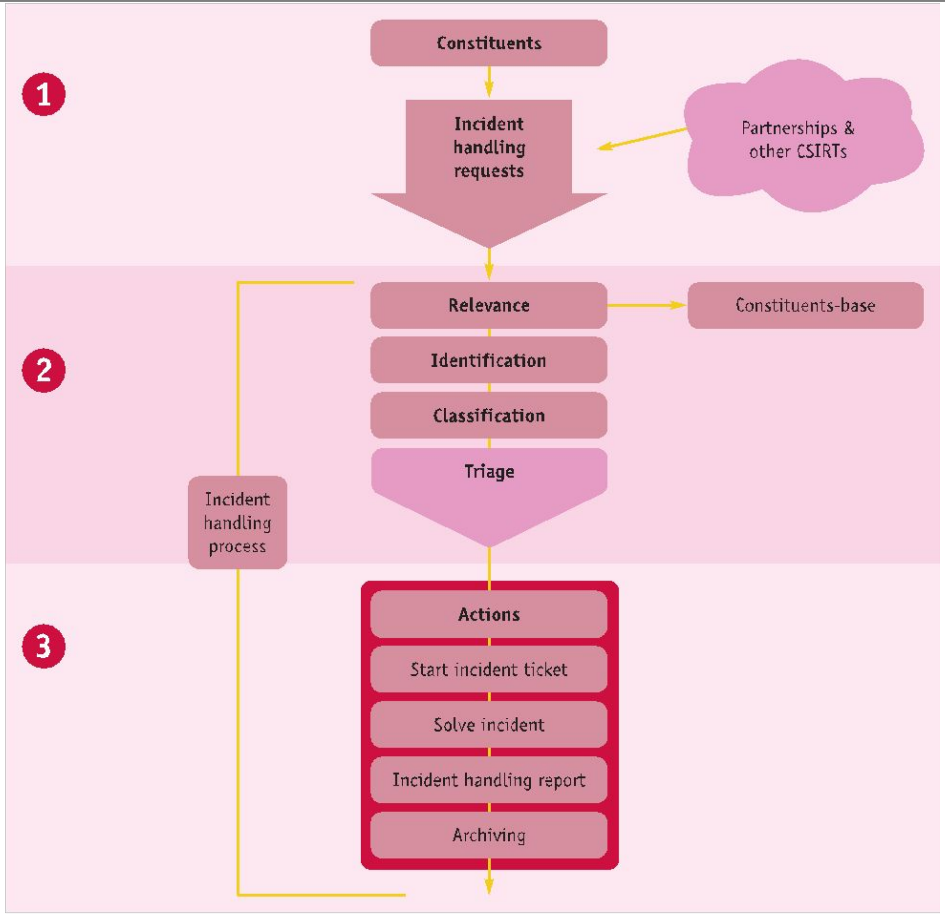


Figure 4 – Incident handling process flow

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

IM Workflows

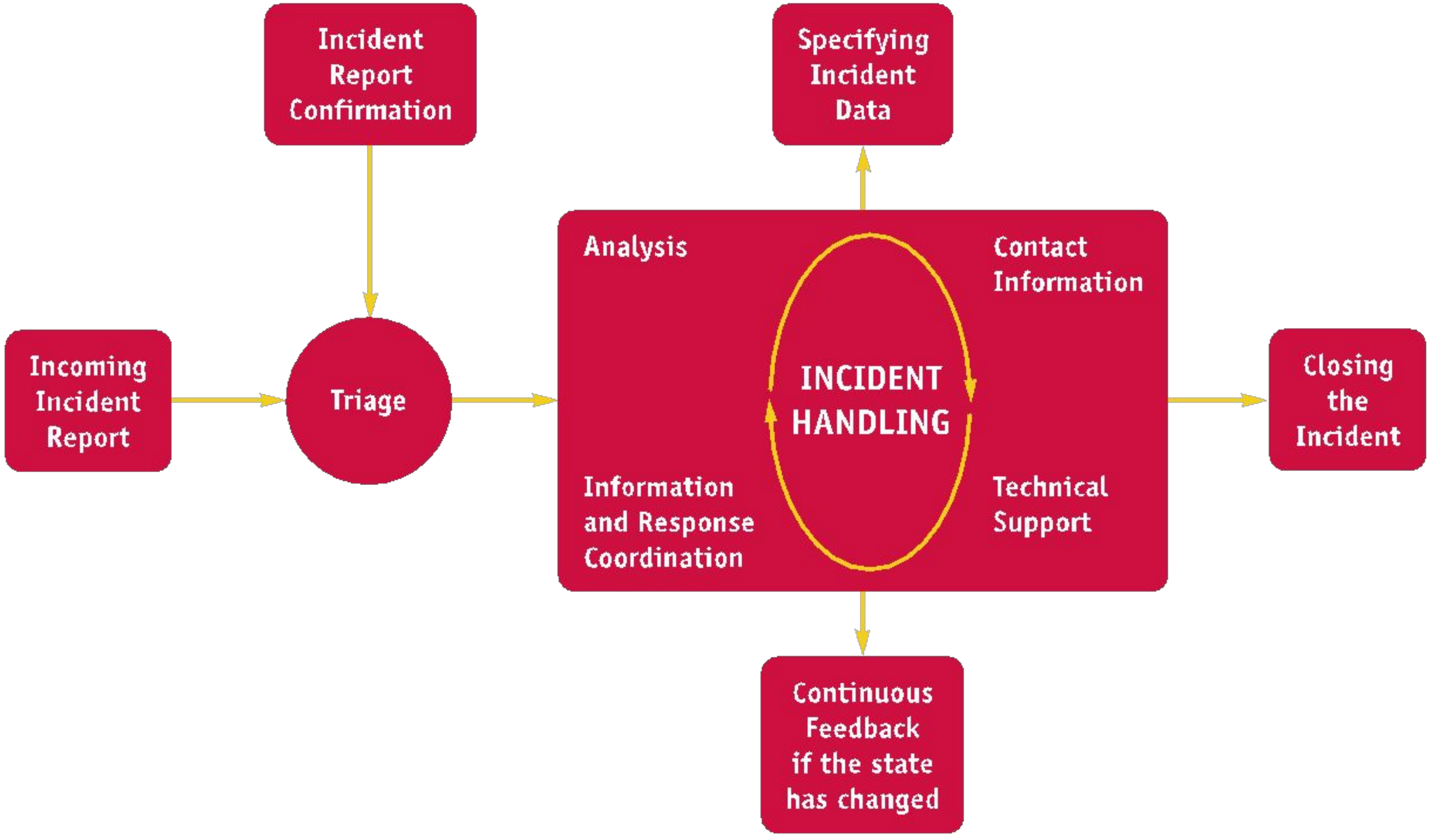


Figure 5 - Incident handling process flow (CERT Hungary example)

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

IM Workflows

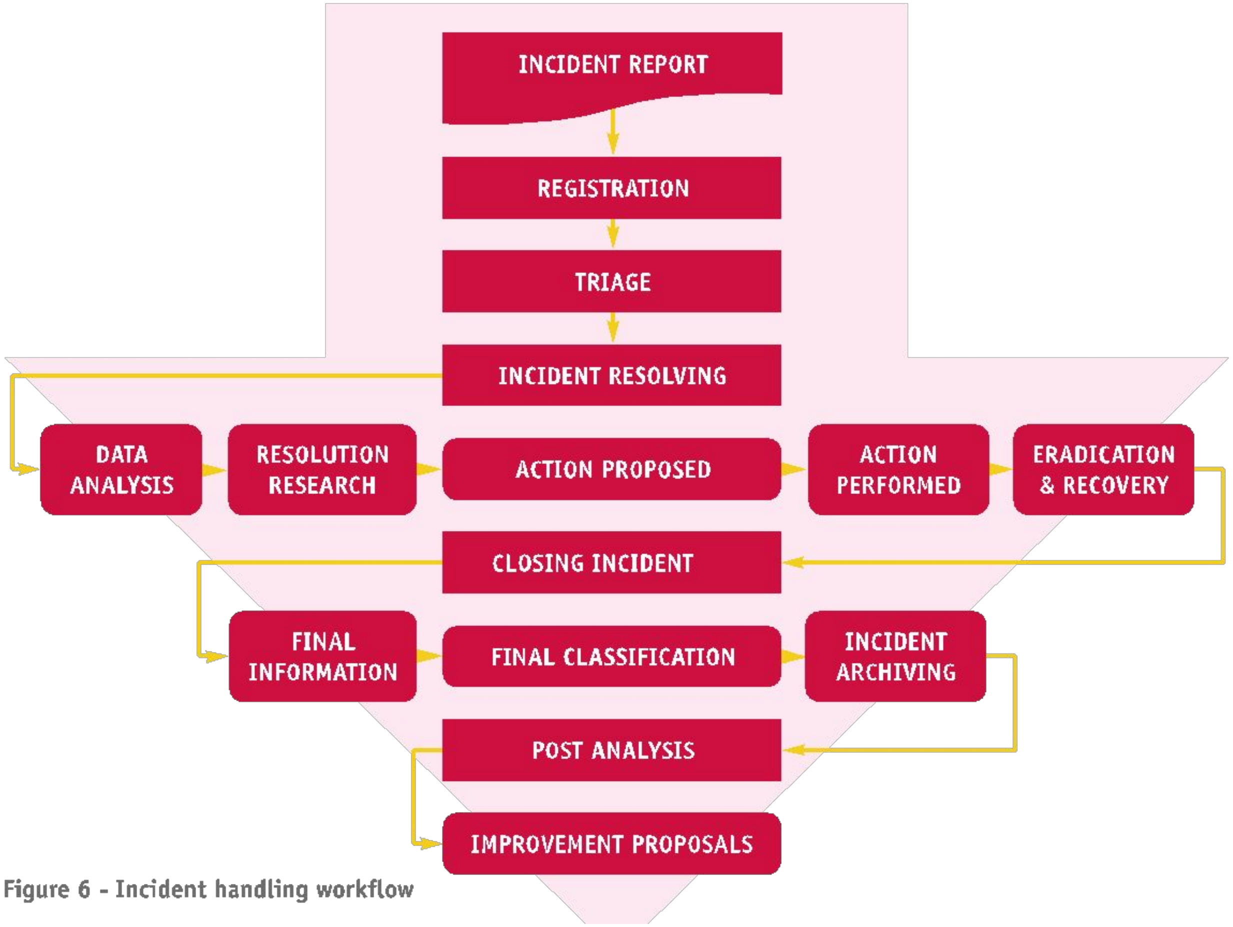


Figure 6 - Incident handling workflow

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

IM Workflows

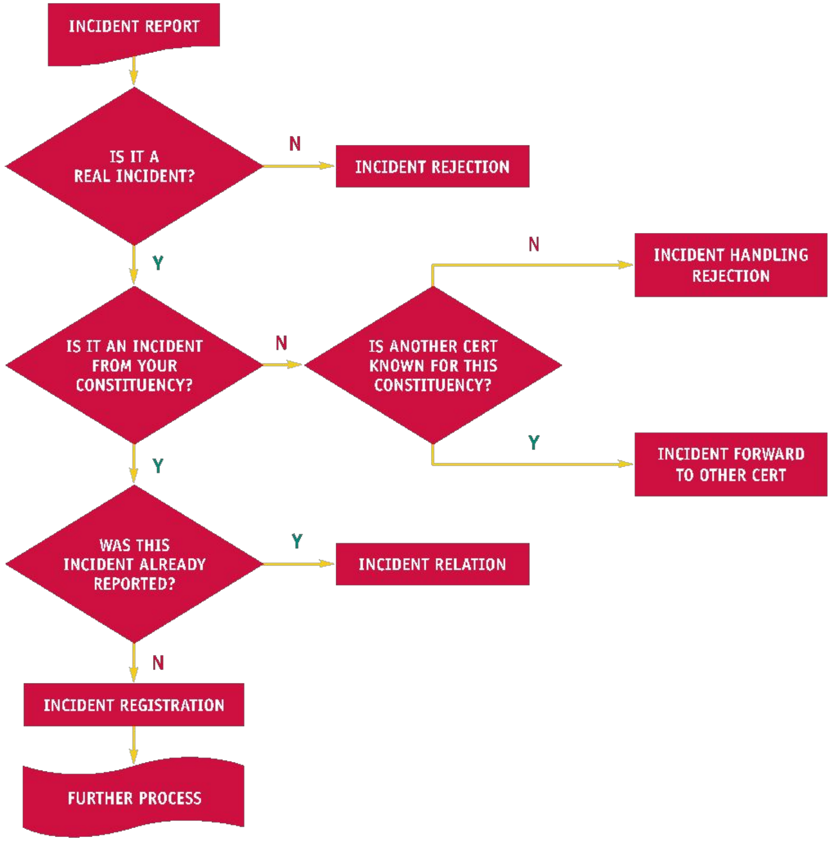
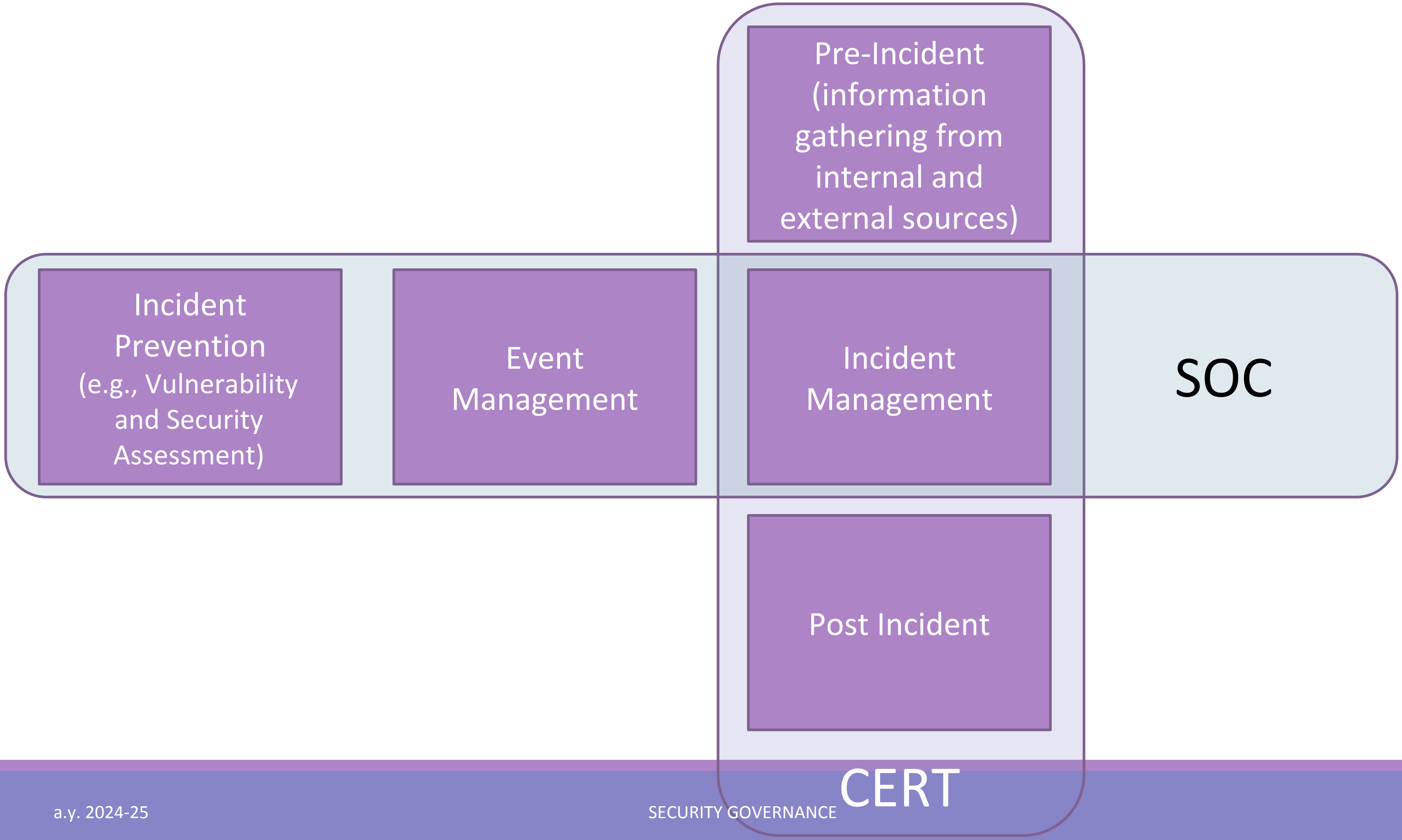

INCIDENT REPORT
IS IT A REAL INCIDENT?
N
INCIDENT REJECTION
Y
N
INCIDENT HANDLING REJECTION
IS IT AN INCIDENT FROM YOUR CONSTITUENCY?
N
IS ANOTHER CERT KNOWN FOR THIS CONSTITUENCY?
Y
INCIDENT FORWARD TO OTHER CERT
Y
WAS THIS INCIDENT ALREADY REPORTED?
Y
INCIDENT RELATION
N
INCIDENT REGISTRATION
FURTHER 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 https://www.tahawultech.com/sans/assets/docs/WP-building-world-class-security-operations-center-roadmap-35907.pdf

2. ENISA – BEST PRACTICES FOR CYBER CRISIS MANAGEMENT https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf

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/