

Security operations and Incident Management

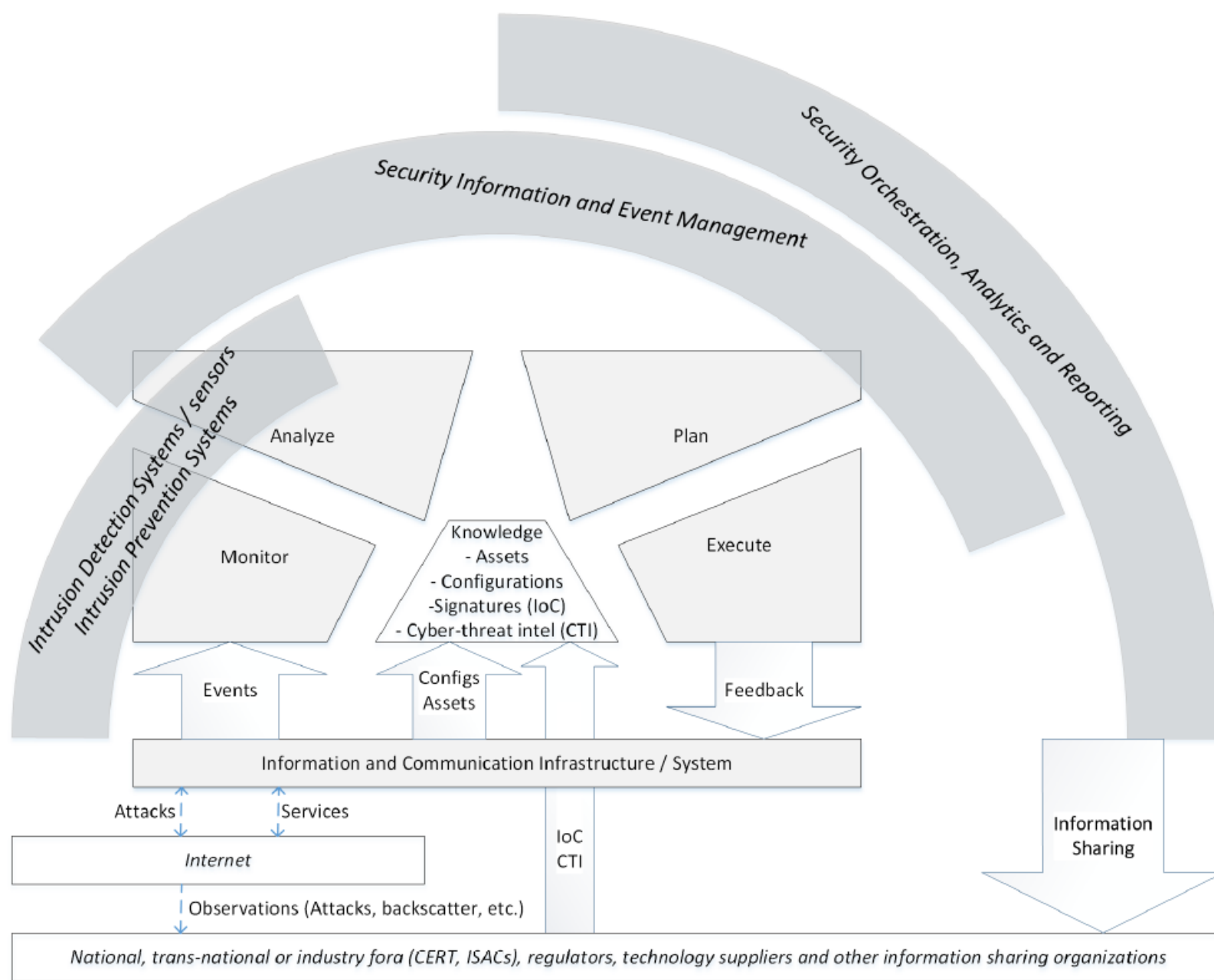
Basic concepts

- 1981 James Anderson:

Full protection of the information and communication infrastructure **is impossible**.

It would require **complete** and **ubiquitous control** and certification, which **would block or limit** usefulness and **usability**.

-> use of detection techniques

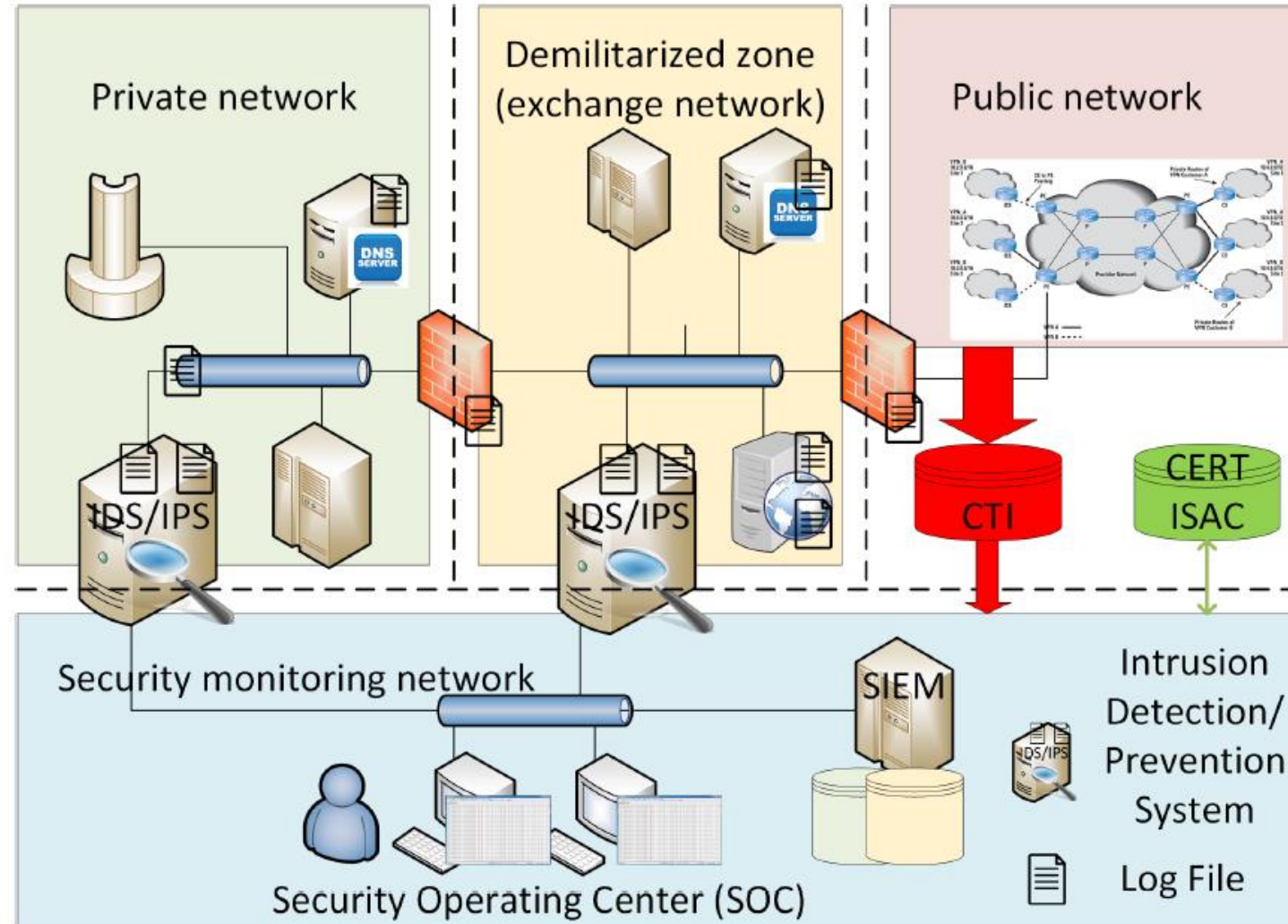


MAPE loop for Security Operations and Incident Management

MAPE loop for Security Operations and Incident Management

- The Internet is the source of both **service requests** and **threats**, but also **information** about these threats.
- **Regulatory bodies** such as national agencies, and **industry bodies provide** additional **threat and detection information** and **request information** sharing.
- 3 partial loops:
 - *Intrusion Detection Systems* (IDS), covering monitoring and detection. Technology has evolved to a point where IDS-es have been transformed into *Intrusion Prevention Systems* (IDPS).
 - Monitor and Analyse activities
 - *Security Information and Event Management* (SIEM) platforms, extends detection and covers response planning and execution. They provide both additional analysis and initial planning to respond to attacks. These platforms together form the *Security Operating Center* (SOC), providing both technological and human resources.
 - Plan and Execute activities
 - *Security Orchestration, Analytics and Reporting* (SOAR) platforms have driven further analytics and responses, provide more global information exchange.
 - Risk and Incident Management

Architecture

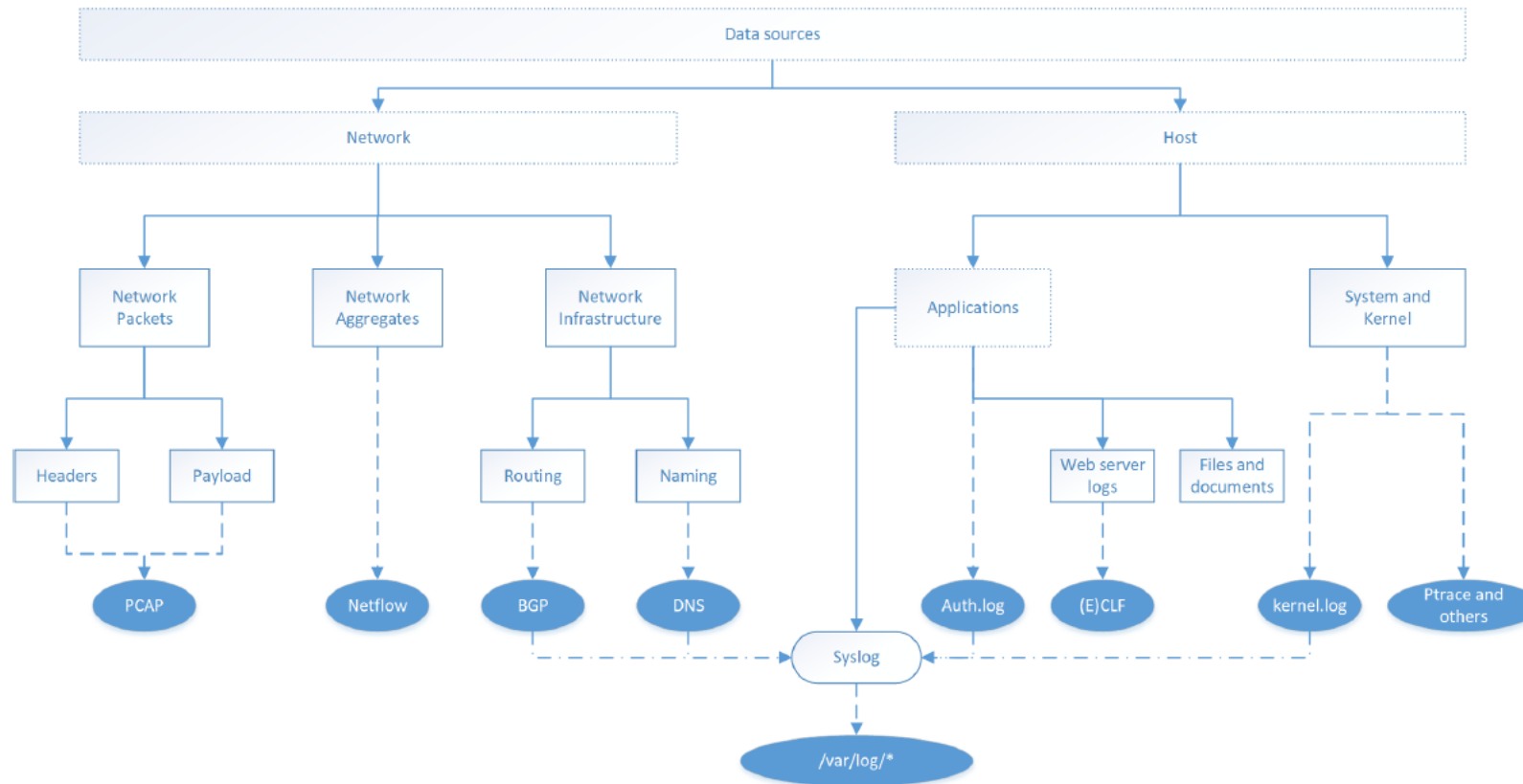


Architecture

- Attacks from the Internet cannot be blocked by protection mechanisms such as firewalls.
- **Demilitarised Zone (DMZ)** located between the inside private network and the outside Internet, to serve as communication termination, exchange and increased scrutiny through monitoring.
- IDPS sensors can use system or application **log files**, or they are deployed at the network level.
- The sensors often have at least two network attachments: one for **IDS/IPS** and one for **SIEM**.
- **Analysts man** consoles to receive alerts, assess their impact and deploy the appropriate mitigation actions.
- Security Orchestration, Analytics and Reporting components are included through the **Cyber-Threat Intelligence (CTI)** and **Information Sharing and Analysis Center (ISAC)** to obtain **information from external, relevant sources** and to leverage this information to increase their detection efficiency and impact assessment. **CERT and ISAC** entities are trusted organisations governed by regulations. CTI information is provided by commercial companies.

Monitor

- Objective is to **detect localised attempts** to compromise ICT infrastructures in real time from a continuous stream of data. The rectangles describe **concepts**. The ovals describe **concrete implementations** of these data sources.



Monitor

- Data sources broadly describe either host behaviors reporting on **operating systems or applications**, or network behaviors reporting **communication patterns**.
- Data sources are event streams, traces of activity.
- Data sources are inputs to sensors, which produce alerts as outputs. Alerts represent information of interest from a security perspective.
- The most prevalent type of network traffic data is the **full packet capture** (e.g. Wireshark, Pcap)
- **Network aggregates** are mechanisms for counting packets sharing certain characteristics, such as source, destination, protocol or interface. These counts are performed by network equipment as packets cross their interfaces. (e.g. Netflow)
Visualising network communications and relationships. Visual analytics provide a user-friendly way of understanding anomalies and their impact.

Monitor

- The **naming and the routing infrastructure**, are also of significant interest for both attacks and detection.
- Operators who participate in routing and naming usually rely on syslog to collect information.
- Naming: meaningful bits of text, to IP addresses required for network communications but which are difficult to remember.
- Application logs provide an event stream that documents the activity of a **specific application**.
- As **server logs** are written once the request has been served by the server, the attack has already occurred when the sensor receives the log information.
- Another source of application-level information that is particularly interesting and can be found both in transit (in networks) or at rest (in systems) comprises the **documents** produced by some of these applications. -> include malware
- **Operating systems generally provide logs** for debugging and accounting purposes. -> specific audit trail to generate a trace of privileged user activity
- **Kernel logs** now focus on monitoring the internal operations of an operating system, close to the hardware.

Analyse

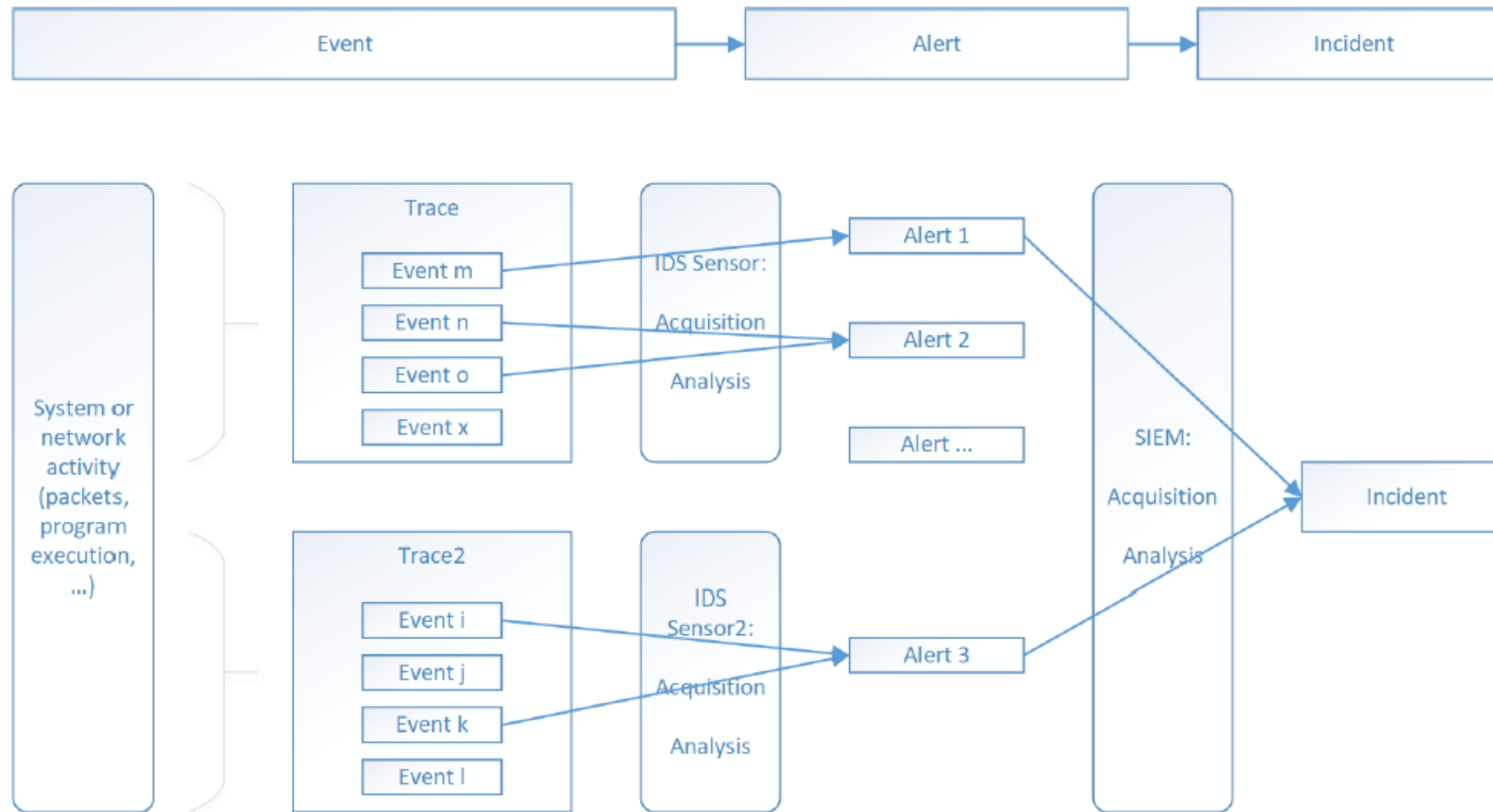


Figure 8.4: Analysis: from event to alert to incident

Analyse

- Collected traces are analysed according to different strategies that aim to separate 'good' events from those that indicate attacks.
- Two families of data analysis techniques (most of the case they are blended)
 - **Misuse detection**: characterise malicious behaviours present in the traces in order to send an alert when the set of malicious behaviour events is recognised in the traces
 - **Anomaly detection** aims to characterise 'normal' behaviour, and sends an alert when events in traces are not associated with normal behaviours.
- A way of mixing anomaly and misuse detection is using machine learning techniques, and particularly supervised learning.

Plan

- Security Information and Event Management form the core of the contribution to the Plan activity.
- Decision support system covers the Analyse and Plan activities.
- SIEM platform **collects** and **centralises** information coming from multiple sensors into a single environment.

Tasks:

- Secure data collection
- Suitable data interpretation
- Alert correlation

SIEM platform

- There must be a communication channel between the sensors providing the alerts and the SIEM platform. This communication channel must be strongly protected, because sensitive information may be included in the alerts. It must also be properly sized so that there is sufficient bandwidth to carry the required information.
- The SIEM must be able to interpret the information provided by the sensors in a coherent manner. The general approach of a SIEM platform is to define a single data structure for the alerts, often a single database table.

Alert correlation

- Alert correlation aims to make sense of the alert stream received by the SIEM platform.
- Objectives:
 - to reduce the number of alerts that the analyst has to process by grouping alerts together,
 - to add contextual elements to enable more accurate and faster analysis of the group of alerts,
 - to add alerts to ongoing higher-level planning and mitigation elements so that they are handled properly, and
 - to discard alerts that are considered false positives and do not require further processing.

Execute: mitigation and countermeasures

- IDPS sensors have been rapidly extended to include Execute capabilities to respond to attacks.
- The ability to act as a gateway or proxy through which all exchanges will be analysed.
- IDPSes are positioned inline in the network, to couple detection and firewalling. If malicious activity is detected by the sensor, the packet is immediately dropped or rejected, or the connection is terminated.
- The advantage of this solution is that attacks are handled at line rate, as soon as they occur. Of course, FP and FN of the detection mechanism will have a direct impact on the efficiency of the IDPS, denying service to legitimate users or letting attacks go through undetected.
- E.g. Web Application Firewalls

Knowledge

- The CTI platform replaces and includes honeypots to provide a comprehensive view of malicious activity that may impact an organisation.
- CERTs and ISACs are regulatory bodies, provide best practice for incident detection and handling.
- Vulnerability information sharing:
 - Common Vulnerabilities and Exposures (CVE) dictionary (<https://www.cvedetails.com/>)
 - Common Vulnerability Scoring System (CVSS) provides a standard way to rate the impact of vulnerabilities
 - Common Weakness Enumeration (CWE) dictionary provides a higher level structure on top of the CVE dictionary

Honeypots, honeynets

- A honeypot is a machine (a honeynet is a set of machines) which is offered as bait to attackers.
- In normal use, these machines should never be accessed by legitimate users, thus any interaction is deemed to be related to malicious use.
- <https://nki.gov.hu/cyberthreatmap/>
- By monitoring the attackers' use of the honeypot, researchers hope to obtain relevant information about attack processes and new malicious code, and to leverage this information for attack detection and mitigation.

Incident management

It defines three broad activities that an organisation must carry out, **prepare** itself for incidents, **handle** incidents when they occur, and **follow up** on incidents when they are closed.

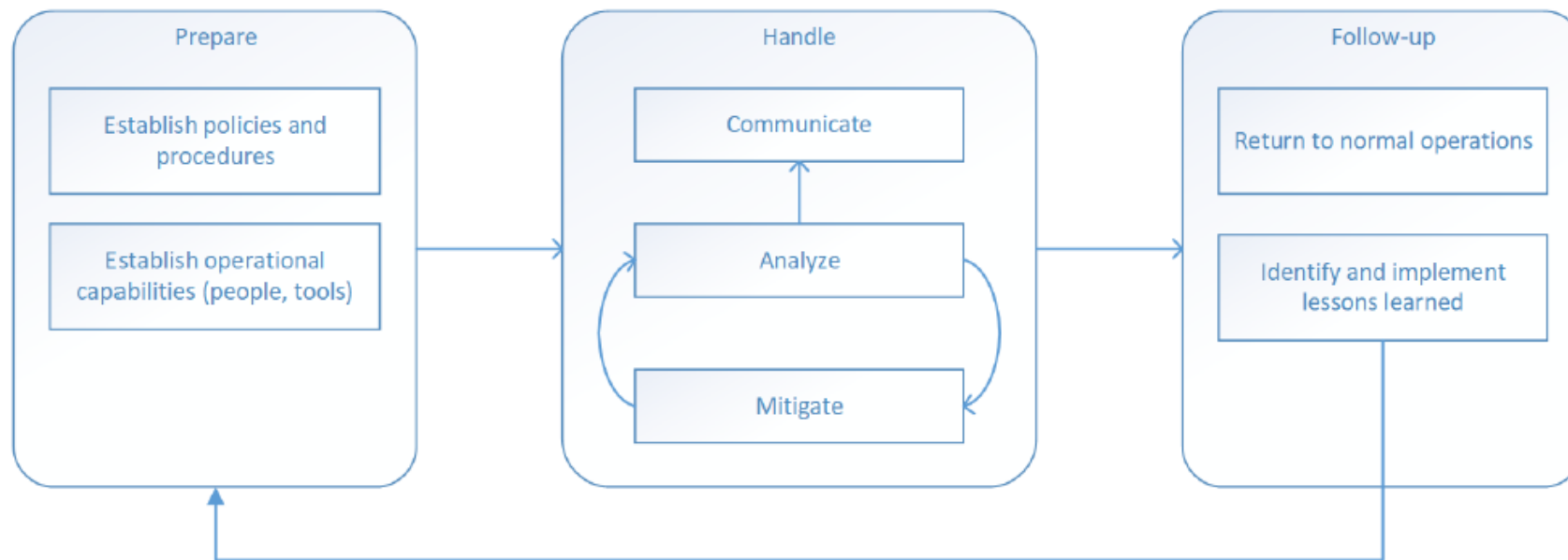


Figure 8.5: incident management lifecycle

Incident management - Preparation

- **Establishing policies and procedures** relies on the structure of the organisation and the sector to which it belongs.
- This is a legal requirement for all critical infrastructure operators, and is established by regulations such as the EU Network and Information Systems (NIS) directive.
- An important part of this preparation activity is related to communication in many forms. Incidents are **reported to the authorities**.
- Organisations should be ready to communicate when cyber-security incidents affect customers. General Data Protection Regulation (GDPR) establishes the need to **report to users** in case of information leakage.
- Preparation also includes the establishment of **a team**, usually a CSIRT.

Incident management - Handling

- Analysis is related to incident investigation, to understand the extent of the compromise and of the damage to the systems, particularly data.
 - What was compromised
 - the time the compromise occurred
- Mitigation is related to the deployment of emergency measures that can contain the incident and limit its impact.
 - blocking network accesses in certain perimeters
 - shutting down services, systems or communications
- it is necessary to alert the authorities and comply with regulations as needed.

Incident management - Follow-up

- The final step in an incident response is to verify that the full extent of the compromise has been realised and to **clean up the system**.
- Another important aspect of post-incident activities is to **measure the performance of the team and the procedures**, in order to improve them.
- The objective is to understand where and why the attack came from, and in particular the motivations of the attacker. The **impact of the incident** should be taken into account.
- Communication is also an important aspect of follow-up. Lessons learned from **incidents should impact incident training**, to ensure that responders are up to date with attacker methods.