Security measures

- Intrusion detection is positioned as one of the coherent security measures against an incident (e.g. an intrusion).
- The measures are presented using the security incident cycle, which is visualized in figure 1.

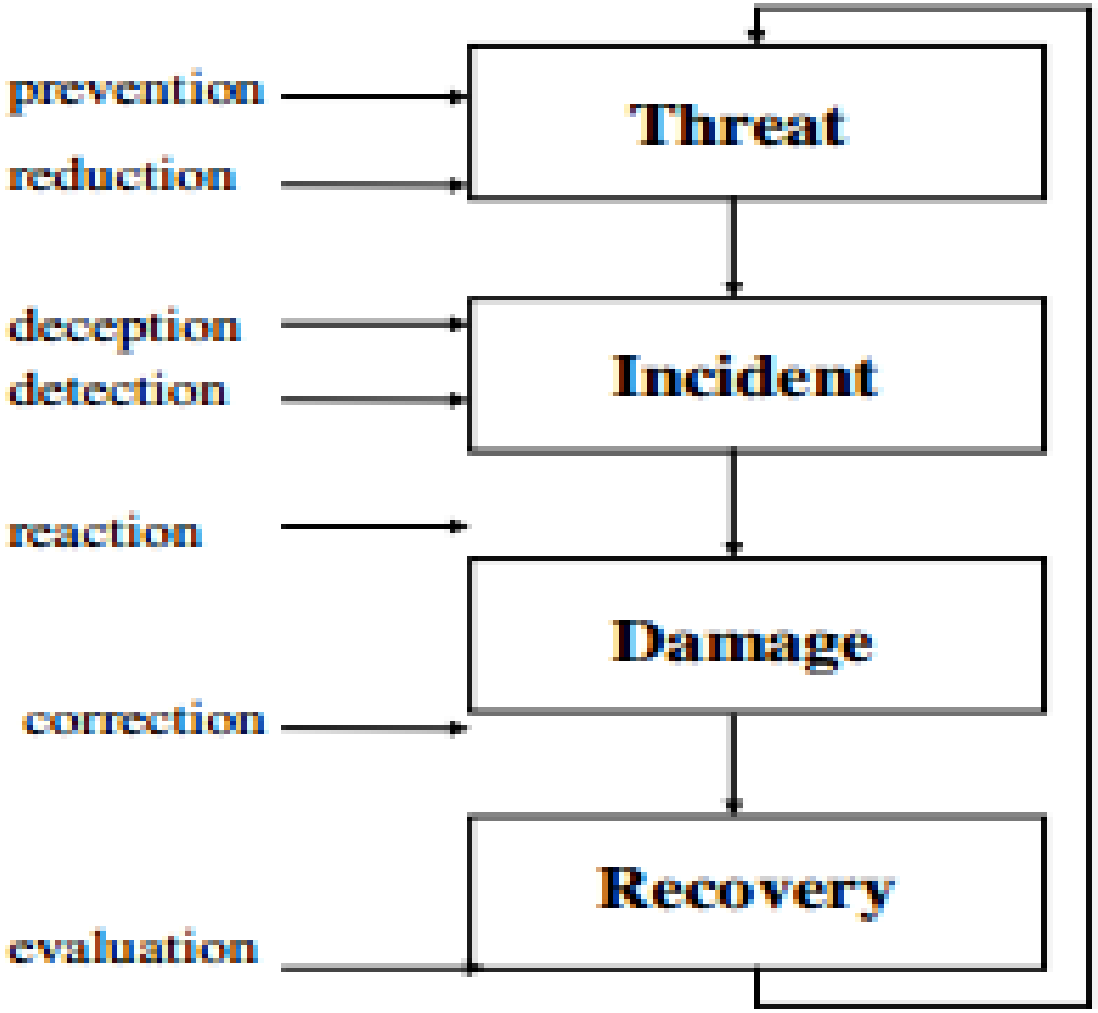


Figure 1: Security incident cycle

- The security incident cycle has to deal with threats to the confidentiality, integrity and availability
- The cycle consists of four elements:
  - the threat
  - the incident
  - the occurrence of damage
  - the recovery

- The following different types of security measures are related to these elements:
  - prevention
  - Reduction
  - Deception
  - Detection
  - Reaction
  - Correction
  - evaluation

- A defender first of all takes prevention measures.
- Example of a prevention measure to protect an internal network is a Boundary Protection Device (BPD) or scanning for known vulnerabilities and thereafter correcting these vulnerabilities by implementing patches or changing configuration parameters

- Reduction measures are measures that are performed in advance to reduce possible damage of an incident such as an intrusion.
- Examples of reduction measures are redundant systems, limitation of bandwidth, and regular back-ups

- Deception measures are a special type of security measures.
- They have the purpose to
  - give false information to intruders
  - reduce the possibility of an incident
  - to allow easier detection of an incident
  - slow intruders down
  - obtain operational benefits over the intruding party

- Prevention, reduction and deception measures reduce the probability and the impact of an incident. However, this does not exclude possible occurrence. Therefore, the defender takes detection measures

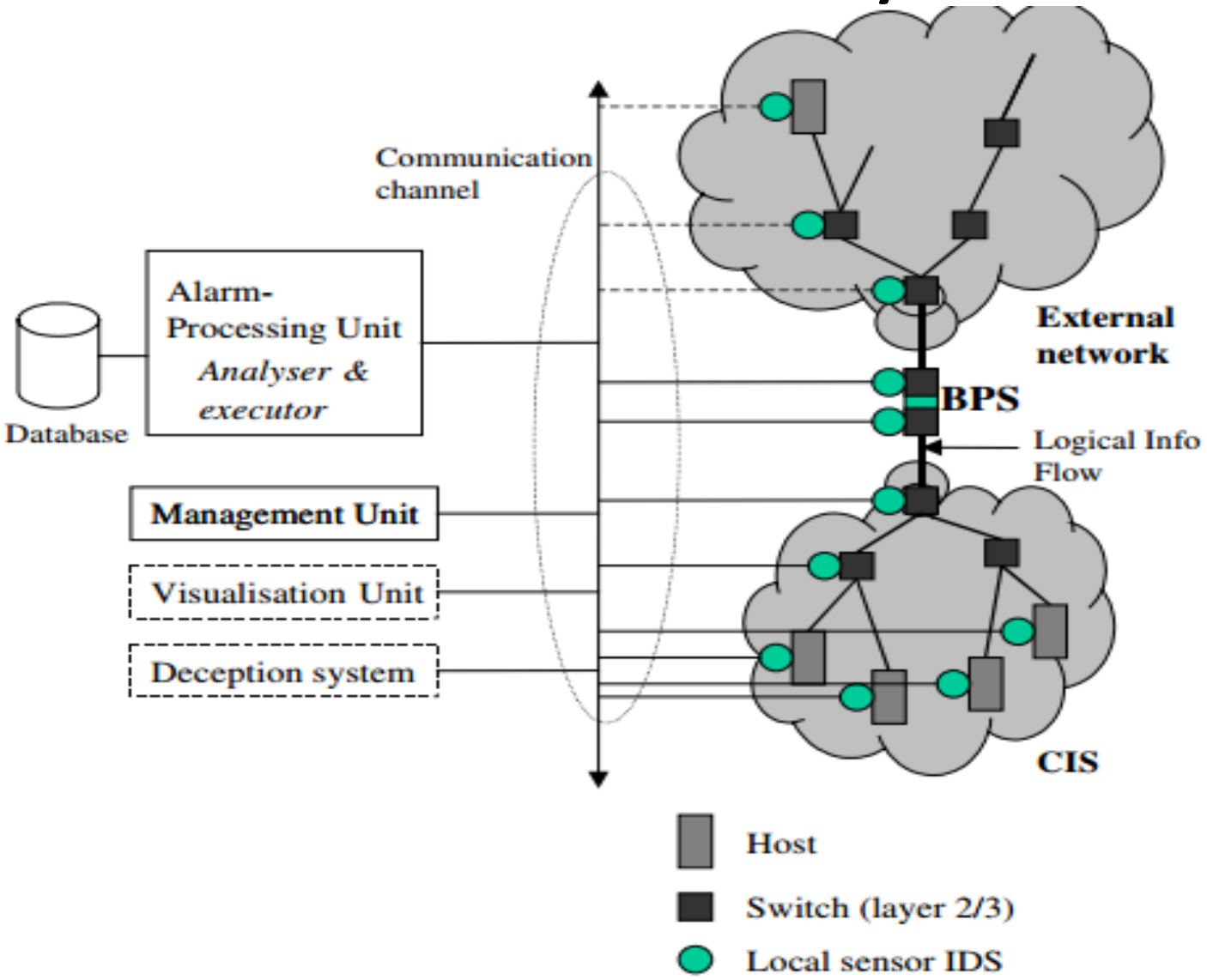
- All intrusions have to be detected as early as possible. In this way, the defender does not loose valuable time over the intruder.
- This time can be used to identify the intruder and to take more extensive prevention, reduction, and deception measures to minimize damage and to maximize the possibility for a proper reaction

- After an intrusion is detected, the defender takes reaction measures.
- These reaction measures can be repressive in order to block the repetition of the intrusion.
- The reaction measures can also include tracing an intruder.

- When an intrusion results in damage to the integrity or availability of information, the next step in the security incident cycle is to take correction measures to undo at best the damage that was done.
- The operational status of vital parts of the system has to be reconstituted as soon as possible.
- This is where reduction measures such as back-ups prove their usefulness.

- The final step in the security-incident cycle consists of an effectiveness evaluation of the security measures taken.

Distributed hierarchy of IDSs



- Each sensor consists of an IDS operating at a lower level of abstraction in the network.
- different alarm messages from a distributed IDS corresponding to different hosts can be communicated with an IDS one level of abstraction higher, by adding an extra layer to the model.

Management Unit

- The management of an IDS is divided in four categories:
  - Detection management
  - Response management
  - Update management
  - Availability management

- Detection management involves communicating with the IDSs via e.g. a graphical user interface that visualizes possible intrusions.
- Furthermore it can involve manual analysis of data by a manager, e.g. to double-check IDS alarms.

- The intrusion detection system, when it is signature or rule based, has to be updated very regularly. As we already noted, new attacks arise every moment, hence the updating of signature based IDSs is an ongoing task.
- The process of updating the system is called update management

- Availability management deals with ensuring that the system is available at all times.
- Both the hardware and software components can go out of service and then need maintenance. Furthermore, IDSs can be under a denial-of-service attack.

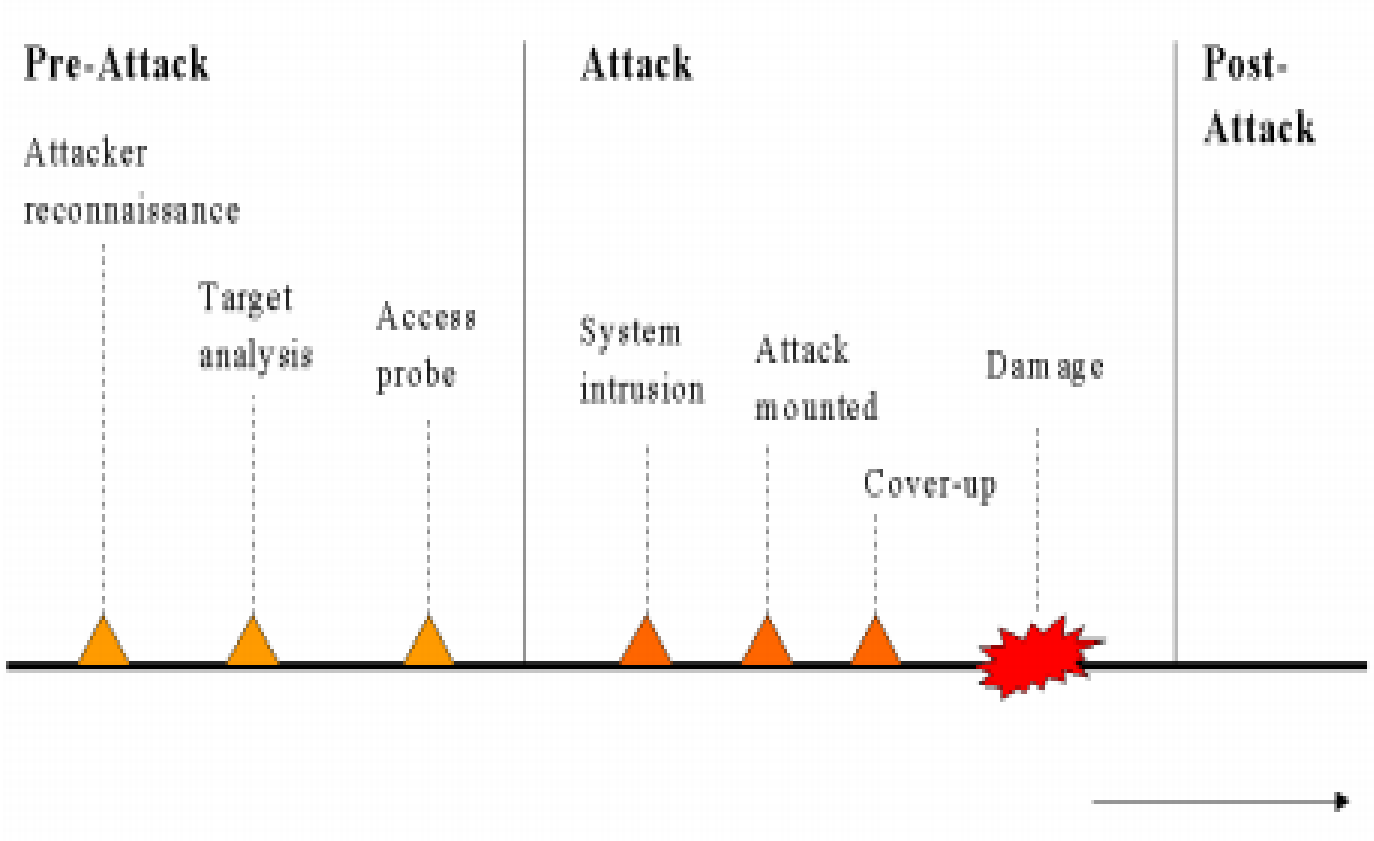
Visualisation Unit

- It can combine information of intrusions with other information such as the network (link) performance (e.g. availability and usage).
- The visualisation component can be tightly linked to an IDS alarm processor, but preferably also able to fuse information from various types of sources, such as network performance monitors

Deception systems

- These can be used to attract attackers to certain parts of the infrastructure.
- Preferably the deception system is on a stand-alone system. This has the advantage, that all network traffic directed to the system is suspicious and indicates an intrusion.
- when the attacker spends time intruding the deception system, valuable time is gained over the attacker. This time can be used to protect the real server and/or to trace the intruder.

Time axis model of an attack



- Time-axis model is used to describe the time-line of an attack.
- The actual attack is preceded by a pre-attack stage. The attacker will begin this stage by defining an end-state with regard to the target.
- This end-state is a clearly defined and obtainable objective. Desired results may be denial-of-service, acquisition of sensitive information

- After setting the objective the attacker will seek to identify and define problems associated with breaching the target defenses, gather information and make assumptions about the system.

- In the time-axis model, three steps are distinguished in the pre-attack stage:
  - attacker reconnaissance
  - target analysis
  - access probing.

- In the first step: attacker reconnaissance, the attacker starts acquiring critical information about the target.
- This includes execution of most, if not all, of the following steps: foot printing, scanning, enumeration, vulnerability mapping, and social engineering (i.e. using social skills to obtain info from employees)

- The second step: target-analysis consists of analysing the available information, making assumptions and then developing multiple course of actions (COAs).

- In the third step, access probing, the attacker tests the COA, and then selects the best COA.
- The testing is often done, by sending probes to the target or by stimulating the target.

- After the pre attack stage, the actual attack starts.
- Here, the attacker will try to cover up the operation and/or leave a backdoor (e.g. a Trojan Horse or a kernel patch) in the system.
- An attack can be very hard to recognize when the cover up operation is performed well.

- After the damage is done, the post-attack stage starts.
- This is the stage, where the defender will try to take corrective measures

- The time-axis model can be related to the incident cycle described above. Both models have a point where an intrusion leads to damage.
- Where the incident-cycle models the defender’s actions in the periods of time before and after the damage, the time-axis model shows the attacker’s actions for these two periods of time.

- The point of detection of the incident from the incident cycle can also be related to the time-axis model.
- When an attack is detected in the pre-attack stage, this is called pre-attack detection. Similarly when an attack is detected in the actual attack stage this is called attack-detection

- The detection of an attack in the post-attack stage is defined as damage detection or post-attack detection.
- IDSs should operate in a real-time manner.

- Real-time intrusion detection can be seen from two viewpoints.
  - within the boundaries of technology an alarm should be available to the response managers as soon as possible.
  - an intrusion should be detected as early as possible on the timeline of an attack.

  An important property of the analyser to achieve the latter is the ability to correlate data

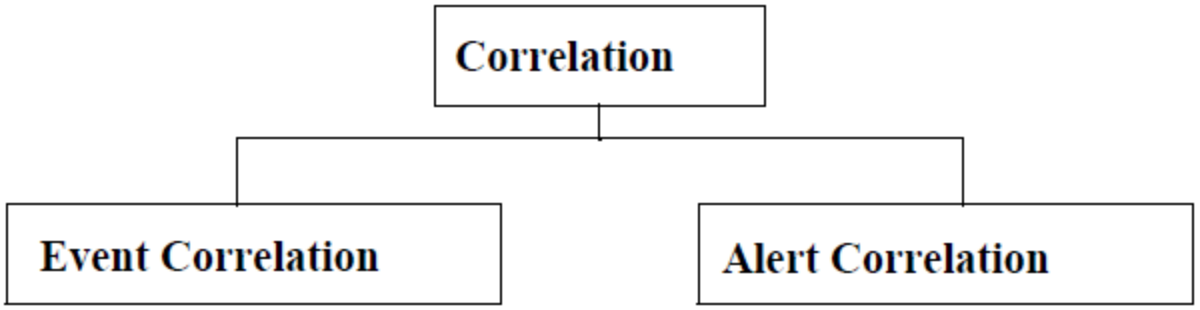
Correlation of data

- The process of interpreting, combining and analyzing the information of all available sources (such as IDS in the target, but also available information from other sources) is called correlation or fusion.

- Different sensor IDSs (located in the target or even in external network) can collect information from different stages of the attack.
- To optimally use this information for early warning the IDS should be able to correlate the information in real-time.

- This should especially include information from the pre-attack stage, since the first signs of an attack are visible in this stage.
- The information used could be in-band information or all-band information.
- In-band information is all information from activity inherent to the target system. All-band information can be any other information that can be used in the correlation, including information from human intelligence sources

- The problem of intrusion correlation can be divided into at least two sub-problems; intrusion event correlation, and intrusion alert correlation.



- Event correlation analyses neutral events, meanwhile intrusion alert correlation analyses identified misuse or anomalies.
- Generally, every time an analyzer detects an event that it has been configured to look for, it sends an Alert message to its manager(s).
- Depending on the analyzer, an Alert message may correspond to a single detected event, or multiple detected events. Alerts occur asynchronously in response to outside events

- Major problems are:
  - A common format for all-band information
  - Different confidence levels for all-band information

- Related Work:
  - IETF is developing the Intrusion Detection Message Exchange Format (IDMEF) draft standard
  - IBM has developed an Aggregation and Correlation Component (ACC), Aggregation relationships are used to group alerts into attack situations according to various selection criteria.

- A successful correlation will result in the merging of information from two or more alert messages, and the new correlated alert will become a superset of its parts.
- Sometimes the information in the various alerts may be conflicting.
- This may require special handling in the form of precedence and priority.

- Various look-up functions are used during the correlation process.
- This includes functions to translate between IP addresses and host names, port numbers and service names, and vice versa.
- Additionally, time functions are used to enable a global time base.

- One important factor during correlation is the freshness of information.
- If the look-up is not performed close enough to the event, alert or correlation, then stale information may be fed into the correlation process.