Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Early Warning System
→ Basic concept

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- Structure of EWS
- Process of EWS
- Different realization of EWS
- Summary

Content

- **Aim and outcomes of this lecture**
- Motivation of Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- Structure of EWS
- Process of EWS
- Different realization of EWS
- Summary

Early Warning System
→ Aims and outcomes of this lecture

Aims

- To introduce the motivation and the target of an Early Warning System
- To explore the structure of an Early Warning System
- To analyze the processes of an Early Warning System
- To assess the need of an Early Warning System

At the end of this lecture you will:

- Understand the meaning of an Early Warning System.
- Know the basic structure of an Early Warning System.
- Understand how the processes could be organize.
- Understand the problems that arise by developing an Early Warning System.

Content

- Aim and outcomes of this lecture
- **Motivation of Early Warning Systems (EWS)**
- Attacks
- Targets of EWS
- Structure of EWS
- Process of EWS
- Different realization of EWS
- Summary

Early Warning Systems
→ Motivation

If you can't measure it,

you can't manage it!

Content

- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- **Attacks**
- Targets of EWS
- Structure of EWS
- Process of EWS
- Different realization of EWS
- Summary

Attacks
→ General Idea

- An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

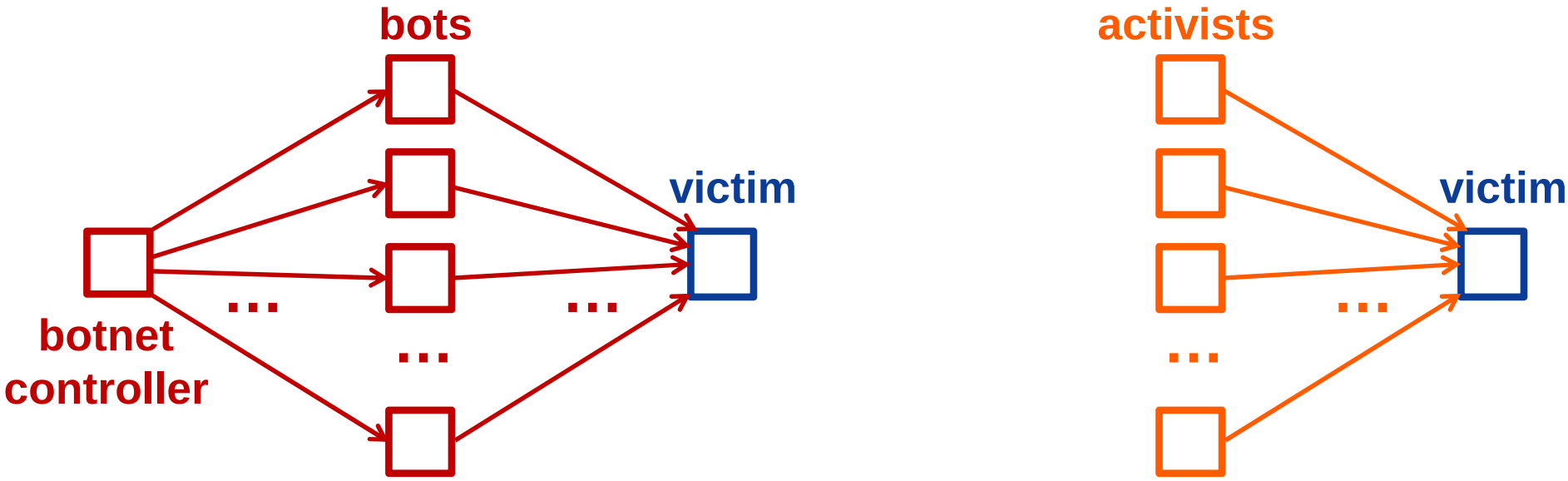
Assets

Attack structure
→ M : 1

- **Example:**
  - M attacker := bots of a botnet (insecure IT systems)

    or

    coordinated attack by activists (e.g. anonymous group)
  - 1 victim := webserver or other services

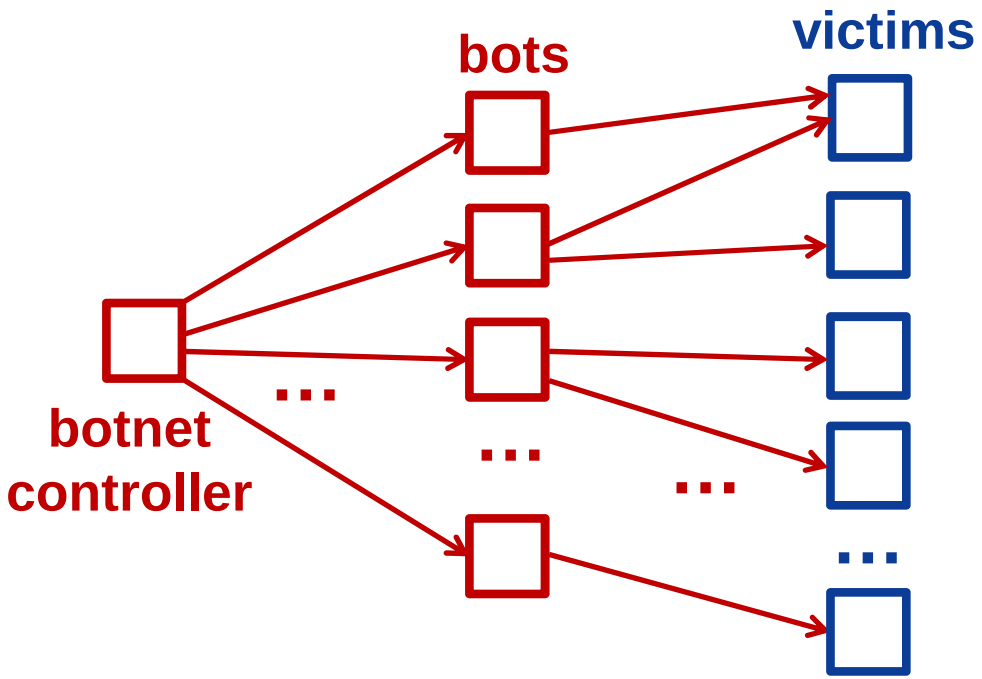


- **Type of attack, e.g.**
  - Distributed Denial of Service (DDoS), **...**

Attack structure
→ M : N

- **Example:**
  - M attacker := bots of a botnet (insecure IT systems)
  - N victims := e-mail boxes (Spam), websites (Click fraud), …

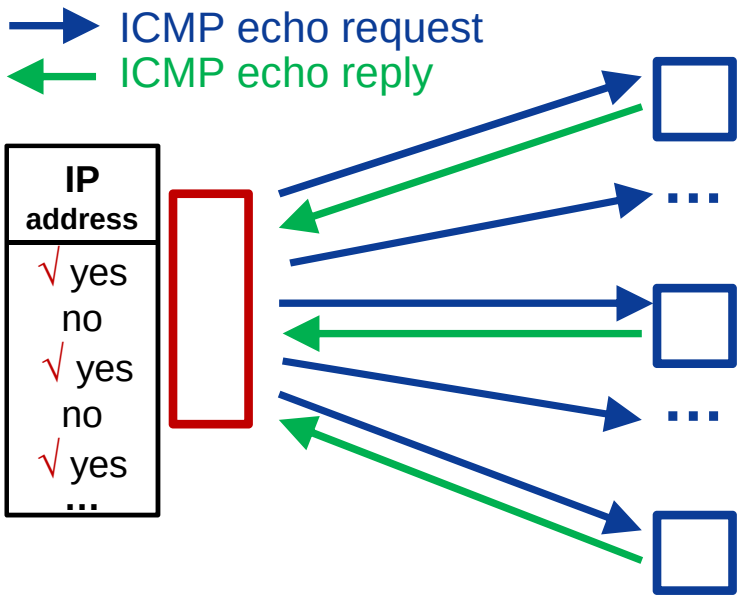
N > M



- **Type of attack, e.g.**
  - Spam (e-mail)
  - Click fraud (websites)
  - **…**

Attack structure
→ 1 : N (preparation of an attack) – 1/3

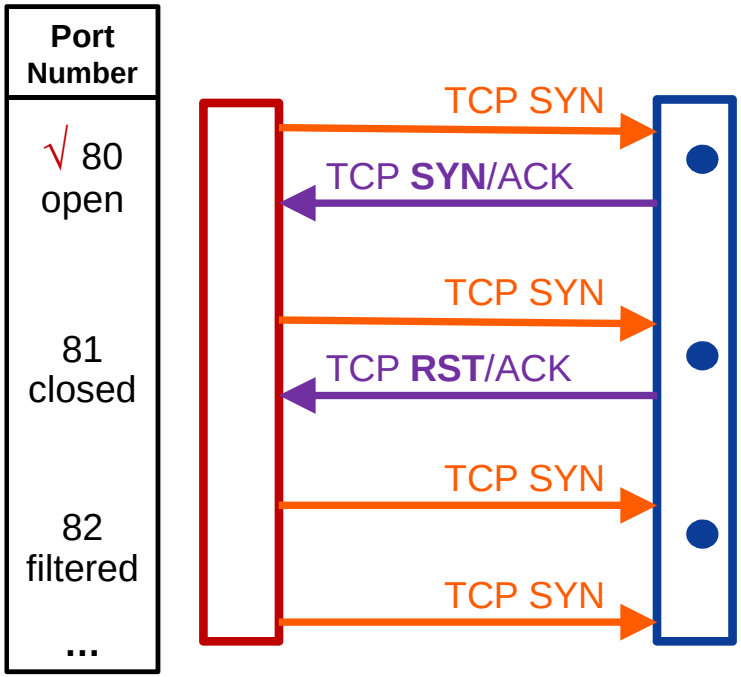
- **Example:**
  - 1 attacker := attack preparation
  - N victims := IT system in the Internet



- **Type of attack, e.g.**
  - "Ping scan"
    (to find available IT systems in the network)

Attack structure
→ 1 : N (preparation of an attack) – 2/3

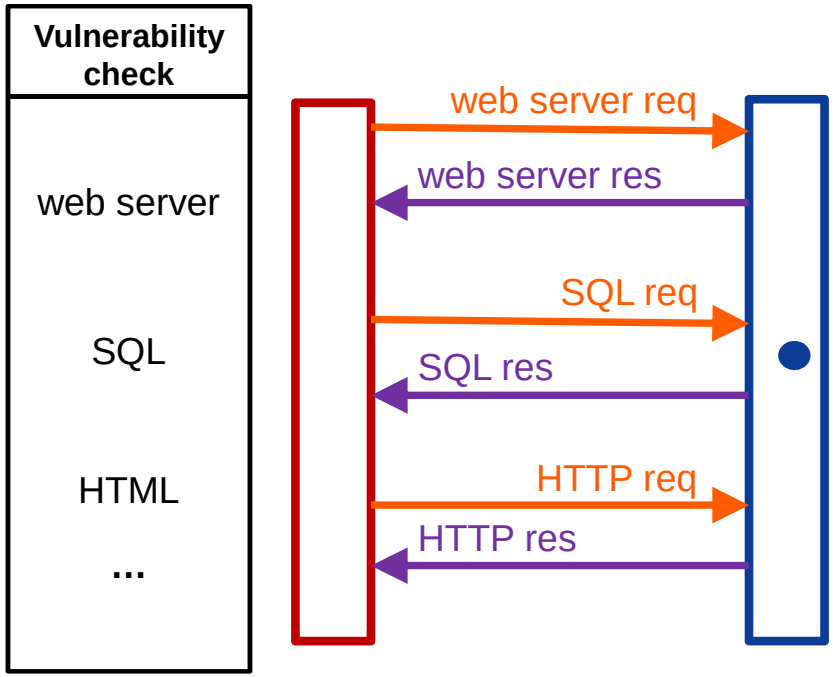
- **Example:**
  - 1 attacker := attack preparation
  - N victims := IT system in the Internet



- **Type of attack, e.g.**
  - Port scan
    (to find available services on a available IT systems)

Attack structure
→ 1 : N (preparation of an attack) – 3/3

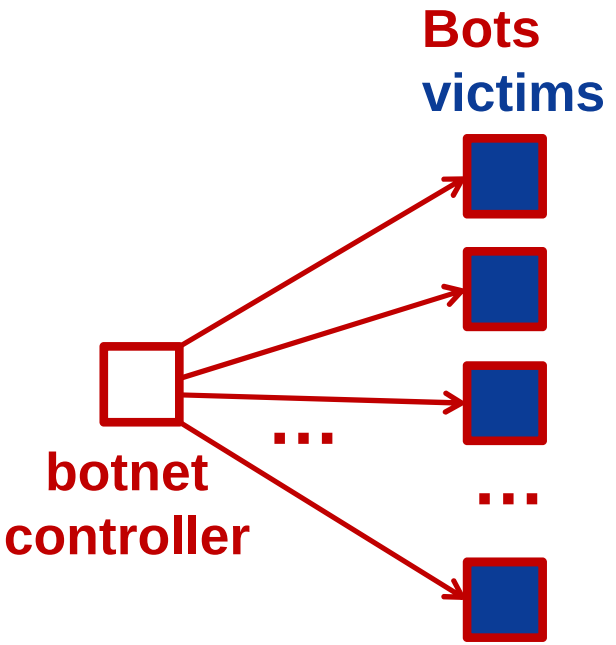
- **Example:**
  - 1 attacker := attack preparation
  - N victims := IT system in the Internet



- **Type of attack, e.g.**
  - Vulnerability scanner
    a tool used to check computers (OS, apps, DB, …) for known weaknesses.
    (to find vulnerabilities in available services on a available IT systems)

Attack structure
→ 1 : N (execute an attack)

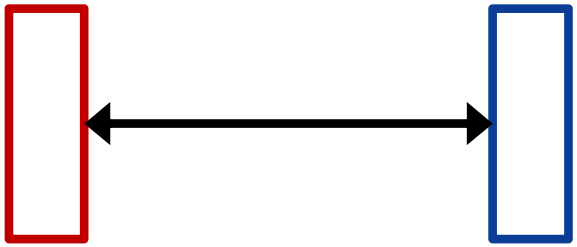
- **Example:**
  - 1 attacker := criminal organization (own or rent the botnet)
  - N victims := insecure IT systems in the Internet



- **Type of attack, e.g.**
  - Data theft (ID, PW, important information)
  - data manipulation
  - data encryption / ransom
  - **...**

Attack structure
→ 1 : 1

- **Example:**
  - 1 attacker := professional attacker performs a targeted attack
  - 1 victim := company, government organization, …
    (insecure IT systems, social engineering, …)



- **Type of attack, e.g.**
  - With the help of intelligence-gathering techniques, continuous monitoring and interaction to achieve the defined objectives of the threat (Advanced Persistent Threat - APT)

Content

- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- Attacks
- **Targets of EWS**
- Structure of EWS
- Process of EWS
- Different realization of EWS
- Summary

Early Warning System
→ Targets

- **Security** and **trustworthiness** of the used IT infrastructure of an organization must be **improved** and **developed** in a **resistant fashion.**

- To establish this, information about the **status** of the IT infrastructure is **continuously generated** and evaluated by means of an Early Warning System

- In addition, efficient reactions on incidents will be - preferably automated - initiated and implemented

Targets of Early Warning Systems
→ Functional requirements (1/3)

- **Detection of Attacks**
  - At an early stage, best before actual damage is caused
  - … but always early enough to minimize the potential damage.
  - Known and unknown attacks
- **Support** in the **decision making process** and in the **development of counteractive measures**
  - Tools for analyzing and to display results
  - Decision-making aid by the use of expert systems
- **Assistance in the collection of evidence (forensic)**
  - Collection of evidence for a later legal reaction

Targets of Early Warning Systems
→ Functional requirements (2/3)

- **Monitoring of the development of IT infrastructure**
  - How is the traffic going to develop?
  - In what direction will expand the infrustructure?
  - Which technologies will gain or loose importance in the future?

- **Creation of a IT security situation awareness**
  - Overview over all security relevant incidents
  - Appropriated methods to visualize the IT security situation awareness

Targets of Early Warning Systems
→ Functional requirements (3/3)

- **Further requirements for an Early Warning System**
  - Reliability
  - Security of the System towards attacks
  - Ensuring privacy and protection of confidence
  - Maintainability
  - Expandability
  - Performance / Scalability

Content

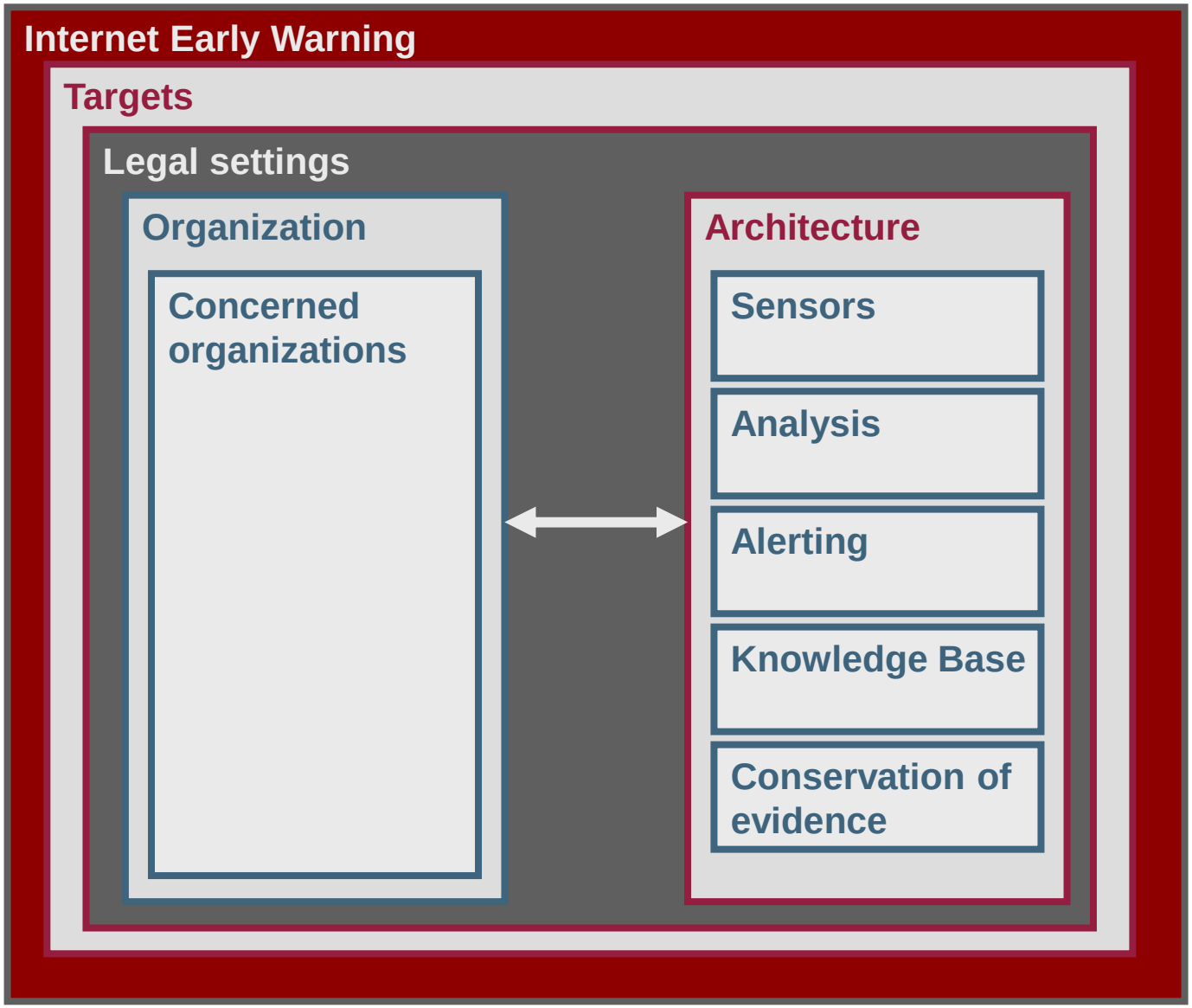
- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- **Structure of EWS**
- Process of EWS
- Different realization of EWS
- Summary

Structure of an Early Warning System → General Idea

- An Early Warning System (EWS) consists of a **number of components**

- An Early Warning System differs depending on the “environment”
  - **Targets to be achieved** by the use of an EWS
  - **Legal conditions**
  - **Partners participating** in development and operation of an EWS

Structure of an Early Warning System → Model



Structure of an Early Warning System → Abstractly phrased

$$EWS = f(I, O, L, T, E)$$

with:

- EWS := Early Warning System
- I := IT **I**nfrastructure, which is monitored
- O:= **O**rganization, definition of the relations of the concerned and of the processes
- L := **L**egal framework, which is relevant for operation
- T := **T**argets, which are aimed to be established by the use of an Early Warning System
- E := technical **E**lements of the Early Warning System

Structure of an Early Warning System → Element: IT Infrastructure (I)

- The IT infrastructure that should to be monitored
- Important due to different aspects
  - Position of the sensors
  - Distribution of the sensors
  - Spreading of failures
  - Conducting of counteractive measures
- Open Questions
  - How can the IT infrastructure of an organization be captured?
  - On which level of abstraction should the IT infrastructure be described?
  - Which are the most important components?

Structure of an Early Warning System → Element: Organization (O) – (1/2)

- Organizational structure of the Early Warning System
- Organizational and operational structure

$$O = (O_{Operational}, O_{Organizational})$$

- **Organizational structure**
  - Definition of the organizational units
    - Sensor operator, assessment centers, CERTs, operators of critical infrastructure
  - Definition of the relations between these units
  - Definition of the responsibility of the units

Structure of an Early Warning System → Element: Organization (O) – (2/2)

- **Operational Organization**
  - Definition of the processes for the operation
    - Reaction in case of an incident
    - Flow of information between organizational units

- **Important aspects**
  - Short decision processes
  - Efficient paths for information flow
  - Strictly defined responsibilities

Structure of an Early Warning System → Element: Legal framework (L)

- The legal framework has an influence on the operation of an Early Warning System
- Depending on the **legal situation** the operation might be subject to more or less **limitations**
- Relevant areas of the law
  - Privacy (data protection)
  - Protection of confidence
  - Law of contract
- The legal framework sometimes defines the ability of an Early Warning System to reach the aimed targets

Structure of an Early Warning System → Element: Technical Elements (E)

- Technical Elements of an Early Warning System

$$E = f(S, A, AL, KB, CE, AR)$$

  - S := Sensors
  - A := Analysis
  - AL := Alerting
  - KB := Knowledge Base
  - CE := Conservation of evidence
  - AR := Architecture

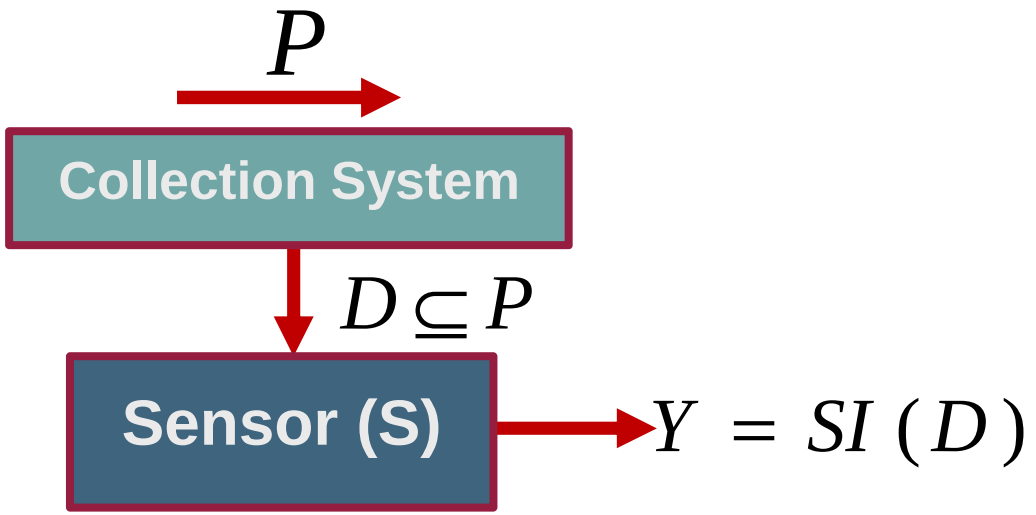
- The interaction of these technical elements offers the functionality of an Early Warning System

Technical Elements of an EWS
→ Sensor (S): Overview

- Sensor collects data, which is used to determine the current status of the IT infrastructure.
- Sensors are distributed throughout the entire IT infrastructure (I), to gain a representative overview of the IT infrastructure

- **Different types of sensors can be used:**
  - Complete recording of the network traffic (e.g. Wireshark)
  - Netflow (Router), sFlow (Switch)
  - Network sensors (statistical approach, DPI, IDS, …)
  - Network Management (e.g. SNMP)
  - Honeypots
  - Availability of services, nodes, server and components
  - LogData analysis
    (net-sys (Firewall, Router, …), …, IT-sys (App, OS, data, …), …)
  - …

Technical Elements of an EWS
→ Sensor (S) – Basic principle



- **P** := complete data
  (communication traffic, application behavior, data state, LogData, …)
- **D** := data going through the sensor
- **Y** := result of the processing conducted by the sensor S(D)
  (Y will normally send to an Analysis System)
- **Collection System** := tap, router, switch, end devices, server, …
- The **security information (SI)** content is: $SI(Y) \leq SI(D) \leq SI(P)$

Technical Elements of an EWS
→ Sensor: Optimal target

- **What is the best sensor?**
  - **very high degree of the reduction of bytes → Y <<< P**

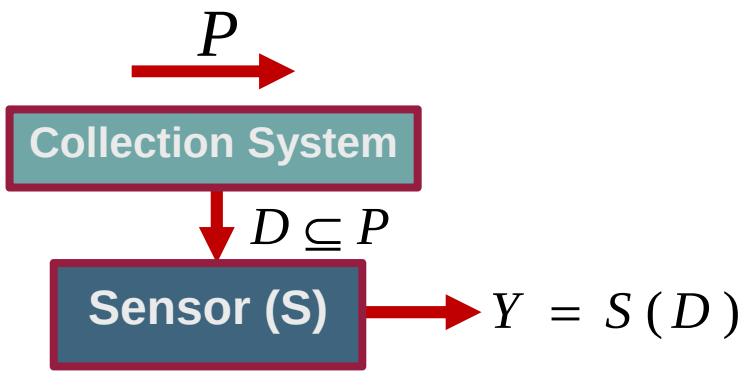
    but

  - **a small reduction of security information → SI (Y) ≤ SI (P)**

    ideal: $SI(Y) = SI(P)$

    and

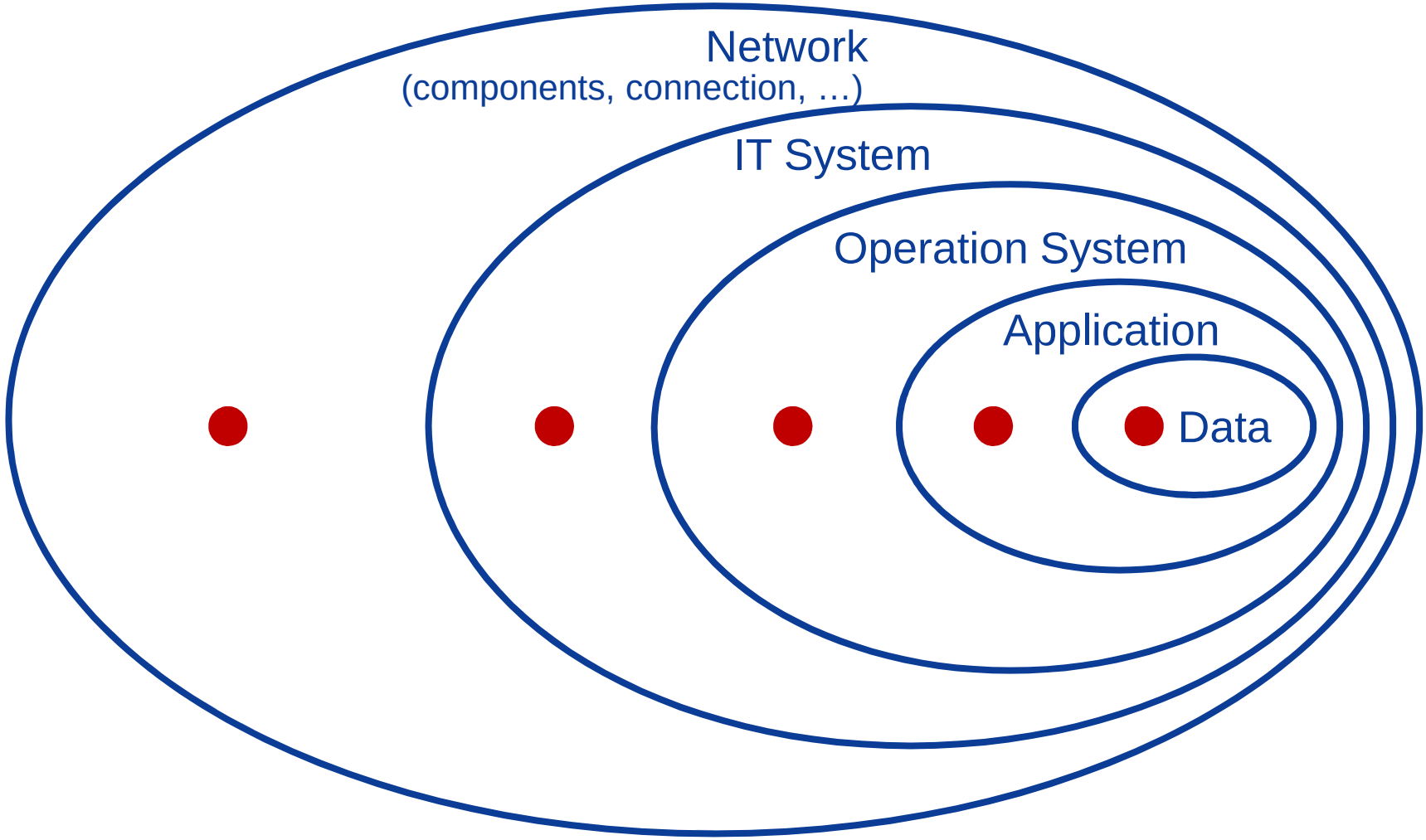
  - **the gathered security information helps to reduce risk and damage**



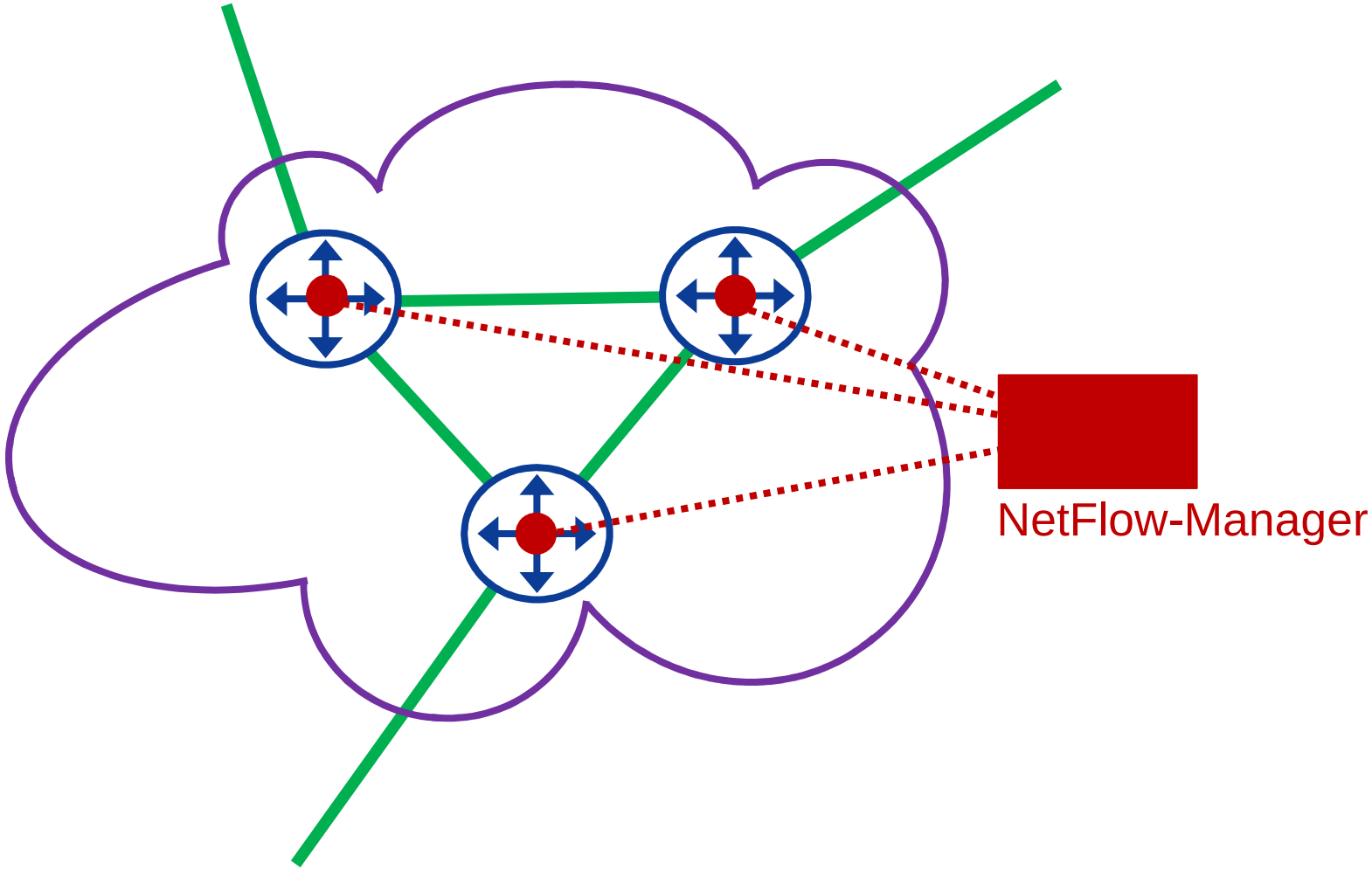
Technical Elements of an EWS
→ Sensor: Measurement method

- **Active measurement**
  - The sensor generates data and action to measure a behavior
    - ping, trace route, application / services execution, …
- **Passive measurement**
  - The sensor measures different aspect passive
    - Tap on the communication line, measure IP packets

Technical Elements of an EWS
→ Sensor: Location



Technical Elements of an EWS
→ Sensor: NetFlow-Agent → Overview



● NetFlow-Agent (sensor)

Technical Elements of an EWS
→ Sensor: NetFlow-Agent → Basic idea

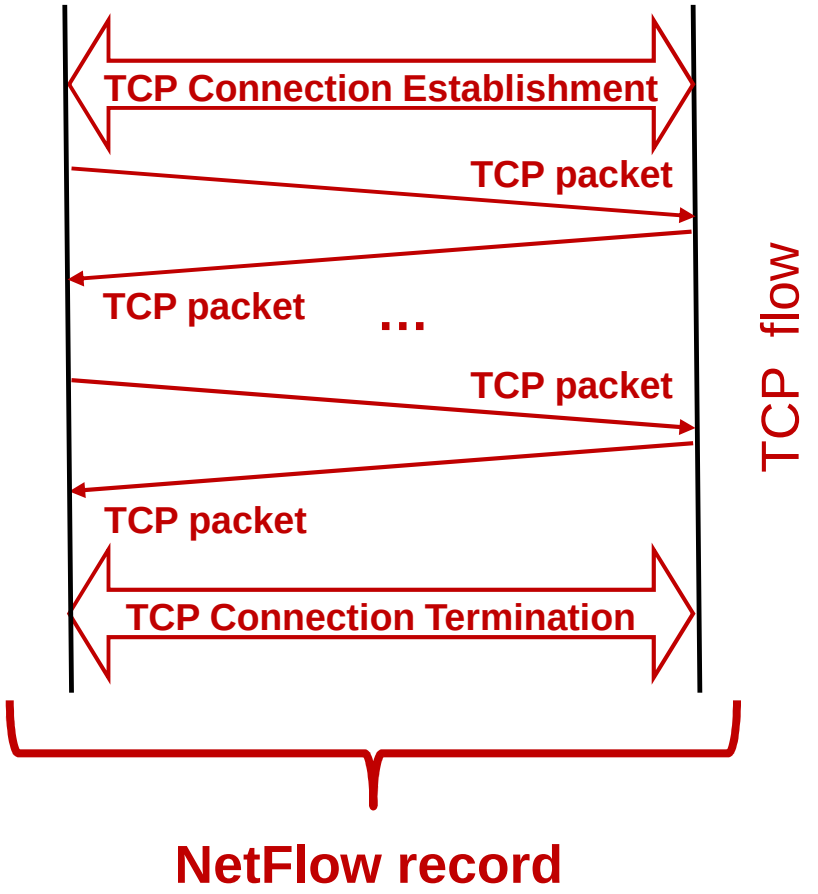
- Standard in routers for collecting IP traffic information (traffic monitoring) in the form of NetFlow records

- **NetFlow Record**
  - ...
  - Timestamps for the **flow** (start and finish time)
  - **Number** of **bytes** and **packets** observed in the flow
  - Layer 3 headers:
    - **Source & destination IP addresses**
    - **Source and destination port numbers** for TCP,UDP, SCTP
    - ICMP Type and Code.
    - IP protocol
    - Type of Service (ToS) value
  - For TCP flows, the union of **all TCP flags** observed over the life of the flow.
  - ...

- The NetFlow records are sent by UDP to the collector (NetFlow-Manager)

Technical Elements of an EWS
→ Sensor: NetFlow-Agent → Principle

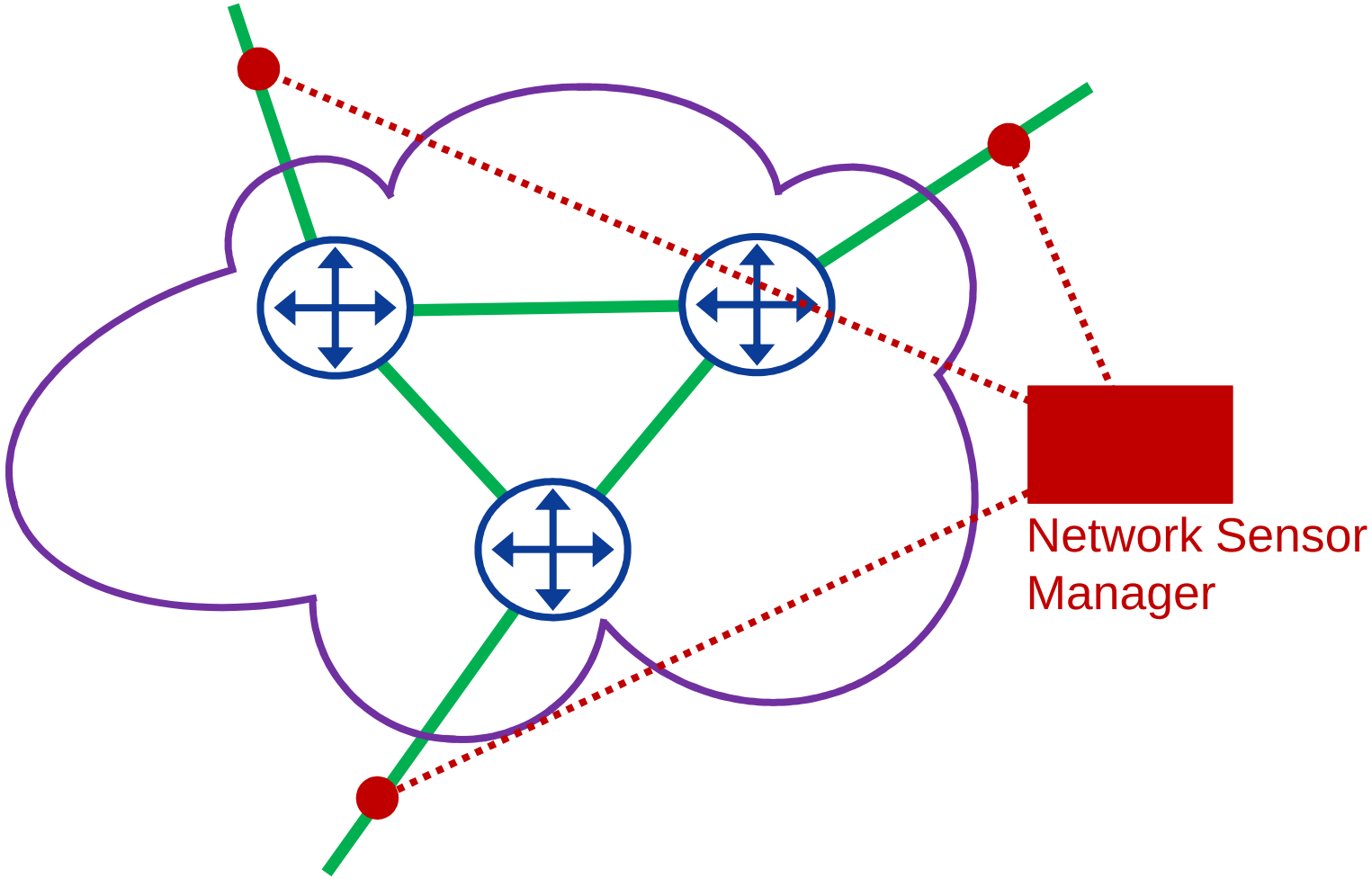
- P := all IP packets
- D := P
- S(D) := generate NetFlow records
- Y := NetFlow records
- Analysis of security information only in the Analysis System (NetFlow-Collector)



Technical Elements of an EWS
→ Sensor: NetFlow-Agent → Evaluation

- **General aspect:**
  - Originally designed for the accounting of the network traffic
- **Location:**
  - Network
    - Feature in routers
- **Security Information:** + *(little)*
- **Pros:**
  - The sensor is already available in the router (as a feature available)
  - Very fast and no problems with high bandwidth
- **Cons:**
  - Little security information available

Technical Elements of an EWS
→ Sensor: Network → Overview



● Network Agent (sensor)

Technical Elements of an EWS
→ Sensor: Network → Basic idea

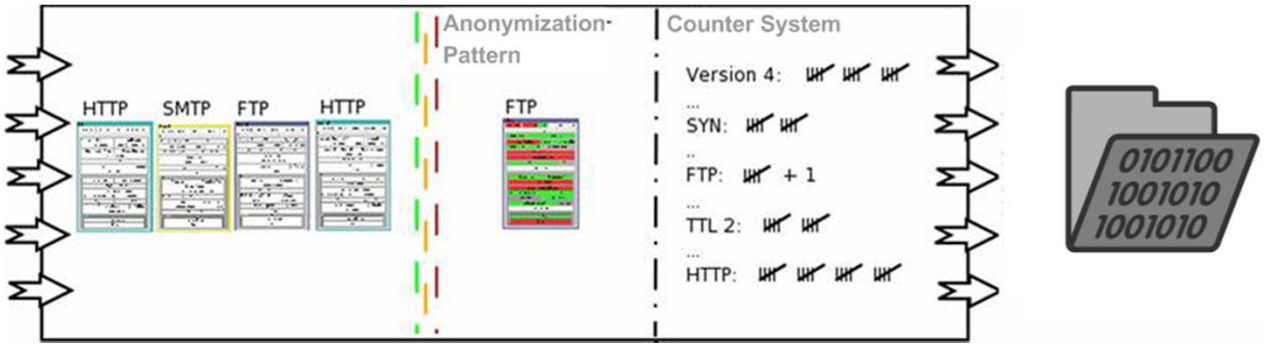
- A “Network Sensor” is a network device that monitors network for malicious activities or policy violations.

- Network Sensor could be:
  - **Intrusion detection system (IDS)**
    - network (*and host*) based
    - e.g. snort
  - **Deep Packet Inspection (DPI)**
    - intensive analysis of the header and the data part
    - e.g. ???
  - **Statistical approaches**
    - only the headers analyzed (no data protection issues)
    - e.g. Internet Analysis System (IAS)

Technical Elements of an EWS
→ Sensor: Network → Principle

- P := all IP packets
- D := P
- S(D) := deep packet inspection
  and/or
  intrusion detection
  and/or
  statistical approaches (no data protection issues)

Typical : signature- and anomaly-based analysis



- Y := raw data / security events
- Analysis of security information in the Sensor and/or Analysis System

Technical Elements of an EWS
→ Sensor: Network → Evaluation

- **General aspect:**
  - Every IP packet can be analyzed / reduced
- **Location:**
  - Network
    - Separate sensor (network device)
    - Integrated in network components (Router, switch, …)
- **Security Information:** +++ *(high)*
- **Pros:**
  - Independent of network components
  - Best detection capabilities, work on all communication layers
  - …
- **Cons:**
  - Higher cost, privacy issues, very intensive performance,
  - …

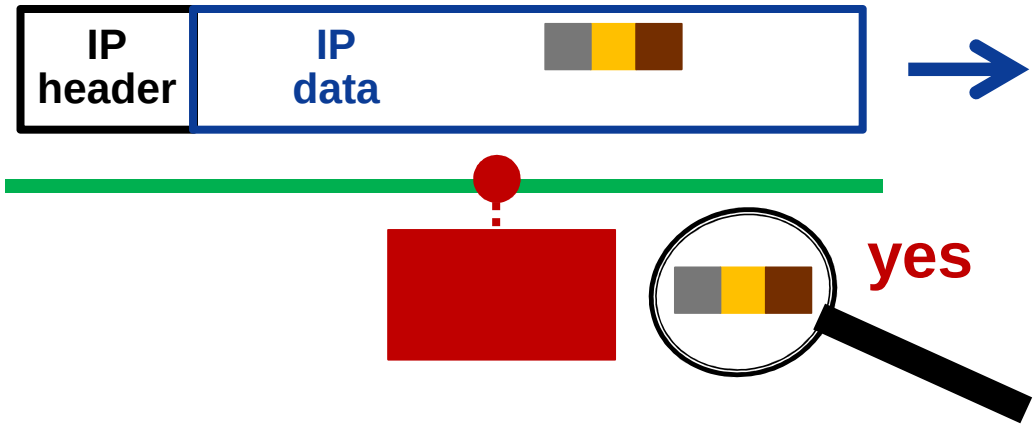
Technical Elements of an EWS
→ Network Sensor: Challenges (1/2)

- **Complete data traffic (P)**
  - Size of data traffic (up to 2,5 Tbit /s (~1,5 Tbit/s) – DE-CIX)
  - Legal conditions (accesses)
  - …
- **Data traffic going through the sensor (D)**
  - Performance (CPU, …)
  - Size of the data (100 M/Bit → 1 Tbyte/24 h)
  - Method of reduction/analyze (bytes vs. information)
  - …
- **Result by the sensor (Y)**
  - What is the best security information?
  - How long can we store the security information (size of data)?
  - Legal conditions (pseudonymisation and anonymization)?
  - …

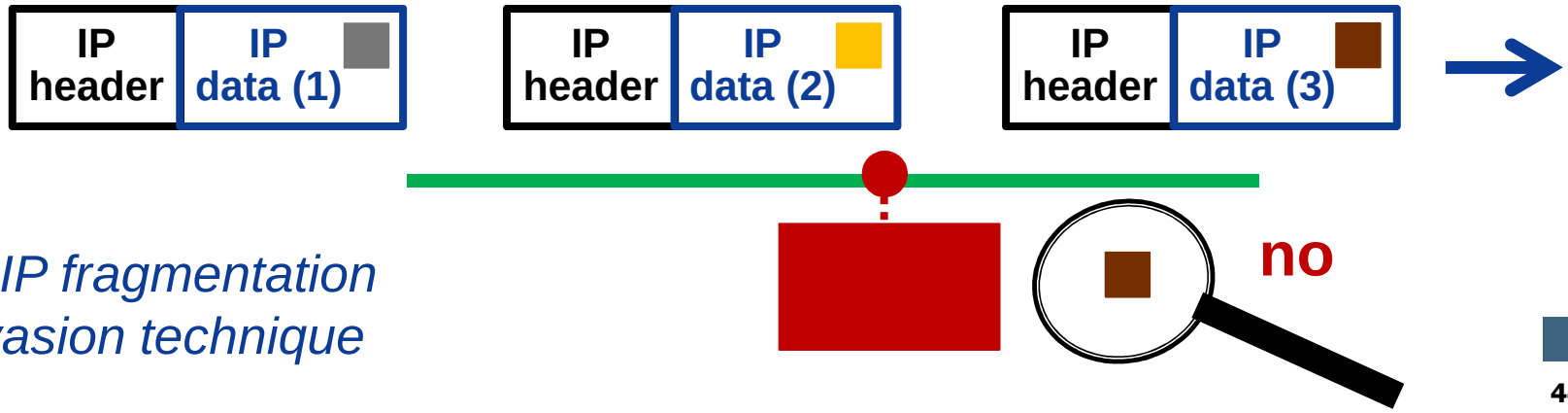
Technical Elements of an EWS
→ Network Sensor: Challenges (2/2)

- **Advanced Evasion Techniques (AET)**
  - Techniques of bypassing a network sensor in order to deliver an attack to a target network or IT system, without detection.

Identifying an attack signature (attack pattern) in an IP packet

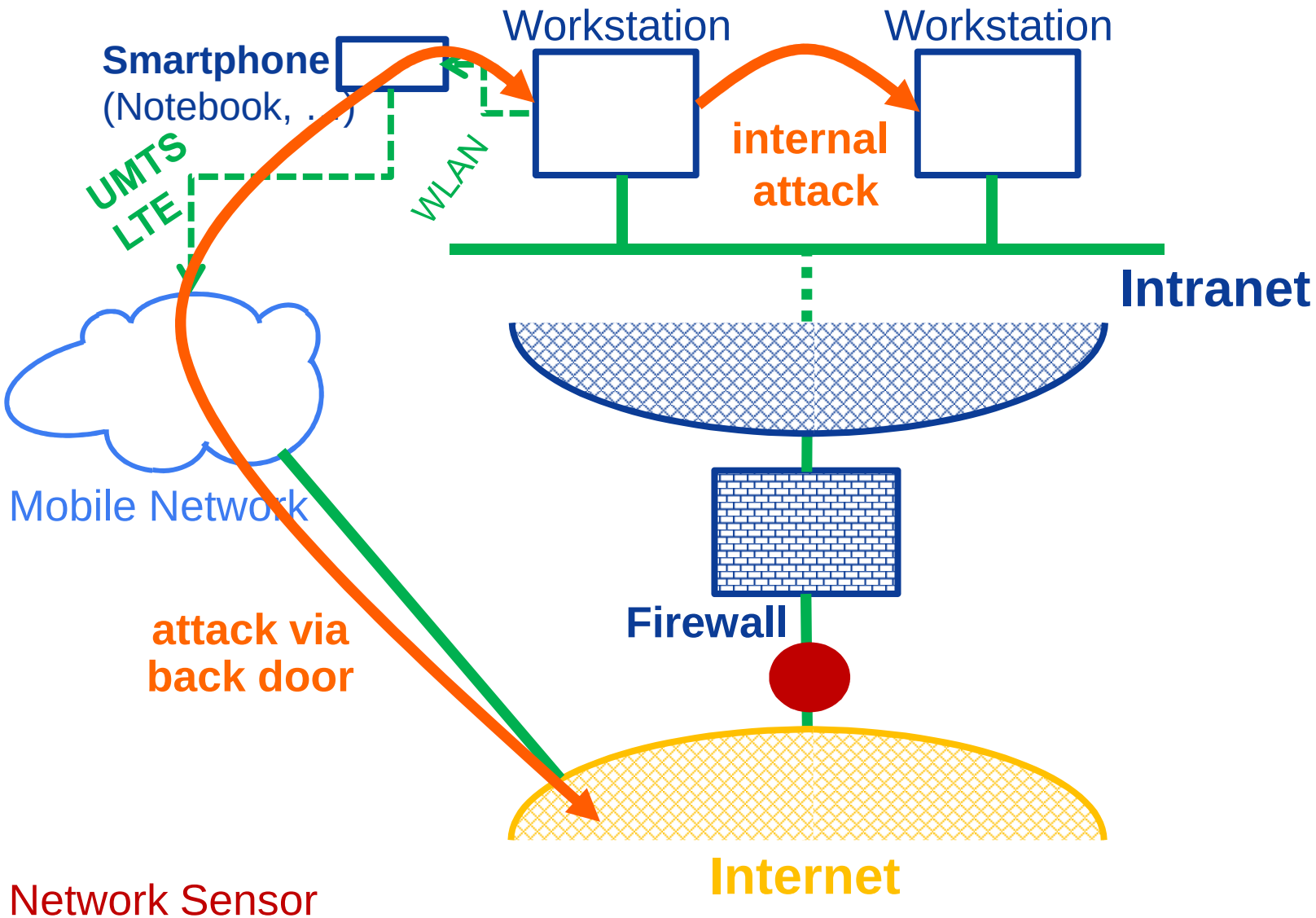


attack pattern

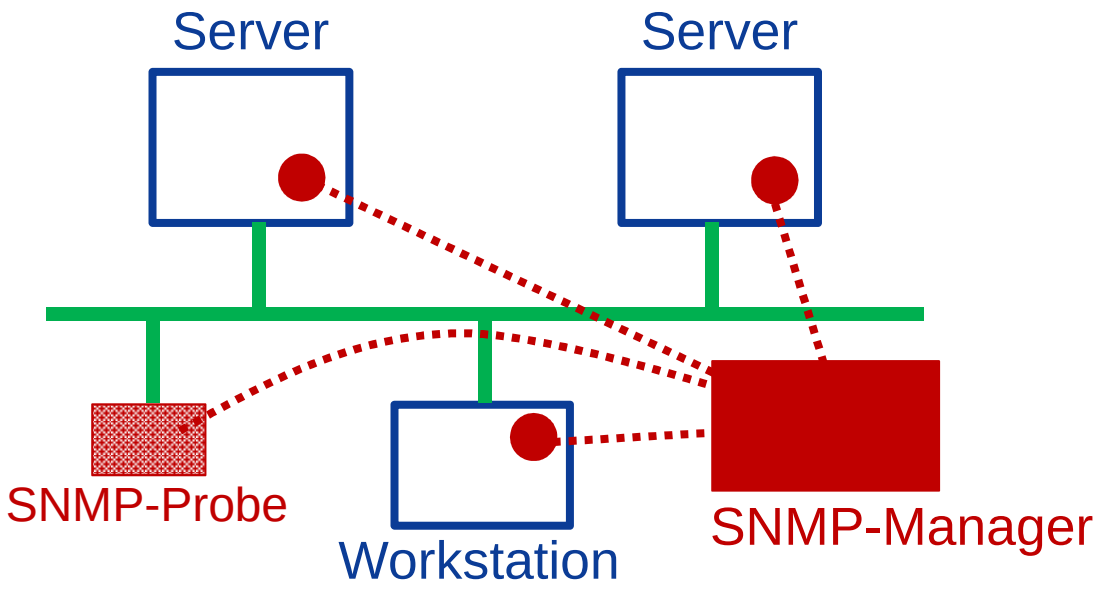


Using IP fragmentation as evasion technique

Technical Elements of an EWS
→ Network Sensor: Limits



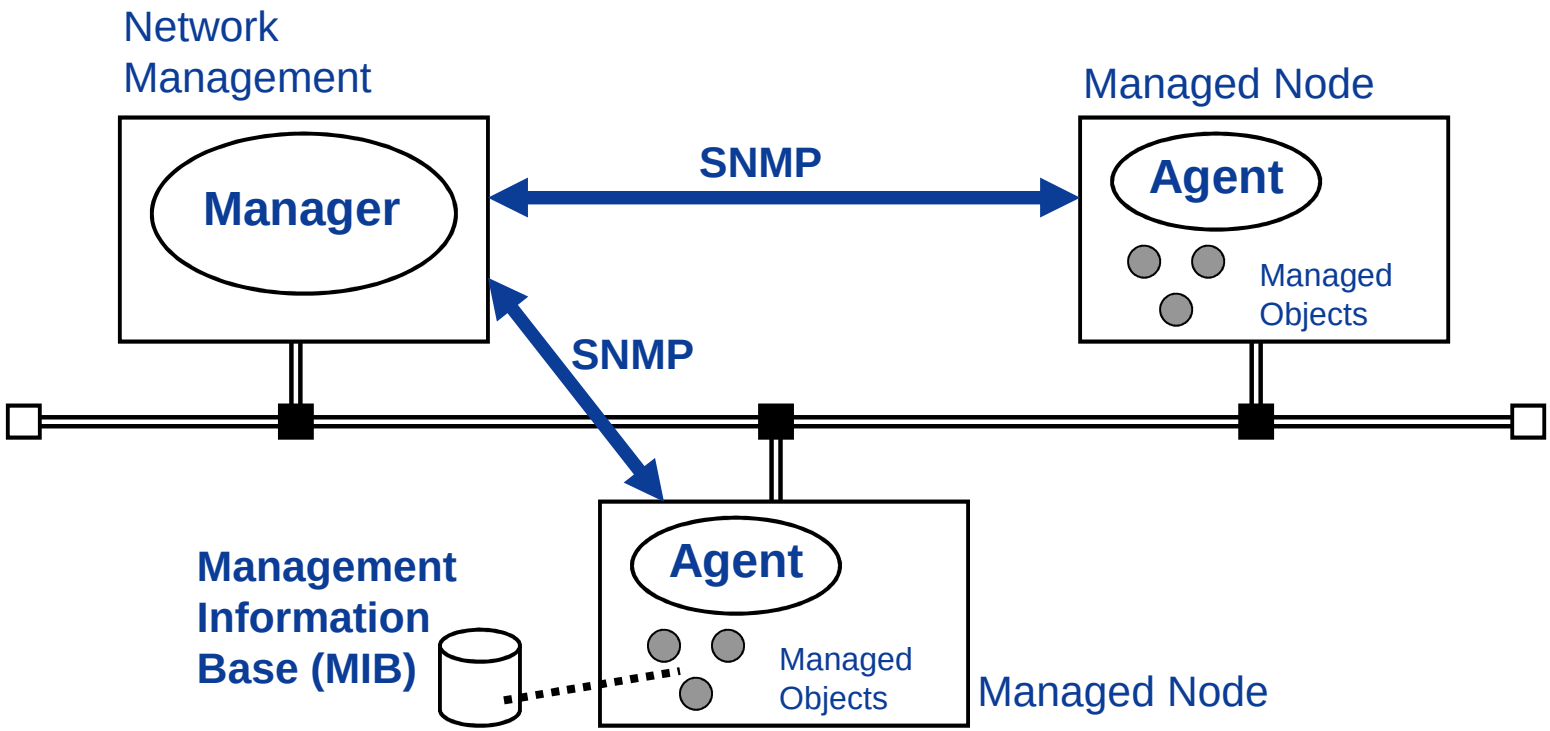
Technical Elements of an EWS
→ Sensor: SNMP-Agent → Overview



● SNMP-Agent (sensor)

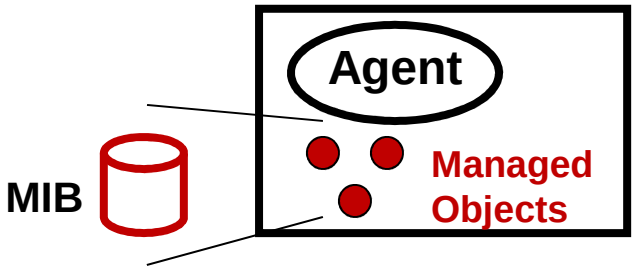
Technical Elements of an EWS
→ Sensor: SNMP-Agent → Basic idea

- Internet-standard protocol for **managing devices on IP networks**.
- Devices are routers, switches, servers, workstations, printers, modem racks, and more.
- It is used mostly in network management systems to monitor network-attached devices for conditions that warrant **administrative attention**.



Technical Elements of an EWS
→ Sensor: SNMP-Agent → Principle

- P := all IP Packets
  and/or
  additional data depending on the used MIBs (hard disc, CPU, …)
- D := a reduction of P
- S(D) := definition of managed objects
  definition of snmp-traps (MIB)
  and/or
  snmp-get actions
  (SNMP-Manager request information from the MIB)



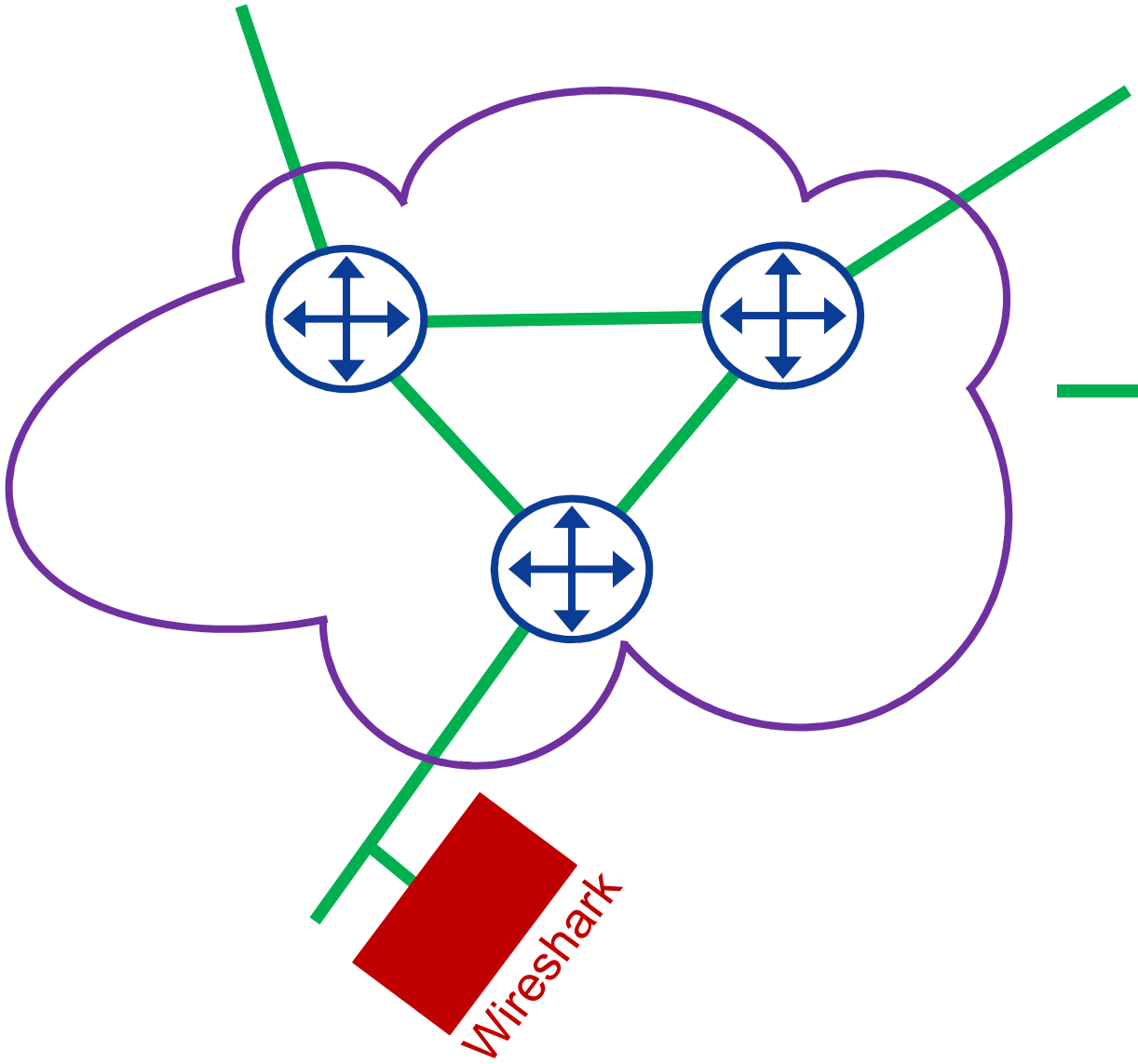
definition of managed objects

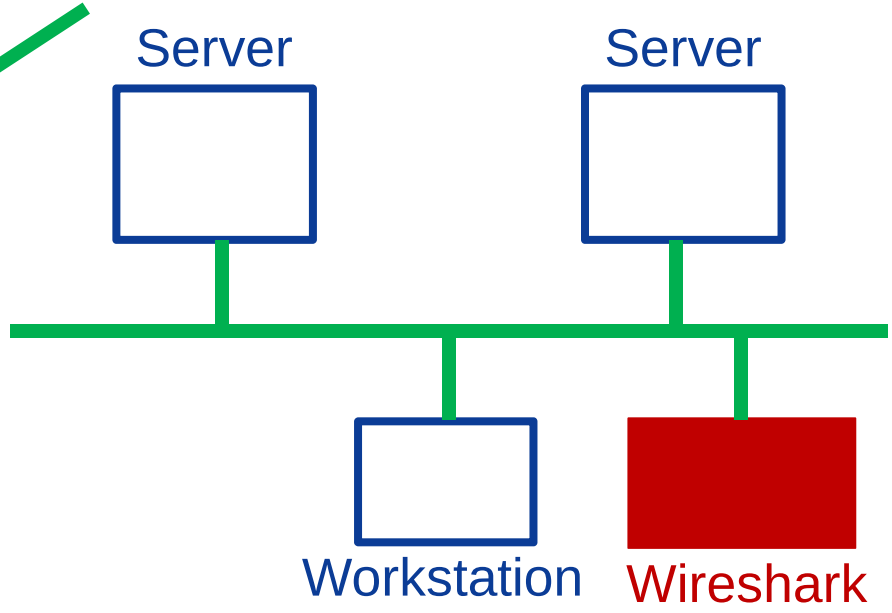
- Y := SNMP-Message (content of managed objects)
- Analysis of security information only in the Analysis System (SNMP-Manager)

Technical Elements of an EWS
→ Sensor: SNMP-Agent → Evaluation

- **General aspect:**
  - Monitoring and/or managing a group of IP devices on a network.
- **Location:**
  - Network
    - SNMP-Agent is an app in the IP devices
- **Security Information:** + *(little)*
- **Pros:**
  - The sensor is already available in the IP devices (as a feature available)
  - Perfect for testing the availability of local network devices, server, services, …
- **Cons:**
  - Little security information available in the MIBs
  - Network management rather than IT security
  - …

Technical Elements of an EWS
→ Sensor: Wireshark → Overview

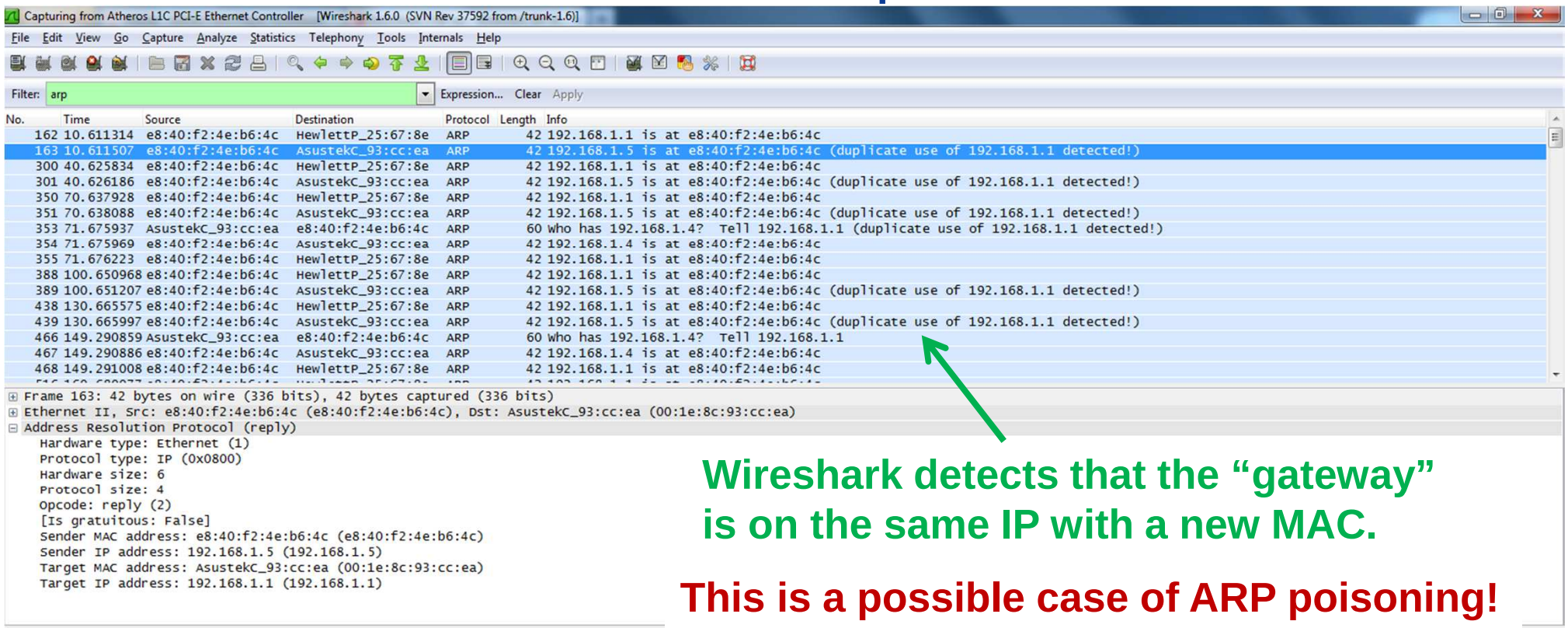




Technical Elements of an EWS
→ Sensor: Wireshark → Basic idea

- Wireshark is a packet analyzer.
- It is used for network troubleshooting, analysis and communications protocol development.

An example of how to work with Wireshark.



Wireshark detects that the "gateway" is on the same IP with a new MAC.

This is a possible case of ARP poisoning!

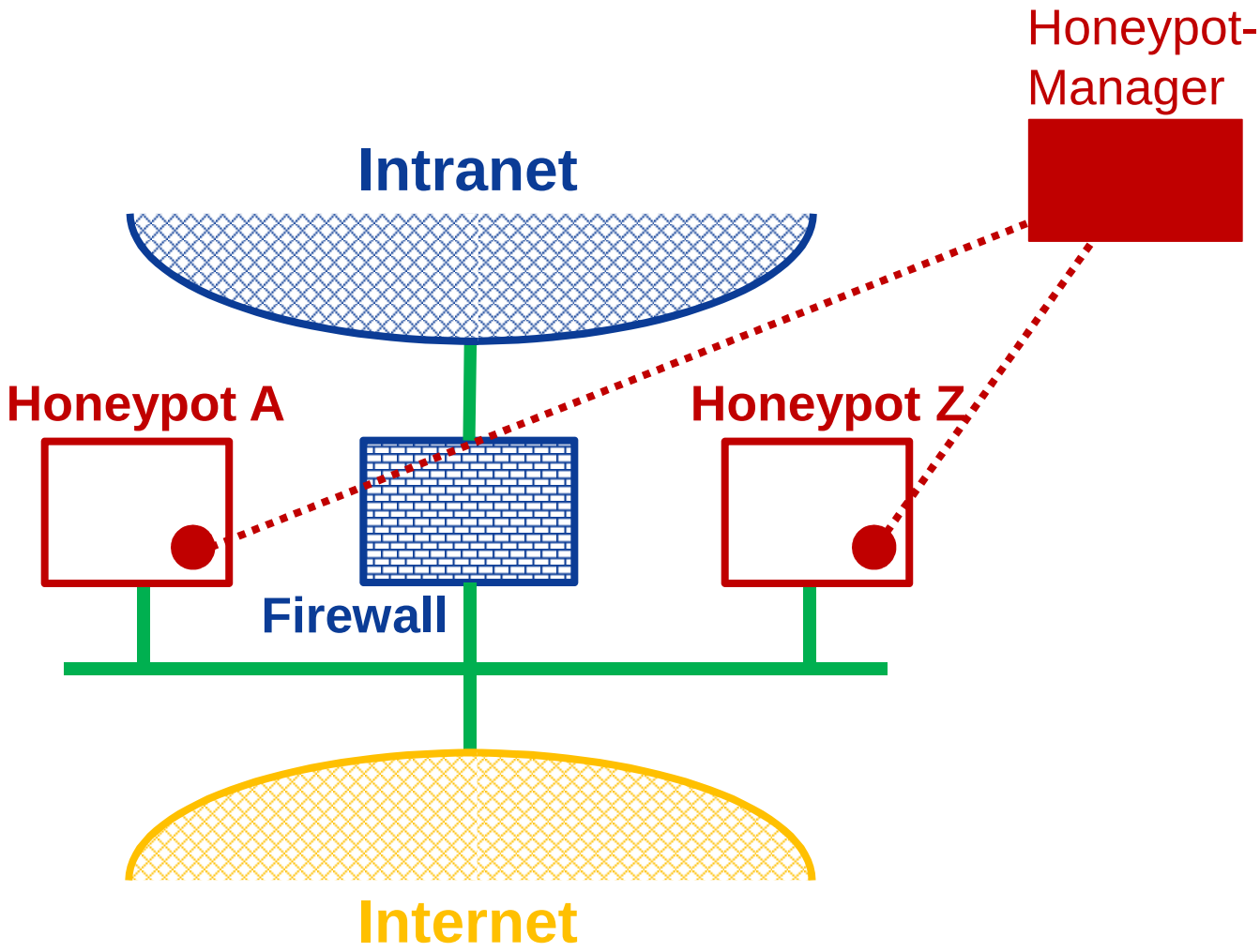
Technical Elements of an EWS
→ Sensor: Wireshark → Principle

- P := all IP packets
- D := P
- S(D) := use of filter
- Y := Interpretation of the security expert
- The analysis of security information is local (Wireshark app)

Technical Elements of an EWS
→ Sensor: Wireshark → Evaluation

- **General aspect:**
  - Wireshark is very useful for the detailed analysis of an attack.
- **Location:**
  - Network
    - Integrated as an app in a computer system (notebook, PC)
- **Security Information:** +++ *(high)*
- **Pros:**
  - All security information available
  - Not only security but also network information
- **Cons:**
  - Too much information - size of the data (100 M/Bit/s →1005,8 Gbyte/24 h)
  - Extremely complex; only manual analysis
  - …

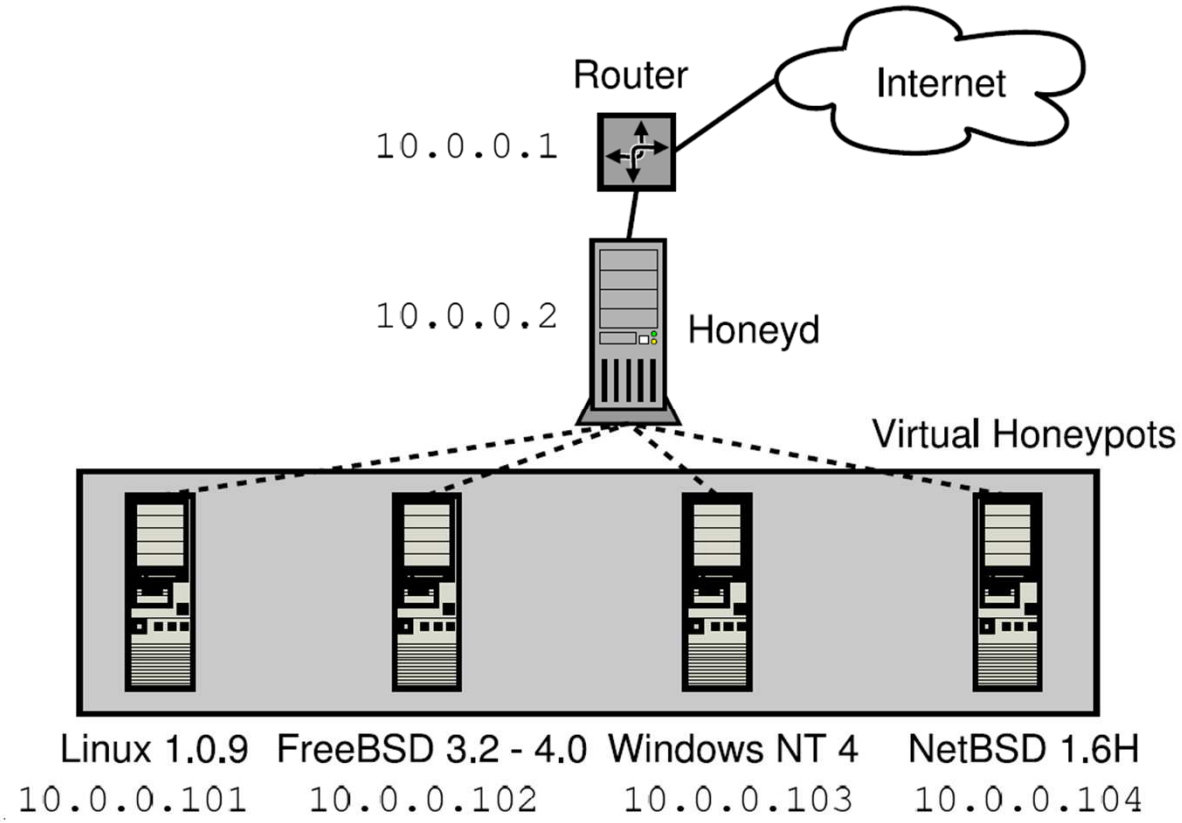
Technical Elements of an EWS
→ Sensor: Honeypot → Overview



● Honeypot (sensor)

Technical Elements of an EWS
→ Sensor: Honeypot → Basic idea

- A honeypot is a **trap** set to **detect or deflect attacks**.
- A honeypot seems to contain information or a resource of value to attackers.
- A honeypot system **helps to understand** which kind of attacks are available (**malware, exploits, attack strategies, …**)
- Low-interaction = emulation, high-interaction = full service stack



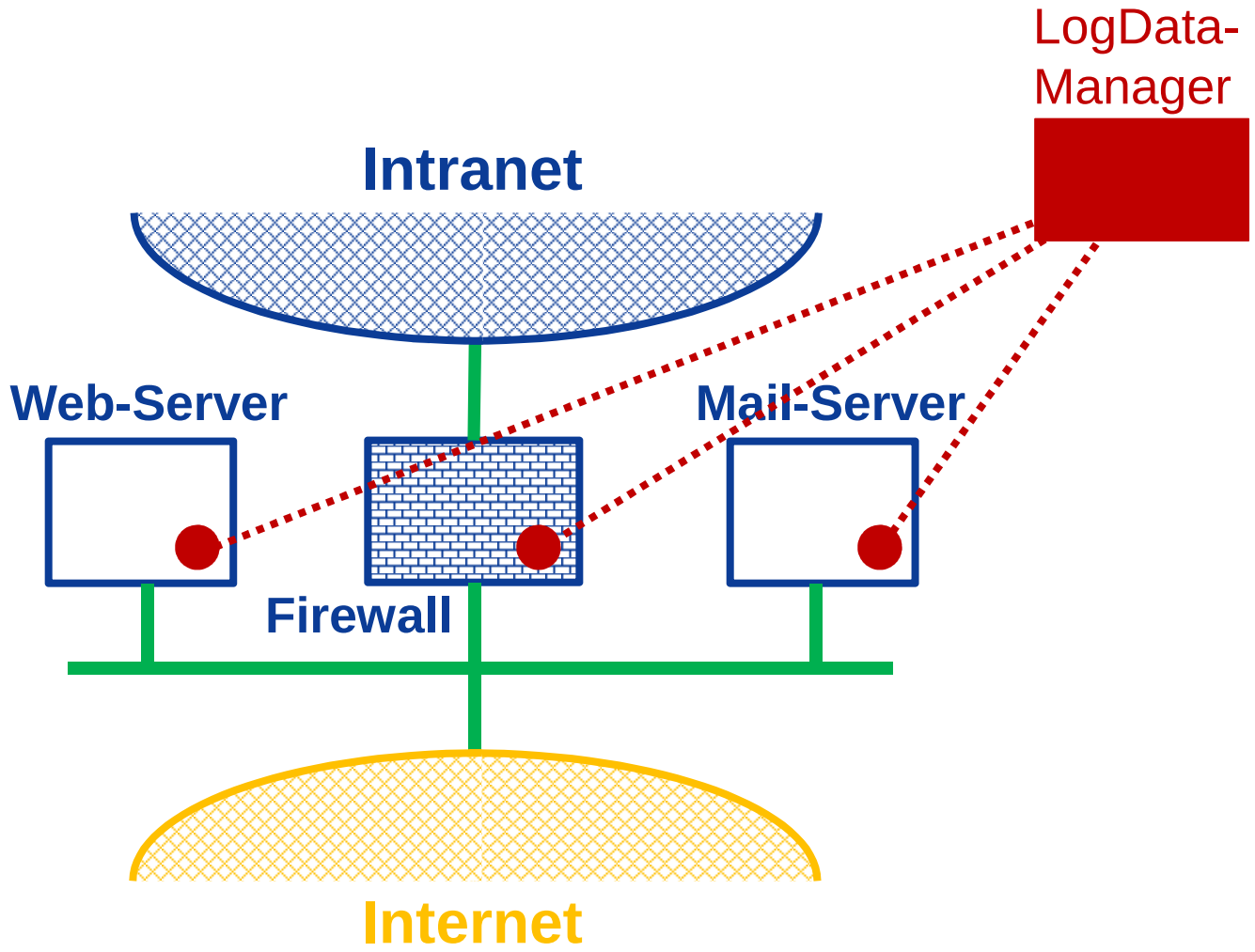
Technical Elements of an EWS
→ Sensor: Honeypot → Principle

- P := all IP packets
  and
  Events in the Computer System (OS, App, Data)
- D := subset of network definition of rules for logging
- S(D) := monitor use of otherwise unused hosts/networks
- Y := detailed attack traces (network / host)
- Analysis of security information in the Sensor and Analysis System

Technical Elements of an EWS
→ Sensor: Honeypot → Evaluation

- **General aspect:**
  - All interactions with honeypots (fake services) are threats
- **Location:**
  - Network
    - Separate senor
- **Security Information:** ++ *(medium)*
- **Pros:**
  - Qualitative security information
  - Understands patterns of attacks
- **Cons:**
  - High-maintenance
  - Hard to lure attackers to fake systems
  - Honeypots can be identified as such

Technical Elements of an EWS
→ Sensor: LogData-Agent → Overview



● LogData-Agent

Technical Elements of an EWS
→ Sensor: LogData-Agent → Basic idea

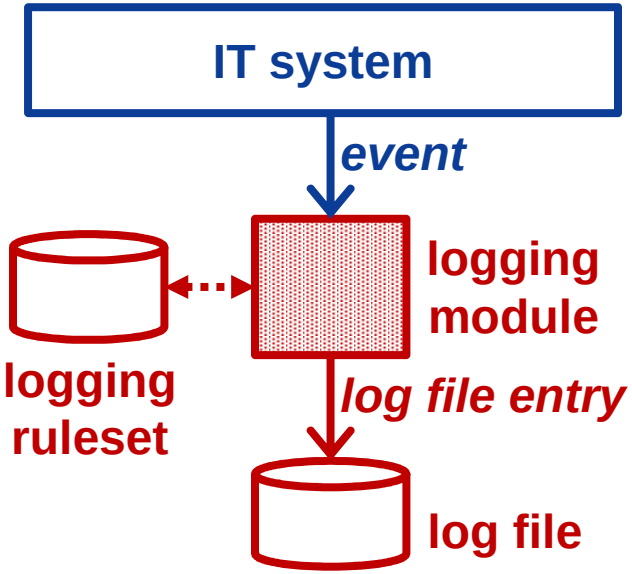
- Data logging is the process of recording events in log files.
- Data logging provides an audit trail that can be used to understand the activity of the IT system.
- Helps to diagnose problems (process, security, …).
- It can also be useful to combine log file entries from multiple sources.
  - Network, operation system, application and data
  - Webserver, mail-server, firewall, DNS server, VoIP server, …

Log file:

```
Oct 19 06:12:55 fb5gwint kernel: forward Rule 13 - ACCEPT IN=eth0 OUT=eth2
SRC=63.97.52.4 DST=194.94.127.1 LEN=48 TOS=0x00 PREC=0x00 TTL=112 ID=32274 DF   PROTO=TCP
SPT=1703 DPT=3306 WINDOW=65535 RES=0x00 SYN URGP=0
Oct 19 06:12:55 fb5gwint kernel: forward Rule 13 - ACCEPT IN=eth0 OUT=eth2
SRC=63.97.52.4 DST=194.94.127.2 LEN=48 TOS=0x00 PREC=0x00 TTL=112 ID=32275 DF PROTO=TCP
SPT=1704 DPT=3306 WINDOW=65535 RES=0x00 SYN URGP=0
Oct 19 06:12:55 fb5gwint kernel: Internet Rule 12 - DENY IN=eth0 OUT=eth2
SRC=63.97.52.4 DST=194.94.127.3 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=32276 DF PROTO=TCP
SPT=1705 DPT=3306 WINDOW=65535 RES=0x00 SYN URGP=0
Oct 19 06:12:55 fb5gwint kernel: forward Rule 13 - ACCEPT IN=eth0 OUT=eth2
SRC=63.97.52.4 DST=194.94.127.4 LEN=48 TOS=0x00 PREC=0x00 TTL=112 ID=32277 DF PROTO=TCP
SPT=1706 DPT=3306 WINDOW=65535 RES=0x00 SYN URGP=0
Oct 19 06:12:55 fb5gwint kernel: forward Rule 13 - ACCEPT IN=eth0 OUT=eth2
SRC=63.97.52.4 DST=194.94.127.6 LEN=48 TOS=0x00 PREC=0x00 TTL=112 ID=32279 DF PROTO=TCP
SPT=1708 DPT=3306 WINDOW=65535 RES=0x00 SYN URGP=0
Oct 19 06:12:55 fb5gwint kernel: forward Rule 13 - ACCEPT IN=eth0 OUT=eth2
…
```

Technical Elements of an EWS
→ Sensor: LogData-Agent → Principle

- P := activities in IT systems
  - network
    and/or
  - computer systems (OS, app, data)
- D := events (collection system)
- S(D) := logging process depends on the ruleset
  (signature- and anomaly-based analysis)

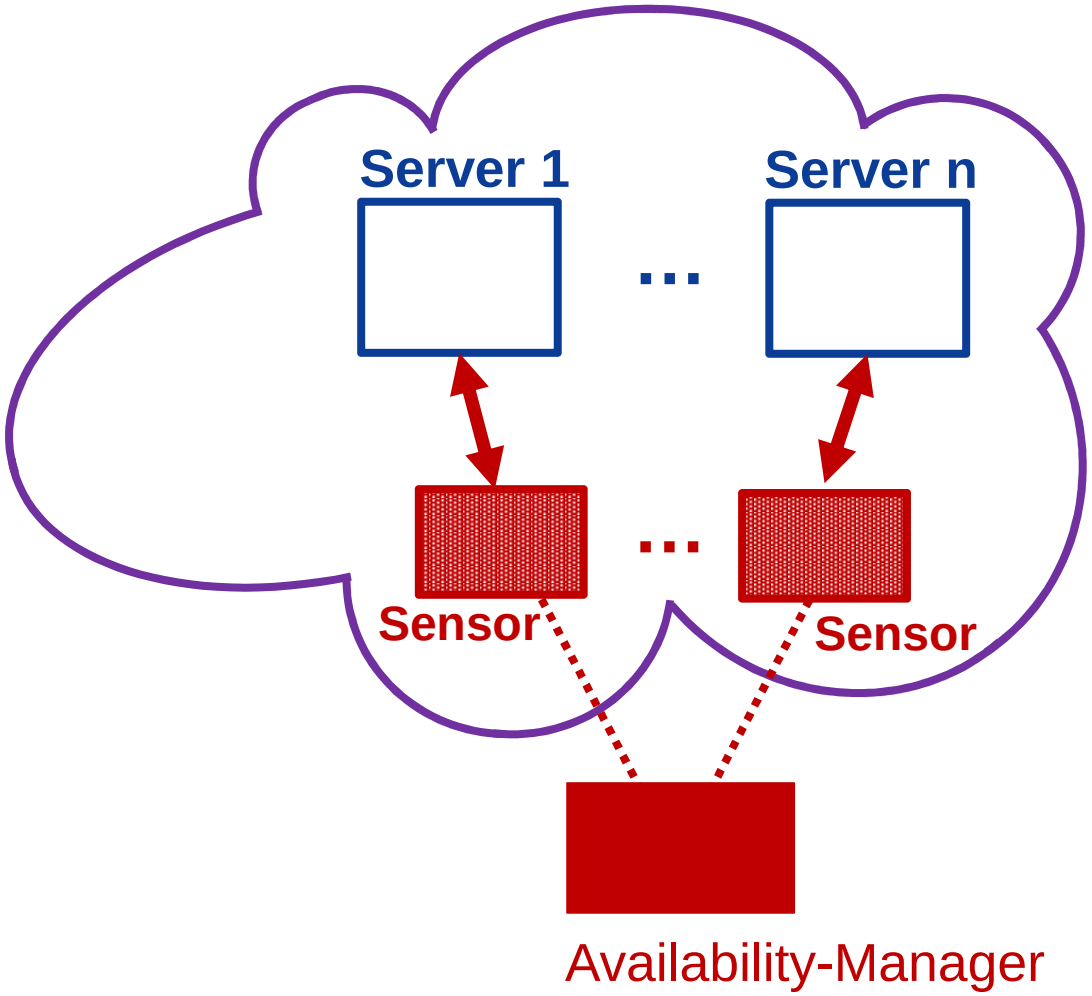


- Y := (security) events and/or log file (entries)
- Analysis of security information in the Sensor and Analysis System

Technical Elements of an EWS
→ Sensor: LogData-Agent → Evaluation

- **General aspect:**
  - Generates an audit trail and helps to understand activities (attacks).
- **Location:**
  - Network
    - Network components (Firewall, …)
  - Computer system
    - OS, app and data
- **Security Information:** +++ *(high)*
- **Pros:**
  - Detailed security information
  - Attack trail can be analyzed
  - Successful attacks can be saved
- **Cons:**
  - Difficult definition of the events and an appropriated ruleset
  - Problem: SI <-> number of entries (only 5 % are important)
  - Successful attacks have already happened when it was logged

Technical Elements of an EWS
→ Sensor: Availability-Agent → Overview



Server: Web, Mail, DNS, SIP, …

Technical Elements of an EWS
→ Sensor: Availability-Agent → Basic idea

- An availability system monitors the availability of IT systems and services.
- The properties that are being monitored are:
  - Quality of Service
    - Bandwidth, Jitter, Delay, Packet Loss Rate
    - …
  - Quality of Experience (Data Interpretation)
- Measurement tools are:
  - Ping, trace route, application / services execution, ….

Technical Elements of an EWS
→ Sensor: Availability-Agent → Principle

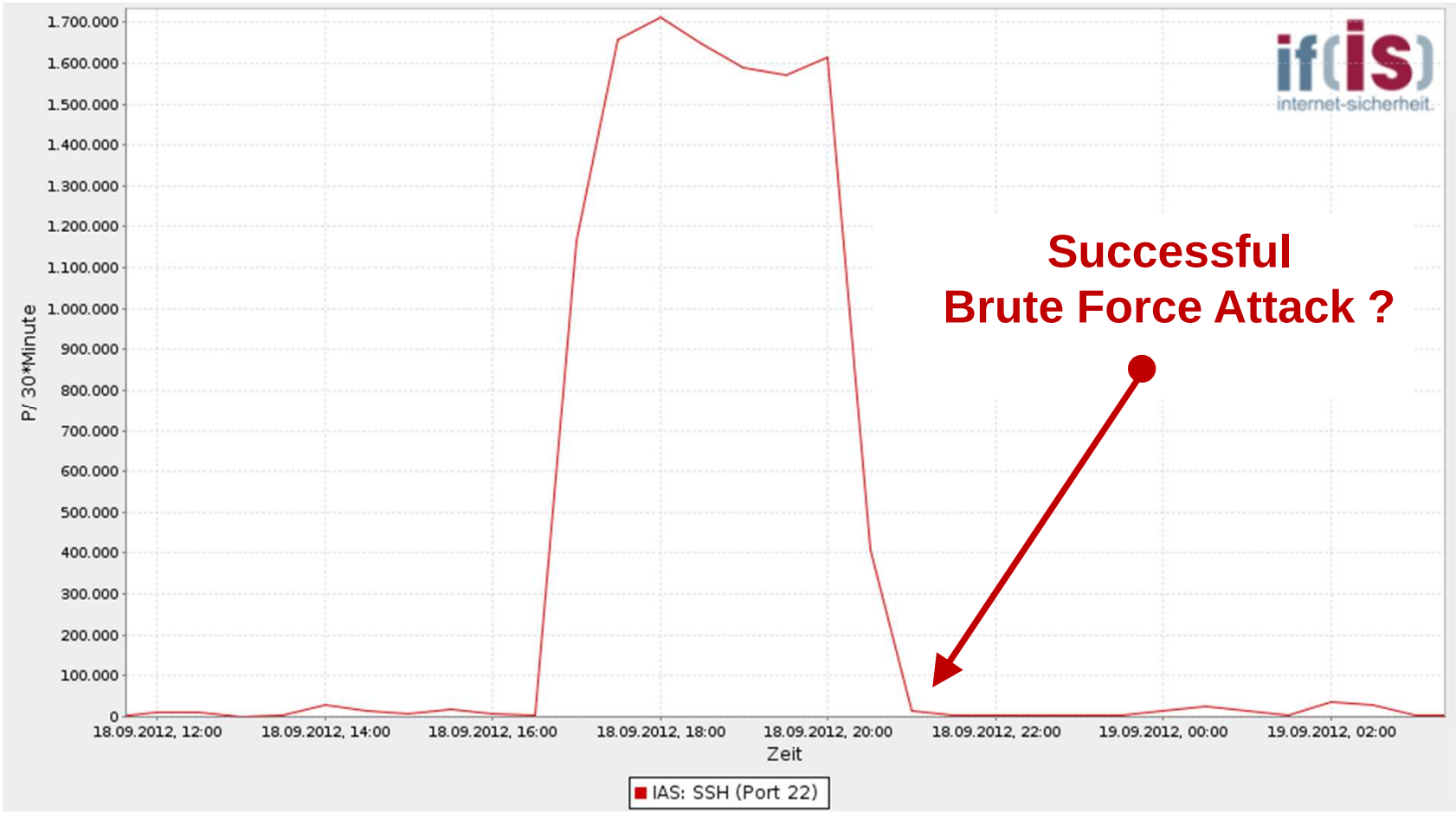
- P := behavior information
- D := quality of service (QoS) and quality of experience (QoE) parameter
- S(D) := interpretation of the measured parameter
- Y := Security events *and/or* QoS / QoE parameter
- Analysis of security information in the Sensor and Analysis System

Technical Elements of an EWS
→ Sensor: Availability-Agent → Evaluation

- **General aspect:**
  - Helps to understand the availability situation of IT systems and services.
- **Location:**
  - Network
- **Security Information:** ++ *(medium)*
- **Pros:**
  - Real security information
- **Cons:**
  - Cost of additional traffic, CPU, …

Technical Elements of an EWS
→ Interpretation or clearly identify (1/2)

- **Network sensor**
  - Interpretation of attack pattern
    - Could be a successful attack but we do not know



Technical Elements of an EWS
→ Interpretation or clearly identify (2/2)

- **LogData sensor**
  - Clear identification of events (Events identify a successful attack)

…
Sep 23 04:02:49 prometheus sshd[30395]: **Failed password** for root from 140.114.78.131 port 56003 ssh2
Sep 23 04:02:49 prometheus sshd[30396]: Received disconnect from 140.114.78.131: 11: Bye Bye
Sep 23 04:02:52 prometheus unix_chkpwd[30400]: password check failed for user (root)
Sep 23 04:02:52 prometheus sshd[30398]: pam_unix(sshd:auth): authentication failure;
Sep 23 04:02:54 prometheus sshd[30398]: **Failed password** for root from 140.114.78.131 port 57683 ssh2
Sep 23 04:02:54 prometheus sshd[30399]: Received disconnect from 140.1
Sep 23 04:02:56 prometheus unix_chkpwd[30403]: password check failed f
Sep 23 04:02:56 prometheus sshd[30401]: pam_unix(sshd:auth): authentic
Sep 23 04:02:58 prometheus sshd[30401]: **Failed password** for root from 140.114.78.131 port 59293 ssh2
Sep 23 04:02:59 prometheus sshd[30402]: Received disconnect from 140.114.78.131: 11: Bye Bye
Sep 23 04:03:01 prometheus unix_chkpwd[30406]: password check failed for user (root)
Sep 23 04:03:01 prometheus sshd[30404]: pam_unix(sshd:auth): authentication failure;
Sep 23 04:03:03 prometheus sshd[30404]: **Failed password** for root from 140.114.78.131 port 32877 ssh2
Sep 23 04:03:03 prometheus sshd[30405]: Received disconnect from 140.114.78.131: 11: Bye Bye
…
Sep 23 11:42:55 prometheus sshd[683]: **Accepted password** for root from 140.114.78.131 port 56418 ssh
Sep 23 11:42:55 prometheus sshd[683]: pam_unix(sshd:session): session opened for user root by (uid=0)

Successful Brute Force Attack !

Technical Elements of an EWS
→ Overview Sensor

System / Characteristics	IDS	SNMP	LogData	HoneyPot	Wireshark	IAS
Function	Detection of signatures and attack patterns	Detection of failures, configuration, performance, accounting	Control of the events by the means of rules and policies	Detection and analyzing of the intrusion and the used proceeding of hackers	Fault detection, spying on data and information	Actual status, pattern formation, creation of knowledge base, alarm signaling, forecasting
Location	Uplink	In the network	Uplink IT system	Uplink	Uplink & Transit	Uplink & Transit
Realization	Complete analysis of the network traffic	Collection of Information by the means of agents	Analysis events of the network traffic and IT systems	Simulating the behavior of systems	Complete analysis of the network traffic	Complete analysis of the network traffic
Results	Recognition of signatures, Information for pattern formation	Accounting, fault messages, performance data	Security relevant information	Attack patterns and scenarios	Complete network traffic	Statistics, counters, results of further processing
Data privacy	Special agreement with concerned	Special agreement with concerned	Special agreement with concerned	Problem in specific scenarios	Very problematic	privacy compliant by design

Technical Elements of an EWS
→ Sensor: Data protection aspects

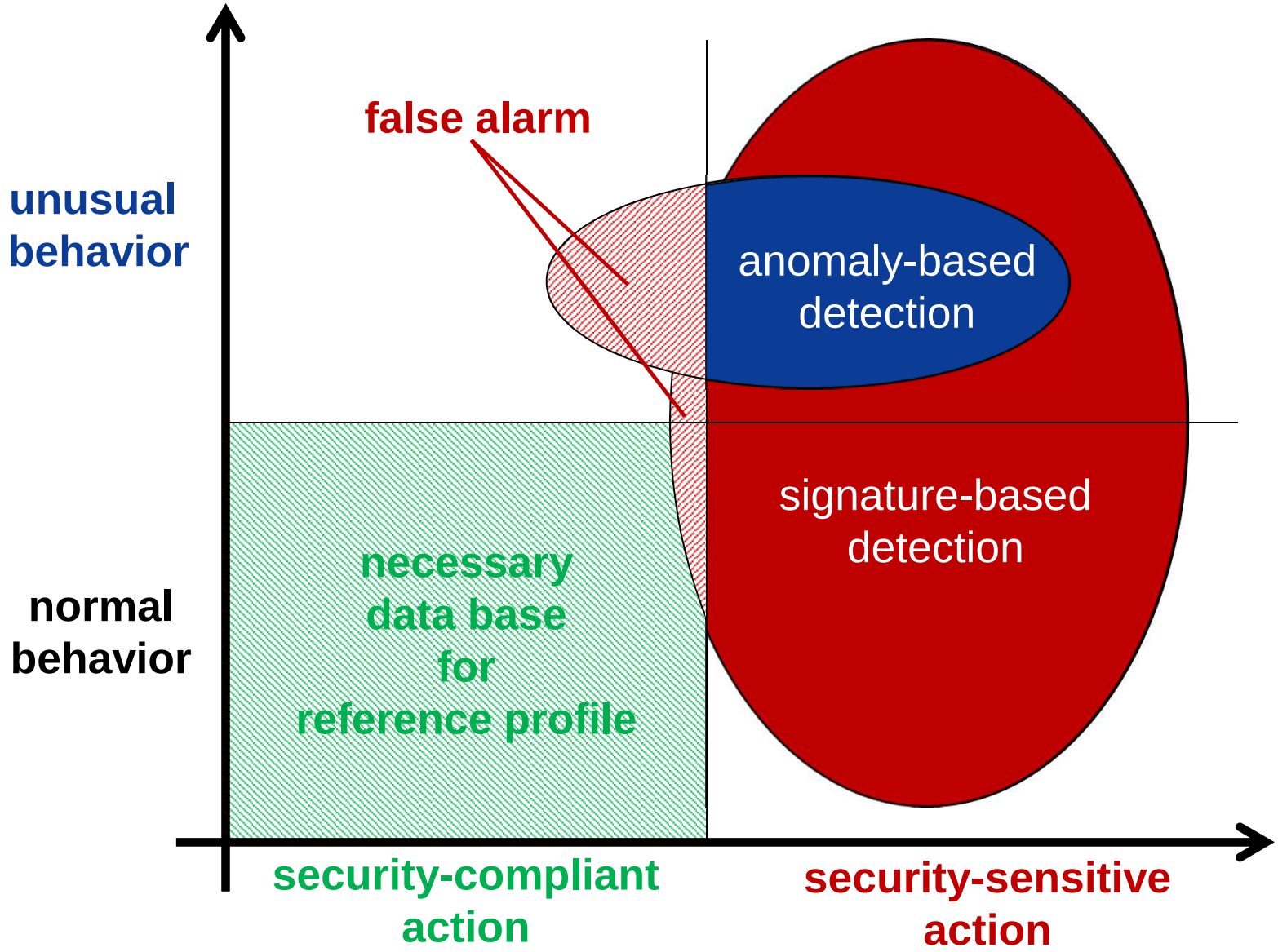
- ***Data relating to people***
  - IP address, E-mail address, …
- ***Personal data***
  - Passwords, IDs, …, user behavior, …, personal letter, …
- **Methods used to satisfy privacy**
  - Don´t analyze personal data or data relation to people
  - Pseudonymisation and anonymization
    - is a procedure in which identifying fields are replaced by artificial identifiers.
    - Pseudonymisation allows tracking back identifying fields to its origins (anonymization not)

Technical Elements of an EWS
→ Analysis concept

- **Signature-based detection**
  - Signature based detection monitors actions and compares with pre-configured and pre-determined attack patterns known as signatures.
  - The issue is that there will be a lag between the new threat action discovered and the signature being applied for detecting the new threat.
  - During this time lag the signature-based detection will be unable to identify the threat.

- **Anomaly-based detection**
  - Anomaly-based detection determines for example normal network activity like what sort of bandwidth is generally used, what protocols are used, what ports and devices generally are connected to each other- and alert when traffic is detected which is anomalous (not normal).

Technical Elements of an EWS
→ Detection of security-sensitive action



Technical Elements of an EWS
→ Analysis (A) – 1/5

- **Core** of an Early Warning System!
- Identification of security relevant incidents and alerting of the relevant authorities
- Monitoring of the development of the collected data
  - Development of the Infrastructure
- **Configuration of the analysis element**
  - ***Signal level***
    - Evaluation of data concerning the current operating condition of the IT infrastructure
    - Identification of abnormal or security relevant incidents
    - signature- and/or anomaly-based analysis
    - Generates events, that can be further processed

Technical Elements of an EWS
→ Analysis (A) – 2/5

- Configuration of the analysis element
  - ***Event-driven level***
    - Correlation of the identified incidents
    - Including further Information from external non-technical sources (e. g. CERTs, ...)
    - Generating Alerts if necessary
  - ***Learning Element***
    - Adjustment of the algorithms used for analysis of the so far generated results
    - For example to adjust the algorithm to the changing network traffic, after a new service has gone online
  - ***Knowledge Base***

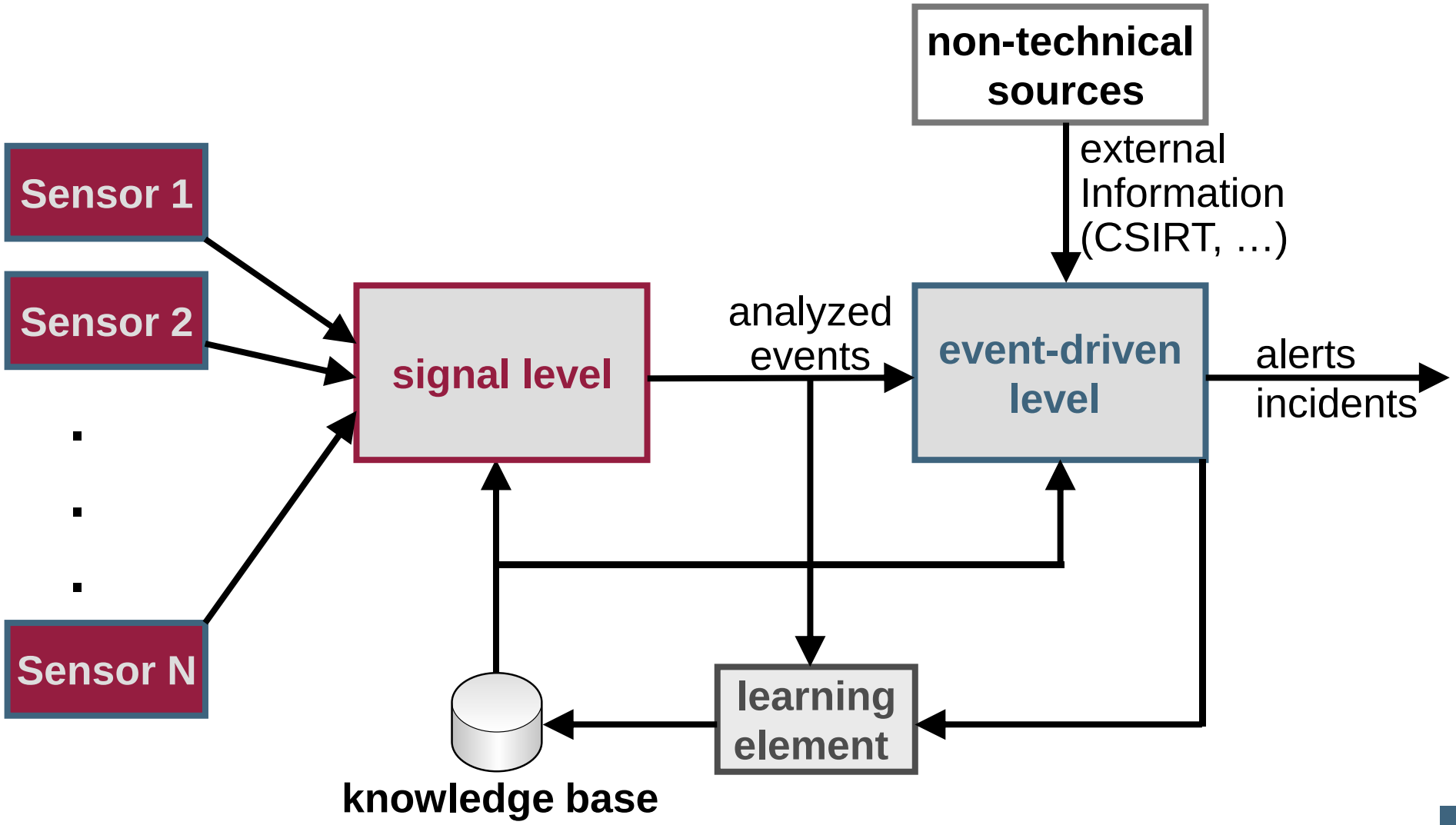
Technical Elements of an EWS
→ Analysis (A) – 3/5

- Internet Early Warning Center at the Institute for Internet Security

Technical Elements of an EWS
→ Analysis (A) – 4/5

- ***Problems***
  - Huge amounts of data
  - Detection of unknown deflections and developing trends
  - Experts are needed who understand networks and attacks

Technical Elements of an EWS
→ Analysis (A) – 5/5



Technical Elements of an EWS
→ Alerting (AL)

- Dissemination and Management of the generated Alerts
- Supporting the people in charge for the handling by offering them the knowledge base
- **Expert System** component
  - Gives hints for the solution of **formerly known problems**!
  - Gives support when working on unrecognized problems
- Offers support when transferring information back into the knowledge base

Technical Elements of an EWS
→ Knowledge Base (KB)

- Knowledge about the “environment”
- Information about
  - **normal state** of the monitored IT infrastructure
  - Definitions / **signatures** of attacks
  - **Counteractive measures**
  - **Proceedings** when “problems” occur
- Needs to be updated frequently
  - Automated generation of virus-/attack-definitions (signatures)
  - Update of the “normal state” of the monitored IT infrastructure
  - Solutions for so far unrecognized problems
- **Problem:** gathering of knowledge

Technical Elements of an EWS
→ Conservation of evidence (CE)

- Safeguarding of evidence in case of an attack
- Shall enable legal prosecution
  - Attacks have been performed …
  - Information of the attacker …
  - Damage caused by the attack …
- **Important aspects**
  - Privacy
    - Access to recorded data only in case of an actual incident
    - Protection of the personal data against misuse
  - Authenticity
    - Tampering must be technically impossible

Technical Elements of an EWS
→ Architecture (AR) – 1/3

- Architecture in which the components are combined
- Different aspects have to be respected
  - reliability, maintainability, complexity, performance, data protection and confidentiality
- Predetermined: distributed sensors
- Possible approach for the architecture
  - Centralized
  - Decentralized
- On top of this a combination of both approaches is also possible

Technical Elements of an EWS
→ Architecture (AR) – 2/3

- **Centralized architecture**
  - Besides the sensors all components are placed at one centralized operational unit
    - **pros**
      - Easy maintainability
      - Limited complexity
    - **cons**
      - Could result in performance problems
      - Centralized bodies are easier to attack (e.g. DDoS)

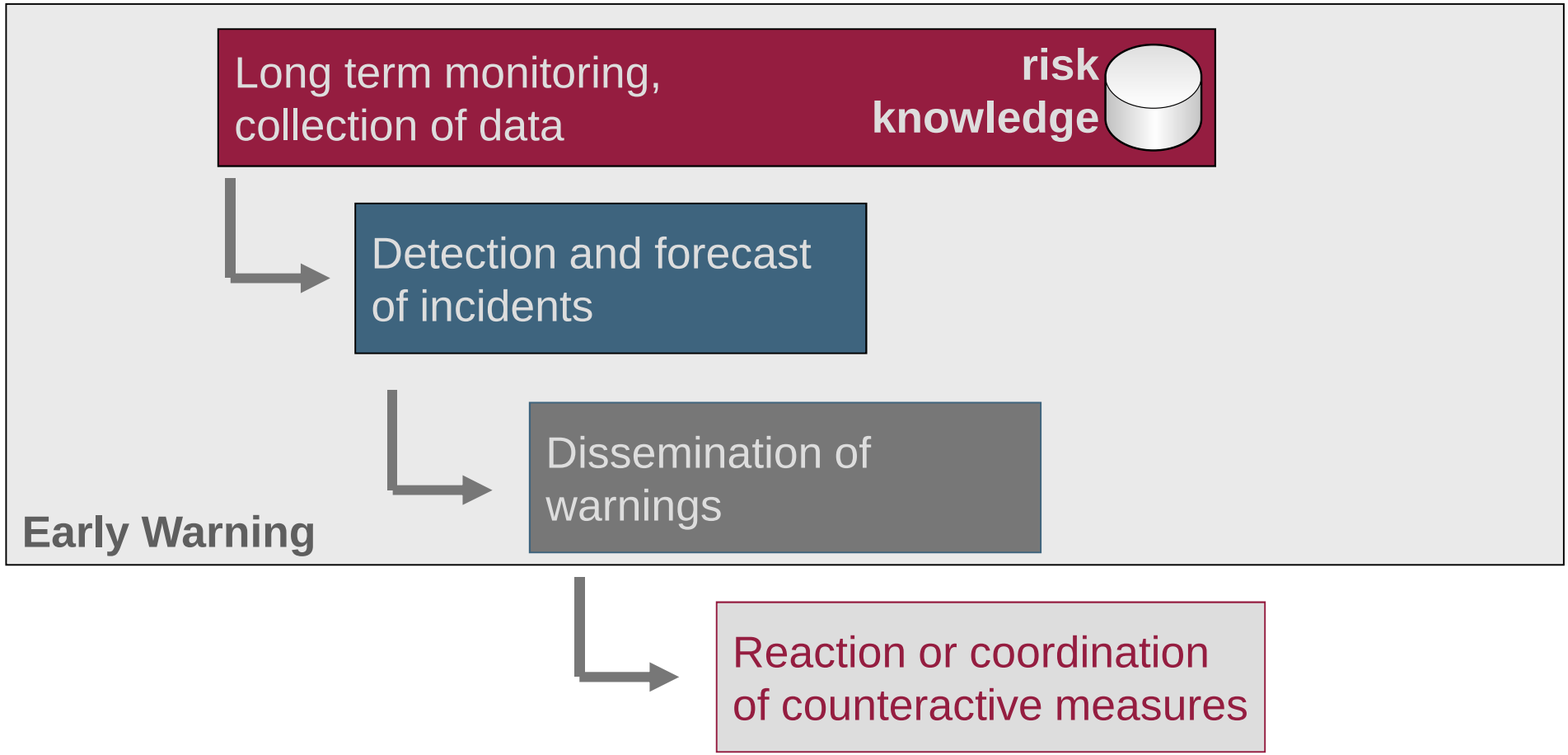
Technical Elements of an EWS
→ Architecture (AR) – 3/3

- **Decentralized architecture**
  - Not just the sensors, but also the analysis component and knowledge base are distributed
  - Whenever necessary the individual components exchange information
  - Alerts can be disseminated from one centralized unit or by the different distributed units
  - **pros**
    - Performance
    - Not so easy to be attacked
  - **cons**
    - More complex
    - Maintainability is more difficult

Content

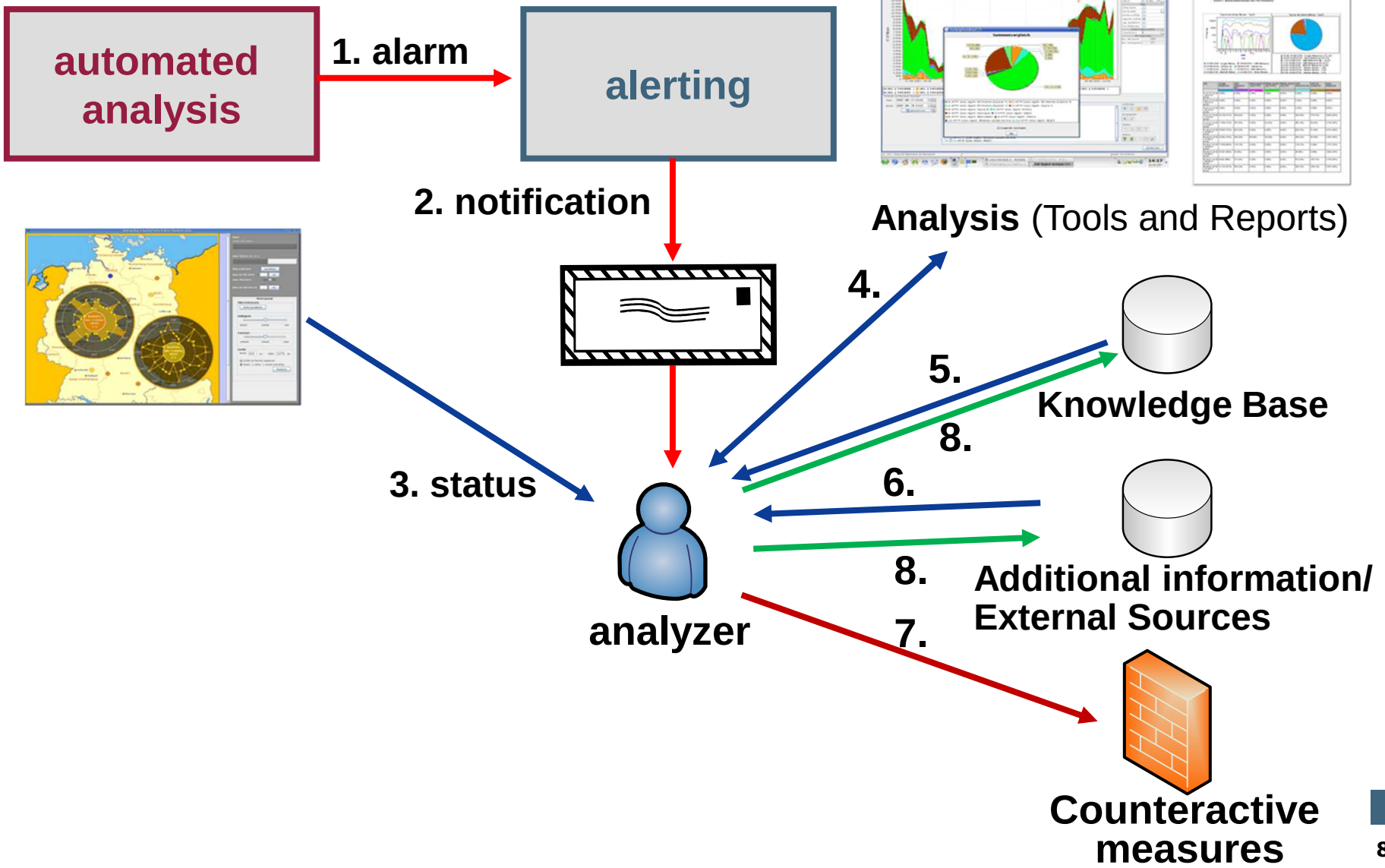
- Aim and outcomes of this lecture
- Motivation of Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- Structure of EWS
- **Process of EWS**
- Different realization of EWS
- Summary

Process of EWS
→ Warning process



- Early warning is a part of the risk management and of national homeland security systems, which protect a national territory from all sorts of natural and man-made hazards

Process of EWS
→Steps (1/2)



Process of EWS
→ Steps (2/2)

- 1. Security incident detected in data (alarm)
- 2. Concerned authorities are notified (e.g. e-mail)
- 3. See status (situation awareness)
- 4. Analyze the situation in more detail
- 5. Access to internal knowledge base
  - Hints for solving the problems
- 6. Access to further knowledge bases and external sources
  - Necessary, if local systems don't deliver enough information to solve the problem
- 7. Initiation of counteractive measures
  - Solving or reducing problems through counteractive measures
- 8. Update knowledge base and other sources
  - Newly generated knowledge, e.g. about problems or solutions to fix problems

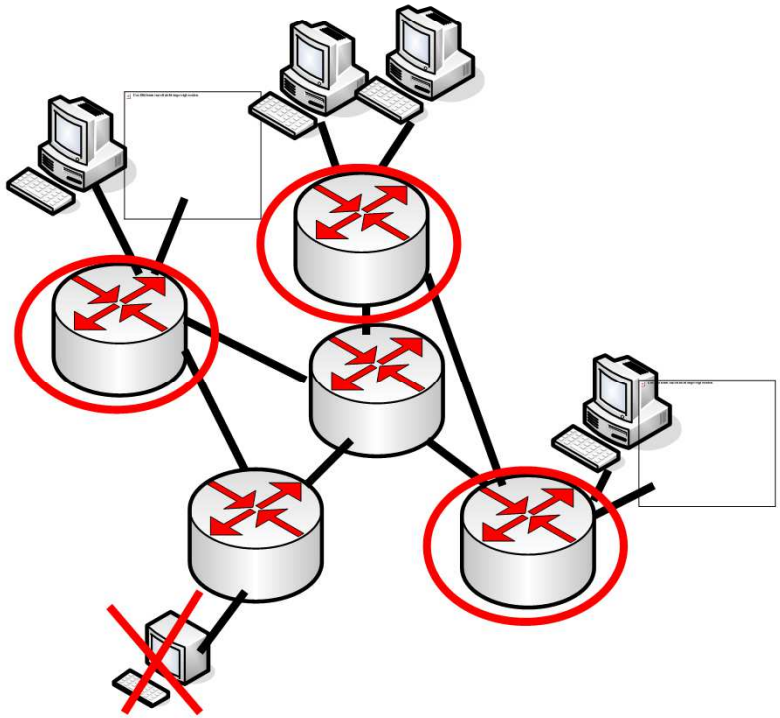
Process of EWS
→ Possible reactions (1/3)

- **Private users / enterprises**
  - Reduction of the possibilities (firewall, …)
  - Increasing security mechanisms
  - Selective shut-down (cut-off) of affected systems
    (without destroying evidence for possible criminal prosecution (forensics))
  - Complete deactivation of the uplink to the internet

- **Internet Service Provider**
  - Access Control Lists
  - Rate-Limiting
  - Blackholing
  - Off-Ramping / Sinkholing

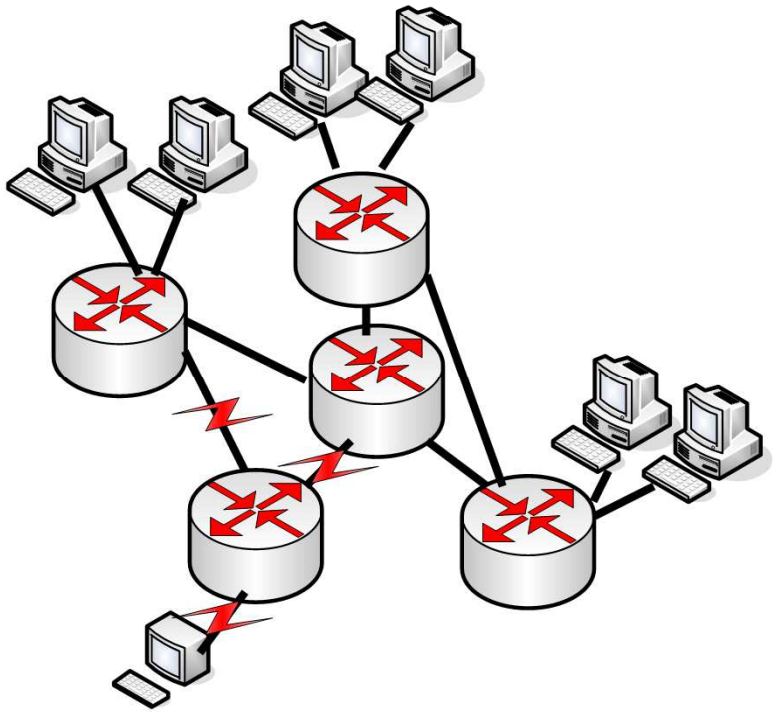
Process of EWS
→ Possible reactions (2/3)

Access Control Lists



e.g. black-, white- or grey-List

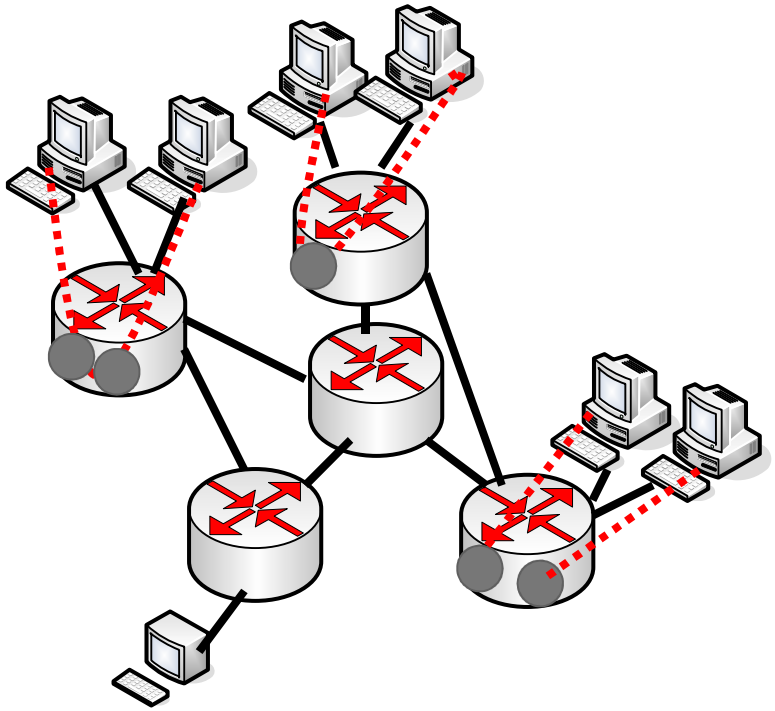
Rate-Limiting



e.g. traffic shaping, packet shaping, bandwidth throttling, …

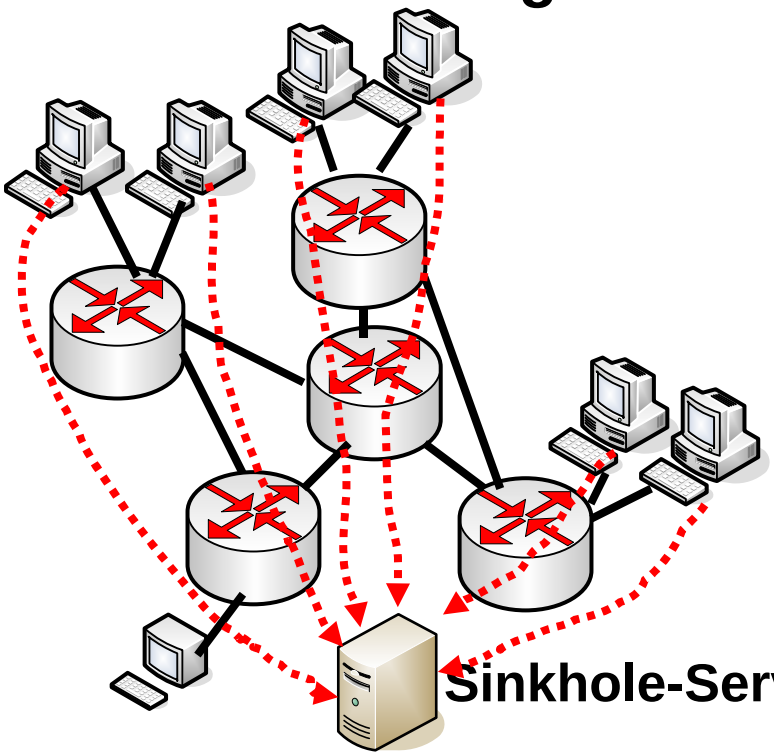
Process of EWS
→ Possible reactions (3/3)

Blackholing

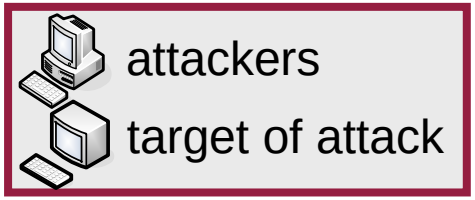


a null route (blackhole route) is a network route (routing table entry) that goes nowhere

Sinkholing



e.g. darknet (unused regions of IP address space), flow collectors, backscatter detectors, packet sniff…

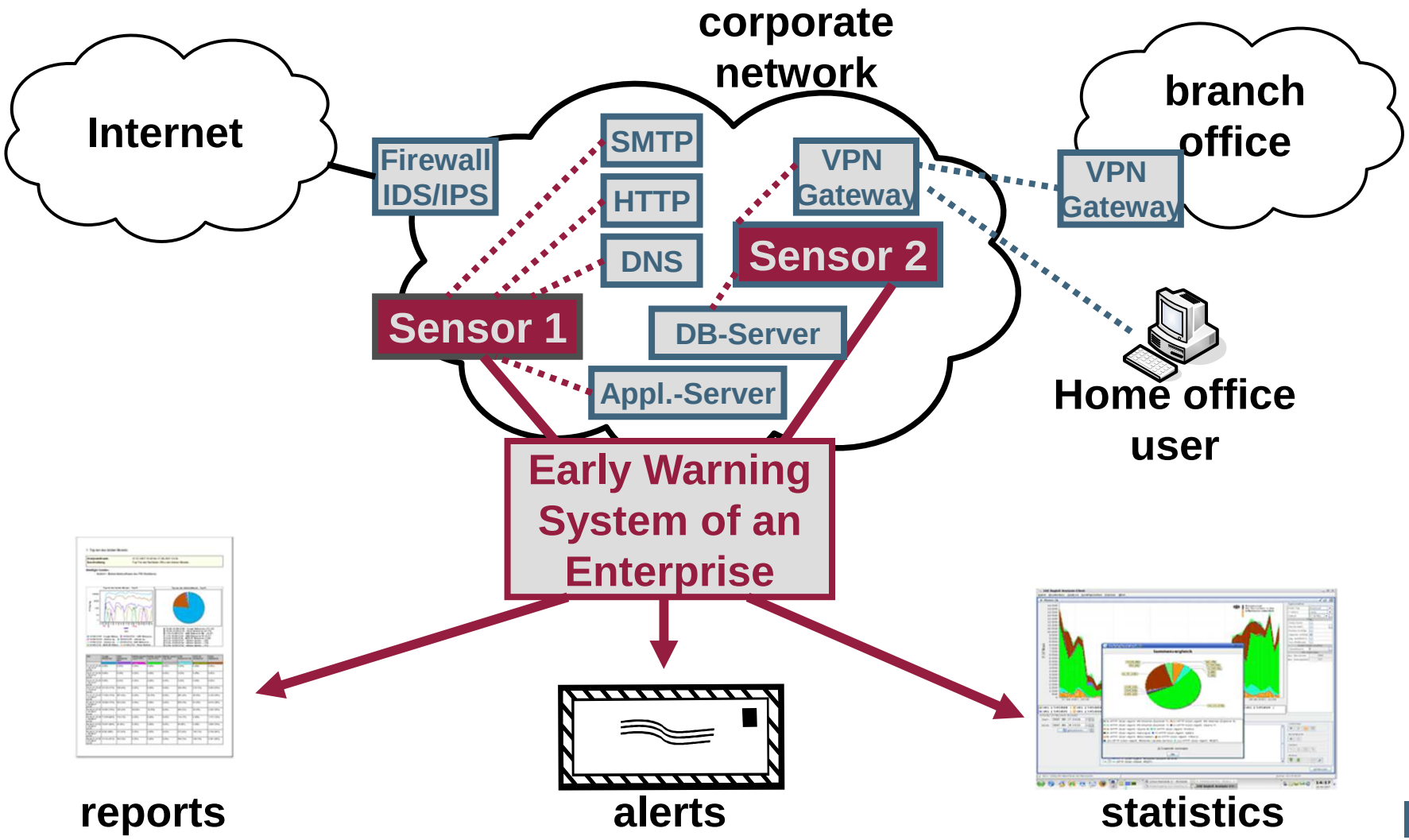


Content

- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- Structure of EWS
- Process of EWS
- **Different realization of EWS**
- Summary

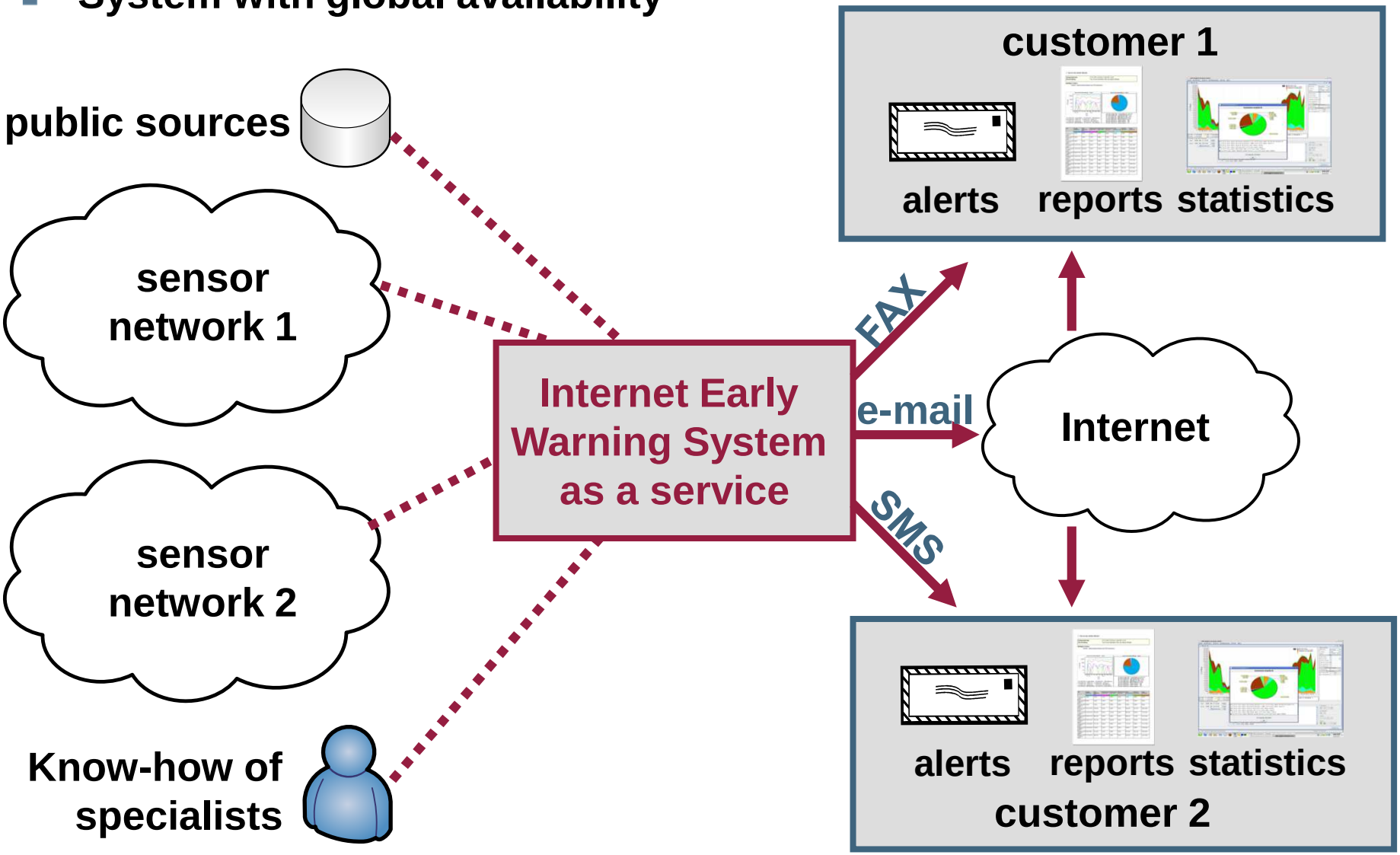
Different realization of EWS
→ Local installation

- Local installation



Different realization of EWS
→ System with global availability

- System with global availability



Different realizations of EWS
→ Existing systems

- Symantec DeepSight Threat Management System
- X-Force Threat Analysis Service von ISS
- Arbor Networks Peakflow X / SP
- Computer Associates – eTrust Network Forensics
- DShield.org – Distributed Intrusion Detection System
- **Internet Analysis System (IAS) of the Institute for Internet Security**
- **Internet Availability System (IVS) of the Institute for Internet Security**
- CarmentiS (Germany)
- NICT Daedalus Cyber-attack alert system

Content

- Aim and outcomes of this lecture
- Motivation of
  Early Warning Systems (EWS)
- Attacks
- Targets of EWS
- Structure of EWS
- Process of EWS
- Different realization of EWS
- **Summary**

Summary
→ Early Warning System (1/2)

- **Generation of an IT security situation awareness of the Internet (global view)**
  - **Current status**
    (Security, availability, load, spreading of protocols and services …)
  - **Existing attack scenarios**
    (Statistics on detected attacks …)
  - **Trends in general**
    (Technology, protocols, services …)
  - **Threat potential of the Internet**
    (Weakness, potential …)

- **The common global view helps:**
  - To judge the own local view more precisely.
  - React on developing trends very early to encounter potential damage in time.

Summary
→ Conclusion

- **Internet**
  - The internet is a critical infrastructure for our society
  - We need a trusted infrastructure to protect our future
  - Organisations running the infrastructure need to cooperate
- **We need the global view of the Internet**
  - To identify the current status
  - To see the new trends
  - To get ´early warnings´ to reduce damage
  - To make forecasts which help us to avoid damage
- Analogical to natural disaster warning systems, like the Tsunami warning system, we need a warning system for the internet to be able to issue counteractive measures before the actual threat strikes at us.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Early Warning System
→ Basic concept

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Early Warning System
→ Literature

- [1] Dr. Sabine Graumann and Florian Neinert. Monitoring Informationswirtschaft 9. Faktenbericht 2005, 2006.
- [2] BSI. Die Lage der IT-Sicherheit in Deutschland 2005. Technical Report, Bundesamt für Sicherheit in der Informationstechnik, 2005.
- [3] http://de.wikipedia.org
- [4] Stefan Korte: Internet-Frühwarnsysteme (internet early warning systems), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2006

Links:

Institute for Internet Security:
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/internet-frhwarnsysteme/

SANS Internet Storm Center
http://isc.sans.org/