Cybersecurity Management
GCS-1.1.Monitoring

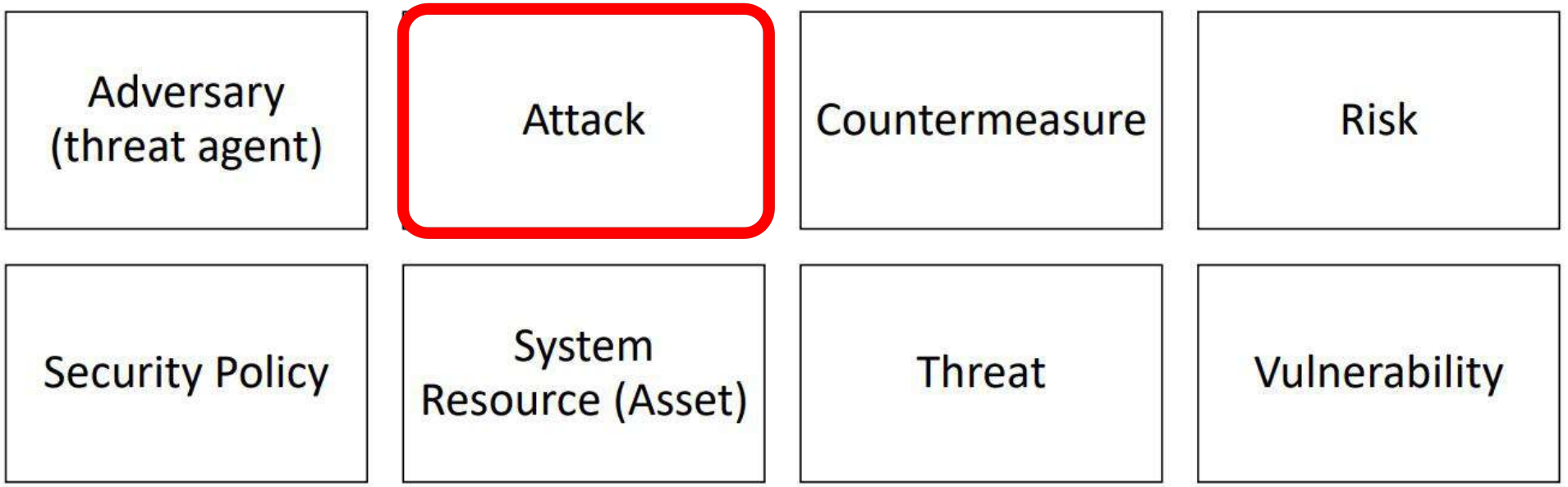
2022-2023

Prof. Raül Roca

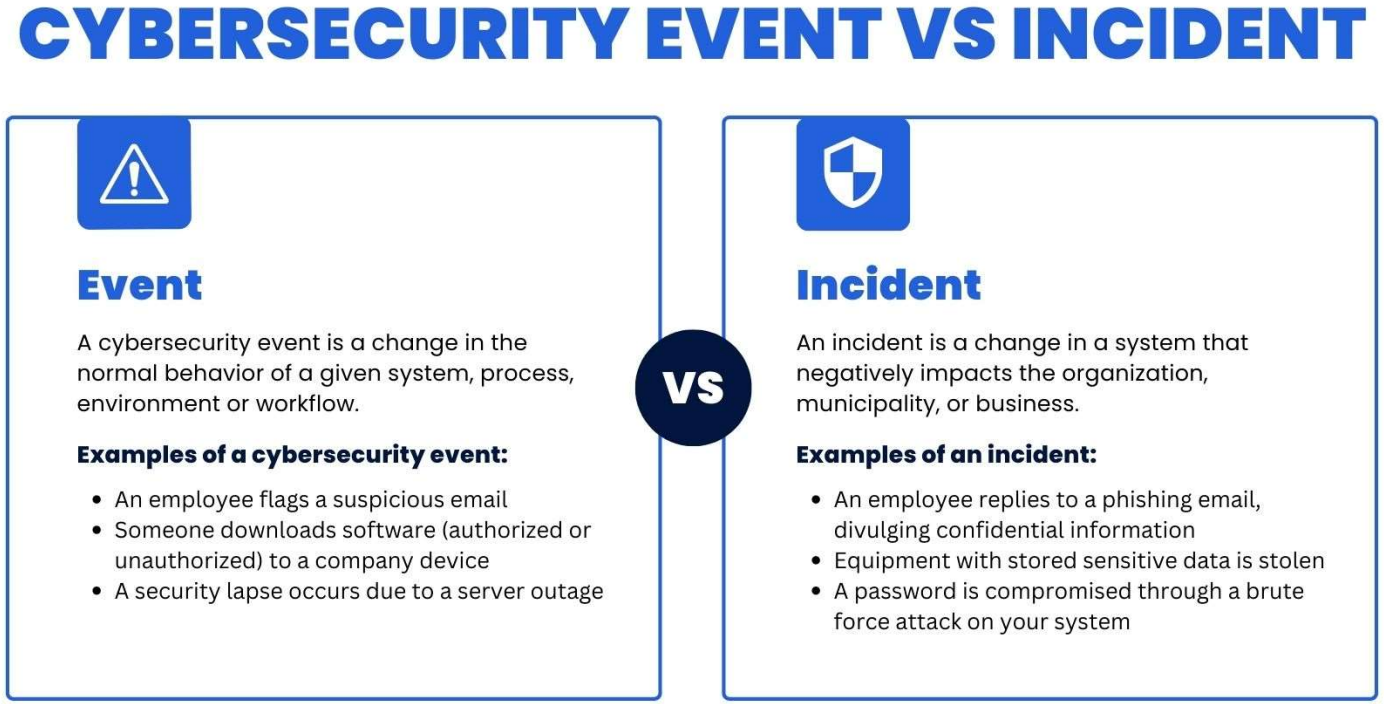
raul.roca-canovas@upc.edu

linkedin.com/in/roca-cybersecurity

Basic concepts



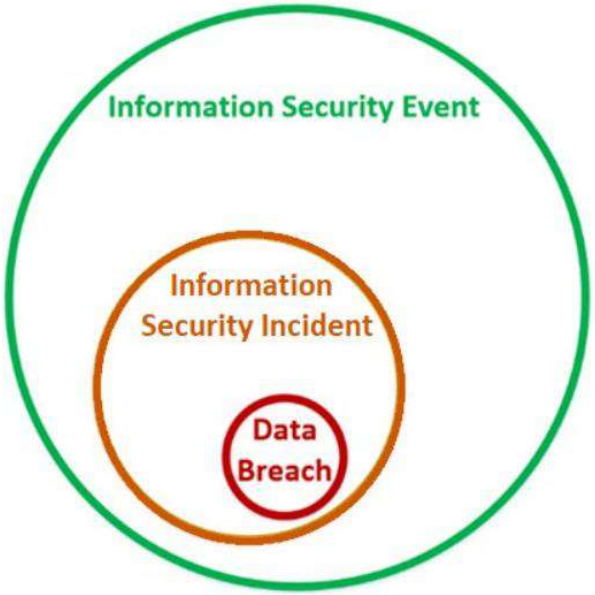
Additional concepts (related to attacks)



Additional concepts (related to attacks)

Information Security Event Definition:
Any observable occurrence in the operations of a network or information technology service, system or data indicating that a security policy may have been violated or a security safeguard may have failed.

Information Security Incident Definition:
An information security **event** where it is alleged or suspected that unauthorized access, use, modification, or disclosure of printed, electronic, audio or visual non-public institutional data to an unauthorized individual or entity may have occurred.

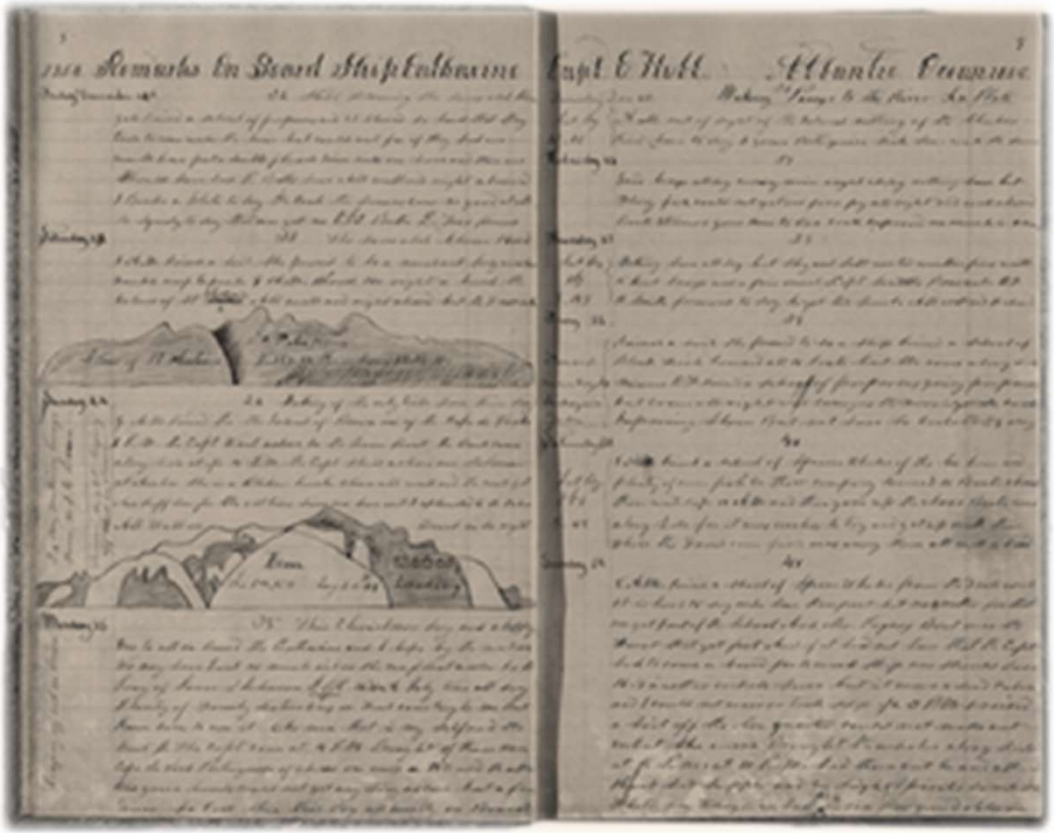


Information Data Breach Definition:
An information security **incident** validated by the Data Incident Response Team where unauthorized access, use, modification, or disclosure of information has occurred.

Exercise: read the four examples in https://cybersecurity.osu.edu/sites/default/files/security_events_to_potential_breach_examples.pdf

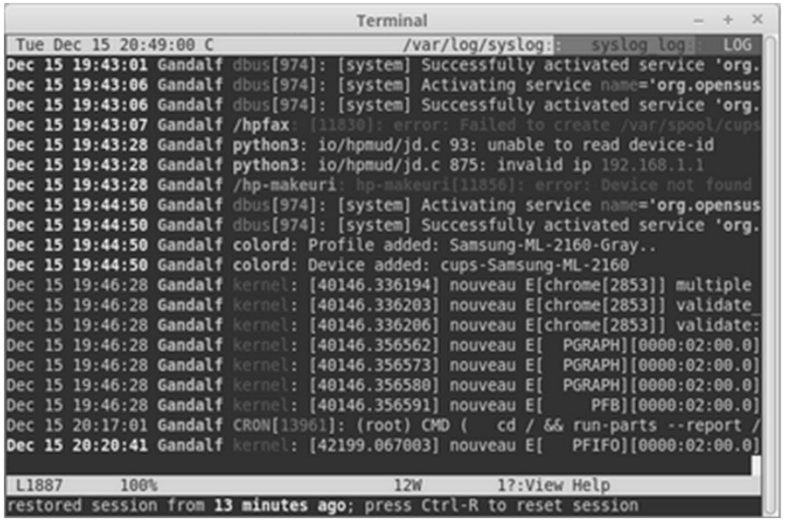
Introduction to logs

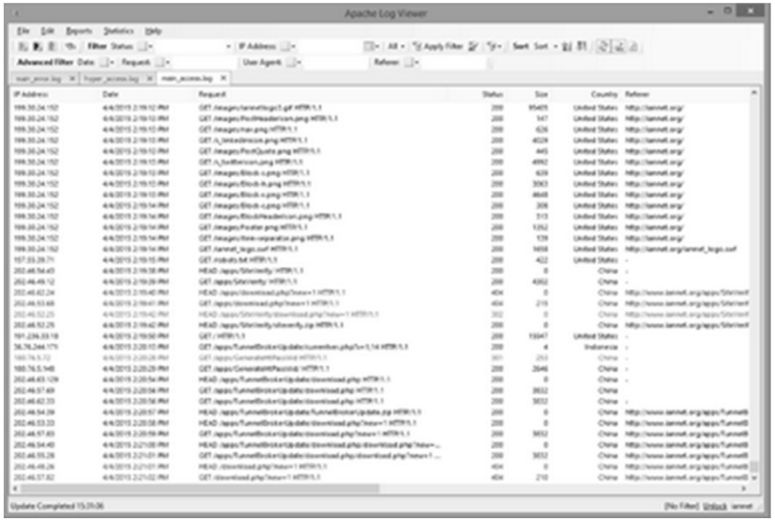
Logbook (cuaderno de bitácora)



Logbook (cuaderno de bitácora)

- System logs





- In IT: log (one record of a single event) = log file = logbook

Logbook (cuaderno de bitácora)

- Relevant event in a System. Questions:
  - Are there records of the System?
  - **Who** manages records?
  - How long are records **kept stored**?
- **logbook →**
  - **WHAT** happened
  - Lessons learned

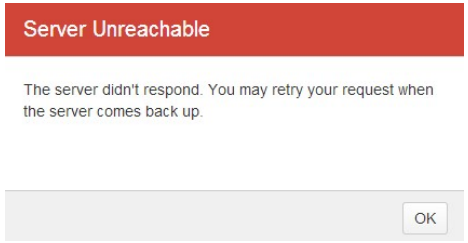
Aircraft black box

Logbook (cuaderno de bitácora)

- It is a key element in:
  - **Auditing**
    - validate everything to get a certification
  - **Regulations/Certifications**
    - demonstrate our behavior & the application of established processes
  - **Forensic Analysis**
    - follow an agreed process in order to preserve them as a **clue** in case of court trial

Events: Kinds of

Primary event	Derived event	Complex event
• Any circumstance, action or change in a System	• New event as a result of the application of a method or process applied to previous events.	• Abstraction of other events, known as dominant ones.



Events: potential logging issues

- DoD → t(between events) < t(needed to process them)
- Lack of storage space in a centralized system

Security events

- Must provide: **Traceability & Auditability.**
- Answers to:
  - **What** component was manipulated?
  - **When** did it happen?
  - **Who** did interact with the component of our interest?
  - **How** did the event happen?
  - **Why** the event was foreseen?

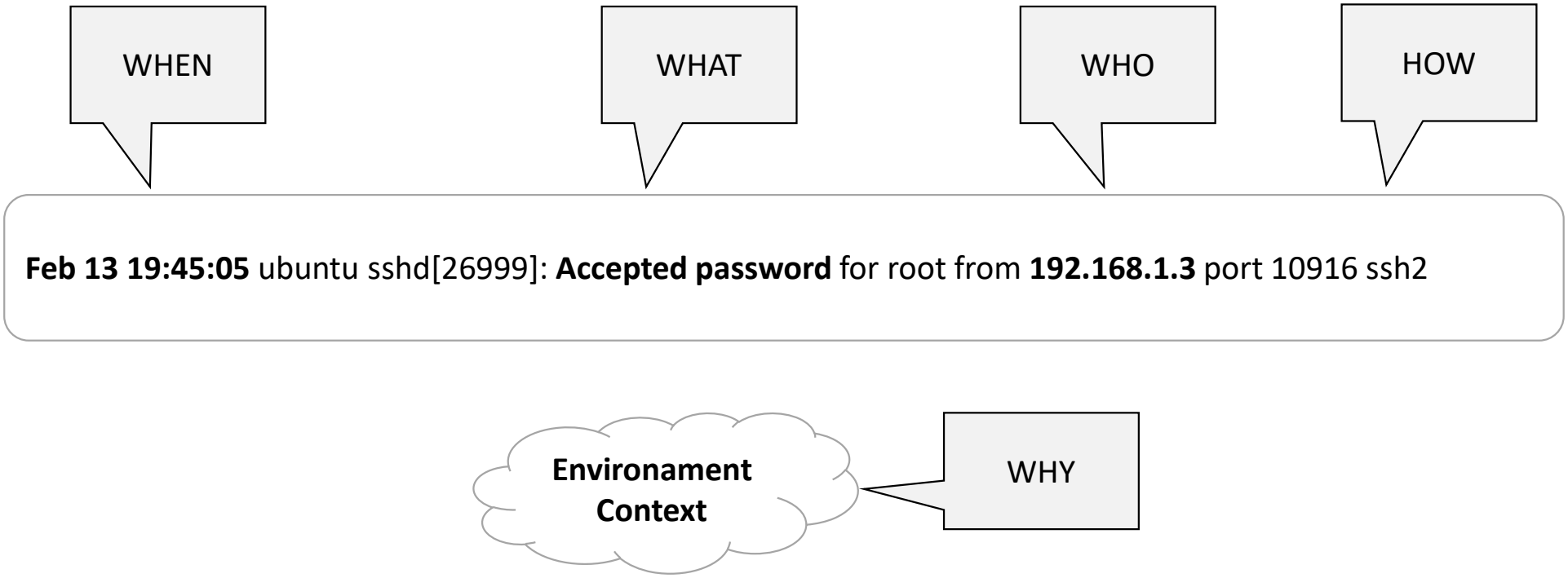
Security events: examples

Feb 13 06:55:26:%SEC_LOGIN-5-**LOGIN_SUCCESS:**Login Success [user: cisco] [Source: 10.10.1.5] [localport: 23] at 06:55:26 **UTC** Fri Feb 13 2015

Feb 13 19:45:05 ubuntu sshd[26999]: **Accepted password** for root from 192.168.1.3 port 10916 ssh2

Event Type: **Success** Audit Event Source: Security Event Category: Account **Logon** Event ID: 680 Date: 2015-02-13 Time: 23:53:00 User: NT AUTHORITY\SYSTEM Computer: MYSERVERNAME Description: Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: Administrator Source Workstation: MYCOMPUTER Error Code: 0x0

Security events: information

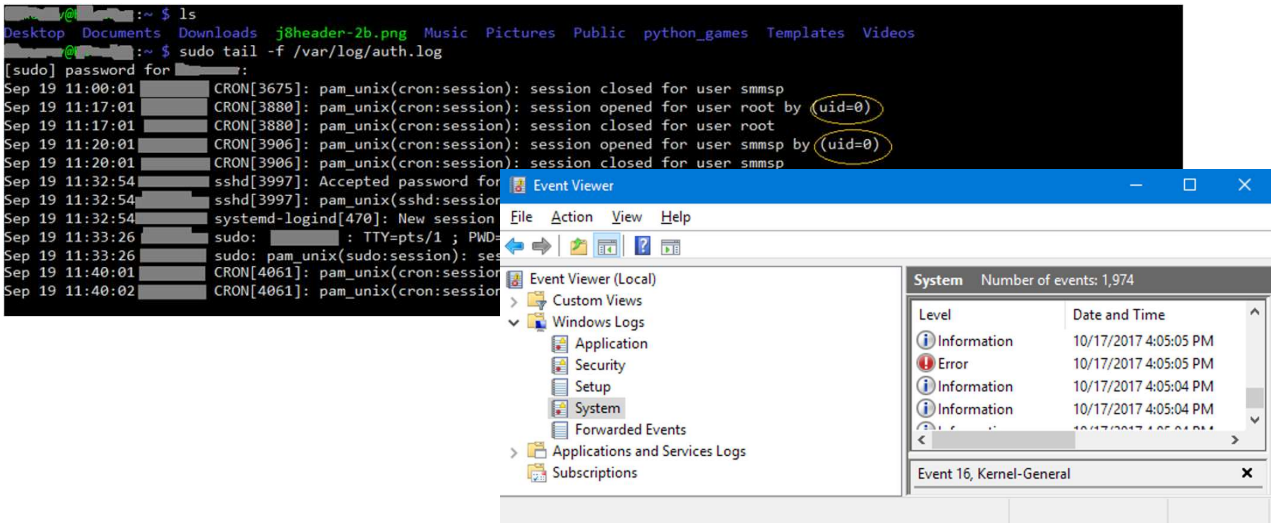


Security events: kind of

- **Out of working hours**
- **Brute force**
- **Unauthorized access**
- **Scans**
- **Spam**
- **Malware**
- Etc.

System Logs

- Files and directories used for:
  a) research & state the cause of a problem, or
  b) periodically monitor preventively
- Linux (GNU/Linux)
  - /var/log
- Microsoft Windows
  - Events (of Windows)
  - Record (log)



Log Management (LM)

- Processes large volumes of records
- Includes
  - **Collecting** event records (logs)
  - Centralized **Aggregation** of logs
  - Long-term **Retention → Granularity** changes over time
  - **Log Analysis**: in **Real Time** and **Bulk** after their storage
  - Record **Search**
  - **Report** production/compilation, submission/delivery

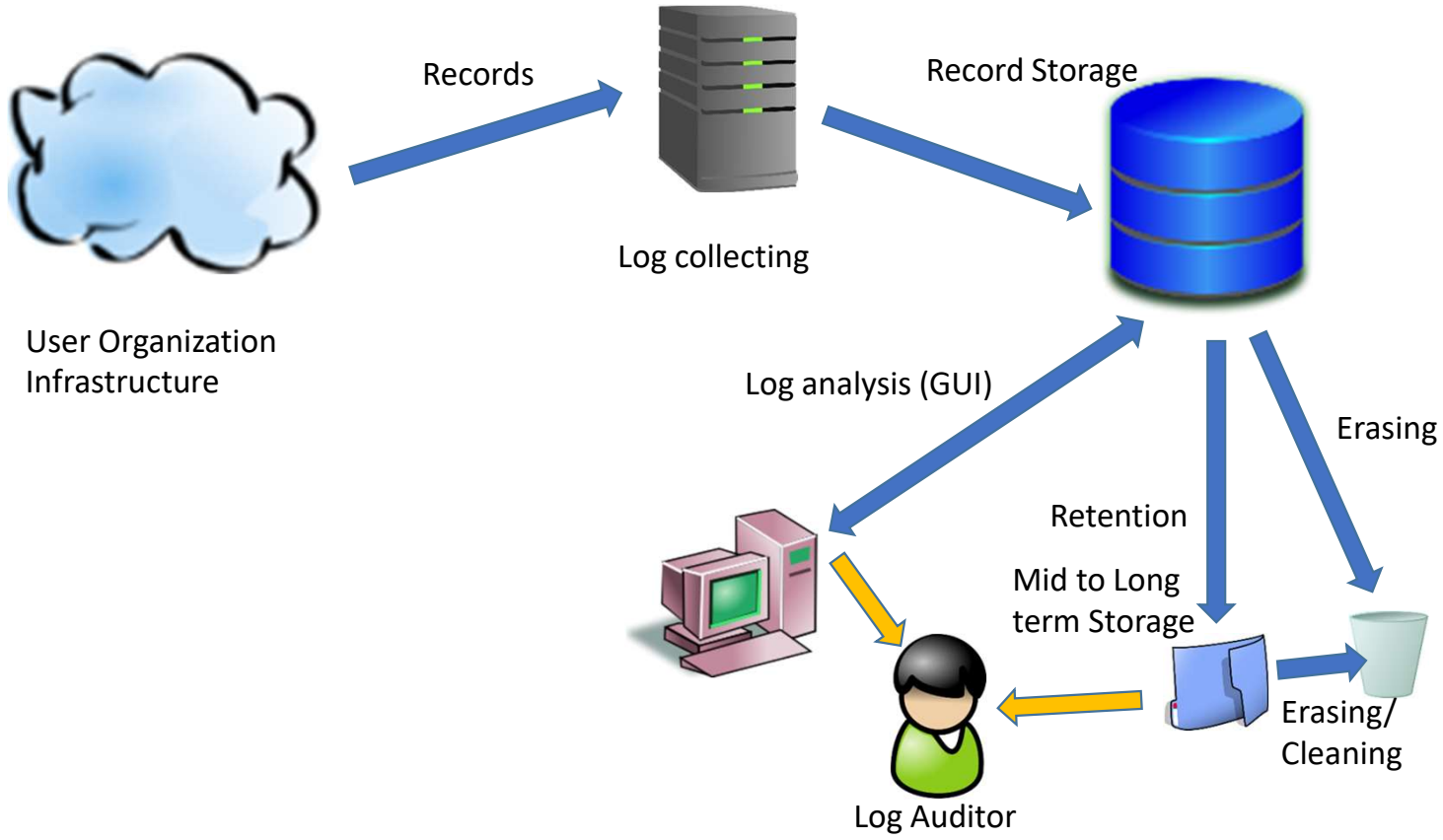
Log Management: Challenges

- Security Intelligence
- Centralized Collecting
- Effectiveness of analysis (Why? How?)
- Data → **Information**
- Traceability
- **IT Regulation Compliance**
  - E.g., NIST-800-53, PCI-DSS, GDPR, DNIS, etc.

Log Management: Key Elements

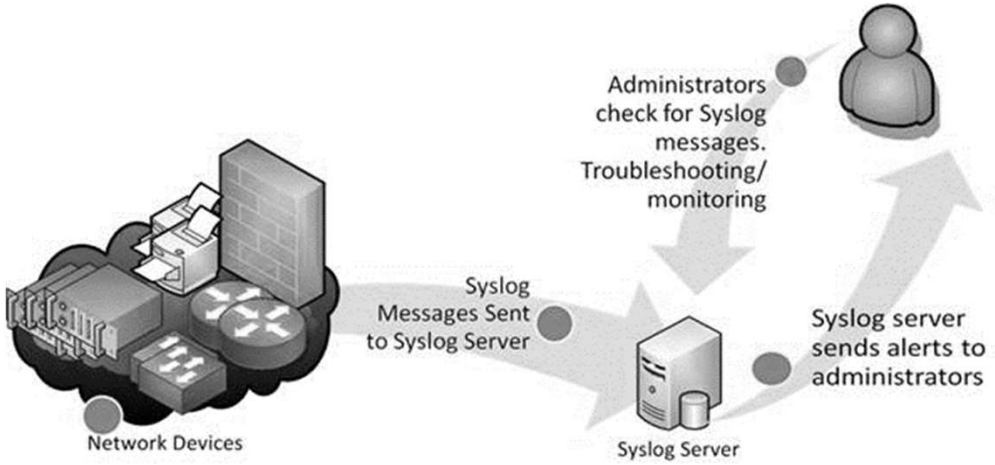
- Logs **volume**: Data Granularity & Retention time
- Logs **Format heterogeneity**: common format & parsing
- The **architecture of networks and systems**

Log Management: Schema



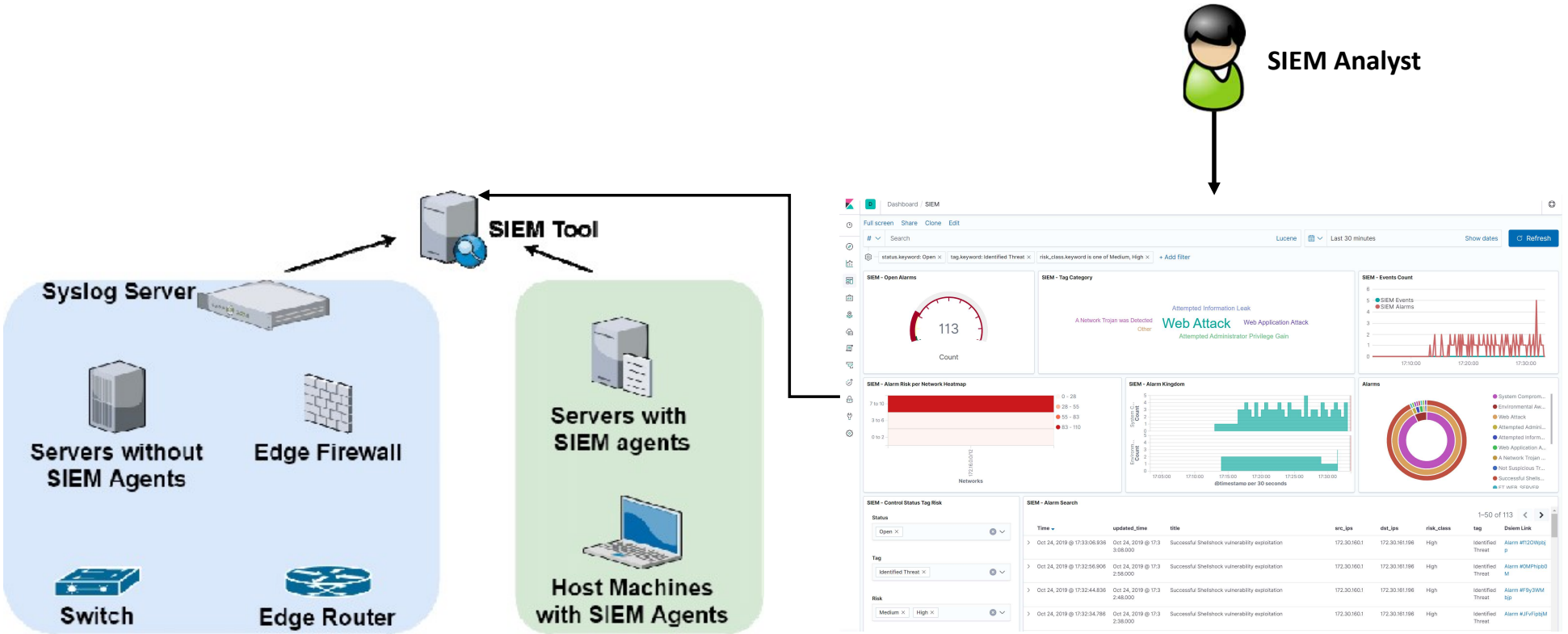
Syslog. Powerful registry system(UNIX)

- UNIX logging mechanism
  - Capturing relevant events
  - Storage facility
  - Protocol → syslog messages
    - **RFC 5424**
    - UDP / 514
    - **No state** between client and server
    - **No authentication** of the sender or reciprocal authentication of the recipient of the messages
    - Without proof reception
    - Brand of **uncoordinated time**
    - Content of the message or its format **non standardized** (noteven suggested**)**




```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo
for ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

SIEM. Security Information & Event Management



SIEM: Schema

SIEM control panel (ELK)

SIEM Use cases

Threat detection

Detect security threats using rule-based log correlation engines, threat modeling framework (MITRE ATT&CK) integrations, and anomaly detection.

Anomaly detection

Spot advanced persistent threats and sophisticated attacks using AI- and ML-driven user and entity behavior analytics (UEBA).

Cloud security

Protect multi-cloud environments by auditing security events and enforcing security policies for access to cloud resources.

Compliance auditing

Prove compliance with regulatory mandates and generate audit-ready reports in a few clicks.

Security analytics

Continuously monitor security events from different sources across the network with analytical dashboards.

Endpoint protection

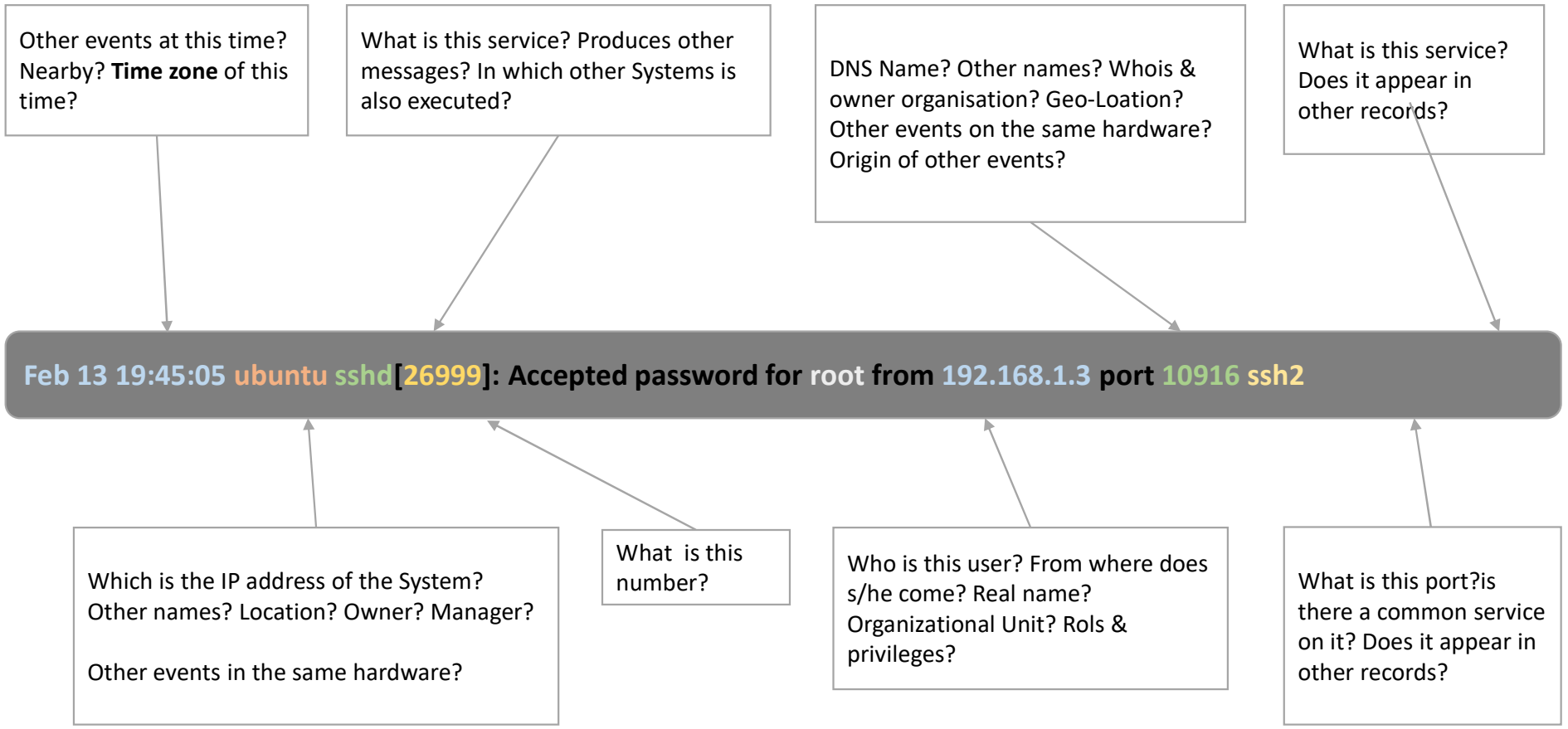
Monitor and protect your endpoints proactively from cyberthreats.

SIEM components

- Security Information Management (SIM)
  - Long-term **storage**
  - **Analysis** of registration data
  - **Reports**
- Security Event Manager (SEM)
  - Real-time **monitoring**
  - **Correlation** of events
  - **Notifications** and alerts
  - Consoles, views, and **dashboards**

SIEM = SIM + SEM = long & short + real-time

SIEM: Record & context

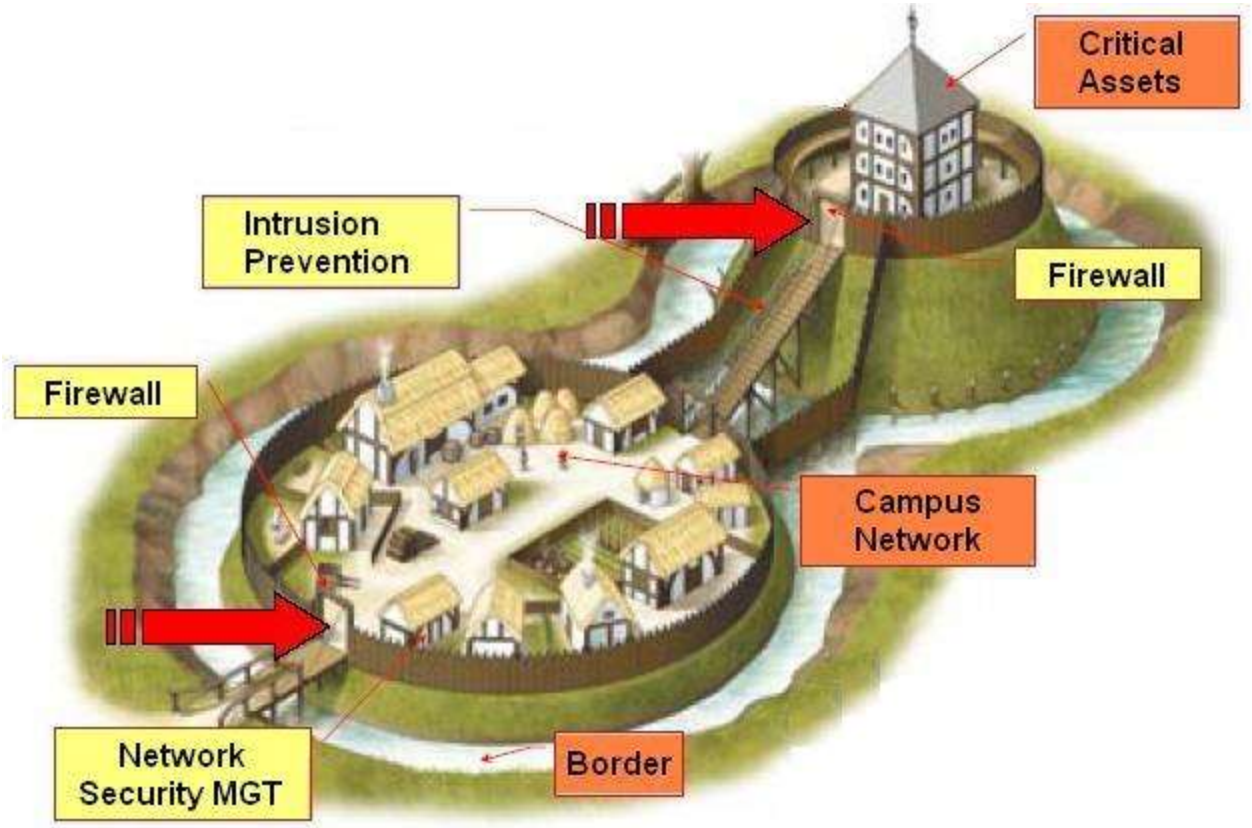


SIEM vs. LM

Functionality	SIEM	LM
Log collection	Collects relevant records for **security & context Data**	Collects all records
Records pre-processing	Analysis, enrichment, **Standardization (harmonization)**, categorization, etc.	Indexing, Analysis or nothing
Logs Retention	Analyzed data retention in Standard format	Analyzed data retention in native format
Reports	Personalized Reports focused in security	General purpose reports
Analysis	Correlation, threat evolution, event prioritization	Full-text analysis, tagging
Alarms and Notifications	Advanced reports, security-focused	Simple Alerts on all logs
Other functionalities	Incident Management, context analysis, etc.	High scalability of collection and storage

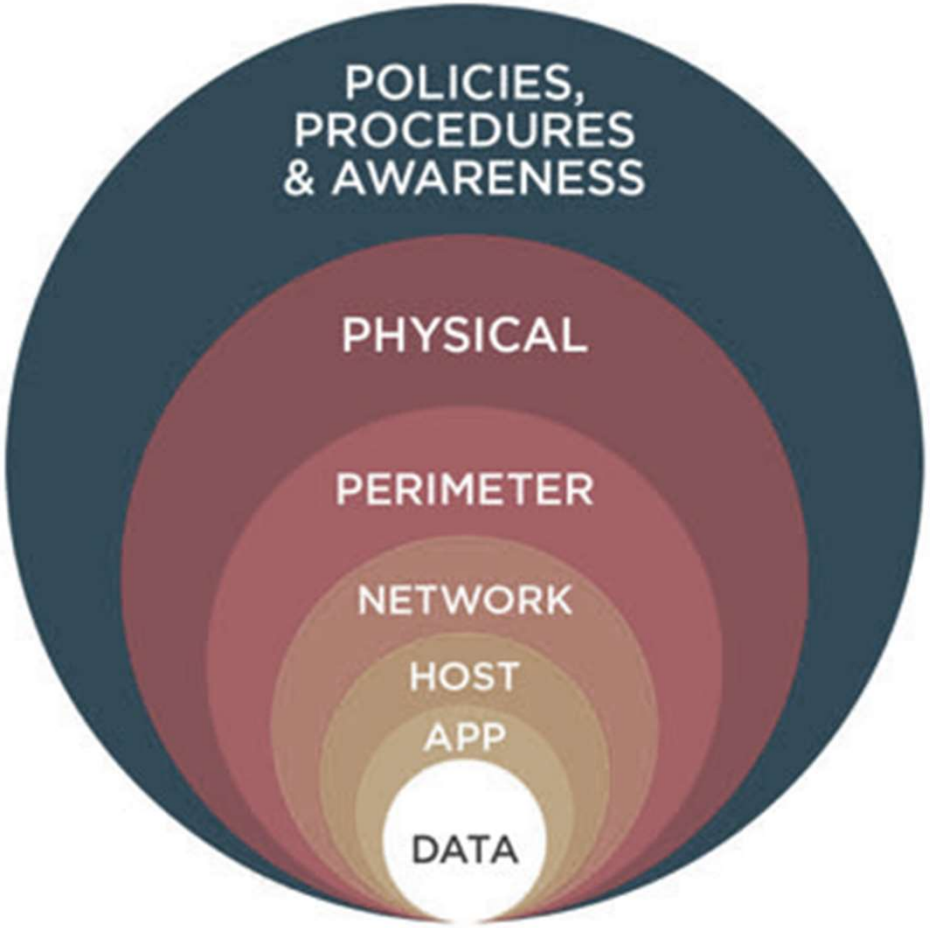
Use case: Intrusion detection

Defense in depth (deep defense or elastic defense)



The attacker can overcome some obstacles but cannot sustain the attack for a long time.

Defense in depth

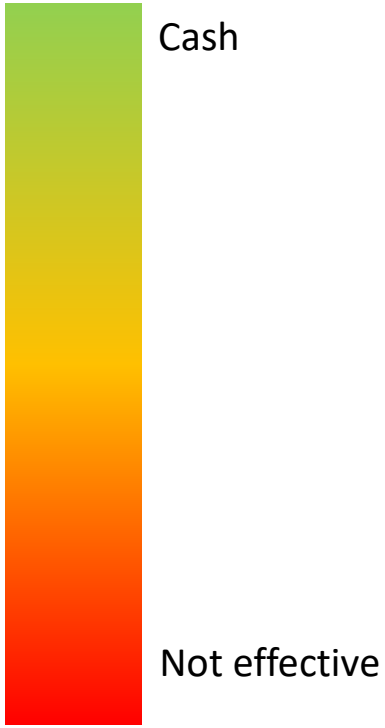


Intrusion Detection System (IDS)

- Intrusion
  - any unauthorized attempt or access to a system
  - malicious use of its resources
- IDS
  - HW/SW
  - identify signs of malicious activity in the network
    - CIA
    - Attacks against a computer or network

Effectiveness of IDS

- **Known** (less sophisticated attacks)
  - Groups Hacktivists
  - Scams by large-scale email
  - n-day attacks
- **Targeted attacks** (more sophisticated attacks)
  - Criminals
  - States, Terrorists
- **New** vulnerabilities
  - Zero-day, 1-day exploits



IDS classification

- **Where** are they running? (**Deployment**)
  - Host-based: **HIDS**
    - Monitoring → Incoming packages, Login activities, Activities of root, File systems
  - Network-based: **NIDS**
    - Monitoring → The traffic on the network to which the hosts are connected

- **How** do they perform the detection? (**Algorithms**)
  - Based on **signatures** (**knowledge**)
  - Based on **anomalies** (**behavior**)

Architecture of an IDS