

# Cybersecurity Management

## GCS-1.1.Monitoring

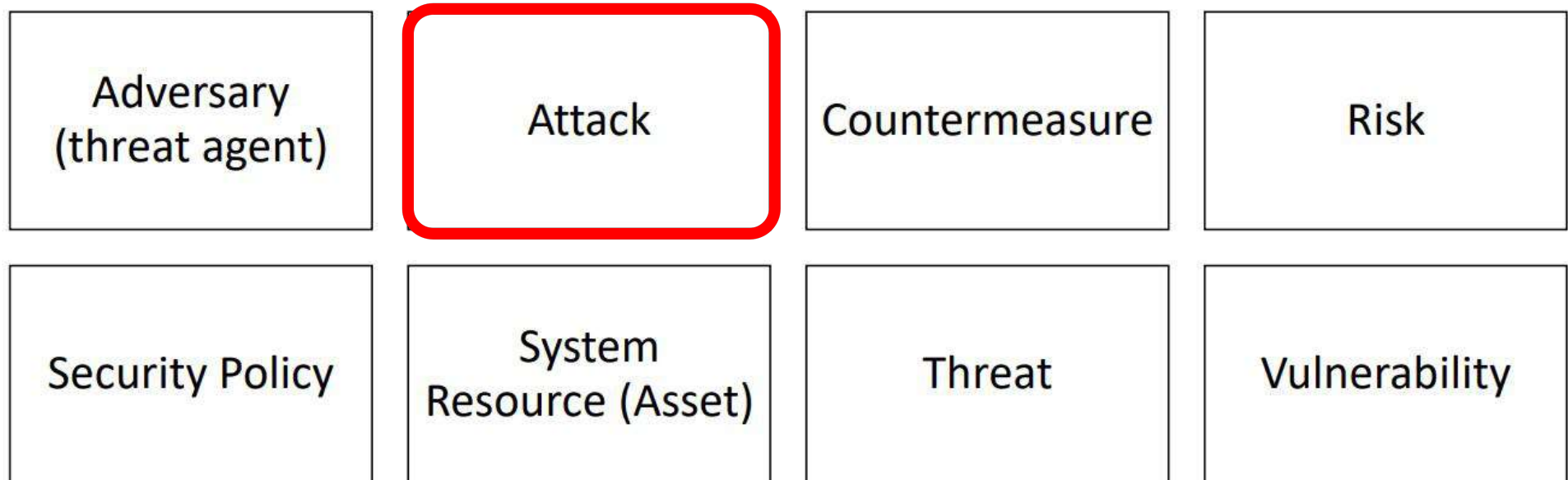
2022-2023

Prof. Raül Roca

[raul.roca-canovas@upc.edu](mailto:raul.roca-canovas@upc.edu)

[linkedin.com/in/roca-cybersecurity](https://www.linkedin.com/in/roca-cybersecurity)

# Basic concepts



# Additional concepts (related to attacks)



## CYBERSECURITY EVENT VS INCIDENT



### Event

A cybersecurity event is a change in the normal behavior of a given system, process, environment or workflow.

#### Examples of a cybersecurity event:

- An employee flags a suspicious email
- Someone downloads software (authorized or unauthorized) to a company device
- A security lapse occurs due to a server outage

VS



### Incident

An incident is a change in a system that negatively impacts the organization, municipality, or business.

#### Examples of an incident:

- An employee replies to a phishing email, divulging confidential information
- Equipment with stored sensitive data is stolen
- A password is compromised through a brute force attack on your system

# Additional concepts (related to attacks)

## Information Security Event Definition:

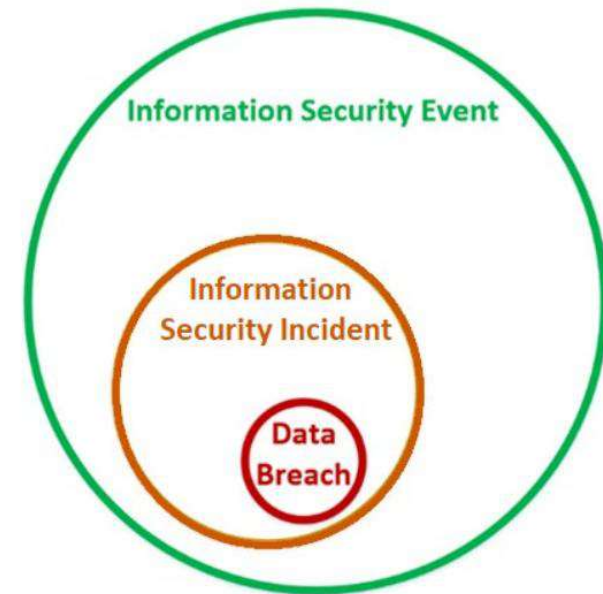
Any observable occurrence in the operations of a network or information technology service, system or data indicating that a security policy may have been violated or a security safeguard may have failed.

## 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.

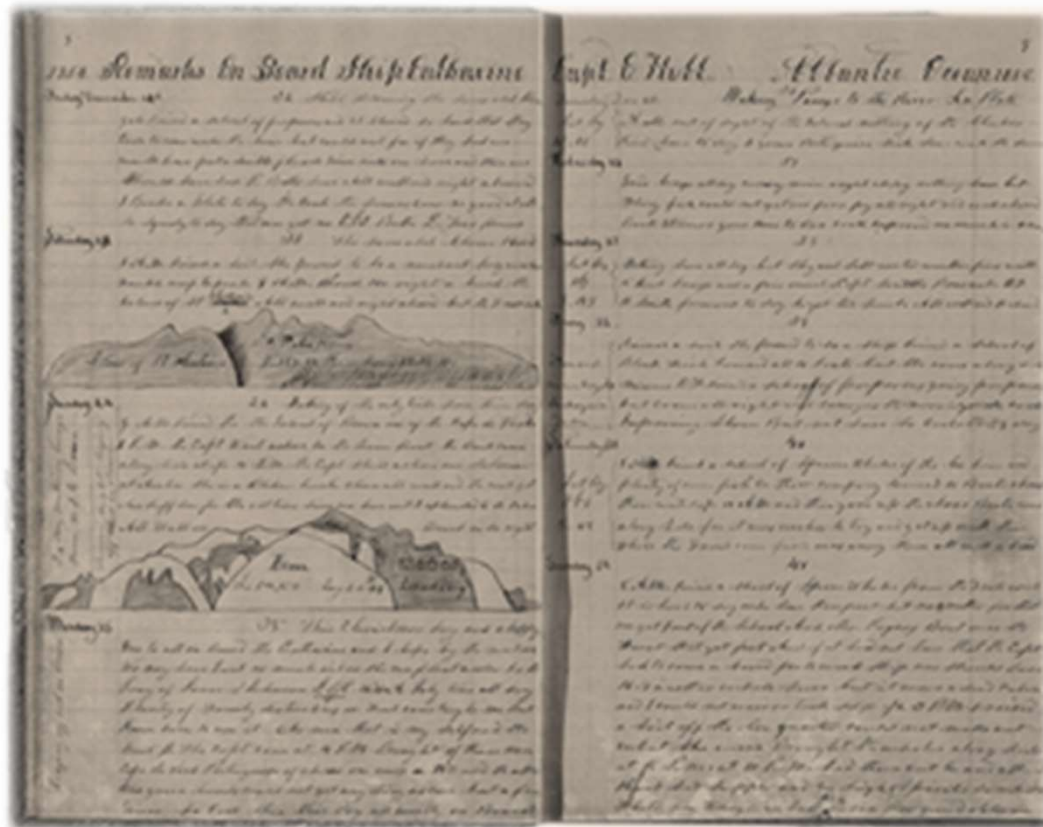


**Exercise:** read the four examples in

[https://cybersecurity.osu.edu/sites/default/files/security\\_events\\_to\\_potential\\_breach\\_examples.pdf](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

```

Terminal
Tue Dec 15 20:49:00 C /var/log/syslog: syslog log: LOG
Dec 15 19:43:01 Gandalf dbus[974]: [system] Successfully activated service 'org.
Dec 15 19:43:06 Gandalf dbus[974]: [system] Activating service name='org.opensu
Dec 15 19:43:06 Gandalf dbus[974]: [system] Successfully activated service 'org.
Dec 15 19:43:07 Gandalf /hpfax [11830]: error: failed to create /var/spool/cups
Dec 15 19:43:28 Gandalf python3: io/hpmdm/jd.c 93: unable to read device-id
Dec 15 19:43:28 Gandalf python3: io/hpmdm/jd.c 875: invalid ip 192.168.1.1
Dec 15 19:43:28 Gandalf /hp-makeuri: hp-makeuri[11856]: error: Device not found.
Dec 15 19:44:50 Gandalf dbus[974]: [system] Activating service name='org.opensu
Dec 15 19:44:50 Gandalf dbus[974]: [system] Successfully activated service 'org.
Dec 15 19:44:50 Gandalf colord: Profile added: Samsung-ML-2160-Gray..
Dec 15 19:44:50 Gandalf colord: Device added: cups-Samsung-ML-2160
Dec 15 19:46:28 Gandalf kernel: [40146.336194] nouveau E[chrome[2853]] multiple
Dec 15 19:46:28 Gandalf kernel: [40146.336203] nouveau E[chrome[2853]] validate
Dec 15 19:46:28 Gandalf kernel: [40146.336206] nouveau E[chrome[2853]] validate:
Dec 15 19:46:28 Gandalf kernel: [40146.356562] nouveau E[ PGRAPH][0000:02:00.0
Dec 15 19:46:28 Gandalf kernel: [40146.356573] nouveau E[ PGRAPH][0000:02:00.0]
Dec 15 19:46:28 Gandalf kernel: [40146.356580] nouveau E[ PGRAPH][0000:02:00.0]
Dec 15 19:46:28 Gandalf kernel: [40146.356591] nouveau E[ PFB][0000:02:00.0]
Dec 15 20:17:01 Gandalf CRON[13961]: (root) CMD ( cd / && run-parts --report /
Dec 15 20:20:41 Gandalf kernel: [42199.067003] nouveau E[ PFIFO][0000:02:00.0]

L1887 100% 12W 17:View Help
restored session from 13 minutes ago; press Ctrl-R to reset session

```

Apache Log Viewer						
File	Error	Status	Details	Help		
Filter Name		IP Address	All	Apply Filter	Sort	Search
Advanced Filter Data		Request	Use Apache			
Log File	Log File	Log File	Log File	Log File	Log File	Log File
IP Address	Date	Request	Status	Size	Country	Referer
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	64675	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.24.192	200	547	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/healthcheck.php?ip=198.50.24.192	200	626	United States	http://www.198.50.24.192
198.50.24.192	4/4/2015 2:10:12 AM	GET /api/status.php?ip=198.50.2				

- 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

- Any circumstance, action or change in a System

## Derived event

- New event as a result of the application of a method or process applied to previous events.

## Complex event

- Abstraction of other events, known as dominant ones.



ICMP *failure*

### Server Unreachable

The server didn't respond. You may retry your request when the server comes back up.

OK

# Events: potential logging issues

- DoD  $\rightarrow t(\text{between events}) < t(\text{needed to process them})$
- 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

WHEN

WHAT

WHO

HOW

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

**Environament  
Context**

WHY

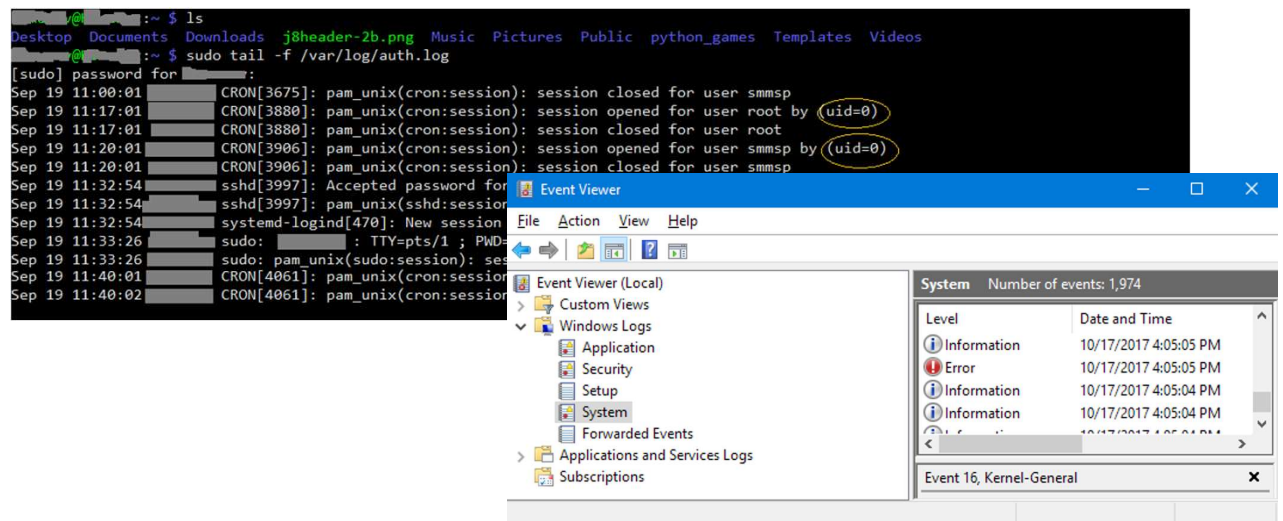
# Security events: kind of

- **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

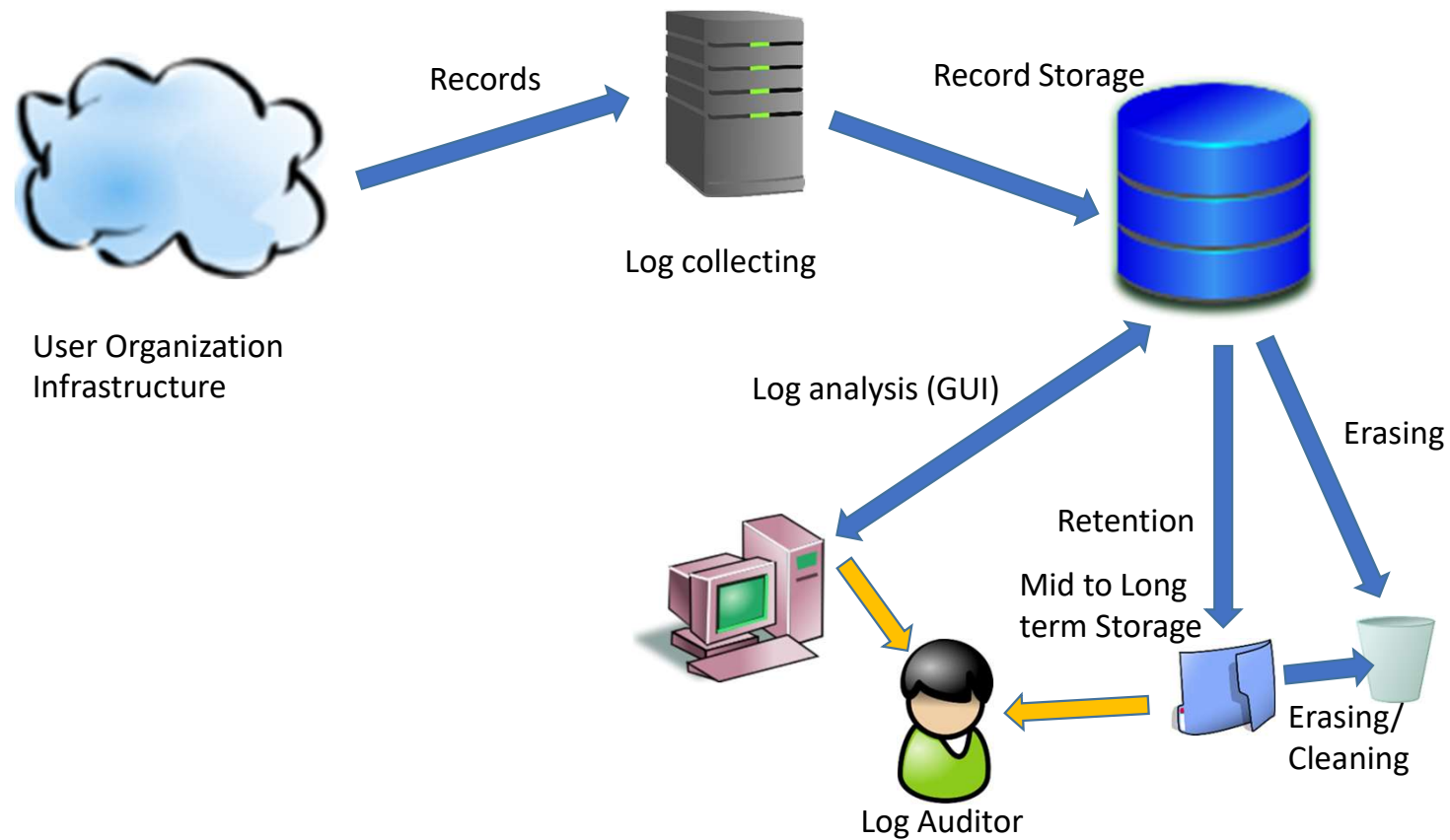
# Log Management: Challenges

- 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

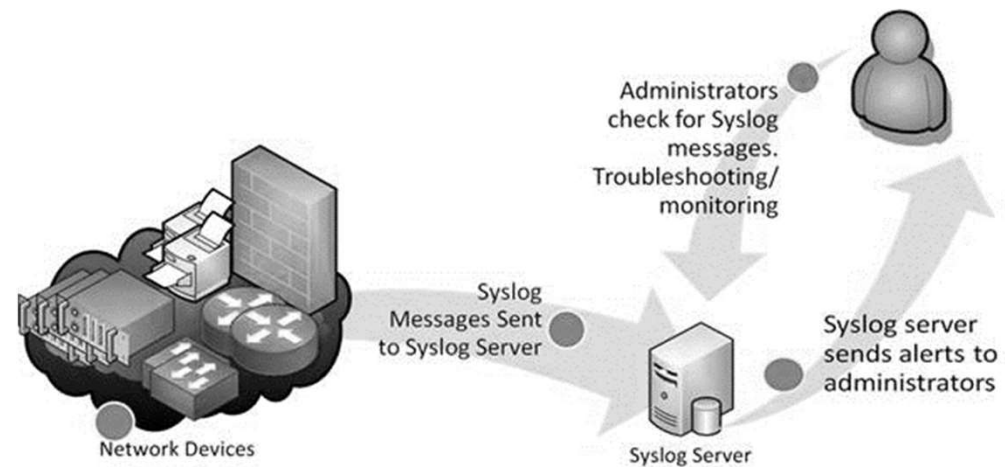
- Logs **volume**: Data Granularity & Retention time
- Logs **Format heterogeneity**: common format & parsing
- The **architecture of networks and systems**

# Log Management: Schema



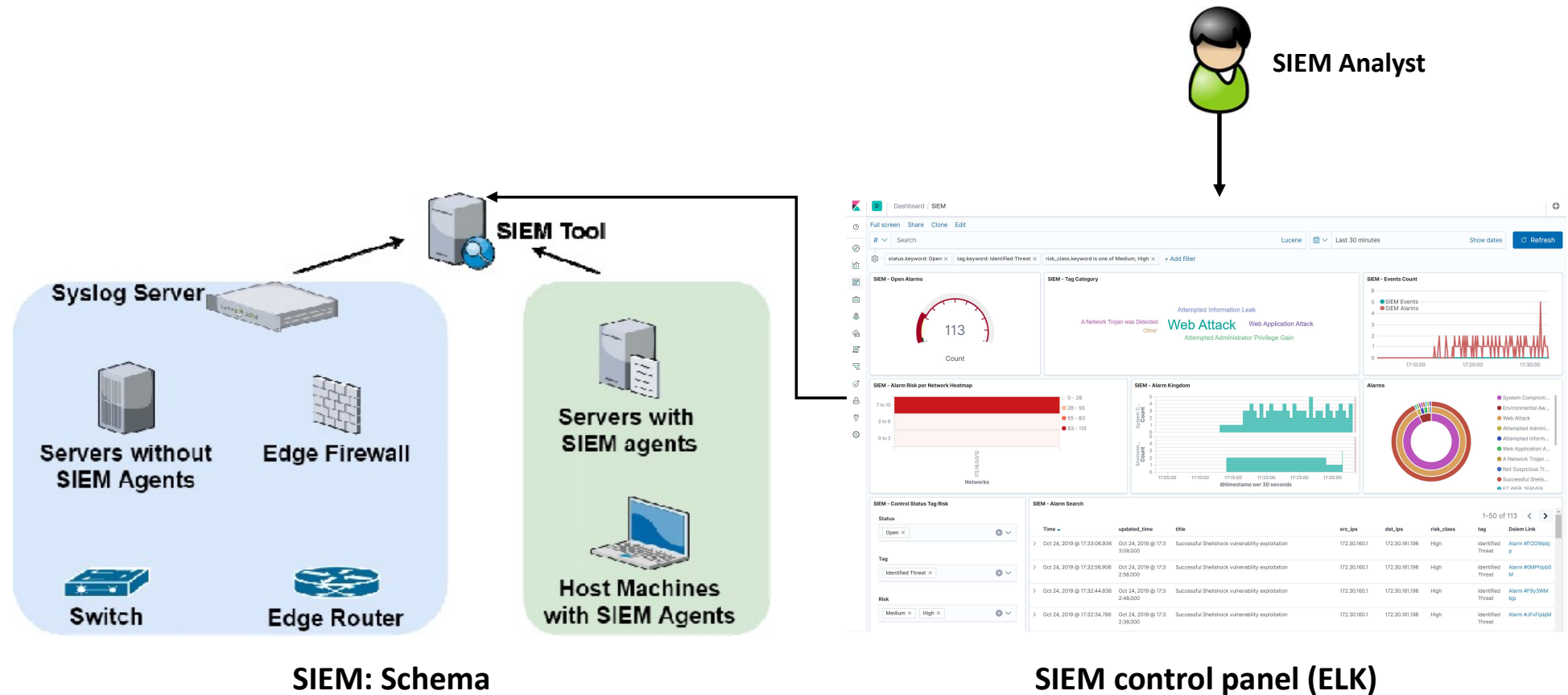
# Syslog. Powerful registry system(UNIX)

- 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/tty2
Mar 1 07:28:41 server1 su: kkent to root on /dev/tty2
```

# SIEM. Security Information & Event Management





# 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.



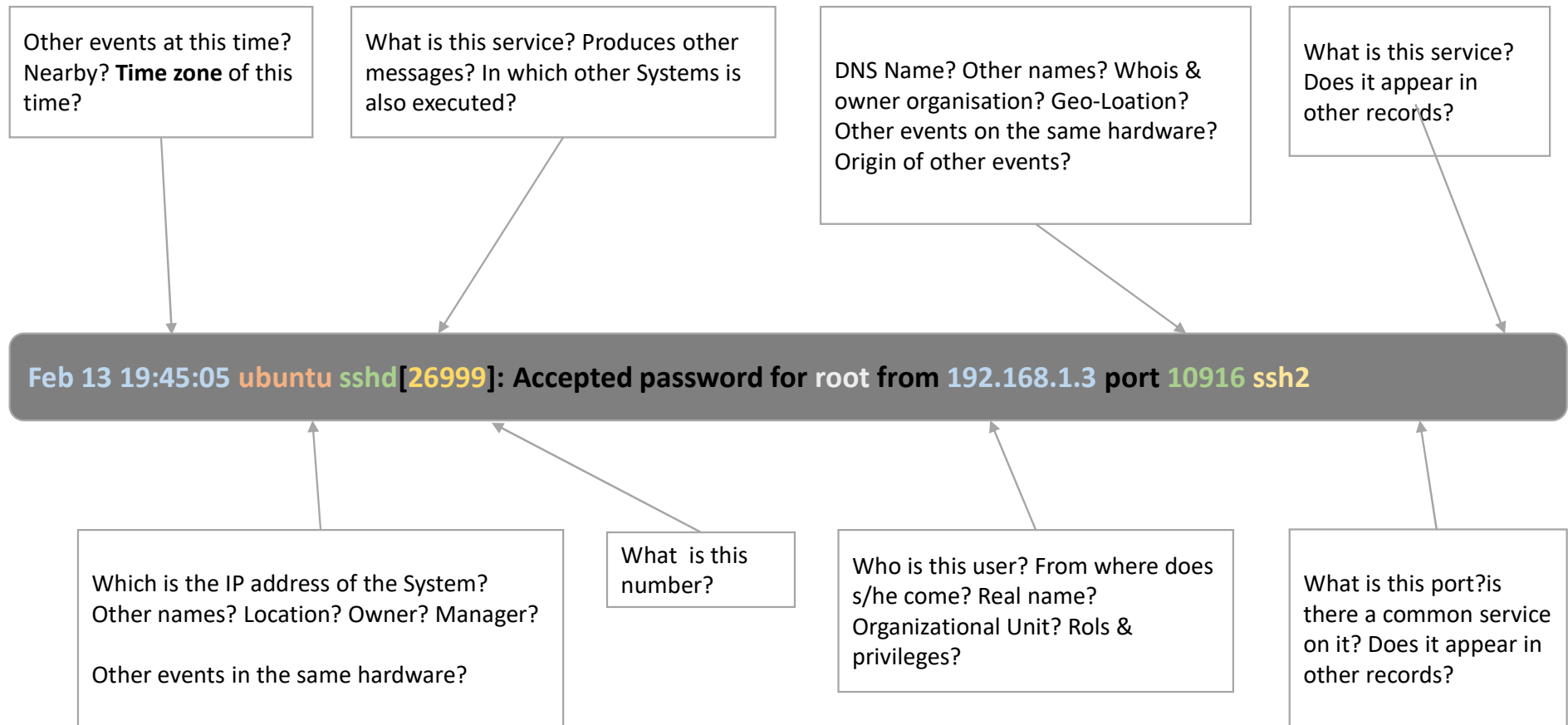
## **Endpoint protection**

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



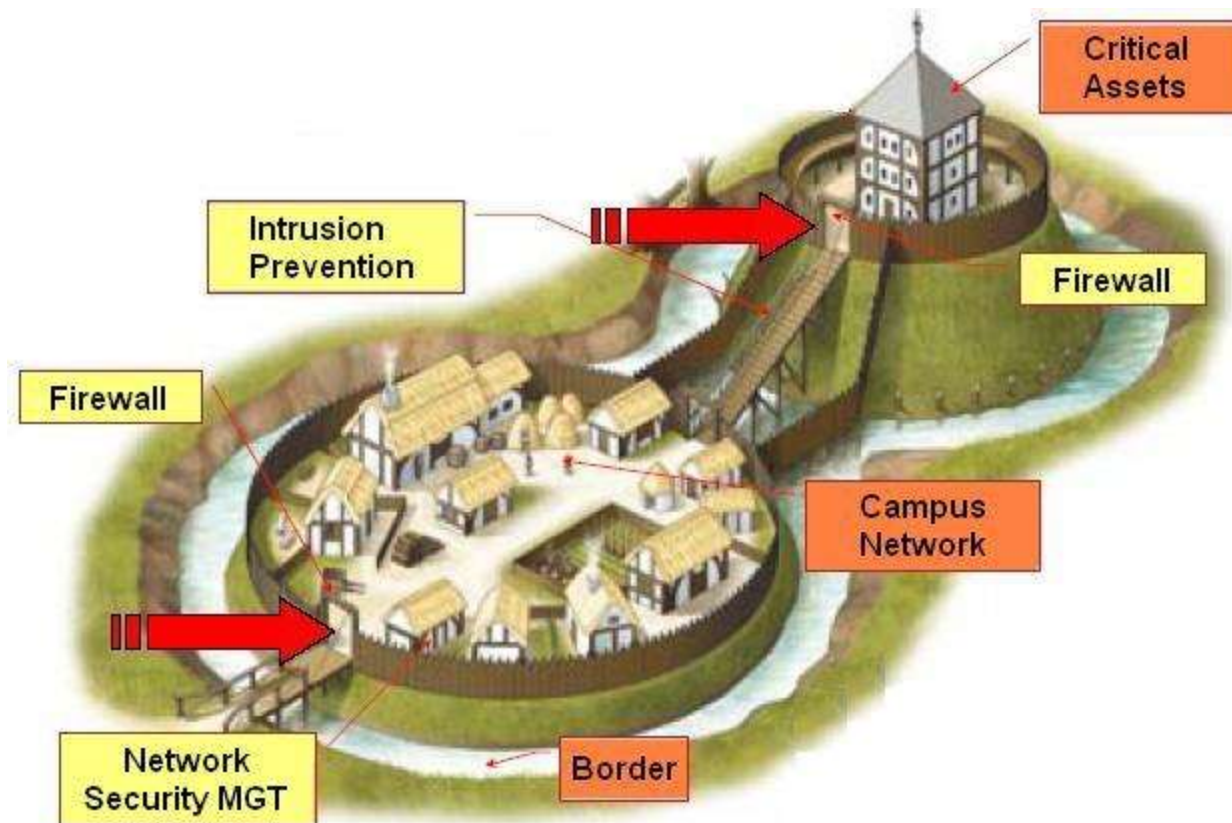
# SIEM vs. LM

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



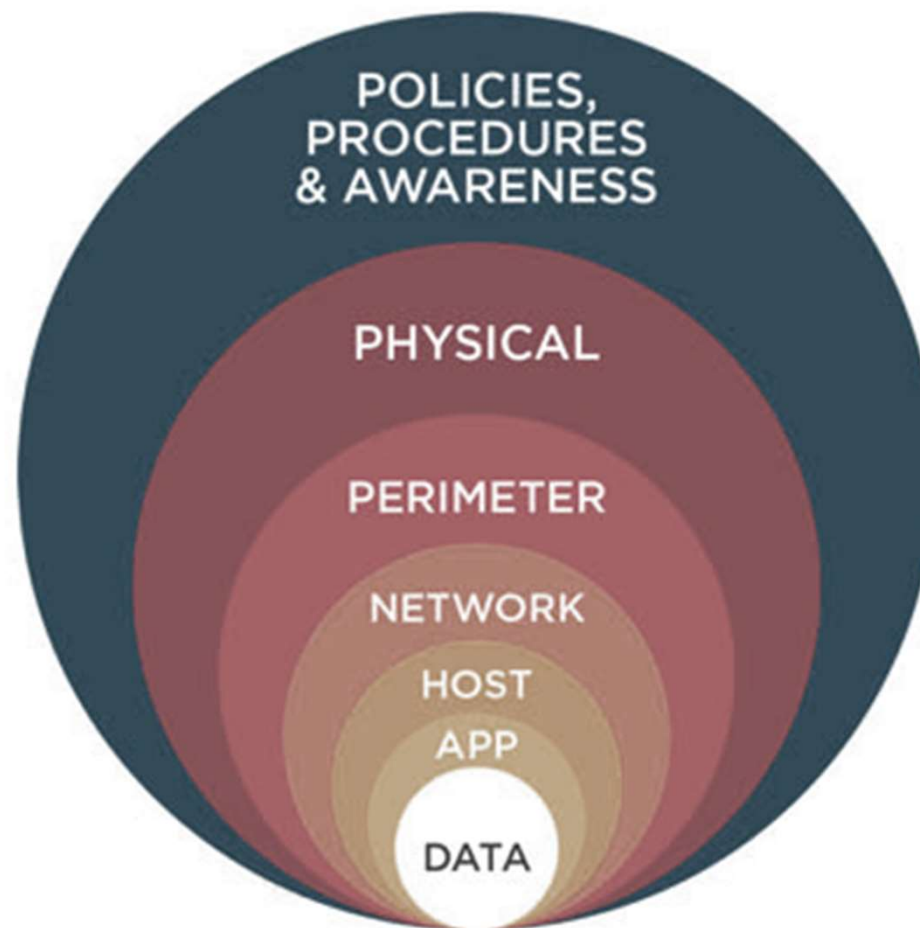
Use case: Intrusion detection

# 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



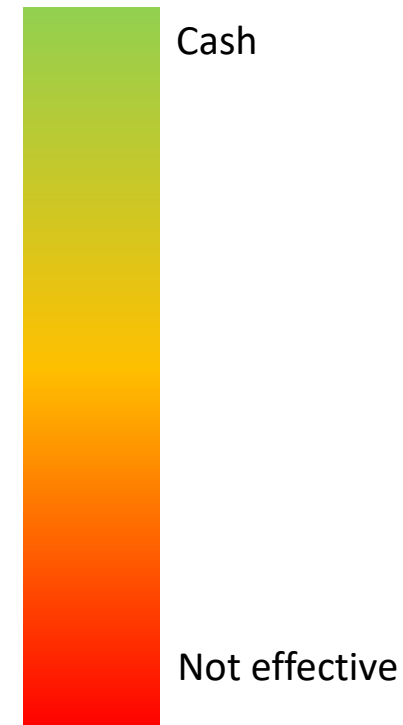


# Intrusion Detection System (IDS)

- 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

