Cybersecurity Management

Monitoring

marc.ruiz-ramirez@upc.edu

Outline

- **Cybersecurity events and incidents**
- **System Logs management**
- **Security Information and Event Management (SIEM)**

Computer Security Model

Vulnerability

Weakness in a system, application, network, or infrastructure

Can be exploited by an adversary to compromise the confidentiality, integrity, or availability of information or resources

Threat

Any circumstance, event, or actor with the **potential** to exploit vulnerabilities and cause harm to an organization's assets, operations, or objectives

Attack

Deliberate **action(s)** carried out by a threat actor to exploit vulnerabilities and compromise the security of a target system, network, or organization

Introduction to logs

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

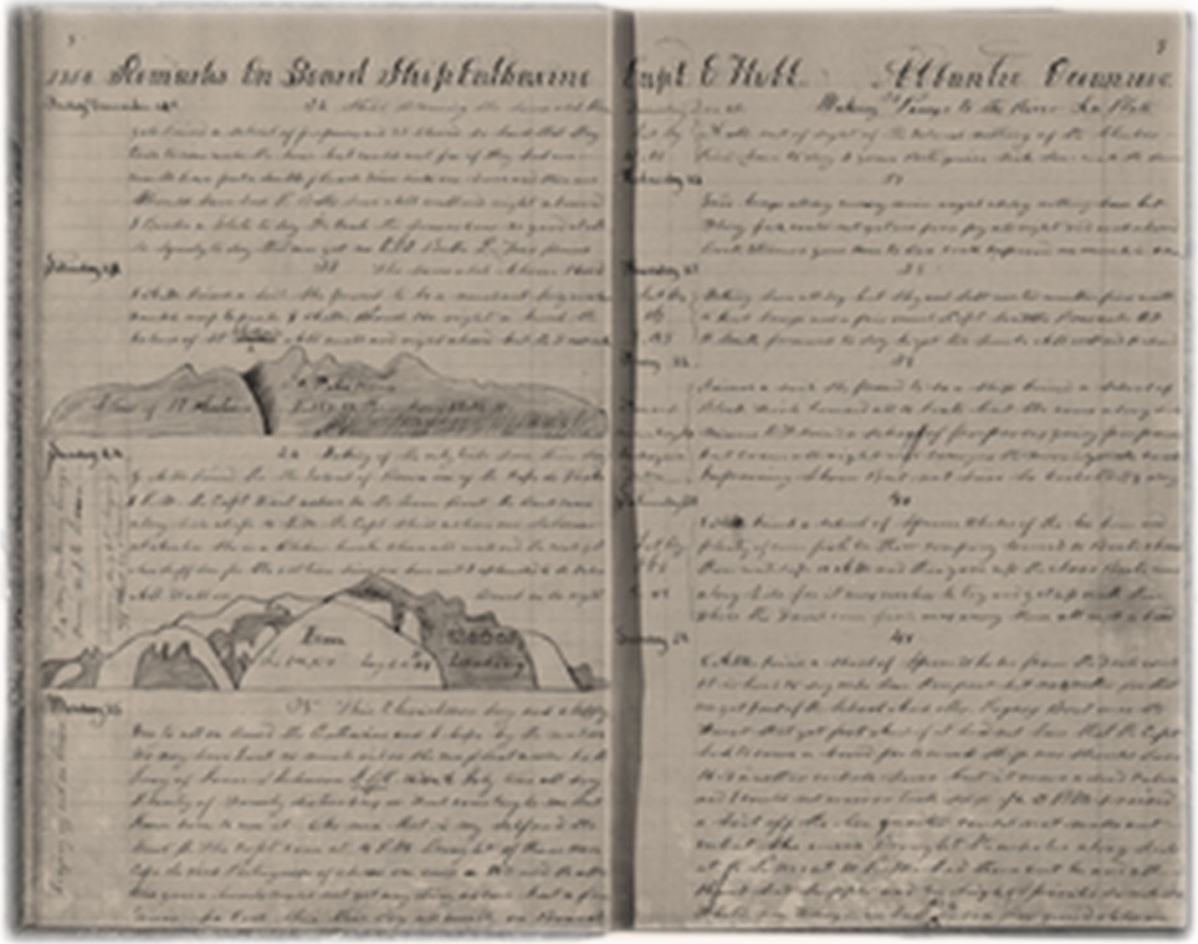
Incident

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

Logbook (cuaderno de bitácora)



Remarks On Board Ship [illegible] Capt E Holt Atlantic Ocean

[illegible]

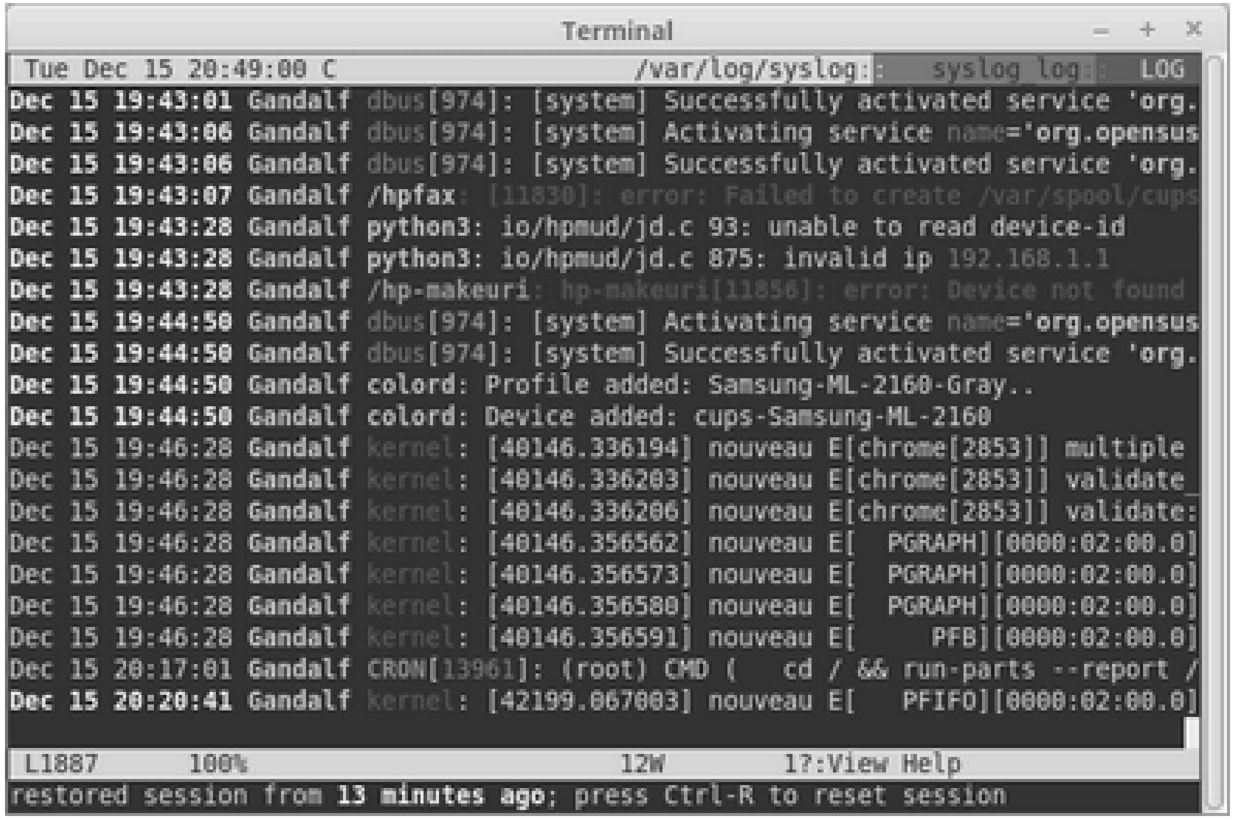
Logbook (cuaderno de bitácora)

- 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

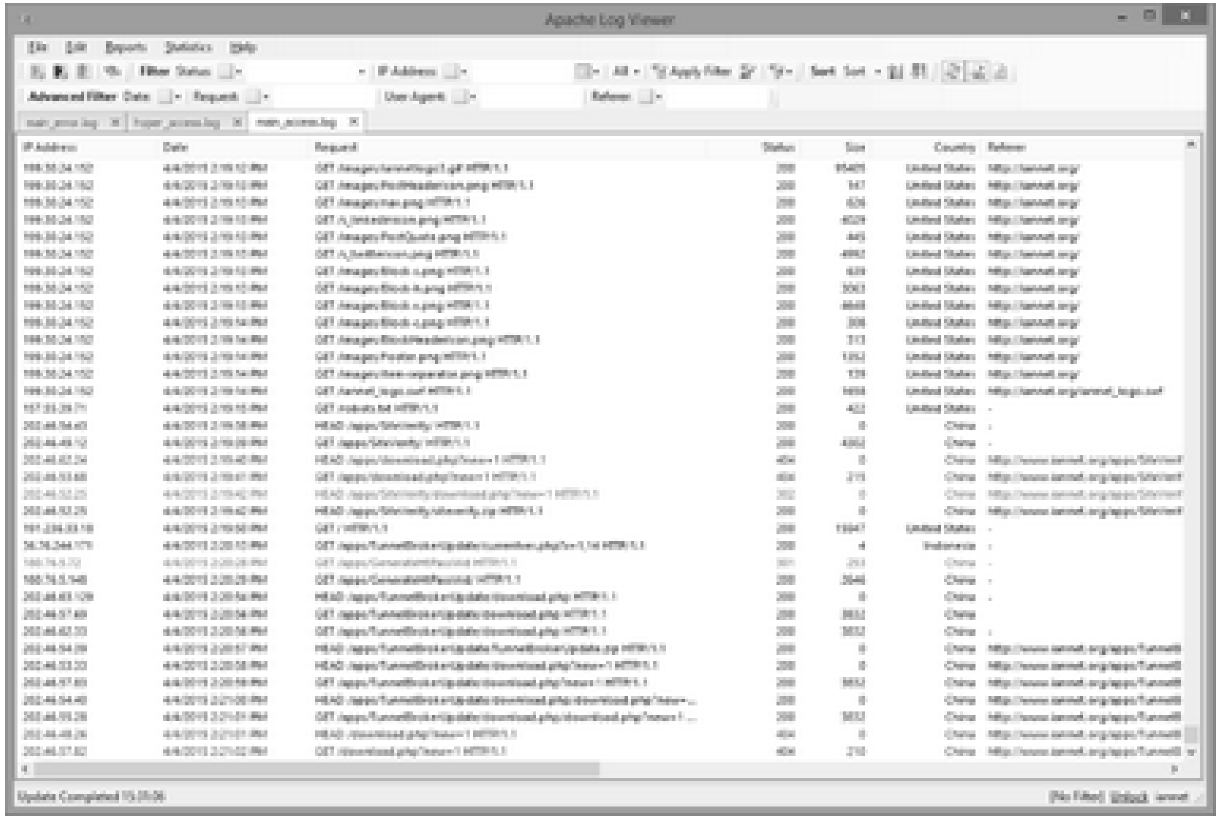
Logbook (cuaderno de bitácora)

- A mechanism to keep a record of all the events in a system
- In IT: log (one record of a single event) = log file = logbook



```
 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.opensus
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/hpmud/jd.c 93: unable to read device-id
Dec 15 19:43:28 Gandalf python3: io/hpmud/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.opensus
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       1?:View Help
restored session from 13 minutes ago; press Ctrl-R to reset session
```



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**
    - detailed investigation for detecting and documenting the course, reasons, culprits, and consequences of a security incident or violation of rules of the organization or state laws
    - follow an agreed process in order to preserve them as a **clue** in case of court trial

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?

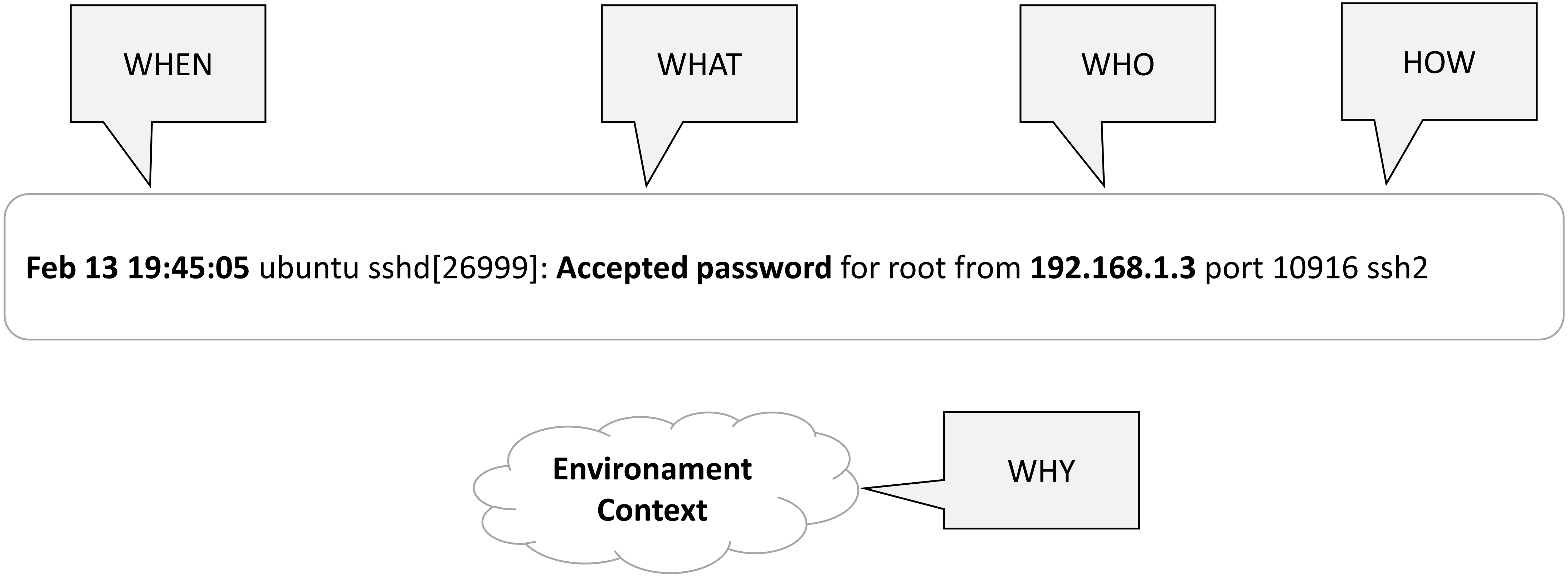
Security events: examples

```
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



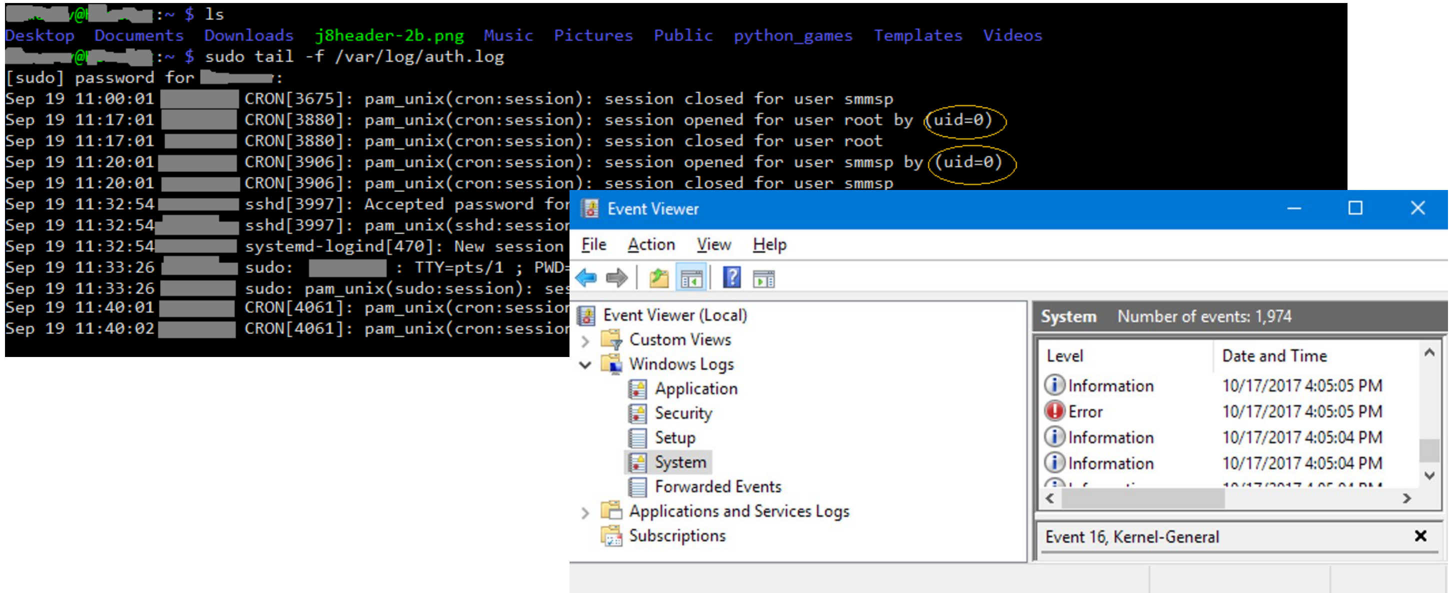
```
Feb 13 19:45:05 ubuntu sshd[26999]: Accepted password for root from 192.168.1.3 port 10916 ssh2
```

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)
    - Visor de Evntos
  - Record (log)



```
[redacted]@[redacted]:~ $ ls
Desktop  Documents  Downloads  j8header-2b.png  Music  Pictures  Public  python_games  Templates  Videos
[redacted]@[redacted]:~ $ sudo tail -f /var/log/auth.log
[sudo] password for [redacted]:
Sep 19 11:00:01 [redacted] CRON[3675]: pam_unix(cron:session): session closed for user smmsp
Sep 19 11:17:01 [redacted] CRON[3880]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 19 11:17:01 [redacted] CRON[3880]: pam_unix(cron:session): session closed for user root
Sep 19 11:20:01 [redacted] CRON[3906]: pam_unix(cron:session): session opened for user smmsp by (uid=0)
Sep 19 11:20:01 [redacted] CRON[3906]: pam_unix(cron:session): session closed for user smmsp
Sep 19 11:32:54 [redacted] sshd[3997]: Accepted password for
Sep 19 11:32:54 [redacted] sshd[3997]: pam_unix(sshd:session
Sep 19 11:32:54 [redacted] systemd-logind[470]: New session
Sep 19 11:33:26 [redacted] sudo: [redacted] : TTY=pts/1 ; PWD=
Sep 19 11:33:26 [redacted] sudo: pam_unix(sudo:session): ses
Sep 19 11:40:01 [redacted] CRON[4061]: pam_unix(cron:sessio
Sep 19 11:40:02 [redacted] CRON[4061]: pam_unix(cron:sessio
```

System Number of events: 1,974

Level	Date and Time
Information	10/17/2017 4:05:05 PM
Error	10/17/2017 4:05:05 PM
Information	10/17/2017 4:05:04 PM
Information	10/17/2017 4:05:04 PM

Event 16, Kernel-General

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

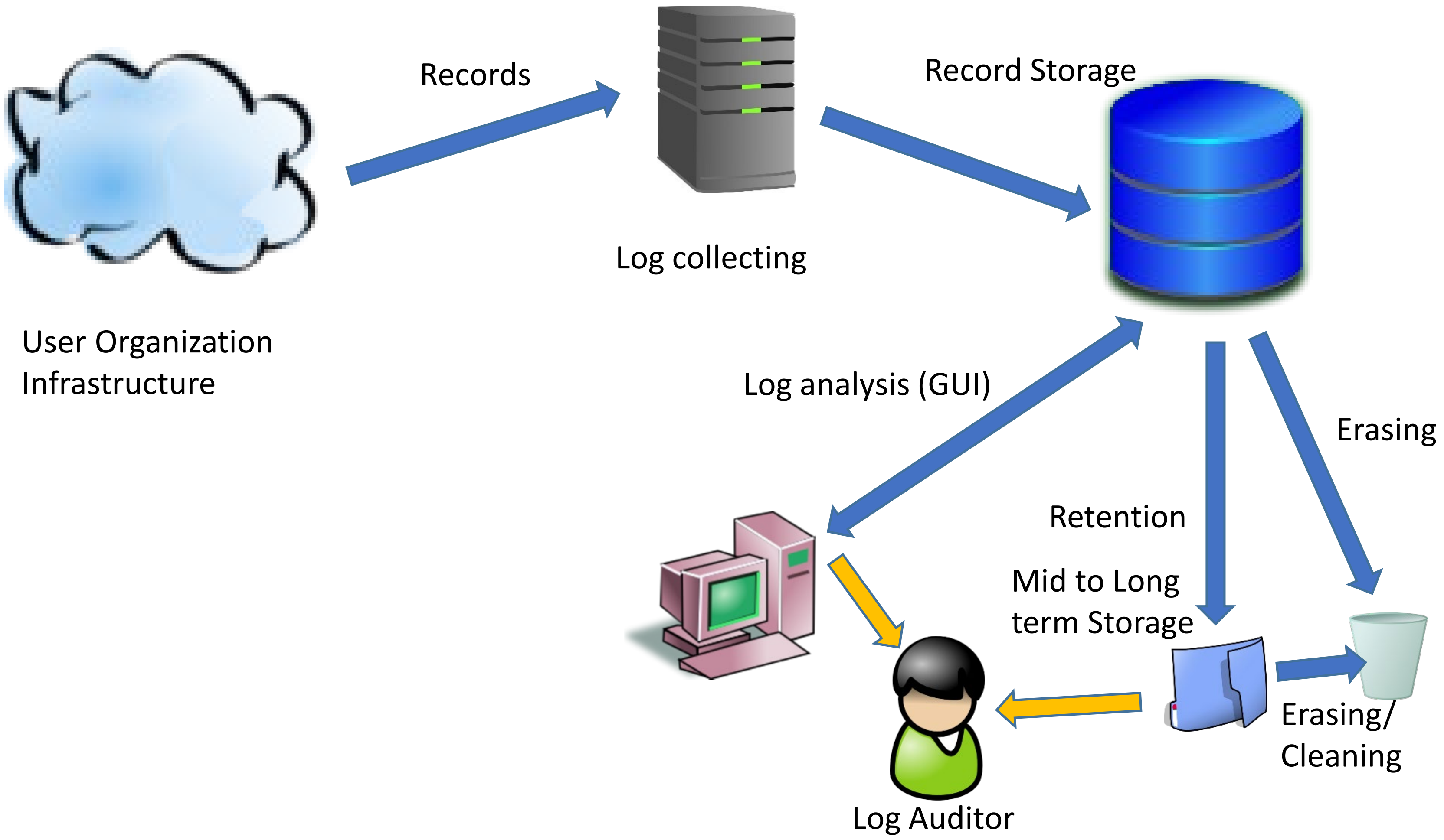
Log Management: Challenges

- 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

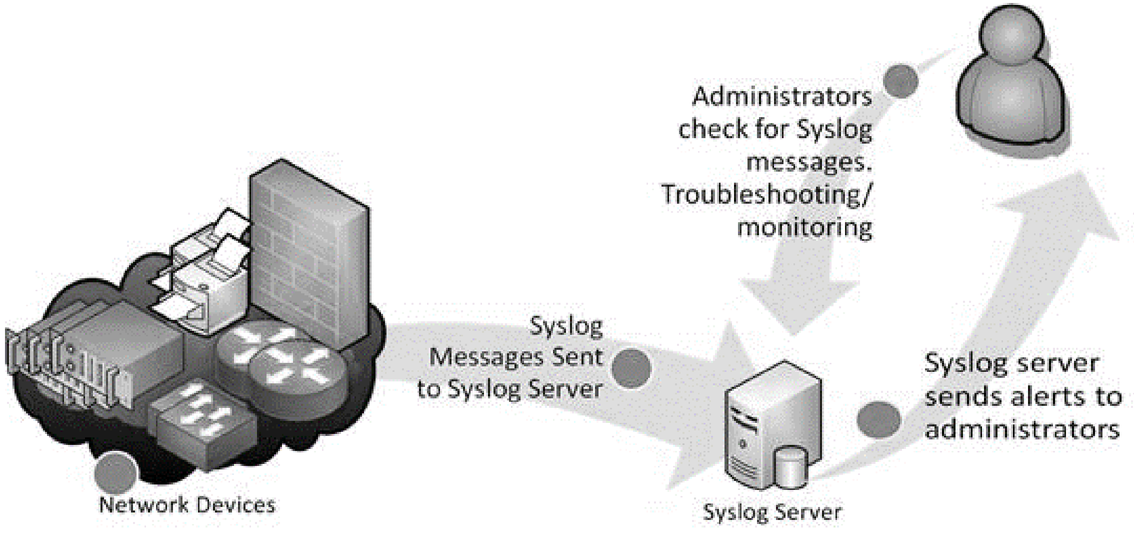
- Logs **volume**: Data Granularity & Retention time
- Logs **Format heterogeneity**: common format & parsing
- The **architecture of networks and systems**

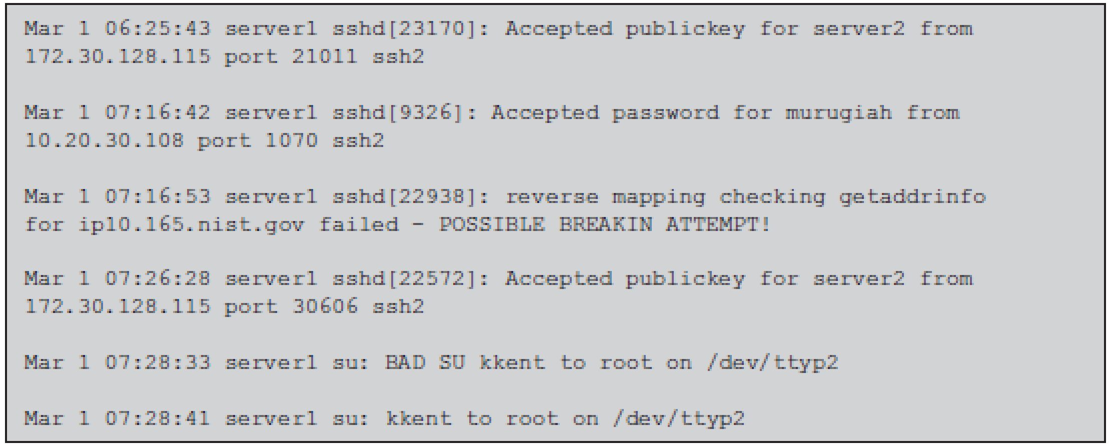
Log Management: Schema



Syslog. Powerful registry system(UNIX)

- UNIX logging mechanism
  - Capturing relevant events
  - Syslog Protocol:
    - Facilitates the transfer of information from network devices to the syslog server.
    - It is a crucial part of network monitoring as it helps to track the overall health of network
    - Network devices (such as routers and switches) support this protocol for event logging.
    - **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** (not even suggested**)**


Administrators check for Syslog messages. Troubleshooting/ monitoring
Syslog Messages Sent to Syslog Server
Syslog server sends alerts to administrators
Network Devices
Syslog Server



```
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 technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.
- Helps organizations to detect, analyze, and respond to security threats.
- SIEM combines both security information management (SIM) and security event management (SEM) into one security management system.
- SIEM systems functionalities: log management, event correlation, and incident monitoring and response

SIEM

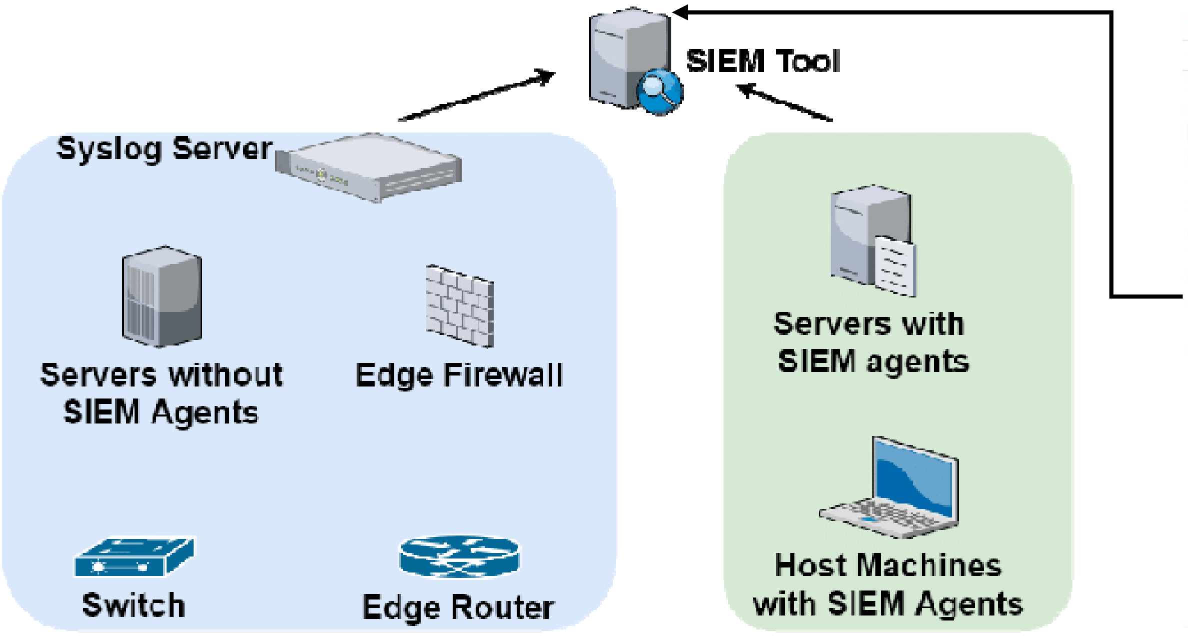
- SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements.
- SIEM solutions gather and consolidate large amounts of data from:
  - organization’s applications, devices, servers, and users in real-time
  - allowing security teams to detect and prevent attacks.
- To identify potential threats and issue alerts:
  - SIEM tools employ predefined or customized rules that aid security teams in defining and categorizing potential dangers.
- SIEM has become more efficient (integration of AI)
  - allowing for faster and more intelligent threat detection and incident response.

SIEM components

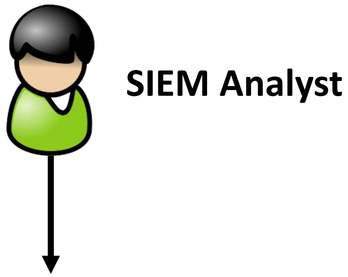
- Security Information Management (SIM)
  - Long-term **storage**
  - **Analysis** of registration data
  - **Reports**
- Security Event Manager (SEM)
  - Real-time **monitoring**
  - **Correlation** of events
  - **Notifications** and alerts
  - Consoles, views, and **dashboards**

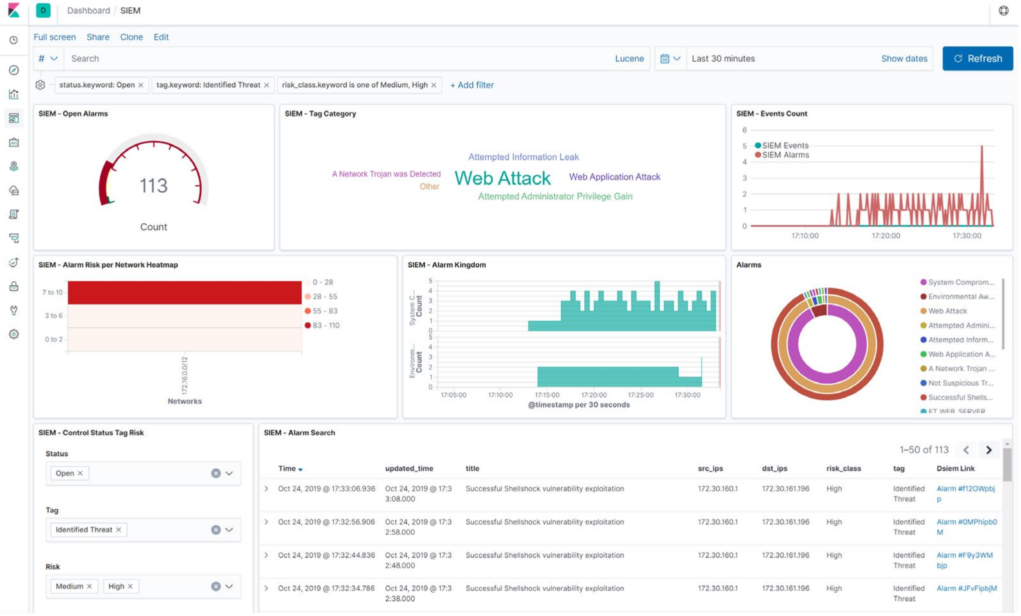
SIEM = SIM + SEM = long & short + real-time

SIEM. Security Information & Event Management



SIEM: Schema





status.keyword: Open ×   tag.keyword: Identified Threat ×   risk_class.keyword is one of Medium, High ×

SIEM - Control Status Tag Risk

Status: Open ×

Tag: Identified Threat ×

Risk: Medium × High ×

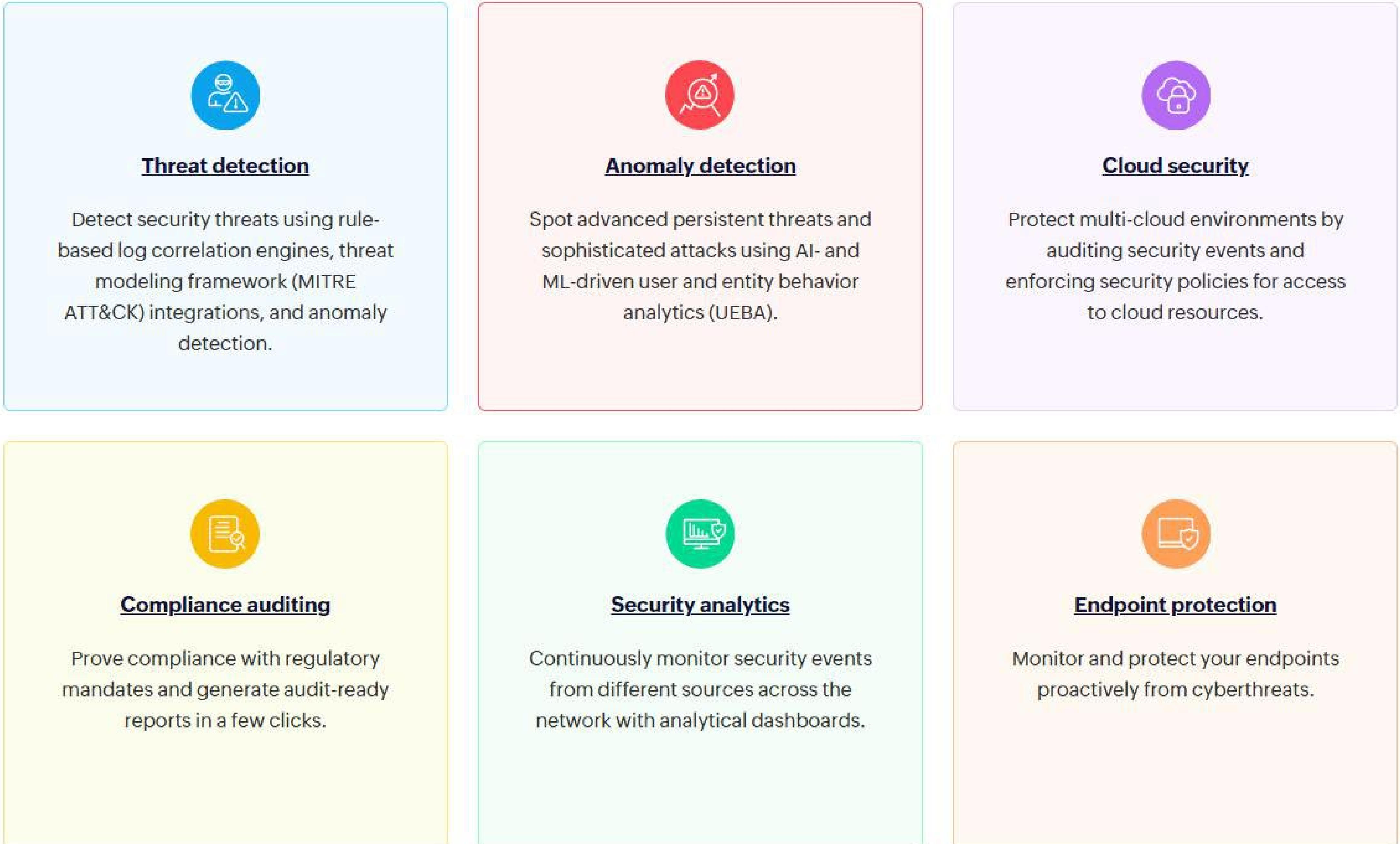
SIEM - Alarm Search

1–50 of 113

Time	updated_time	title	src_ips	dst_ips	risk_class	tag	Dsiem Link
Oct 24, 2019 @ 17:33:06.936	Oct 24, 2019 @ 17:33:08.000	Successful Shellshock vulnerability exploitation	172.30.160.1	172.30.161.196	High	Identified Threat	Alarm #f12OWpbjp
Oct 24, 2019 @ 17:32:56.906	Oct 24, 2019 @ 17:32:58.000	Successful Shellshock vulnerability exploitation	172.30.160.1	172.30.161.196	High	Identified Threat	Alarm #0MPhipb0M
Oct 24, 2019 @ 17:32:44.836	Oct 24, 2019 @ 17:32:48.000	Successful Shellshock vulnerability exploitation	172.30.160.1	172.30.161.196	High	Identified Threat	Alarm #F9y3WMbjp
Oct 24, 2019 @ 17:32:34.786	Oct 24, 2019 @ 17:32:38.000	Successful Shellshock vulnerability exploitation	172.30.160.1	172.30.161.196	High	Identified Threat	Alarm #JFvFipbjM

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

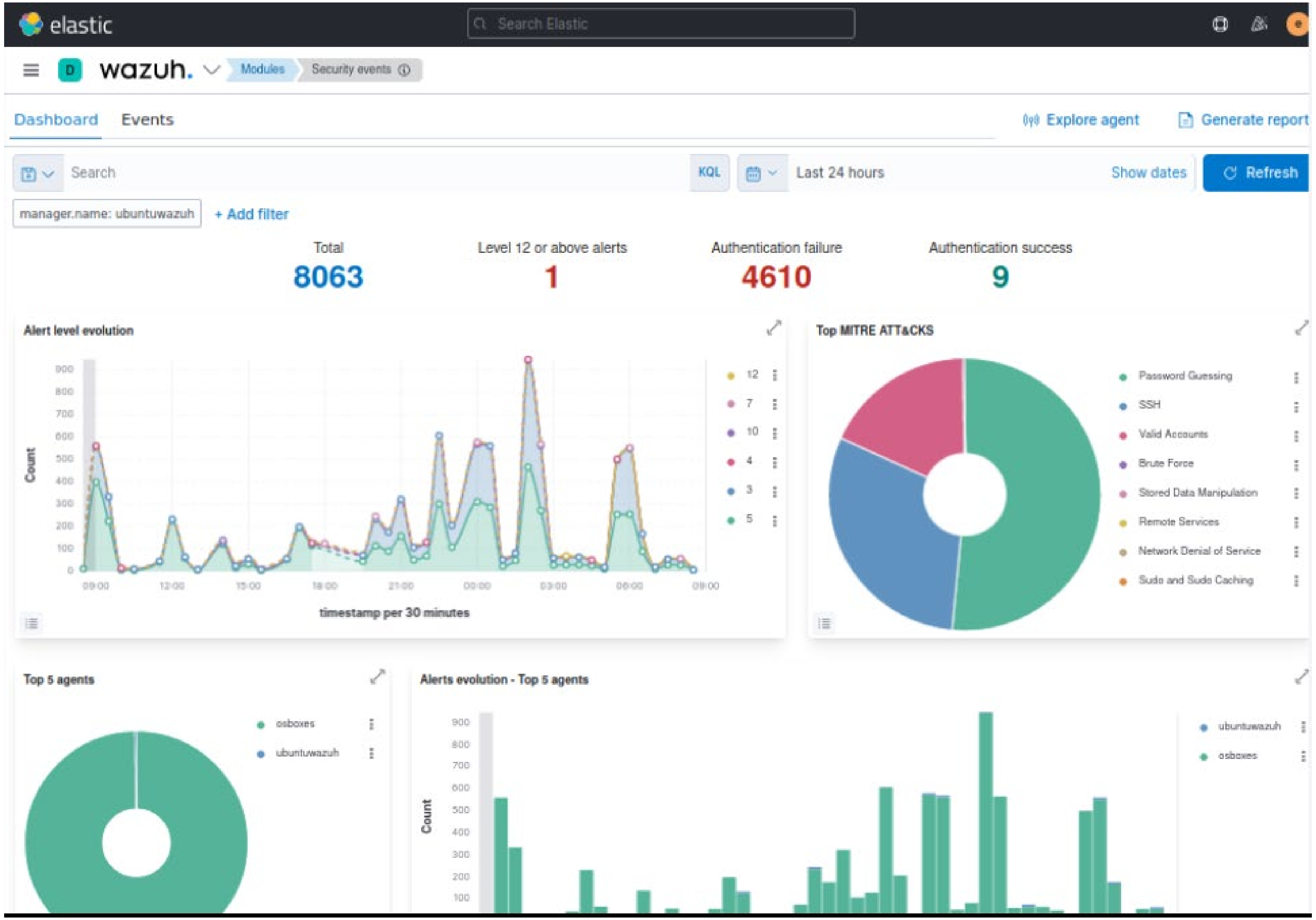
Monitor and protect your endpoints proactively from cyberthreats.

Open Source SIEMs

- AlienVault OSSIM
- Apache Metron
- MozDef
- Wazuh

Wazuh SIEM

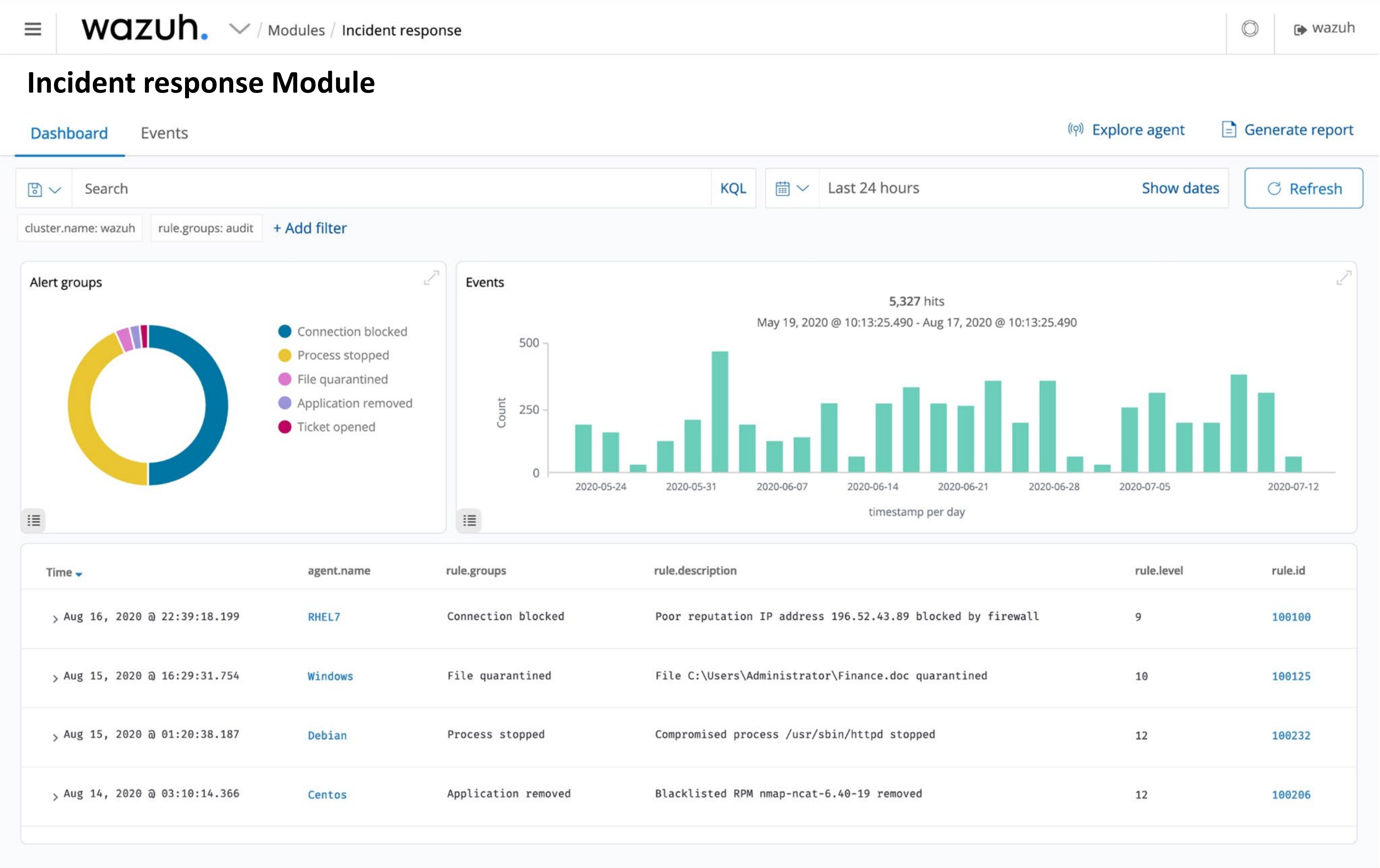
- Provides monitoring, detection, and alerting of security events and incidents.



manager.name: ubuntuwazuh

Last 24 hours

Total	Level 12 or above alerts	Authentication failure	Authentication success
8063	1	4610	9



Incident response Module

Time	agent.name	rule.groups	rule.description	rule.level	rule.id
› Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	9	100100
› Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
› Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100232
› Aug 14, 2020 @ 03:10:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100206

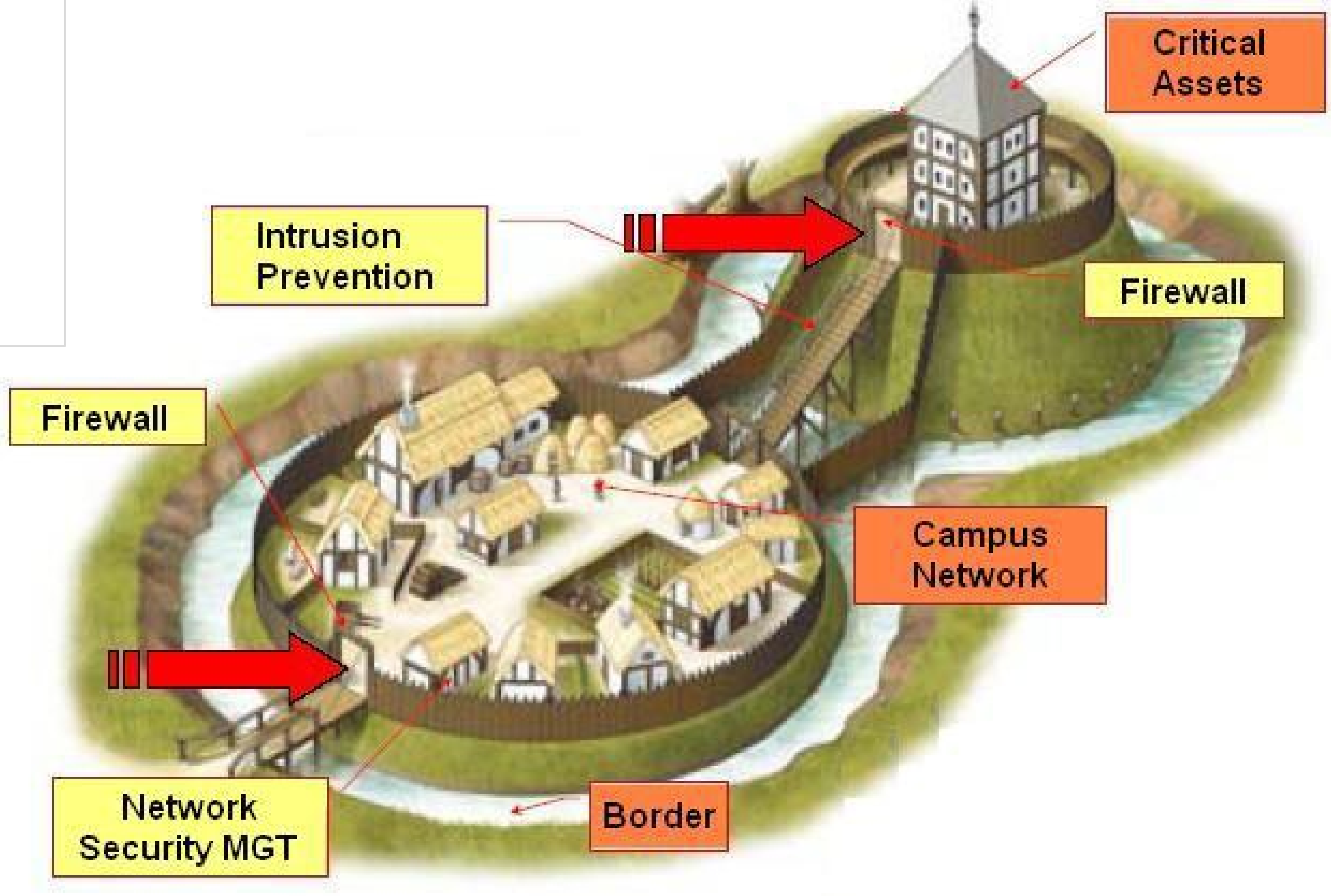
SIEM vs. LM

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

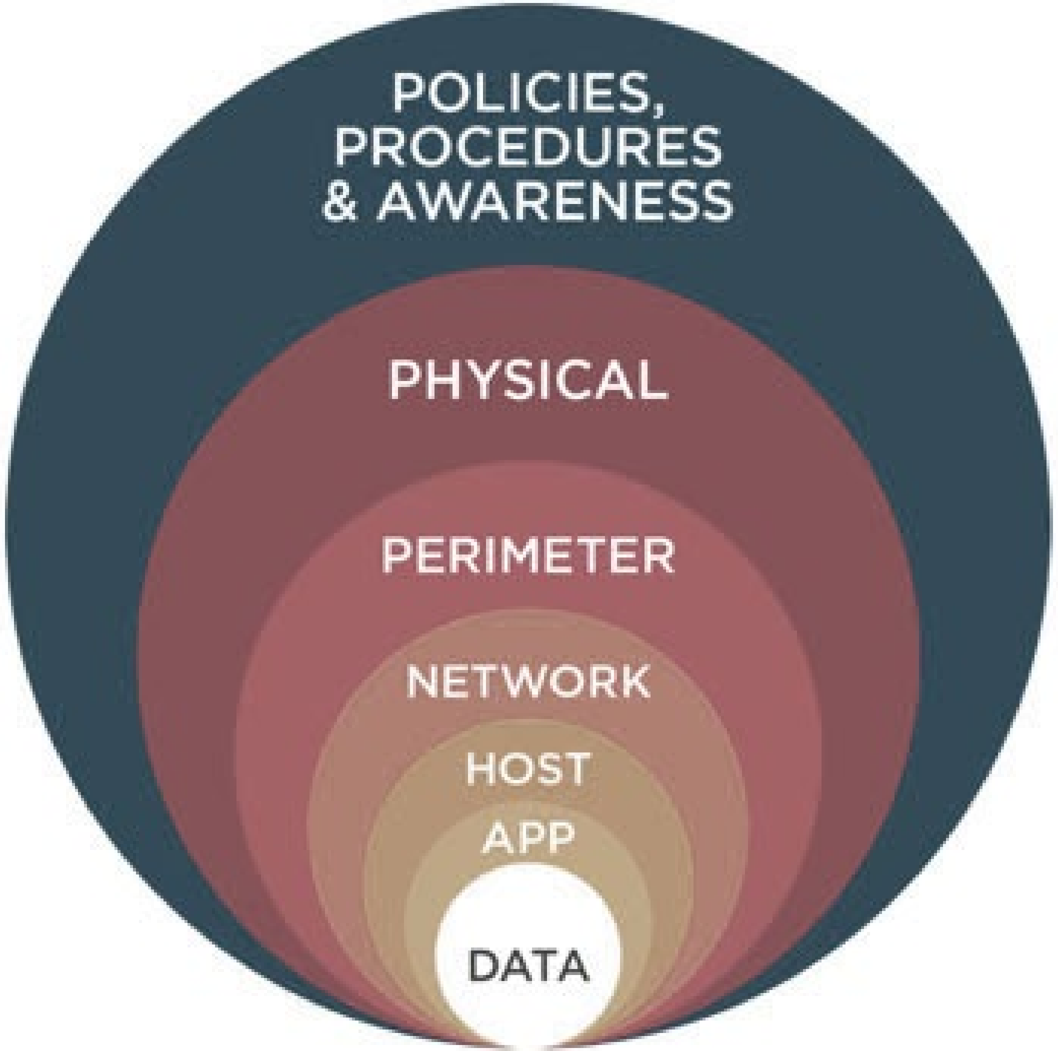
Defense in depth (aka deep defense or elastic defense)

Military strategy
seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space



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

Defense in depth

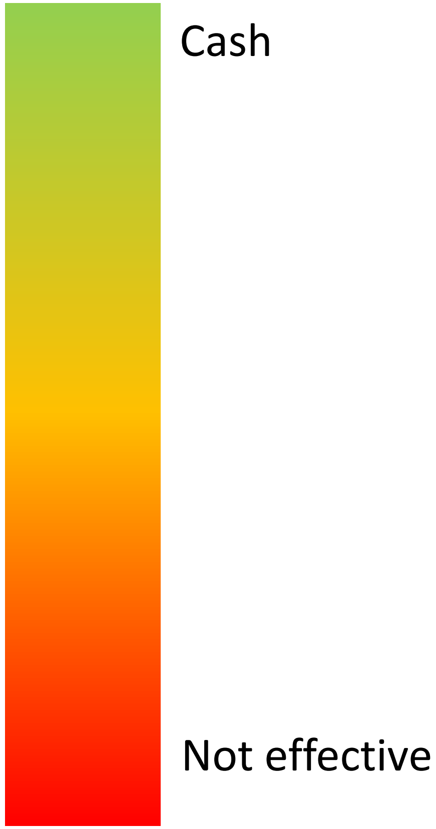


Intrusion Detection System (IDS)

- Intrusion
  - any unauthorized attempt or access to a system
  - malicious use of its resources
- IDS
  - identify signs of malicious activity in the network
    - CIA
    - Attacks against a computer or network
- Open Source IDS
  - Suricata
  - Snort

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**)

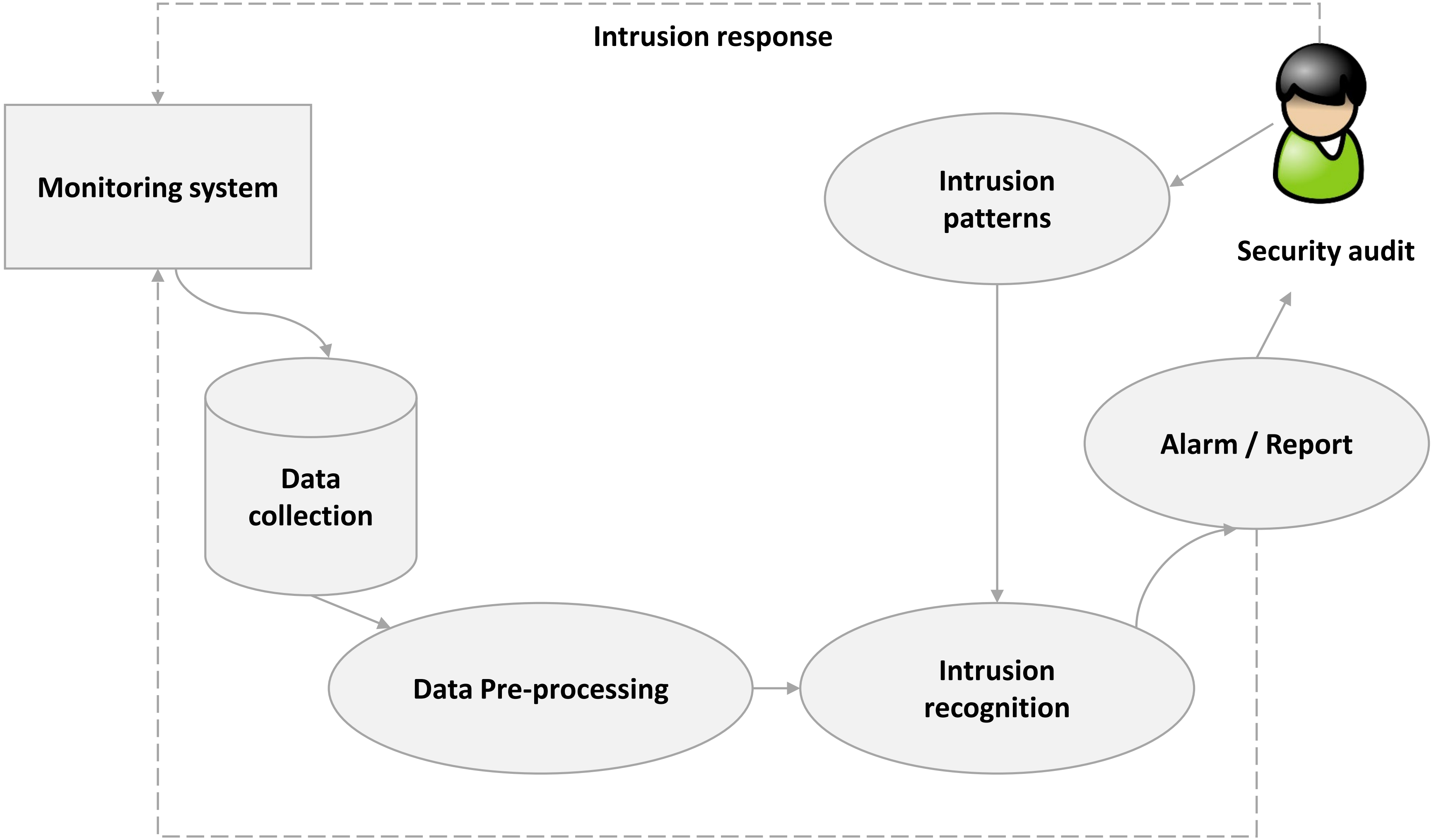
NIDS vs HIDS

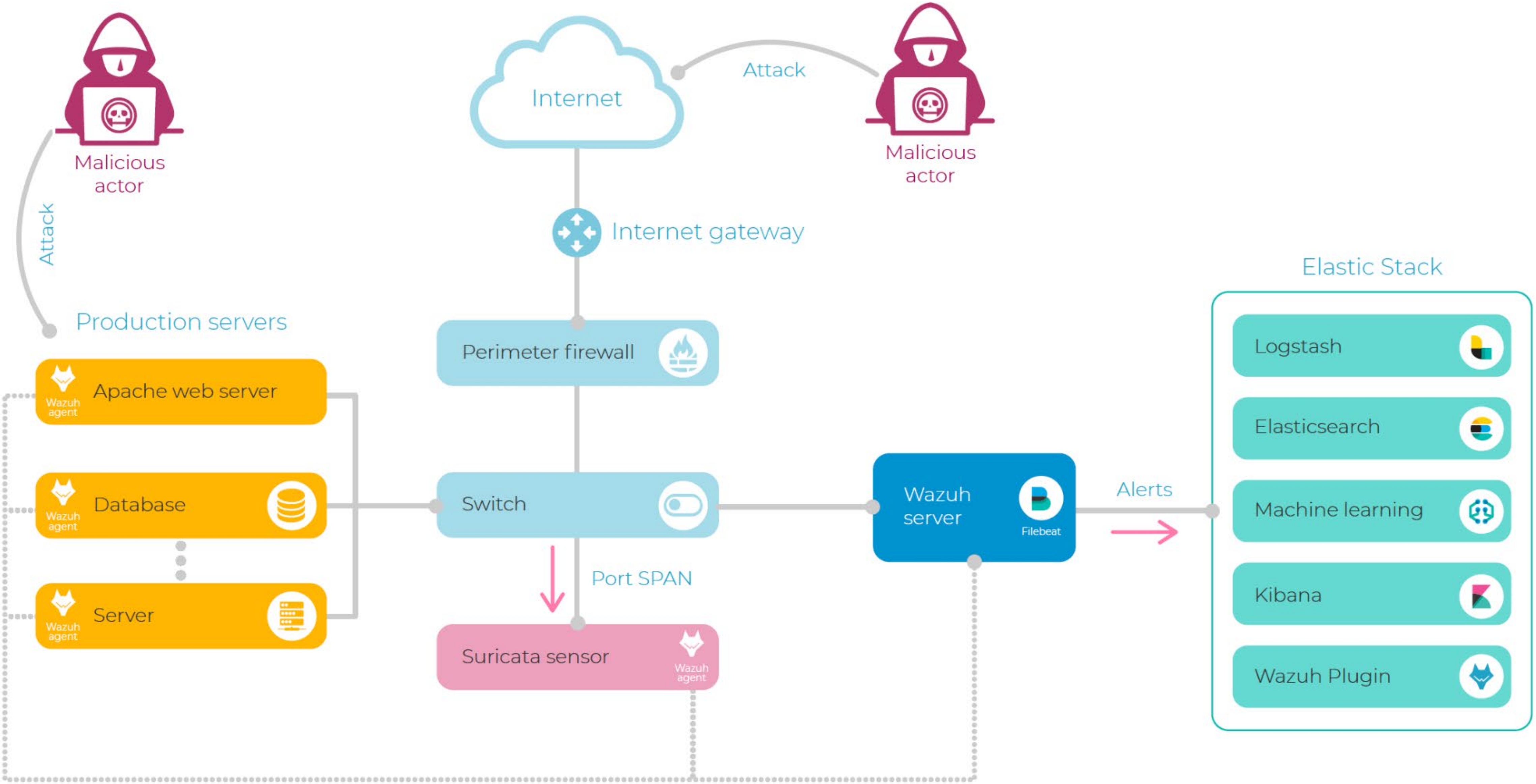
- **Network-level Intrusion Detection System (NIDS)**
  - Monitors network traffic and detects anomalies.
  - Cannot inspect encrypted traffic (Unlike HIDS)
- **Host Intrusion Detection Systems (HIDS)**
  - IDS at the equipment level: detects events on a server or workstation.
  - Generate alerts (similar to a NIDS), but it is also capable of inspecting the communication flow comprehensively.
  - Encrypted communications can be monitored because HIDS inspects traffic before encryption)

IDS classification

- **How** do they perform the detection? (**Algorithms**)
  - Based on **signatures** (**knowledge**)
    - Detect known attacks based on predefined patterns for malicious network activities.
    - High accuracy in detection, but they cannot detect zero-day attacks
  - Based on **anomalies** (**behavior**)
    - Aim to identify unknown attacks.
    - The detection is based on the definition of normal and anomalous behavior patterns.
    - Lack high accuracy.

Architecture of an IDS




Malicious actor
Attack
Internet
Attack
Malicious actor
Internet gateway
Production servers
Wazuh agent
Apache web server
Wazuh agent
Database
Wazuh agent
Server
Perimeter firewall
Switch
Port SPAN
Suricata sensor
Wazuh agent
Wazuh server
Filebeat
Alerts
Elastic Stack
Logstash
Elasticsearch
Machine learning
Kibana
Wazuh Plugin