AIR INSTITUTE

www.air-institute.com

competitividad empresarial ice | Junta de Castilla y León | Centr@Tec Servicios Avanzados de Innovación para Pymes

Centro de Operaciones de Ciberseguridad Inteligente

DeepSIEM

www.deepsiem.com

Content

- SIEM
- Artificial intelligence
- Technologies
- Architecture
- SOC
- Samples

About DeepSIEM

Why?

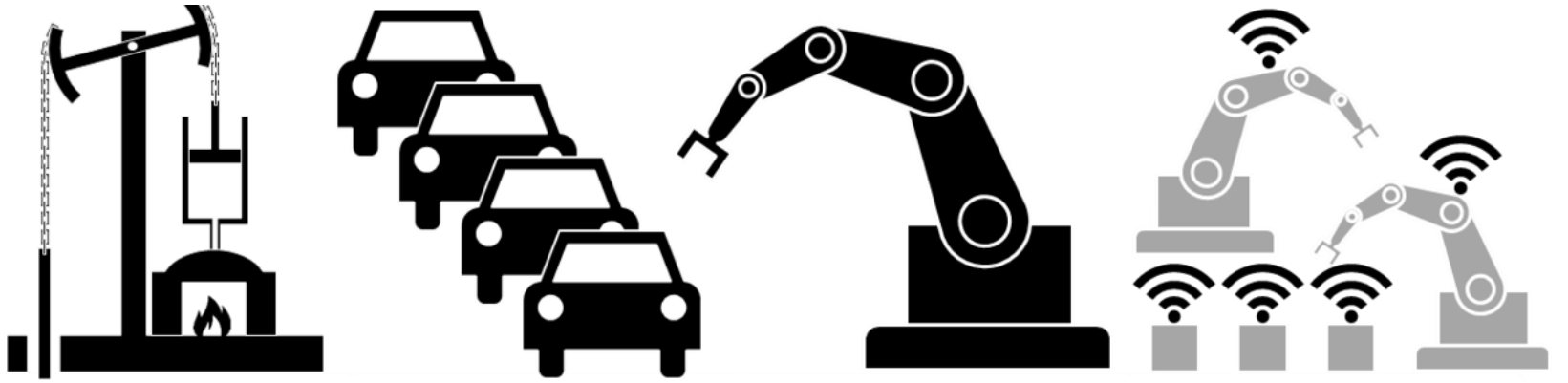
Cybersecurity has been ranked as one of the most important risks in recent years.

The Global Risks Report 2023 ranked cybercrime and cyber insecurity as the eighth most severe global risk within a two-year and a 10-year period, making it clear that cyber risks will remain a constant and significant concern over the next decade.

Specifically, the WEF predicts a rise in cybercrime, with more attacks against agriculture and water, financial systems, public security, transport, energy, communication infrastructure and more. In fact, cyberattacks on critical infrastructure ranked 5th among what the WEF calls “currently manifesting risks” which are expected to have a global impact this year.

The Global Risks Report 2023

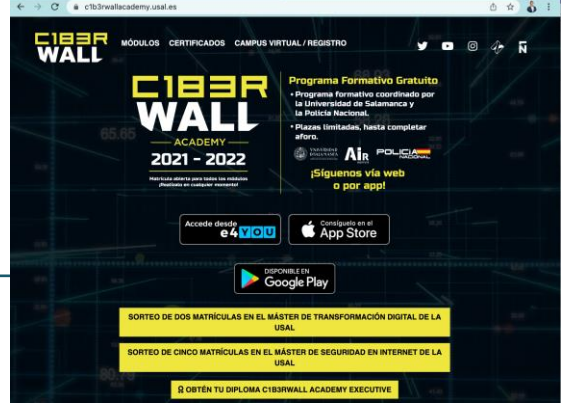
Industry 4.0 – connected industry



1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

AlienVault USM (AT&T)
SPLUNK
Logrhythm
Microsoft Azure Sentinel
Q Radar - IBM

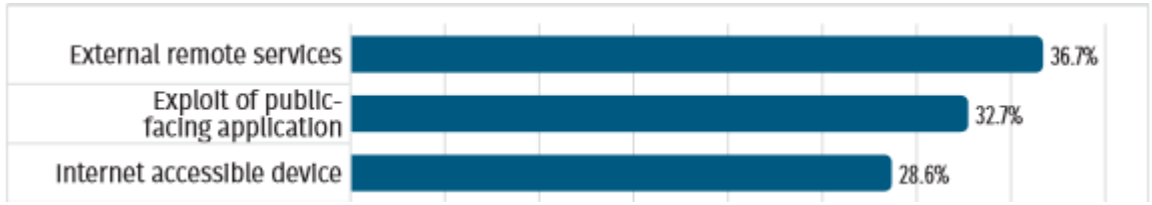
About DeepSIEM



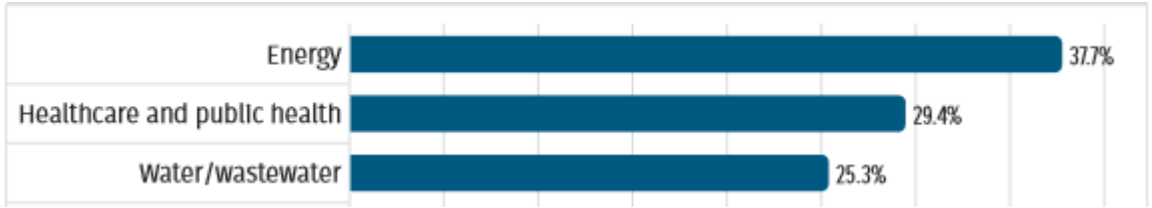
Industrial Enviroments

ICS/SCADA environments are now connecting to the Internet. This opens these environments to attacks and intrusions facing IT environments, making SIEM an increasingly smart security solution choice for industrial environments.

“Organizations now recognize the security of their ICS assets as fundamental to their business, and they expressed as their number one concern ensuring the reliability and availability of control systems.” – SANS 2021 OT/ICS Cybersecurity Survey



Initial attack vectors



Most likely sectors to have a successful ICS compromise

SANS 2021 OT/ICS Cybersecurity Survey

About DeepSIEM

What is?

- DeepSIEM is a security information and event management solution that:
  - Centralizes an organization’s logs.
  - Correlates and analyzes logs in real time in search of cyberthreats.
  - Automatically mitigates detected threats.
  - Visualizes and manages all the platform's functionalities and data.

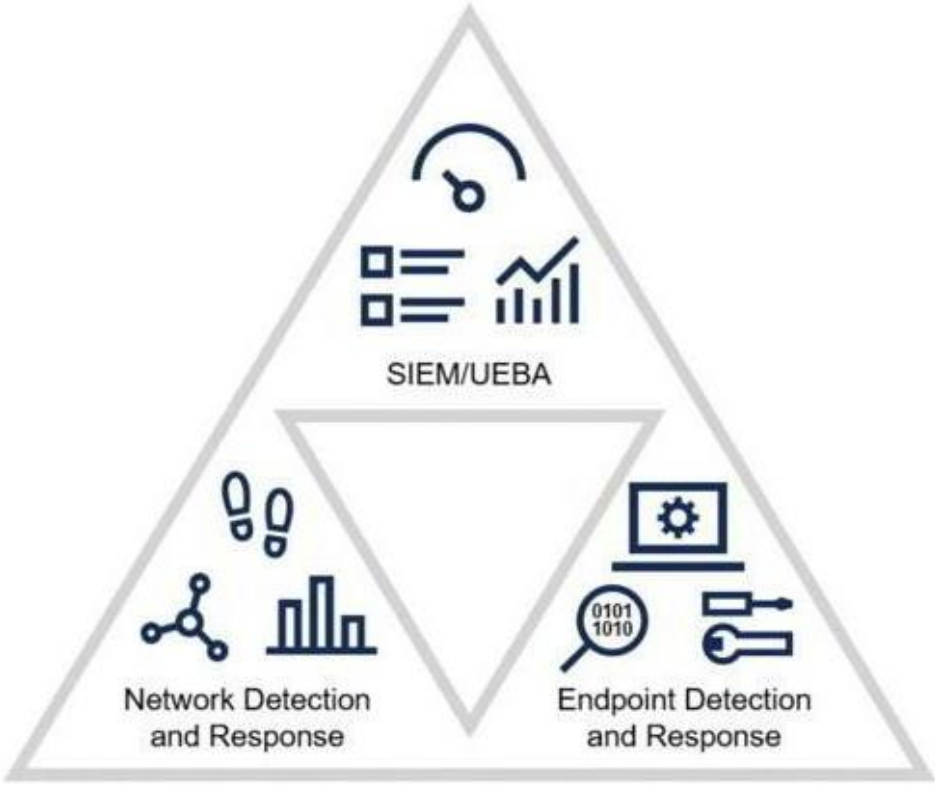
About DeepSIEM

SOC

A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

In industrial processes, the primary objective is to maintain the availability

- User and entity behavior through security information and event management (SIEM).
- Network detection and response (NDR).
- Endpoint detection and response (EDR).



Artificial Intelligence

The cyberattack surface in modern enterprise environments is massive, and it's continuing to grow rapidly. This means that analyzing and improving an organization's cybersecurity posture needs more than mere human intervention.

"Analyzing and improving cybersecurity posture is not a human-scale problem anymore."

AI is able to **quickly analyze millions of events** in order to identify cyber threats.

- **Advantages of AI in Cybersecurity:**
  - Detecting new and unknown threats.
  - Reduce SoC alert fatigue.
  - Better vulnerability management.
  - Battling bots.
  - Better Endpoint Protection.

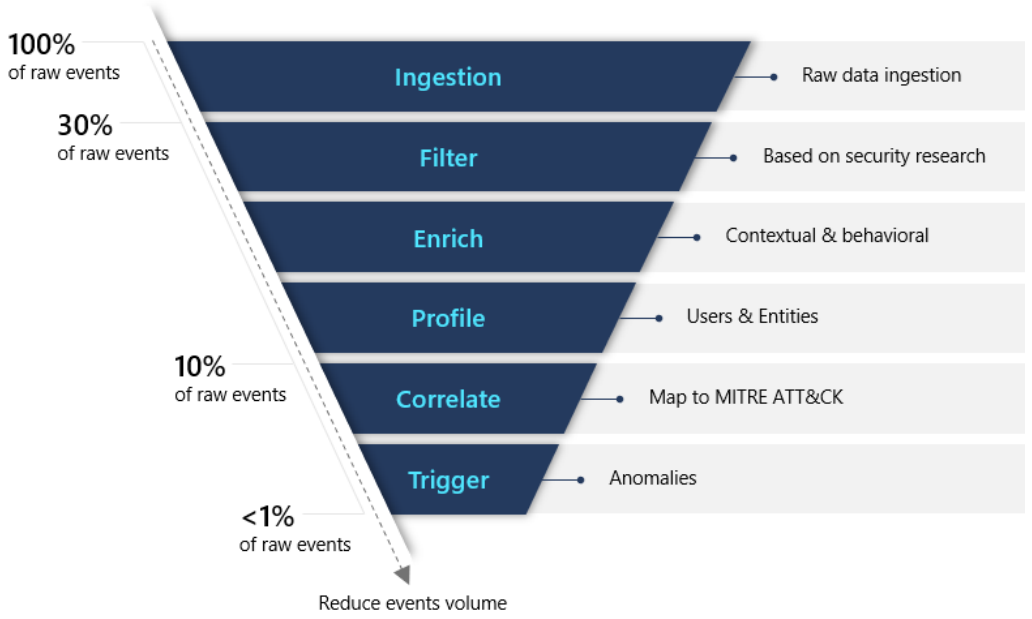
"79% of security teams feel overwhelmed by the volume of threat alerts." - Enterprise Management Associates (EMA)

"The average security operations team receives over 11,000 security alerts daily and 28% of alerts are simply never addressed." - Forrester Consulting

"In 2020, the global average number of days an attacker is acting against an infrastructure before being detected is 24 days," – FireEye SPECIAL REPORT M-TRENDS 2021

Artificial Intelligence

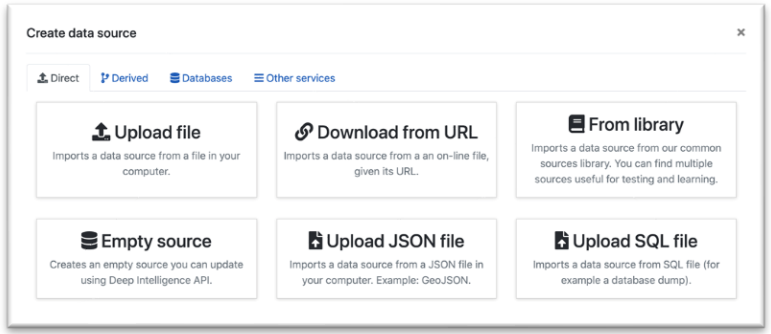
- **Threat Intelligence** and **Artificial Intelligence** techniques are used to combat alert fatigue in SOC.
- **DeepSIEM** has an **artificial intelligence and threat intelligence module** capable of correlating the events of the different detection engines, reducing alerts by approximately 85%.
- Another possible way to reduce alert fatigue is **prioritization**. DeepSIEM learns the importance of events based on the alert management of the organization's analysts. It adapts to the **context of each organization**. The system uses variables such as the target of the possible attack, the type of event and the origin, among others, to prioritize the incidents.



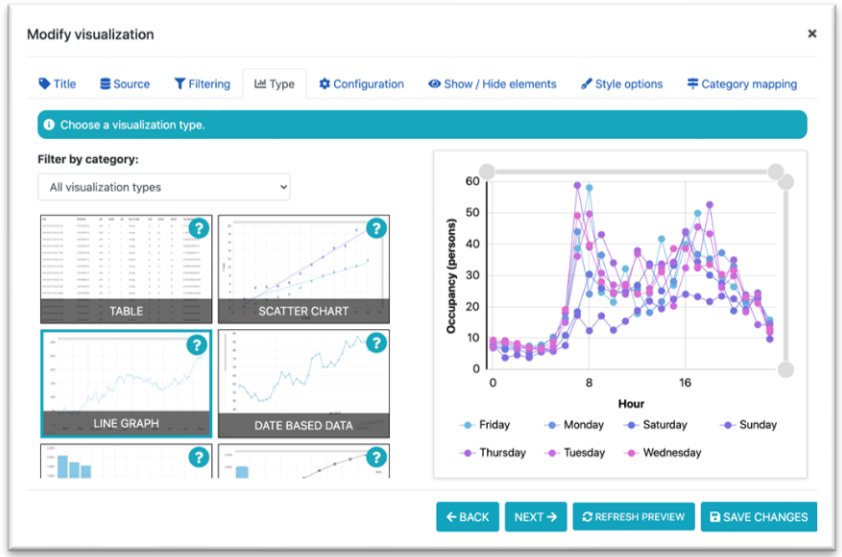
Artificial Intelligence deepint.net

Deep Intelligence (deepint.net) is a tool for analyzing data using artificial intelligence. It provides assisted solutions for all the process, from data ingestión to data visualization and exportation.

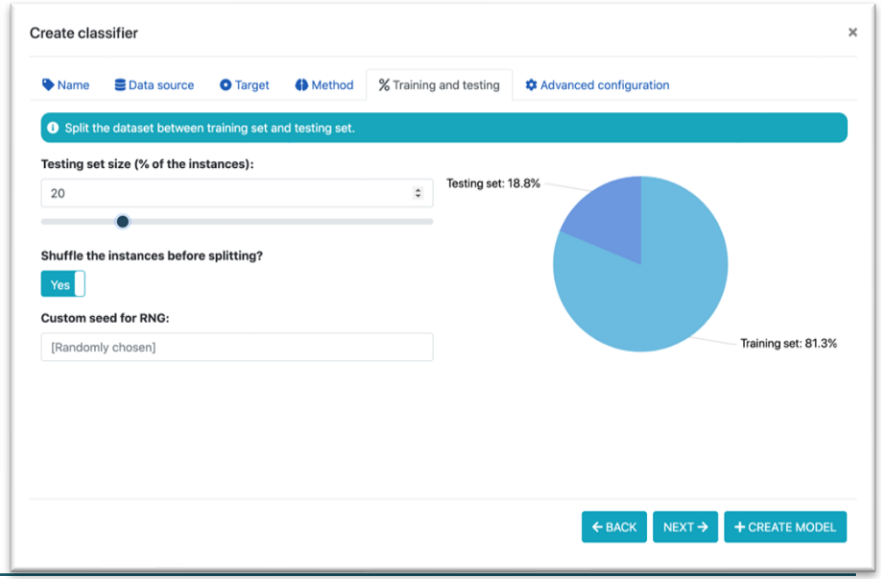
Wizard to import your data



Wizard to create dynamic visualizations



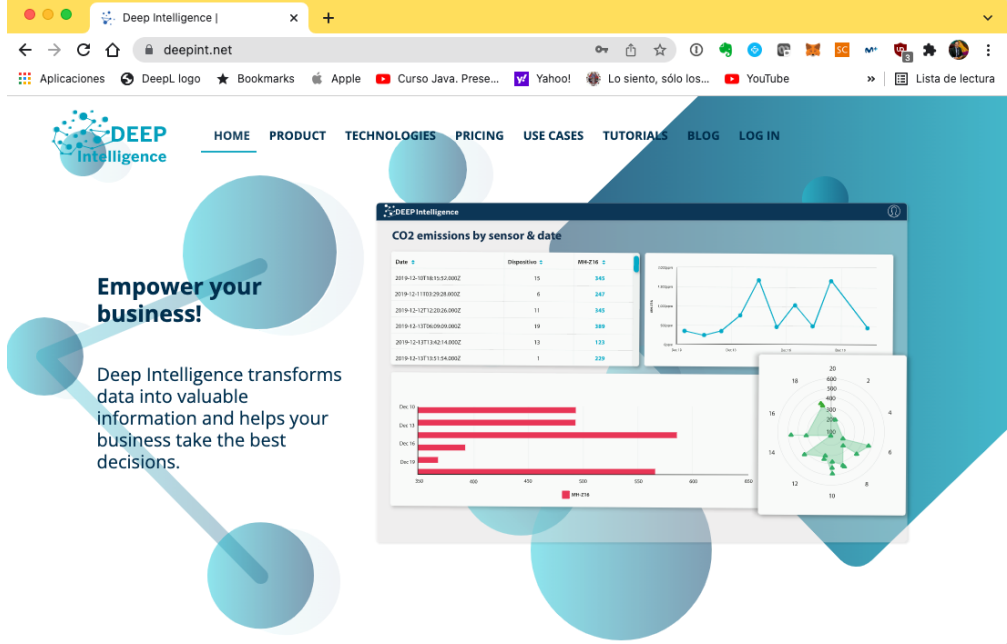
Wizard to create and train your models



Artificial Intelligence

Artificial Intelligence basics

- The system learns automatically from data
- The system is not programmed, it is trained



Supervised learning

The aim is to reproduce some "labels", known values in the data set. It is used to solve prediction problems

Classification

A discreet set of "classes"

Regression

A continuous value

Temporal series

A continuous value as a function of time

Text classification

Image classification

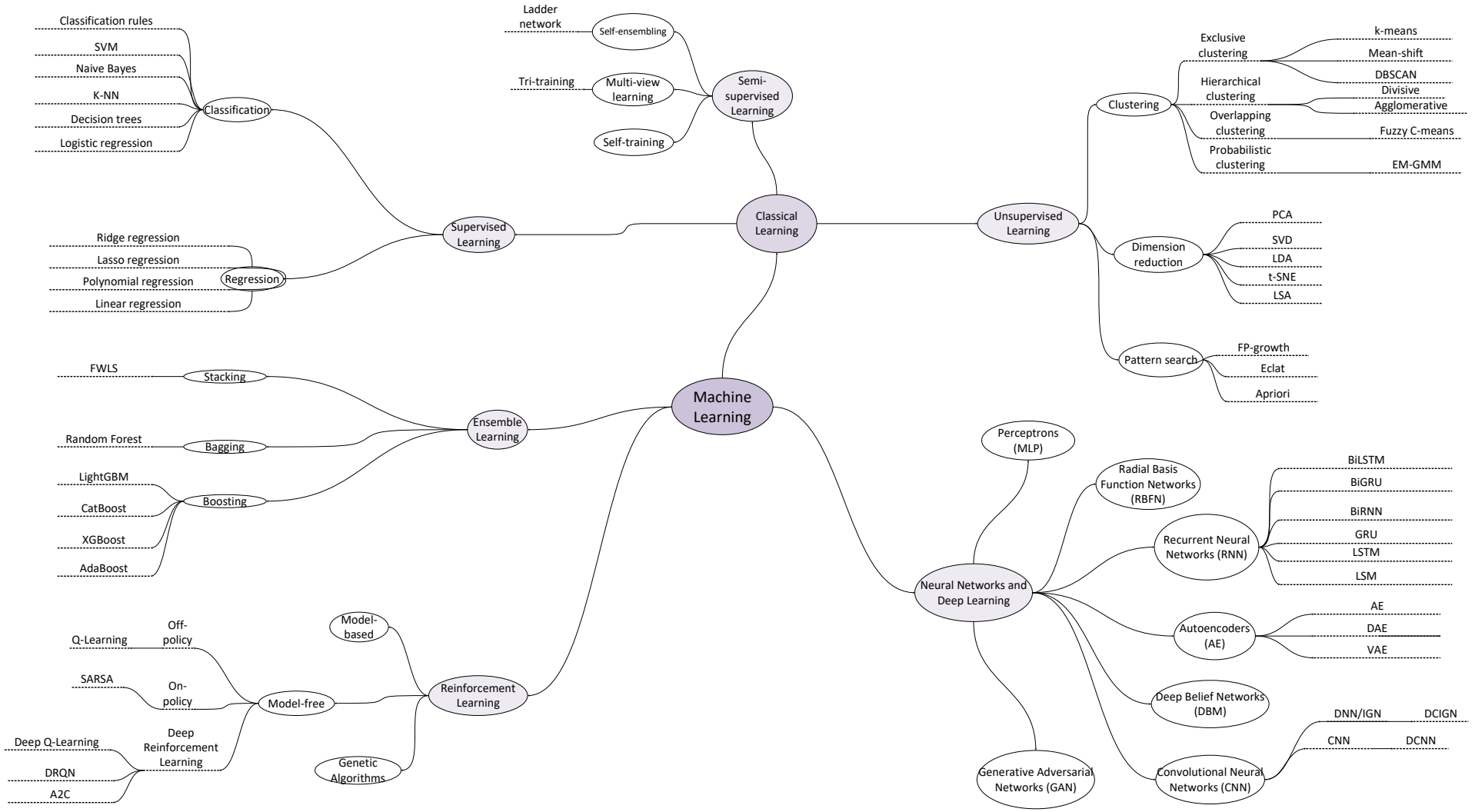
Unsupervised learning

Clustering

Group similar data

...

Reduction of dimensionality, extraction of characteristics, Measures of similarity, Association rules


Machine Learning
Classical Learning
Supervised Learning
Classification
Classification rules
SVM
Naive Bayes
K-NN
Decision trees
Logistic regression
Regression
Ridge regression
Lasso regression
Polynomial regression
Linear regression
Semi-supervised Learning
Self-ensembling
Ladder network
Multi-view learning
Tri-training
Self-training
Unsupervised Learning
Clustering
Exclusive clustering
k-means
Mean-shift
DBSCAN
Hierarchical clustering
Divisive
Agglomerative
Overlapping clustering
Fuzzy C-means
Probabilistic clustering
EM-GMM
Dimension reduction
PCA
SVD
LDA
t-SNE
LSA
Pattern search
FP-growth
Eclat
Apriori
Ensemble Learning
Stacking
FWLS
Bagging
Random Forest
Boosting
LightGBM
CatBoost
XGBoost
AdaBoost
Reinforcement Learning
Model-based
Model-free
Off-policy
Q-Learning
On-policy
SARSA
Deep Reinforcement Learning
Deep Q-Learning
DRQN
A2C
Genetic Algorithms
Neural Networks and Deep Learning
Perceptrons (MLP)
Radial Basis Function Networks (RBFN)
Recurrent Neural Networks (RNN)
BiLSTM
BiGRU
BiRNN
GRU
LSTM
LSM
Autoencoders (AE)
AE
DAE
VAE
Deep Belief Networks (DBM)
Convolutional Neural Networks (CNN)
DNN/IGN
DCIGN
CNN
DCNN
Generative Adversarial Networks (GAN)

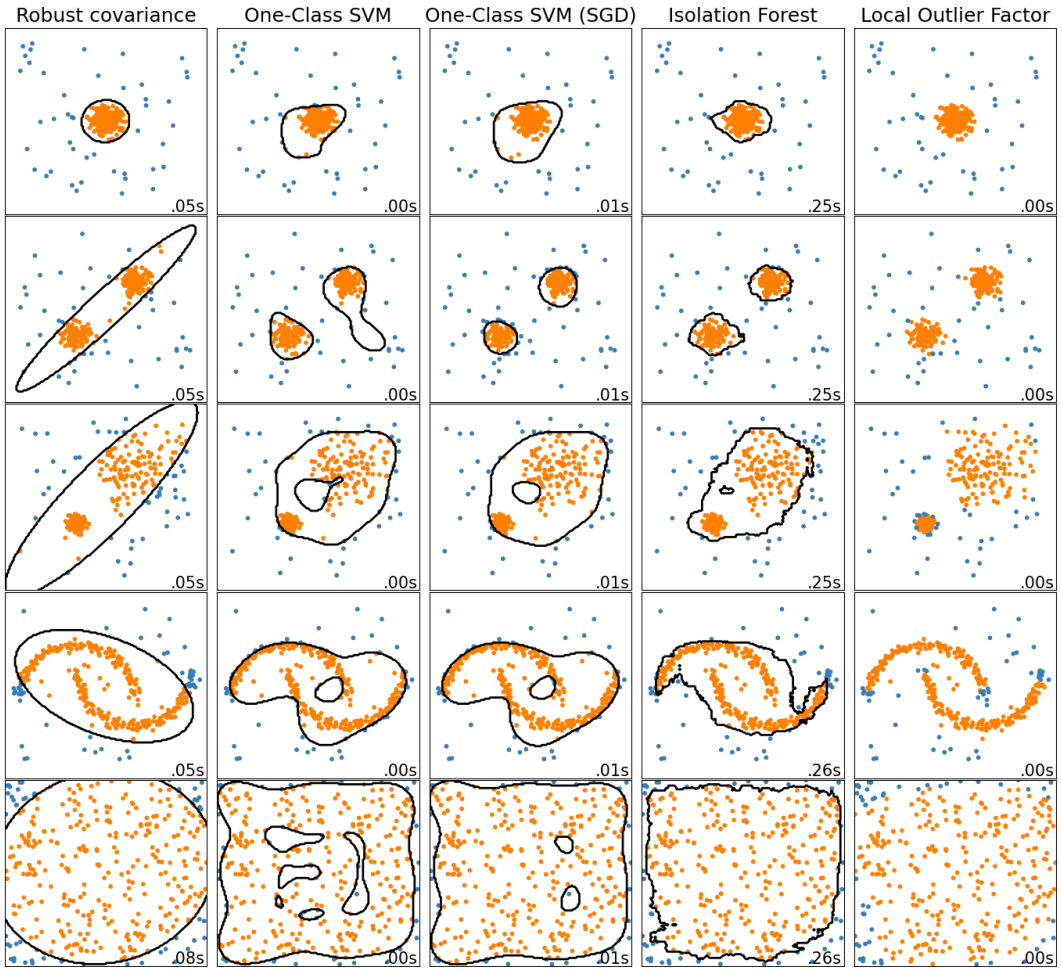
Method	Hyperparameters
Decision tree	- Split criterium - Split strategy - Maximum depth - Minimum samples per split - Minimum samples per leaf - Number of features
Random-forest	- [All of the decision tree parameters] - Number of trees - Whether to bootstrap samples
eXtreme-Gradient-Boosting	- [All of the decision tree parameters] - Type of booster - Learning rate - L1 and L2 regularization weights - Maximum number of trees
Bayes classifier	- Smoothing parameter
Logistic regression	- L1 and L2 regularization weights - Minimization algorithm
Multilayer perceptron	- Activation function - Network topology - Regularization - Solver (type and parameters) - Learning rate
K-nearest neighbours	- Number of neighbours - Weighting (uniform or inverse of distance) - Distance metric
Support vector machines	- Kernel transform (type and coefficients) - Penalty parameter - Tolerance
Linear regression	- Scaling - Intercept term

Artificial Intelligence

- Novelty and Outlier Detection

Outlier and novelty detection algorithms have been used to identify abnormal or unusual network event.

The objective is to analyse network traffic, logs, organization data in general, etc. for which we have created a new model based on a combination of the Isolation Forest and Local Outlier Factor algorithms.



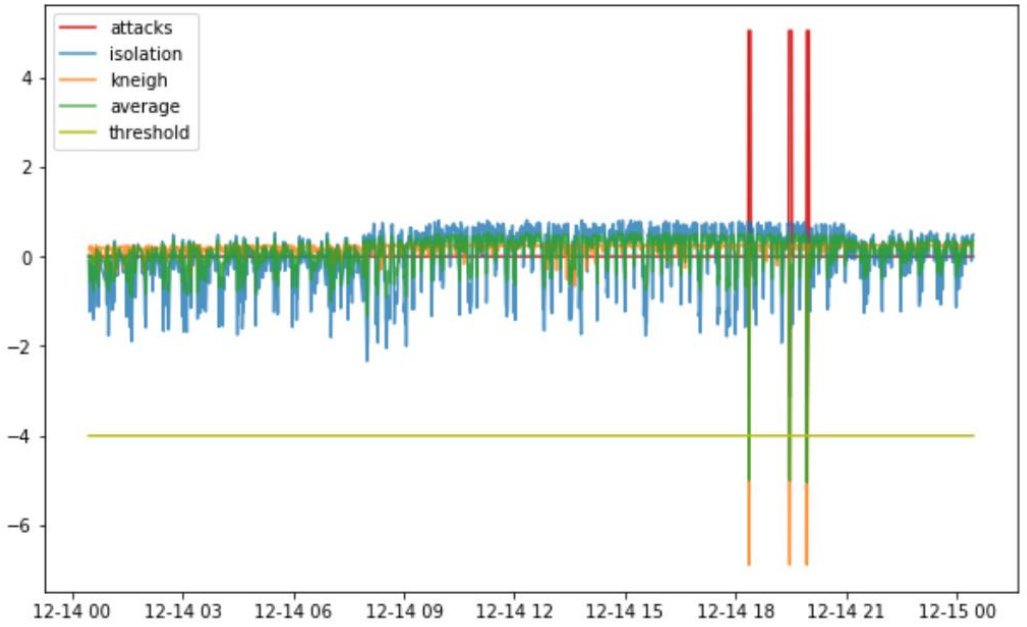
Artificial Intelligence

- Cybersecurity anomalies

DeepSIEM artificial intelligence system learns the organization's habitual behavior and detects in real time all types of anomalies, including advanced persistent threats (APT).

DeepSIEM's intelligent analysis system uses oulier and novelty detection to detect any anomaly, including unknown threats (0-Day).

One of the most important features of DeepSIEM is that the algorithms are scalable and adapt to the traffic of a given organisation/machine and its evolution over time.

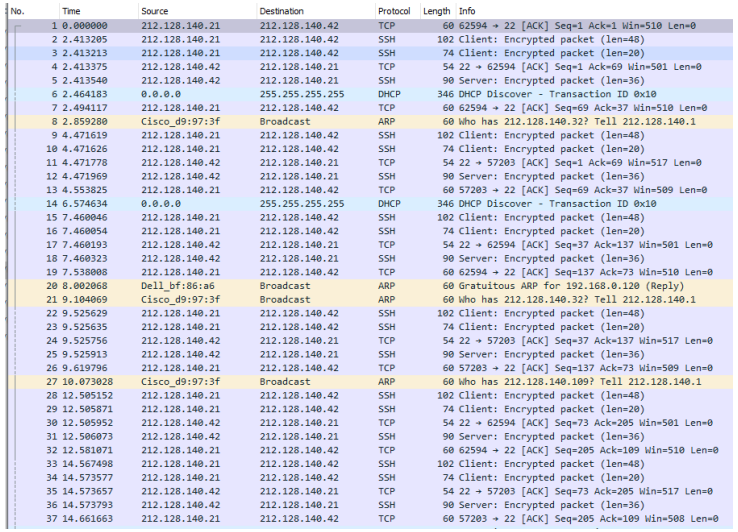


DeepSIEM network analysis using AI

Artificial Intelligence

- Use case: Network analysis

Raw network packets → **Network flows** → **Features and metrics extraction**



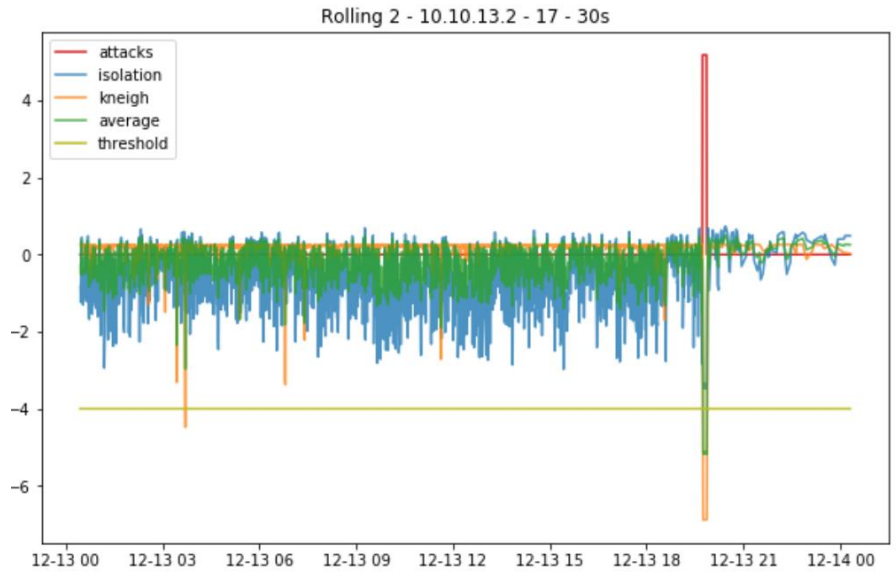
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	212.128.140.21	212.128.140.42	TCP	60	62594 → 22 [ACK] Seq=1 Ack=1 Win=510 Len=0
2	2.413205	212.128.140.21	212.128.140.42	SSH	102	Client: Encrypted packet (len=48)
3	2.413213	212.128.140.21	212.128.140.42	SSH	74	Client: Encrypted packet (len=20)
4	2.413375	212.128.140.42	212.128.140.21	TCP	54	22 → 62594 [ACK] Seq=1 Ack=69 Win=501 Len=0
5	2.413540	212.128.140.42	212.128.140.21	SSH	90	Server: Encrypted packet (len=36)
6	2.464183	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x10
7	2.494117	212.128.140.21	212.128.140.42	TCP	60	62594 → 22 [ACK] Seq=69 Ack=37 Win=510 Len=0
8	2.859280	Cisco_d9:97:3f	Broadcast	ARP	60	Who has 212.128.140.32? Tell 212.128.140.1
9	4.471619	212.128.140.21	212.128.140.42	SSH	102	Client: Encrypted packet (len=48)
10	4.471626	212.128.140.21	212.128.140.42	SSH	74	Client: Encrypted packet (len=20)
11	4.471778	212.128.140.42	212.128.140.21	TCP	54	22 → 57203 [ACK] Seq=1 Ack=69 Win=517 Len=0
12	4.471969	212.128.140.42	212.128.140.21	SSH	90	Server: Encrypted packet (len=36)
13	4.553825	212.128.140.21	212.128.140.42	TCP	60	57203 → 22 [ACK] Seq=69 Ack=37 Win=509 Len=0
14	6.574634	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x10
15	7.460046	212.128.140.21	212.128.140.42	SSH	102	Client: Encrypted packet (len=48)
16	7.460054	212.128.140.21	212.128.140.42	SSH	74	Client: Encrypted packet (len=20)
17	7.460193	212.128.140.42	212.128.140.21	TCP	54	22 → 62594 [ACK] Seq=37 Ack=137 Win=501 Len=0
18	7.460323	212.128.140.42	212.128.140.21	SSH	90	Server: Encrypted packet (len=36)
19	7.538008	212.128.140.21	212.128.140.42	TCP	60	62594 → 22 [ACK] Seq=137 Ack=73 Win=510 Len=0
20	8.002068	Dell_bf:86:a6	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.120 (Reply)
21	9.104069	Cisco_d9:97:3f	Broadcast	ARP	60	Who has 212.128.140.32? Tell 212.128.140.1
22	9.525629	212.128.140.42	212.128.140.21	SSH	102	Client: Encrypted packet (len=48)
23	9.525635	212.128.140.42	212.128.140.21	SSH	74	Client: Encrypted packet (len=20)
24	9.525756	212.128.140.21	212.128.140.42	TCP	54	22 → 57203 [ACK] Seq=37 Ack=137 Win=517 Len=0
25	9.525913	212.128.140.21	212.128.140.42	SSH	90	Server: Encrypted packet (len=36)
26	9.619796	212.128.140.21	212.128.140.42	TCP	60	57203 → 22 [ACK] Seq=137 Ack=73 Win=509 Len=0
27	10.073028	Cisco_d9:97:3f	Broadcast	ARP	60	Who has 212.128.140.109? Tell 212.128.140.1
28	12.505152	212.128.140.21	212.128.140.42	SSH	102	Client: Encrypted packet (len=48)
29	12.505871	212.128.140.21	212.128.140.42	SSH	74	Client: Encrypted packet (len=20)
30	12.505952	212.128.140.42	212.128.140.21	TCP	54	22 → 62594 [ACK] Seq=73 Ack=205 Win=501 Len=0
31	12.506073	212.128.140.42	212.128.140.21	SSH	90	Server: Encrypted packet (len=36)
32	12.581071	212.128.140.21	212.128.140.42	TCP	60	62594 → 22 [ACK] Seq=205 Ack=109 Win=510 Len=0
33	14.567498	212.128.140.42	212.128.140.42	SSH	102	Client: Encrypted packet (len=48)
34	14.573577	212.128.140.21	212.128.140.42	SSH	74	Client: Encrypted packet (len=20)
35	14.573657	212.128.140.42	212.128.140.21	TCP	54	22 → 57203 [ACK] Seq=73 Ack=205 Win=517 Len=0
36	14.573793	212.128.140.42	212.128.140.21	SSH	90	Server: Encrypted packet (len=36)
37	14.661663	212.128.140.21	212.128.140.42	TCP	60	57203 → 22 [ACK] Seq=205 Ack=109 Win=508 Len=0

Artificial Intelligence

- Use case: Network analysis

start_time	fl_dur	tot_fw_pk	tot_bw_pk	fw_win_byt	fw_seg_min	...	atv_min	idl_avg	idl_std	idl_max	idl_min	src_addr	dst_addr	protocol	dst_port	src_port
2021-12-01 18:20:01.174036026	4328676	14	13	343	32	...	0	0	0	0	0	3.70.21.46	10.10.11.2	6	80	47480

- DeepSIEM ingest tool **extracts** more than 60 features of the various network flows.
- DeepSIEM **models** the traffic by differentiating between **day and night**, **business and non-business days**, **network protocol** and **traffic origin**.
- At the moment, the network traffic analysis uses the combination of two different artificial intelligence models.



Artificial Intelligence

- Log and event correlation

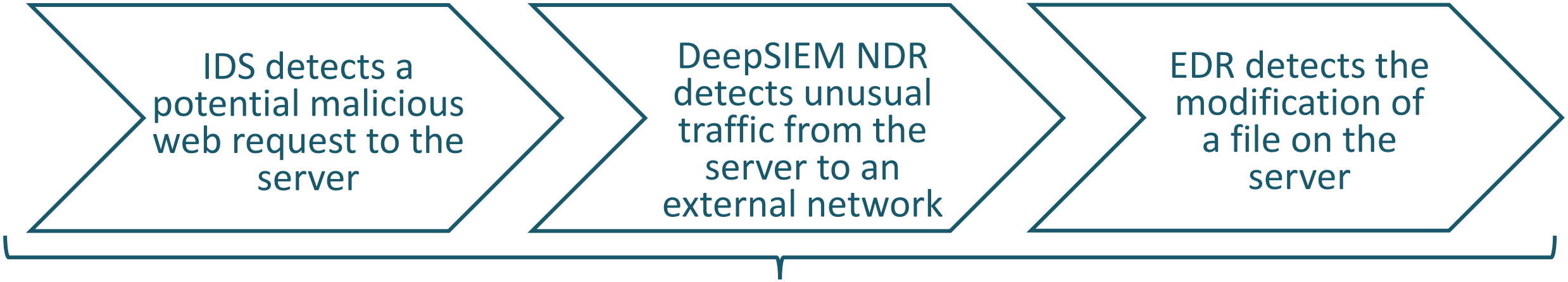
DeepSIEM's ingestion tool includes a built-in correlation engine that allows to obtain data from different services and assets, combine them and analyze them to detect cyber threats.

The solution uses machine learning for detecting new unknown threats that have similar behavior or similar structure and identifiable characteristics to previous or known historical attacks. The algorithms search for patterns in the behavior of the logs and relate them to attack vectors and threats established in fully customizable rules.

The application of these techniques also allows relating different logs to a threat, obtaining more information, detecting the attackers and being able to mitigate the threat effectively.

Artificial Intelligence

- Use case: Threat detection by correlation system



DeepSIEM correlation system detects and reports the threat

IDS Intrusion Detection System **NDR** Network Detection and Response **EDR** Endpoint detection and response

Artificial Intelligence

- Alert priorization with AI

The number of events generated by today's security systems saturates analysts, so they are looking for solutions that reduce the number of false positives and prioritize threats according to the organization's preferences.

All analysis engines included in DeepSIEM are focused on eliminating false positives, but an **intelligent prioritization system** has also been developed.

The **prioritization system** uses **supervised learning** techniques to understand the organization's preferences and start sorting events based on their different fields. Natural language processing algorithms are used on the content of the events and classification algorithms that allow to consider fields such as destination of the attacks, country of origin, the affected service, the time zone, among others.

Artificial Intelligence

- Use case: **Alert priorization**
- The system learns after DeepSIEM deployment for a few days. Simplifying, for example, analysts classify most of detected alerts from China against the "Production web server 1" as high priority.

- Origin: China
- Destination: Production web server 1
- Service: HTTP Service
- Severity: Medium

- Priority: High

EXAMPLE OF ALERT 1

- Origin: Spain
- Destination: Develpment server
- Service: FTP Service
- Severity: Medium

- Priority: Low

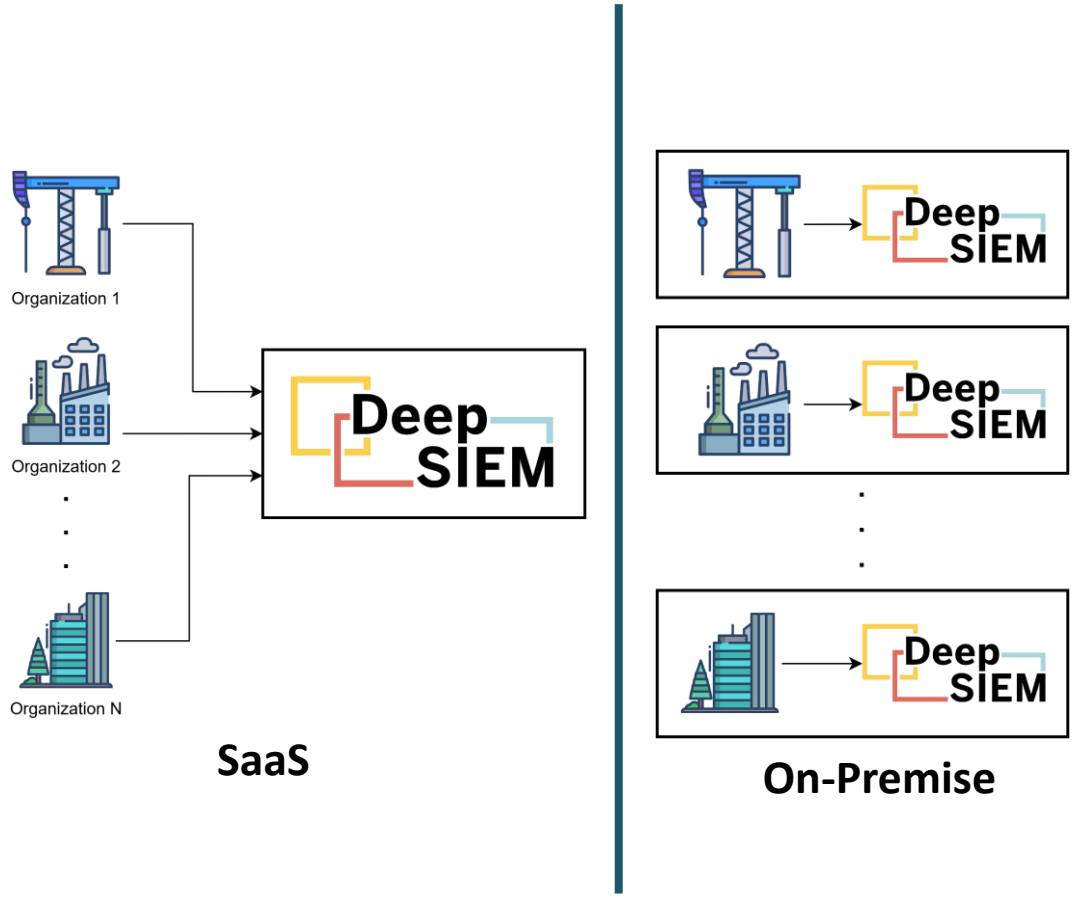
EXAMPLE OF ALERT 2

Technology

Cloud Computing

DeepSIEM's integrated deployment wizard allows a choice of SaaS modes, multi-vendor cloud deployment and on-premise deployment.

Cloud deployment options allow you to leverage the full computing power, configuration facilities and scaling advantages while on-premise deployment allows you to adapt to all the needs and constraints that can occur in complex business environments.



Technology

Big Data

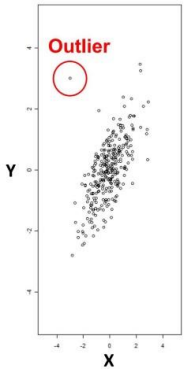
The amount of security event data is so large that security operations centre teams must manage billions of events each day. DeepSIEM integrates Big Data technologies to facilitate real-time ingestion, processing and search for large volumes of data.

Technology

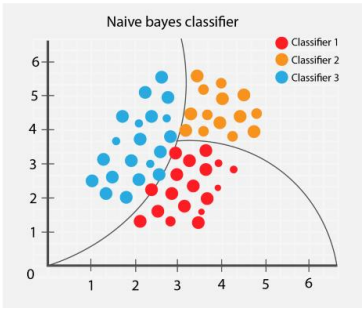
Artificial Intelligence

The data that the platform obtains from the systems it monitors allow for the development of models adapted to each infrastructure. These models trace the behaviour of each device, network and application, making it possible to detect anomalies and advanced attacks that would have been able to elude conventional solutions. DeepSIEM has an automatic learning module that uses global asset and threat data for model evolution and their rapid adaptation to the changing cyber security environment.

- **Threat detection with ML**
  - Outlier detection
  - Novelty detection



- **Event priorization**
  - Supervised algorithms
  - NLP
  - Classification algorithms. Such as:
    - Naive Bayes classifier
    - C-Support Vector Classification



- **Threat Intelligence with AI**
  - Known threats + Machine Learning → Unknown threats detection
  - IoC automatic generation
    (Indicator of compromise)

Technology

Distributed Computing

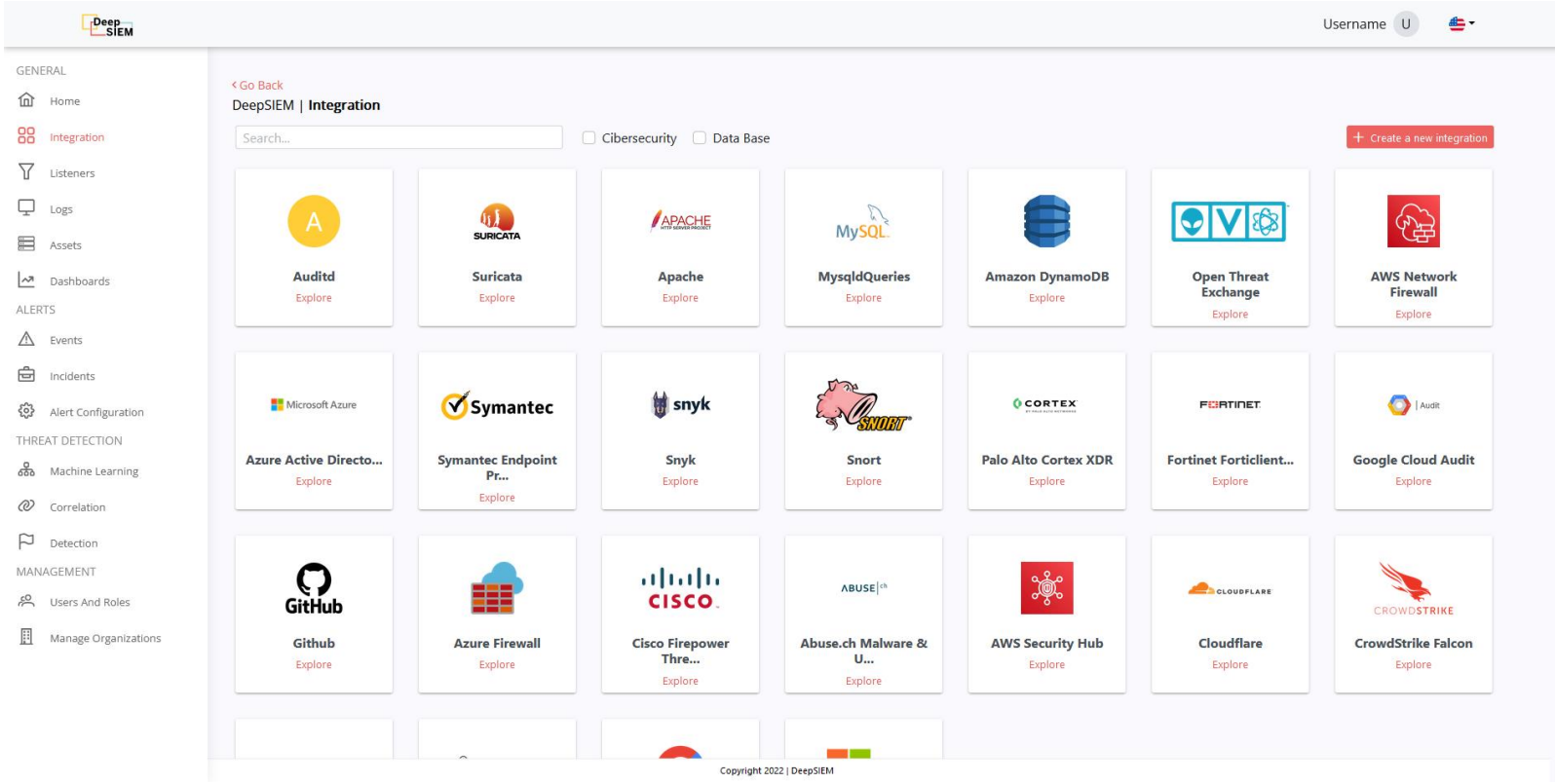
The DeepSIEM platform has been designed for all types of organizations with a heavy data traffic; small, medium and large companies alike. For this reason, its design is fully modular and scalable and can be deployed in environments that are adapted to the needs of the organisation.

Main features

- **Advanced Ingestion System**
  - Support for Linux, Windows, Mac, IoT and industry devices
  - Sources such as Windows events logs, modbus, IDS, EDR, NDR, AV,…
  - Customer-defined custom sources
  - Big data technologies such us Apache NiFi, Apache Kafka, Elasticsearch, MongoDB,…
  - Traditional IT infrastructures, Smart cities, Smart building, IoT and Industry 4.0
  - Data enhancement

Advanced Ingestion System

DeepSIEM's goal is to cover all the needs of a SOC with a single tool. But also, to allow organisations to integrate their own cybersecurity sources and tools.



GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations

Go Back

DeepSIEM | Integration |

AWS Network Firewall

Cibersecurity

AWS Network Firewall is a managed network security service that makes it easy to deploy threat prevention for Amazon Virtual Private Clouds (VPCs).

Configure listener

Edit integration

Intake methods

Auditbeat
ListenBeats
Auditbeat communicates directly with the Linux audit framework, collects the same data as auditd, and sends the events in real time. DeepSIEM will receive auditbeat logs sent using using Libbeat's 'output.logstash'
Explore

KafkaProducer
ConsumeKafka_2_6
Apache Kafka is an open-source distributed event streaming platform used by thousands of companies for high-performance data pipelines, streaming analytics, data integration, and mission-critical applications. DeepSIEM can receive logs from multiples source througth kafka producer
Explore

ListenBeats
ListenBeats
DeepSIEM will receive multyple type of logs sent using using Libbeat's

Listeners

Information
AuditBeat Datacenter3
Auditd sent througth auditbeat from our Datacenter at Australia

Configuration

PORT	MAX SIZE OF MESSAGE QUEUE	MAX Nº OF TCP CONNECTIONS
4552	20000	5

Status

Processor: #1

INPUT_MESSAGES	OUTPUT_MESSAGES	ACTIVE_THREADS
1256	2456	68

Processor: #2

INPUT_MESSAGES	OUTPUT_MESSAGES	ACTIVE_THREADS
1256	2456	68

Information
AuditBeat Datacenter3
Auditd sent througth auditbeat from our Datacenter at Australia

Configuration

PORT	MAX SIZE OF MESSAGE QUEUE	MAX Nº OF TCP CONNECTIONS
4552	20000	5

Status

Processor: #1

INPUT_MESSAGES	OUTPUT_MESSAGES	ACTIVE_THREADS
1256	2456	68

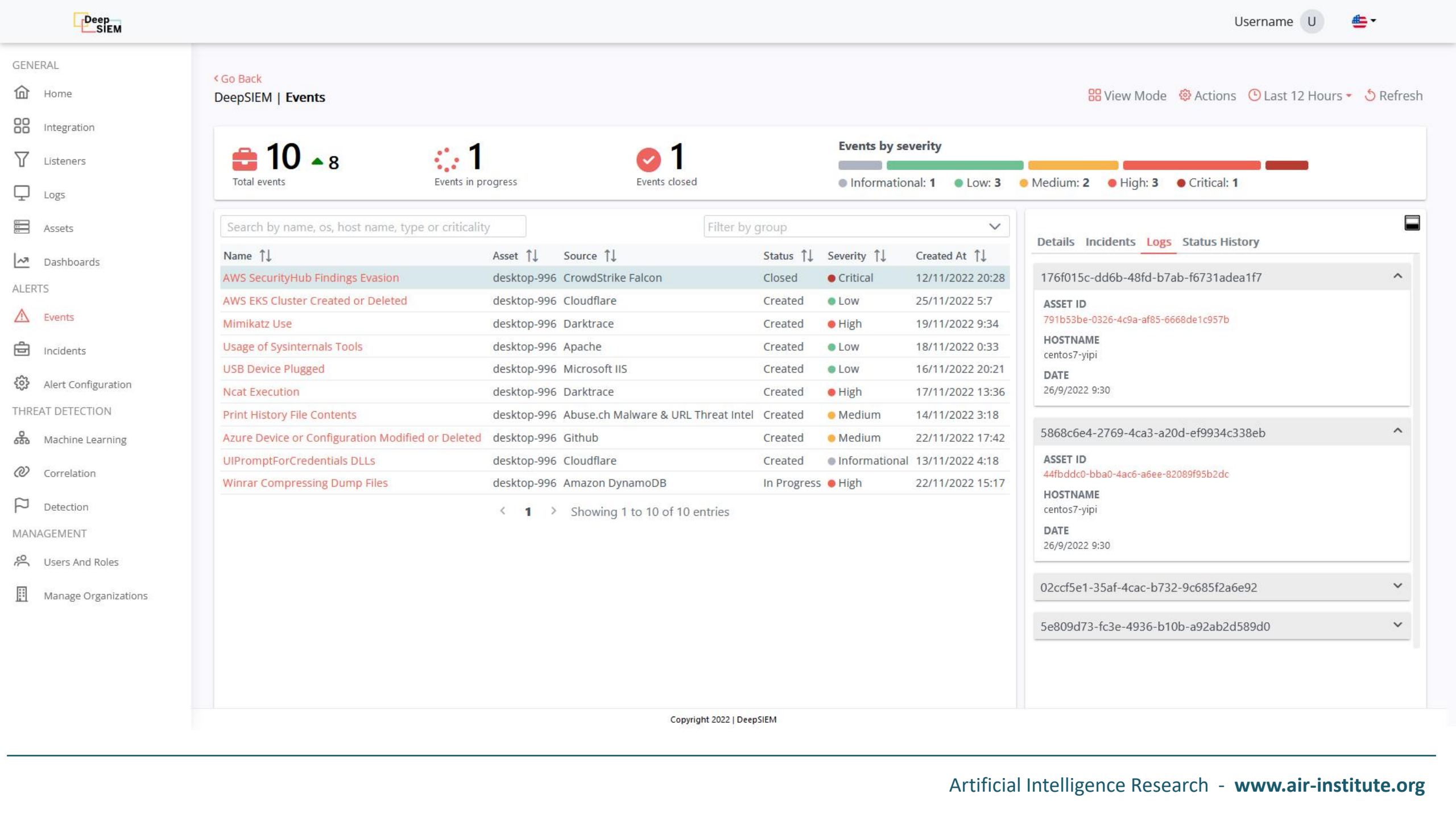
Processor: #2

INPUT_MESSAGES	OUTPUT_MESSAGES	ACTIVE_THREADS
1256	2456	68

Main features

- **Real-time threat detection**
  - Detection provided by third party tools (AV, EDR, NDR, IDS,…), rule-based analysis and anomaly detection with artificial intelligence.
  - Advanced correlation system that uses artificial intelligence to identify patterns and relationships among collected logs and events.




Deep SIEM
Username U
GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations
Go Back
DeepSIEM | Events
View Mode
Actions
Last 12 Hours
Refresh
10 8
Total events
1
Events in progress
1
Events closed
Events by severity
Informational: 1
Low: 3
Medium: 2
High: 3
Critical: 1
Search by name, os, host name, type or criticality
Filter by group
Name
Asset
Source
Status
Severity
Created At
AWS SecurityHub Findings Evasion desktop-996 CrowdStrike Falcon Closed Critical 12/11/2022 20:28
AWS EKS Cluster Created or Deleted desktop-996 Cloudflare Created Low 25/11/2022 5:7
Mimikatz Use desktop-996 Darktrace Created High 19/11/2022 9:34
Usage of Sysinternals Tools desktop-996 Apache Created Low 18/11/2022 0:33
USB Device Plugged desktop-996 Microsoft IIS Created Low 16/11/2022 20:21
Ncat Execution desktop-996 Darktrace Created High 17/11/2022 13:36
Print History File Contents desktop-996 Abuse.ch Malware & URL Threat Intel Created Medium 14/11/2022 3:18
Azure Device or Configuration Modified or Deleted desktop-996 Github Created Medium 22/11/2022 17:42
UIPromptForCredentials DLLs desktop-996 Cloudflare Created Informational 13/11/2022 4:18
Winrar Compressing Dump Files desktop-996 Amazon DynamoDB In Progress High 22/11/2022 15:17
1
Showing 1 to 10 of 10 entries
Details
Incidents
Logs
Status History
176f015c-dd6b-48fd-b7ab-f6731adea1f7
ASSET ID
791b53be-0326-4c9a-af85-6668de1c957b
HOSTNAME
centos7-yipi
DATE
26/9/2022 9:30
5868c6e4-2769-4ca3-a20d-ef9934c338eb
ASSET ID
44fbddc0-bba0-4ac6-a6ee-82089f95b2dc
HOSTNAME
centos7-yipi
DATE
26/9/2022 9:30
02ccf5e1-35af-4cac-b732-9c685f2a6e92
5e809d73-fc3e-4936-b10b-a92ab2d589d0
Copyright 2022 | DeepSIEM

GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations

Go Back

DeepSIEM | **Incidents**

View Mode Actions Last 12 Hours Refresh

5 ▲3
Total incidents

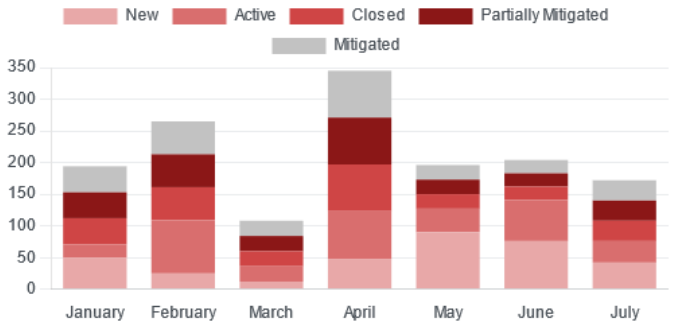
1
Incidents in progress

1
Incidents closed

Incidents by severity

Informational: **0** Low: **2** Medium: **2** High: **1** Critical: **0**

Incidents status by creation time



IncidentsStatus

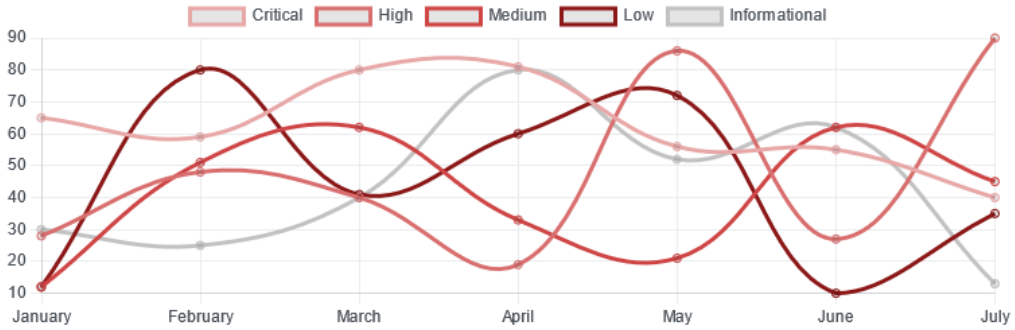
New: **0** Active: **2** Closed: **2** Partially Mitigated: **1** Mitigated: **0**

Mean time to acknowledge
5.20 days

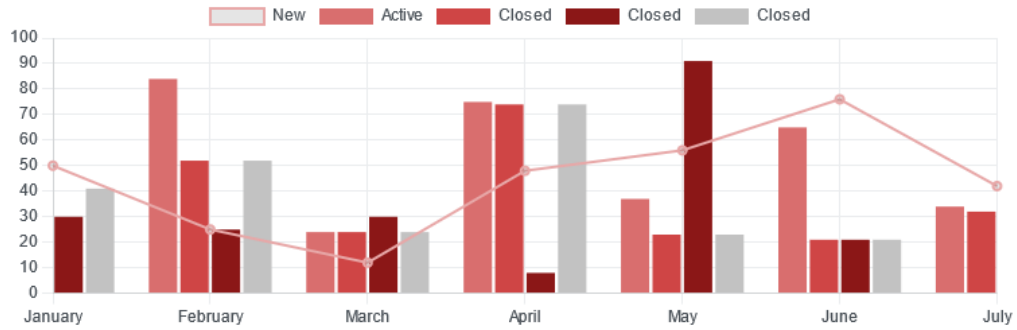
Mean time to close
22.32 min

Mean time to acknowledge
12 days

IncidentsStatus



IncidentsStatus



Main features

- **Incident Management and SOAR**
  - Full management and investigation of **events and incidents** through the user interface allowing you to view, add and edit evidence, add comments and manage the mitigations applied and the generation of security reports.
  - **Assignment of events** and incidents to incident response teams.
  - **Configurable advanced alert** system with notification methods such as SMS, email and Slack, allowing you to select which alerts to generate and who to notify based on the assets affected, the risk or characteristics of events and incidents.
  - Incident and event **prioritisation** system using artificial intelligence based on past cases and recommendation algorithms.
  - An **early response system** that autonomously notifies and mitigates threats based on past cases.

GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations

Go Back

DeepSIEM | Assets | **e85f1784-bf05-4142-9a41-9b731f53d85a**

Main web app Server

e85f1784-bf05-4142-9a41-9b731f53d85a

Server Type

Madrid Location

Low Criticality

DESCRIPTION

Linux server that serves the organization's main web applications.

HOSTNAME

webserver-8771

TAGS:

Backend Server Linux CentOS

NETWORK

IPs:

103.112.2.122 212.128.213.223

MACs:

02:00:00:84:92:42 02:00:00:6d:1c:d8

CREATED AT

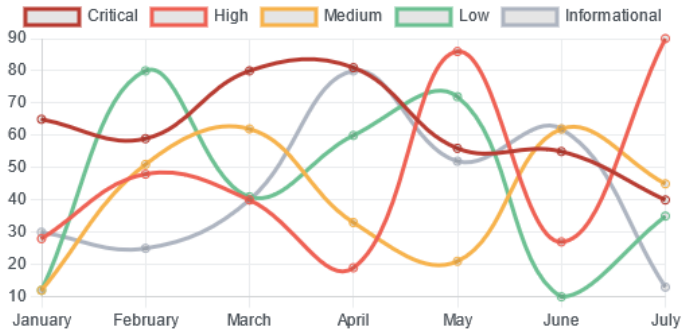
18/11/2022 12:59

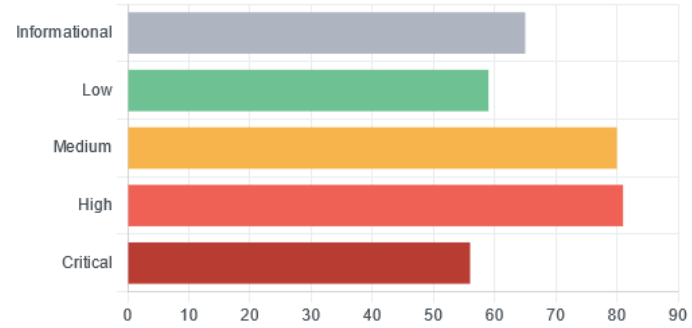
LAST ACTIVITY DATE

18/11/2022 12:59

Actions

Events Incidents Data sources Groups Alert Configuration





ID	Name	Description	N°
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Apache	Apache2 web server	100
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Apache	Apache2 web server	100
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Apache	Apache2 web server	100
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85
a5f7f9d9-3229-4506-8cff-95bbfb9b6d64	Nginx	Nginx web server	85

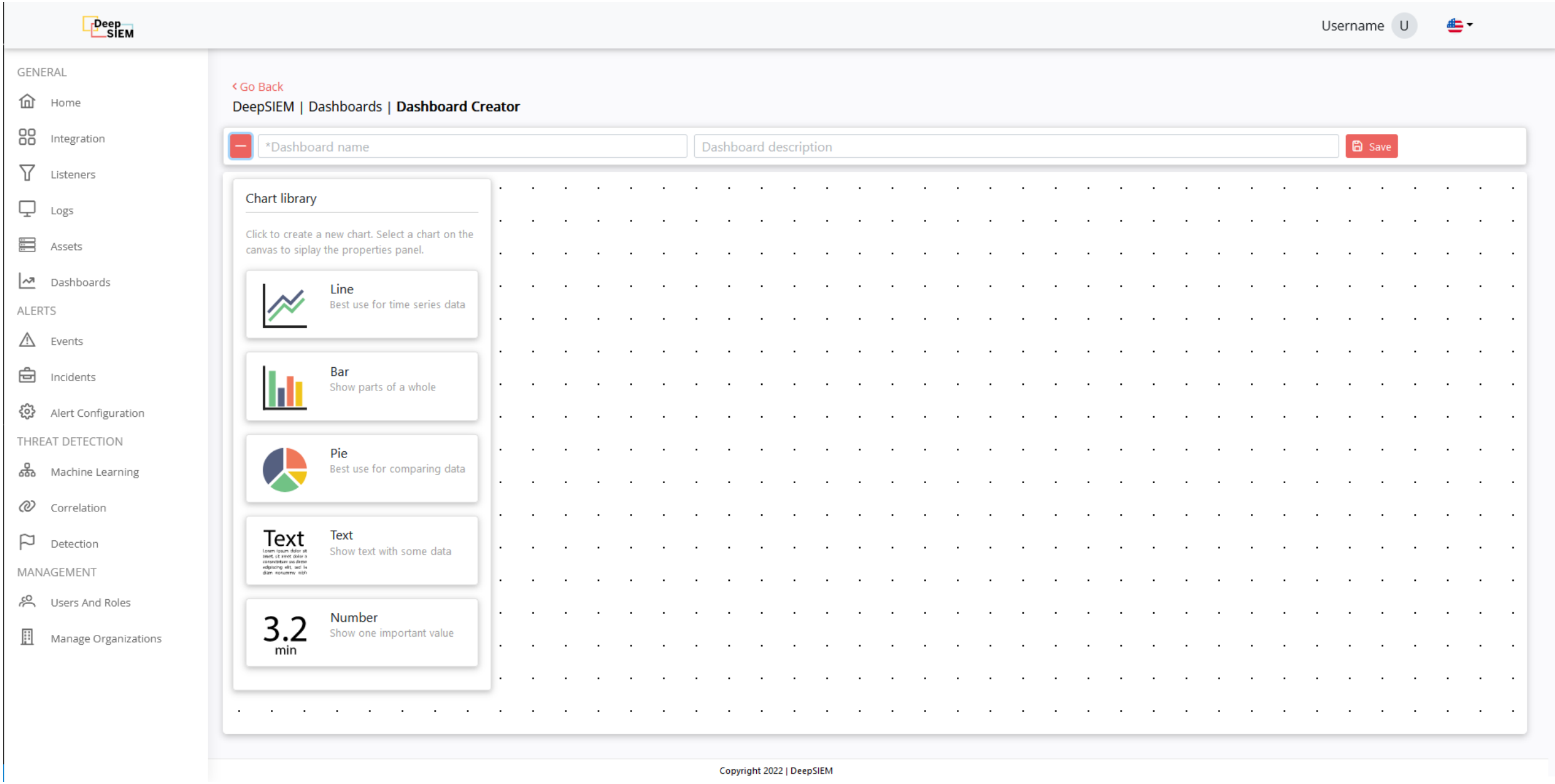
1 Showing 1 to 10 of 10 entries

Main features

- **Compliance**
  - **Security policy compliance** monitoring system using multi-agent systems and a system of rules.
  - Security recommendation system with AI.
- **Threat Intelligence**
  - Repository of threat intelligence sources (**including Dark Web**) to feed detection, alerting and intelligence reporting systems.
  - AI-enabled IoC generation engine to improve detection and future incident management capabilities.

Main features

- **Multi-Organization**
  - Multi-organisational system regardless of size allows monitoring from small companies to service providers managing central SoCs.
  - System of users, permissions, roles and teams to manage incidents.
  - Asset discovery and management for an overview of the organization.
- **GUI**
  - Centralisation of information and management of the entire platform.
  - Fully customisable dashboards.
  - Advanced incident management and investigation.


Deep SIEM
Username U
GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations
Go Back
DeepSIEM | Dashboards | Dashboard Creator
*Dashboard name
Dashboard description
Save
Chart library
Click to create a new chart. Select a chart on the canvas to siplay the properties panel.
Line
Best use for time series data
Bar
Show parts of a whole
Pie
Best use for comparing data
Text
Text
Show text with some data
3.2
min
Number
Show one important value
Copyright 2022 | DeepSIEM

GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations

Go Back

DeepSIEM | Dashboards | **Dashboard Creator**

*Dashboard name

Dashboard description

Save

*Name

New Chart Name

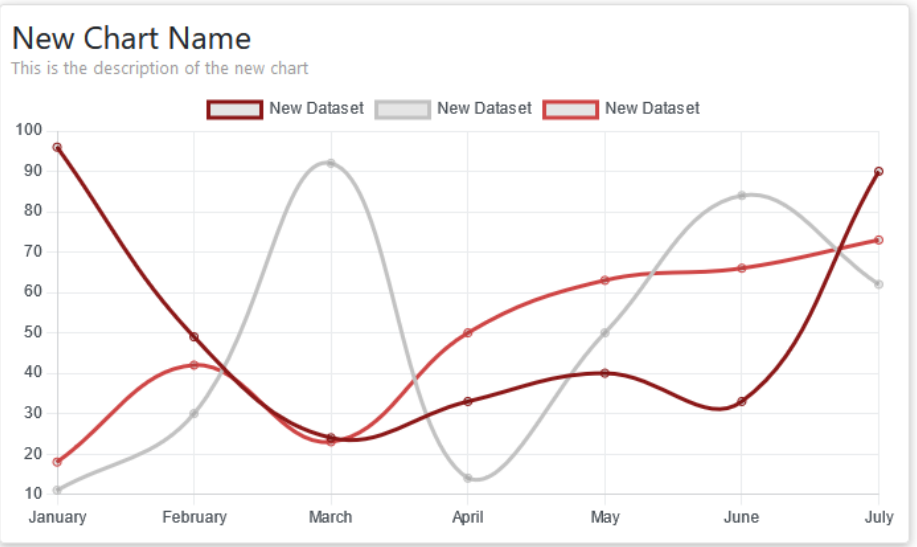
Description

This is the description of the new chart

Rule

(events.status == 1) or (events.status > 3)

Palette



Add to dashboard

GENERAL
Home
Integration
Listeners
Logs
Assets
Dashboards
ALERTS
Events
Incidents
Alert Configuration
THREAT DETECTION
Machine Learning
Correlation
Detection
MANAGEMENT
Users And Roles
Manage Organizations

Go Back

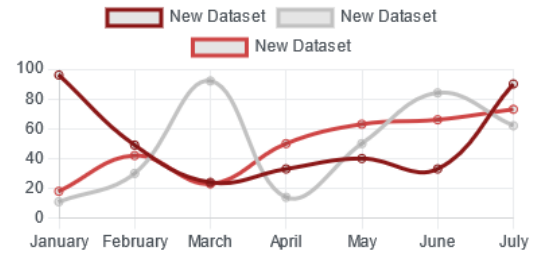
DeepSIEM | Dashboards | **Dashboard Creator**

*Dashboard name

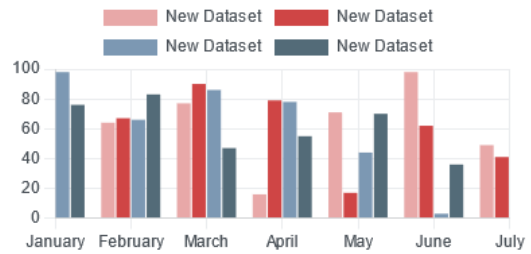
Dashboard description

Save

New Chart Name
This is the description of the new chart



New Chart Name
This is the description of the new chart

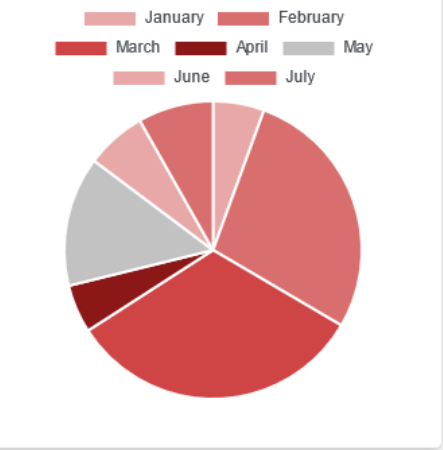


New Chart Name
This is the description of the new chart

252.00

new assets

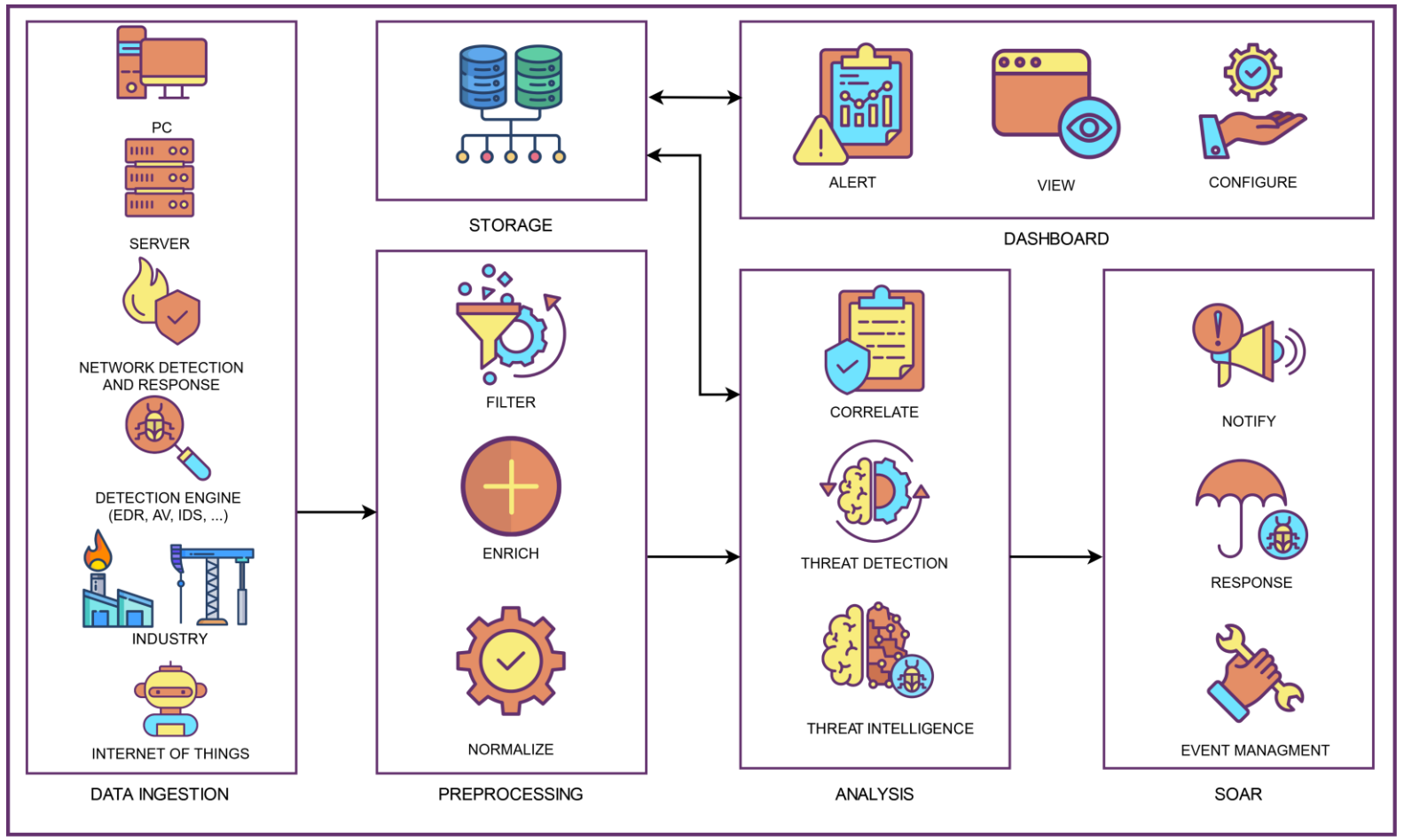
New Chart Name
This is the description of the new chart



New Chart Name
This is the description of the new chart

This is the text you want to show in this chart

Architecture

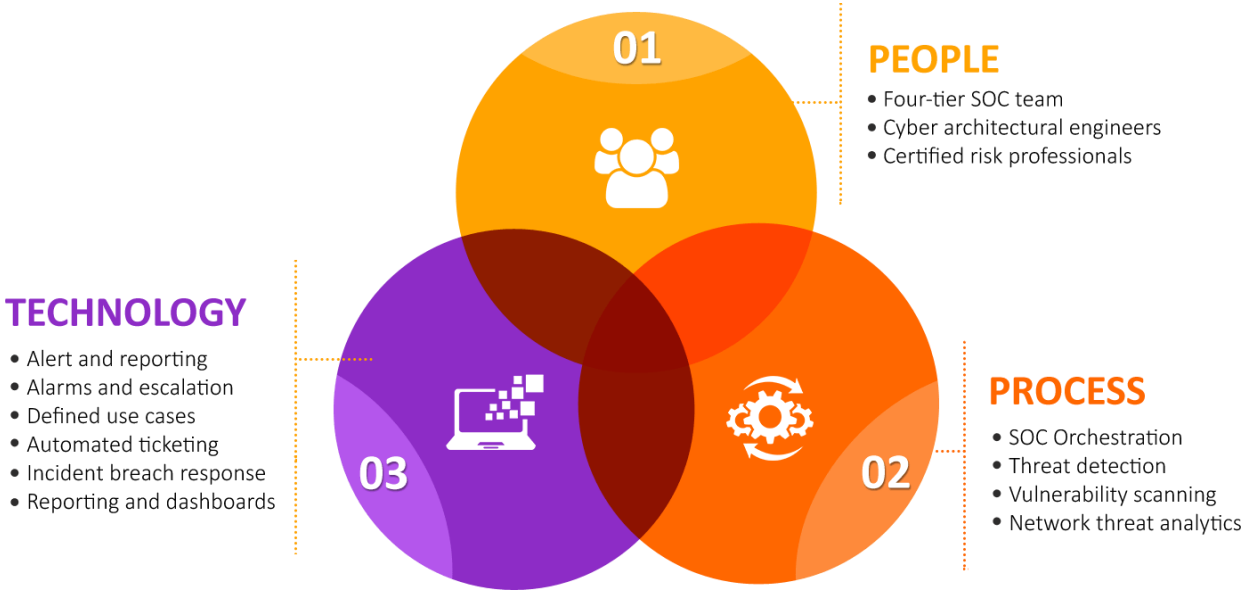


What is a SOC?

Security Operation Center (SOC) is a centralized function that provides prevention, detection and response services to **all areas** of an organization and to **any type of threat**.

We are currently deploying our own **SOC** to provide service to local small and medium-sized enterprises.

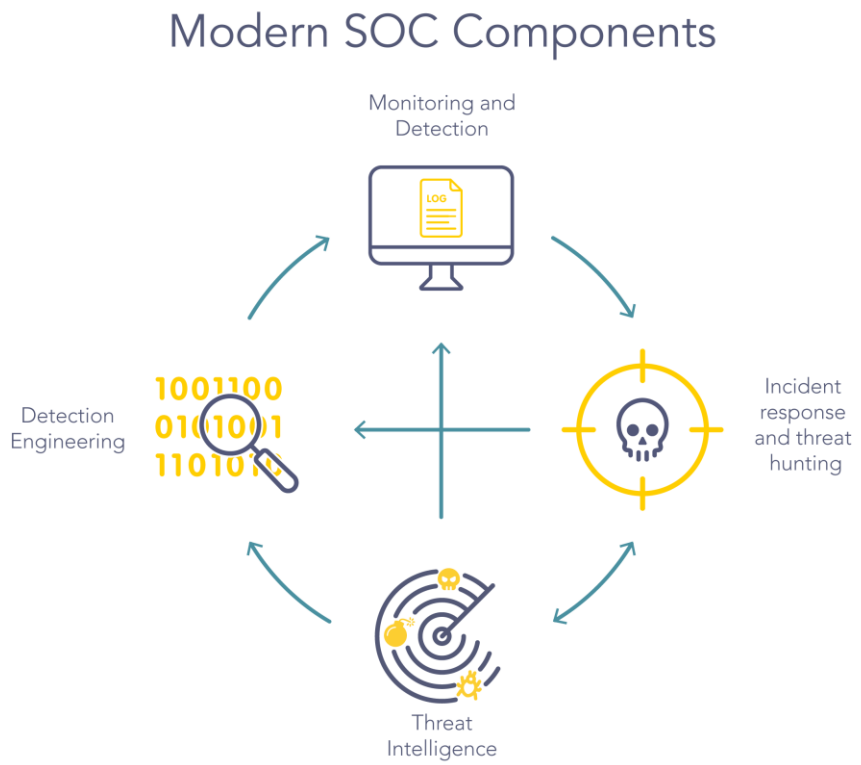
A security operation center has **three main components**:



Tools included in a SOC

The SOC includes a set of tools in a diverse technology stack to help cybersecurity analysts continuously monitor security activities in the organization's IT infrastructure.

- **Collection and Correlation.**
  - SIEM (Security Information and Event Management)
- **Detection and response.**
  - EDR (Endpoint Detection and Response)
  - NDR (Network Detection and Response)
  - IPS (Intrusion Prevention System)
  - IDS (Intrusion Detection System)
  - AV (Antivirus)
- **Incident management**
- **SOAR (Security Orchestration, Automation, and Response)**
- **Threat Intelligence**

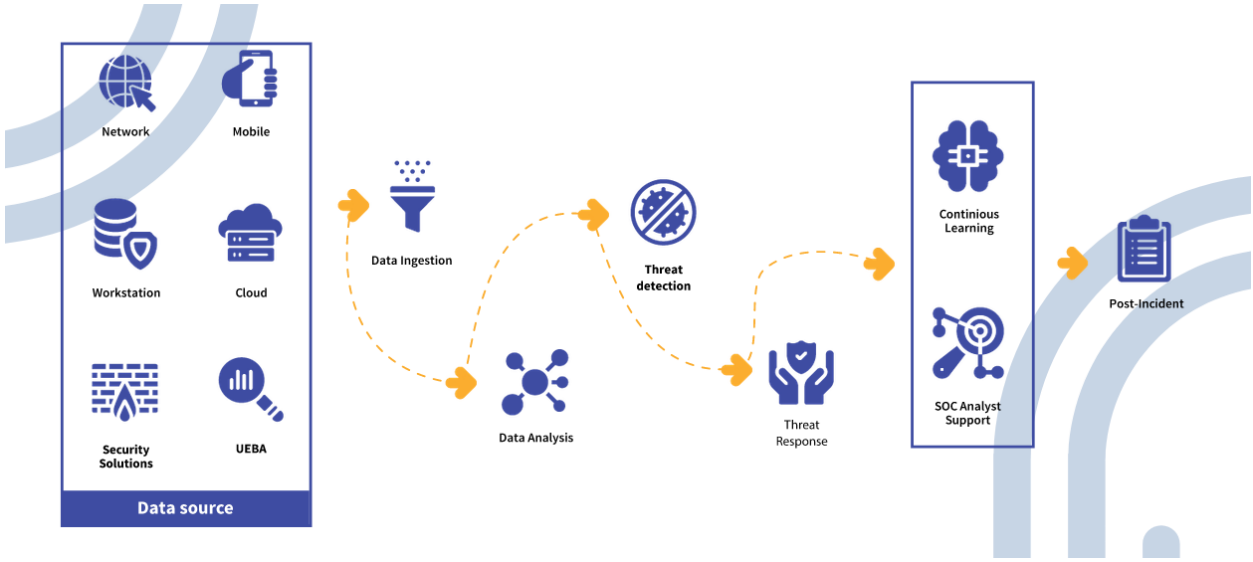


SOC-AI

What is SOC AI?

SOC-AI is an advanced Security Operations Center that uses **artificial intelligence** to detect and respond to cyber threats in real-time. Its main function is to continuously monitor and analyze security events to enhance threat detection and response capabilities.

AI-driven SOC offer organizations of all sizes the latest and most advanced security technologies to keep their networks, systems and data safe.

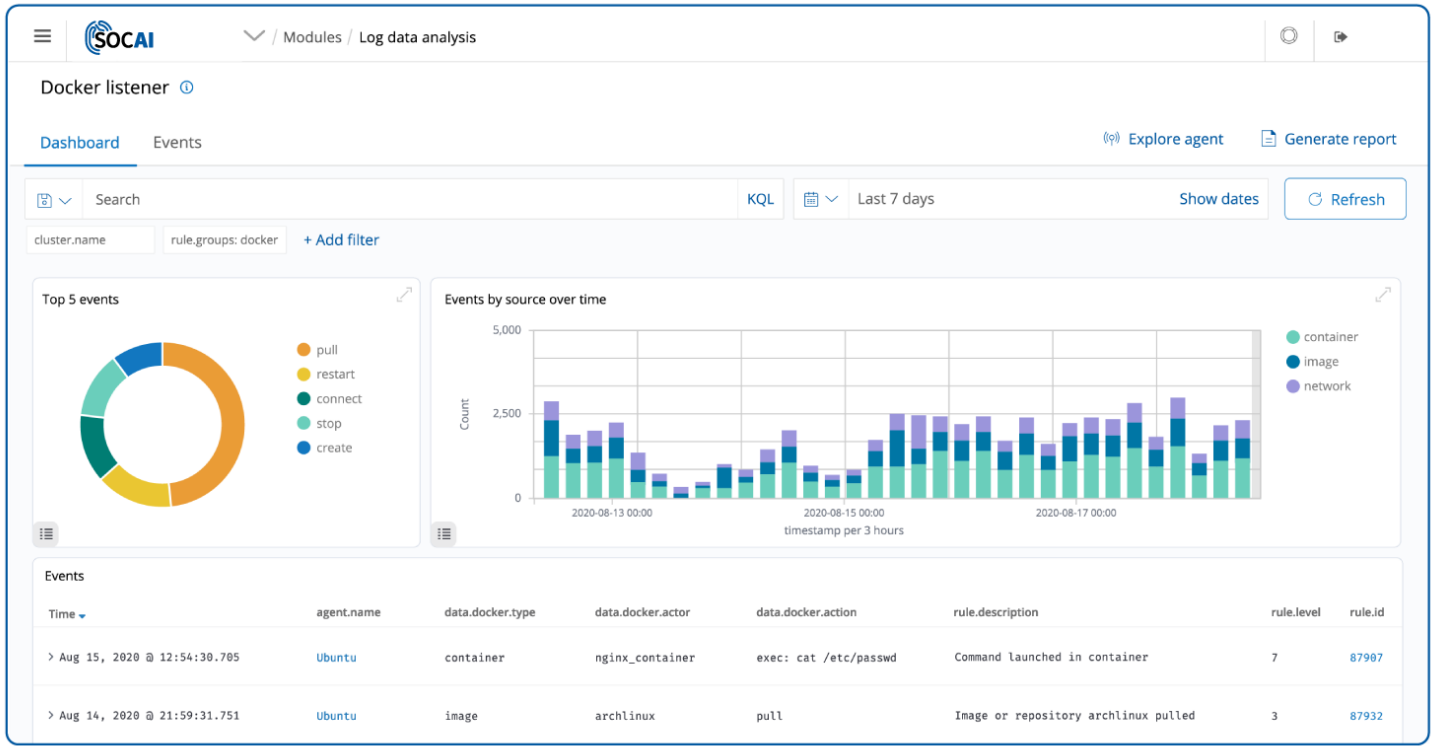


SOC-AI

Data ingestion

SOC-AI provides integration methods to obtain information from multiple sources.

The screenshot shows the information and analysis performed on a linux asset integrated in the platform.

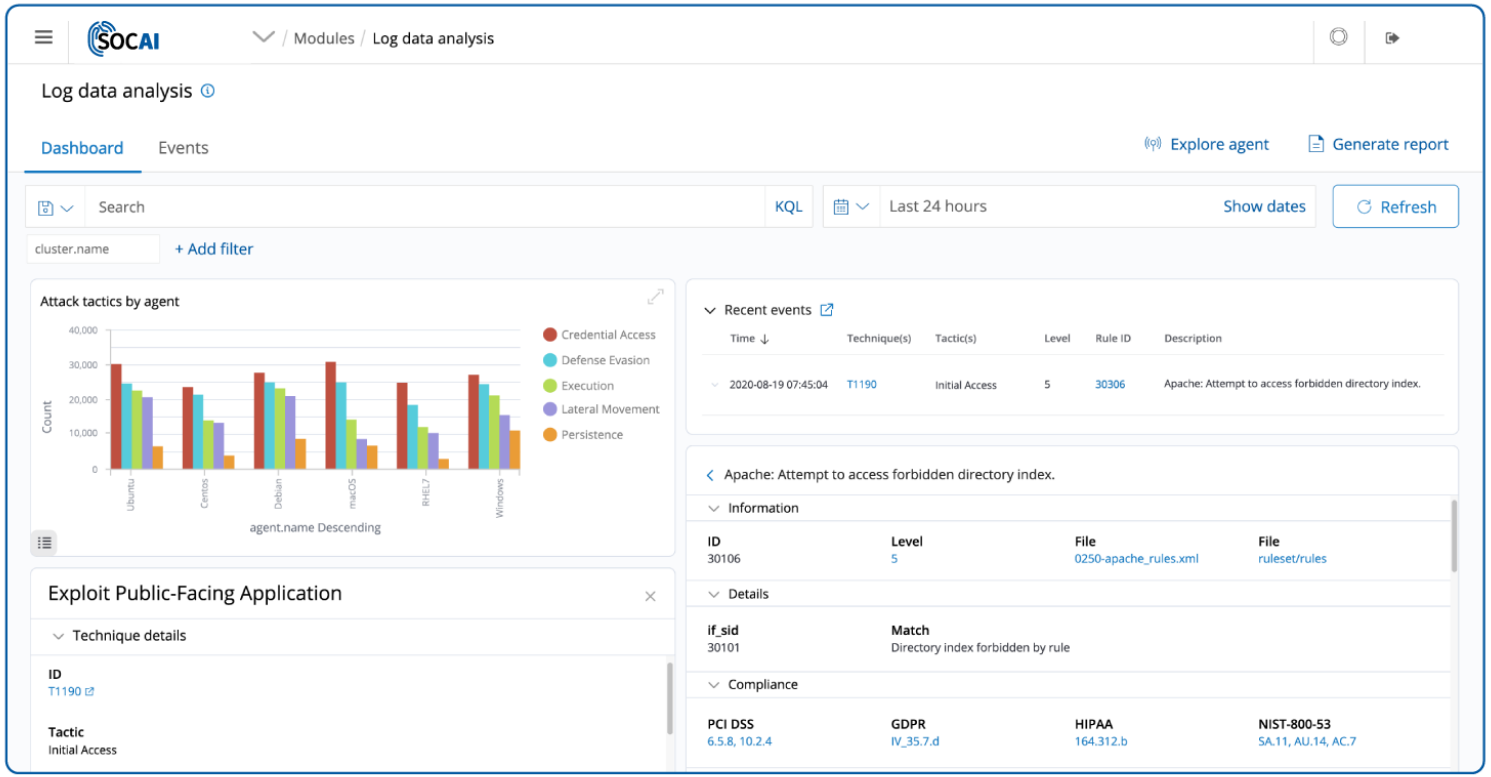


SOC-AI

Data analysis

SOC-AI performs a comprehensive analysis of the data obtained from the integrations to create a complete view of the organisation's assets.

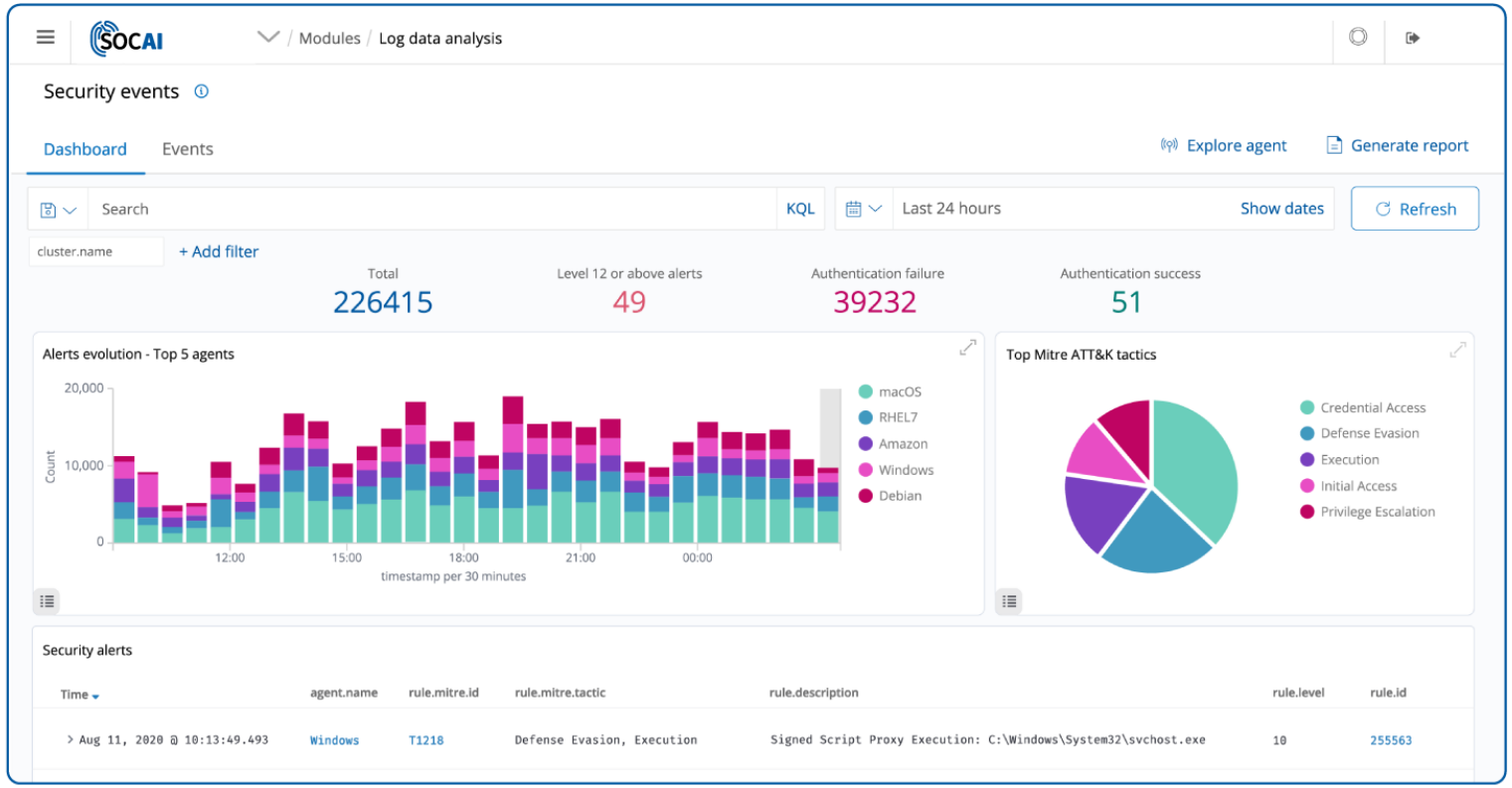
The screenshot shows an automatic study of the attacks detected in each asset.



SOC-AI

Threat detection

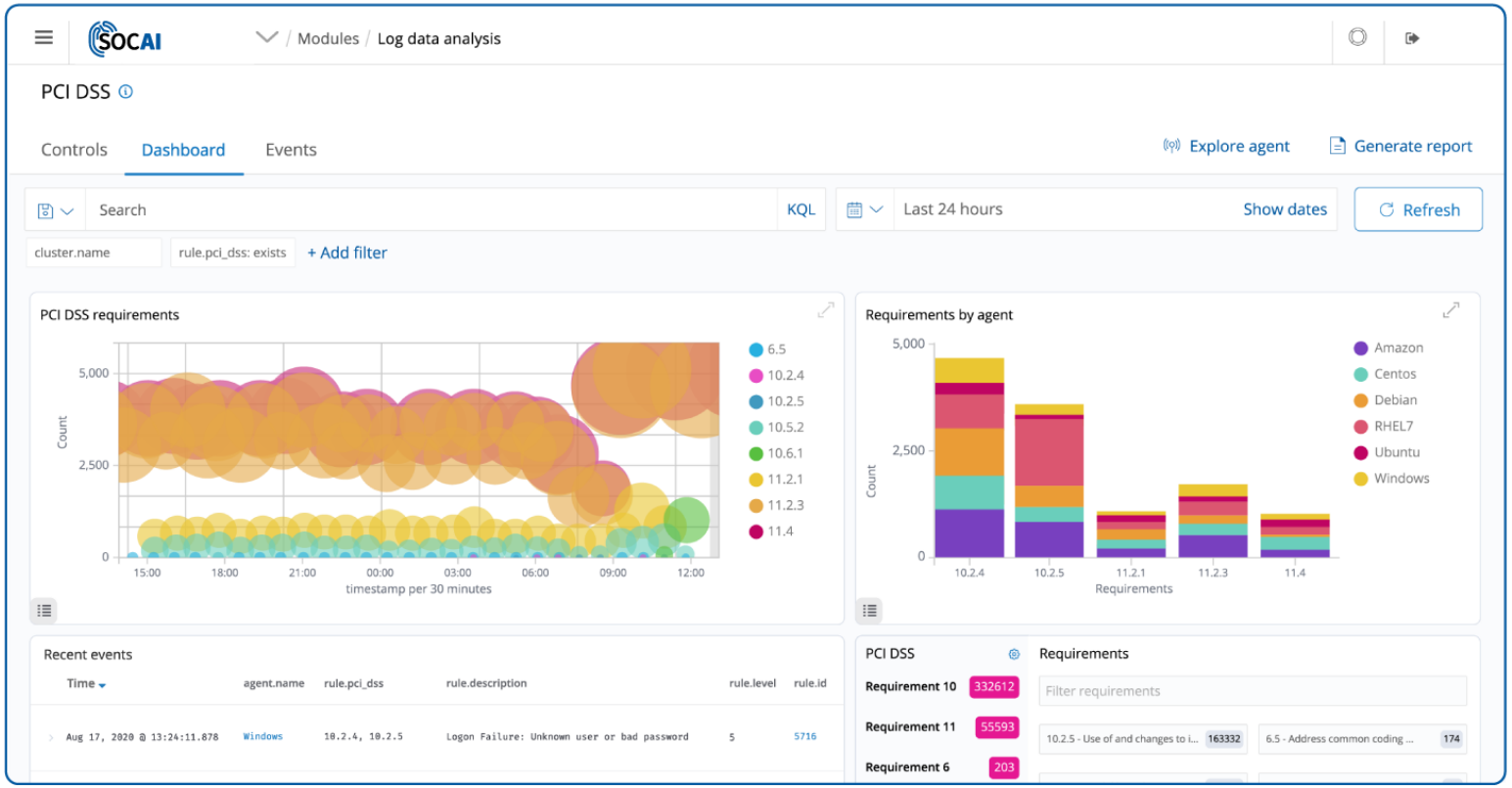
SOC-AI threat detection provides real-time protection against threats. Its detection algorithm is fast and effective, enabling an immediate response to any attack. In addition, it can associate detected threats with the vector according to mittre for better understanding and analysis of the threat.



SOC-AI

Threat response

SOC-AI has an automated response system with mitigation rules, detailed reporting and configurable alert systems. In addition, it has standard measurement systems to automatically assess compliance.



Recent incidents

94% of Spanish companies recognise that they have suffered a cybersecurity incident. In fact, in 2022, Spain ranked third in the world in terms of cyber-attacks.

Cyber-attack on the Clinic in Barcelona

On 5 March 2023, the Clínic received a ransomware attack, a method by which cybercriminals hijack particularly important data and demand a ransom to unlock access. The group of cybercriminals demanded that the Govern de Catalunya pay 4.5 million dollars to free the 4.4 terabytes of affected data, a demand that the authorities have rejected.

Cuatro gigabytes de información robada

Los cibercriminales del Clínic amenazan con publicar datos de pacientes con enfermedades infecciosas

Ransom House también amaga con hacer público el uso de medicamentos experimentales, como ya avanzó EL PERIÓDICO

- La investigación del ciberataque apunta al robo de ensayos del Clínic

Sanitarias del Hospital Clínic. / FERRAN NADEU

Recent incidents

94% of Spanish companies recognise that they have suffered a cybersecurity incident. In fact, in 2022, Spain ranked third in the world in terms of cyber-attacks.

Cyber-attack against MSI

MSI sufrió un ciberataque el día 7 de abril con el que se han robado 1,5 TB de datos y la empresa lanza una recomendación a los usuarios con estos equipos.

La compañía ha emitido un comunicado en el cual se detallan los hechos y se asegura que se está trabajando con las autoridades para investigar el asunto y minimizar los posibles daños que se hayan podido causar.

Recent incidents

94% of Spanish companies recognise that they have suffered a cybersecurity incident. In fact, in 2022, Spain ranked third in the world in terms of cyber-attacks.

Cyber-attack against Yoigo

On 4 April 2023 Yoigo acknowledged that it had been the victim of a cyber-attack. In this incident, third parties outside the organisation were said to have gained access to some of the personal data of the telephone company's users.

20BITS

Yoigo sufre un ataque informático: los ciberdelincuentes han tenido acceso a datos de sus clientes

EP / NOTICIA / 03.04.2023 - 16:36H

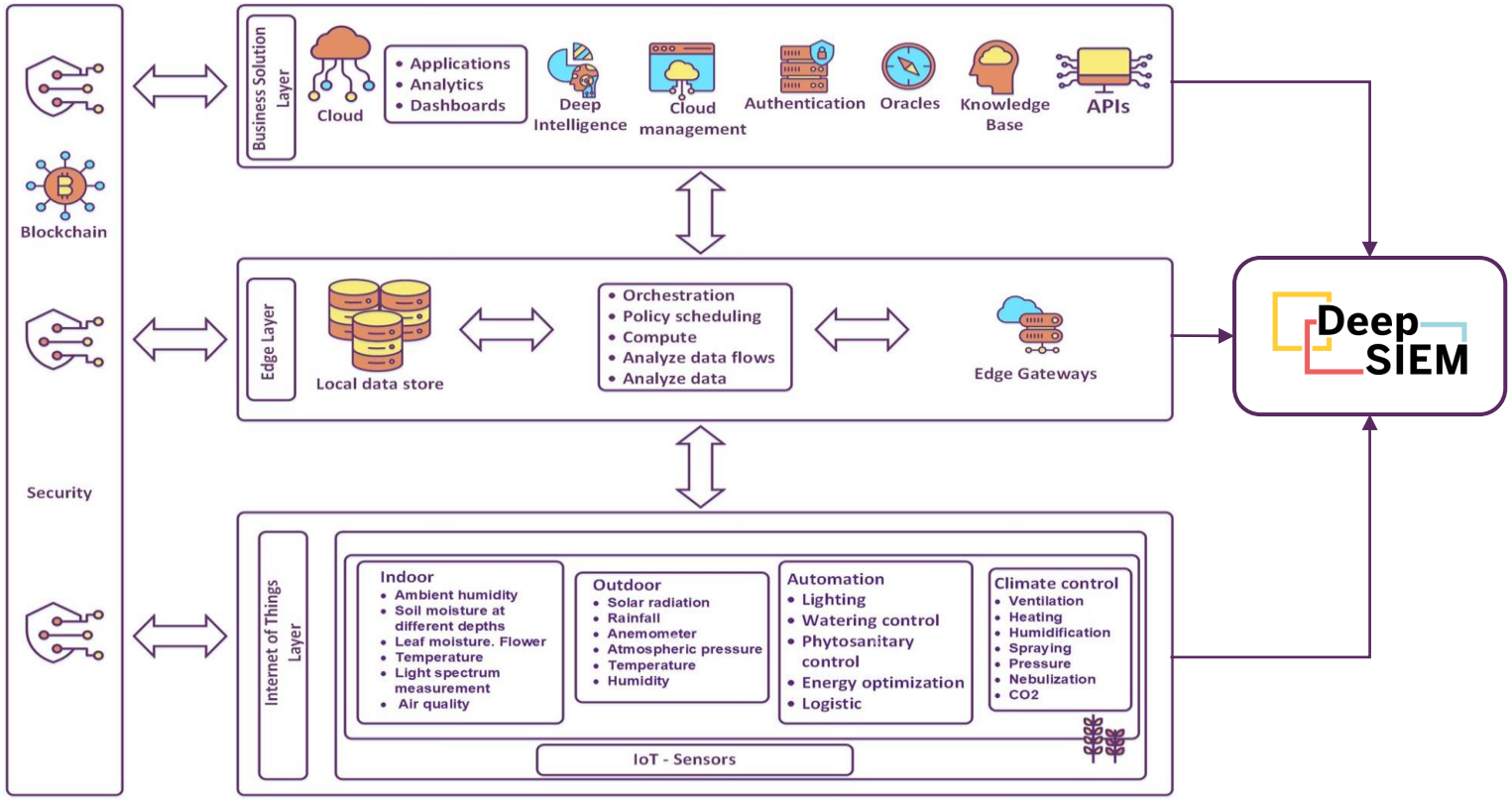
- La teleoperadora ha reconocido que ha sido víctima de un ciberataque este fin de semana y la información robada podría usarse en futuros delitos.
- Detectan una estafa que descarga malware en tu dispositivo simulando un proceso judicial
- La clave para no caer en ciberestafas esta Semana Santa: solo tienes que seguir este consejo

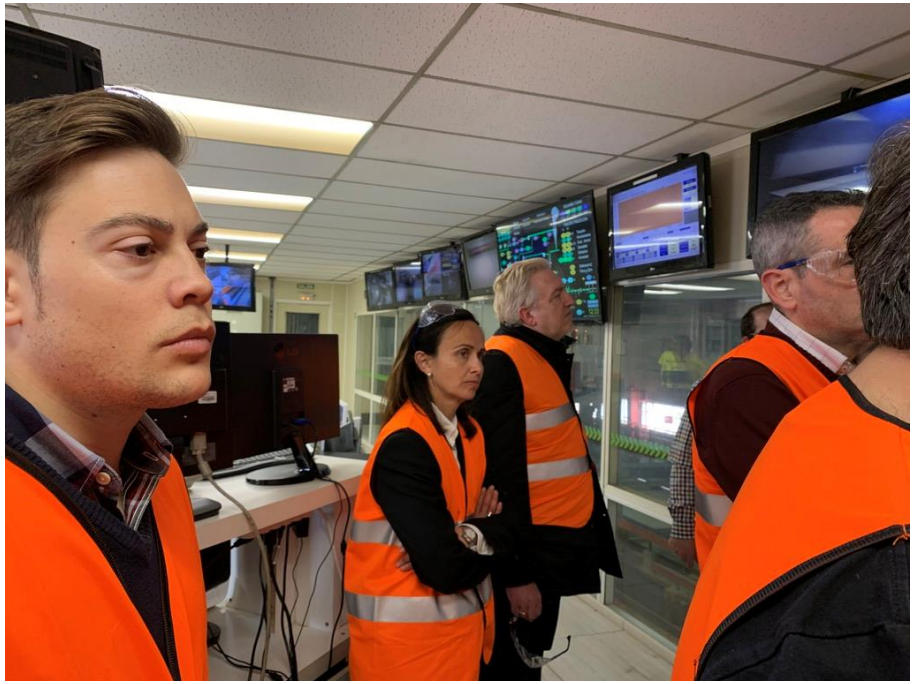
Los datos de algunos clientes de Yoigo se habrán visto comprometidos por el ciberataque. / rattanakun vía Canva.com / Yoigo / Montaje: 20BITS

20 MÁS INFORMACIÓN SOBRE:

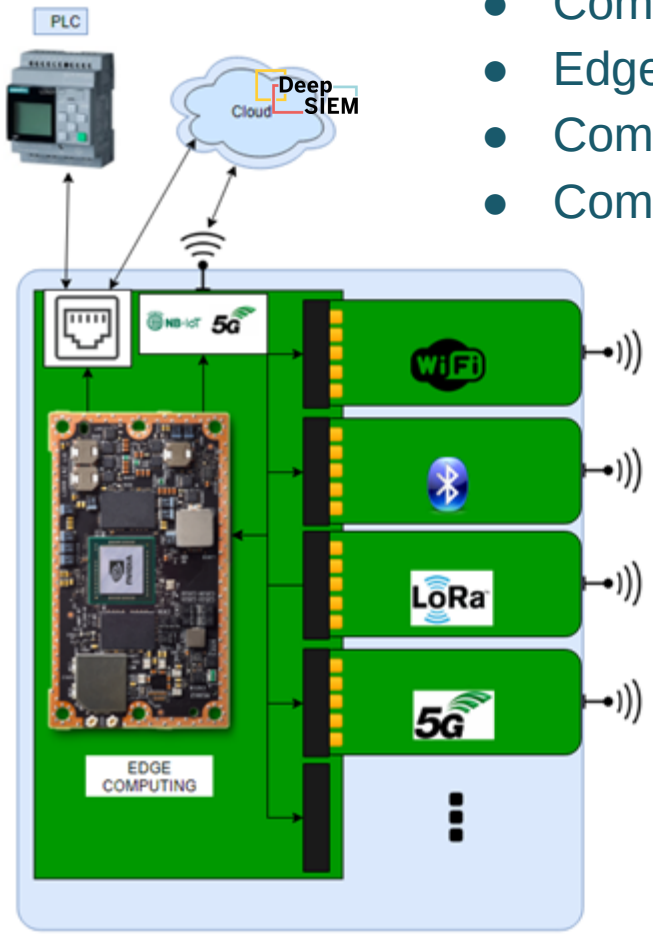
Yoigo | Phishing | Ciberseguridad | Ciberataque

Edge computing architecture for IoT

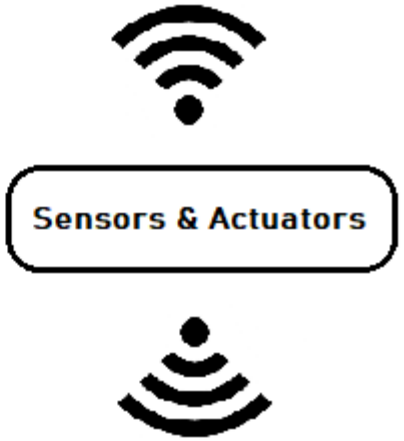




BISITE-PCB for EDGE computing

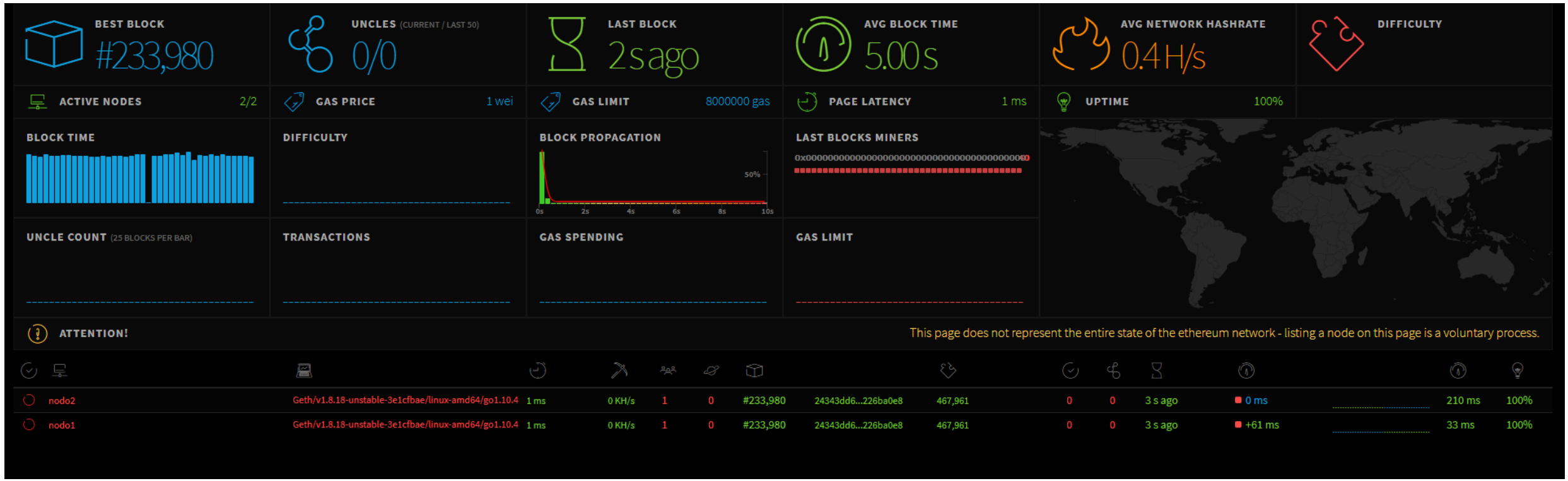


- Communication with sensors/actuators (WiFi, Bluetooth, LoRa...)
- Edge Computing with NVIDIA JETSON
- Communication with Cloud (Ethernet, 3G/4G, NB-IoT...)
- Communication with PLC (Ethernet/IP, ModBUS...)



Blockchain

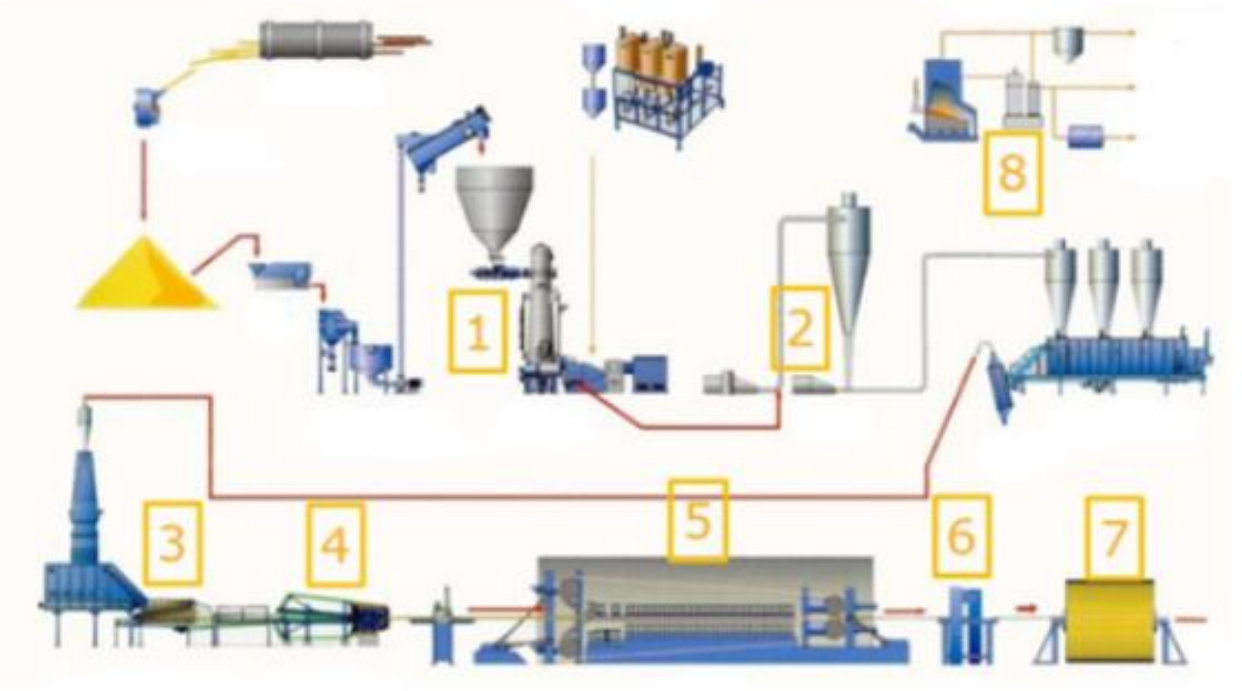
Compliance - trust - irrefutable proof - data integrity

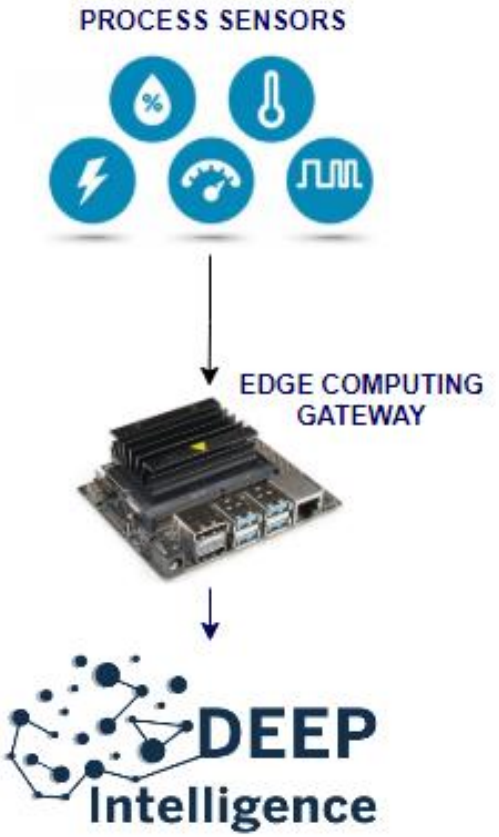


ADIF-RENFE

Int Gases is a sensorization project implemented in hangars. The main objective is to collect data on different pollutants from engine combustion, to be studied later using the intelligent tool Depp Intelillence.

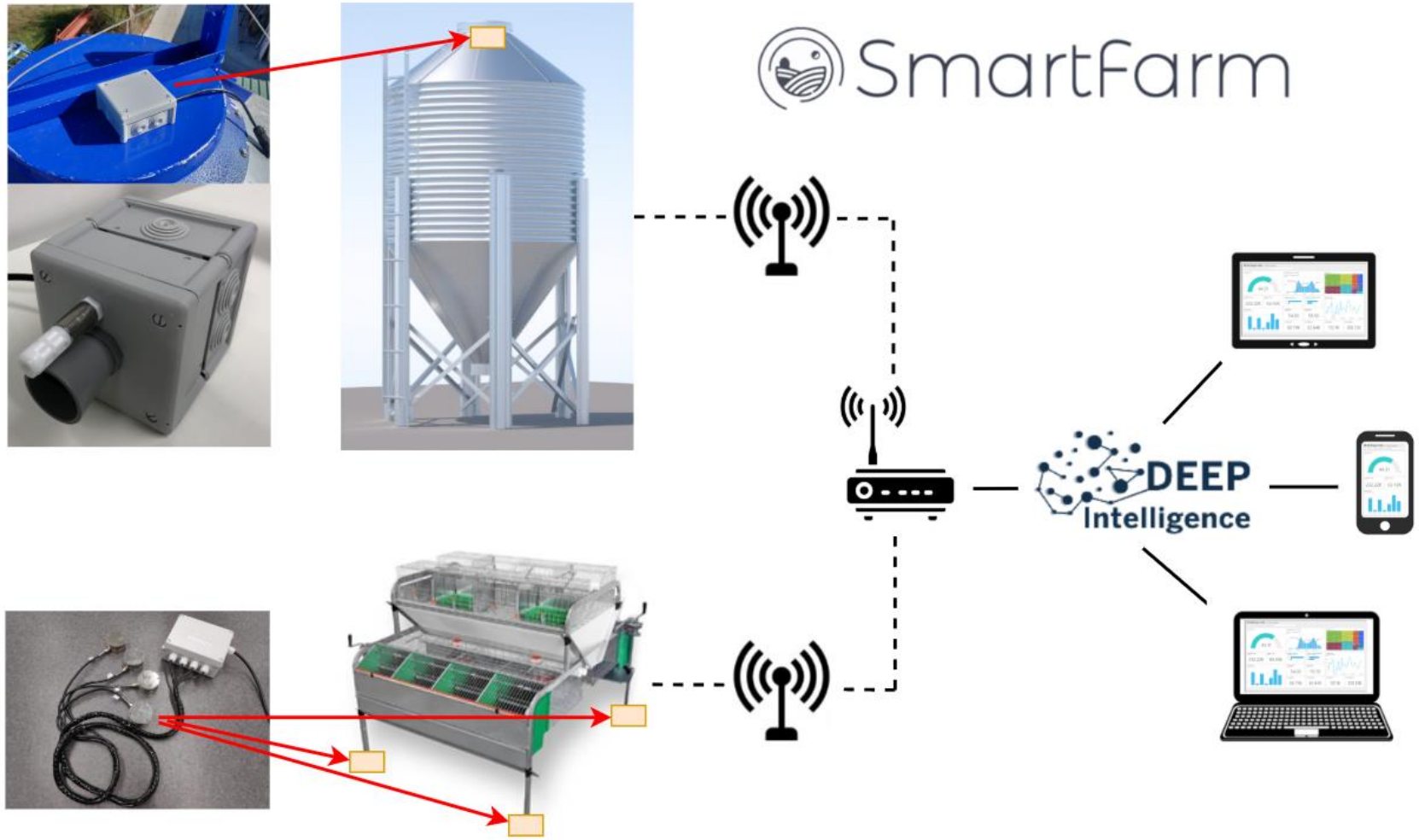
PLATINUM PROJECT



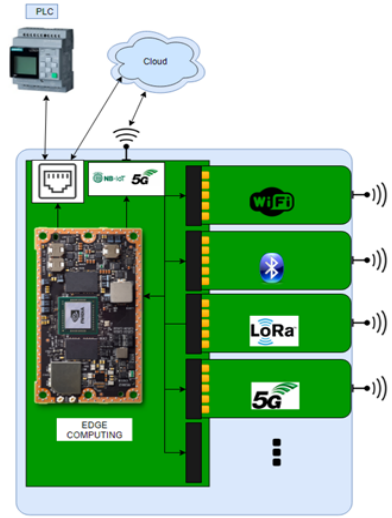


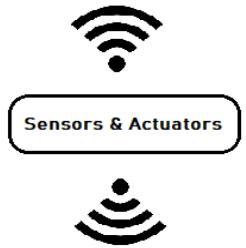
Industrial process variables monitoring for wood plank manufacturing to predict swelling and density parameters and predictive maintenance execution by using Edge Computing Processing and DEEP Intelligence.

SMARTFARM

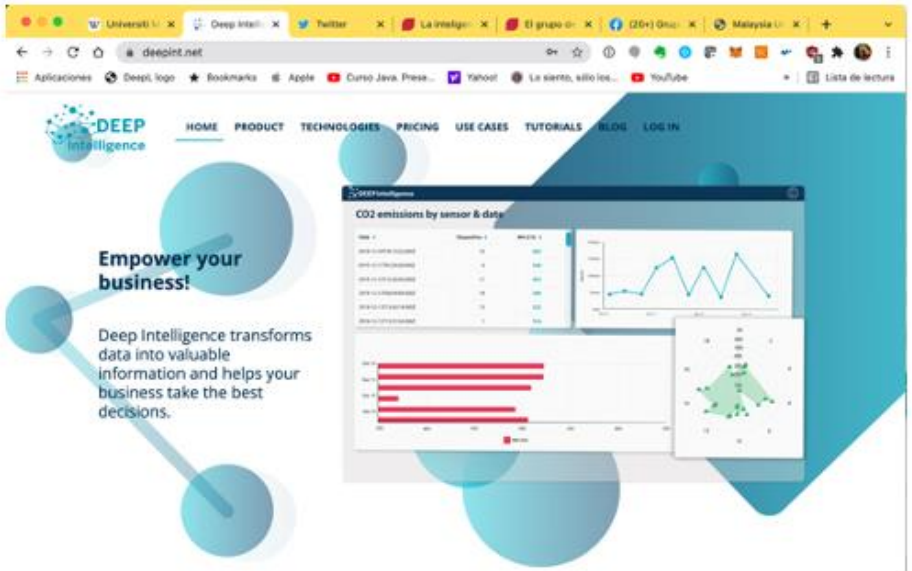


Automatic filling and weight level monitoring system for livestock farms.





BISITE / AIR Institute



AIR INSTITUTE

www.air-institute.com

competitividad empresarial ice | Junta de Castilla y León | Centr@Tec Servicios Avanzados de Innovación para Pymes