Diversity enhancements for Security Information and Event Management

Alysson Bessani

Ciências ULisboa

The DiSIEM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700692.

Outline

- Project Overview
- Technical Overview
- Project Outcomes

- Details about Components deployed on EDP
  - Multi-level risk management
  - OSINT Threat Detector

Project Overview

Horizon 2020 DiSIEM project

- **Work programme:** DS-04-2015 *"Digital Security: Cyber security, Privacy and Trust"*
- **Type of action:** Innovation Action
- **Budget:** €4M (EC contribution: €3.45M)
- **Consortium:**

FC Ciências ULisboa

CITY UNIVERSITY OF LONDON EST 1894

amadeus

edp

Fraunhofer IAIS

DigitalMR market research evolved

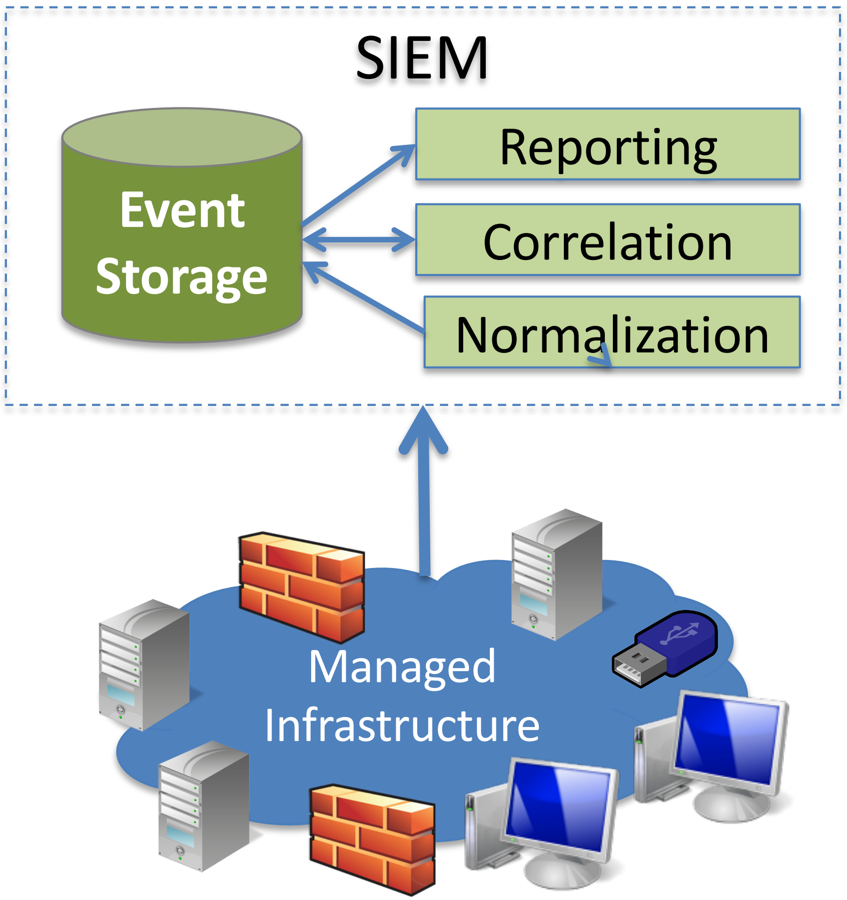
Atos

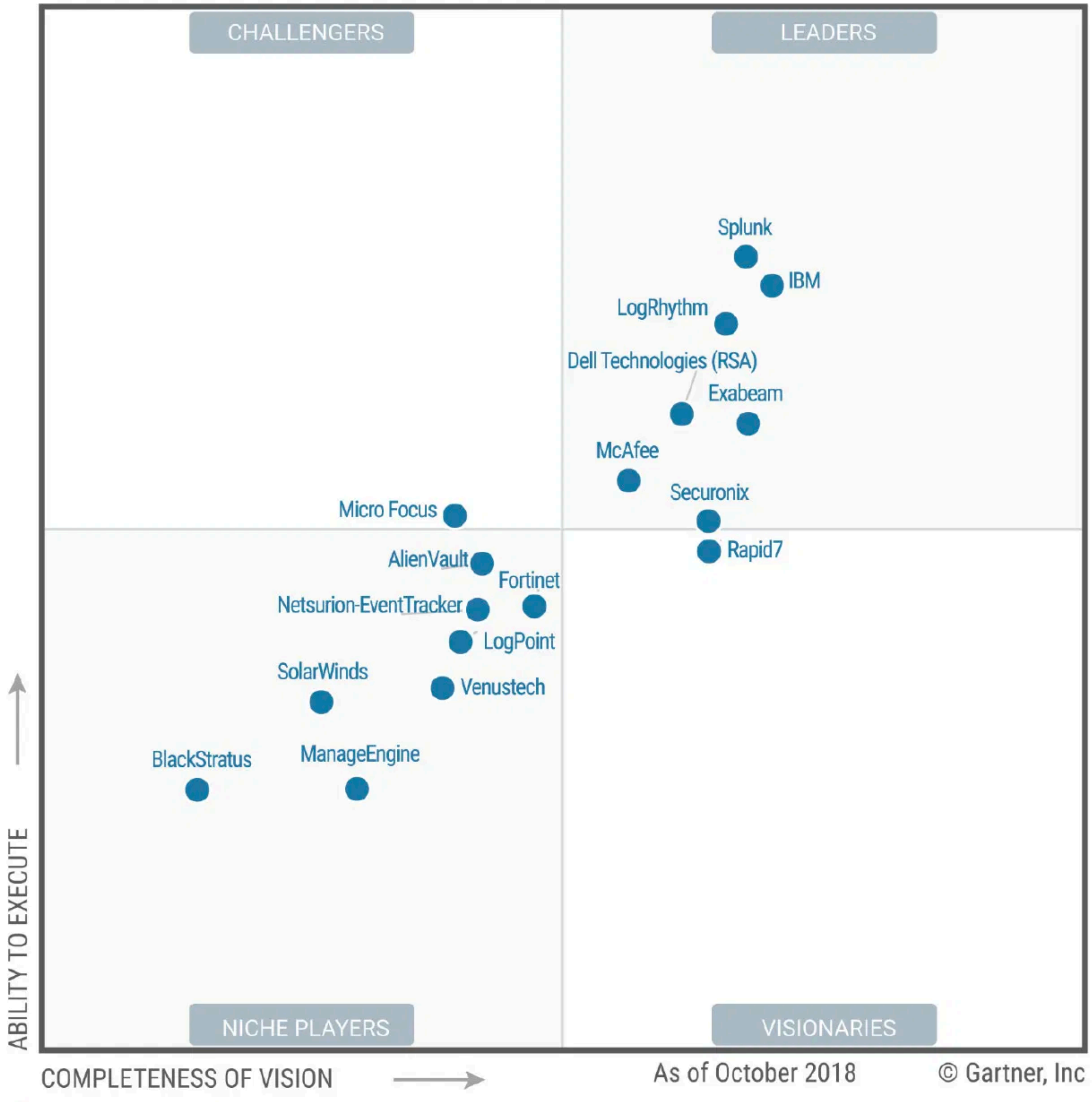
Security Information and Event Management (SIEM) Systems

- Security Operation Centres: monitor and manage security of organizations infrastructures

- SIEM Systems: distributed tools used to collect, analyse and report security events

- Reasons to deploy a SIEM
  - Compliance
  - Threat complexity





Source: Gartner (December 2018)

Gartner's Magic Quadrant for SIEM 2018

Size of the market in 2021: USD ~6 billion

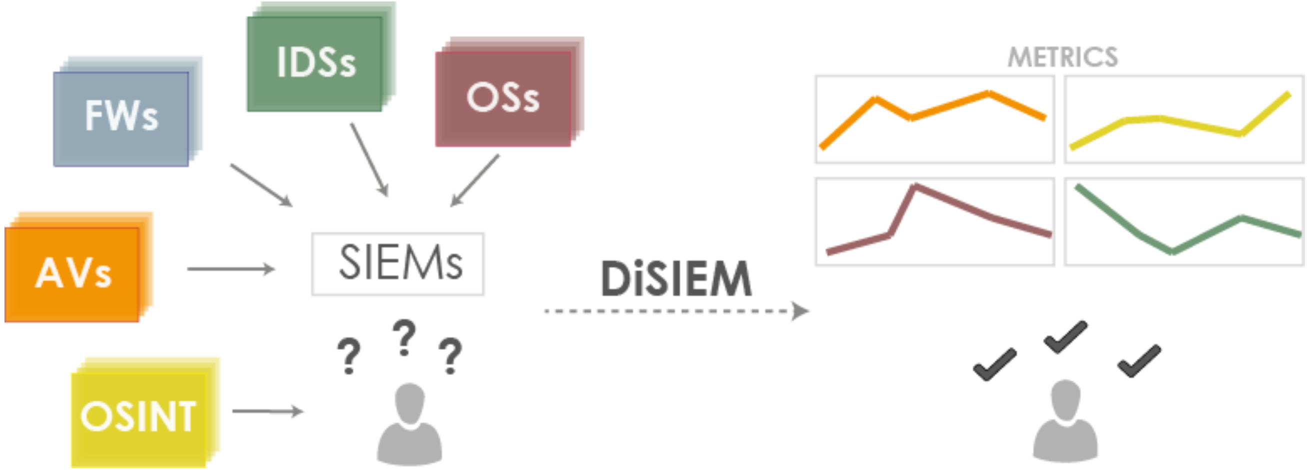
(increase of 12% until 2021)

Limitations of SIEM Systems

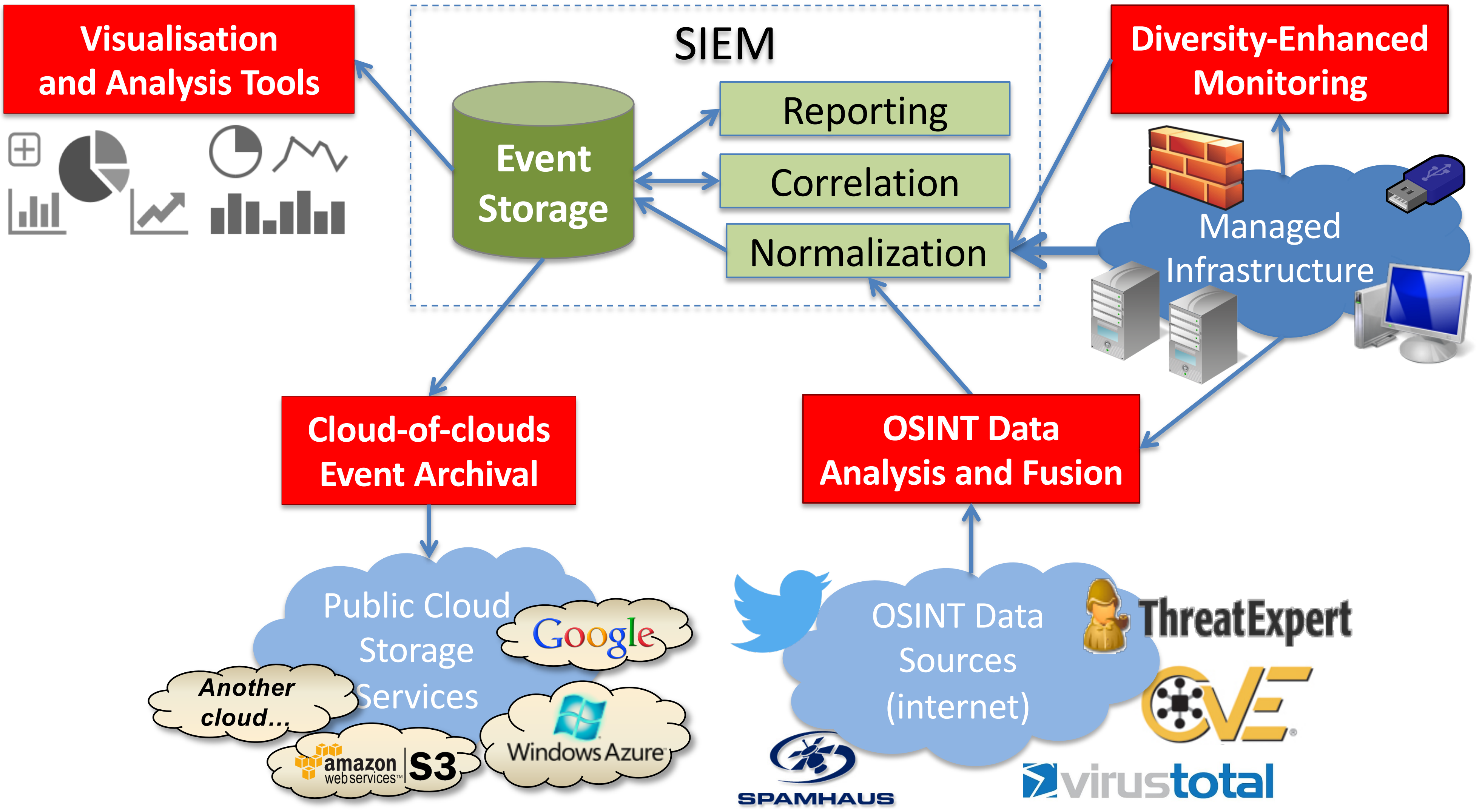
- **Threat intelligence** (i.e., capability of recognize and rank threats) capacity of SIEMs is still in its infancy
- SIEMs can show only “low level” data related with the received events, but they have little “intelligence” to process this data and extract **high-level information for C-level managers**
- Most data **visualisation techniques** in current SIEMs are rudimentary
- Event correlation capabilities of SIEMs are as good as the **quality of the events** fed to it
- SIEMs are incapable of **retaining collected events for a long time**

DiSIEM Objective

The project aimed to address these limitations by enhancing existing SIEMs with components for accessing **diverse** data sources, feeding enhanced events, and generating enhanced reports and metrics to better inform SOCs



Proposed Enhancements



Visualisation and Analysis Tools

SIEM

Event Storage

Reporting

Correlation

Normalization

Diversity-Enhanced Monitoring

Managed Infrastructure

Cloud-of-clouds Event Archival

OSINT Data Analysis and Fusion

Public Cloud Storage Services

Google

Another cloud...

amazon webservices™ S3

Windows Azure

OSINT Data Sources (internet)

ThreatExpert

CVE

SPAMHAUS

virustotal

Extending SIEMs

- Deploying a SIEM has a very high cost
- It is not feasible to change existing deployments
- Existing systems support **extensions**
  - New connectors for feeding events to the system
  - Stored events can be fetched from the system
  - New reports/dashboards can be created on the UI
- Independent side systems can be deployed

ArcSight

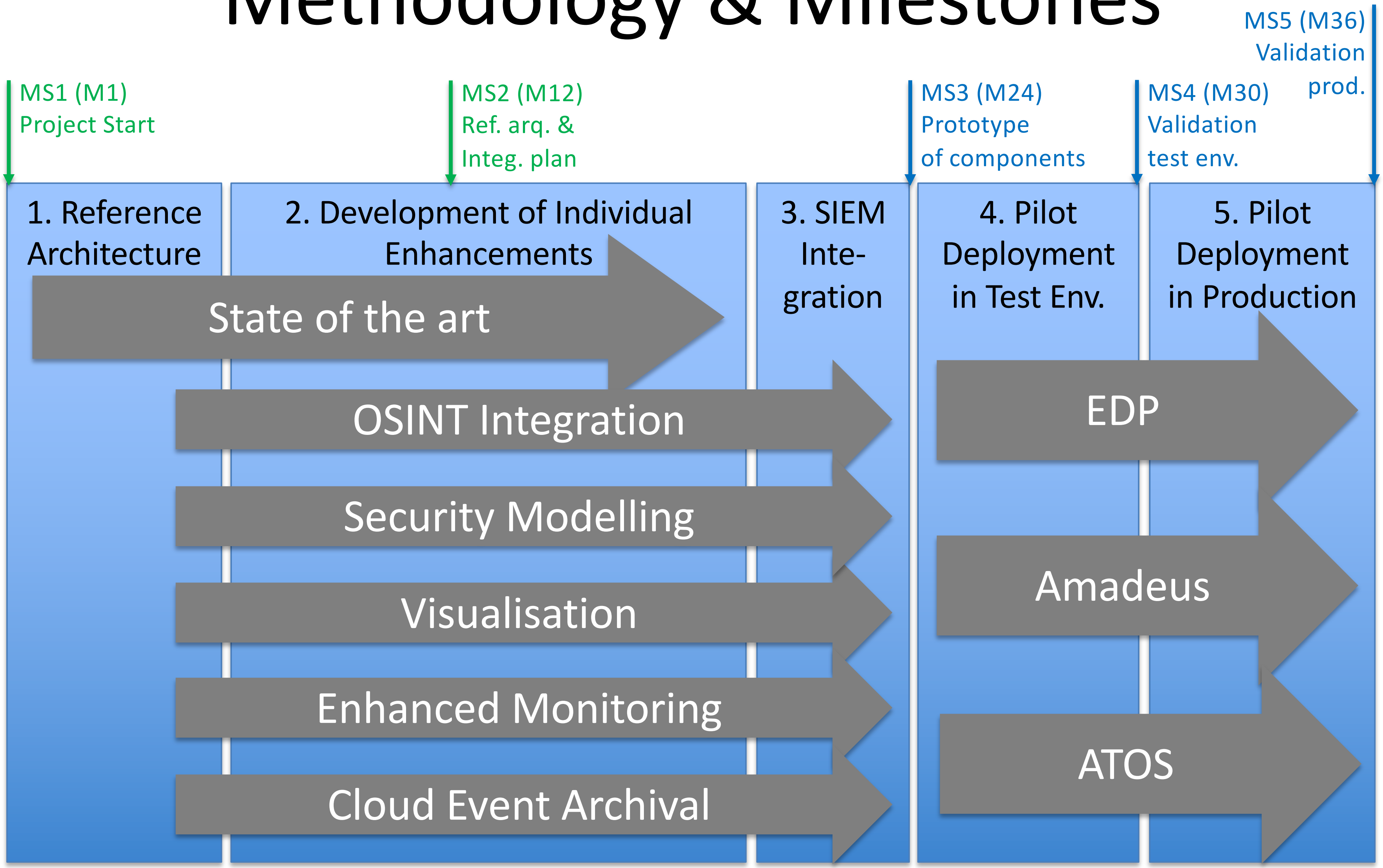
XL-SIEM

elastic

ALIEN VAULT OSSIM

splunk>

Methodology & Milestones



MS1 (M1)
Project Start

MS2 (M12)
Ref. arq. &
Integ. plan

MS3 (M24)
Prototype
of components

MS4 (M30)
Validation
test env.

MS5 (M36)
Validation
prod.

1. Reference Architecture

2. Development of Individual Enhancements

3. SIEM Integration

4. Pilot Deployment in Test Env.

5. Pilot Deployment in Production

State of the art

OSINT Integration

Security Modelling

Visualisation

Enhanced Monitoring

Cloud Event Archival

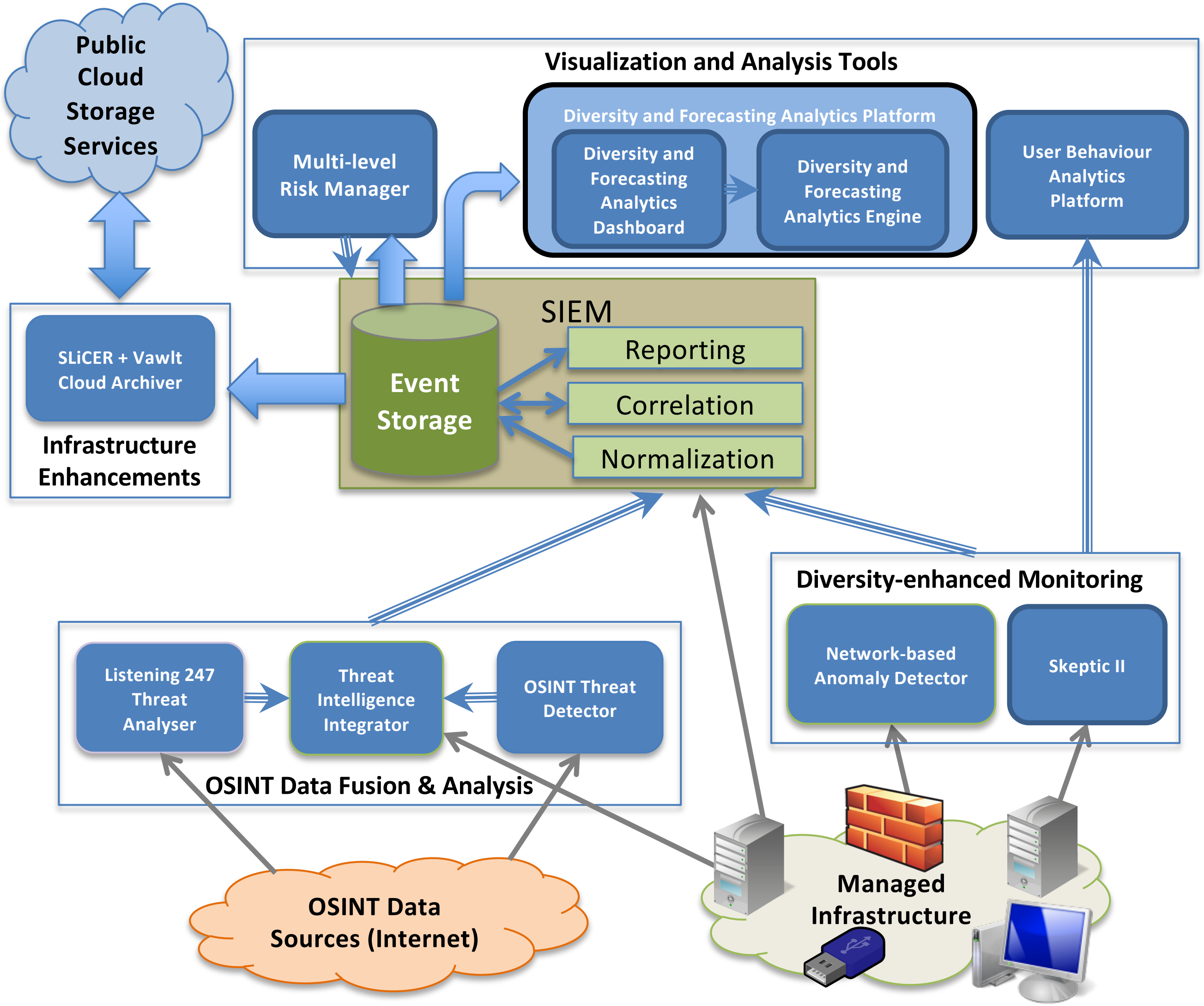
EDP

Amadeus

ATOS

Technical Overview

Reference Architecture



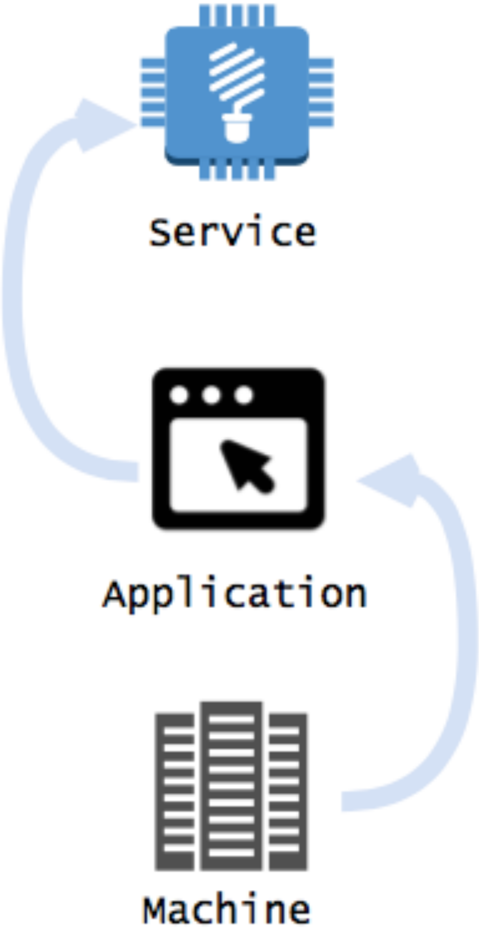
Public Cloud Storage Services
Visualization and Analysis Tools
Multi-level Risk Manager
Diversity and Forecasting Analytics Platform
Diversity and Forecasting Analytics Dashboard
Diversity and Forecasting Analytics Engine
User Behaviour Analytics Platform
SLiCER + Vawlt Cloud Archiver
Infrastructure Enhancements
SIEM
Event Storage
Reporting
Correlation
Normalization
Diversity-enhanced Monitoring
Network-based Anomaly Detector
Skeptic II
Listening 247 Threat Analyser
Threat Intelligence Integrator
OSINT Threat Detector
OSINT Data Fusion & Analysis
OSINT Data Sources (Internet)
Managed Infrastructure

WP3 – Security and Risk Modelling

- Objectives
  - Define security metrics to assess characteristics of interest for security decision making
  - Apply quantitative, probabilistic methods to support decisions on how best to combine multiple defences given a threat environment

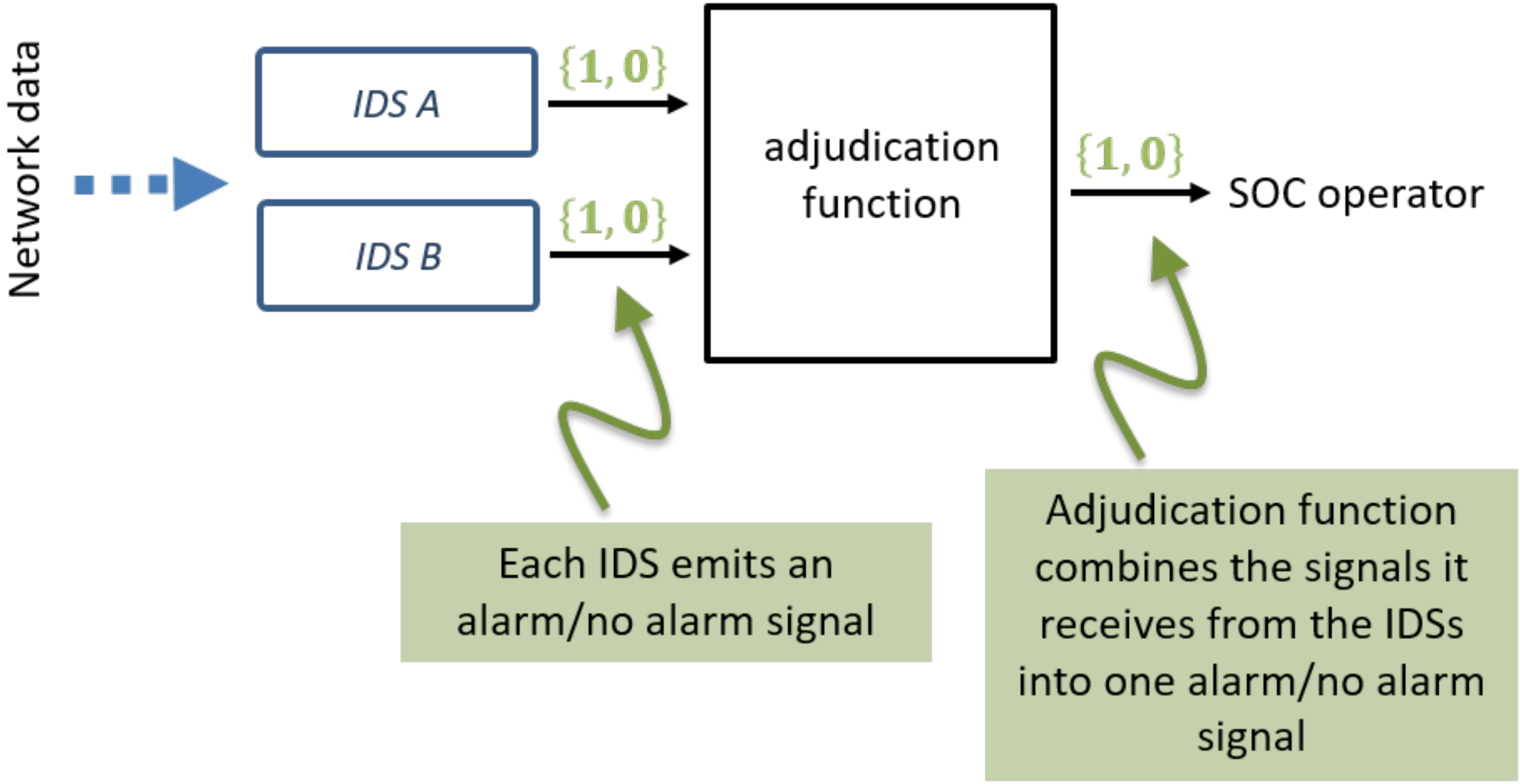
Multi-level Risk Model

- Which considers:
  - A hierarchy of three layers of assets
  - Dependencies and risk spreading
    - Interlayer (applications from hosts, services from applications)
    - Intra-layer (applications and hosts)
  - Risk is scored per asset bottom-up, considering **dependencies**, **vulnerabilities**, and **incidents**



Strategies for Optimal Adjudication

An adjudication function in operation



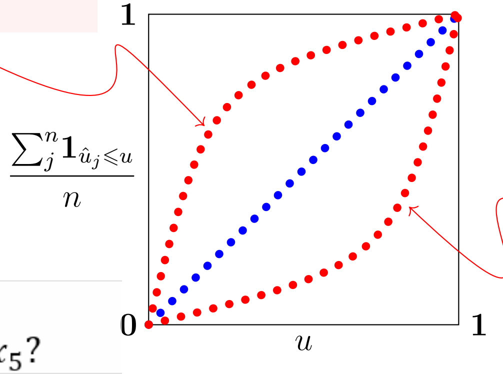
Each IDS emits an alarm/no alarm signal

Adjudication function combines the signals it receives from the IDSs into one alarm/no alarm signal

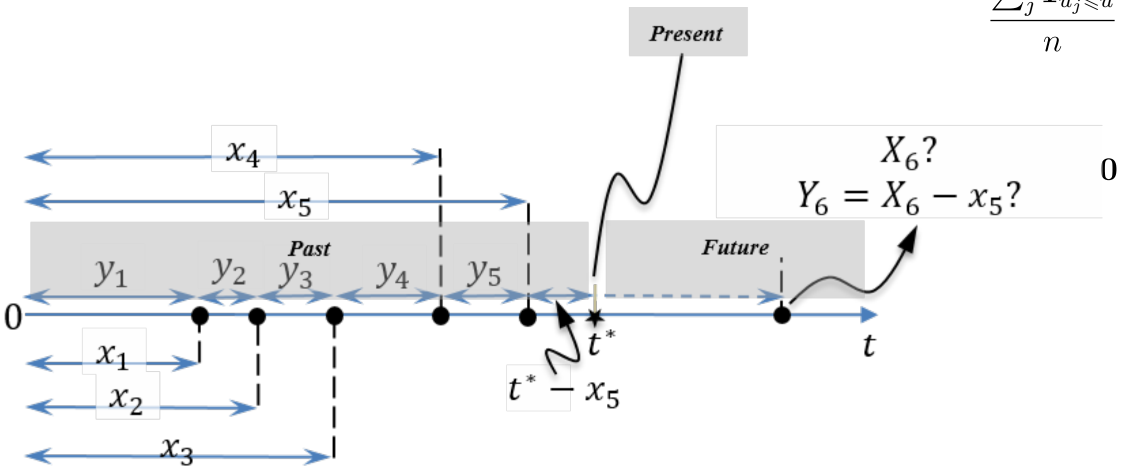
Forecasting Security Risks

- Statistical models for, based on past events, forecast the probability of cybersecurity events in the future

forecasted times are less likely than they should be



forecasted times are more likely than they should be

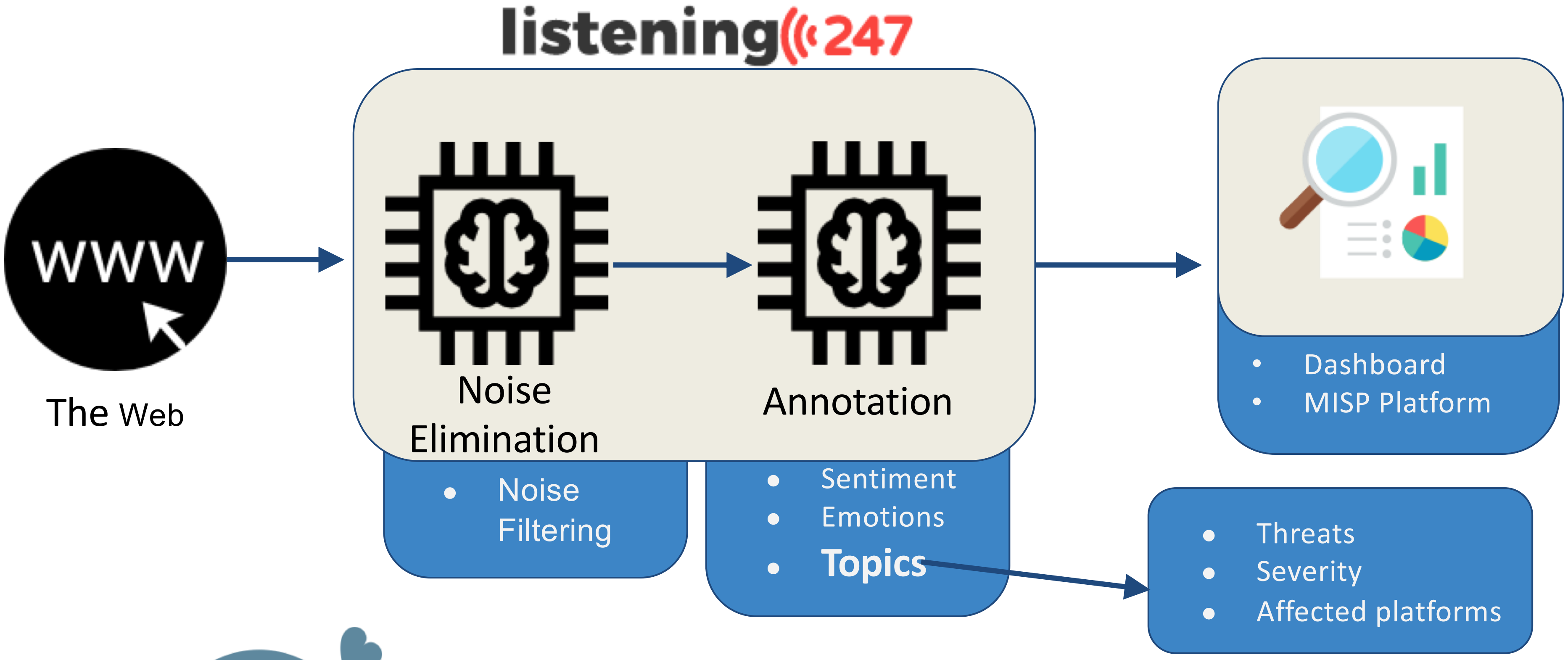


$$x_1 < x_2 < x_3 < x_4 < x_5 < t^* < X_6, X_7, X_8, \ldots$$

WP4 – OSINT Data Fusion and Analysis

- Objectives
  - Fetching and analyzing OSINT data
  - Identify trends that could anticipate threats to an organization
  - Integrate relevant OSINT in the SIEM context

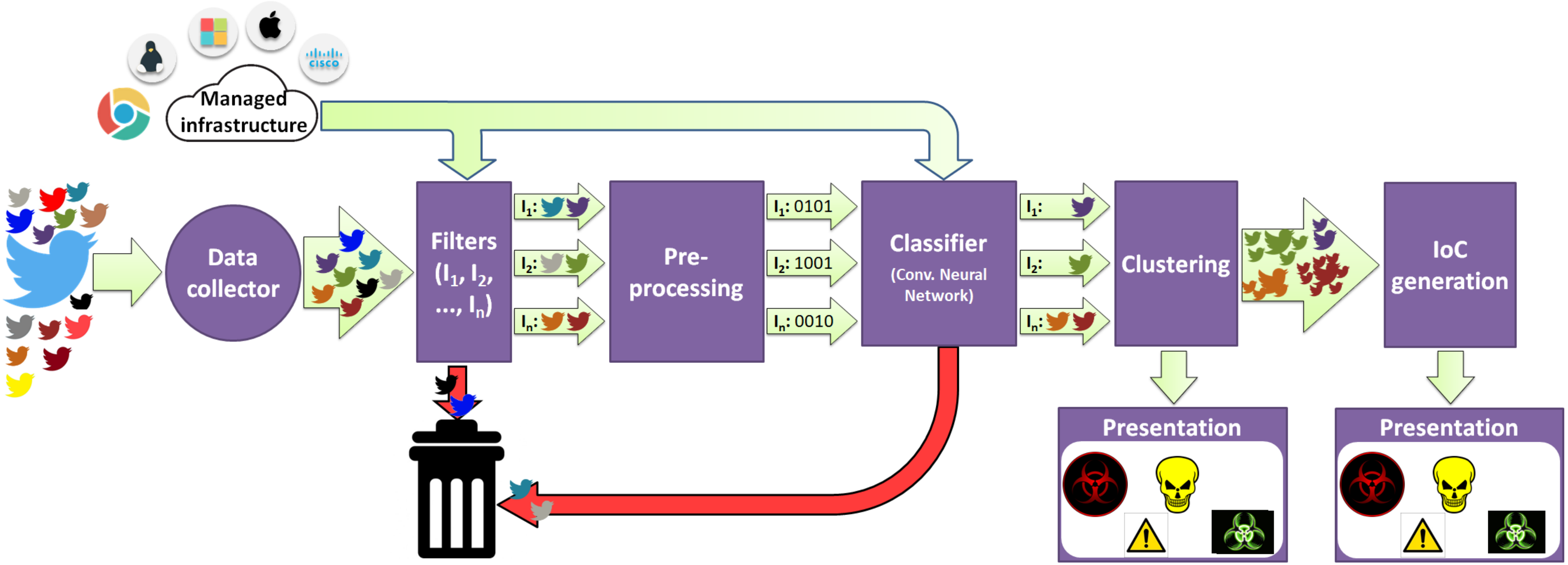
DigitalMR’ listening247 Threat Analyser



Goal: Use ML and NLP Pipeline for threat detection

OSINT Threat Detector

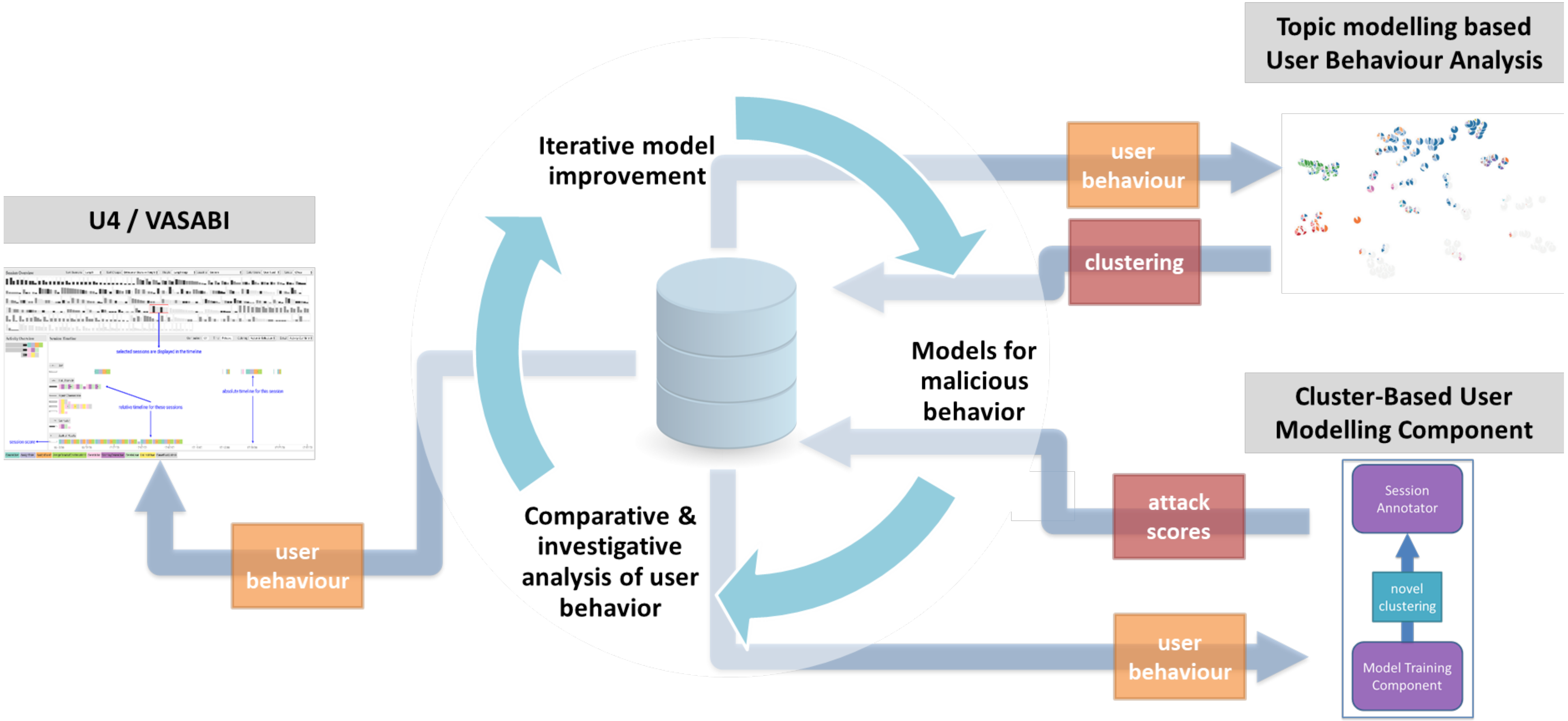
- End-to-end processing pipeline from Twitter accounts to Indicators of Compromise (IoC)
  - Filtering, Classifying, Grouping, Knowledge extraction



WP5 – Visual Analysis Platform

- Objectives
  - Develop data visualisation techniques for supporting security analysts’ decision making
  - Harmonise different data sources
  - Combine visual and computational methods for enhanced data analysis and modelling
  - Eventually support decision-making using such diverse data within SIEMs

User Behaviour Analytics Platform



Topic modelling based User Behaviour Analysis

U4 / VASABI

Iterative model improvement

user behaviour

clustering

Models for malicious behavior

Cluster-Based User Modelling Component

Session Annotator

novel clustering

Model Training Component

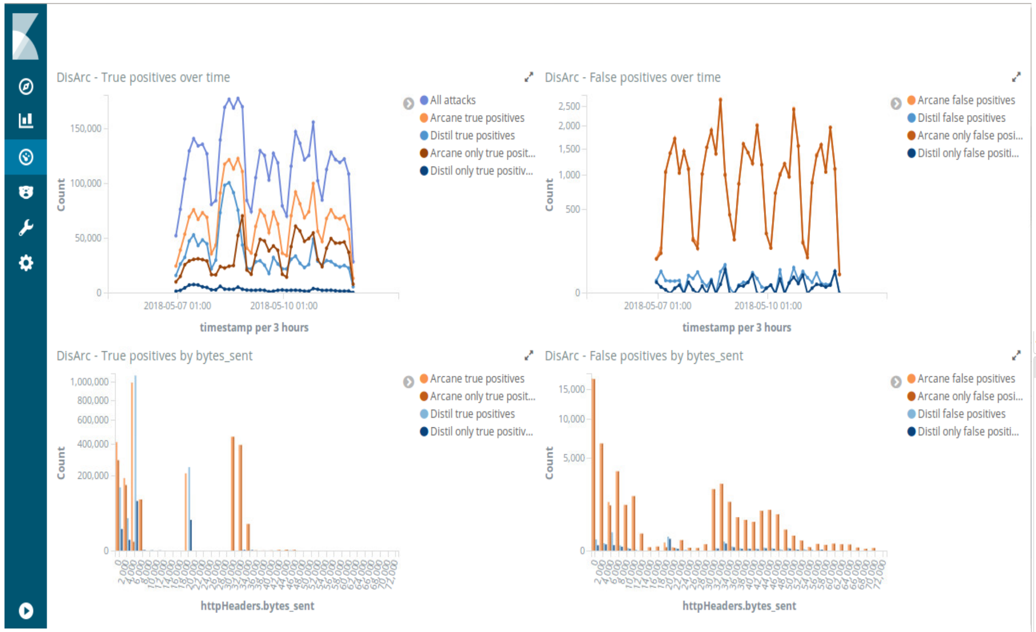
attack scores

Comparative & investigative analysis of user behavior

user behaviour

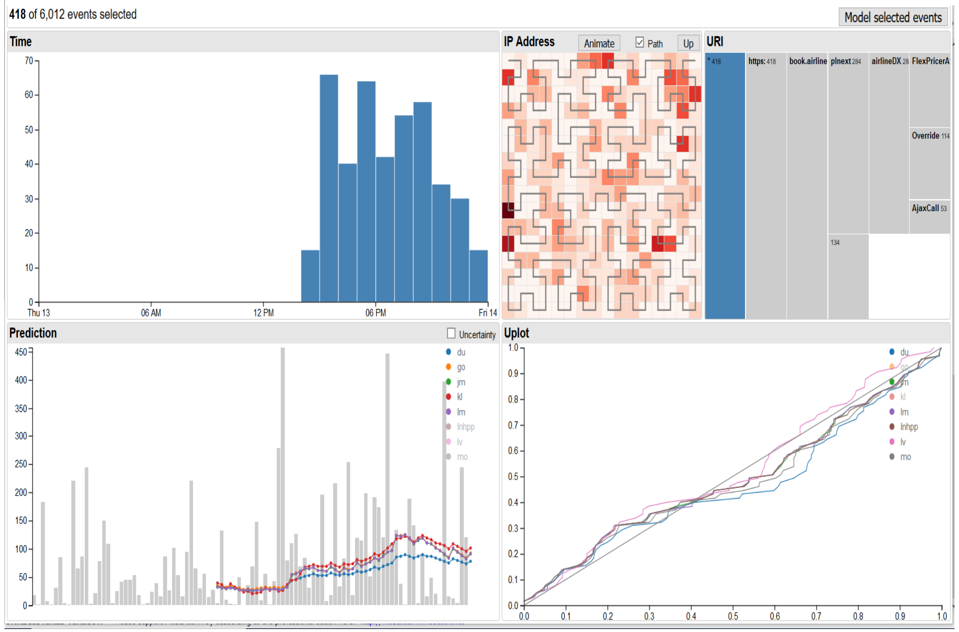
user behaviour

Diversity & Forecasting Analytics Platform



Optimal Adjudication

Forecasting Security Events

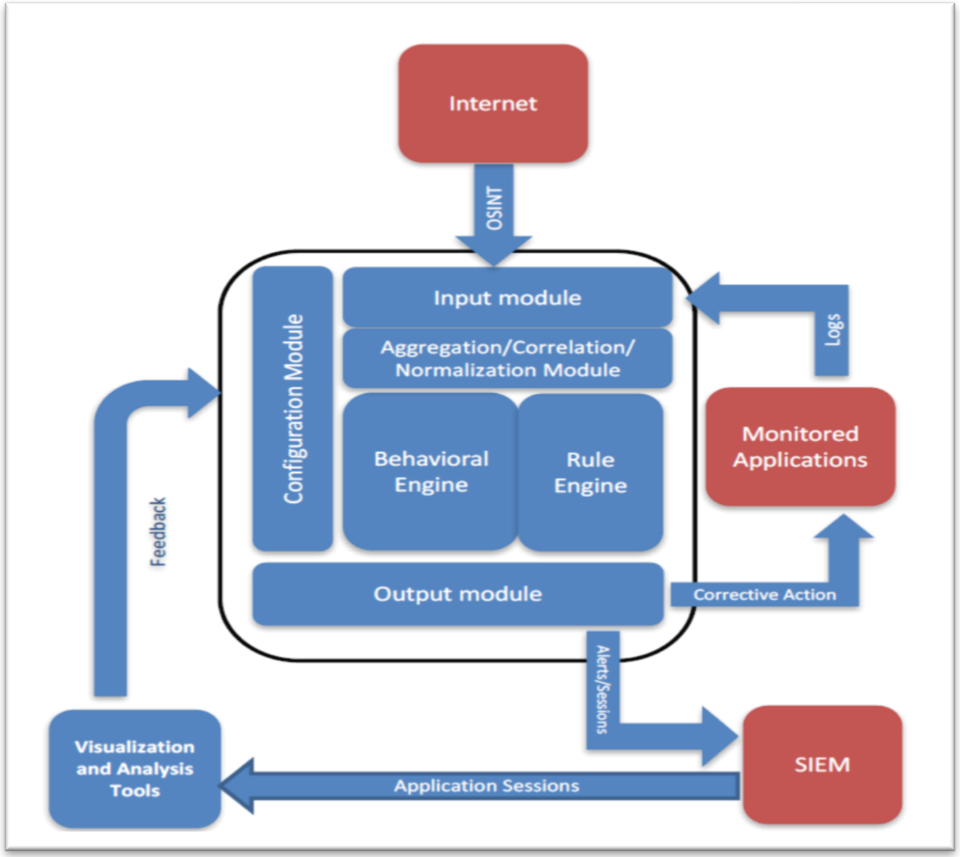

418 of 6,012 events selected

WP6 – Infrastructure Enhancements

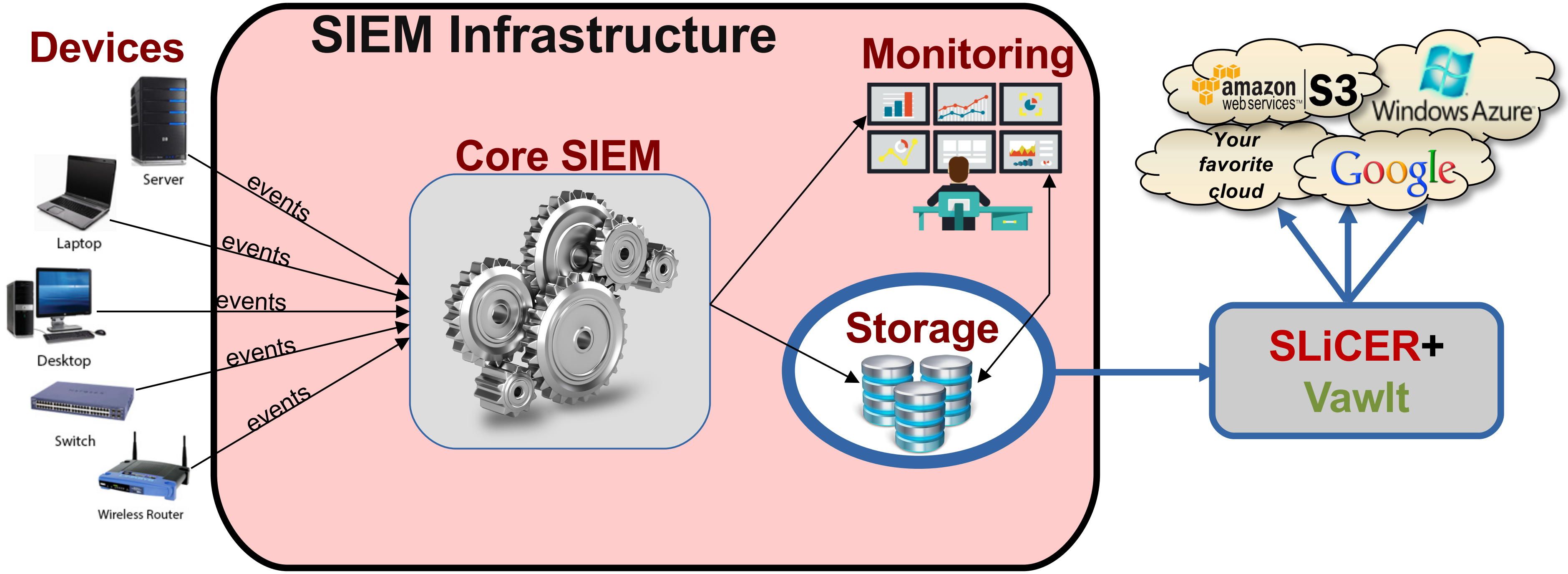
- Objectives
  - Integrate behavioral anomaly detectors (UEBA) for business-critical applications
  - Enhanced sensors and monitoring tools that leverage diversity
  - Develop security analytics tools to improve decision-making
  - Enhance storage capabilities

WP6 – Skeptic II

- A user-centric application anomaly detector
- Enhances application security by leveraging **User Behavioral Analytics** to monitor application user activities
- Allows SIEM operators to focus on distilled application alerts instead of sifting through application audit events



WP6 – SLiCER/Vawlt



SLiCER	Storing, indexing & query events (small files)
Vawlt	Dependable & secure cloud-of-clouds storage

Project Outcomes

Main Results of the Project

- As an Innovation Action, a great effort was made to build high-TRL components

DiSIEM Component	Initial TRL	Final TRL
Listening 247 Threat Analyser	2	6
OSINT Threat Detector	2	7
Threat Intelligence Integrator	2	6
Network-based Anomaly Detector	2	5
Skeptic II	3	8
User Behaviour Analytics Platform	2	7
Diversity & Forecasting Analytics Platform	2	7
Multi-level Risk Manager	2	8
SLiCER/Vawlt	2/5	5/8

Main Results of the Project

- Several components built in the project are deployed in production and will continue to be used after the project ends

DiSIEM Component	Amadeus	Atos	EDP	Other
Listening 247 Threat Analyser	Production	Lab	Production	
OSINT Threat Detector	Production	Lab	Production	CS-AWARE
Threat Intelligence Integrator	Production	Lab	Production	
Network-based Anomaly Detector	-	Lab	-	
Skeptic II	Production	-	-	
User Behaviour Analytics Platform	Production	-	-	
Diversity & Forecasting Analytics Platform	Production	Lab	-	
Multi-level Risk Manager	-	-	Production	
SLiCER/Vawlt	-	Lab	Test	FCUL

OSINT

APP. MONITORING

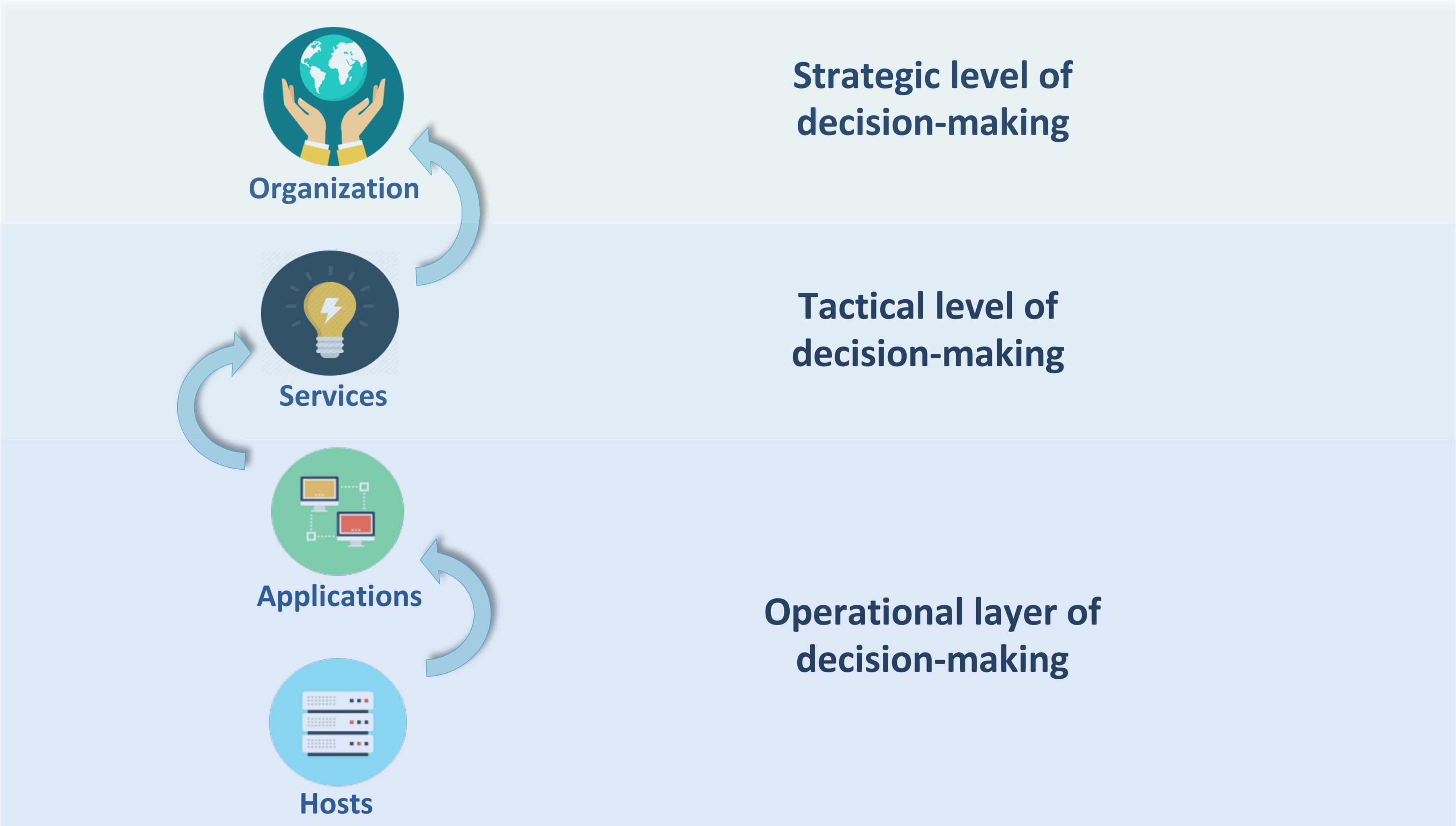
Main Results of the Project

- New business leads
  - Potential joint exploitation between ATOS, DigitalMR, and FCiências.ID
  - DigitalMR’ OSINT thread prediction as a standalone commercial solution in the Listening 247 brand
  - Significant financial impact in the pilot partners SOCs
  - A start-up (Vawlt) was created to exploit one of the components developed in the project
    - Secured 0,5M euros of pre-seed funding from Armilar
    - Currently employing 5 persons (3 worked on DiSIEM)
- 41 papers were published, several of them on prestigious journals and conferences
- Open-source software to boost research impact

Details about components deployed on EDP

Multi-Level Risk Manager

Multi-level Risk Manager: Model

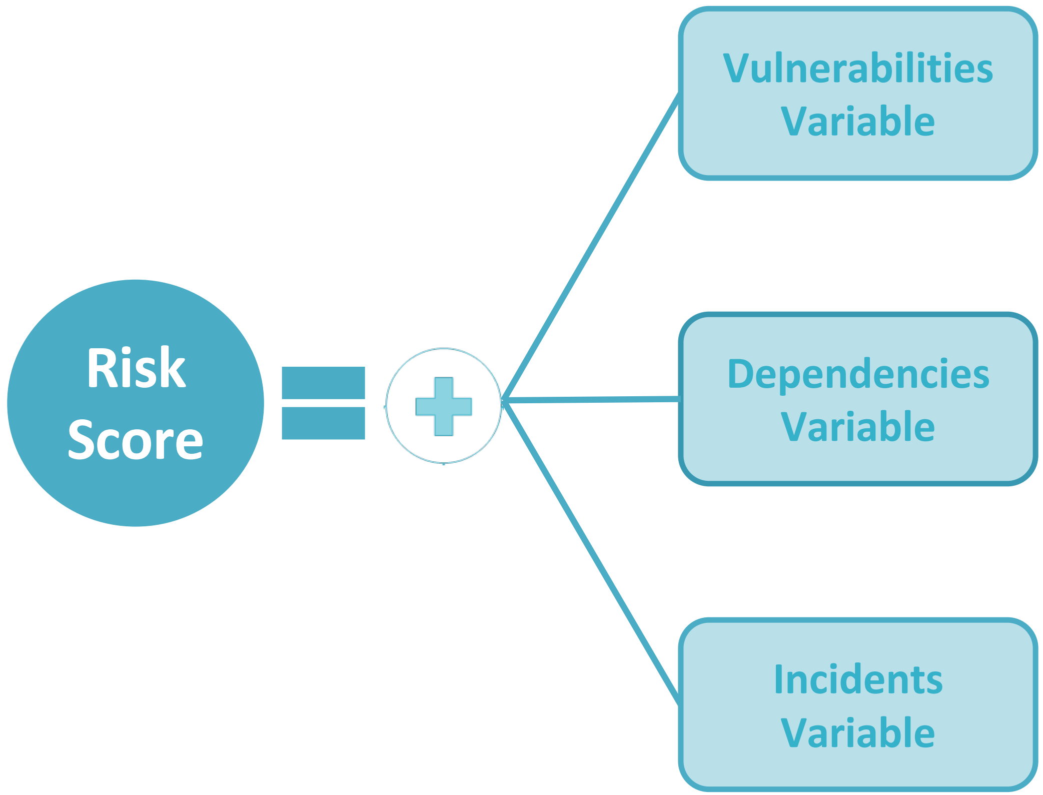


Strategic level of decision-making

Tactical level of decision-making

Operational layer of decision-making

Multi-level Risk Manager: Variables

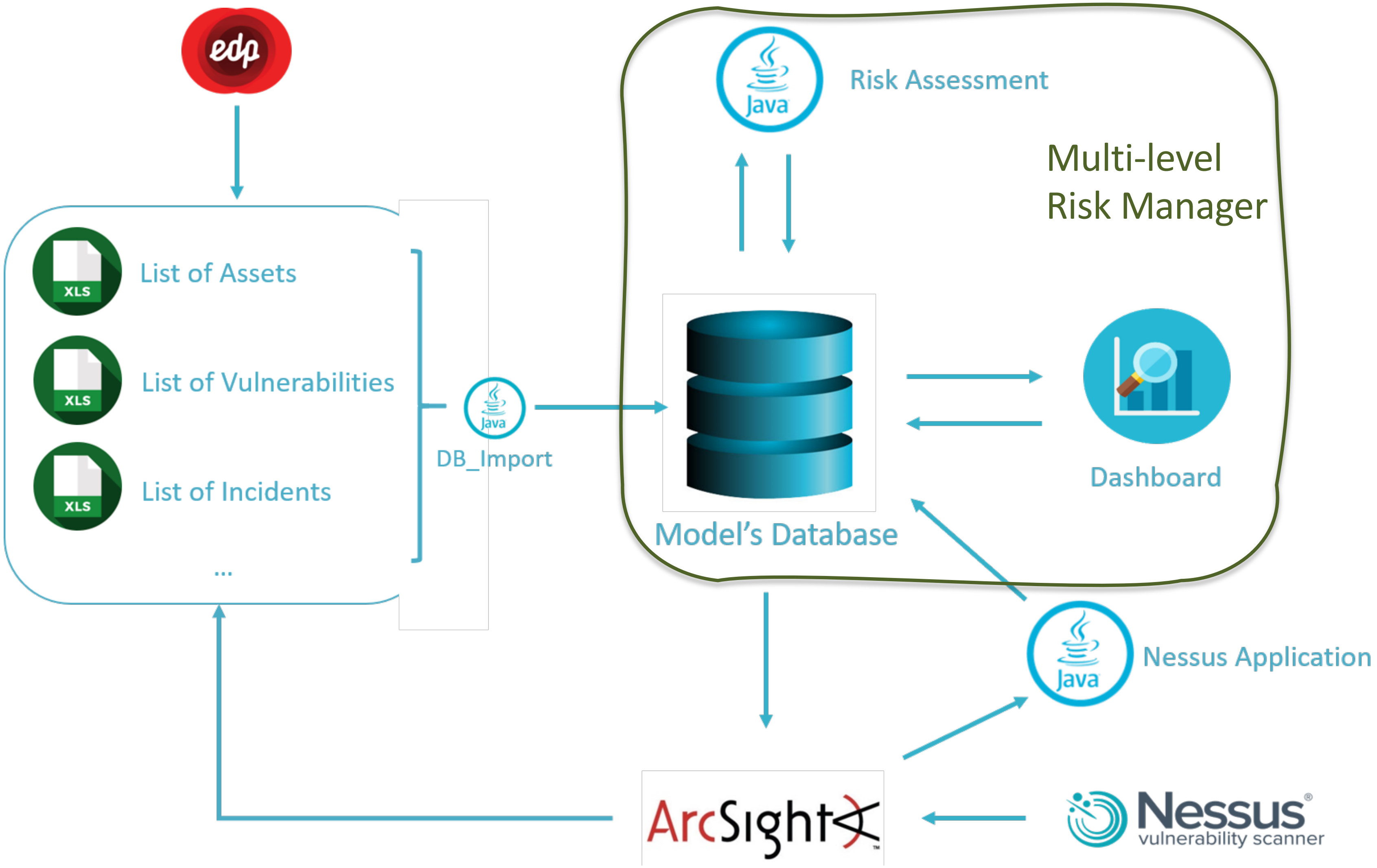


Score of active and historical vulnerabilities in the asset (including the three previous months)

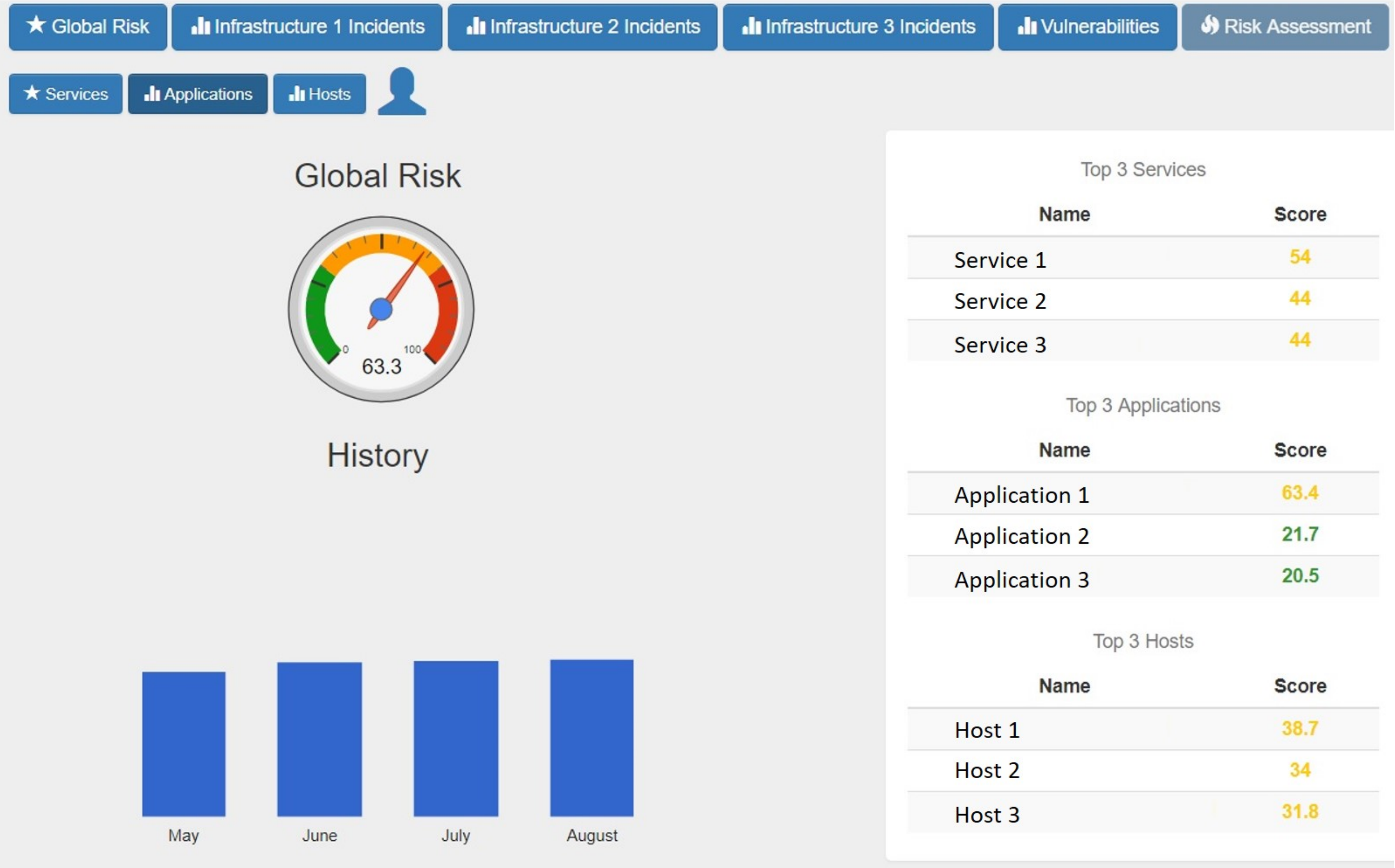
Scores the risk that is inherited from other assets due to the dependency on them

Score of security incidents in the asset (including the three previous months)

Multi-level Risk Manager: Architecture



Dashboard – Global Risk



Top 3 Services

Name	Score
Service 1	54
Service 2	44
Service 3	44

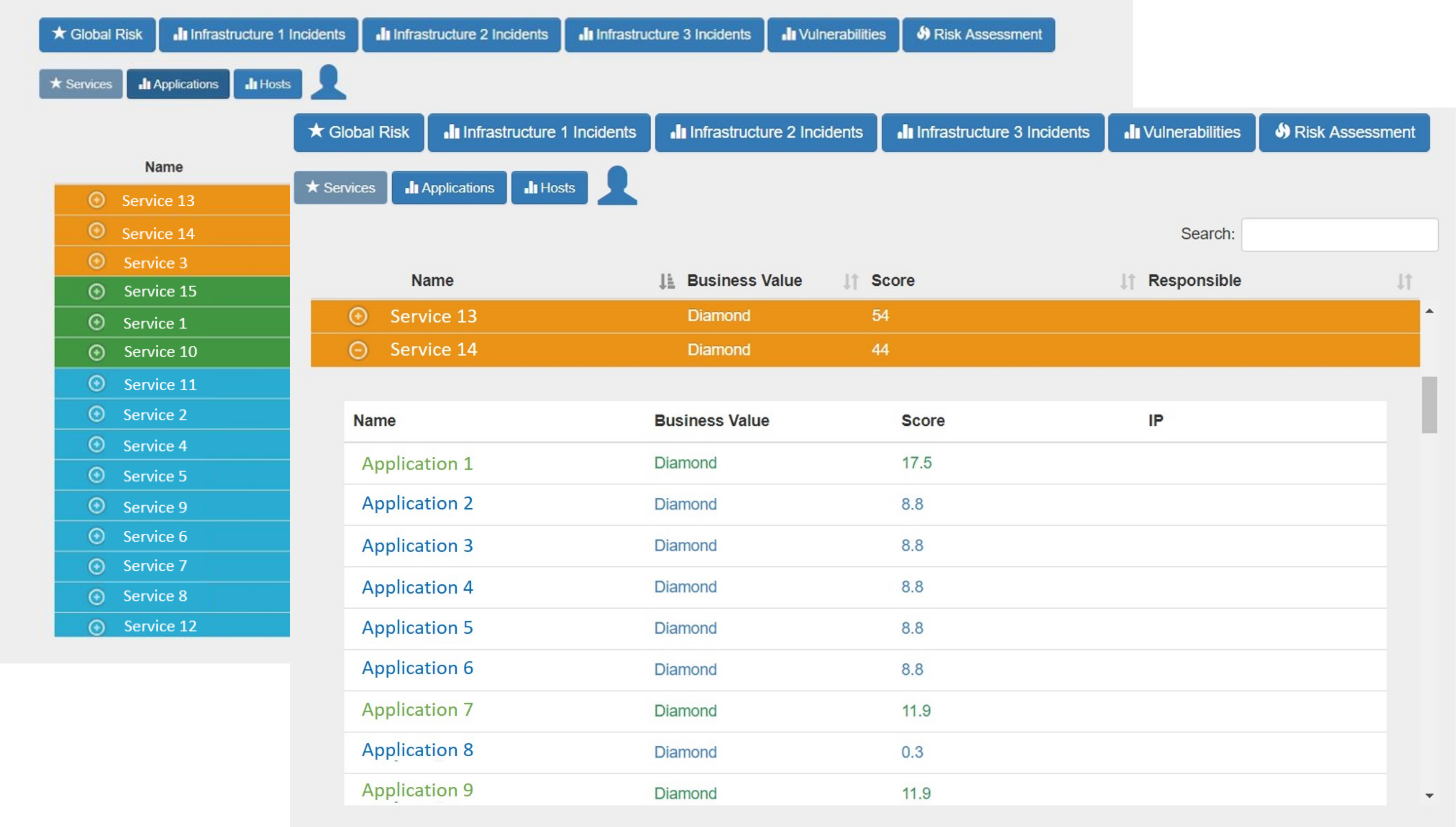
Top 3 Applications

Name	Score
Application 1	63.4
Application 2	21.7
Application 3	20.5

Top 3 Hosts

Name	Score
Host 1	38.7
Host 2	34
Host 3	31.8

Dashboard – Services

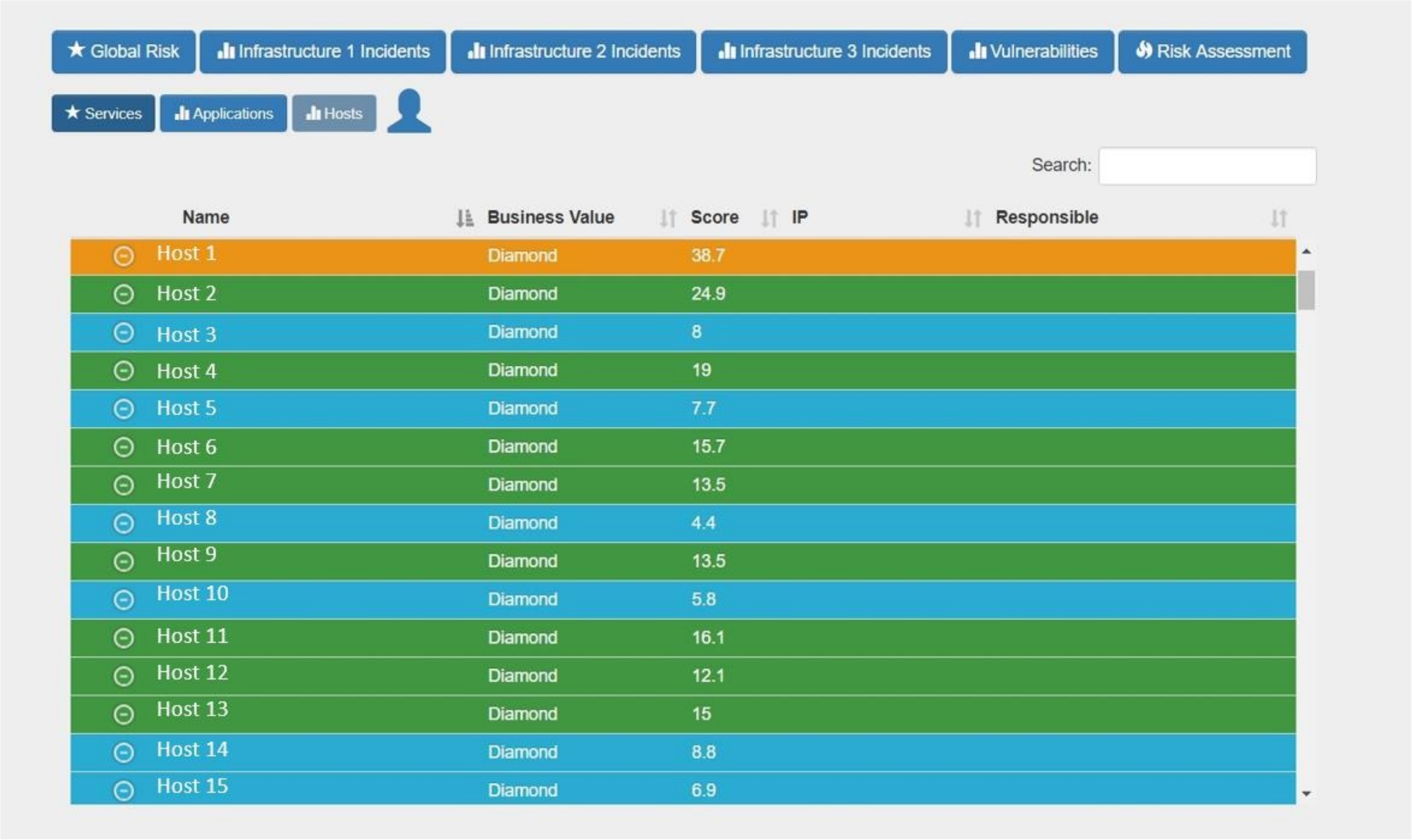

★ Global Risk
Infrastructure 1 Incidents
Infrastructure 2 Incidents
Infrastructure 3 Incidents
Vulnerabilities
Risk Assessment
★ Services
Applications
Hosts
Search:

Name
Service 13
Service 14
Service 3
Service 15
Service 1
Service 10
Service 11
Service 2
Service 4
Service 5
Service 9
Service 6
Service 7
Service 8
Service 12

Name	Business Value	Score	Responsible
Service 13	Diamond	54	
Service 14	Diamond	44	

Name	Business Value	Score	IP
Application 1	Diamond	17.5	
Application 2	Diamond	8.8	
Application 3	Diamond	8.8	
Application 4	Diamond	8.8	
Application 5	Diamond	8.8	
Application 6	Diamond	8.8	
Application 7	Diamond	11.9	
Application 8	Diamond	0.3	
Application 9	Diamond	11.9	

Dashboard – Hosts



★ Global Risk
Infrastructure 1 Incidents
Infrastructure 2 Incidents
Infrastructure 3 Incidents
Vulnerabilities
Risk Assessment
★ Services
Applications
Hosts
Search:

Name	Business Value	Score	IP	Responsible
Host 1	Diamond	38.7		
Host 2	Diamond	24.9		
Host 3	Diamond	8		
Host 4	Diamond	19		
Host 5	Diamond	7.7		
Host 6	Diamond	15.7		
Host 7	Diamond	13.5		
Host 8	Diamond	4.4		
Host 9	Diamond	13.5		
Host 10	Diamond	5.8		
Host 11	Diamond	16.1		
Host 12	Diamond	12.1		
Host 13	Diamond	15		
Host 14	Diamond	8.8		
Host 15	Diamond	6.9		

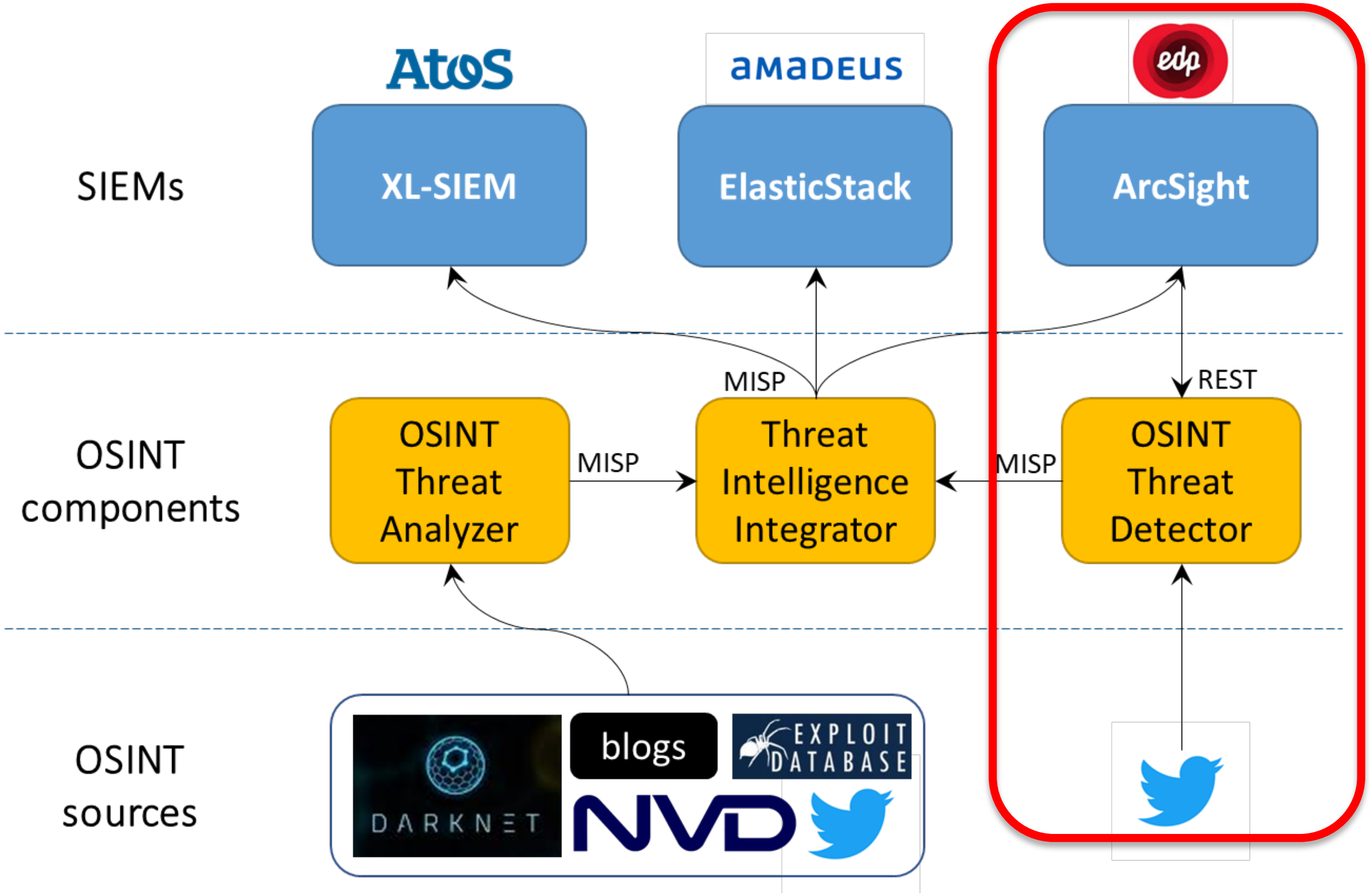
Components Effect on EDP’ SOC

Improve the decision-making process of security analysts and the infrastructure risk visibility for C-level managers

- Introduced a risk viewpoint to the operational day-to-day activities of the SOC
- The relevance, exposure and value of the assets is now used to prioritize incident and vulnerability management efforts
- Security risk became part of the C-level decision-making process

OSINT Threat Detector

OSINT Threat Detector



SIEMs

XL-SIEM

ElasticStack

ArcSight

OSINT components

OSINT Threat Analyzer

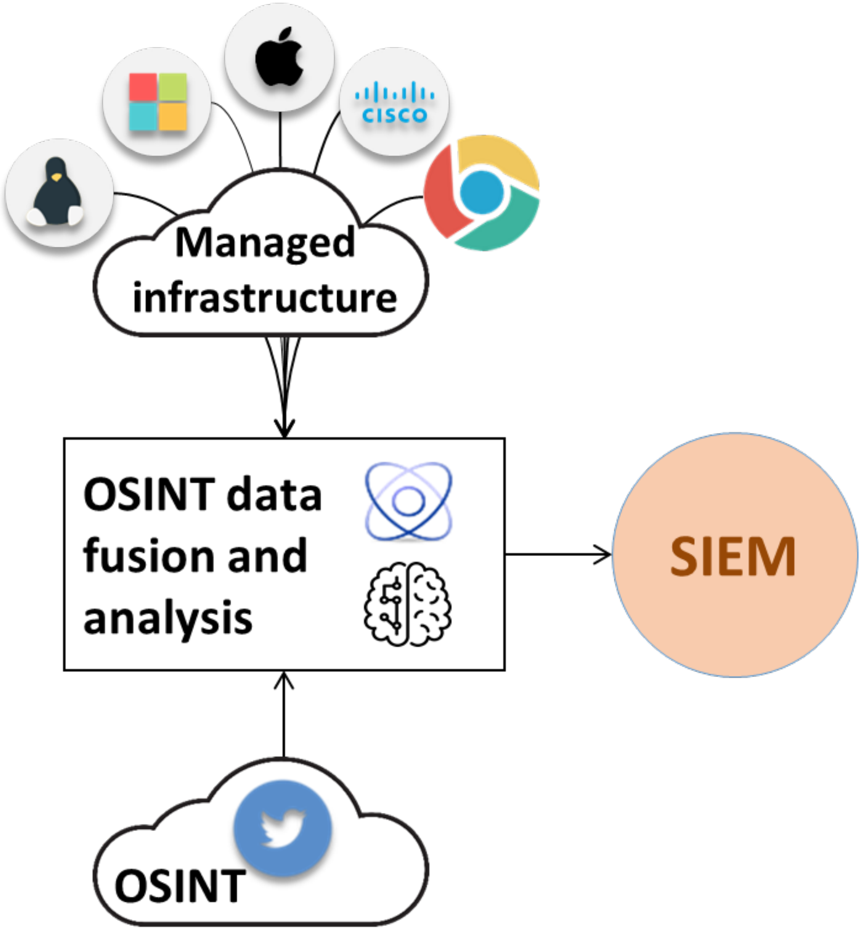
Threat Intelligence Integrator

OSINT Threat Detector

OSINT sources

OSINT Threat Detector

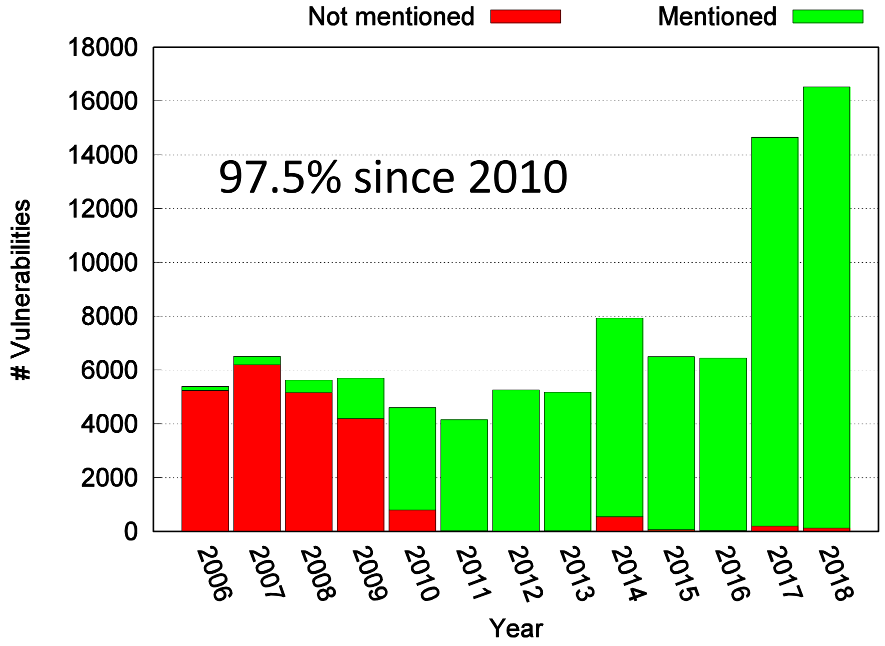
- Find relevant OSINT in Twitter
- Related to the cybersecurity of a specific monitored IT infrastructure
- Feed selected OSINT to the SIEM



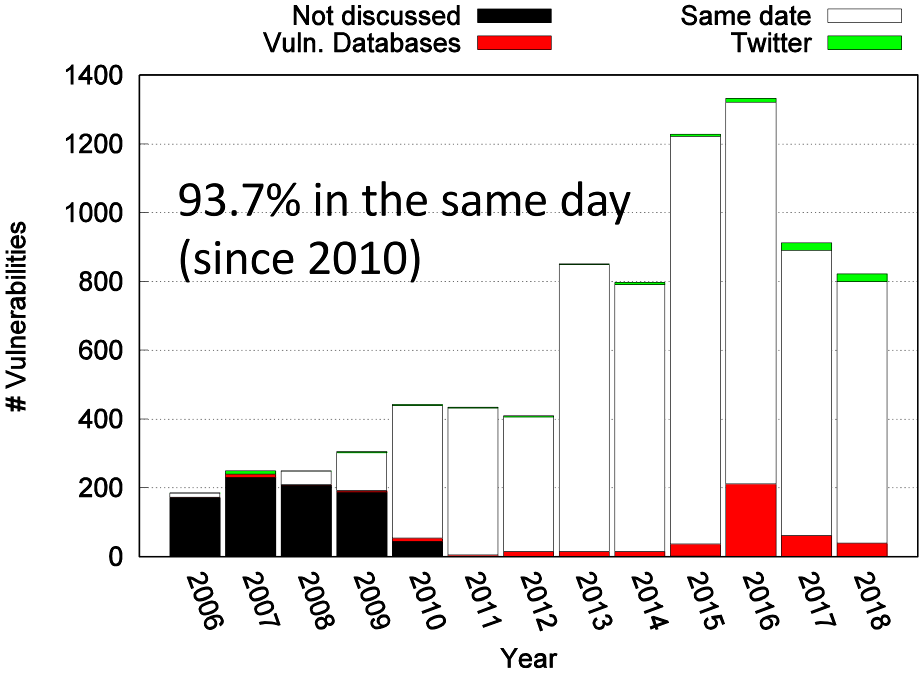
OSINT Threat Detector

- Why Twitter?

Coverage for all vulnerabilities

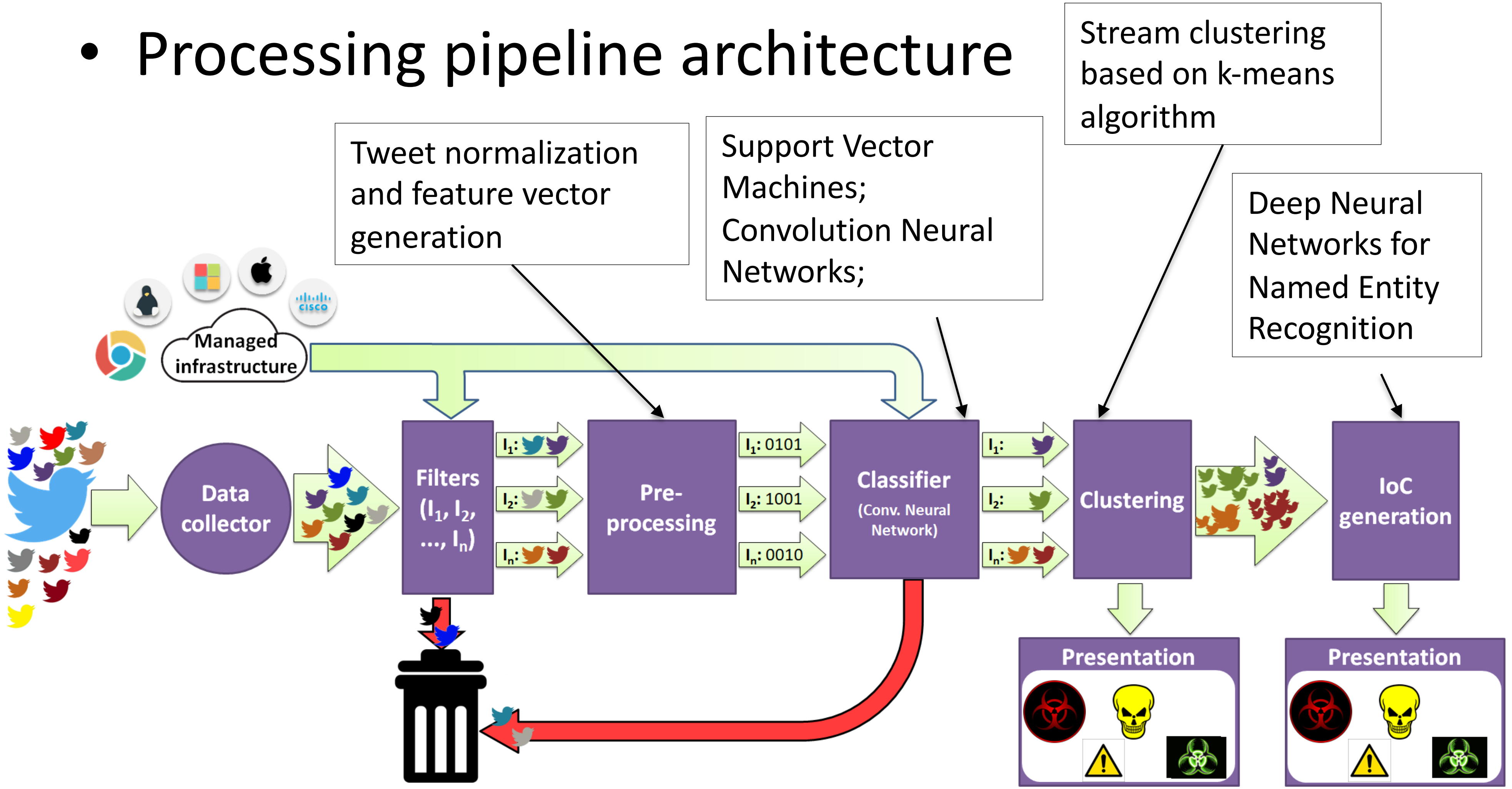


Timeliness for **named vuln.**



OSINT Threat Detector

- Processing pipeline architecture



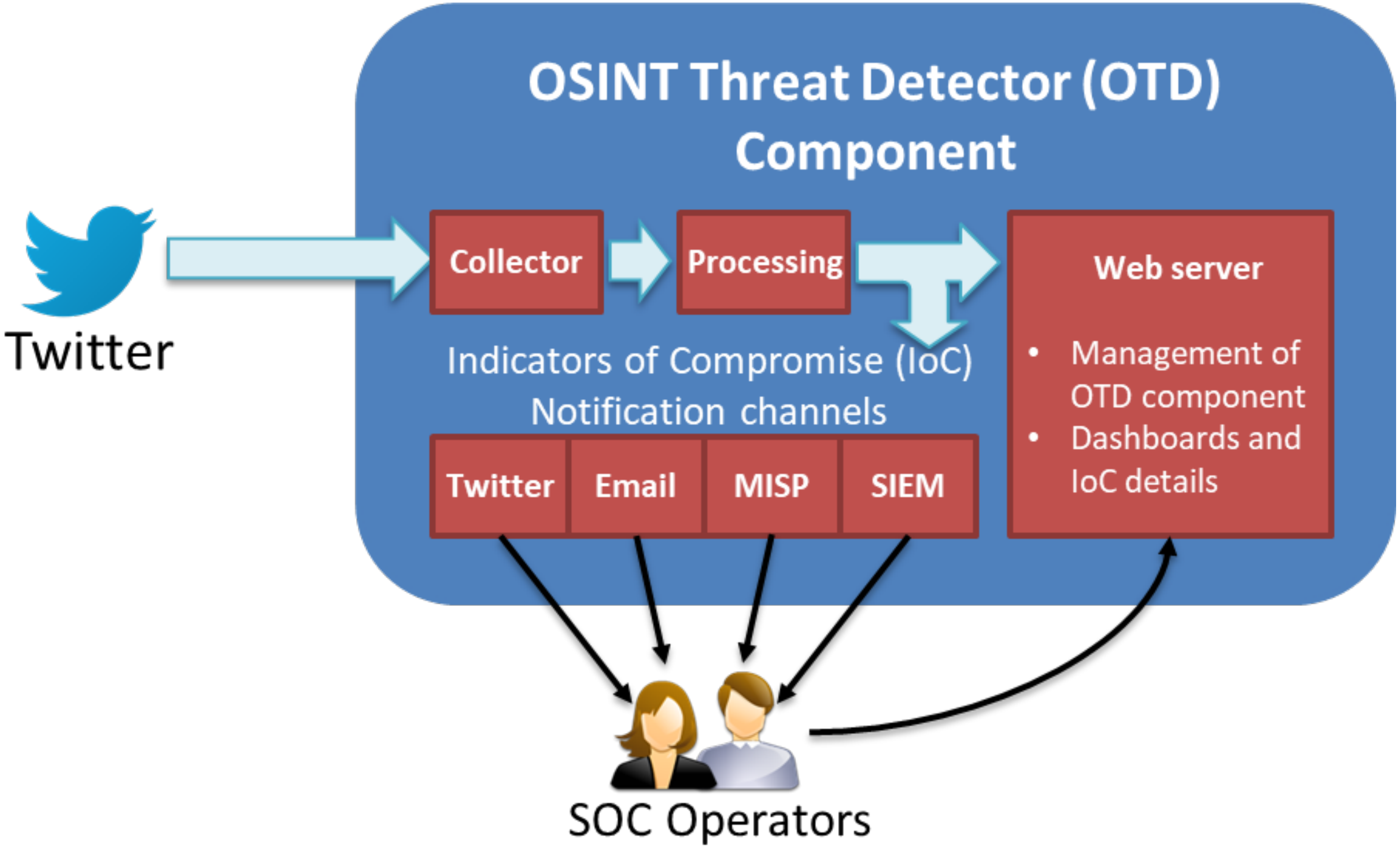
Tweet normalization and feature vector generation

Support Vector Machines; Convolution Neural Networks;

Stream clustering based on k-means algorithm

Deep Neural Networks for Named Entity Recognition

OSINT Threat Detector


Twitter
OSINT Threat Detector (OTD) Component
Collector
Processing
Web server
Management of OTD component
Dashboards and IoC details
Indicators of Compromise (IoC) Notification channels
Twitter
Email
MISP
SIEM
SOC Operators

Integration with Arcsight

- New dashboard
  - Plotting the number of tweets that mention a given product or vulnerability
- New correlation rule and alarm
  - If the number of tweets mentioning a certain asset is greater than 5, raise an alarm
  - Use tweets to enrich alarms from IPS

http://www.disiem-project.eu

Questions?

The DiSIEM project has received funding
from the European Union’s Horizon 2020
research and innovation programme under
grant agreement No 700692.