EvaBssi
a Sopra Steria company

AIRBUS

Insider Threat Protection

AUTHOR : Matthieu Sauvé

AMLD 2022, EPFL Lausanne, 28/03/2022

a unique approach to business challenges

International consulting firm in cybersecurity & IS performance

Our missions

- Control cyber risks
- Identify, protect, detect, respond and recover
- Imagine, build and operate efficient and secure information systems

An answer to our clients' challenges

- EvaBssi combines methodological know-how, high level of technical expertise and Research & Development

2007
Company creation

2021
Acquisition by Sopra Steria

8
Offices on 4 continents

+200
Active clients

34 M€
Turnover 2021

25%
Average yearly growth

280
Average employees' age: 33 years old

EvaBssi
a Sopra Steria company

AIRBUS

Leading *multinational* **aerospace** *company*

"At Airbus, we believe AI is a key competitive advantage that enables us to capitalise on the value of our data."

***863** commercial aircrafts and **332** helicopters delivered in 2019*

- *Design*
- *Manufacturing*
- *Mobility*
- *Cybersecurity*
- *Defence*

Insider Threat

*The potential for an **individual** who has/had **authorized** access to an organization's assets to use their access in order to **harm** that organization*

Unintentional Insider
negligence, accident

Malicious Insider
retaliation, personal gain

External Actor
collusion with an Insider, credentials theft

AIRBUS

EvaBssi
a Sopra Steria company

$11.45M

average cost per incident

in 2020, with 63% of insider threats resulting from employee negligence

-Ponemon Institute Cost of Insider Threats 2020-

207 days

to identify a data breach on average

and 73 days to contain a data breach, in 2020

-IBM Cost of a Data Breach Report 2020-

44%

rise of insider threats incidents

over the past 2 years, with average cost per incident up to $15.38M

-Proofpoint Cost of Insider Threats Global Report 2022-

AIRBUS

EvaBssi a Sopra Steria company

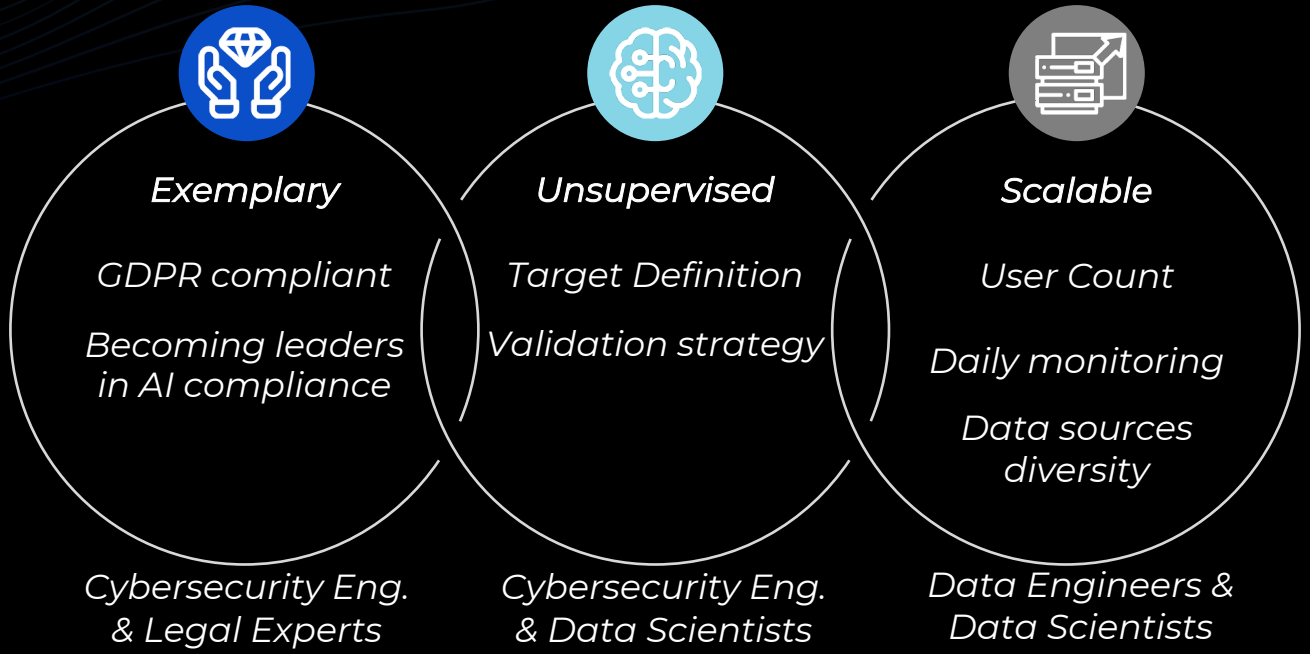
Insider Protection: Setting

Project launched in 2019

*Aim at detecting **potential** Insider Threats*

- *User-centered*
- *Behavioral analysis*
- *End product: Key Trust Indicator*

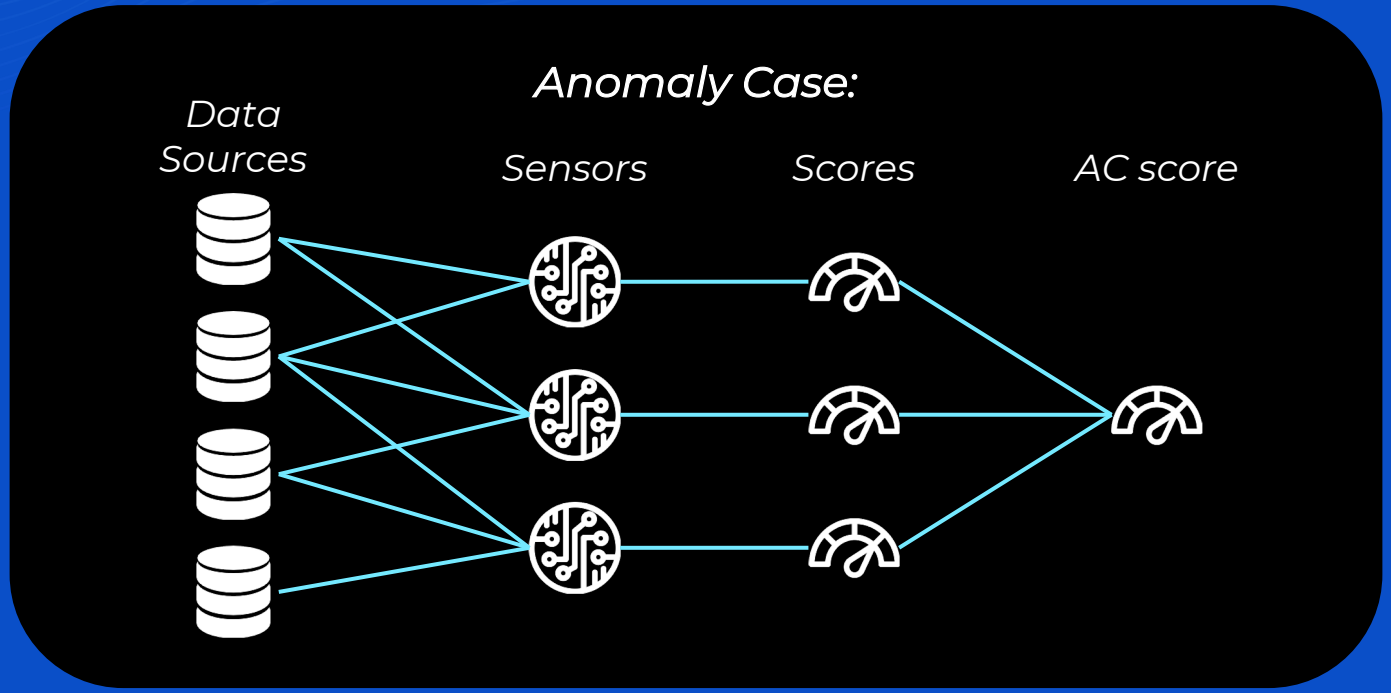
Insider Protection: Challenges



AIRBUS

EvaBssi
a Sopra Steria company

Case-by-case approach



Anomaly case examples

Example: Download/Access substantial amount of data

- *Sensor 1: abnormal downloads from Source 1*
- *Sensor 2: abnormal accesses from Source 1*
- *Sensor 3: abnormal accesses from Source 2*

Connection activity

Use of USB devices

Number of printed files

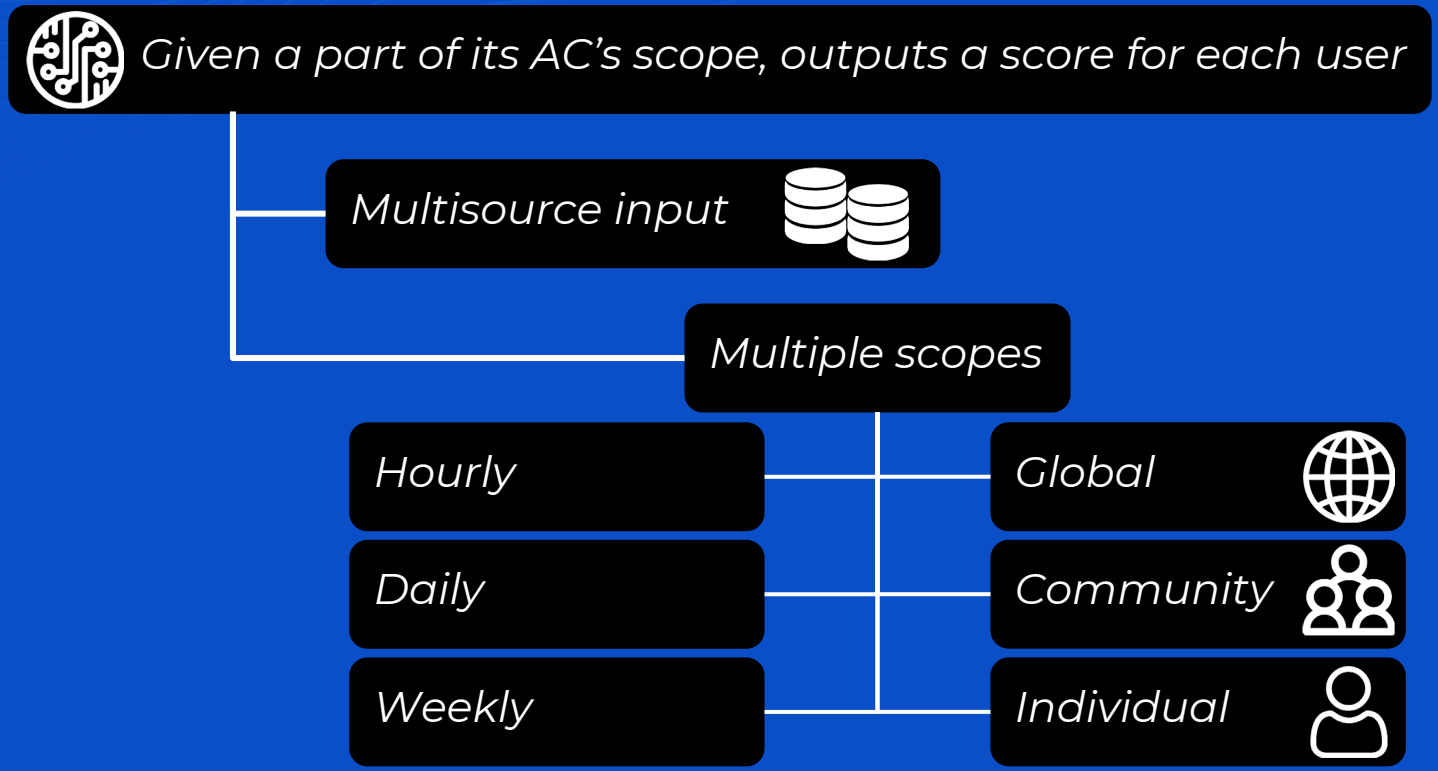
Requests for clearance / higher-level access

Downloading activity

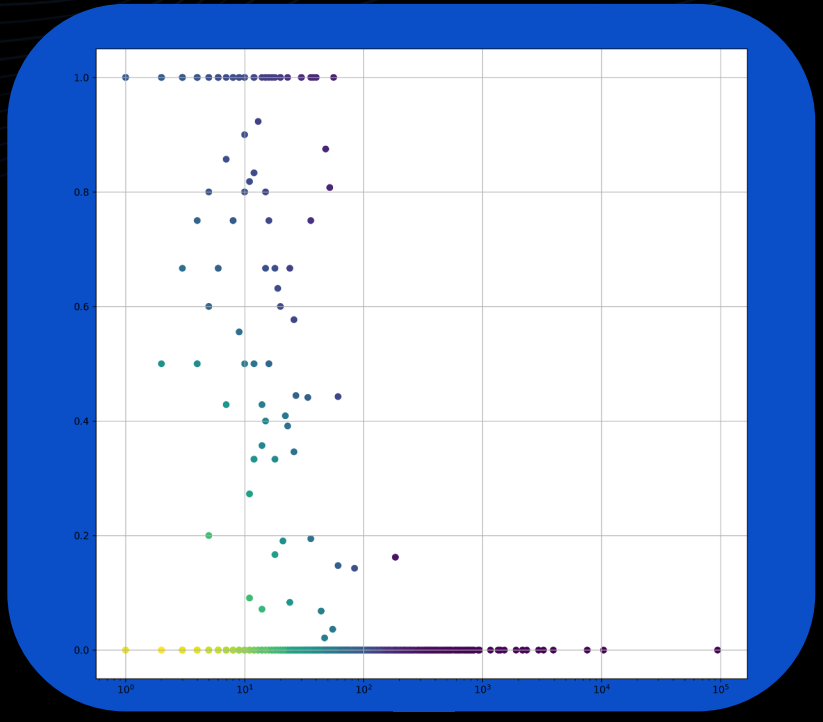
AIRBUS

EvaBssi
a Sopra Steria company

Sensor: general overview



Sensor: global score



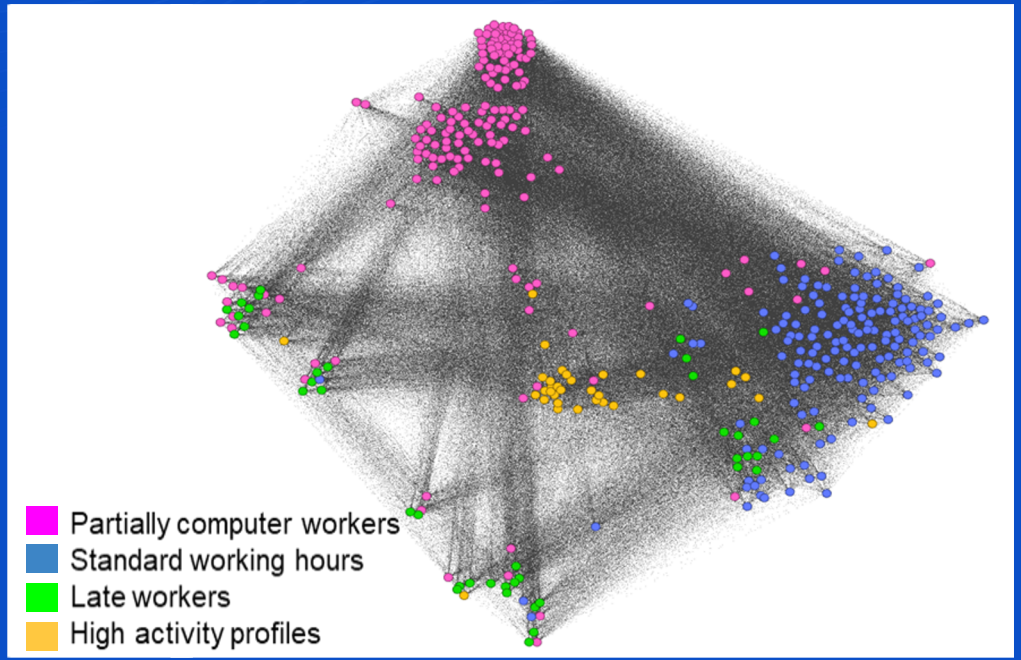
*Each point represents a **daily** value for one of the users*

*The **darker** the colour, the **higher** the anomalous score*

AIRBUS

EvaBssi
a Sopra Steria company

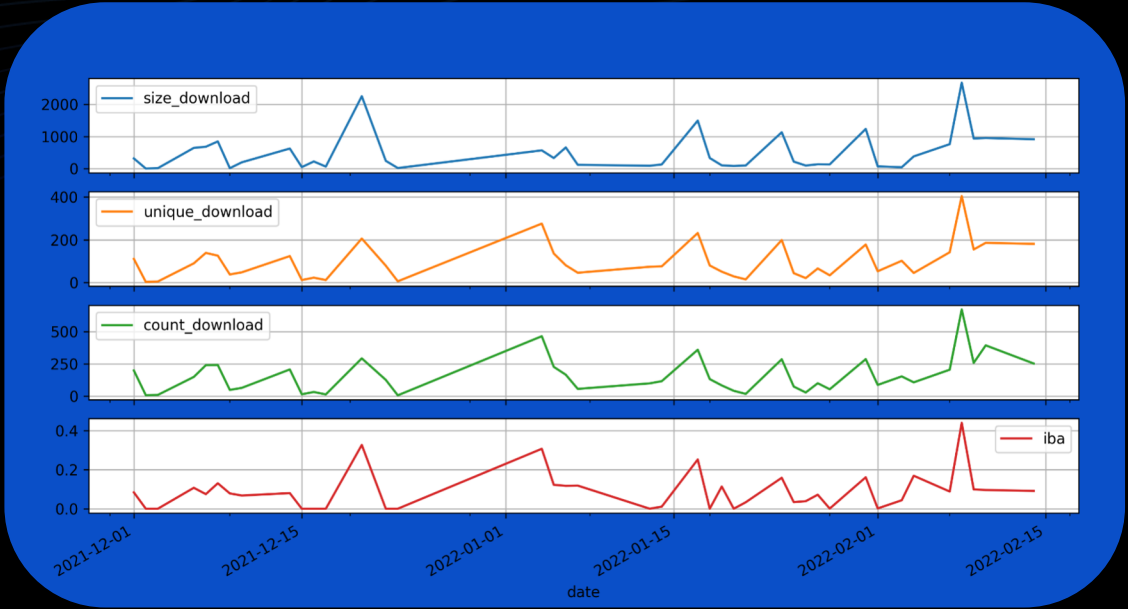
Sensor: community score



Community based score for a user (on a given day):

Average of the distances to every user of his community.

Sensor: individual score



*Each point represents a **daily** value for one of the users*

*The **darker** the colour, the **higher** the anomalous score*

Sensor: combination & aggregation

*Combinations of **contextual** and **temporal** scopes yields behavioral diversity, **ex:** weekly IBA*

*A single sensor can have several scores **ex:** GBA, IBA, weekly IBA*

*Scores capture different **patterns**, hence do not distribute the same*

Density estimation from observed data

Before the aggregation:

Each score observation is transformed into the probability of having a score smaller than the observation

Sensor

Technology:

*Mix of **Machine Learning** and statistical tools*

***Objective:** create an operational **baseline** before complexifying the solutions*

Validation:

***Joint effort** by Cyber Eng. and Data Sci. to analyse the sensor's behavior*

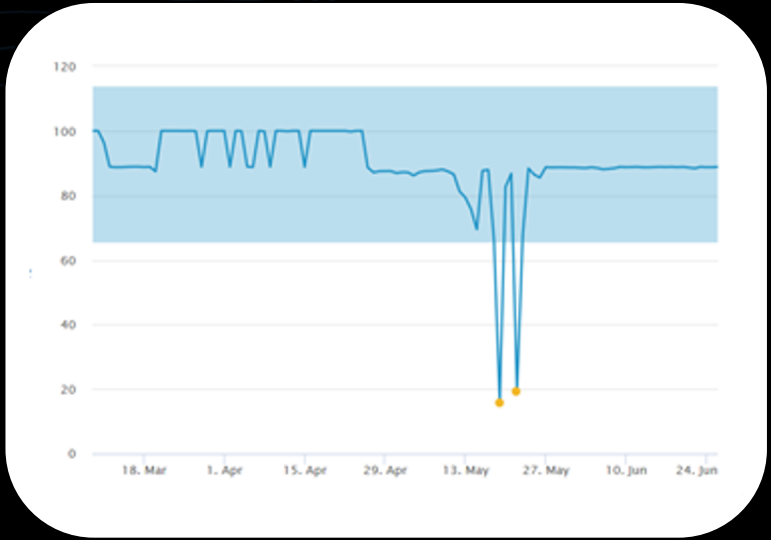
*Use of Internal Evaluation of Unsupervised Outlier Detection (**IREOS**)*

AIRBUS

EvaBssi
a Sopra Steria company

Key Trust Indicator: aggregation

*KTI is computed as a **weighted sum** of Anomaly Case scores*



KTI

- Inverted and scaled between 0 and 100
- The closest to 100, the less suspicious

AC weight: measured by cyber experts using internal criticality indicators, and external indicators (MITRE etc...)

Key Trust Indicator: Value

Visualisation:

Visualisation of the KTI, including the ***contributions*** *of the differents ACs and their sensors*

Enhance ***investigation power*** *for SOC / CERT*

Analysis:

KTI ***values*** *and* ***variations*** *along time can be analysed to determine if an account is* ***compromised***

Enable ***identification*** *of potential* ***Insider Threats***

AIRBUS

EvaBssi
a Sopra Steria company

Insider Protection Usage

AI is **not a decision-maker** here: its goal is to **reinforce** human expertise, not supersede it

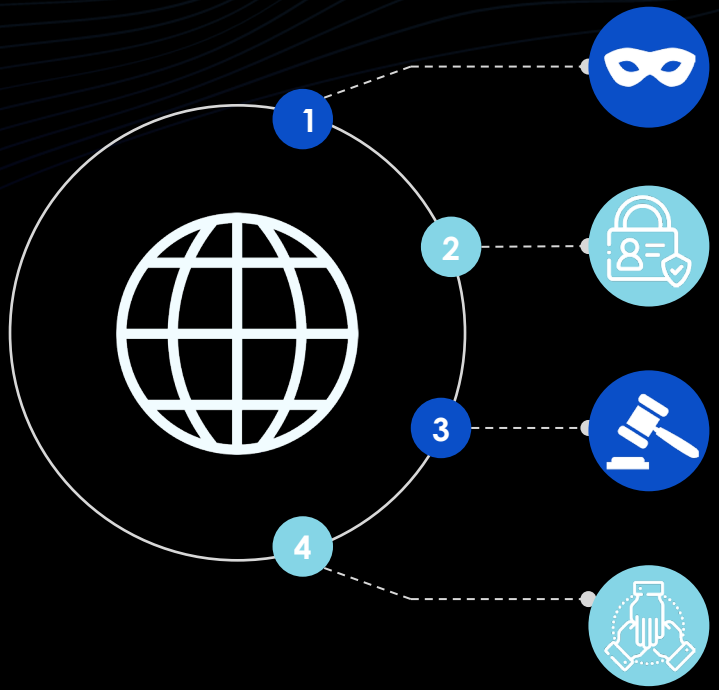
Users ending up on the SOC's radar can be **suspended** or **revoked**

Evasion & Poisoning	*Need to blend in or blur the outliers*	*Distributed design and scores' diversity makes it hard* *Tedious information gathering*
Model stealing & Inference	*Need to probe the models*	*High risk of popping up on SOC radar*

AIRBUS

EvaBssi
a Sopra Steria company

Ethics and Legal Context



Data pseudonymisation

- *No connection between the user and the private individual, only between the user and the data*

Compartmentalisation of the project

- *Only authorised personnel (SOC analysts) can link a user to its private individuals*
- *Penetration test audit*

Legal Team implication from the start

- *Objective: ensure Insider Protection complies with the GDPR*
- *Dictates which data can be used or not by Insider Protection*
- *Each Anomaly Case needs to be approved before any development*

Airbus European AI Act Task Force

- *All-round multidisciplinary team composed of technical and legal experts from all across Airbus*
- *Objective: define the impact of future regulations on the group and anticipate the compliance of Airbus projects*

AIRBUS

EvaBssi
a Sopra Steria company

EvaBssi
a Sopra Steria company

Thank you!

EvaBssi Europe

40 Rue du Louvre, 75001 Paris

+33 1 86 52 96 40

evabssi.com