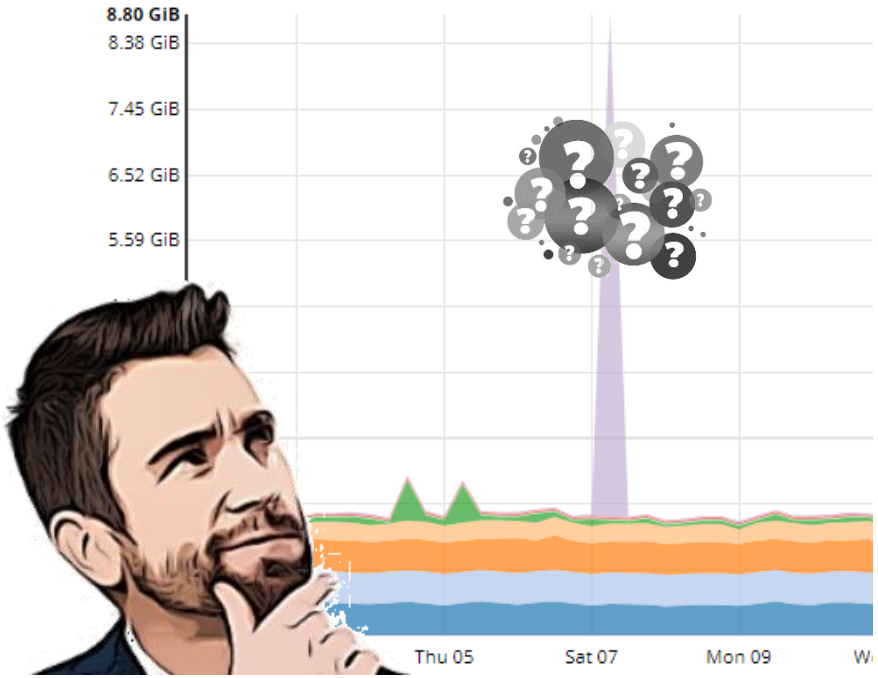
IDS Design and Implementation

***João Gaspar**, Cyber Security Analyst*
EDP Distribuição



June 18th , 2020
SmartGrid Forums - Webconference

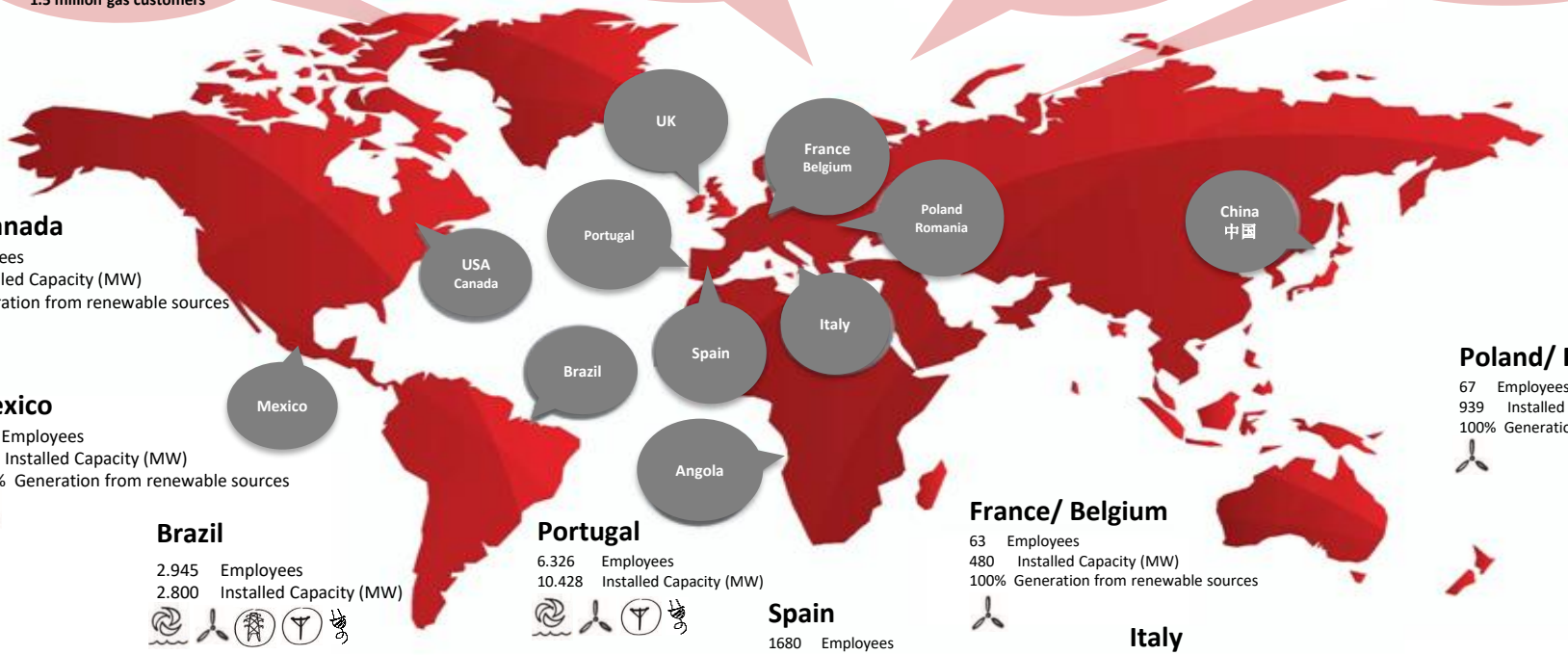
EDP Distribuição is a company of the EDP Group, being a global energy player with a strong presence in Europe, Brazil and considerable investments in the USA

11 million
CUSTOMERS
9.8 million electricity customers
1.5 million gas customers

#4 World wind energy company

26,7 GW
Installed Capacity
>70%
Renewable Generation

MEMBER OF Dow Jones Sustainability Indices In Collaboration with RobecoSAM



USA/ Canada
493 Employees
5.085 Installed Capacity (MW)
100% Generation from renewable sources

Mexico
9 Employees
200 Installed Capacity (MW)
100% Generation from renewable sources

Brazil
2.945 Employees
2.800 Installed Capacity (MW)

Portugal
6.326 Employees
10.428 Installed Capacity (MW)

Spain
1680 Employees
6 087 Installed Capacity (MW)

Italy
28 Employees
144 Installed Capacity (MW)

France/ Belgium
63 Employees
480 Installed Capacity (MW)
100% Generation from renewable sources

United Kingdom
42 Employees

Poland/ Romania
67 Employees
939 Installed Capacity (MW)
100% Generation from renewable sources

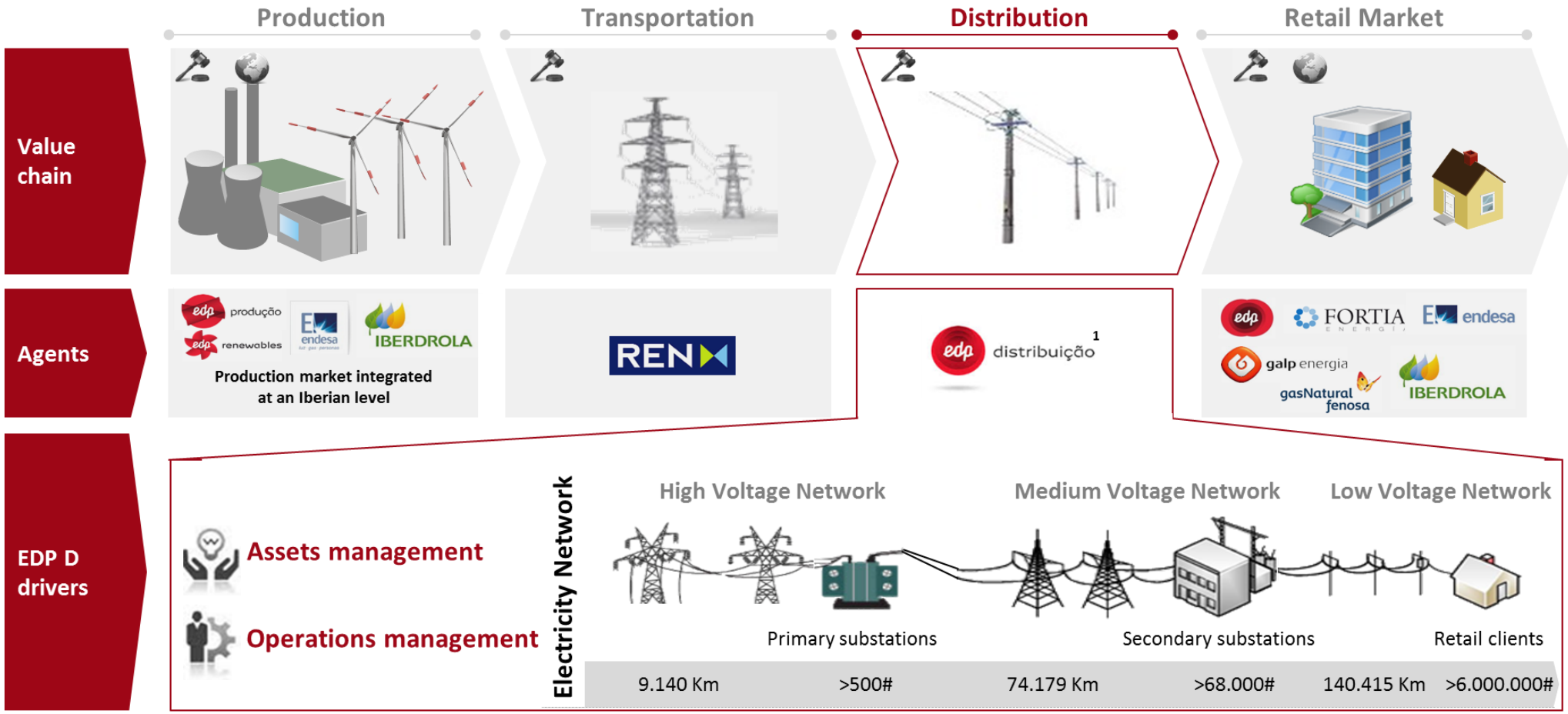
2017 WORLD'S MOST ETHICAL COMPANIES® WWW.ETHISPHERE.COM

Production Renewables Transport Distribution Retail

edp distribuição

The Portuguese National Electricity System includes EDP Distribuição as the regulated electricity distribution company, acting under a public service concession

EDP Distribuição in the National Electricity Sector



Regulated activity

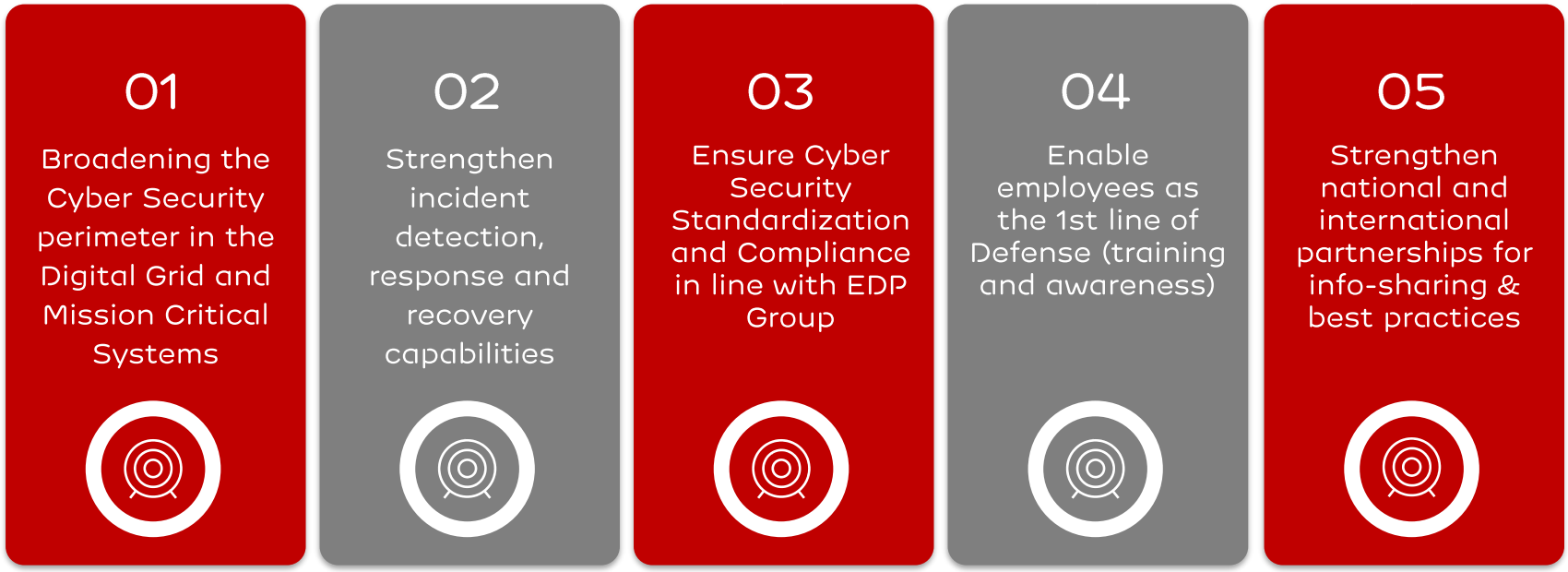
Liberalized activity

1. & small cooperatives (<1%)

distribuição

OT cyber security objectives combines the strategy of EDP Distribuição and the practices of the EDP Group

OT Strategic Objectives



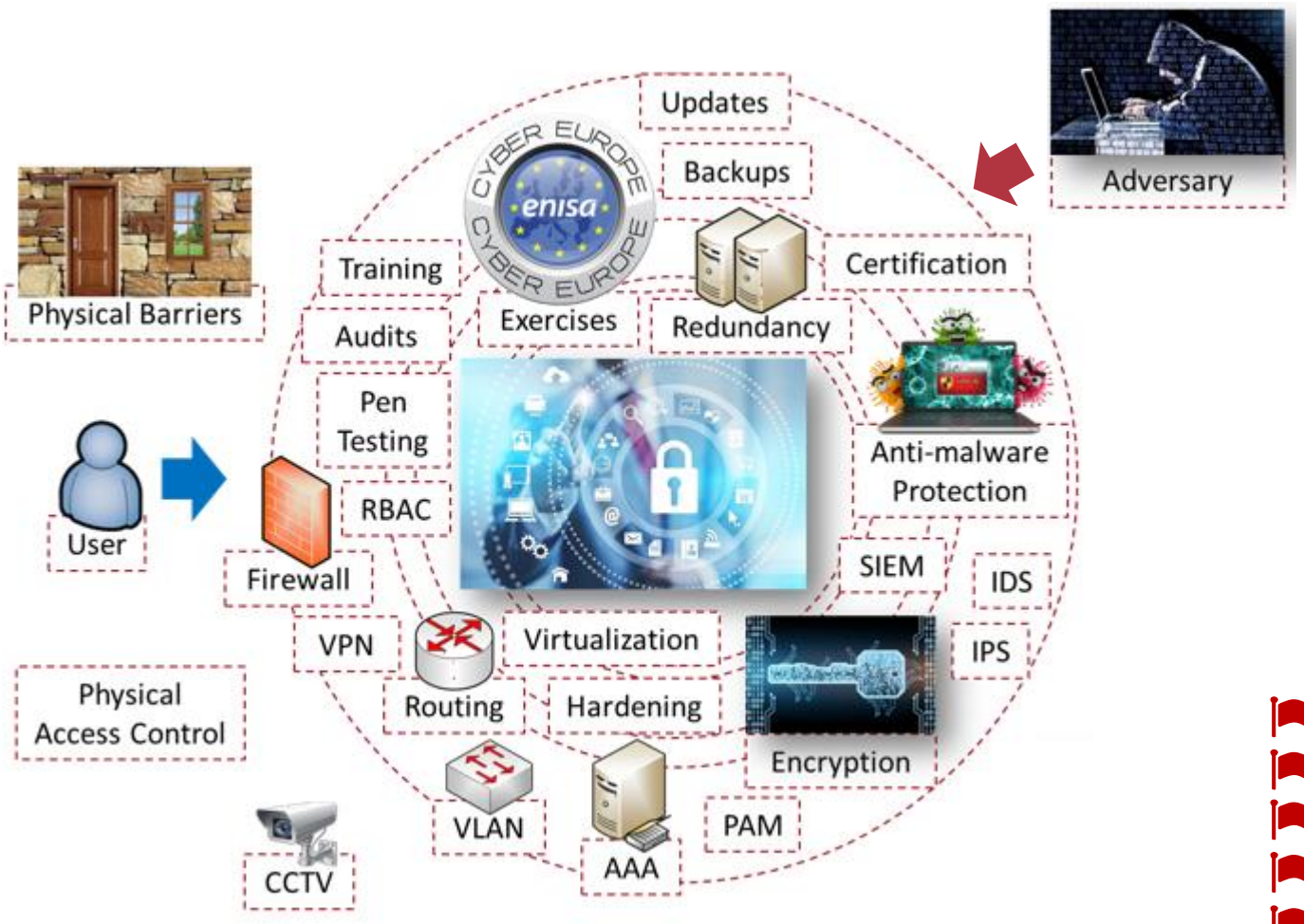
OT cyber security objectives combines the strategy of EDP Distribuição and the practices of the EDP Group

OT Strategic Objectives

- **Reducing organization risk** by reducing the potential impact of cyberattacks
- Improve procedures to **reduce detection and recovery time** after cyberattacks

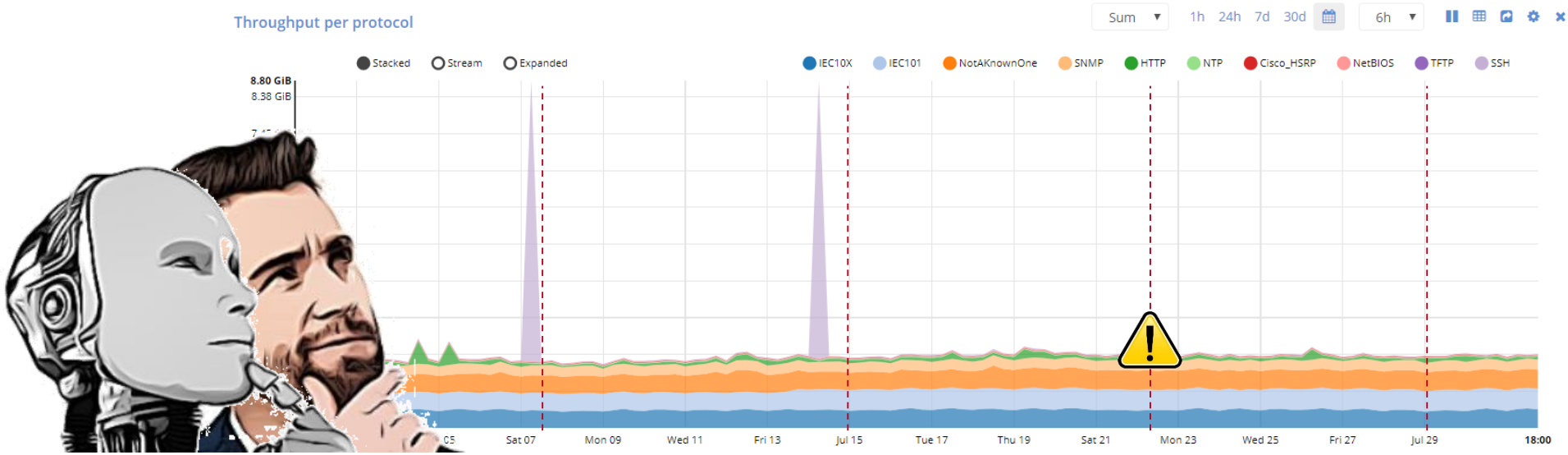
Security anomaly detection is a key component for strengthening incident detection and response capabilities.

OT cyber security traditionally relies on dedicated instances of IT security solutions, which are mostly based on signatures, whitelisting and blacklisting



- **ACLs Firewalls**
- **Anti-virus malware signatures**
- **IDS/IPS attacks signatures**
- **SIEM filters**
- **Etc.**

OT security analytics solutions are using AI and ML to learn patterns in the behaviour of the network, specific machines, users and malicious agents, as a baseline to detect anomalies and execute predefined actions. Being OT focused, they have knowledge of industrial protocols



1. Learning **2. Tunning** **3. Detection and reaction** **4. Analysis and feedback**

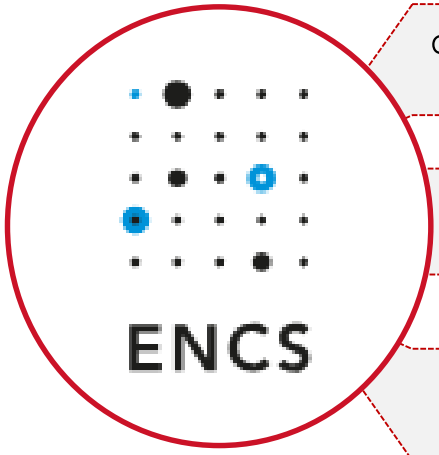
Human intervention

Machine intervention

RESPONSE AND RECOVERY

▼ Knowledge-based + ▲ Behaviour-based = Advanced detection

The ENCS OT Security Monitoring project provided a requirement basis and with that, we got enough confidence to develop a proof of concept with one of the analysed solutions, and consequently to advance for a tender



OT Security Monitoring Member project with European DSOs

Set of detection Use Cases

a. of Known Attacks
b. of new Hosts
c. of Unusual Network Connections
d. of Malformed Packets
e. of unusual Commands or Parameters
f. of Flow-Based Anomalies
g. of Web Attacks
h. of Weak Protocol Configurations

Analysis of several OT security monitoring solutions

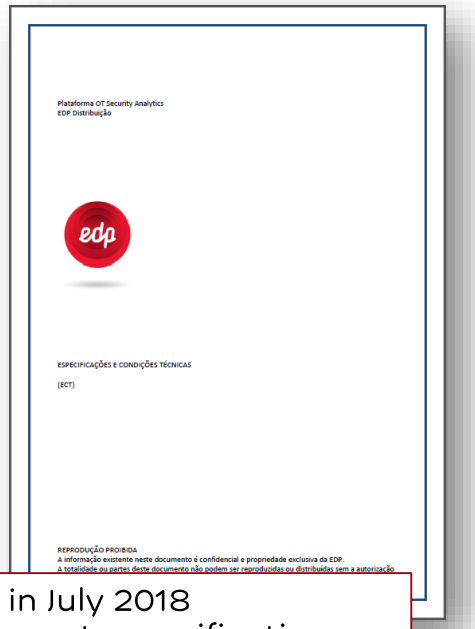
SILENTDEFENSE™

POC and pratical learning about the solution

edp distribuição

On the tender published, EDP Distribuição's defined that the OT security analytics platform shall support (by default or after customization) the following requirements and use cases

- Baseline learning, including an extensive list of parameters, IT and OT protocols and other communcation details
- Detection and correlation of abnormal and malicious activities based on the baseline communication standards
- Detection feautures according to ENCS OT Monitoring Use Cases
- Ease of navigation;
  Analysis Filters availability;
  Information Extraction in .csv and .pcap formats
- Integration with EDPD systems including the SIEM

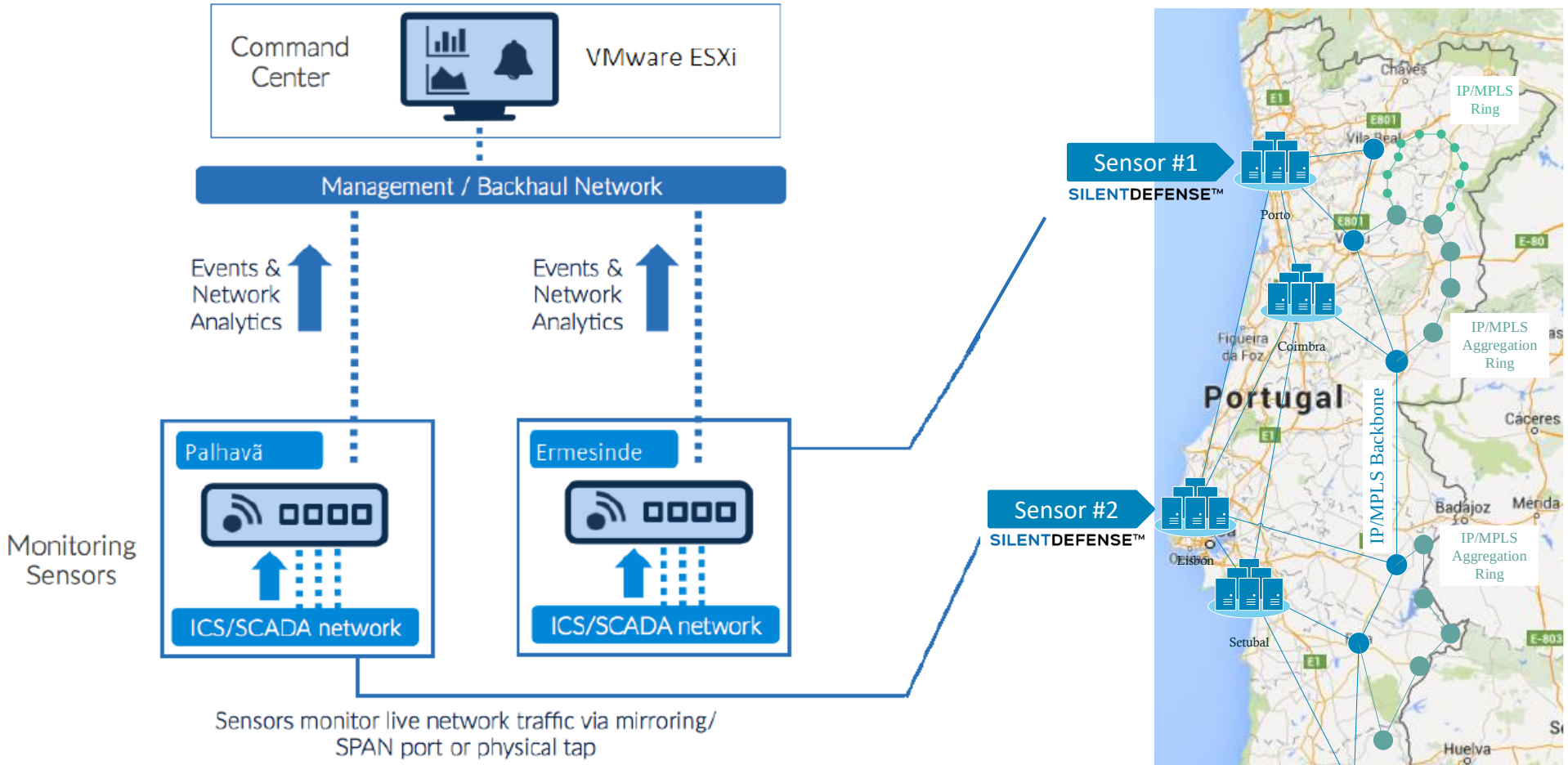


- Tender in July 2018
- Requirements specification

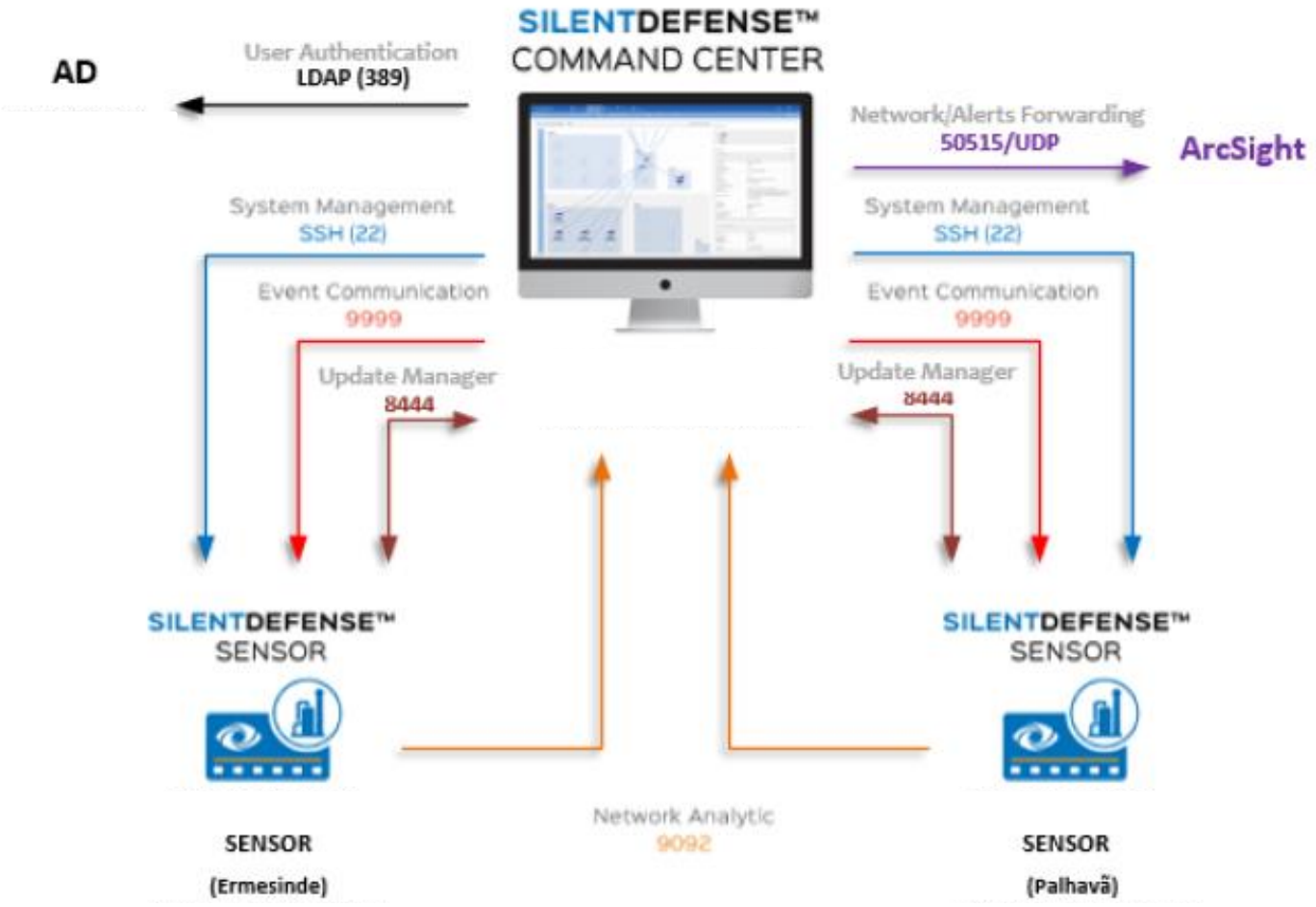
- Security Matters' Silent Defense
- 2 sensors and 1 CC
- Detection only
- On request support hours

INITIAL SCOPE

The infrastructure that best fit our needs revealed to be the implementation of 2 sensors, each one on a core network node, both supported and managed by a virtualized Command Center



The solution conectivity diagram works as it's showen on the diagram below



The implementation project following the adjudication in late October, 2018, consisted on a 4 stage project plan

SECURITY ANALYTICS PROJECT

Adjudication
October 2018

Secur.Net
Always online, always secure!
<) FORESCOUT

Stage #1
November 2018

- Architecture review
- Product documentation
- Deployment checklist
- Test planning

Stage #2
December 2018

- HW & SW instalation
- Initial tests
- Learning start

Stage #3
January 2019

- Finetuning
- Scripting

Customization required for full compliance with requirements.

Stage #4
February 2019

- Acceptance tests
- Training and SOC integration
- Solution documentation

edp distribuição

LESSON #1

Training should happen before costumization 1) to take advantage of the already operational platform and 2) to facilitate the costumization process

SECURITY ANALYTICS PROJECT

Adjudication

October 2018

Secur.Net
Always online, always secure!
<) FORESCOUT

Stage #1

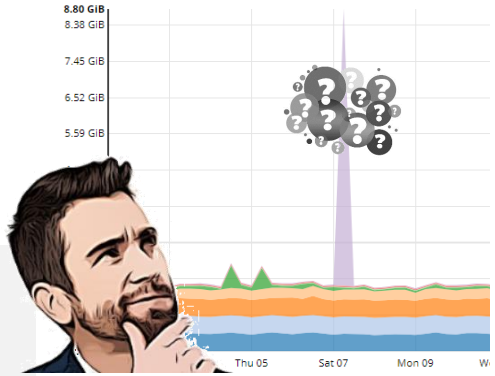
November 2018

- Architecture review
- Product documentation
- Deployment checklist
- Test planning

Stage #2

December 2018

- HW & SW instalation
- Initial tests
- Learning start



PLAN CHANGE

- Training

Customization required for full compliance with requirements.

Stage #3

January 2019

- Finetuning
- Scripting

Stage #4

February 2019

- Acceptance tests
- Training and SOC integration
- Solution documentation

edp distribuição

LESSON #2

A POC is very important to understand the technology, and its lessons are valuable for an eventual implementation

POC lessons

- Aggregation of field communications reduces the number of required sensors
- POC system configurations (e.g., learned models, LDAP and SIEM integration)
- Using the firewall ACLs to validate the initial self-learned model accelerates fine-tuning
- Security analytics SIEM use cases are essential for integration of the solution in the incident detection and response process
- Human intelligence and experience required for fine-tunning and alert analysis

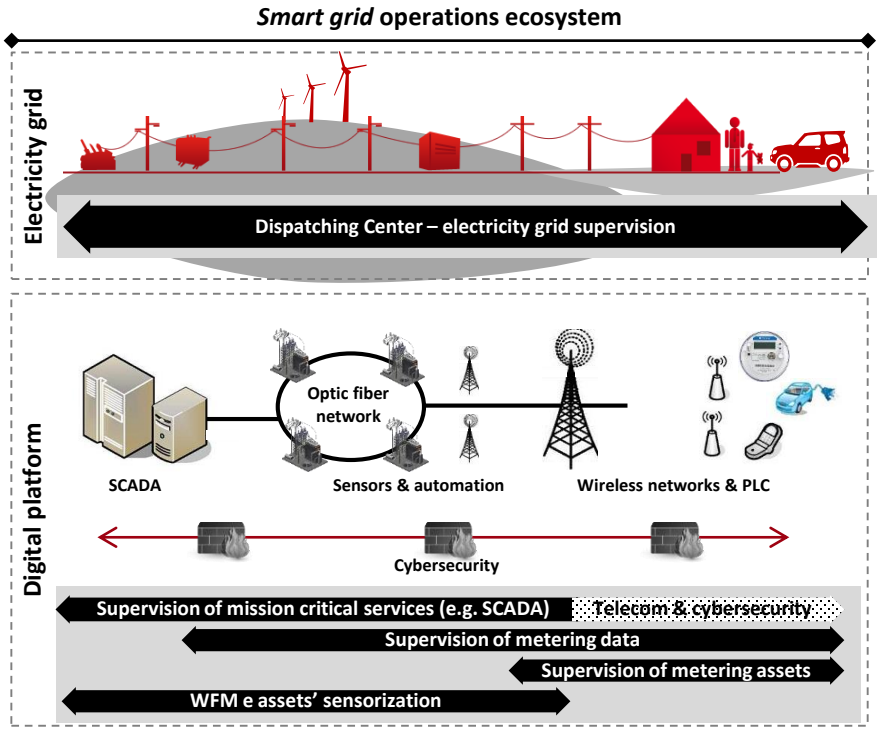
edp distribuição

EDP Distribuição faces new challenges on operate and supervise an electrical grid with increasingly intelligence and complexity. The OT Security Analytics solution is a key component of its Integrated Supervision Center, providing visibility over previously unseen potential threats

02

Strengthen incident detection, response and recovery capabilities

SILENTDEFENSE™



Adjusting people and process strategy around advanced IDS implementation ensure seamless integration with the overall cybersecurity strategy

edp distribuição

Thank you for your attention!

João Gaspar
joao.gaspar@edp.pt

edp distribuição

IDS Design and Implementation