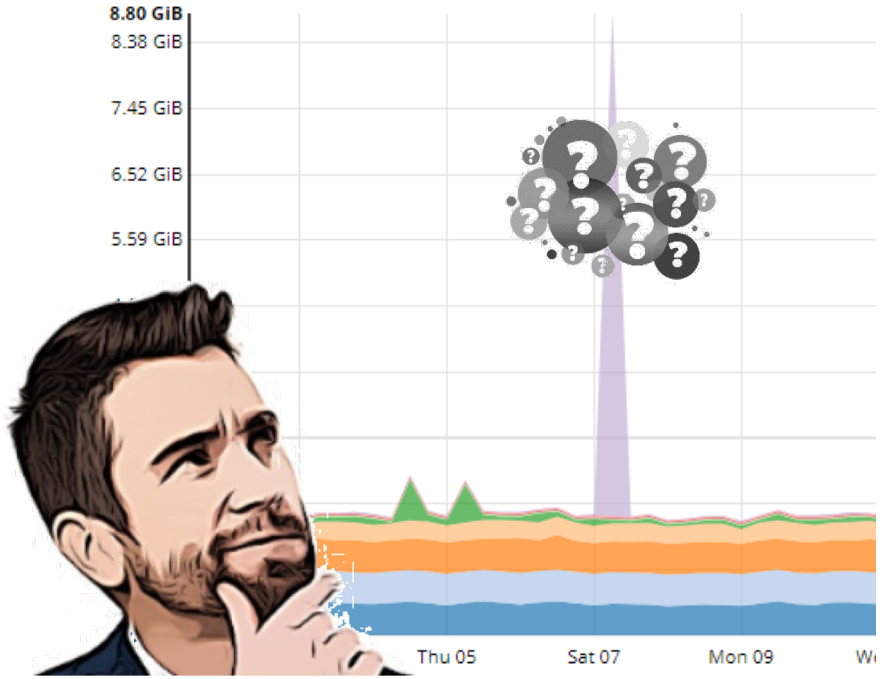
IDS Implementation and Integration

***Nuno Pereira**, OT Cyber Security Officer*

EDP Distribuição



Energy Intrusion Detection

January 29th , 2019

Amsterdam, The Netherlands

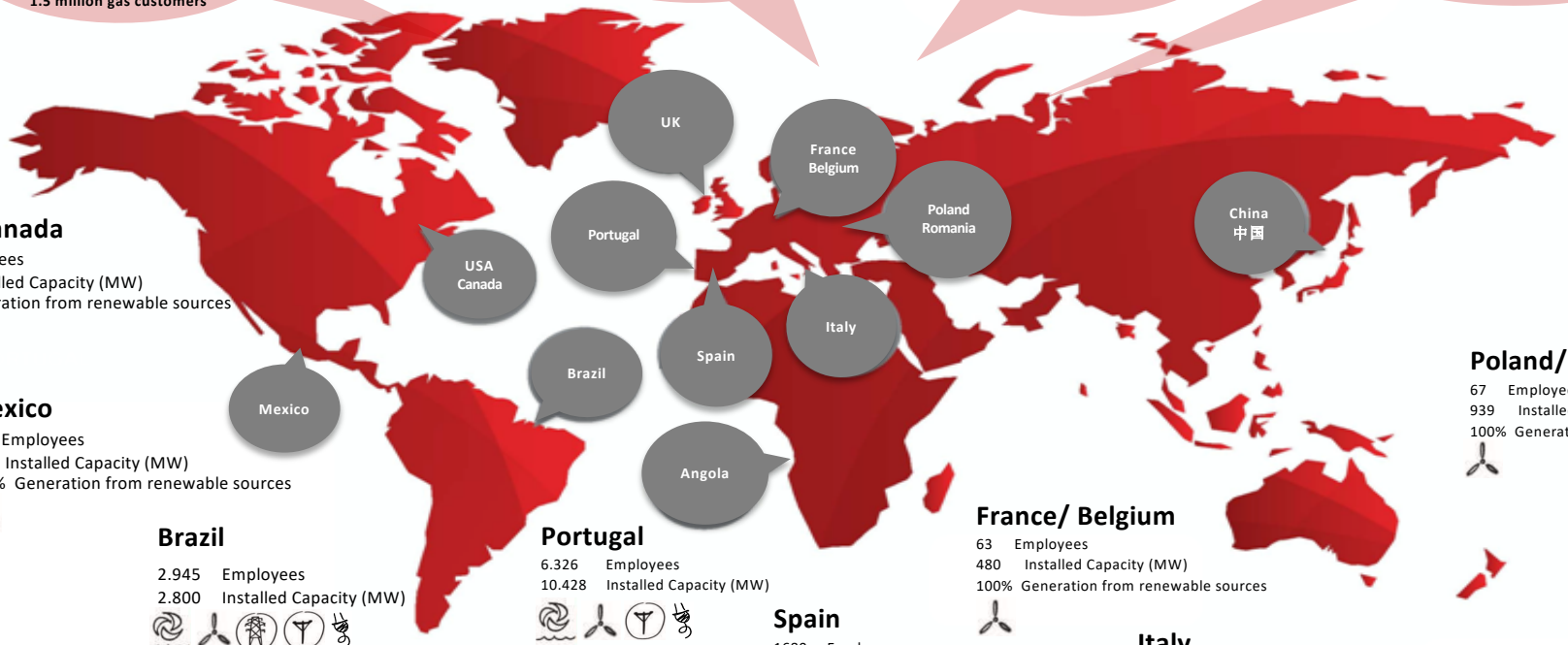
EDP Distribuição is a company of the EDP Group, this being a global energy player with a strong presence in Europe, Brazil and considerable investments in the USA.

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)

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

Italy
28 Employees
144 Installed Capacity (MW)

United Kingdom
42 Employees

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

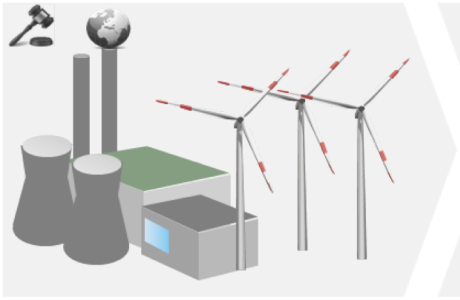
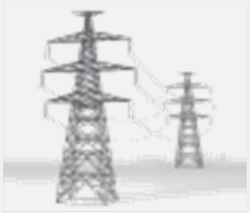
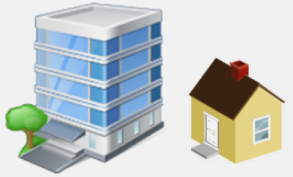
2017 WORLD'S MOST ETHICAL COMPANIES® WWW.ETHISPHERE.COM

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

	Production	Transportation	Distribution	Retail Market
Value chain				
Agents	edp produção, edp renewables, endesa, IBERDROLA Production market integrated at an Iberian level	REN	edp distribuição [1]	edp, FORTIA ENERGIA, endesa, galp energia, gasNatural fenosa, IBERDROLA
EDP D drivers	Assets management Operations management			

Electricity Network

High Voltage Network		Medium Voltage Network		Low Voltage Network	
9.140 Km	>500#	74.179 Km	>68.000#	140.415 Km	>6.000.000#

Regulated activity

Liberalized activity

1. & small cooperatives (<1%)

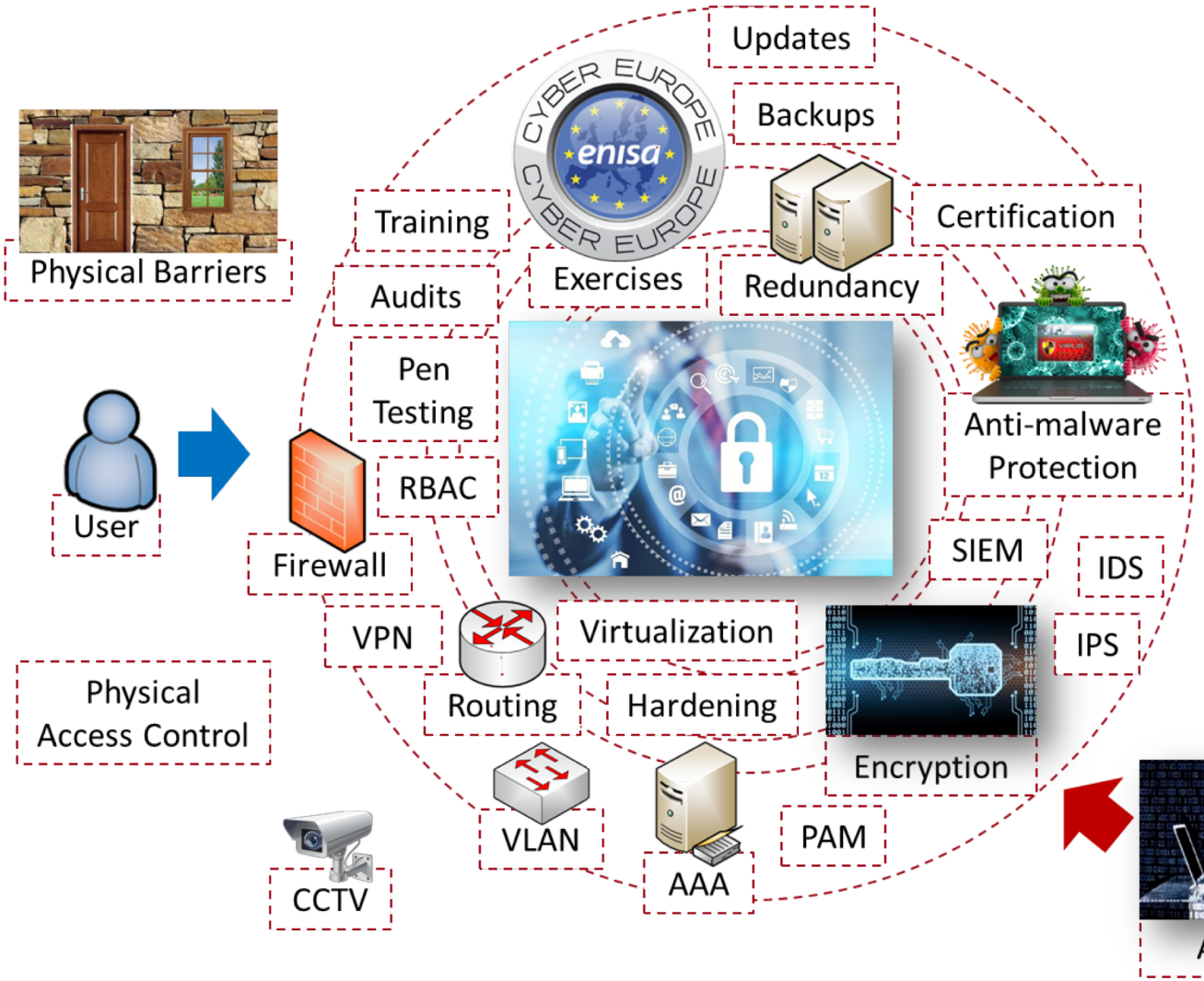
edp distribuição

OT cyber security targets combines into areas of focus the strategy of EDP Distribuição and the practices of the EDP Group. Security anomaly detection is a key component for strengthening incident detection and response capabilities.

OT Strategic Objectives

1 Broadening the Cyber Security perimeter in the Digital Grid and Mission Critical Systems	▪ **Coverage of all Digital Grid assets** from a cyber and physical security perspective (Priority for Substations and Smart Metering devices) ▪ **End-to-end control and monitoring** of assets and related events
2 Strengthen incident detection, response and recovery capabilities	▪ **Reducing organization risk** by reducing the potential impact of cyberattacks ▪ Improve procedures to **reduce detection and recovery time** after cyberattacks
3 Ensure Cyber Security Standardization and Compliance in line with EDP Group	▪ **ISO27001 standard adoption** and continued risk management ▪ **Compliance with applicable regulations** under the scope of Cybersecurity and Privacy
4 Enable employees as the 1st line of Defense (training and awareness)	▪ Developing **Cybersecurity awareness culture** on all employees ▪ **Advanced training** of cybersecurity teams
5 Strengthen national and international partnerships for info-sharing & best practices	▪ **Improved ability to detect and respond** to incidents with inter-organizational impact ▪ Continuous update of **cybersecurity benchmarking** and collaboration

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

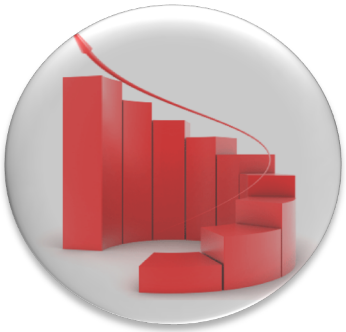


- Firewalls: ACLs
- Antivirus: malware signatures
- IDS/IPS: attack signatures
- SIEM: filters
- Etc.

There is a clear paradigm shift in the energy sector, which carries many new and complex challenges for DSOs, that require a profound business transformation.

Historical Challenges

Quality of Service



Operational Efficiency

- **Supply customers with high quality of service**
- **Minimize OPEX and CAPEX**

New Challenges

Advanced Metering Infrastructure

Renewables and Distributed Generation

MV/LV automation & sensoring

Smart Grid

Electric vehicle

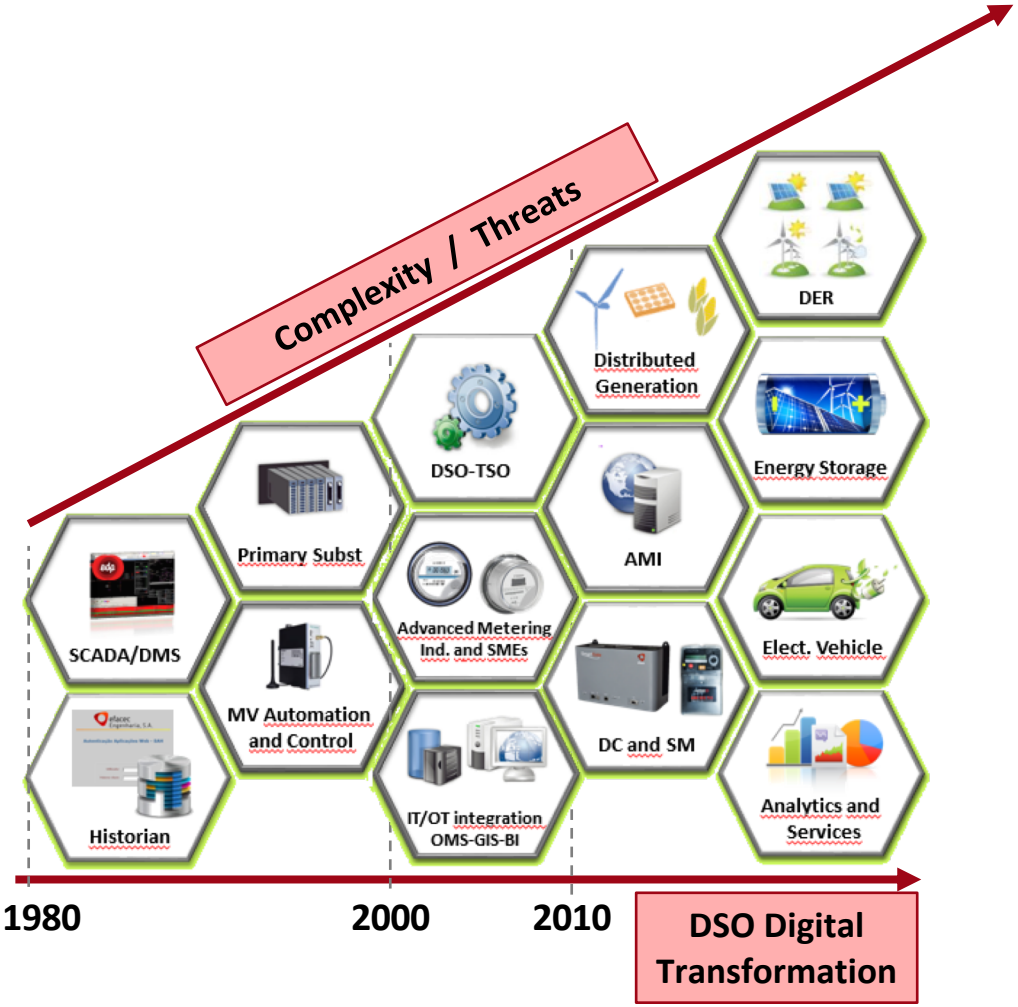
Energy efficiency and new business models

A smarter distribution grid to new challenges

- **New ways of planning and managing the grid (e.g. DG, bidirectional energy flows...)**
- **More information to customer energy efficiency**
- **New technologies (e.g. energy storage) and new business models (e.g. DSM, dynamic energy prices...)**
- **EV integration (e.g. V2G, smart charging...)**

edp distribuição

The DSOs Business and Infrastructures are increasingly digitizing, driving a Digital Grid transformation and new challenges.



Exposure	• Everywhere • Multiple connections • Millions of Nodes
Communications	• Multiple Standard protocols & networks
Systems	• Complex and highly Interconnected
Human Resources	• Hundreds in & out • Remote Access
Security Approach	• Perimeter Security • Defense in depth • Something different

edp distribuição

DSOs are facing different and complex threats accompanying its digitalization, having to deal with the risks of cyber-based Blackouts.

December 2015 - Ukraine:

- **3 DSOs compromised**
- **250.000 people affected**
- **1 to 6 hours to recover**

… and it could have been worse!

December 2016 - Ukraine:

- **1 TSOs compromised**
- **People affected – tbc**
- **Swift recover**

CNET › Security › Ukraine blackout is a cyberattack milestone

Ukraine blackout is a cyberattack milestone

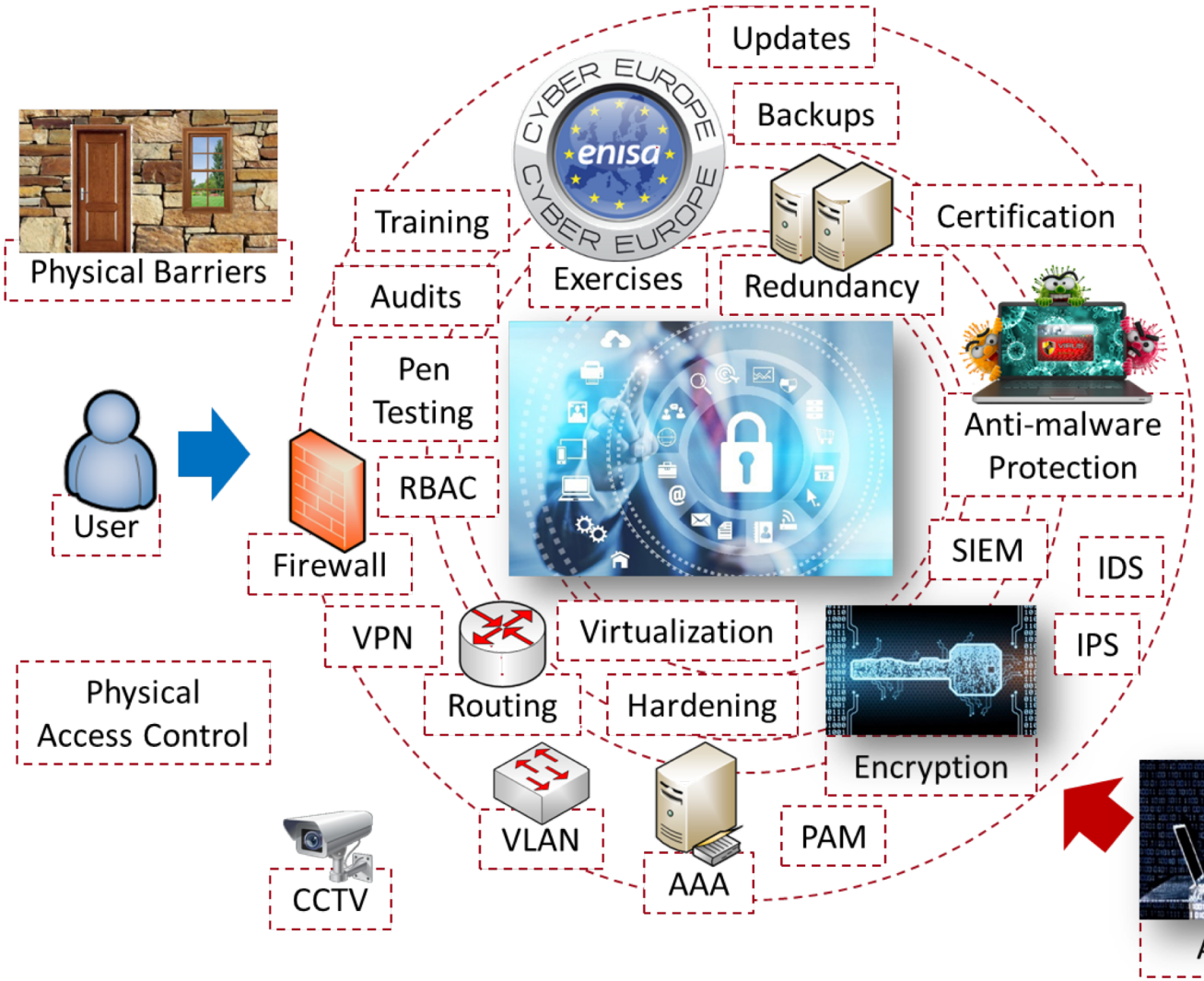
Hundreds of thousands of homes were left in the dark in what security experts say was a first for hackers with ill intent.

The Age of Hacker-Caused Blackouts Is Upon Us

A malware attack left thousands of homes without power in Ukraine and this is only the beginning.

edp distribuição

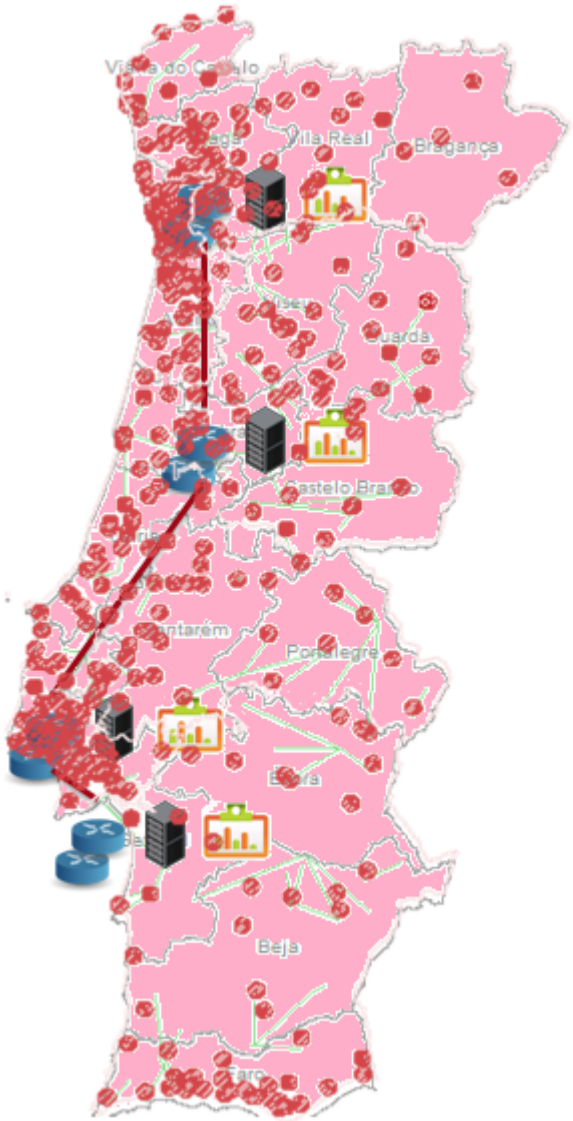
OT cyber security is highly dependent on existing knowledge of the processes and infrastructure, with zero tolerance for failure. Moreover, traditional IT security solutions do not provide visibility or control over specific industrial protocols, such as IEC 104, 61850, DLMS, etc.

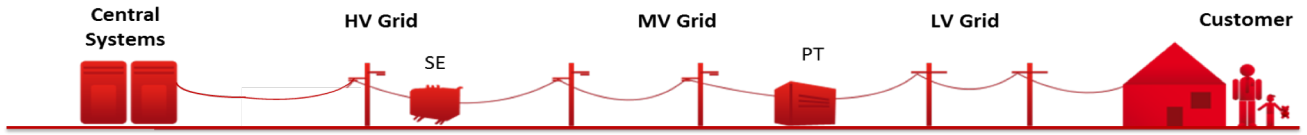


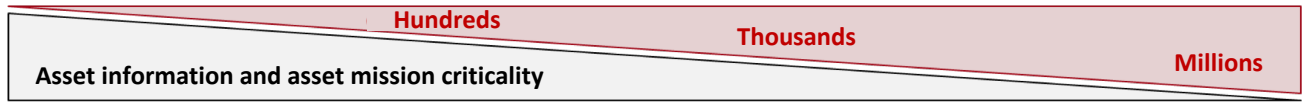
- Visualizing commands in context is crutial for a real **understanding** of the network to be protected.

- Allowing only a set of commands between two machines might **prevent** a potential blackout.

The high dependence on user knowledge and lack of visibility are identified risks in the ISO 27001 ISMS certification project, which foresees 5 stages, each adding new people, processes and technology to the previous scope, according to their relevance and criticality to the management and operation of the critical information infrastructure.







Stage 1: Communications network

Stage 2: Infrastructure and Applications

Stage 3: Primary Substations' Protection, Command and Control Systems (HV)

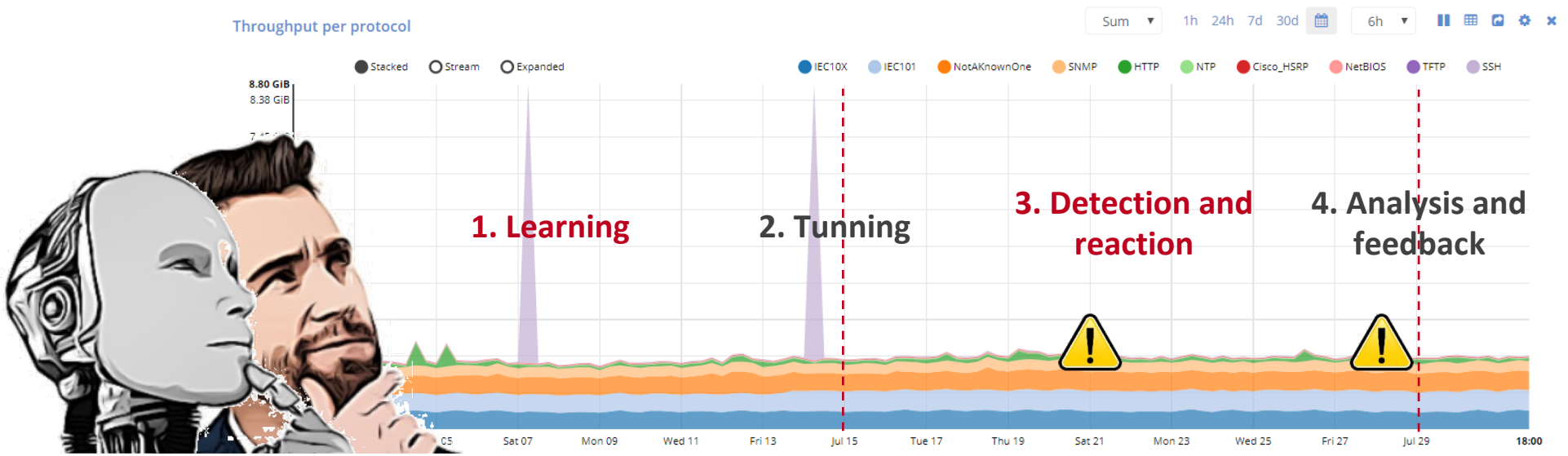
Stage 4: Secondary Substations and Distributed Automation (MV)

Stage 5: Sensoring (LV)

End-to-End ISMS 27001 SGSI Certification

edp distribuição

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.



RESPONSE AND RECOVERY

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

1. Blacklisting and white listing (error-prone)

- Perimeter protection (firewalls)
- Antivirus
- IDS and IPS
- SIEM, etc.

Human intervention Machine intervention

edp distribuição

The ENCS OT Security Monitoring project provided a requirement basis and enough confidence to develop a proof of concept with one of the analysed solutions.

1

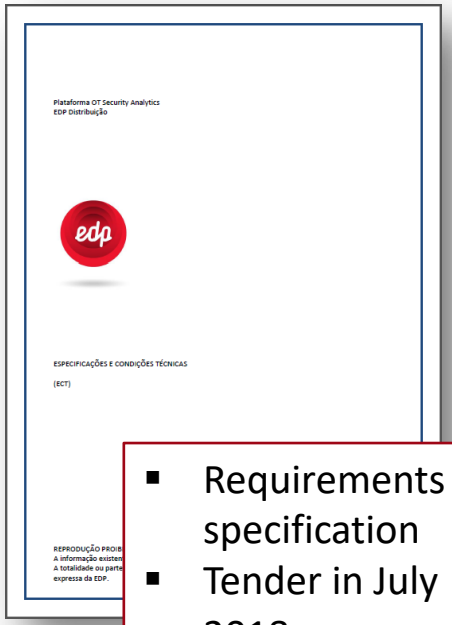
ENCS

- OT Security Monitoring Member project with European DSOs.
- Set of detection use cases.
  - Detecting of Known Attacks
  - Detecting New Hosts
  - Detecting of Unusual Network Connections
  - Detecting Malformed Packets
  - Detecting Unusual Commands or Parameters
  - Detecting Flow-Based Anomalies
  - Detecting Web Attacks
  - Detecting Weak Protocol Configurations
- Analysis of several OT security monitoring solutions.

2

SECURITY MATTERS

- EDP Distribuição proof of concept with silent defence.
  - Practical learning about the solution.
  - Decision for follow up.



3

- Requirements specification
- Tender in July 2018

edp distribuição

The OT security analytics platform for EDP Distribuição's critical information infrastructure shall support (by default or after customization) the following requirements and use cases.

LEARNING

- Baseline learning, including the following parameters:
  - User
  - Source name
  - Source IP address
  - Source geolocation
  - L3 protocol
  - L7 protocol
  - Message content, including support for industrial protocols 104, 61850 and DLMS
  - Number of bytes
  - Source port
  - Destination name
  - Destination IP address
  - Destination geolocation
  - Destination port
  - Network segment
  - Time of communication
  - Duration of communication
  - Frequency of communication
  - Precedence, sequence, etc. between communications

DETECTION AND CORRELATION

- Baseline navigation for system/ network/ security admin learning and stats retrieval.
- Current communications and history navigation, including:
  - Summarized communication stats.
  - Detailed communication data.
- Abnormal activity detection based on baseline comparison.
- Malicious activity detection based on signatures.
- Correlation of alerts, including baseline-based with signature-based alerts.
- Correlation alerts should generate only one user event with the correlated alerts in its details and accessible to the user.

edp distribuição

The OT security analytics platform for EDP Distribuição's critical information infrastructure shall support (by default or after customization) the following requirements and use cases.

DETECTION ENCS OT SECURITY MONITORING

- At least the following detection capabilities:
  - Detecting of Known Attacks
  - Detecting New Hosts
  - Detecting of Unusual Network Connections
  - Detecting Malformed Packets
  - Detecting Unusual Commands or Parameters
  - Detecting Flow-Based Anomalies
  - Detecting Web Attacks
  - Detecting Weak Protocol Configurations

NAVIGATION

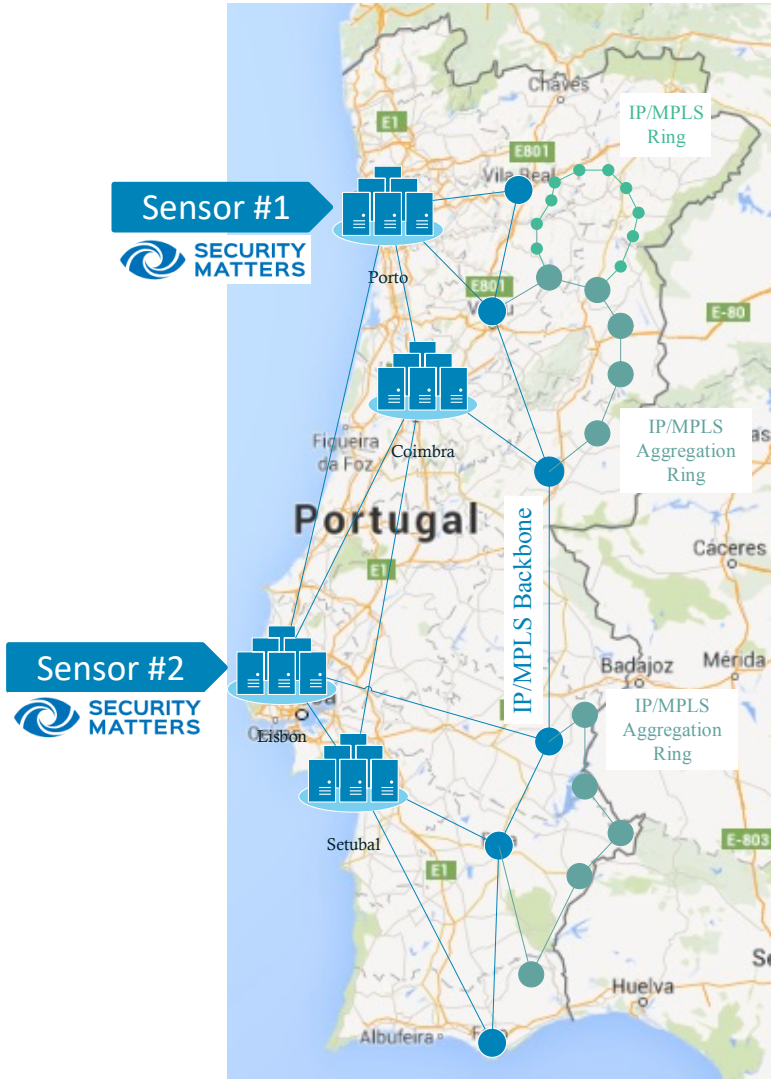
- Ease of navigation; for example:
  - Analysis filters, using as inputs the parameters above.
  - Dashboards and tables.
  - Point and click and drag like interface.
- Extraction of communication and alert information in csv format.
- Extraction of packet capture files, including past events and new events.

INTEGRATION

- Microsoft AD integration for user authentication, including:
  - Only members of a certain AD security group can login and perform admin actions.
  - Only members of a certain AD security group can login and perform read actions.
- Microsoft DNS integration for reverse name resolution.
- SIEM Microfocus Arcsight integration for security log monitoring, including:
  - Communication of platform security events.
  - Communication of detection events.
  - A set of use case descriptions should be delivered, after being adapted to our own context.
- Microfocus OMi integration for health and performance monitoring.
- SMTP integration for event communication through email.

The tender was launched in July 2018 to implement an initial scope of the EDP Distribuição's OT Security Analytics Platform.

CONTEXT	▪ Evolving OT security analytics solutions ▪ Internal expertise to be further developed ▪ Successful POC with Security Matters
SCOPE RESTRICTION	▪ Security Matters' Silent Defense ▪ 2 sensors (and 1 command center) ▪ Detection only ▪ On request support hours INITIAL SCOPE
MONITORING	▪ 2 years (KPIs to be decided) ▪ Market evolution
EVALUATION & EVOLUTION	▪ Current solution evaluation ▪ Technology and/ or scope evolution



Following the adjudication in late October, 2018, a 4 stage project plan was designed with SecurNet, with the support from Forescout (who acquired Security Matters).

SECURITY ANALYTICS PROJECT

Secur.Net
Always online, always secure!
FORESCOUT

Adjudication
October 2018

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

Site surveys to sensor deployment locations are critical to avoid delays and extra expenses. Beyond the VLANs to monitor and the mirroring to be configured, check if you need extra fiber or copper cables, and where and how to install them.

SECURITY ANALYTICS PROJECT

Secur.Net
Always online, always secure!

<) FORESCOUT

Adjudication
October 2018

Stage #1
November 2018

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

- Sensor sites surveys

Stage #2
December 2018

- HW & SW instalation
- Initial tests
- Learning start

Stage #3
January 2019

- Finetuning
- Scripting

Stage #4
February 2019

- Acceptance tests
- Training and SOC integration
- Solution documentation

edp distribuição

LESSON #2

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

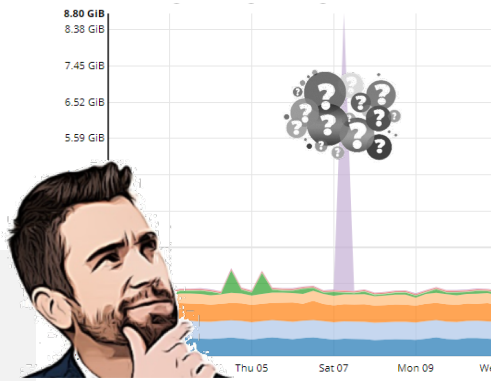
SECURITY ANALYTICS PROJECT

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

Adjudication
October 2018

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

Stage #3
January 2019
- Finetuning
- Scripting

Stage #4
February 2019
- Acceptance tests
- Training and SOC integration
- Solution documentation

edp distribuição

LESSON #3

A POC is very important to understand the technology, and its lessons are valuable for an eventual implementation, but beware of the gap between the POC scope and the rollout scope, and of the infrastructure evolution in the meantime.

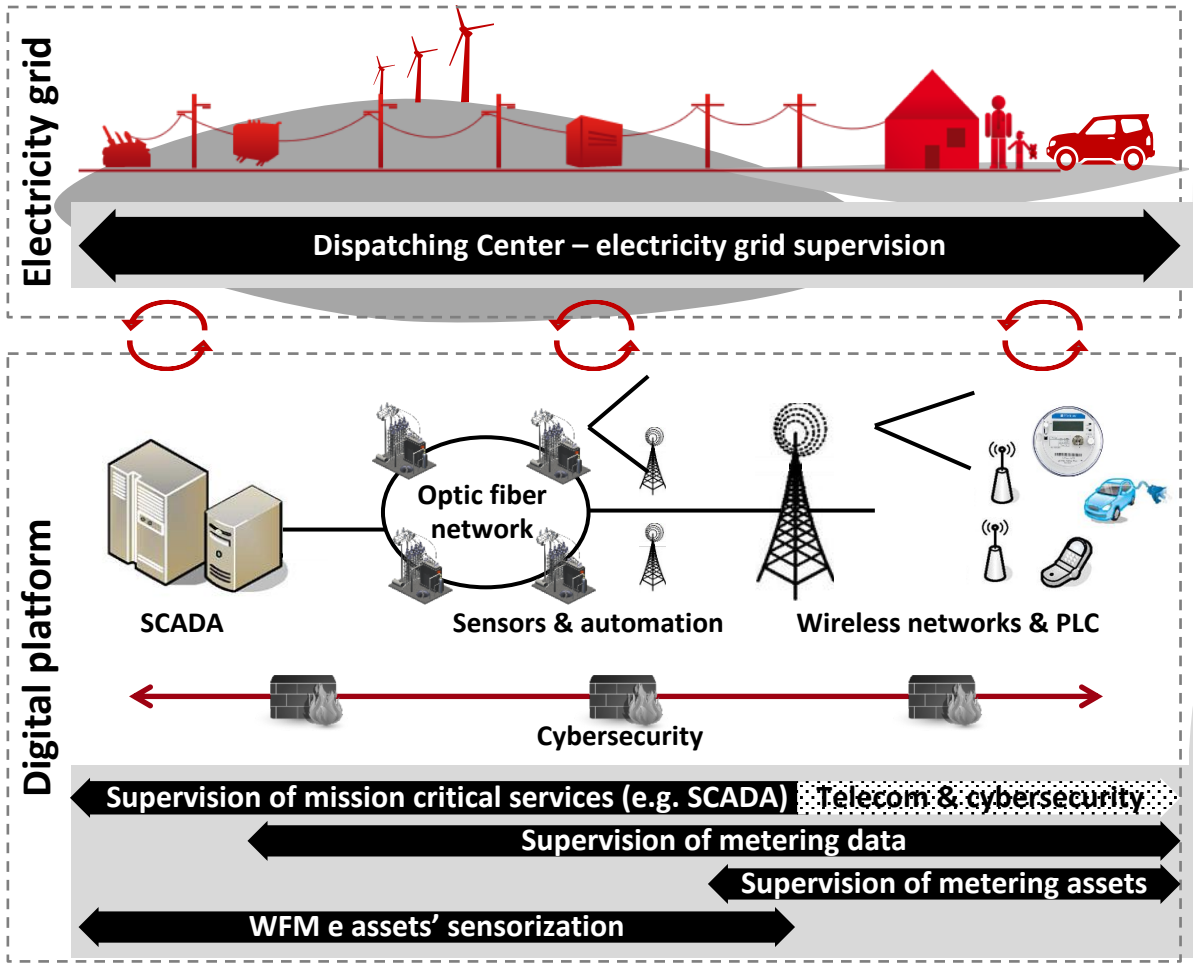
POC lessons

- Aggregation of field communications reduces the number of required sensors. — Stage #1
- POC system configurations (e.g., learned models, LDAP and SIEM integration). — Stage #2
- Using the firewall ACLs to validate the initial self-learned model accelerates fine-tuning. — Stage #3
- Security analytics SIEM use cases are essential for integration of the solution in the incident detection and response process. — Stage #4
- Human intelligence and experience required for fine-tunning and alert analysis. — Always

edp distribuição

The OT Security Analytics solution will be a key component of the EDP Distribuição's Integrated Supervision Center, providing visibility over previously unseen potential threats.

Smart grid operations ecosystem

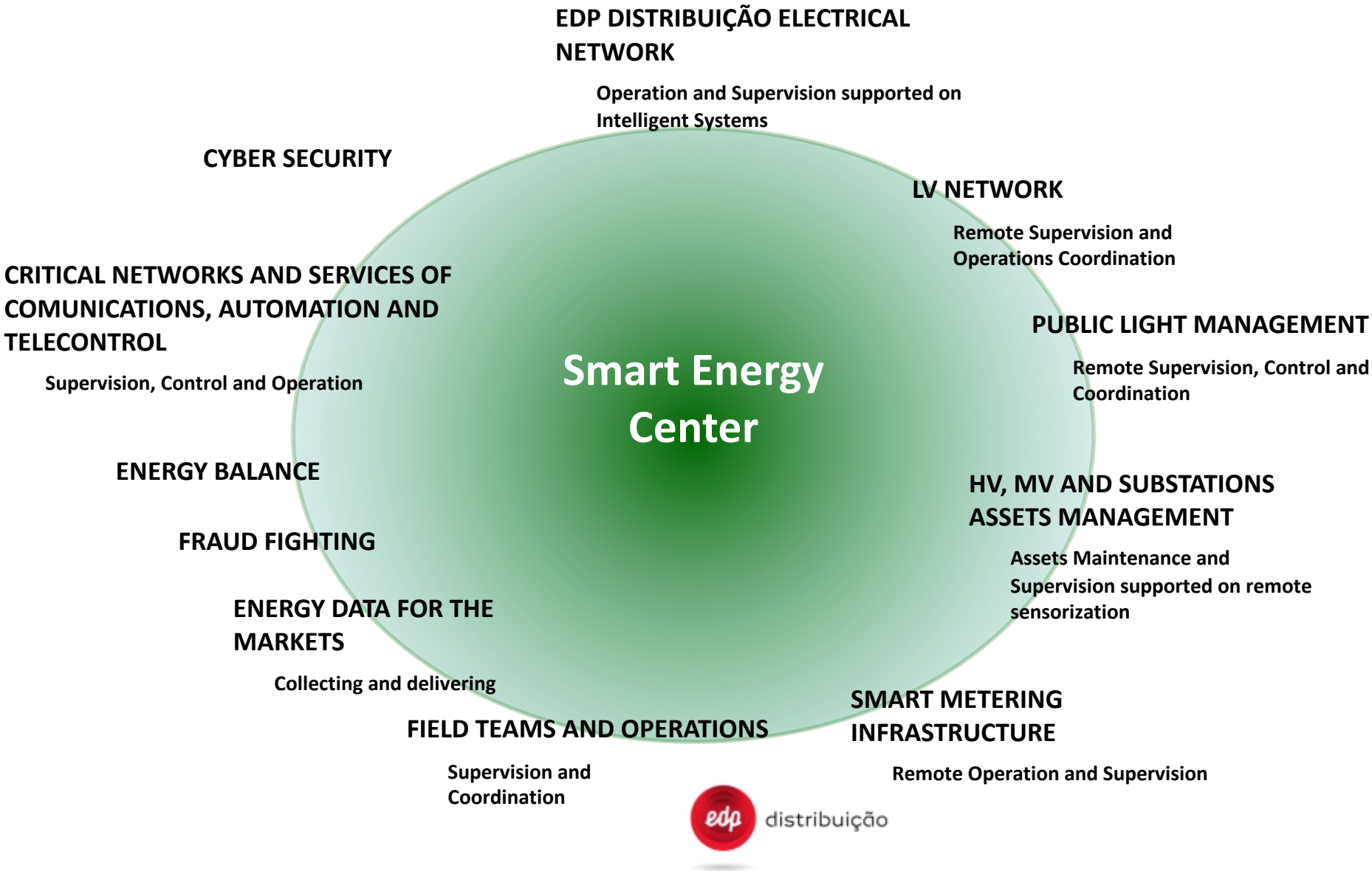


Smart Energy Center

- **Integration of all operation and supervision centers, ensuring real time or near real time operations**
  - Asset Maintenance Operations and WFM
  - Grid Automation
  - Energy Management
  - Dispatch Center *(future vision)*
- **Better communication** between teams
- **Integration of** technical and functional **skills**

edp distribuição

EDP Distribuição faces new challenges on operate and supervise an electrical grid with increasingly intelligence and complexity, daily generating huge amounts of data. Information criticality and interdependency leads to the need of the different operational units to share the same physical space, with high security and redundancy requirements.



Thank you for your attention

Nuno Pereira
nunoemanuel.pereira@edp.pt

IDS Implementation and Integration