



Italian National Agency for New Technologies,  
Energy and Sustainable Economic Development

**RdS**  
RICERCA DI SISTEMA

# Securing the Power Grid: Strategic Methodologies and Technical Solutions

*Massimo Celino*

**ENEA**

February 9, 2025

ITASEC 9/2/2026

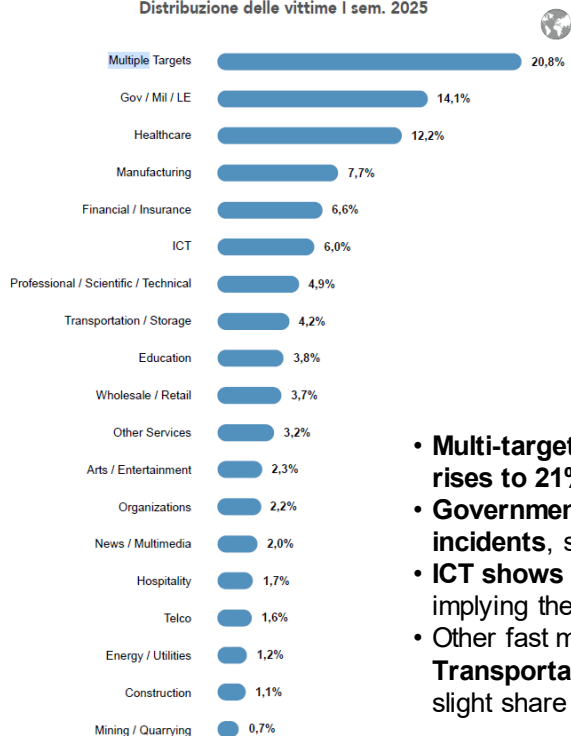


1101 0110 1100  
0101 0010 1101  
0001 0110 1110  
1101 0010 1101  
1111 1010 0000

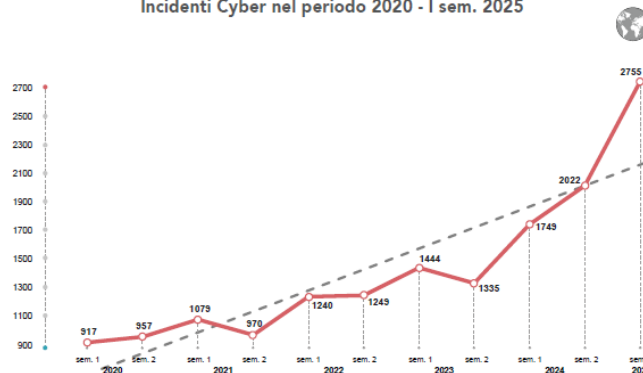


# Cyber Incidents by Sector: H1 2025 vs 2024

Distribuzione delle vittime I sem. 2025



Incidenti Cyber nel periodo 2020 - I sem. 2025



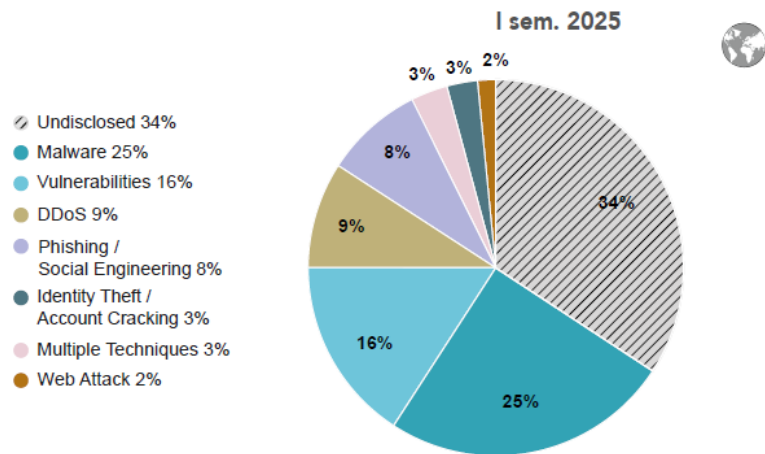
© Clusit - Rapporto 2025 sulla Cybersecurity - Aggiornamento giugno 2025



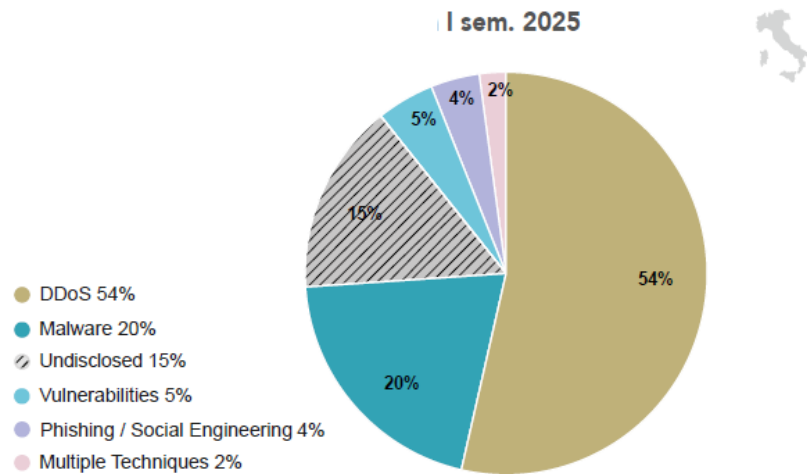
- **Multi-target incidents are surging:** in just H1 2025 they already exceed **85% of 2024's total**, and their **victim share rises to 21% (+3pp)**.
- **Government is “stable” in share (14%) but accelerating in volume:** by mid-2025 it's already at **75% of all 2024 incidents**, suggesting strong momentum even without a percentage-share increase.
- **ICT shows no meaningful movement:** it follows a **similar trajectory to 2024** with **no significant trend shift**, implying the threat level remains steady rather than rapidly worsening relative to other sectors.
- Other fast movers by mid-year vs 2024 totals: **Manufacturing (90%)**, **Professional/Scientific/Technical (94%)**, and **Transportation/Storage (110%)**; **Healthcare** is also high in absolute pace (**67% of 2024 in six months**) despite a slight share decline.

© Clusit - Rapporto 2025 sulla Cybersecurity - Aggiornamento giugno 2025

# Italy: DDoS Dominates Cyber Incidents



© Clusit - Rapporto 2025 sulla Cybersecurity - Aggiornamento giugno 2025

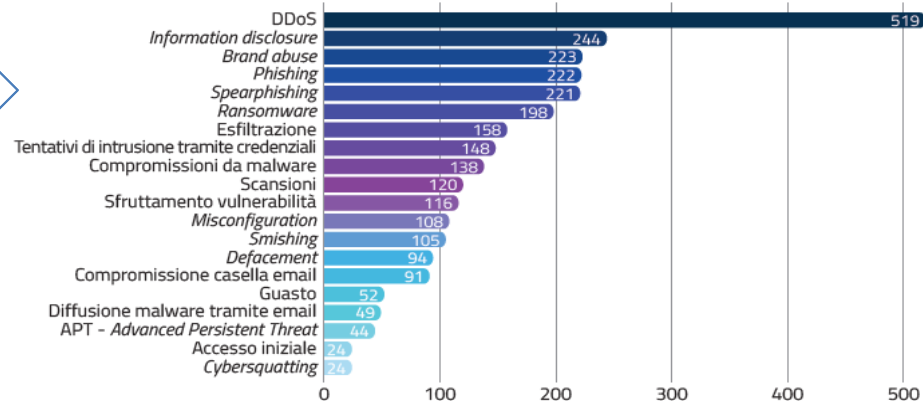


In **Italy**, the predominant technique in recorded incidents is DDoS, which has returned to 1st place as in 2023: it accounts for 54% of incidents, a value far higher than the global figure (9%). This confirms the correlation with hacktivism campaigns, which often use DDoS to disrupt the operations of the victim organization/institution's services and to draw greater attention to their cause. In fact, disrupting internet services is an effective way to make a message of denunciation or protest visible to the public.

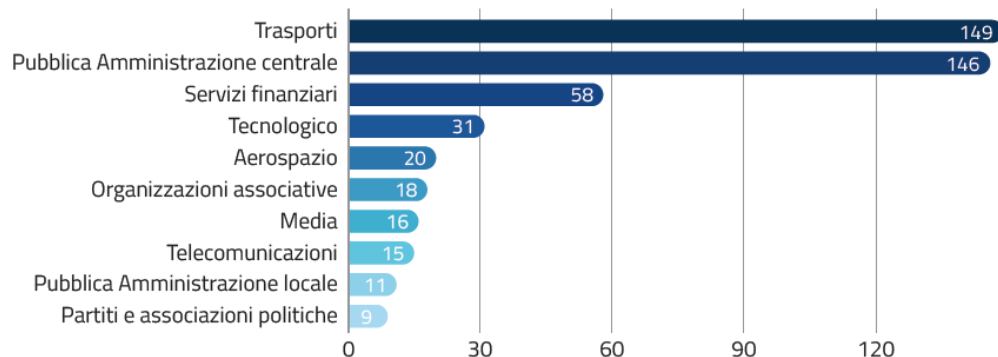
# Cyber events in 2024



Threats detected in the  
cyber events handled in  
2024

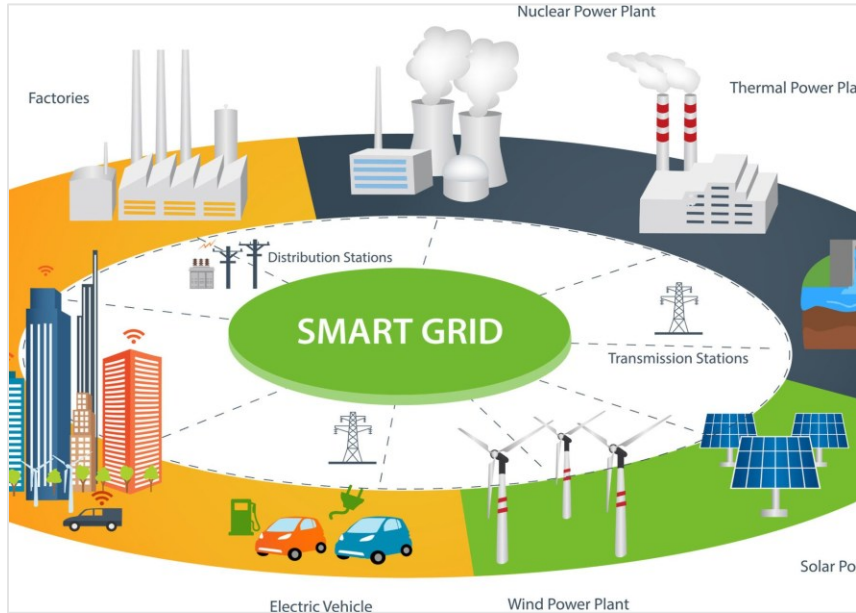


Number of DDoS events by the  
victim's economic sector of  
activity



# Why are Smart Grids a “special” target?

## Smart grid



## Characteristics of Cyber-Physical Systems (CPS) and inherent vulnerabilities

- **Cyber-Physical Nature:** A digital attack doesn't affect only data; it also degrades the availability and integrity of the electricity service, causing physical damage to equipment and end users.

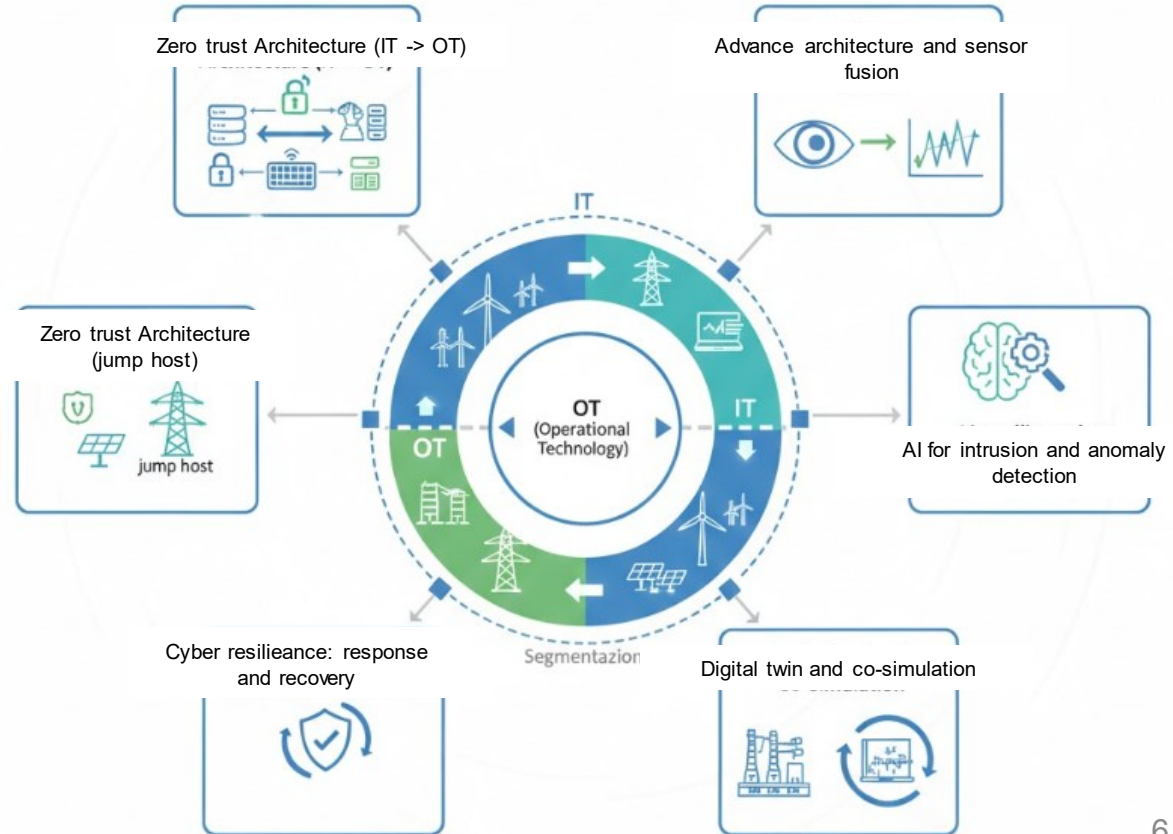
### The 3 Critical Challenges:

- **Expanded Attack Surface:** Integration between the IT world (offices, cloud) and OT/ICS (SCADA, smart meters, substations, microgrids).
- **Real-Time & Safety Constraints:** It's not feasible to apply aggressive security blocks that could cause blackouts or instability.
- **Legacy Systems:** Industrial assets with decades-long lifecycles, hard to update and based on protocols that were created without “security-by-design.”

# Smart Grid Security: Global Research Trends

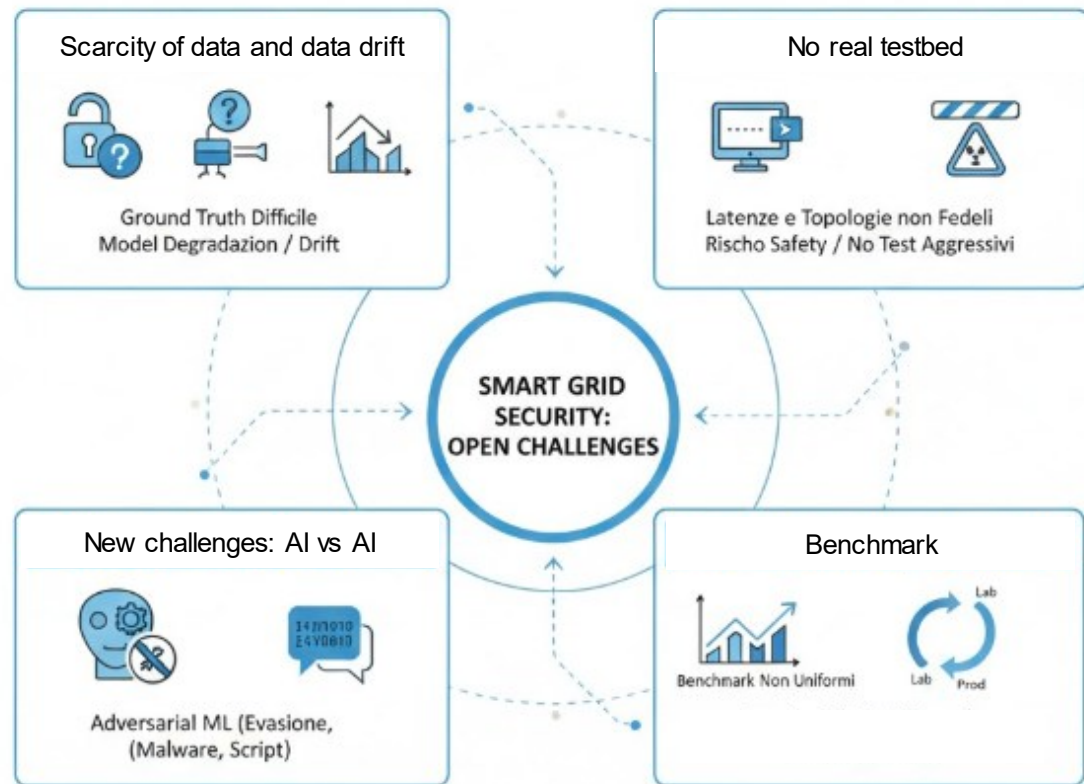
## IT/OT Convergence

A Smart Grid is no longer an isolated system, but an ecosystem where traditional information technology (IT) and the operational technologies of power plants and substations (OT) are merged together.



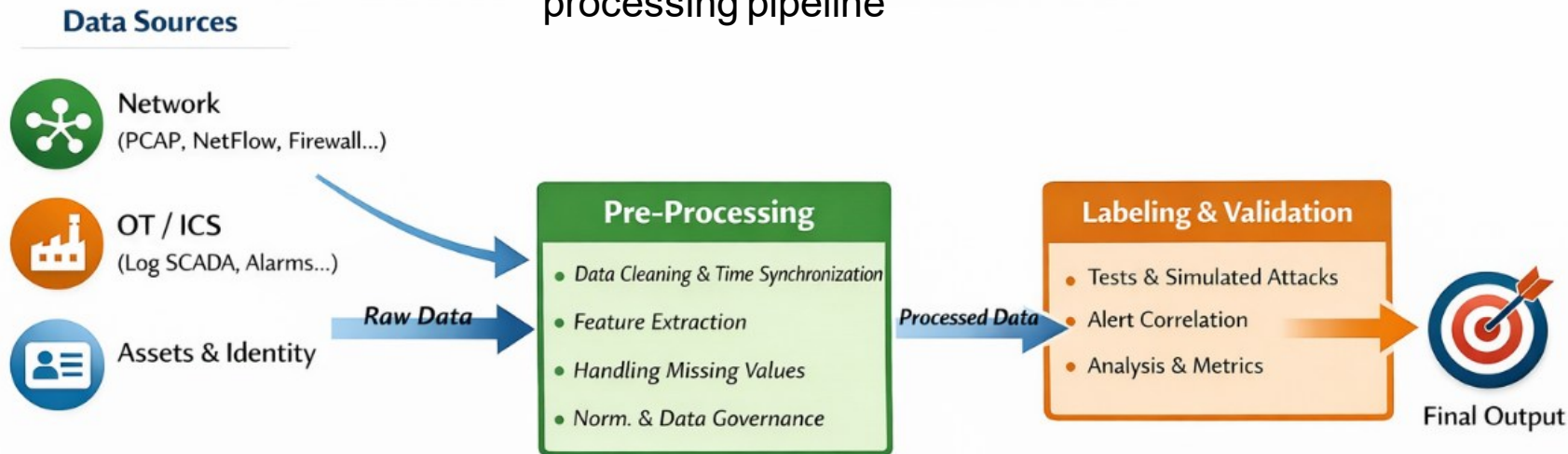
# Open challenges

Four gaps to be addressed by the research in the cybersecurity for smart grids



# Data processing pipeline

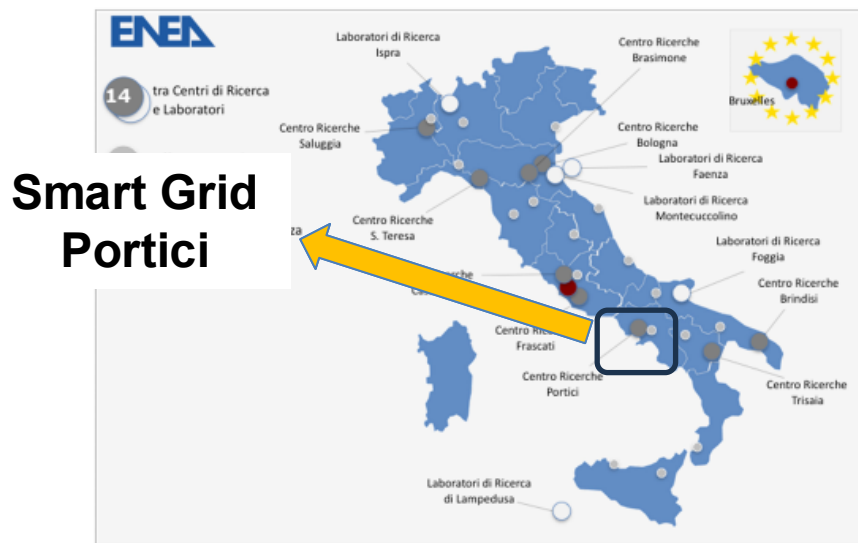
To understand how a modern defense system makes decisions, we need to look at its data processing pipeline





# Computing infrastructure testbed

Implementation of a high-performance computing infrastructure for the cyber control of cyber-resilient smart electrical grids.



Implementation of a data network infrastructure including a group of sensors/actuators hosted on a dedicated VLAN, network devices needed for the project's purposes, a firewall, a computing system, and a storage system.

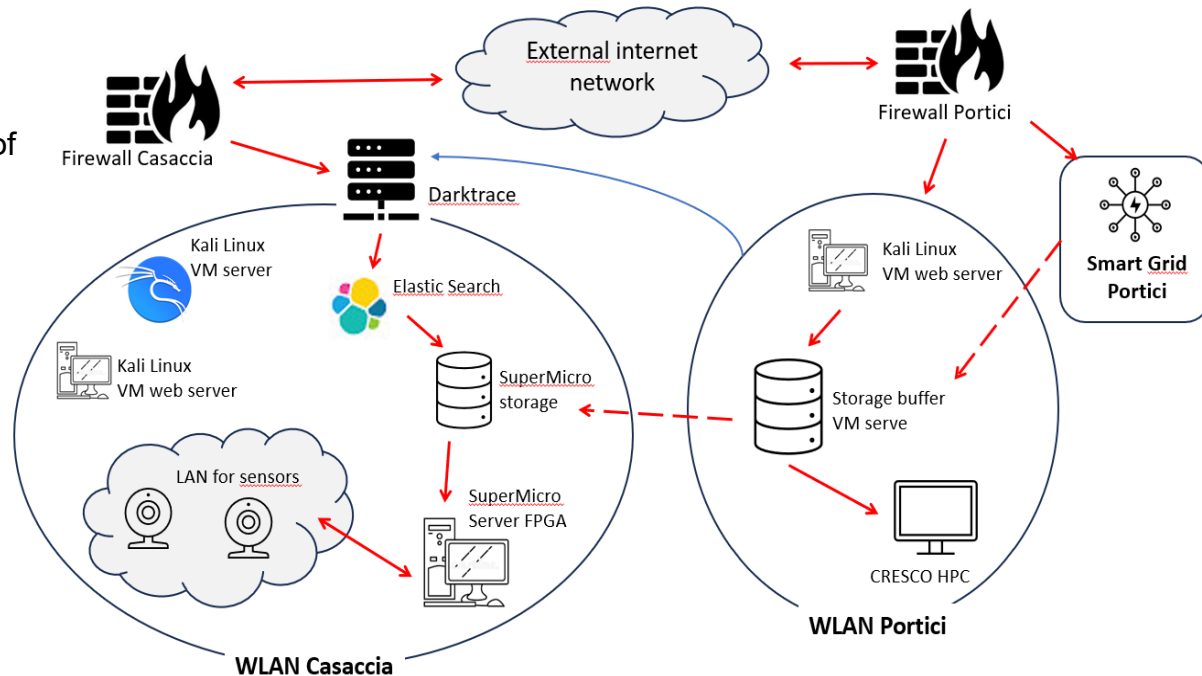
- Implementation of the network infrastructure with high security performance, based on next-generation **Palo Alto** firewalls and the **Darktrace Threat AI Analyzer**
- Implementation of a low-power HPC computing hardware infrastructure consisting of a **Supermicro** compute server and storage
- Simulation of malicious traffic in order to test the data flow generated and handled by the infrastructure
- Description of the software solutions that make it possible to index, store historically (archive), and pseudo-anonymize the data, in compliance with current privacy regulations.

# Distributed platform for cyber data

## OBJECTIVE

Build an infrastructure that, in addition to delivering high computing power, is able to guarantee—in real time—the cybersecurity of the data traffic generated by the electrical grid.

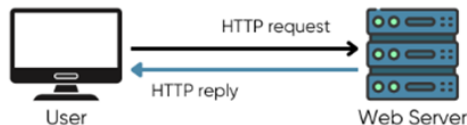
- **Integrated IT system** based on containers and resource virtualization.
- **Platform for stream processing** of messages coming from multiple communication data sources, following a producer–consumer approach.
- **Data analysis platform** using machine learning and artificial intelligence algorithms.
- **Dashboard** for monitoring and managing the components of the integrated stream analytics system.



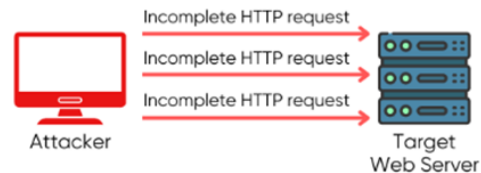
# DDoS Slowloris attack

A **Distributed Denial of Service (DDoS) attack** aimed at making a server's service unavailable to legitimate users. It is difficult to detect because it uses **low bandwidth (LOW)** and slowly consumes the server's resources over time (**SLOW**).

Normal HTTP Request - Response Connection



Slowloris Attack



A **Slowloris attack** exploits resource limits by sending multiple partial HTTP requests to a web server. In this way, the attacker can occupy all available connections on the web server and prevent other legitimate users from accessing the website.

The DDoS attack was generated using the **SlowHTTP Test** tool available on **Kali Linux** servers.

# Brute force attack

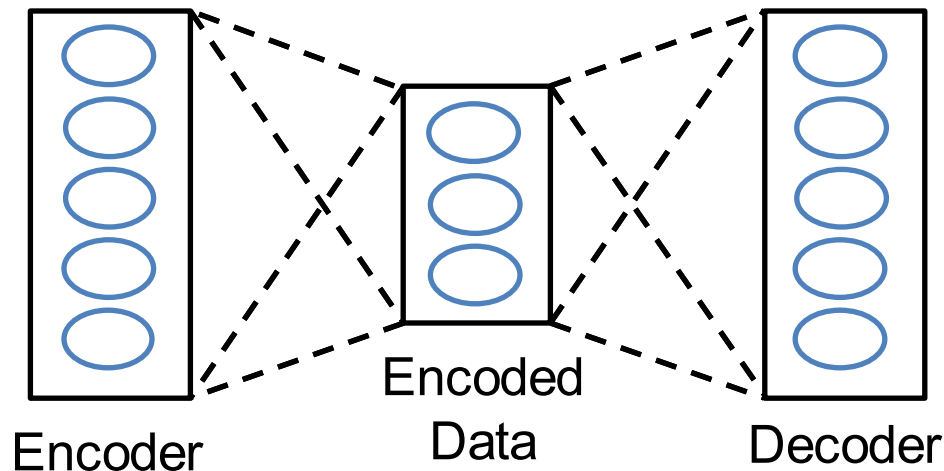


A brute-force attack consists of discovering a password by trying all possible combinations of letters, special characters, and numbers according to predefined criteria.

The brute-force attack used for the development of the project, specifically a dictionary attack over the SSH protocol, was generated on the Kali Linux servers using the Hydra tool.

# Unsupervised neural networks

- **Design of an innovative intrusion detection mechanism for energy networks based on autoencoders**, i.e., an artificial neural network capable of detecting anomalies without the need for a training phase using labeled data.
- **Prototype implementation** of the designed system and its release as an **open-source** solution.
- **Experimental evaluation** of the system using real-world data provided by **ENEA**, with results showing a **high level of accuracy** in detecting cyber intrusions.



# Future directions

- Development of AI-based software for intrusion detection in energy networks, to be integrated into ENEA protection devices (UniRM3).
- Design of an innovative AI-based system for the detection and automated response to intrusions in energy networks (UniRM3)..
- Identification of threats in the automated control of **cloud-native** smart grids (UniTN).
- Development of an innovative system for modeling and detecting **adversarial ML** intrusions in energy and communication networks (ENEA).
- Design of a prototype environment for implementing **large-scale attacks and automated response**, leveraging AI techniques for intrusion detection in energy networks (ENEA).
- Analysis and implementation of a **blockchain** for energy smart grids on conventional architectures (ENEA).

# Acknowledgments

## ENEA

- Angelo Mariano, Serena D'Onofrio, Paolo Palazzari, Fiorenzo Ambrosino, Michele Casà, Luigi Acampora.
- The ENEA CRESCO Team

## UniRM3

- Riccardo Torlone, Stefano Iannucci, Tommaso Caiazzzi, Simone Albero

## UniTN

- Domenico Corona



Massimo Celino  
[massimo.celino@enea.it](mailto:massimo.celino@enea.it)

Many thanks for your kind attention!