Co-funded by the European Union

Technical University of Madrid (UPM), 5/5/25

CYBERSECURITY at UPM

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them."

Víctor A. Villagrá
Director of UPM Cybersecurity Master

UNIVERSIDAD POLITÉCNICA DE MADRID

Cybersecurity

The evolution of the classical Information Security research area, where the focus is no longer just the Information, but also the services, systems, platforms, appliances, etc.

Capabilities

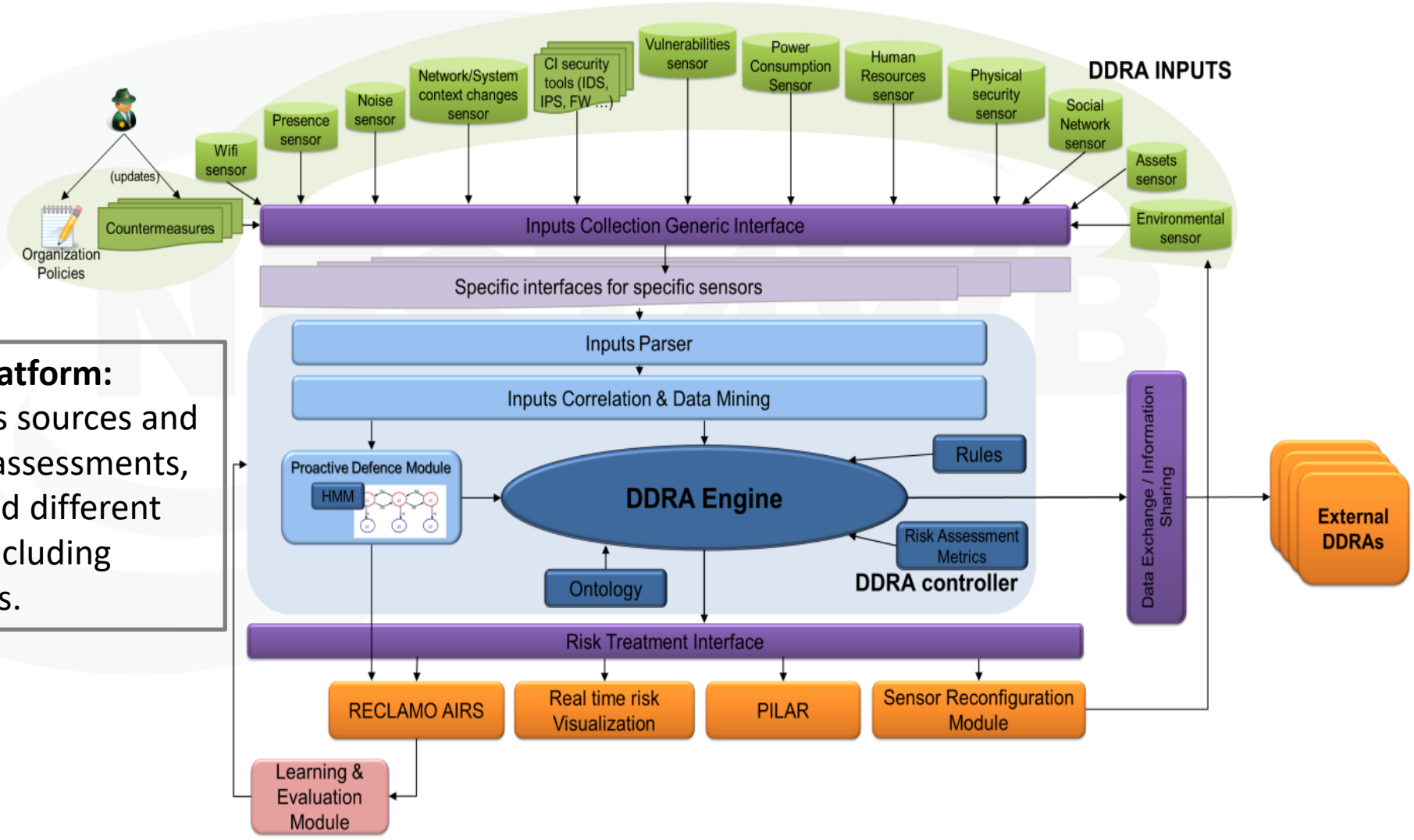
- Some of the recent work in this area by our UPM research groups include:

- Cybersecurity Awareness:
  - Dynamic Risk management, with the integration of heterogeneous sensors
  - Proactive detection of multistep attacks
  - Machine learning technologies for event correlation and intrusion detection

- Automatic Intrusion Response Systems
- Vulnerabilities on IoT devices
- IoT botnets detection
- Applicacion of Attribute-based Encryption for context-based DLP

Cybersecurity Awareness: Dynamic Risk Management Platform

Dynamic Risk Management platform:
Collection from heterogeneous sources and dynamic modifications of risk assessments, including proactive defence and different countermeasures strategies, including automatic intelligent responses.



NEST4WB

Co-funded by the European Union

Cybersecurity Teaching

THREATS: KNOW YOUR ENEMY

Motivation: knowing the threats and the enemies

Attacks targets

How are they done?

Comnsequences

PLANNING AND GOVERNANCE

Design of a Cybersecurity Policy

Risk Assessment and Management

Law Compliance

ISMS Standars

Certification and Auditing

CYBERSECURITY TECHNOLOGIES

Understanding foundations, objectives and how they work

Choosing technology for your policy

Technologies for all the areas:

- IT envorinoments: systems, networks, data, etc.
- Cloud, IoT, Industry 4.0, Radio, etc.

CYBERSECURITY OPERATION

Process deployment: SOC

Montoring and Reaction

Contingency Plans

Training, exercices

Ethical Hacking

Forensic Analysis

Reverse Engineering

Threat Intelligence

Horizontal skills:

Management and leadership, Business Fundamentals, etc.

KNOW YOUR ENEMY: CYBERSECURITY THREATS

- Understand the actors, motivations and tools used by the attackers
- Two main threat sources:
  - Human Threats: people are the weakest link
    - Social Engineering techniques
  - Technological Threats:
    - Exploiting software and configuration failures
- Best strategy: prevent them
  - User training
  - Security in software lifecycle

CYBERSECURITY GOVERNANCE

- Design of a Complete Organization Cybersecurity Policy:
  - Risk Assessment and Management
  - Compliance Issues: Data Privacy (GDPR), etc.
  - Best Practices and ISMS standards
  - Business continuity
  - Training, etc.
- Cybersecurity Master Plan

CYBERSECURITY TECHNOLOGIES

- Understand current cybersecurity technology
  - Adapted to your policy (not the other way round)
- How to protect your different areas:
  - Your Corporate IT Infrastructure, but also…
    - Your resources in the Cloud
    - Your Industry 4.0 devices
    - Your network communications
    - Your IoT devices, etc.

CYBERSECURITY OPERATION

- Deployment of the cybersecurity processes
  - Complete Event and Incident Monitoring
  - Threat Intelligence: knowledge sharing
  - Threat Hunting
  - Application of AI and Machine Learning to Cybersecurity
  - Cybersecurity Awareness
- Incident Response Plans
- Disaster Recovery plans

NEST4WB

Co-funded by the European Union

UPM Cybersecurity Masters: 60 ECTS

THREATS: KNOW YOUR ENEMY

CSCA: CYBERSECURITY. CONTEXT AND THREATS

PLANNING AND GOVERNANCE

DECC: DESIGN OF CYBERSECURITY CORPORATE STRATEGIES

SGSI: INFORMATION SECURITY MANAGEMENT SYSTEMS

SEFC: PHYSICAL SECURITY AND CONVERGENCE

CYBERSECURITY TECHNOLOGIES

SECA: ACCESS CONTROL SECURITY SERVICES

SESR: NETWORK SECURITY SERVICES

PRSS: SERVICES AND SYSTEMS SECURITY

PRIN: INFORMATION SECURITY

SEDS: SOFTWARE DEVELOPMENT SECURITY

CYBERSECURITY OPERATION

GROC RISK MANAGEMENT AND CYBERSECURITY OPERATIONS

AUTS: SECURITY TECHNICAL AUDITING

EVFO: FORENSIC EVIDENCES

IIAM: REVERSE ENGINEERING AND MALWARE ANALYSIS

Horizontal skills:

***DECC*: DESIGN OF CYBERSECURITY CORPORATE STRATEGIES.**