Security Conference

The proposed Framework for AI good Cybersecurity Practices (FAICP)

Presented by: Professor Nineta Polemi

19/10/2023

Agenda

- Rational
- Aim and Objectives
- Structure & Characteristics of Framework
- Going deeper
- Training needs
- Conclusions

FAICP – A scalable framework for AI-related cybersecurity good practices (ENISA 7/6/23)

Aims & Design Principles of FAICP

Aim: a framework for AI good cybersecurity practices (FAICP) necessary for securing the ICT infrastructures and the hosted AI, taking into account the AI life cycle which goes beyond ML (from system concept to decommissioning) and all elements of the AI supply chain, associated actors, processes and technologies;

Design Principles

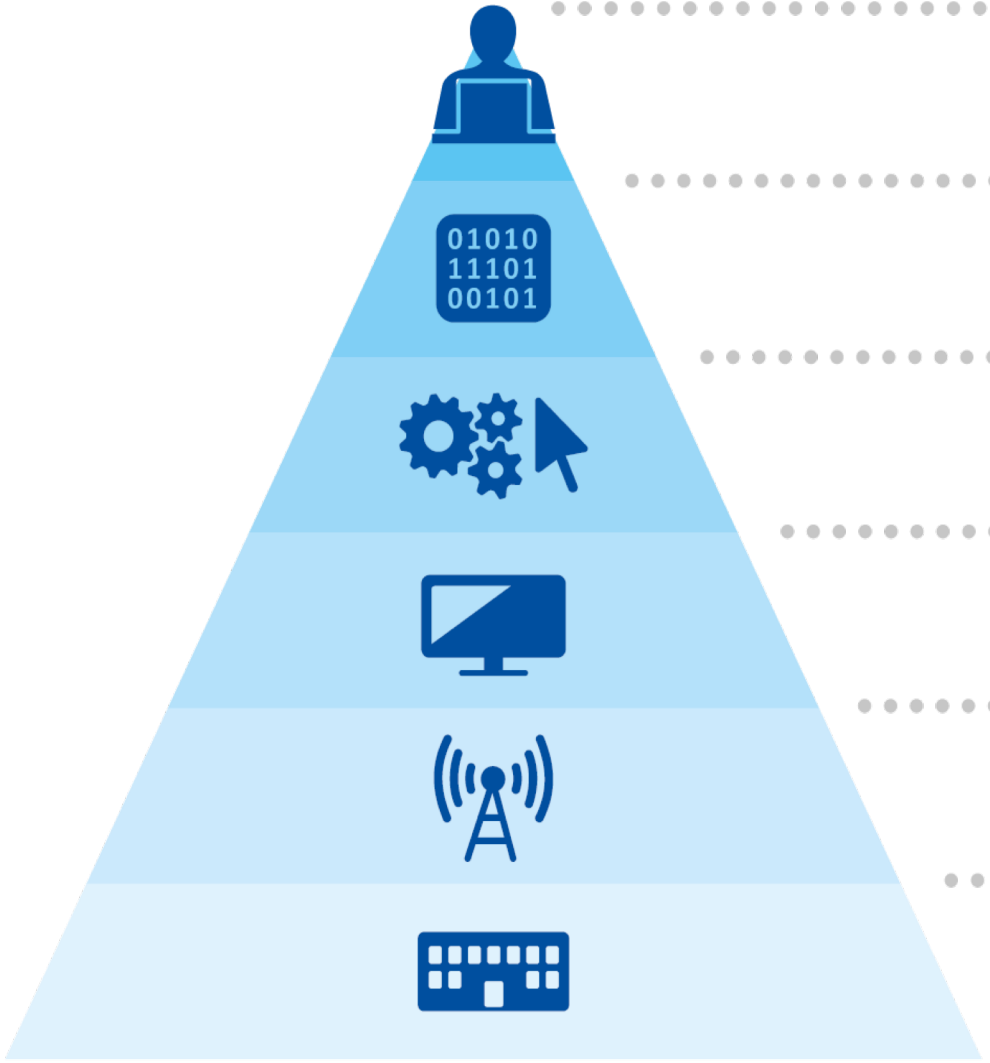
- **Inclusive**. Uses past experience and builds upon it.
- **Holistic**. Considers the AI systems within the ICT infrastructure and embraces all cybersecurity practices needed around and within the AI systems and their individual components.
- **Expandable**. Its generic and yet embracing structure can include future developments in all three layers.
- **Multi-use**. Useful to AI stakeholders independently of the sector.
- **International**. Includes European and international efforts, standards and recommendations.

Benefits & Beneficiaries

Benefits:
Help stakeholders to identify the existing standards and best practices in order to secure their AI systems, identify their security requirements, monitor and enforce compliance with these requirements.

Beneficiaries: The following stakeholders: developers, integrators, providers, supply chain business partners, users of AI systems, supply chain, EU national competent authorities

AI IS PART OF THE ICT



USERS/PROCEDURES
(physical users, smart objects, security processes)

DATA & DATA PROCESSES
(ad-hoc, proprietary, Big data, data analytics/ management,/training models)

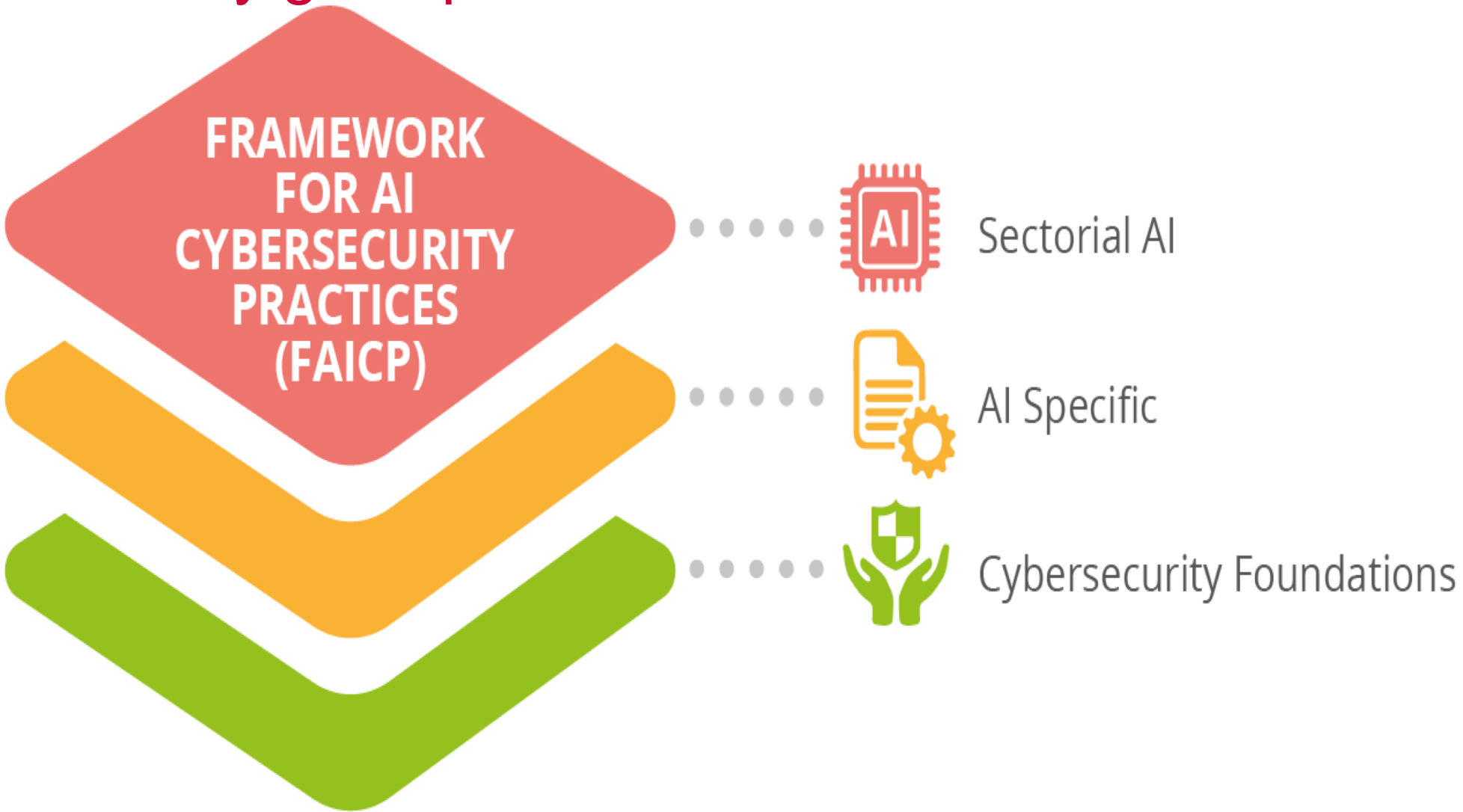
DOMAIN/SECTORIAL E/M-SERVICES
(e-health, e-invoicing, logistics, e-procurement..)

IT APPLICATIONS & TECHNOLOGIES
(ML/AI, IoT, servers, ERPs, smart appliances)

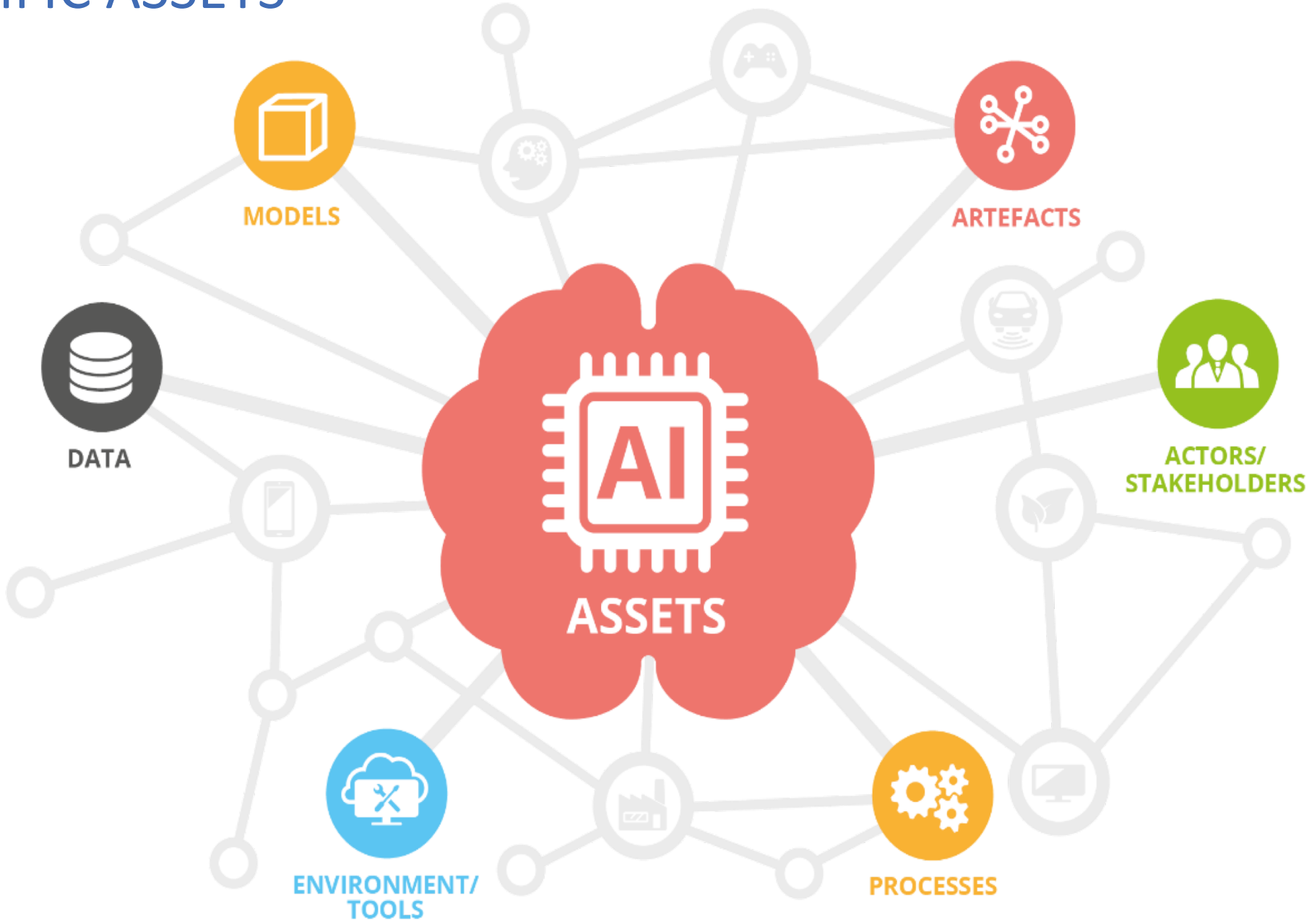
TELECOM
(networks, satellites, routers, optical fibers, telecom devices..)

INFRASTRUCTURE
(buildings, terminals, gates, data centers)

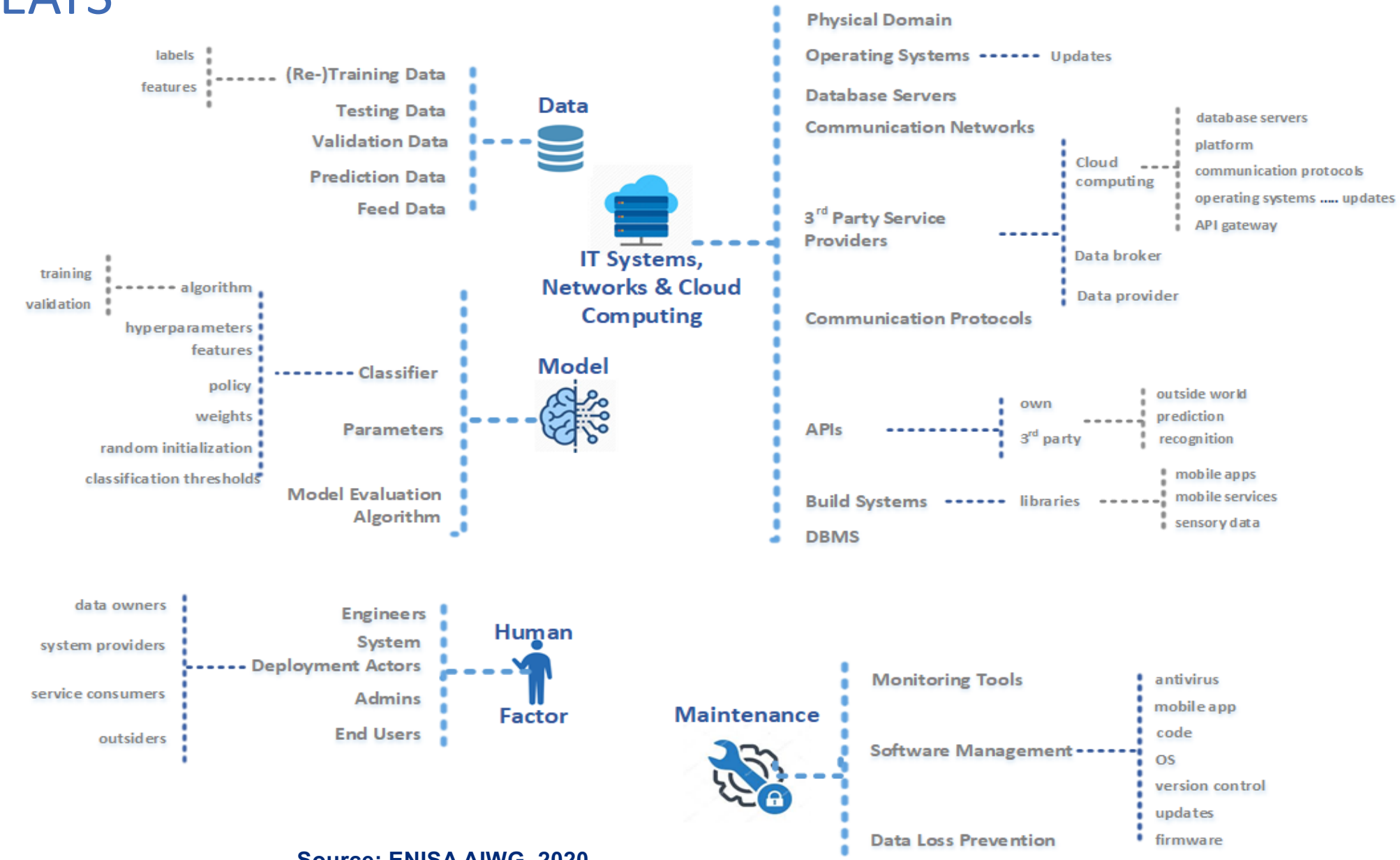
FAICP – A scalable framework for AI-related cybersecurity good practices



AI SPECIFIC ASSETS



AI THREATS



Source: ENISA AIWG, 2020

DESIGN

- ETSI GR SAI 006 V1.1.1 (2022-03) Securing Artificial Intelligence (SAI); The role of hardware in security of AI
- ETSI GR SAI 001 V1.1.1 (2022-01) Securing Artificial Intelligence (SAI); AI Threat Ontology
- ETSI GR SAI 004 V1.1.1 (2020-12) Securing Artificial Intelligence (SAI); Problem Statement
- ETSI GR SAI 002 V1.1.1 (2021-08) Securing Artificial Intelligence (SAI); Data Supply Chain Security
- IEEE 2976 eXplainable Artificial Intelligence – for Achieving Clarity and Interoperability of AI Systems Design
- ISO/IEC TR 24028:2020 – Information technology – AI – Overview of trustworthiness in artificial intelligence
- ISO/IEC DTR 27563 – Security and privacy in artificial intelligence use cases – Best practices

DEVELOPMENT

- ISO/IEC TR 24029-1:2021 Artificial Intelligence (AI) – Assessment of the robustness of neutral networks – Part 1: Overview
- ISO/IEC DTR 24368 Information technology – Artificial intelligence – Overview of ethical and societal concerns
- IEEE 2976 eXplainable Artificial Intelligence – for Achieving Clarity and Interoperability of AI Systems Design

DEPLOYMENT

- ISO/IEC DTR 24368 Information technology – Artificial intelligence – Overview of ethical and societal concerns
- ISO/IEC CD 42001.2 Information technology – Artificial intelligence – Management system
- IEEE 2941 – 2021 – IEEE Standard for Artificial Intelligence (AI) Model representation, Compression, Distribution, and Management

MONITORING

- ETSI GR SAI 005 V1.1.1 (2021-03) Securing Artificial Intelligence (SAI); Mitigation Strategy Report

TRAINING NEEDS

Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for A Skilled Workforce In the European Digital Single Market and Industries (CyberSecpro)

DESK STUDY+ SURVEY REVEALED THE MARKET NEED FOR MORE TRAINING IN CYBERSECURITY AI and ML

(27 EU training providers)

European Commission

CYBERSECPRO

CEN/CLC/JTC 21

European Standard “AI Risk Management” proposal under preparation

Challenges

- Interoperability of data
- Risks longitudinally (since AI systems continue learning after deployment, risks)
- Dynamic risk measurements /metrics (static measurements are not realistic)
- Global framework for AI ethics (that are accepted globally)
- Interdisciplinary, multi-perceptive approaches are needed
- From policy requirements to design principles

THANK YOU FOR YOUR ATTENTION

Professor Nineta Polemi

University of Piraeus, Dpt. of Informatics, Cybersecurity Lab

TRUSTILIO b.v.

dpolemi@gmail.com

skype: nineta.polemi

LinkeDin: dr Nineta polemi

trustilio
Enhance your Trustworthiness