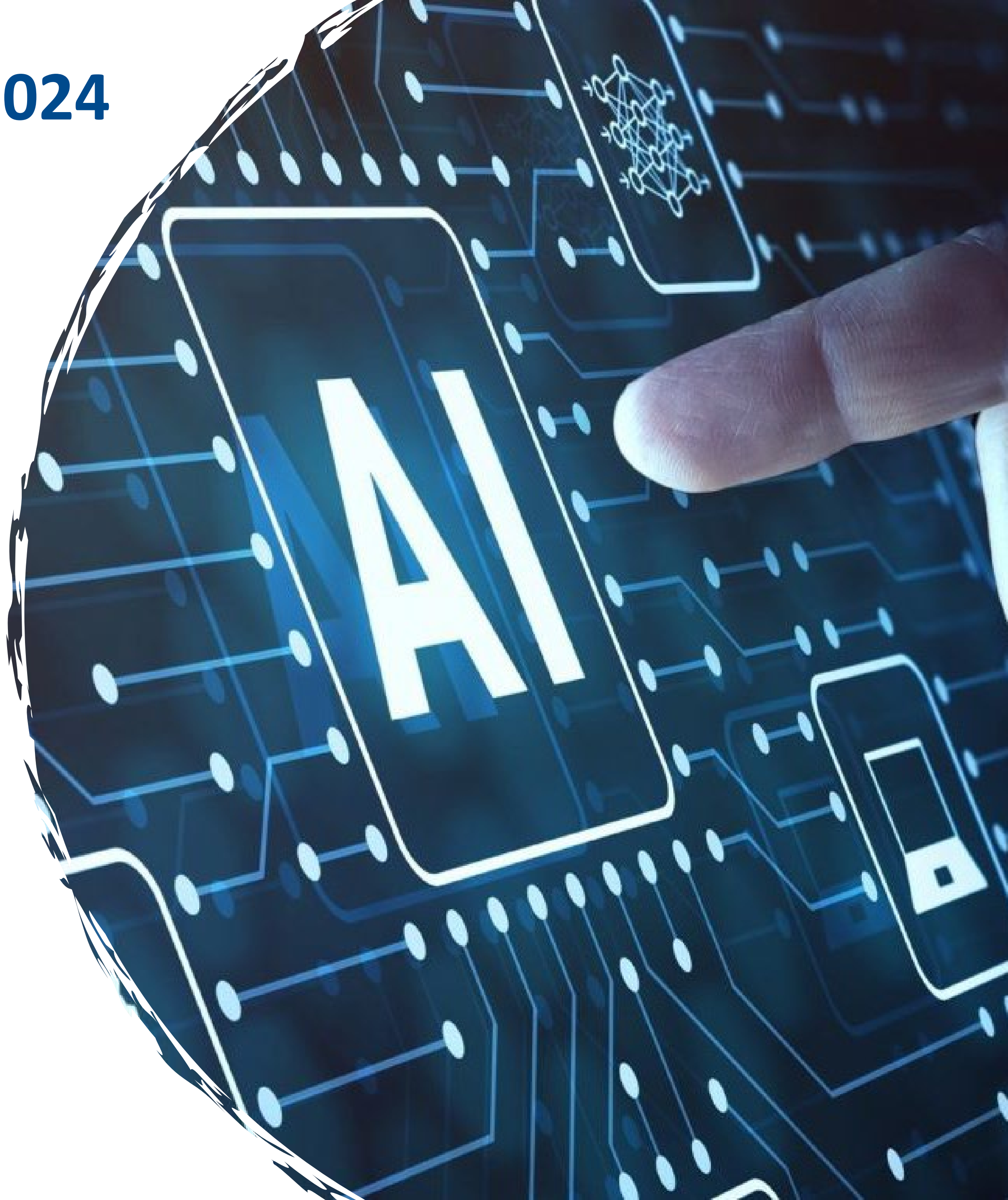
The Standards People

ETSI AI Conference 2024



How to deal with Cyber AI?

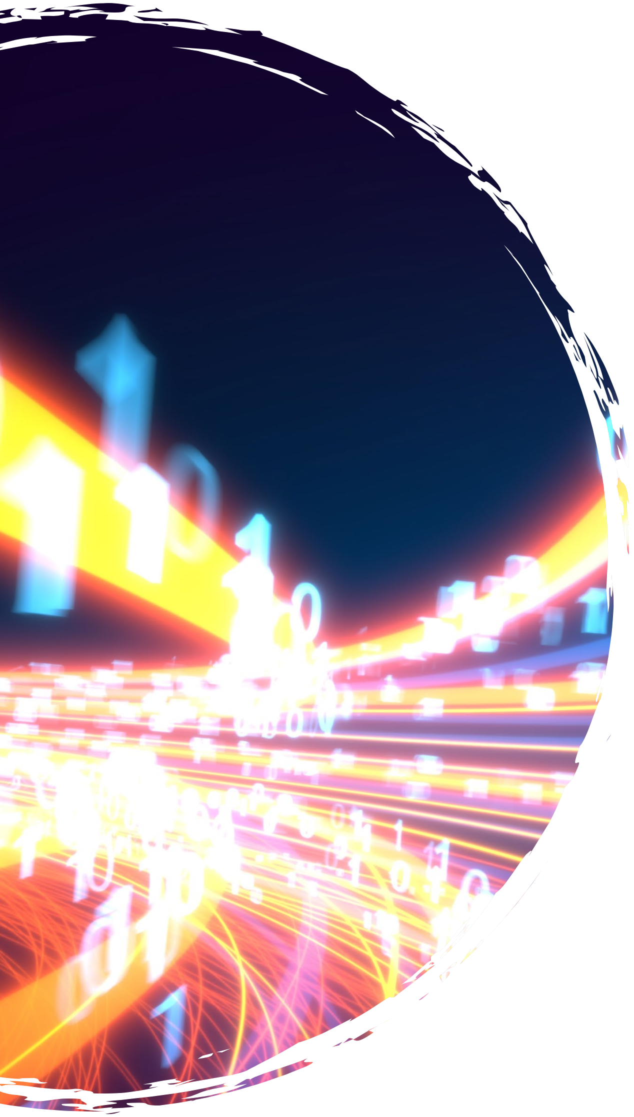
Overlaps of AI with the standardization work in ETSI TC CYBER

Presented by: Dr. Samim Ahmadi

06/02/2024

Agenda

- AI in Consumer IoT Security
- AI meets Cybersecurity Legislation
- AI in Security Services and Controls



AI in Consumer IoT Security

Update of ETSI TS 103 645 - Baseline Security Standard for Consumer IoT

new recommendation: data aggregation (e.g. based on Federated Learning)

Provision 6-7 When the **purpose** of **data collection from consumer IoT devices**, or processing on the consumer IoT device, is solely to compute an aggregate result, the **data collected should be the minimum required to compute the aggregate**, the aggregation should happen as early as possible, and the retention of both collected data and the resulting aggregate should be minimized.

EXAMPLE 5: Federated learning and analytics enable multiple devices to collaboratively train machine learning models or compute data queries, under the coordination of a central server. Each **device's raw data is stored locally** and not exchanged or transferred; instead, focused updates intended for immediate aggregation are uploaded to achieve the learning objective.

AI in Consumer IoT Security

Smart voice-controlled devices (SVD) security (TS 103 927)

Provision SVD 8-4 (added): The SVD shall **not retain any user voice recordings** and their derivatives locally or on an associated service operated in control of the device manufacturer **without explicit user's consent**.

NOTE: In the case where **SVD collects users' voices to improve AI models**, this provision applies. Both the user's voice and the intermediate produced during the training process are considered user data.

Recommendation 4: The SVD should be **resistant to voice imitation attacks**.

NOTE: Voice imitation attacks refer to the act of mimicking or impersonating someone's voice to gain access to their system or sensitive information. This attack can be done using various techniques such as speech synthesis, voice cloning, or **deep learning algorithms to replicate the victim's voice**. […]

Standards meet Legislation

Implementation of NIS 2 Directive (TR 103 866)

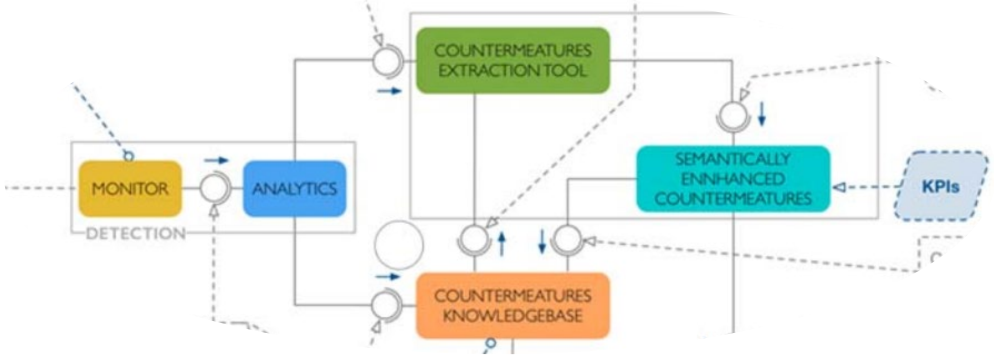
- Critical Security Controls meet **AI based Malware protection**: additional Control Safeguards supported by AI based or non-signature-based malware protection is required for **effective protection against** ever evolving **zero-day exploits** by sophisticated threat actors
- **Zero-Trust**: To enable real-time risk determination and deliver ongoing protection in evolving organizations, **contextual data is analysed and frequently re-evaluated with machine learning algorithms**

Implementation of AI Act

- Risk Assessment required in the context of cyber
  - According to **ETSI TR 103 935 on cyber risk assessment** based on products' properties to support market placement – the AI act sets classification rules and **identifies two main categories of high-risk AI systems**:
    - **AI systems intended to be used as safety component** of products that are subject to third party ex-ante conformity assessment.
    - **Other standalone AI systems with mainly fundamental rights** implications that are explicitly listed in Annex III of the AI Act.
  - **No specific risk assessment methodology determined in AI Act**

AI in Security Services and Controls

AI in SOCs as part of Managed Security Services, examples given in TR 103 644 – “Increasing smart meter security”


COUNTERMEATURES EXTRACTION TOOL
MONITOR
DETECTION
ANALYTICS
SEMANTICALLY ENNHANCED COUNTERMEATURES
KPIs
COUNTERMEATURES KNOWLEDGEBASE

(image extracted from TR 103 644)

AI consideration in security controls and related, e.g.

1) **AI based malware defences**
   - Mentioned in TR 103 866 – “Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls”
   - Side information: Even modern variants of malware leverage machine learning techniques (see ETSI TR 103 305-1 – “Critical Security Controls”)
2) **AI based network analysis**
   - Mentioned in TS 103 961 – “Optical Network and Device Security”
   - **Reference made to ETSI TC SAI**: where AI is used, guidance from ETSI TC SAI applies

Thank you for your attention

Follow us on:

Any further questions?

Contact me:

samim.ahmadi@de.ey.com