ECCO
European Cybersecurity COmmunity

Challenges and intersection of AI and Cybersecurity

ECCO Community Roadmapping knowledge sharing webinar

May 29 2024, 11:00-12:00

Fabio Martinelli (CNR) and Christian Banse (FhG)

Agenda

Title	Presenter
Welcome and ECCO Roadmapping WG	Fabio Martinelli, CNR, Christian Banse, Fraunhofer AIESEC
Introduction	Philippe Massonet, CETIC
The role of Machine Learning in Network Intrusion Detection Systems.	Bruno Volckaert, IDLab, Ghent University/IMEC.
Cyber Threat Intelligence improvement with LLMs.	Erkuden Rios, Tecnalia. (Project Manager of AI4CYBER project)
Generative AI-supported cyber incident simulation.	Eider Iturbe, Tecnalia. (Technical Manager of DYNABIC project)
Question and answers	

ECCO Community Roadmapping WG

- **Governance & Participants**
- Chairs:
  - Roadmapping: Christian Banse and Claudia Eckert (Fraunhofer)
  - Development of the Community: Fabio Martinelli (CNR)
- ECCO Proto-Community on Roadmapping: The members of this Community Group are growing stemming from the ECCO experts and the ones in the initial proposal (from ECSO and the 4 Pilots). The initial experts have been carefully selected to ensure a diverse composition, with contributors representing the research and industry community or with close links to ensure an interesting mix of competencies for the identification of relevant topics in support to the ECCC Strategic Agenda implementation and as such the European cybersecurity ecosystem.
- It is in the process to be expanded with other experts from ECCO proposal and also according to suggestions by ECCC, NCCCs, etc.

ECCO Community Roadmapping WG (II)

- **Objectives**
- The approach and objectives have been updated to meet the needs of the NCCs Network and ECCC GB, and in support of the implementation of the ECCC Strategic Agenda and its main objective: "*By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan*".
- The initial objectives of the ECCO Community Group on road-mapping have been articulated and agreed upon. They are:
  - Build the ECCO proto-community of experts on road-mapping for capability and capacity building to address the priorities of the Strategic Agenda (future DEP projects and pan-European actions).
  - Deep dive road-mapping on priorities for DEP
  - Map concepts from the ECCC Strategic Agenda to other roadmaps (e.g. results of pilots, ECSO, ENISA, etc.) as well as to the cyber resilience landscape.
  - Consolidate and find synergies among recommendations for implementation of the Strategic Agenda from other ECCO Community Groups.
  - Support the NCCs in the implementation of the Strategic Agenda's Action Plan for improved research, development and innovation expertise and competitiveness of the EU cybersecurity community, e.g., through a series of webinars.

Initial planned webinars

- Perform knowledge sharing webinars with ECCC, NCCCs and wider community

- Initial topics identified by the community WG to be covered in the next period

1. Automated compliance and Cyber-Resilience (done!)
2. Digital twins and cybersecurity (done!)
3. AI and cybersecurity (today!)
4. Data Spaces and Data Sovereignty
5. Cyber threat management
6. ...

- We are open re-address and insert new ones for the future according to ECCC and NCCCs needs and requests.

- For experts willing to join the ECCO community send a request to the chairs – community_roadmapping-owner@list.cyber-ecco.eu

ECCO
European Cybersecurity COmmunity

Challenges and intersection of AI and Cybersecurity

29 May 2024, Webinar

Philippe Massonet (CETIC)
Philippe.massonet@cetic.be

Rise of AI Impacting Society

Self-driving car

AI based virtual assistants (Siri, Alexa, …)

Medical diagnosis

Financial trading

Customer service, chatbots

…

OpenAI
ChatGPT

Artificial Intelligence/Machine Learning ⇄ Cybersecurity

Cybersecurity for AI

- AI systems are:
  - complex and interconnected which makes them more vulnerable to cyberattacks,
  - used to collect, store and process sensitive data,
  - used in real-time applications,
  - increasingly being used in critical infrastructure, such as power grids and transportation systems.

- New cybersecurity risks that make AI systems vulnerable to new types of cyberattacks (e.g. https://atlas.mitre.org/)

- Adversarial machine learning: study of attacks/defenses on ML algorithms

AI for Cybersecurity 1/2

AI plays a crucial role in cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats:

- Threat Detection and Intelligence
  - Anomaly Detection with AI algorithms
  - Learn unknown threats from data to identify new types of attack

- Malware Detection:
  - Behavioral Analysis: AI can analyze the behavior to identify patterns consistent with malware
  - Signature-based Detection: AI models can be trained to recognize known malware signatures and patterns.

AI for Cybersecurity 2/2

- Network Security:
  - Intrusion Detection Systems (IDS): AI network traffic monitoring to detect unusual patterns or malicious activities,
  - Firewall Optimization: AI can learn and optimize firewall rules and configurations based on network traffic analysis.

Network Security

- Vulnerability Management:
  - Automated Scanning: AI can scan networks and systems for vulnerabilities and prioritize them based on potential risks,
  - Patch Management: AI can assist in identifying and applying patches to vulnerable systems.

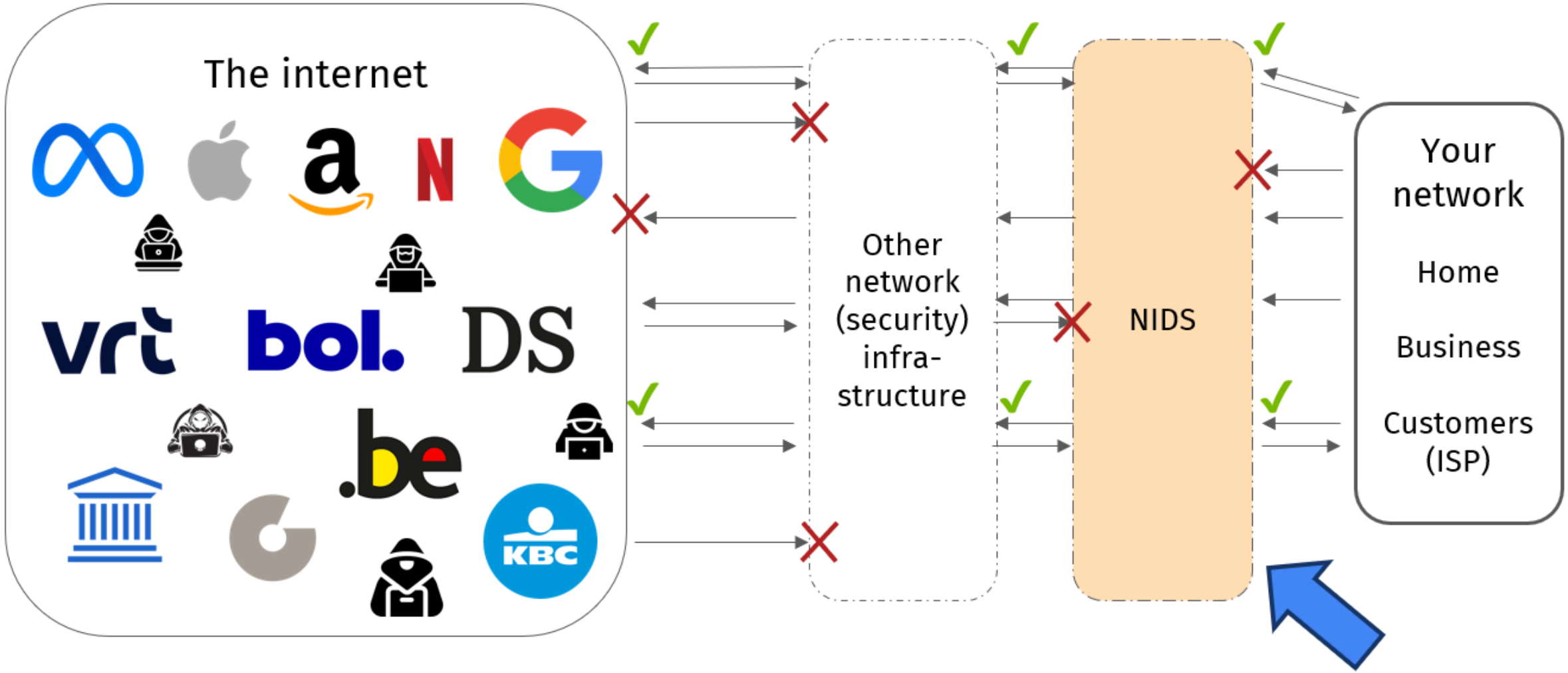
- Adversarial Machine Learning: use of AI to generate adversarial examples to improve the robustness of AI-systems against attacks.

- ...

The role of machine learning in Network Intrusion Detection Systems

Prof Dr Bruno Volckaert
University of Ghent and IMEC

Network Intrusion Detection Systems (NIDS)



NIDS: Mostly rule/signature based

- Rule/signature-based
  - Strengths: Precise, easily explainable, shareable
  - Drawbacks: Fragile, not scaling well, costly to maintain, weakened by encryption

1998

1998

2004

2009

```
alert tcp 1.2.3.4 any -> 5.6.7.8 443
```

Machine learning as a way forward

- ML = science of getting computers to act without being explicitly programmed
  - Learn rules from data, do not write them yourself
  - Strengths: promises of robustness and scalability
  - Drawbacks: requires training with lots of examples, less precise, less explainable
- In research since +/- 2005

Why have machine-learned IDS not crossed from academic research into real-world use?

Literature: great classification results!

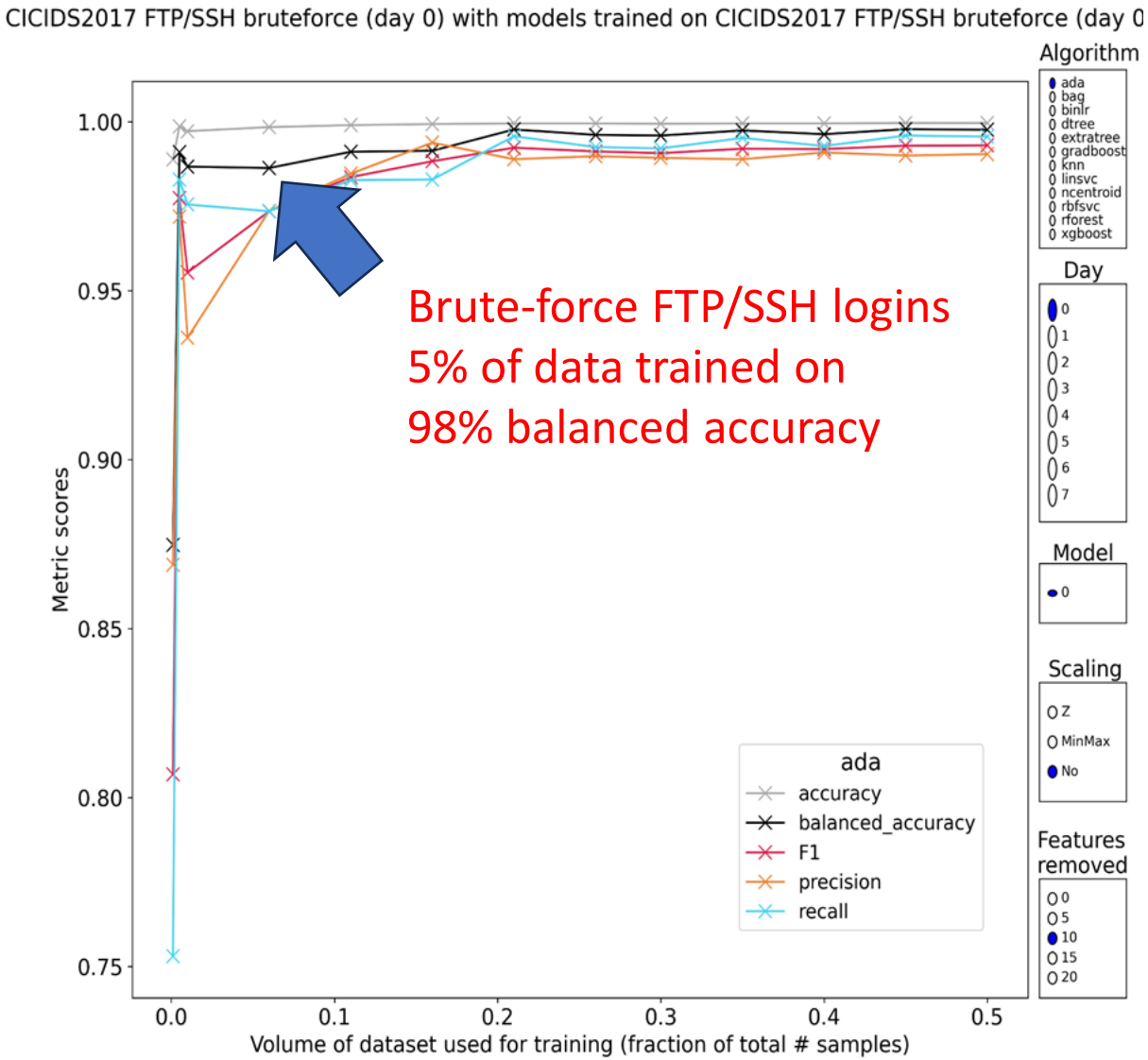
- Benign vs Malicious network traffic: **99%+** accuracy is no exception

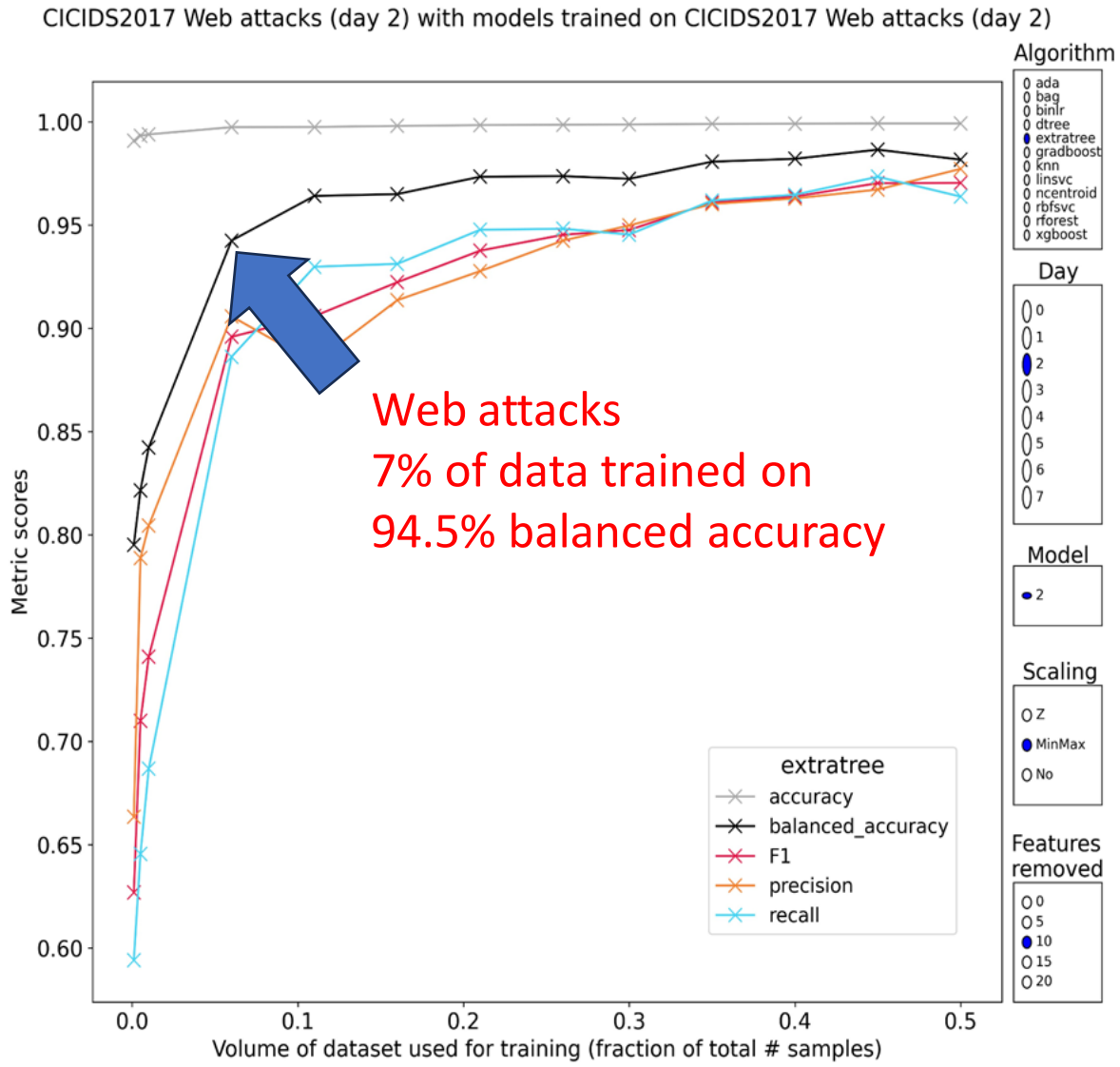
Table 3. Comparison of ML based IDS based on accuracy.

ML Architecture	Article	Accuracy (%)
LMRDT-SVM	Huiwen Wang.et al. [30]	99.31
K-NN	Lin et a [31]	99.89
Naive Bayes classifier.	Monika Vishwakarma.et al. [32]	98.59
K-NN	Wenchao Li.et al. [33]	98.5
Naïve Bayes algorithm	Sharmila B S et al. [34]	83
Random Forest Logistic Regression	S. Waskle et al. [35]	96.78
Random Forest	Belouch, M et al. [36]	97.49
Random Forest	Abdulhammed, R et al. [37]	99.64
K-Means+RF	K. Samunnisa et al. [42]	92.77

Source: A comprehensive review of AI based intrusion detection systems, Measurement: Sensors, Vol 28, Elsevier, August 2023

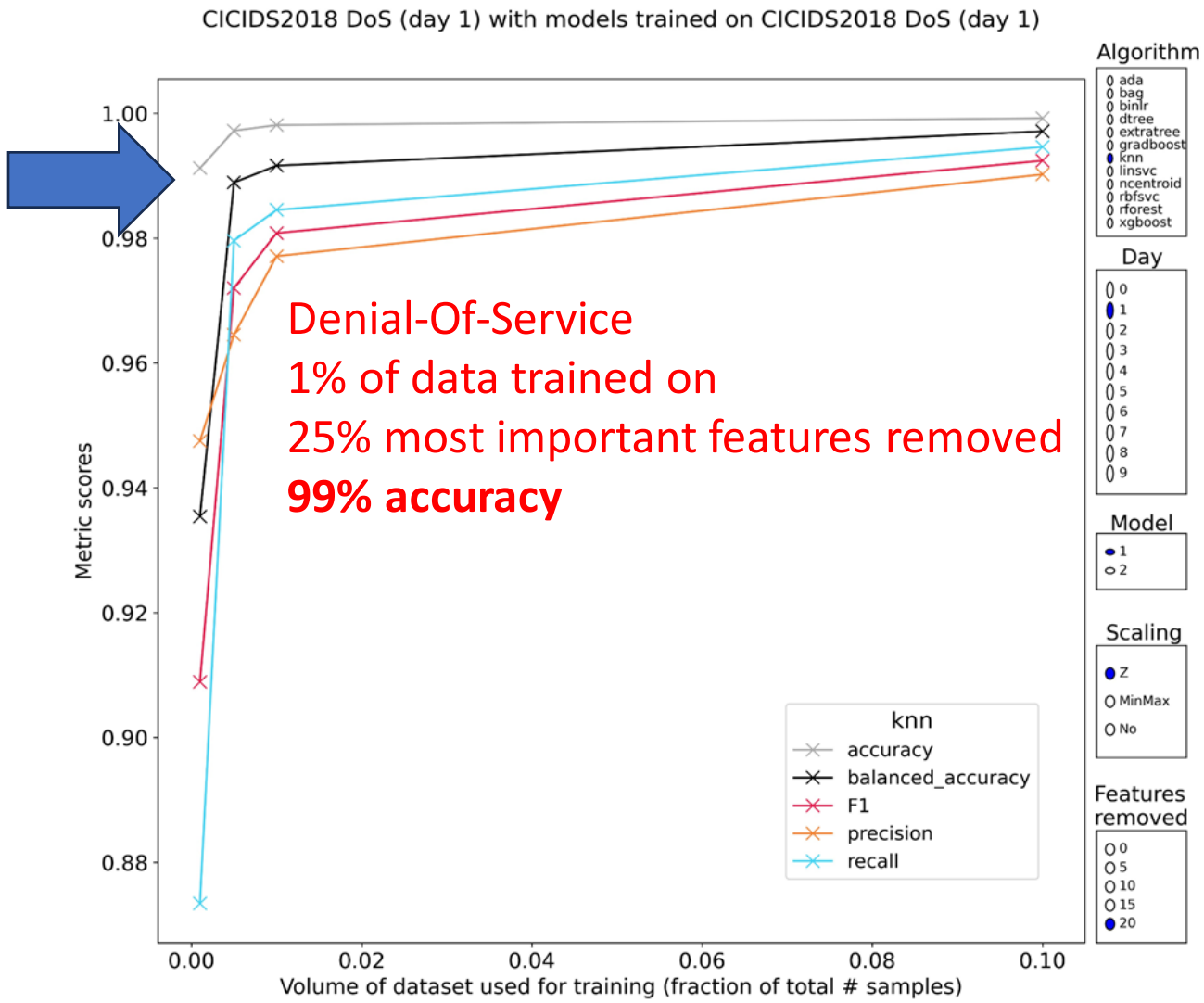
Initial research confirmed: great classification





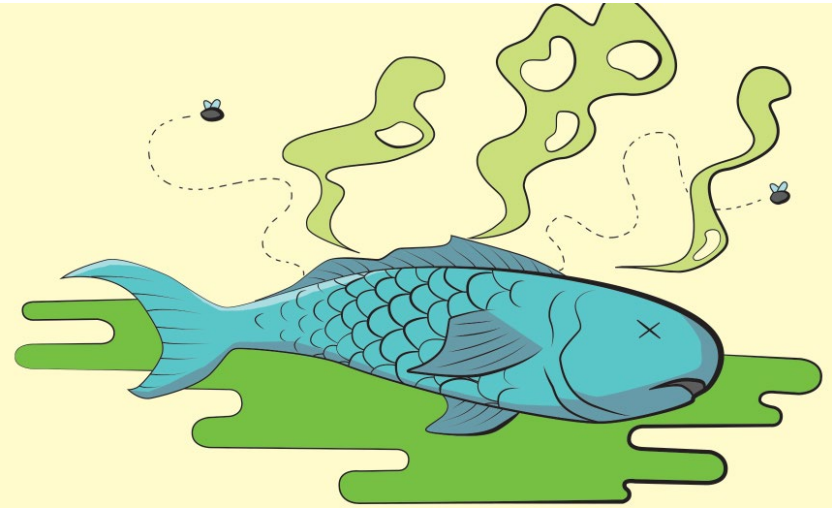
What if we make training more difficult?

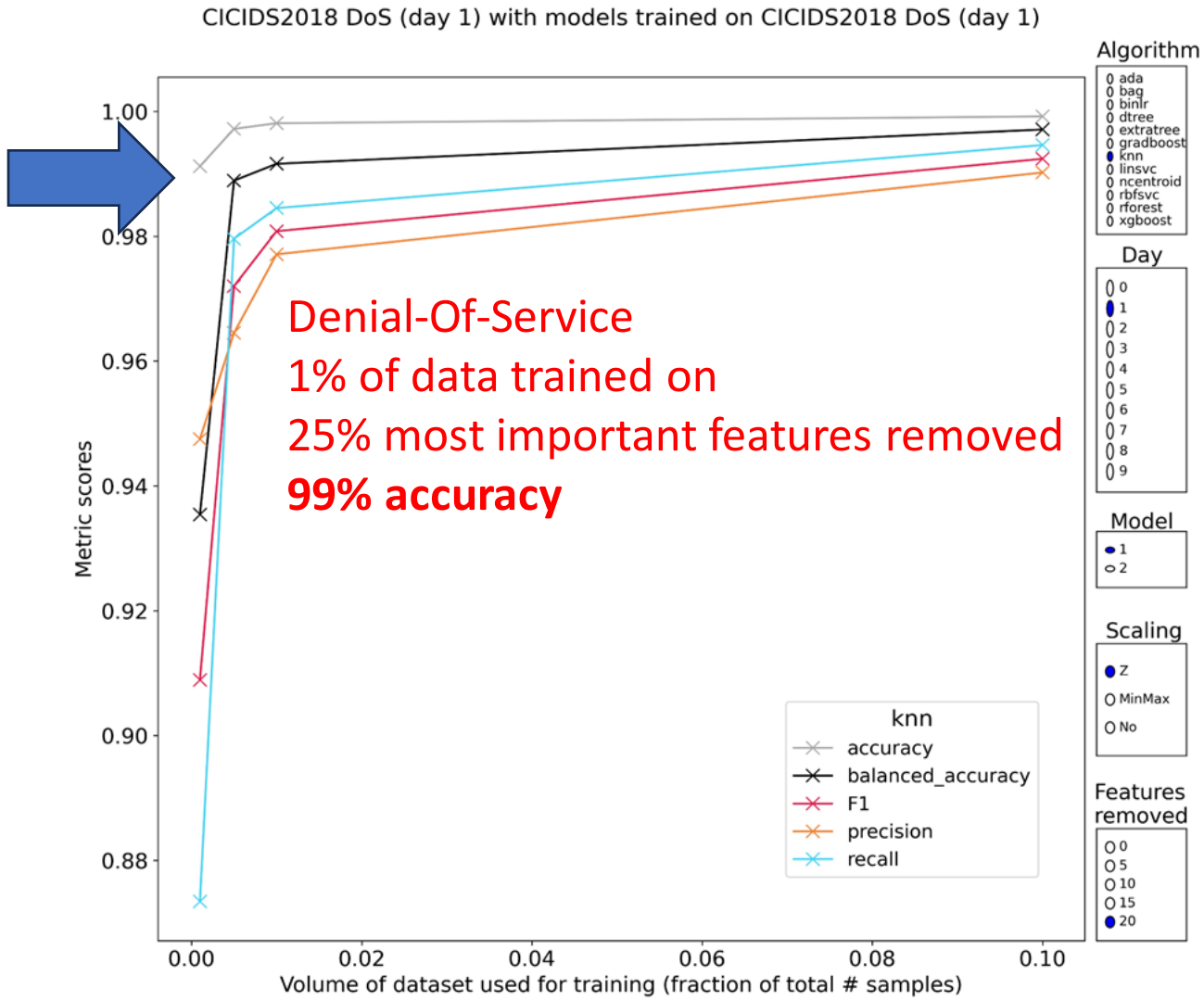
- Deliberately make classification difficult
  - **Remove 25% best features** (of a total of 80 features)
  - **Limit training / testing proportions** all the way down to 0.1% training / 99.9% testing



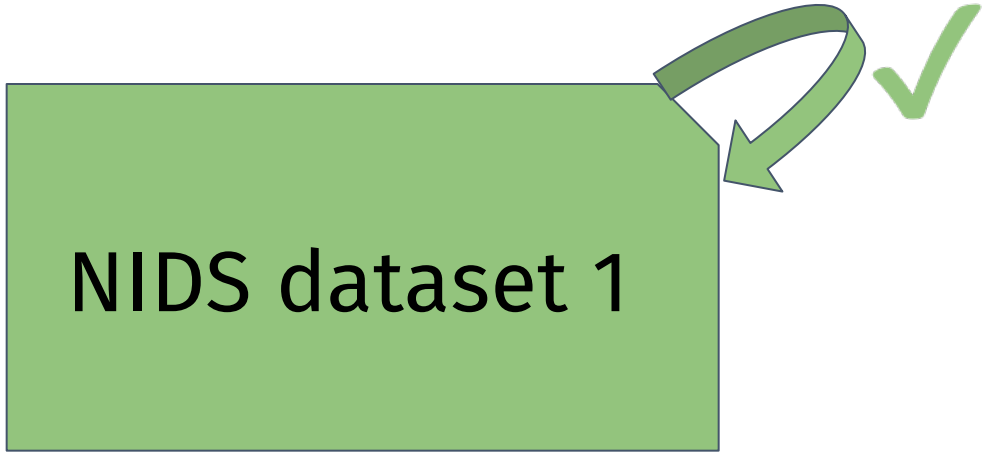
What if we make training more difficult?

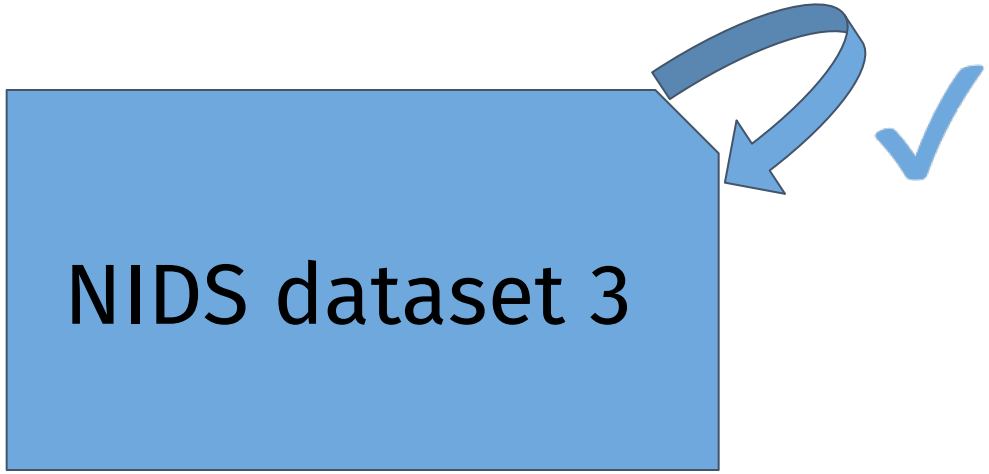
- Deliberately make classification difficult
  - **Remove 25% best features** (of a total of 80 features)
  - **Limit training / testing proportions** all the way down to 0.1% training / 99.9% testing



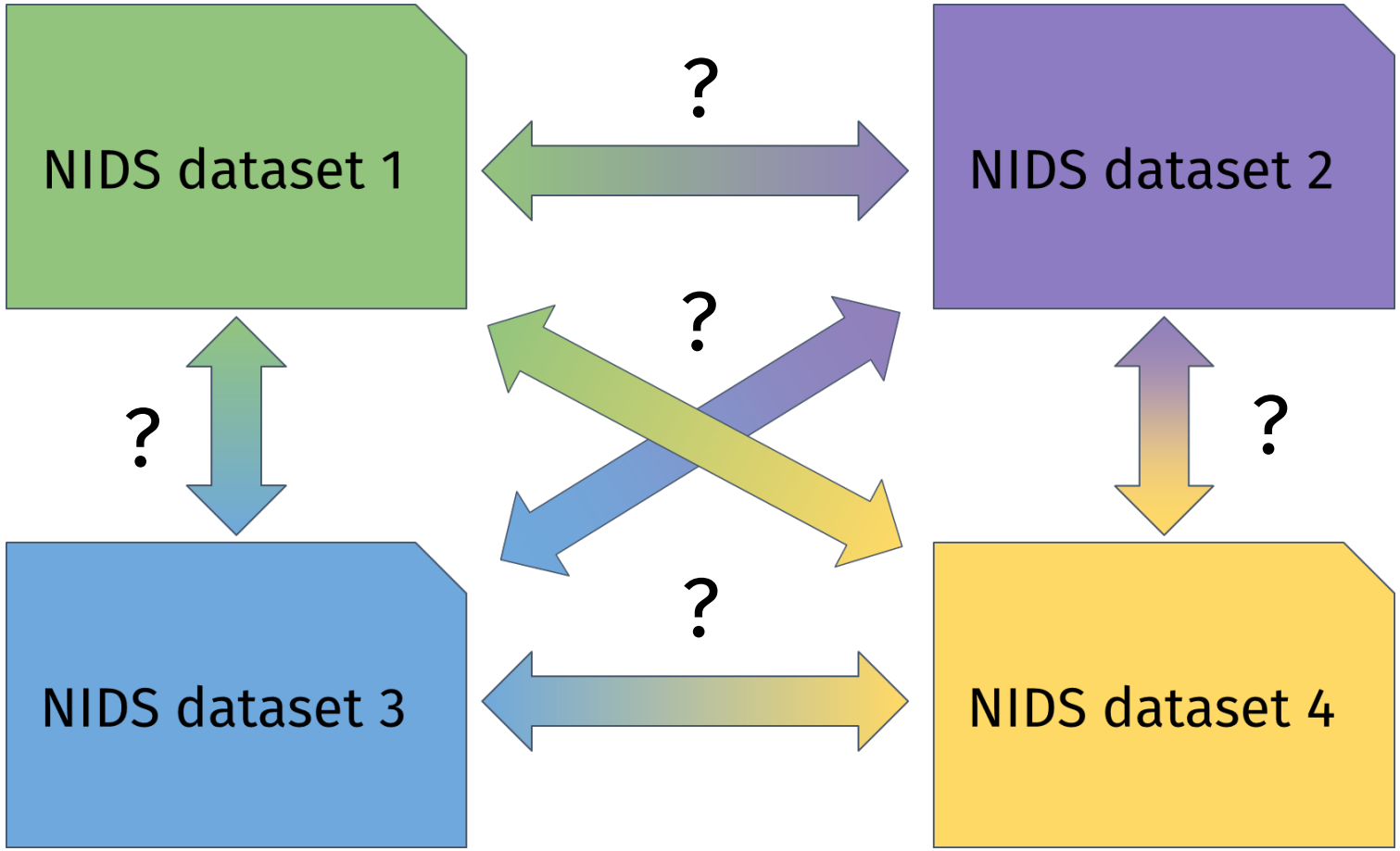


On isolated datasets, classification is excellent



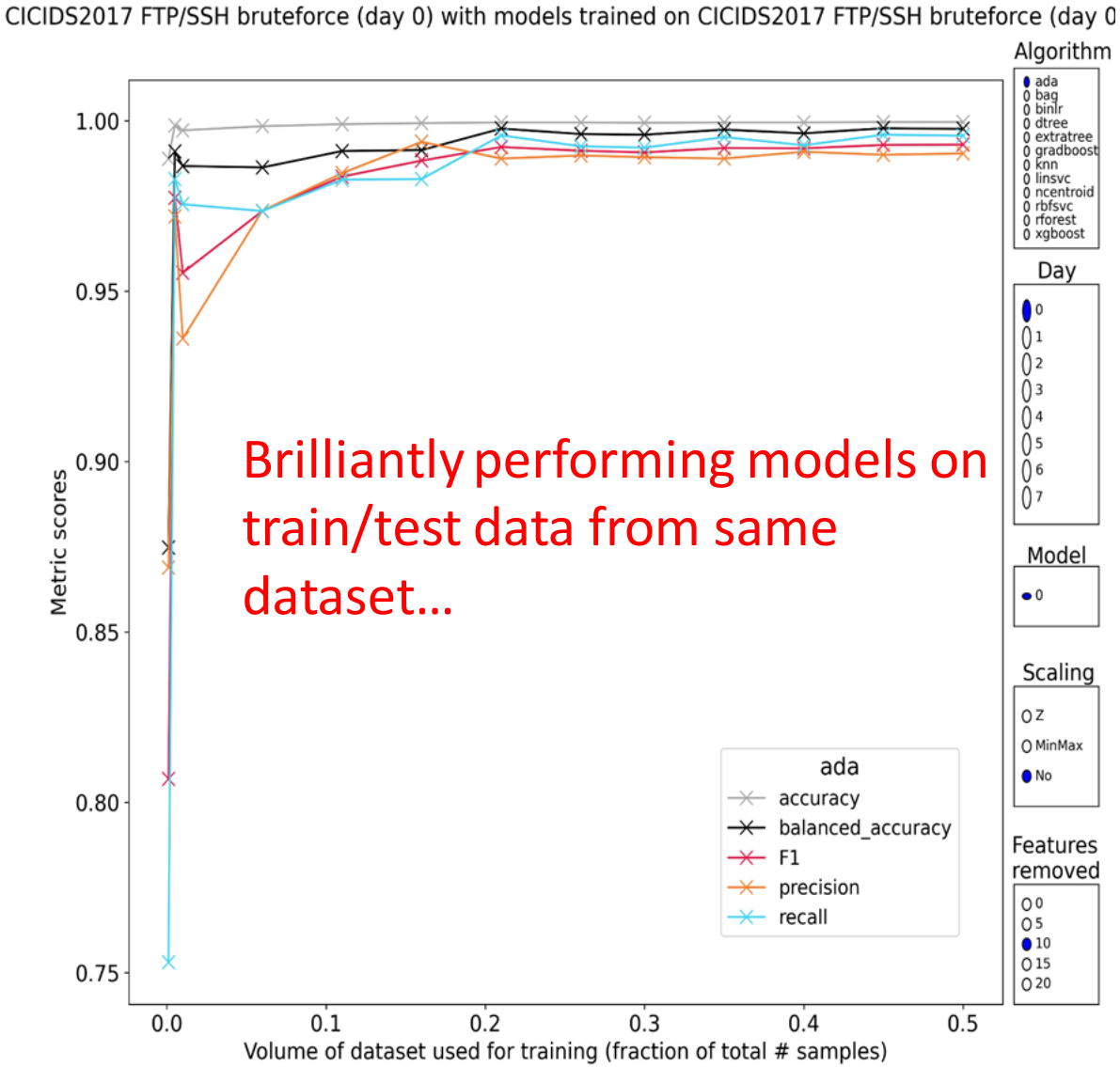


The real objective: well-generalizing models

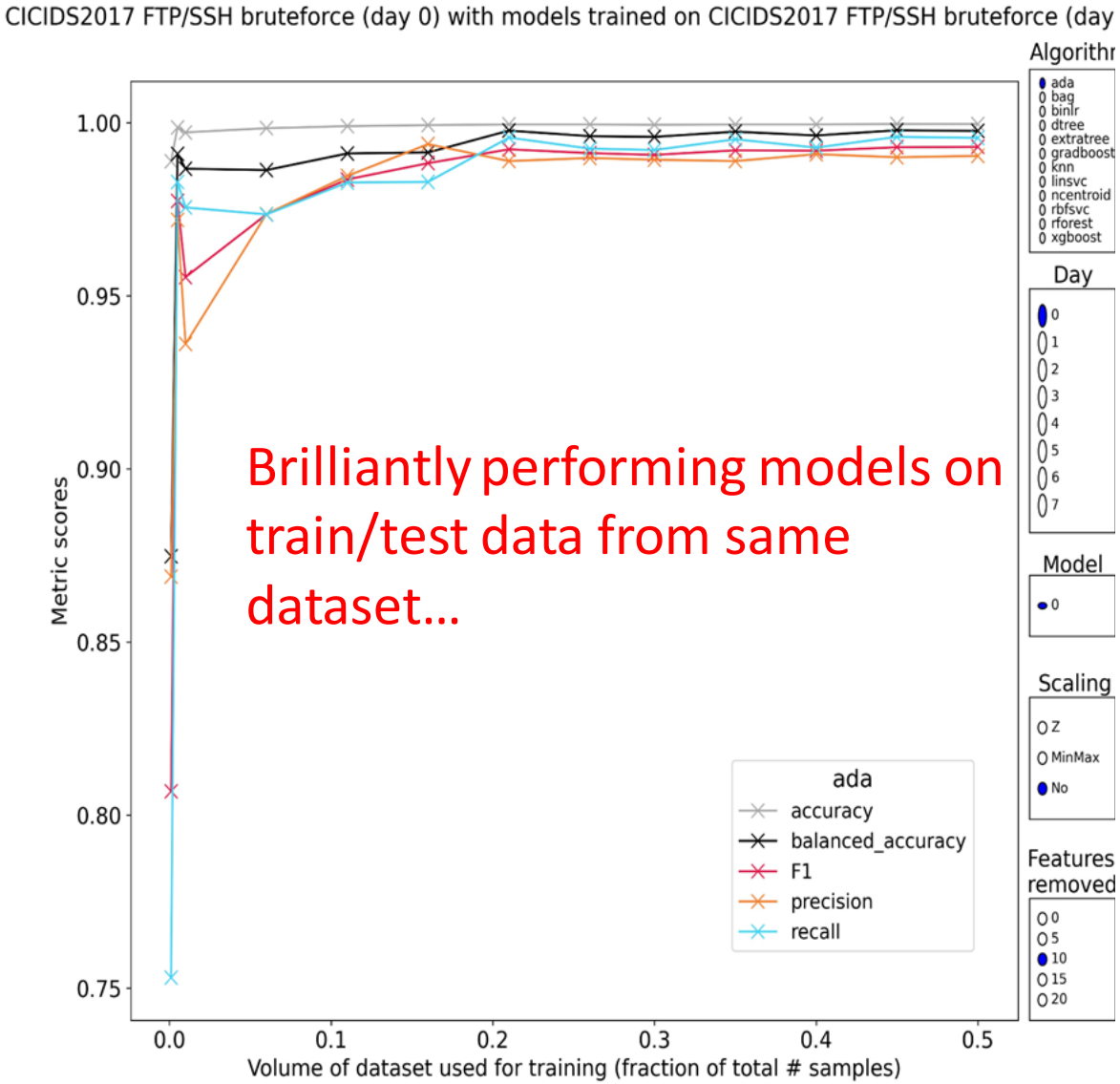


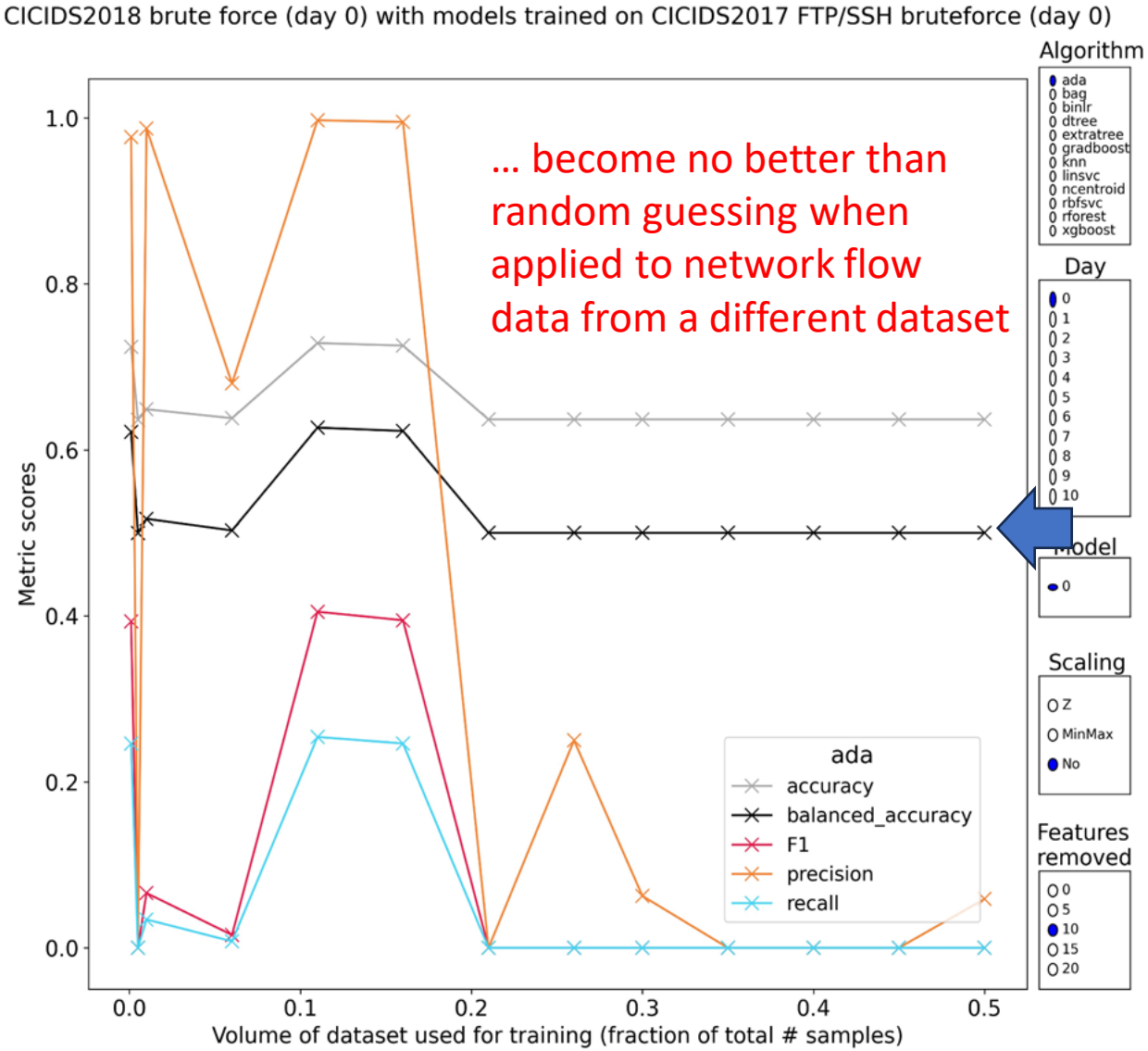
Model able to classify an attack trained on dataset 1 should be able to identify that same attack on any other dataset

Reality: catastrophic losses in generalized performance

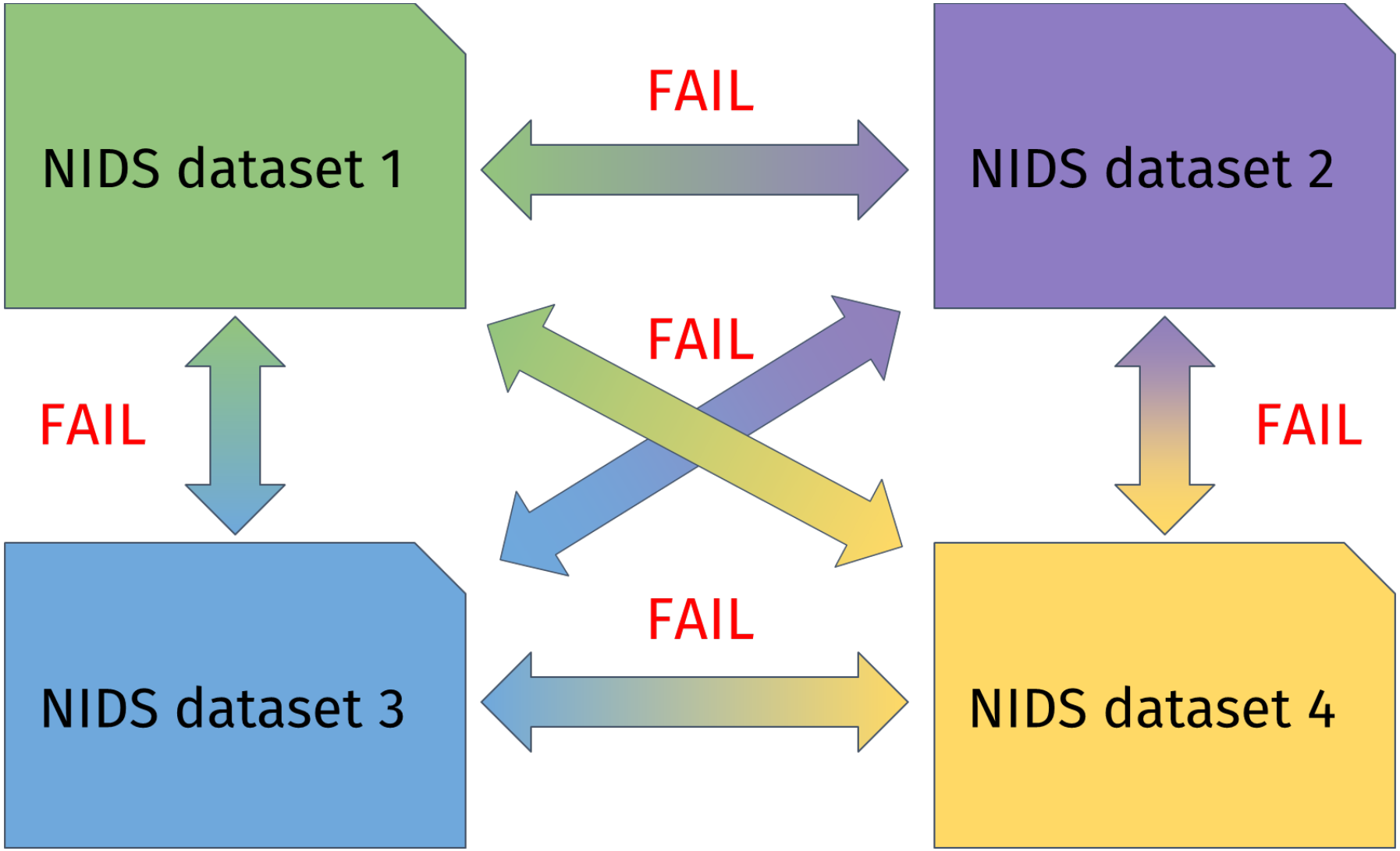


Reality: catastrophic losses in generalized performance



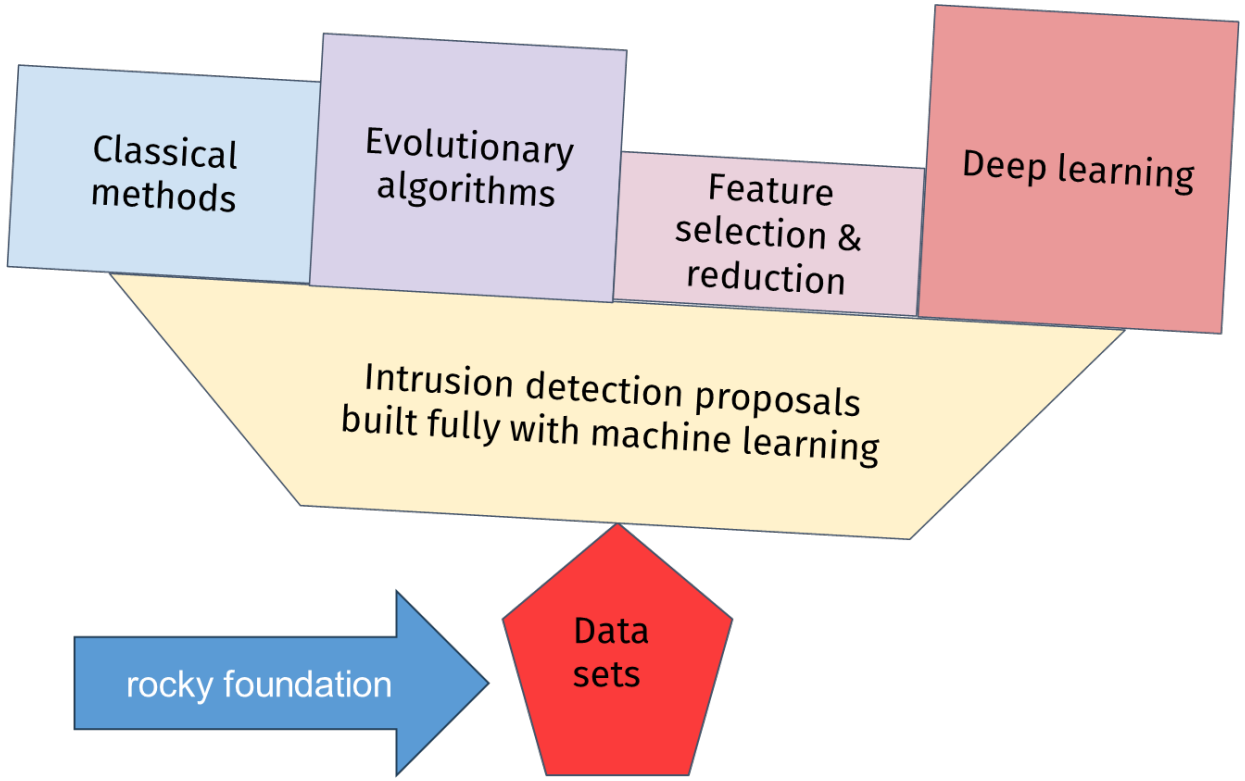


Generalization is weak, regardless of model choice



Poor data as a basis for IDS models

- Insufficient variability in current IDS datasets
- Contaminating features
  - Attacks from same IP (range)
  - Attacks starting at predictable times
  - Features giving away the use of attack tools
    - e.g. TTL always set to 0
  - And many, many more…
- ML learns
  - How the intrusion experiments are created
  - Vs learning to identify malicious traffic



Why have machine-learned IDS not crossed from academic research into real-world use?

Why have machine-learned IDS not crossed from academic research into real-world use?

Because the wrong objective has been targeted

&

The datasets on which these models were trained have fundamental flaws

Current issues do not mean dead end

- Practical ML-advances require **methodological rigor**
  - Advancing accuracy of practically useless methods, remains useless
  - Focus: methods that stand generalization tests + extensive quality control
- **New, cleaned datasets released**
  - **All major NIDS datasets:** https://www.kaggle.com/dhoogla/datasets
  - Dataset / feature standard can bring much-needed dataset interoperability
- Combined with anonymized datasets based on real network flow data, captured at many different locations
  - Belgian federal AIDE project is looking into **federated learning methods** for NIDS
    - No privacy sensitive flow information disclosed, but model updates (newly detected threats) do get shared with partners

Key points

- When something looks too good to be true, it likely is
  - ML-based intrusion detection requires **significant further research** to be applicable in practice
  - **Foundation: correct and diverse datasets** on which models can be trained / tested
- Ongoing research avenues
  - Lab-based dataset creation through highly diverse emulated scenarios mimicking real-life attacks
  - Real-time high bandwidth (10Gbps+) flow monitoring
  - ML models aiming to detect technique sequences (e.g. scanning -> exploitation -> lateral movement -> …) defined in MITRE ATT&CK chains
  - Federated learning: aims to improve privacy of involved parties AND come up with continuously strengthening models

Contact information

- Prof. Dr. Bruno Volckaert
- IDlab – University of Ghent / IMEC
- E: bruno.volckaert@ugent.be
- LI: www.linkedin.com/in/bvolckae

- Research / publications: https://www.researchgate.net/profile/Bruno-Volckaert-2
  - Results discussed in following publication (freely downloadable on ResearchGate)

IoTBDS 2023

Best Paper Award

Castles Built on Sand: Observations from Classifying Academic Cybersecurity Datasets with Minimalist Methods
Laurens D'hooge, Miel Verkerken, Tim Wauters, Filip De Turck and Bruno Volckaert

ECCO
European Cybersecurity COmmunity

Challenges and intersection of AI and Cybersecurity

ECCO Roadmap WG Webinar on AI and Cybersecurity

29th May 2024

ECCO
European Cybersecurity COmmunity

Session 3: Cyber Threat Intelligence improvement with LLMs

Erkuden Rios

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

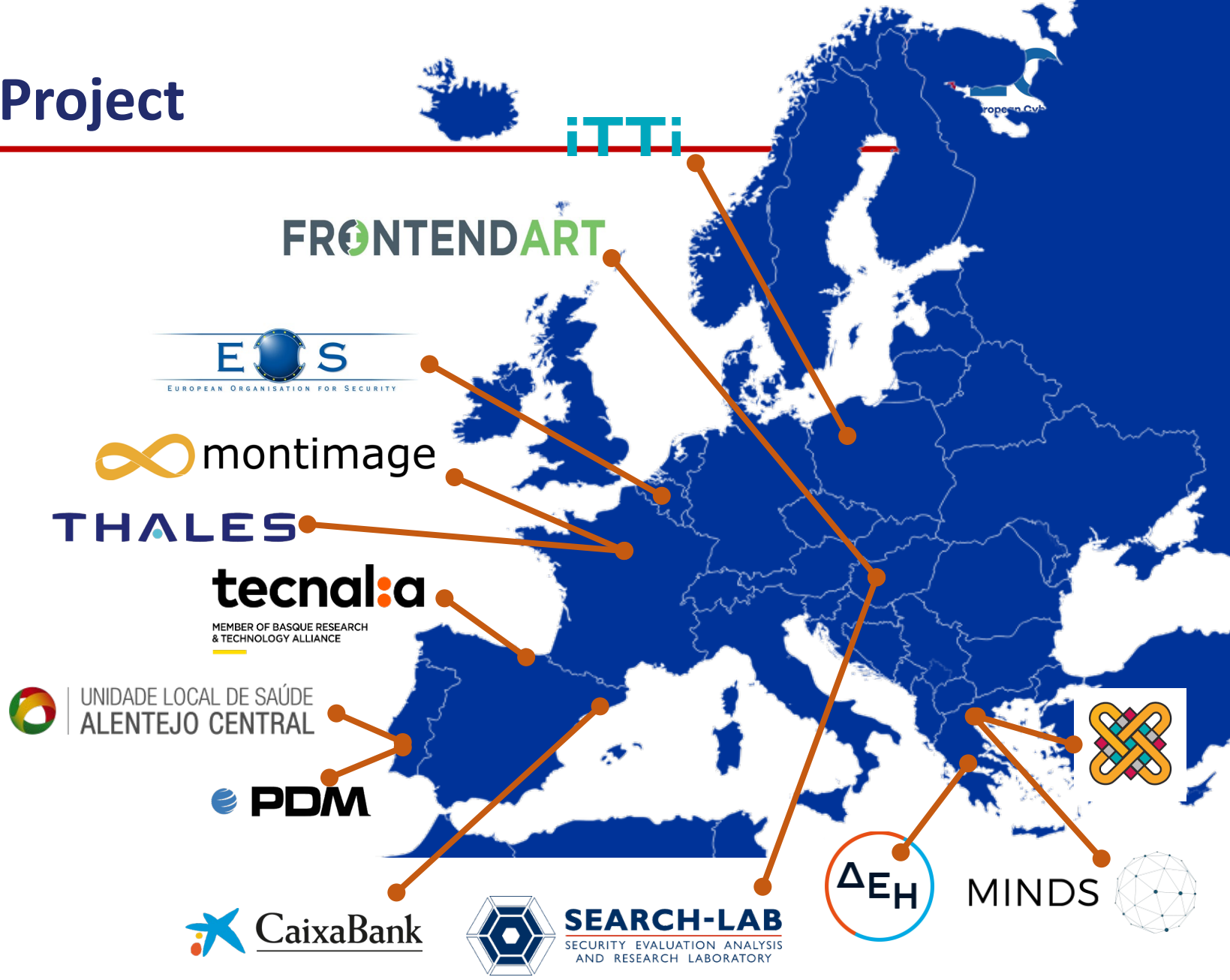
AI4CYBER

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

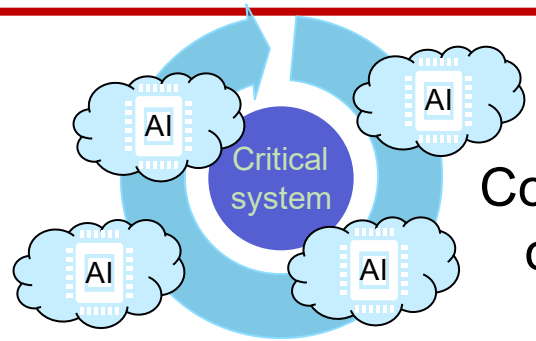
The context: AI4CYBER Project

- Grant Agreement ID: 101070450
- Project Type: RIA
- Project Coordinator: Tecnalia
- Consortium: 13 partners
- Budget: € 3.998.413
- Start Date: 01/09/2022
- Duration: 3 years



AI4CYBER Key objectives

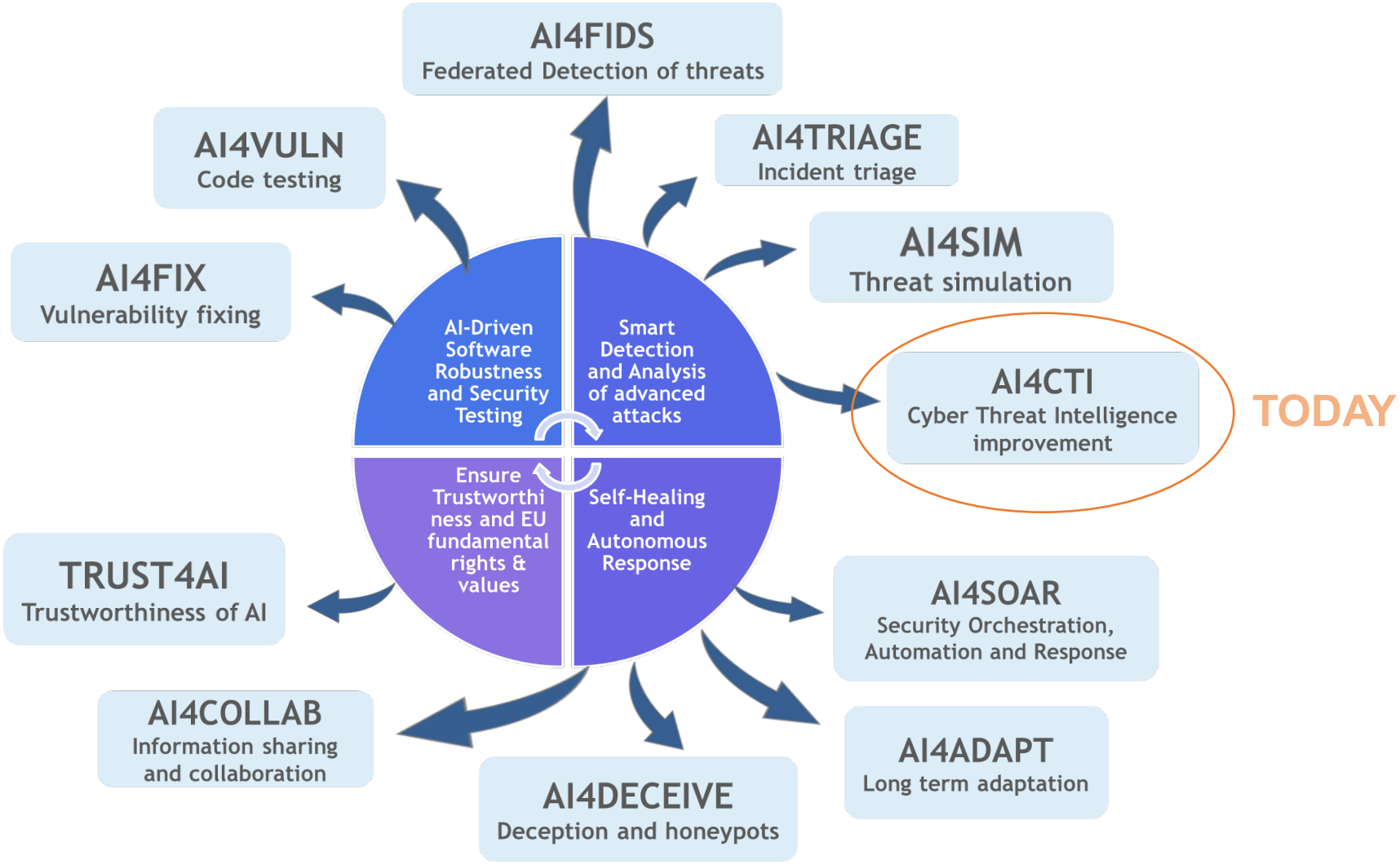
To establish an **Ecosystem Framework of next generation AI-based services** for supporting critical system developers and operators to **efficiently manage** system **robustness**, **resilience**, and appropriate **response** in the face of **advanced and AI-powered cyberattacks**.



Continuum of care

O1	O2	O3	O4	O5	O6
AI4CYBER Ecosystem Framework of next-generation trustworthy cybersecurity services.	**AI-driven software robustness** and **security testing services** for **flaw identification** and **code fixing automation**.	**Services** for **detection** and **analysis** of **advanced** and **AI-powered attacks** to prepare the critical systems to be resilient against them.	Mechanisms to **optimize the orchestration of security protections**, and continuously learn from system status and defences' efficiency.	Ensure European **fundamental rights and values-based AI technology** in AI4CYBER, ensuring **explainability, fairness** and **security**	**Foster open innovation** and **business opportunities** through **demonstration of AI4CYBER services** integrated into **critical services.**

AI4CYBER Framework



AI4CTI Objective and challenges

- Objective: From open CTI information sources extract Tactics, Techniques and Procedures (TTPs) of attacks in order -> improve and order detection focus and order responses.

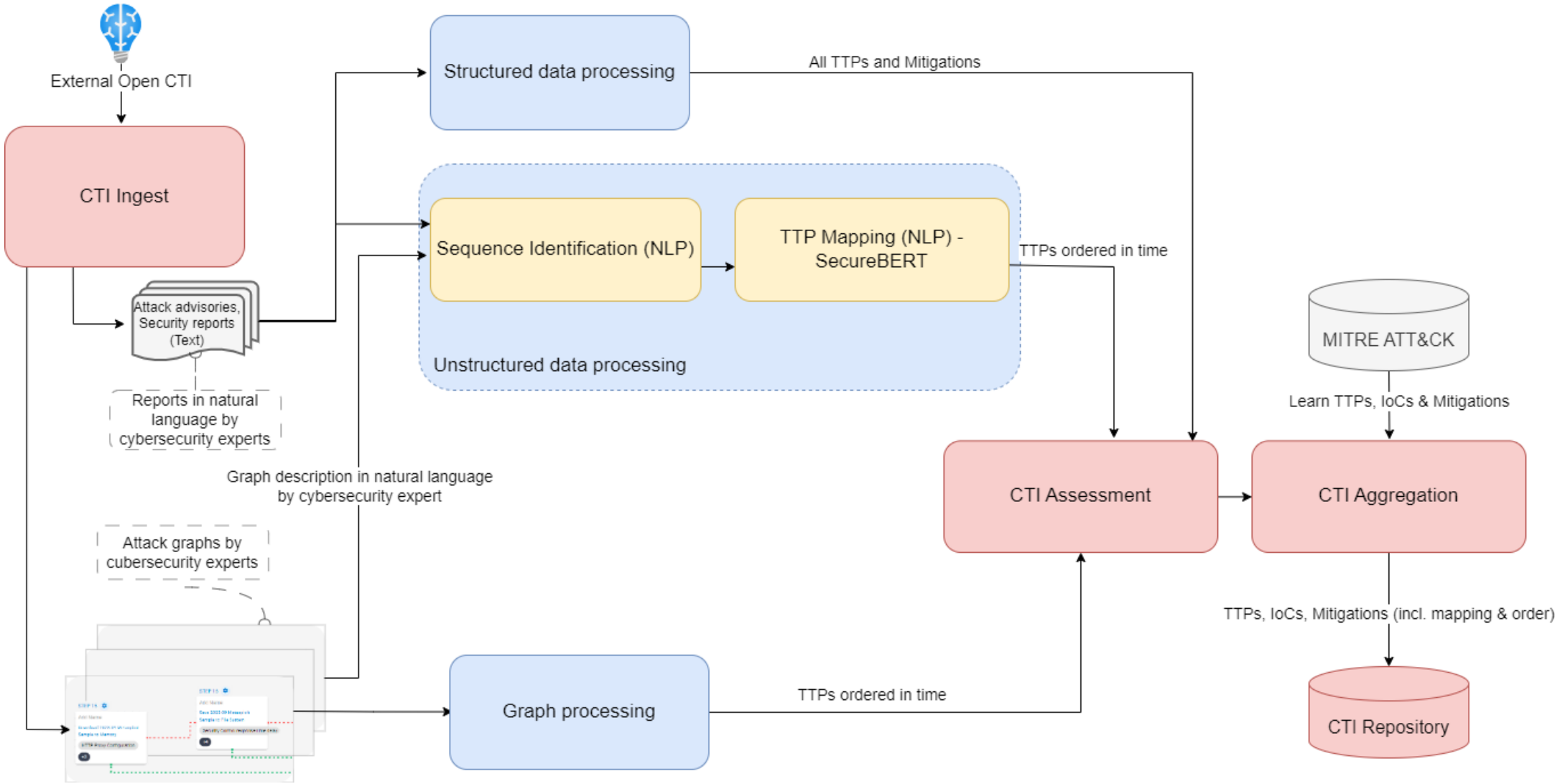
- Challenges: diversity of CTI sources, mix of structured and non-structured data, text written in natural language by different cybersecurity experts, graphical data may also exist, etc.

- Could NLP and LLMs help in the automation and efficiency?
  - Identify TTPs and mitigations -> Analyse CTI texts from experts through the use of NLP for NER analysis and mapping of TTPs and mitigations.
  - Order them.
  - Use LLMs to further improve accuracy.

AI4CTI Functionalities

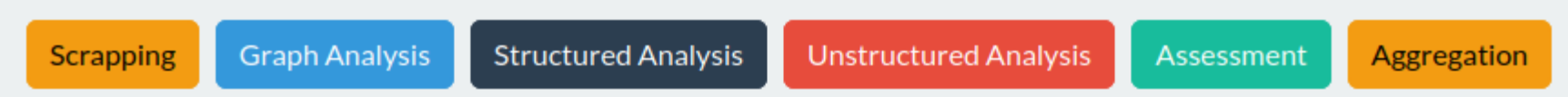
- Initial design and implementation of the core functionality ready:
  - CTI Ingestion
  - Structured processing: TTP info extraction.
  - Unstructured processing: NLP techniques, including LLMs (SecureBert and LlaMa2).
  - Attack graph processing: attack steps extraction with OpenCV and Tesseract
  - CTI assessment -> verify and validate TTP list and sequence.
  - CTI aggregation -> add mitigations.
- Currently working on improving TTP and order extraction with LLMs.

AI4CTI High-level Architecture



AI4CTI demo

- The security engineer uses the AI4CTI to learn on TTPs and mitigations of selected attack. The tool aids in identifying also the sequence of TTPs and mitigations.
- The tool allows the user to select the step:



  - Scrapping: Ingest advisories and attack graphs from Internet.
  - Graph Analysis:
    - Extract temporal relationships from the attack graph.
    - Visualise and fix possible errors in the detected steps in attack graph.
  - Structured Analysis: Extract TTPs from structured data.
  - Unstructured Analysis: Detect and temporarily order events (and TTPs) related to the attack from natural language reports (using LLMs).
  - Assessment: assess detected TTPs and order, and verify correctness.
  - Aggregation: adds mapped mitigations in order.

AI4CTI Future work

- Improve accuracy of sequencing and mapping of TTPs.
- Currently comparing results of several open source LLMs: miqu-1-70b-sf, Llama-2-70B, Mixtral-8x7B, etc.
- Currently defining a model of metrics for best result.
- In the early future: test with additional LLMs: Llama-3-70B, Mixtral-8x22B, ChatGPT4, etc.

AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

https://ai4cyber.eu/

https://twitter.com/Ai4Cyber

https://www.linkedin.com/company/ai4cyber/

Erkuden Rios

Project Coordinator

erkuden.ríos@tecnalia.com

Thank you for your attention!

Thank you for your attention

Questions?

ECCO
European Cybersecurity COmmunity

Challenges and intersection of AI and Cybersecurity

ECCO Roadmap WG Webinar on AI and Cybersecurity

29th May 2024

ECCO
European Cybersecurity COmmunity

Session 4: Generative AI-supported cyber incident simulation

Eider Iturbe

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

DYNABIC

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070455.


DYNABIC
cco
ybersecurity COmmunity
nal:a
QUE RESEARCH
ALLIANCE

Dynamic threat landscape

Need of proactive cybersecurity measures

New regulatory requirements

ECCO
European Cybersecurity COmmunity

DYNABIC

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Challenges

↓Real systems testing
↓System replica

DYNABIC

Challenges

↓Real systems testing

↓System replica

Simulation as a Solution

✓Simulation models

✓Digital Twin

Generative AI techniques

✓Potential replicating different types of data

Enhanced Incident Indicators

✓Aligned with reference entities


CYBER-PHYSICAL INCIDENT SIMULATION SYSTEM
SIM4BC
DYNABIC
tecnalia
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

SIM4BC

CYBER-PHYSICAL INCIDENT SIMULATION SYSTEM

ECCO
European Cybersecurity COmmunity

Simulation of cyber-physical attacks **without disrupting** business operations.

Graph-based threat modelling that provides an expert system to predict the effect of the incident within the system under study

AI-based synthetic incident-related data generation that accurately replicates multiple layers of the target system and simulates the trends of the data during a real incident

A **multi-layer approach** based on simulated environment

DYNABIC

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Simulation training

Real System
Incident Data Collection:
Capturing Real-world
Scenarios for Analysis

Incident reports
& dataset

Incident modeller

Rule-based
Expert System

Incident data
generator

AI models set

Simulation execution

SIM4BC Cyber Incident Simulation System

System security engineer

Incident modeller

Incident impact

Incident data generator

Incident synthetic data

Anomaly-based intrusion detection systems and other security controls

Attack graph

Selection of incident data to be simulated

SIM4BC

SYSTEM

NETWORK LAYERS

LOGS

APPLLICATION

Deploy in

Real System

DYNABIC

tecnalia

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

SIM4BC

The system enhances cyber security controls through the simulation of various incident scenarios

Data-driven predictions

Anomaly-based Intrusion Detection Systems utilize the simulated data to improve their detection algorithms.

The Cyber Incident Simulation System empowers defence capabilities against emerging sophisticated cyber security threats.

ECCO
European Cybersecurity COmmunity

DYNABIC

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Thank you for your attention

- **Website:** https://dynabic.eu
- **Follow us on Twitter:** @dynabic_eu
- **Follow us on LinkedIn:** https://www.linkedin.com/company/dynabic-eu/
- **Contact:** Erkuden.Rios@tecnalia.com

Jason.Mansell@tecnalia.com