

# ADVANCED CYBER SITUATIONAL AWARENESS FOR CYBER DEFENCE

From Research to Application

Florian Skopik, [florian.skopik@ait.ac.at](mailto:florian.skopik@ait.ac.at)

Markus Wurzenberger, [markus.wurzenberger@ait.ac.at](mailto:markus.wurzenberger@ait.ac.at)

Wien, 18.09.2024



# AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

 Federal Ministry  
Republic of Austria  
Climate Action, Environment,  
Energy, Mobility,  
Innovation and Technology

50,46%

 **INDUSTRIELLEN  
VEREINIGUNG**

Federation of Austrian  
Industries

49,54%

*“As a national and international network node at the interface of science and industry AIT enables innovation through its scientific-technological expertise, market experience, tight customer relationships and high quality research infrastructure.”*

AIT Austrian Institute of Technology

**Employees:** 1500+  
**Total Revenues:** 199,7 Mio €  
**Business Model:** 40:30:30

Digital Safety &  
Security

Health &  
Bioresources


Vision,  
Automation &  
Control

Innovation  
Systems & Policy

Energy

Transport  
Technologies

Technology  
Experience

 Federal Ministry  
Interior

 Federal Ministry  
Republic of Austria  
Defence

 EUROPA  
INTEGRATION  
AUSSERES  
BUNDESMINISTERIUM  
REPUBLIK ÖSTERREICH




 Federal Chancellery



Strategic Partnerships

Innovation System

# THE CYBER SECURITY RESEARCH PROGRAM

- Cyber security research program established 2009, now approx. 50 people
- **One stop shop** for cyber security with high **expertise in selected areas**
- **OpenScience** = OpenSource  + OpenData  + OpenAccess 
- Strong partnership with **national authorities**: MoD, ministry of the interior
- Strong **research** networks (EU EDF/HEU/KDT, ECSO, EARTO...)
- Strong **industry** connections, including some strategic partnerships, with ...

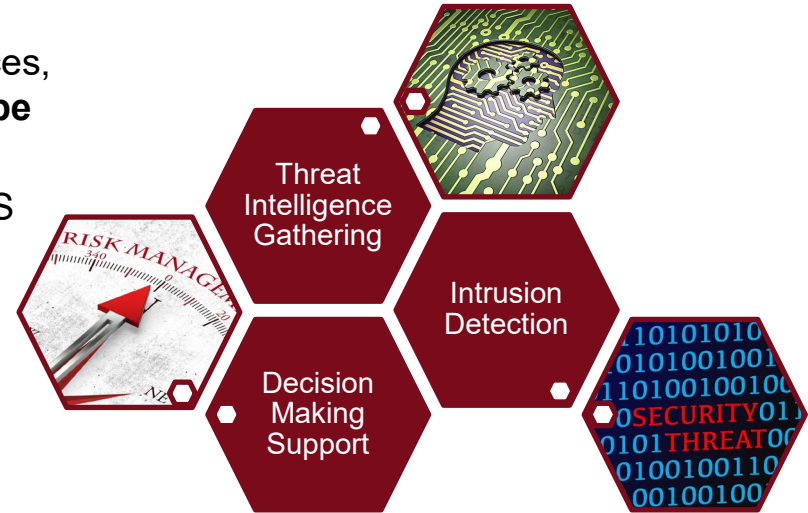


# WHAT IS SITUATIONAL AWARENESS?

- **Common Definition**
  - “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future” (Endsley, 1995).
  - **Three levels of increasing awareness:** **Perception** of the elements in the environment within a volume of time and space, the **comprehension** of their meaning and the **projection** of their status in the near future
- **Multifaceted Concept**
  - **Technical view:** compiling, processing, and fusing data
    - **Relate** and **evaluate** pieces of information relative to each other
  - **Cognitive view:** capacity to comprehend the technical implications and draw conclusions to take informed decisions
  - Focus often primarily on cognitive aspects

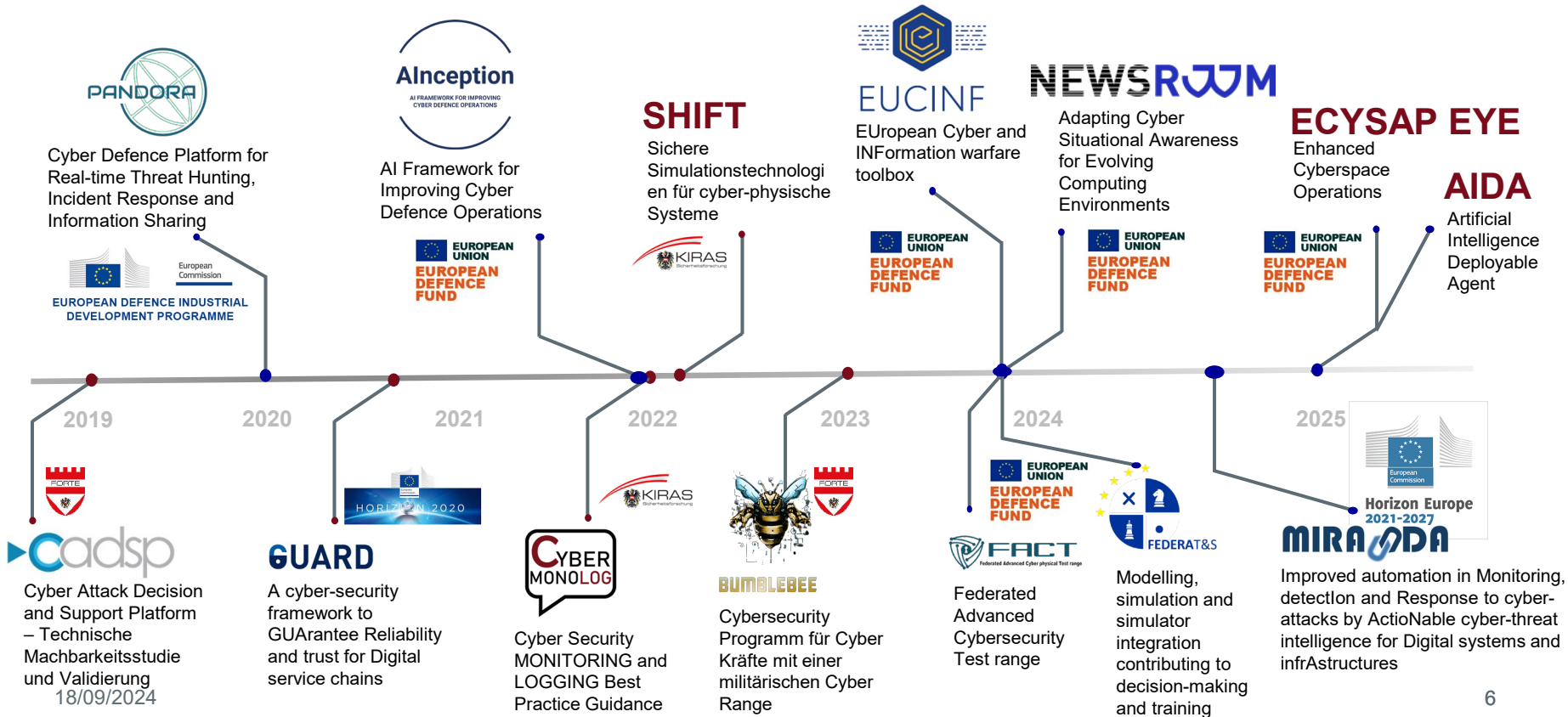
# WHAT IS CYBER SITUATIONAL AWARENESS AND WHY DO I NEED IT?

- **Cyber Situational Awareness (CSA)**
  - Use of **data from IT sensors** (IDSs, OSINT sources, etc.) that can be **fed to a data fusion** process or **be interpreted** directly by the decision-maker
  - Example: Combination of a cyber sensor (e.g., IDS alert) and an ordinary sensor (e.g., a human intelligence report) enhance CSA overall
- Many **Applications of CSA**
  - **Proactive Risk Management** and Attack Surface Reduction
  - **Threat Identification** and Response
  - Informed **Decision Making** and Strategic Planning

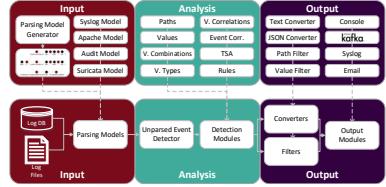


Franke, Ulrik, and Joel Brynielsson. "Cyber situational awareness—a systematic review of the literature." *Computers & security* 46 (2014): 18-31.

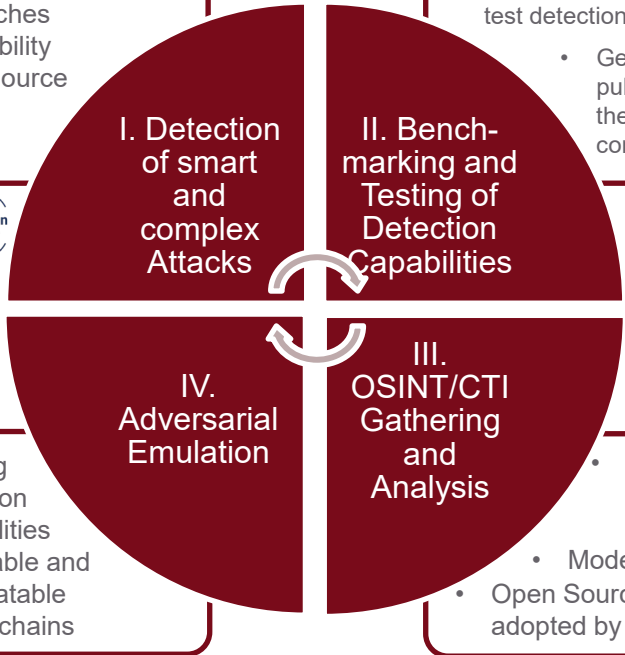
# CYBER DEFENSE RESEARCH PROJECTS @ AIT



# RESEARCH TOPICS IN ATTACK & DEFEND



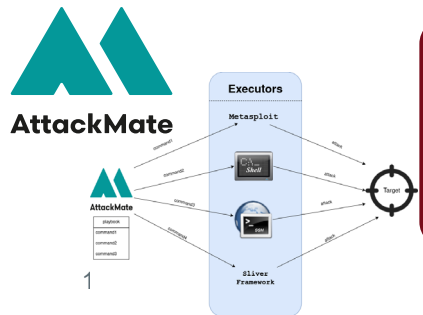
- Novel ML/AI approaches
- Int'l visibility
- Open Source sensor



- Virtual environments to test detection solutions
- Generation of public data for the research community

- Testing detection capabilities
- Adaptable and automatable attack chains

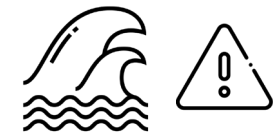
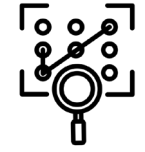
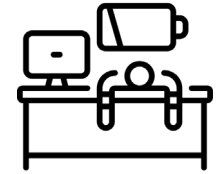
- Decision making support
- Modern NLP
- Open Source solutions adopted by CERTs



# DETECTION OF SMART AND COMPLEX ATTACKS (1/2)

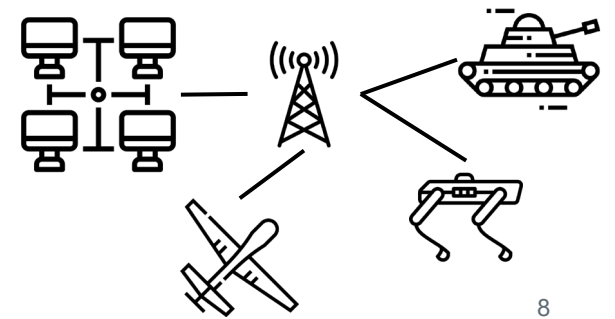
- **Current situation**

- Rapidly growing complex digital infrastructures and fast changing threat landscape
- Distributed networks lacking connectivity and resources, require autonomous IDS
- Anomaly detection causes thousands of context free alerts → **>80% false positives** and duplicates
- Manual triage is cumbersome and labor-intensive → **Alert fatigue**
- Virtualization and encryption make network analysis impossible



- **Objectives**

- Improve log parsing using Transformers
- Automate configuration of IDS and establish self-adaptability
- Resolve existing issues with detection using deep learning
- Automate triage and interpretation of alerts



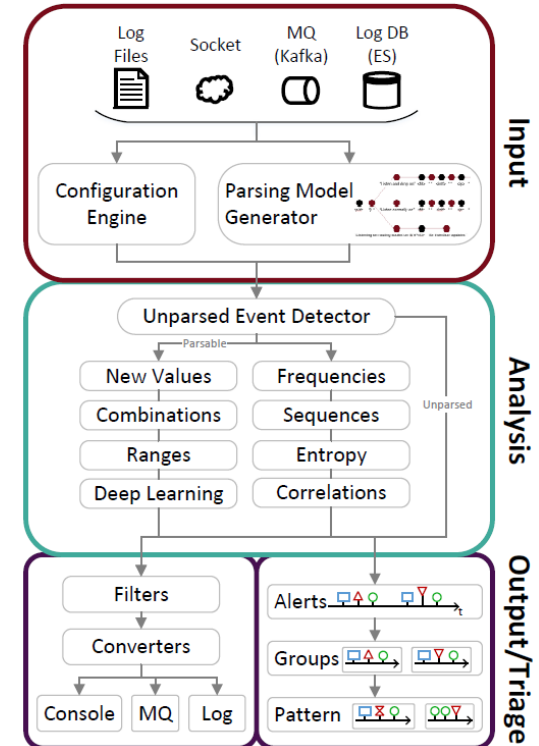


# DETECTION OF SMART AND COMPLEX ATTACKS (2/2)

## Log data anomaly detection made in Austria

- **Automatically learn baseline of normal behavior**
  - Parser generator → Analyze verbose custom logs
  - Configuration engine → Select detectors and parameters
- **Lightweight online detection**
  - Enable resource-efficient and decentralized detection
  - Mitigate impact of alert flooding
  - Integrate with existing solutions: Flexible interfaces
- **Use science based cutting edge technologies**
  - Data science, machine learning, and statistics
  - AI, Deep, federated, and transfer learning
  - Transformers: Word and sentence embeddings

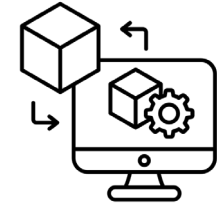
## AMiner Pipeline



# BENCHMARKING AND TESTING OF DETECTION CAPABILITIES (1/2)

## Objectives

- Verify protection against current and emerging threats
- Test IDS and compare configurations outside productive systems

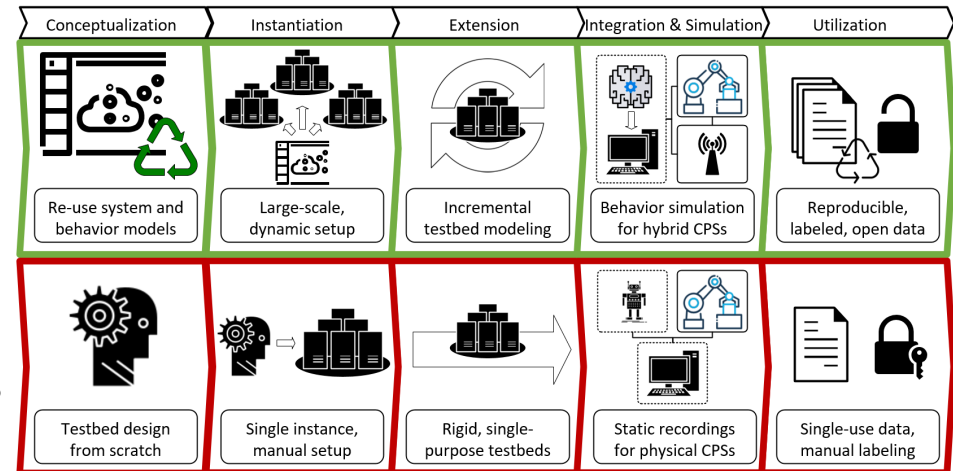


## Current challenges in testbed design

- Comply with today's complex infrastructures (IoT, CPS, ICS, ect.)
- Dynamic, and reproducible testbeds
- Generate realistic and relevant data

## Application areas of testbeds

- Training and exercise environments
- Deception technologies and digital twins
- Research dataset generation



# BENCHMARKING AND TESTING OF DETECTION CAPABILITIES (2/2)

## AIT Testbed - AttackBed

- Model-driven, reproducible, portable, and customizable
- Integration of physical components (CPS, IoT, ICS, etc.)
- Labelled Open data including realistic normal behavior and relevant attacks

## State of the art technologies

- Open Stack
- Ansible
- Terragrunt
- Open source



ANSIBLE

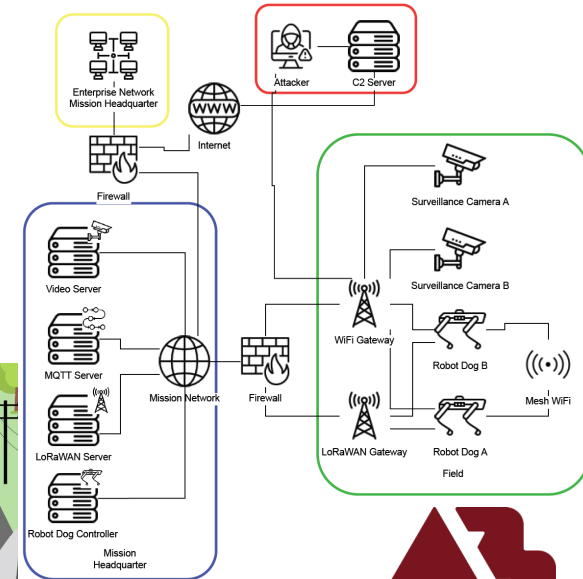
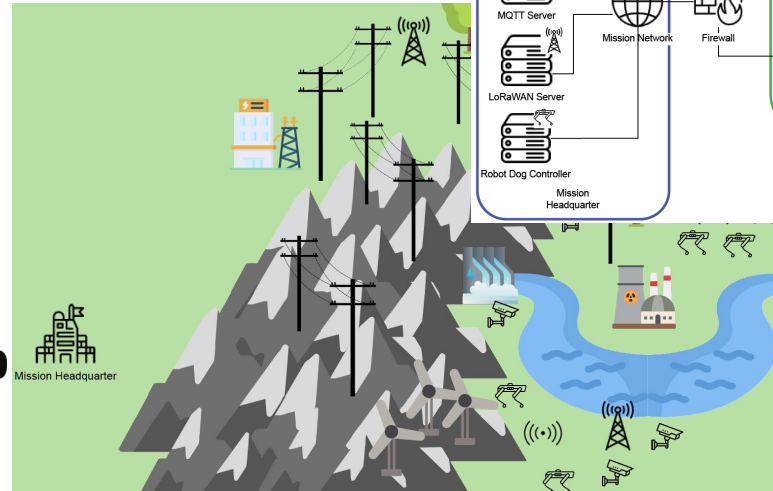


zenodo

<https://github.com/ait-testbed>

<https://zenodo.org/records/5789064>

18/09/2024

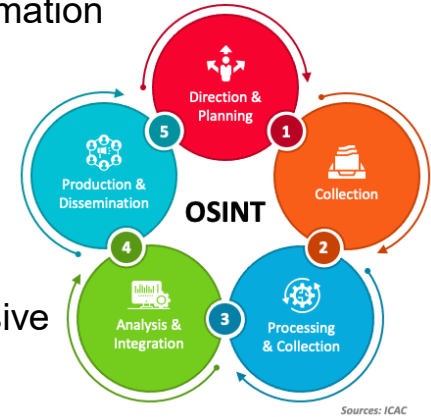


AttackBed

NEWS ROOM

# OSINT/CTI GATHERING AND ANALYSIS (1/2)

- OSINT: open source information – structured data v.s. unstructured information
- Usage of “soft” CTI in natural language for human consumption
  - News about threat actors
  - New (features of) security products
  - News about breaches, incidents, campaigns
  - News about vulnerabilities, patches, mitigations, counter-measures, ...
- Number of OSINT sources is high and the number of news items is massive
  - **Grasp quickly what’s relevant and omit the rest**
  - Maintain situational awareness and take early counter actions
- NLP and LLM capabilities
  - Extraction of relevant **named entities**
  - **Clustering** of related **news items**
  - **Summaries** of “story clusters”
  - **Recommendations** of news items
  - Support for **creating OSINT products** (“reports”)



**User Story 1:** *What are the 'hot topics' of the last 24 hours?*

**User Story 2:** *What do we know about a specific entity?*

**User Story 3:** *How can I find more related news items?*

**User Story 4:** *Which news items are relevant for my mission?*

**User Story 5:** *How can I efficiently sum up my findings for decision makers?*



# OSINT/CTI GATHERING AND ANALYSIS (2/2)

**NER**

**Relevance Ranking**

**Advanced Search**

**Summary Creation**

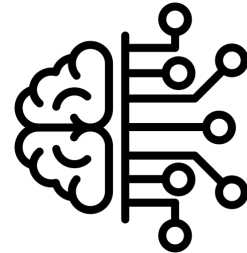
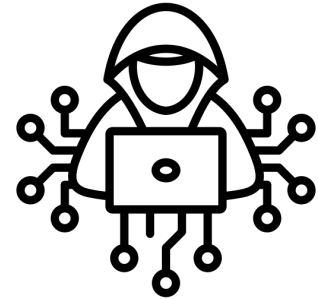
**Story Clustering**

The screenshot displays the TARANIS AI search results page for the query 'crowdstrike'. The interface includes a search bar at the top left with the query 'crowdstrike' and a 'NER' callout. Below the search bar are filters for 'Source Group', 'Source', and 'Filter' (day, week, 24h). A 'Relevance Ranking' callout points to the 'relevance' sort option. The main content area shows a list of search results, with the top result expanded to show a detailed article snippet. A 'Summary Creation' callout points to the article text. At the bottom right, a 'Story Clustering' callout points to the article's metadata. The interface also shows a 'Dashboard', 'Administration', 'Assess', 'Analyze', 'Publish', and 'Assets' menu at the top right. The search results list includes the following entries:

- Published:** 2024-07-22 22:47, 2024-07-24 17:33. **Tags:** Falcon, Origin, ESPO, Changelist, Rapid, Windows, Crowdstrike, Microsoft, Microsofts, JPC, Template Type, Avast, Intel, Acron, Onpoint, One, Kernel, Linux, Repository. **Article:** arstechnica.com
- Published:** Jul 24, 2024, 17:33. **Author:** arstechnica.com. **Article:** arstechnica.com
- Published:** Jul 24, 2024, 05:17. **Author:** og.theregister.com. **Article:** og.theregister.com
- Published:** Jul 24, 2024, 17:25. **Author:** heise.de. **Article:** heise.de
- Published:** Jul 24, 2024, 14:28. **Author:** darkreading.com. **Article:** darkreading.com
- Published:** Jul 24, 2024, 14:02. **Author:** thehackernews.com. **Article:** thehackernews.com
- Published:** Jul 24, 2024, 12:20. **Author:** hellobotsecurity.com. **Article:** hellobotsecurity.com
- Published:** Jul 24, 2024, 10:16. **Article:** thehackernews.com

# ADVERSARIAL EMULATION (1/2)

- Objectives
  - Attack surface monitoring: Reveal zero-day vulnerabilities
  - Verify protection against current threats
  - Implement complex attacks following cyber kill chain
  - Adapt emulation depending on the circumstances (living off the land)
- Requirements
  - Automate attack orchestration and emulation
  - Employ AI for threat hunting (e.g., reinforcement learning)
- Relevance and related areas
  - Lack of security support for heterogenous infrastructures including IT, OT, IoT, CPS, legacy systems, proprietary and customized military systems
  - Red teaming, cyber range trainings and exercises, penetration testing





# OPEN SOURCE TOOLS READY TO BE USED ...



<https://github.com/ait-aecid/logdata-anomaly-miner>



<https://github.com/ait-testbed/attackbed>



<https://github.com/ait-testbed/attackmate>



<https://taranis.ai/>



# BENEFIT FOR AUSTRIA?

- **Insights** into the military domain and **cutting-edge technologies** from market leaders
- Networking and stakeholder engagement across Europe – **Visibility!**
  - Even facilitates cooperation with other Austrian stakeholders
- Solutions are **Open Source**
  - **Dual use** – Military and civil application!
  - Focus on documentation, GettingStarted, and easy deployment for quick adoption
- **Multiplier for national research projects**
  - AT->EU: significantly increase TRL of national results; exploitation on EU level
  - EU->AT: access to EU cyber defence technologies, collaboration with large industries, adoption of knowledge from European partners

## IN EIGNER SACHE ...

- Wir suchen **Verstärkung** für unser **Team!**
    - Entwickler\*innen / DevOps
    - Researcher\*innen
    - Projektleiter\*innen
  - Jobs werden die nächsten Wochen ausgeschrieben.
  - Bei Interesse wenden Sie sich bitte schon jetzt an [florian.skopik@ait.ac.at](mailto:florian.skopik@ait.ac.at)
  - Details gerne auch am Stand!
- **Umfrage** zu IT Nutzerverhalten und Herausforderungen des Security Monitorings in Security Operations Centers (SOCs)
  - <https://survey.ait.training>



# THANK YOU!

Please contact:

[florian.skopik@ait.ac.at](mailto:florian.skopik@ait.ac.at)

[markus.wurzenberger@ait.ac.at](mailto:markus.wurzenberger@ait.ac.at)

