AIT CYBER SECURITY

Cyber Security Research and Training

Martin Stierle

AIT Austrian Institute of Technology

Center for Digital Safety & Security

Martin.Stierle@ait.ac.at

25. Mai 2022

AIT CYBER SECURITY FOCUS AREAS

Anomaly Detection & Threat Intelligence

New Risk Management Approaches

Safety and Security co-engineering

Next Generation Cryptography

Cyber Range: Cyber Security Training and Exercise

Penetration Testing

ANOMALY DETECTION - THE ÆCID ECO-SYSTEM

AUSTRIAN INSTITUTE OF TECHNOLOGY

Today's Cyber Security Challenges

Advanced Persistent Threats

- targeted high-profile attacks
- unknown attack anatomy
- multiple attack vectors
- unknown traces in the network and on the host in numerous log data sources
- However, often similar traces across organizations with similar systems!

Signature-based solutions cannot protect from Zero Day exploits and individual attacks**.**

AIT Technologies

Data Acquisition
across technological layers on different machines, systems and organizational units

Self learning / Self Adaptive AD
Reduction of false positives; low human effort; flexible adaption to new attack vectors

Algorithms and PoCs
machine learning on computer log data Proof-of-Concepts (in Linux Debian/Ubuntu)

Cyber Threat Intelligence
Extraction of indicators and TTPs from anomalies and sharing/validation via MISP

MISP Threat Sharing

AIRBUS

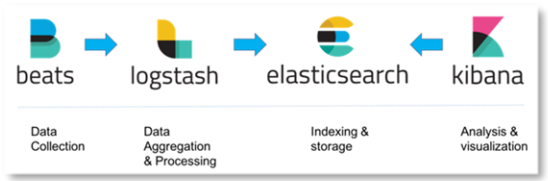
T-Systems

CyberTrap

REPUBLIC OF AUSTRIA FEDERAL MINISTRY OF DEFENCE

IAEA International Atomic Energy Agency

TITLE	CITED BY	YEAR
Combating advanced persistent threats: From network event correlation to incident detection I Friedberg, F Skopik, G Settanni, R Fiedler Computers & Security 48, 35-57	128	2015



AIT Solution: ÆCID

https://aecid.ait.ac.at

Distributed Anomaly Detection Engine
Self-learning and flexible anomaly detection

- Learns the structure of log data of any form on the fly
- Creates and continuously evaluates hypotheses of good system behavior
- Adapts to system changes with minimal human effort
- Uses customized and patented cutting-edge machine learning technology
- 100% AIT's IPR – room for improvements in research projects
- Interfaces well with Kafka and RabbitMQ, as well as the (B)ELK Stack
- Validates findings through MISP
- Packages for Debian and Ubuntu

debian

CYBER SECURITY BY DESIGN FOR MISSION CRITICAL SYSTEMS

AUSTRIAN INSTITUTE OF TECHNOLOGY

LieberLieber · msg PLAUT · AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

www.threatget.com

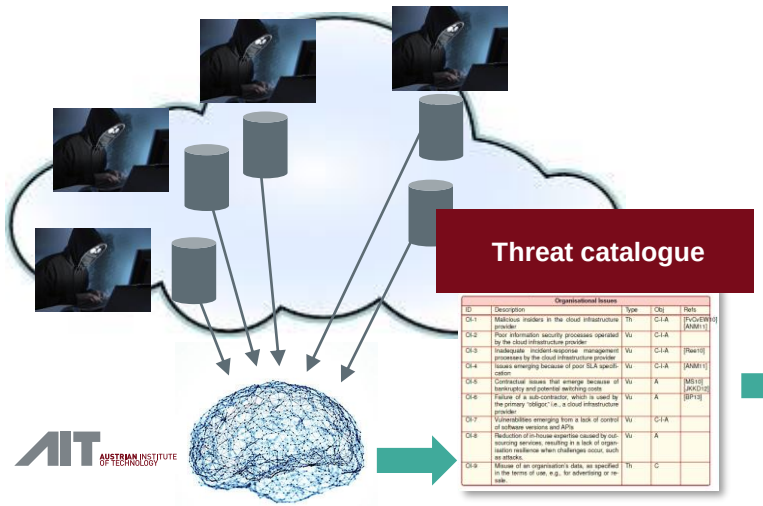
SAFETY & SECURITY BY DESIGN FÜR AUTOMOTIVE

Modell-based System engineering

Threats Automated Generation

Standards Compliance

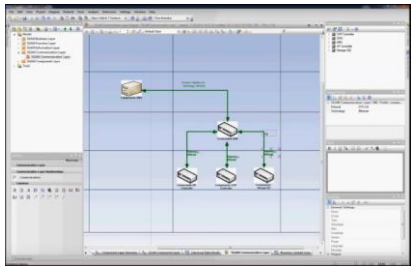
Safety & Security Modelling

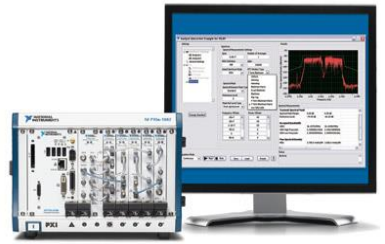


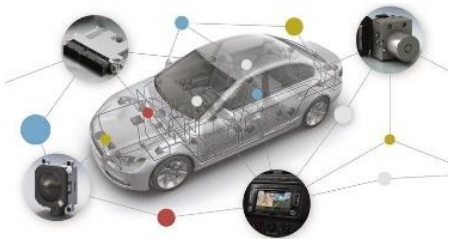
Threat catalogue

EN 50128 | ISO 27001 | ISO 26262 | ISO 21434 | IEC 62443

FMVEA
Model based System Design







LieberLieber

ENTERPRISE ARCHITECT

www.threatget.com

DEVELOPED BY AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

CYBER SECURITY RISK ASSESSMENT

IMPACT	LIKELIHOOD: 1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain	
1 Trivial	1	2	3	4	5	Low 1:5
2 Minor	2	4	6	8	10	Medium 6:10
3 Moderate	3	6	9	12	15	High 11:16
4 Major	4	8	12	16	20	Extreme 17:25
5 Critical	5	10	15	20	25	

THREATGET

FFG Forschung wirkt. Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie | KIRAS | HORIZON 2020 | ECSEL Austria | CySiVuS | IoT4CPS Trustworthy IoT for CPS | Productive 4.0 | AQUAS | afarcloud | SECREDAS

NEXT GENERATION CRYPTOGRAPHY

AUSTRIAN INSTITUTE OF TECHNOLOGY

CATCH. DIRECT

DAS NEUE ZEITALTER DER PRODUKTIVITÄT

Automatisierte Auftragsabwicklung entlang der Lieferkette.

EBNER® Industrieofenbau GmbH

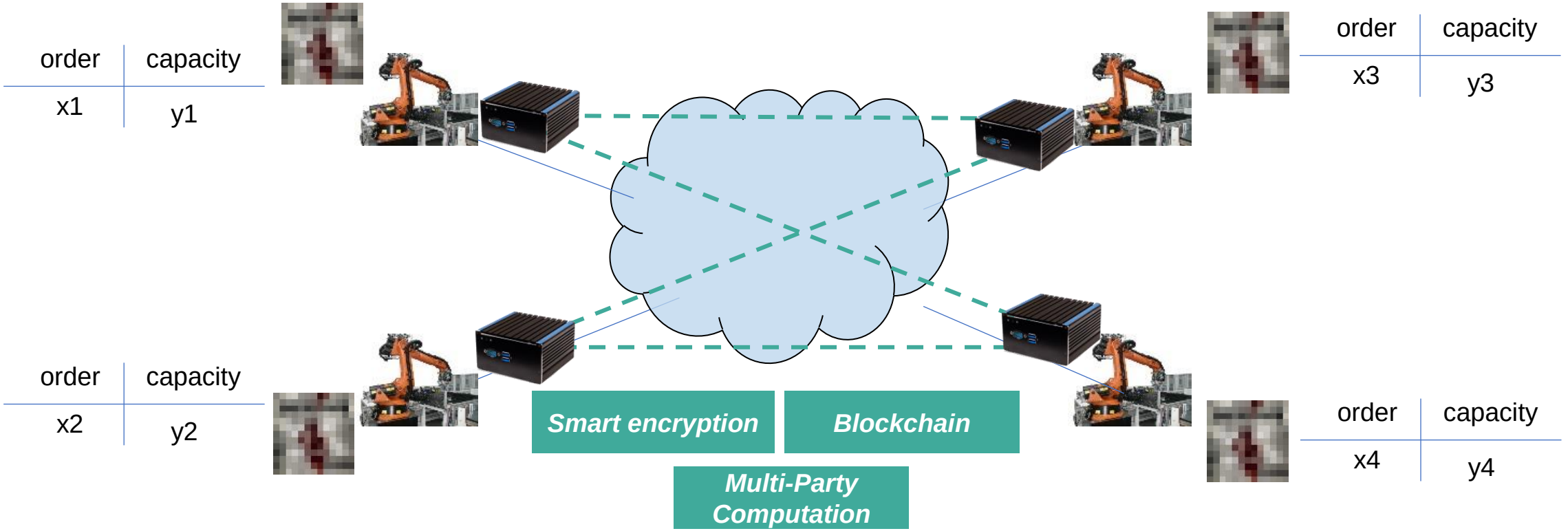
NET SERVICES

AUSTRIAN INSTITUTE OF TECHNOLOGY

https://www.catch.direct/

MARKET PLACE 4.0 – SECURE AUCTIONS OF PRODUCTION CAPACITIES

- Secure and verifiable auctions of production capacities
- No central data management
- Decentralized data matching on encrypted data
- Production data cannot be seen by externals



AIT CYBER RANGE

WHAT IS A CYBER RANGE

REFERENCE PROJECTS

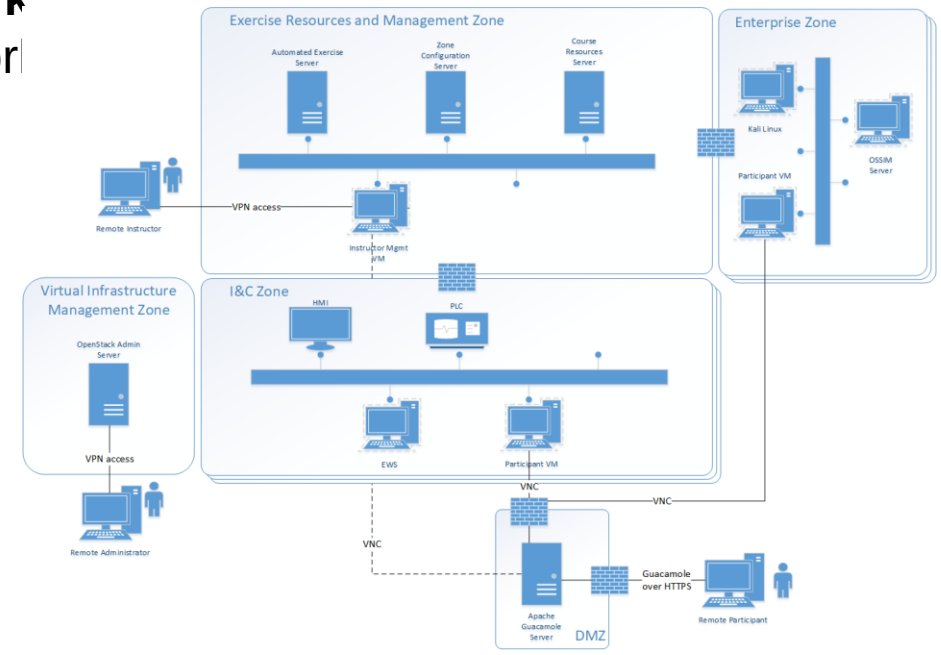
www.cyberrange.at

AIT´S CYBER RANGE TRAININGS

CYBER RANGE

Virtuel environment for ICT infrastructers

- Allows simulation or emulation **of large and complex network structures** with different (flexible) system components, networ and users
- Is a secure and realistic environment for testing and analysis of incidents **without attacking the real producion systems**
- For different **application domains** (Information Technology, Operational Technology, etc.)



INTERNATIONAL COMPETENCE CENTER FOR IT/OT CYBER SECURITY TRAINING


Advanced Persistent Threat (APT)


Ransomware


Trojaner / Remote Access Trojaner


Botnets


Data breach (DSGVO)


Phishing


Vulnerability


DDoS


Misconfiguration


News


Simulation of Stakeholder (z.B. CERT, Trust Circle)


And many more…

KURATORIUM SICHERES ÖSTERREICH

Federal Chancellery Republic of Austria

Federal Ministry Interior

Federal Ministry Republic of Austria Defence

OSCE

EUROPEAN SECURITY AND DEFENCE COLLEGE — ESDC — COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE — CESD

ESCD
European Security Defence College

CEE

Kasachstan

Korea

Oman

IAEA

INL Idaho National Laboratory

URS

WINS

IAEA

Nuclear Security Training and Support Centres (NSSC Network)

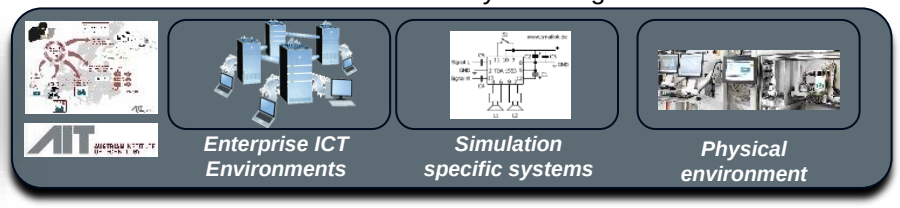
UNITED NATIONS OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

EVN

Verbund

AIT Cyber Range

DEVELOPED BY AIT AUSTRIAN INSTITUTE OF TECHNOLOGY




Industry 4.0 *Smart City* *Connected Cars* *Digital Transport* *Smart Grid*

AIT's Cyber Range Training platform for IT/OT

KIRAS Sicherheitsforschung

HORIZON 2020

sparks SMART GRID PROTECTION AGAINST CYBER ATTACKS

prisma cloud

SOCCRATES

CREDENTIAL

Nobel Grid Smart energy for people

seccrit SEcure Cloud computing for CRitical infrastructure IT

Ecossian

GUARD

THANK YOU!

Martin Stierle
Head of Competence Unit
Security & Communication Technologies
Center for Digital Safety & Security

AIT Austrian Institute of Technology GmbH
Giefinggasse, 1210 Wien, Austria
Martin.stierle@ait.ac.at | www.ait.ac.at

https://cyberrange.at