Towards a fully automated Blue Team at Locked Shields

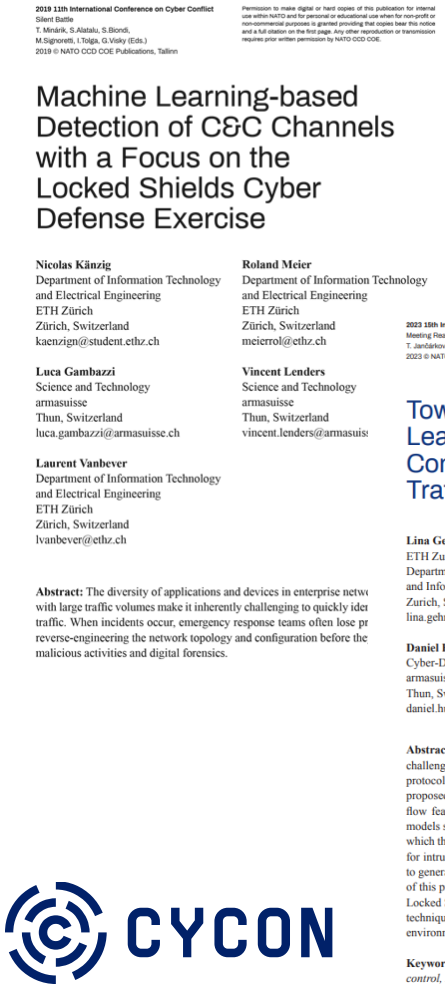
Dr. Roland Meier

armasuisse

Switzerland

CYCON

The history



2019 11th International Conference on Cyber Conflict
Silent Battle
T. Minárik, S.Alatalu, S.Biondi,
M.Signoretti, I.Tolga, G.Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Permission to make digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission by NATO CCD COE.

Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise

Nicolas Känzig
Department of Information Technology and Electrical Engineering
ETH Zürich
Zürich, Switzerland
kaenzign@student.ethz.ch

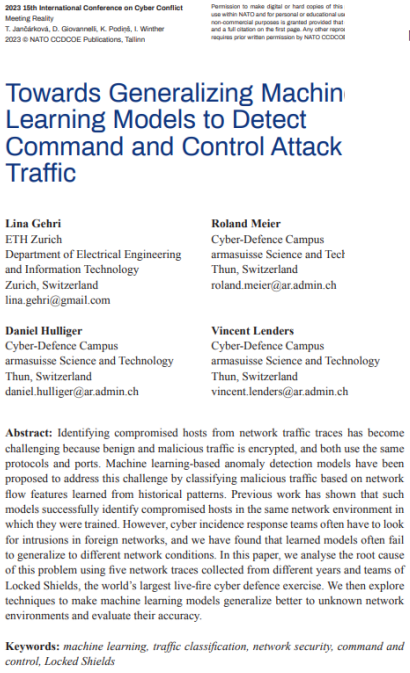
Roland Meier
Department of Information Technology and Electrical Engineering
ETH Zürich
Zürich, Switzerland
meierrol@ethz.ch

Luca Gambazzi
Science and Technology
armasuisse
Thun, Switzerland
luca.gambazzi@armasuisse.ch

Vincent Lenders
Science and Technology
armasuisse
Thun, Switzerland
vincent.lenders@armasuis

Laurent Vanbever
Department of Information Technology and Electrical Engineering
ETH Zürich
Zürich, Switzerland
lvanbever@ethz.ch

Abstract: The diversity of applications and devices in enterprise netwo with large traffic volumes make it inherently challenging to quickly ider traffic. When incidents occur, emergency response teams often lose pr reverse-engineering the network topology and configuration before the malicious activities and digital forensics.



2023 15th International Conference on Cyber Conflict
Meeting Reality
T. Jančárková, D. Giovannelli, K. Podiņš, I. Winther
2023 © NATO CCDCOE Publications, Tallinn

Permission to make digital or hard copies of this use within NATO and for personal or educational use non-commercial purposes is granted provided that and a full citation on the first page. Any other repro requires prior written permission by NATO CCDCOE

Towards Generalizing Machin Learning Models to Detect Command and Control Attack Traffic

Lina Gehri
ETH Zurich
Department of Electrical Engineering and Information Technology
Zurich, Switzerland
lina.gehri@gmail.com

Roland Meier
Cyber-Defence Campus
armasuisse Science and Tech
Thun, Switzerland
roland.meier@ar.admin.ch

Daniel Hulliger
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland
daniel.hulliger@ar.admin.ch

Vincent Lenders
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland
vincent.lenders@ar.admin.ch

Abstract: Identifying compromised hosts from network traffic traces has become challenging because benign and malicious traffic is encrypted, and both use the same protocols and ports. Machine learning-based anomaly detection models have been proposed to address this challenge by classifying malicious traffic based on network flow features learned from historical patterns. Previous work has shown that such models successfully identify compromised hosts in the same network environment in which they were trained. However, cyber incidence response teams often have to look for intrusions in foreign networks, and we have found that learned models often fail to generalize to different network conditions. In this paper, we analyse the root cause of this problem using five network traces collected from different years and teams of Locked Shields, the world's largest live-fire cyber defence exercise. We then explore techniques to make machine learning models generalize better to unknown network environments and evaluate their accuracy.

Keywords: *machine learning, traffic classification, network security, command and control, Locked Shields*

TAL TECH

DOCTORAL THESIS

Automating Defences against Cyber Operations in Computer Networks

Mauno Pihelgas

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2021

Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture

Paul Theron
Thales
Salon de Provence, France
paul.theron@thalesgroup.com

Alexander Kott
U.S. Army Research Laboratory
Adelphi, MD, USA
alexander.kott1.civ@mail.mil

Martin Drašar
Masaryk University
Brno, Czech Republic
drasar@ics.muni.cz

Krzysztof Rzadca
University of Warsaw
Warsaw, Poland
krzadca@mimuw.edu.pl

Benoît LeBlanc
Ecole Nationale Supérieure de Cognitique
Bordeaux, France
benoit.leblanc@ensc.fr

Mauno Pihelgas
NATO CCDCOE
Tallinn, Estonia

Luigi Mancini
Sapienza University
Rome, Italy

Agostino Panico
Sapienza University
Rome, Italy

***Abstract*—Within the future complex massively interconnecte vehicles, sensors and effectors, an demanding extremely low failure r operators cannot have an easy a enough reactions to cyber-attacks, and intelligent cyber defense. Mu Defense may provide an answer to presents the concept and archi Intelligent Cyber defense Agent (rationale of the AICA concept. methodology and purpose that dri Reference Architecture (AICARA) and Technology Group. Thirdly, features and challenges of Multi defense Agent (MAICA). Fourth assumed AICA Reference Architec our preliminary research issues, a we present the future lines of resea test the AICA / MAICA concept.**

Keywords—intelligent agent, a security

I. RATIONALE FOR TE

Today, five broad types of syste Air operations:

- Office and information includes web service information managemen human resource manag

This paper is based on NATO "Intelligent, Autonomous and and Resilience."

978-1-5386-4559-8/18/$31.00 C2018 IEE

2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Towards an AI-powered Player in Cyber Defence Exercises

Roland Meier
Department of Information Technology and Electrical Engineering
ETH Zürich
Zürich, Switzerland
meierrol@ethz.ch

Artūrs Lavrenovs
NATO CCDCOE
Tallinn, Estonia
arturs.lavrenovs@ccdcoe.org

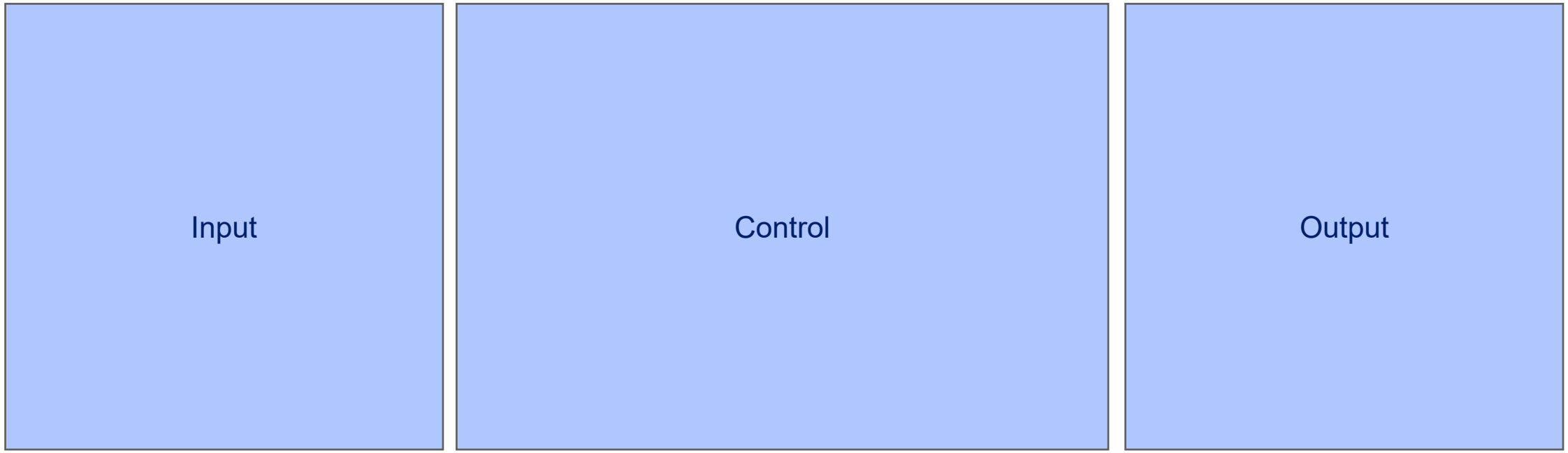
Kimmo Heinäaro
NATO CCDCOE
Tallinn, Estonia
kimmo.heinaaro@mil.fi

Luca Gambazzi
Science and Technology
armasuisse
Thun, Switzerland
luca.gambazzi@armasuisse.ch

Vincent Lenders
Science and Technology
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

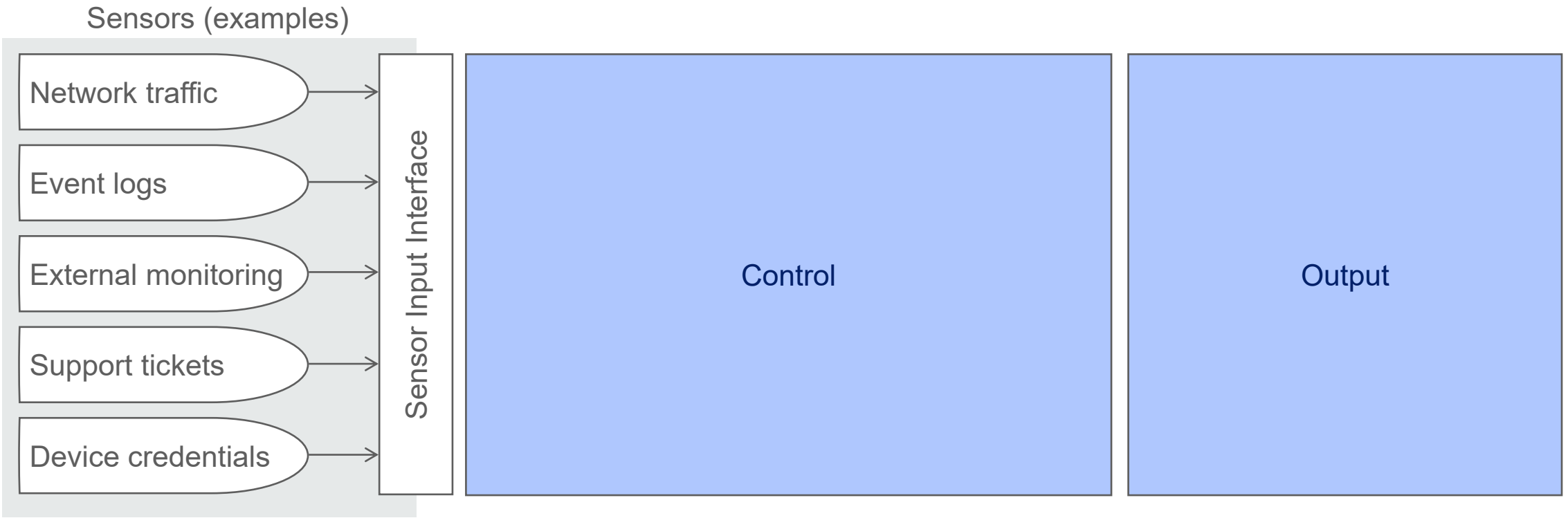
CYCON

Automated Blue Team framework overview



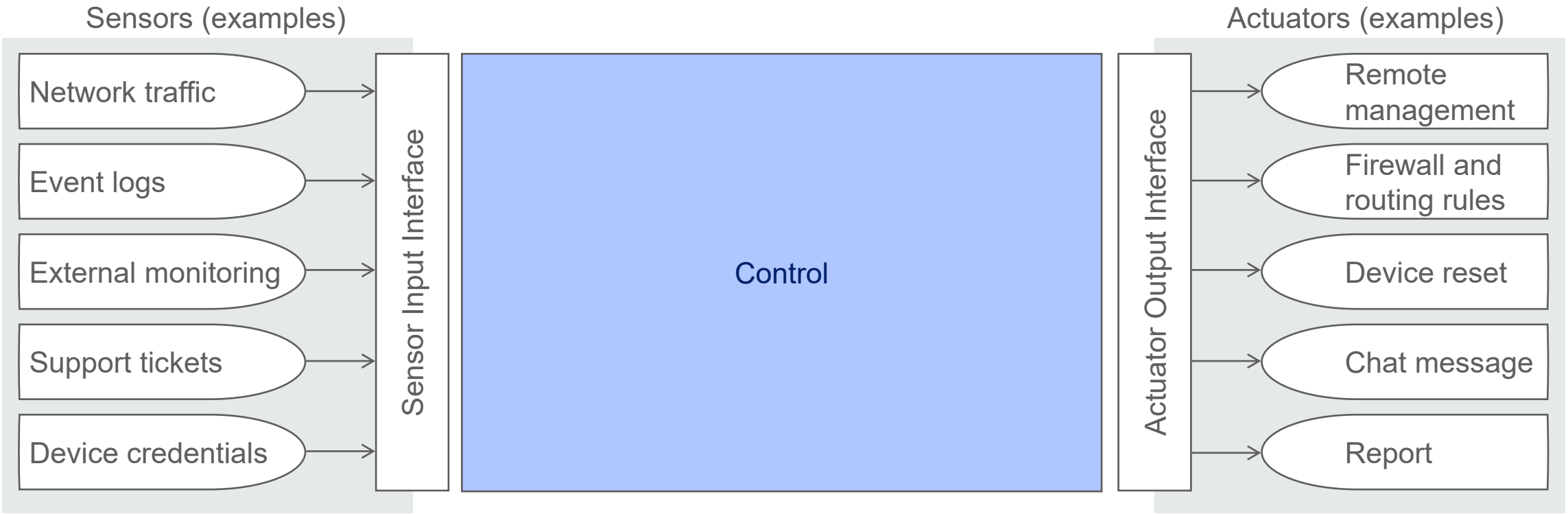
CYCON

Automated Blue Team framework overview



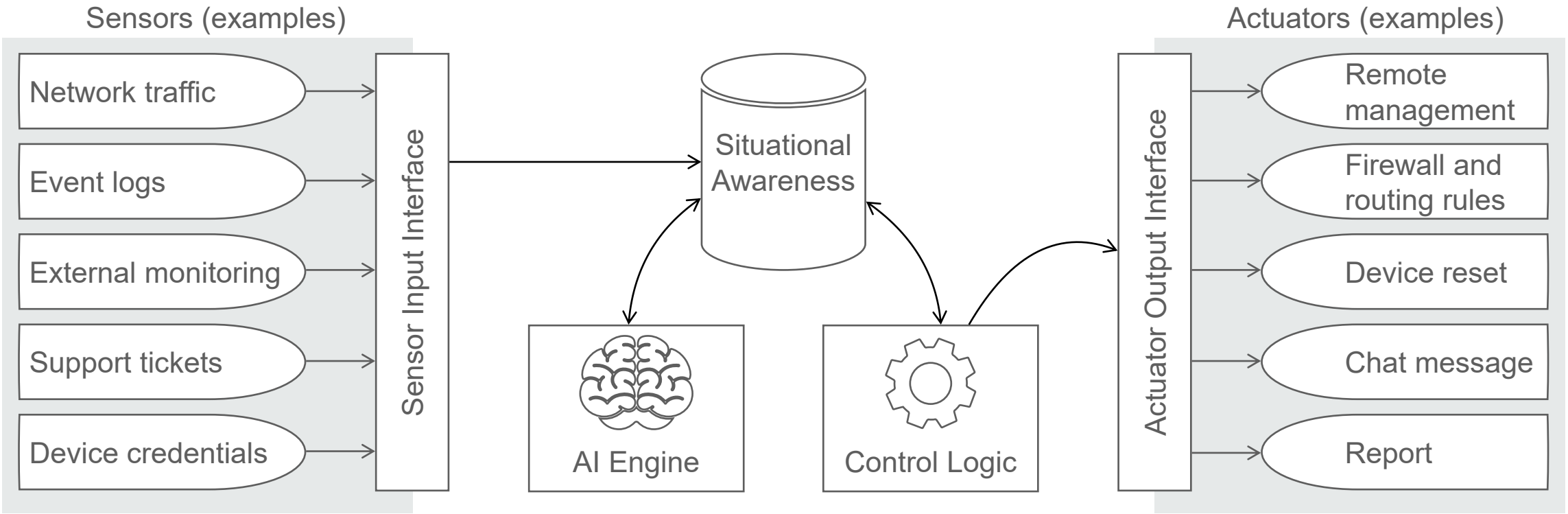
CYCON

Automated Blue Team framework overview



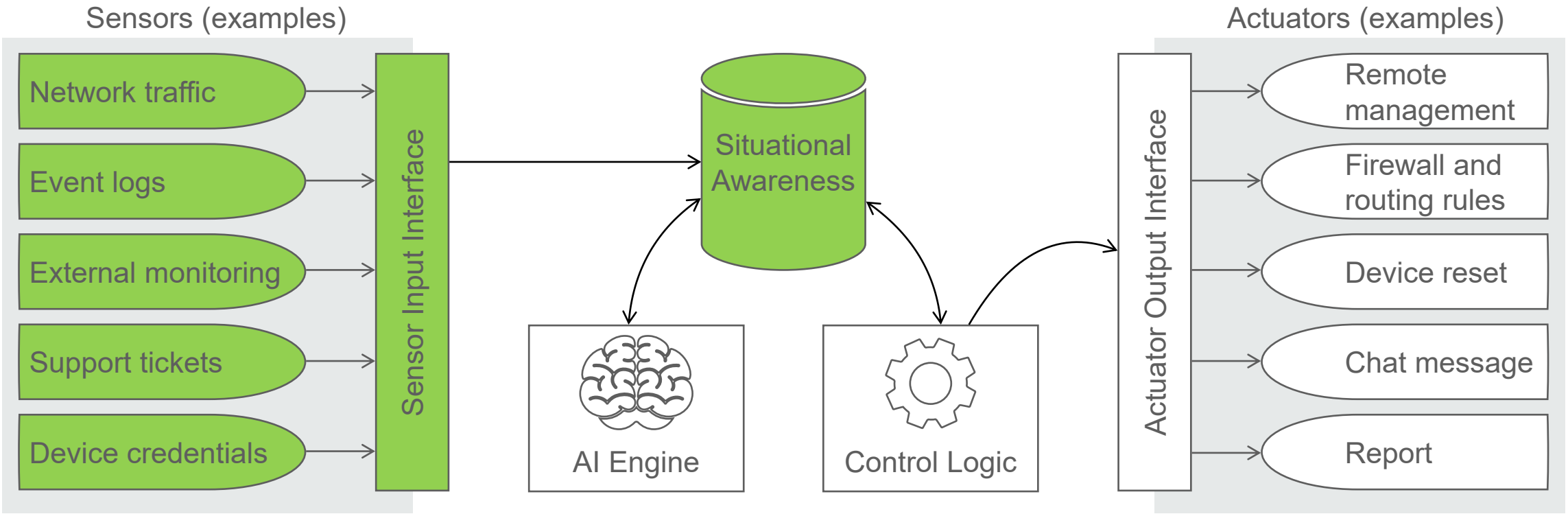
CYCON

Automated Blue Team framework overview



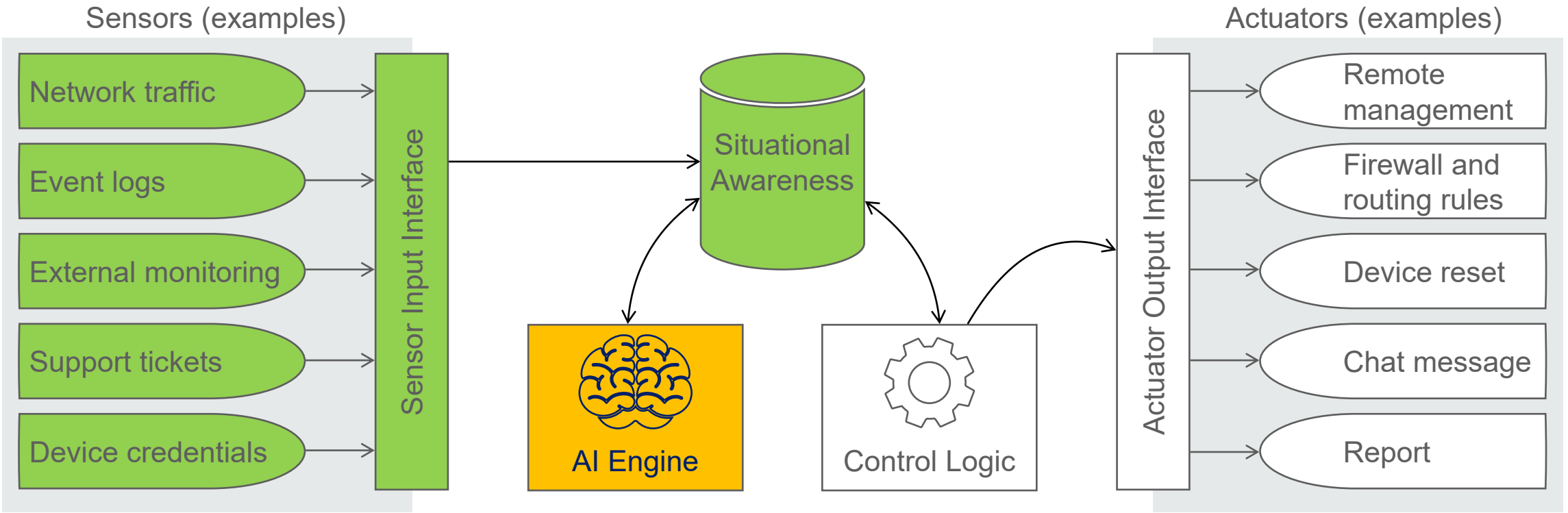
CYCON

Automated Blue Team framework overview



CYCON

Automated Blue Team framework overview



CYCON

Four levels of AI

CYCON

Four levels of AI

Level 0: Reactive narrow AI

Signature-based decisions

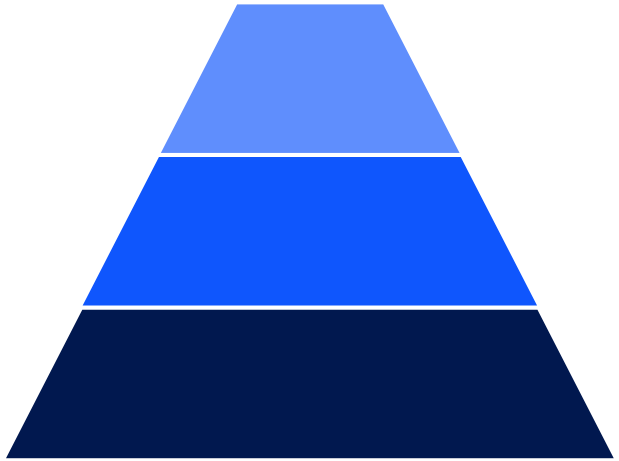
CYCON

Four levels of AI

Level 1: Limited-memory narrow AI	“Machine learning” today
Level 0: Reactive narrow AI	Signature-based decisions

CYCON

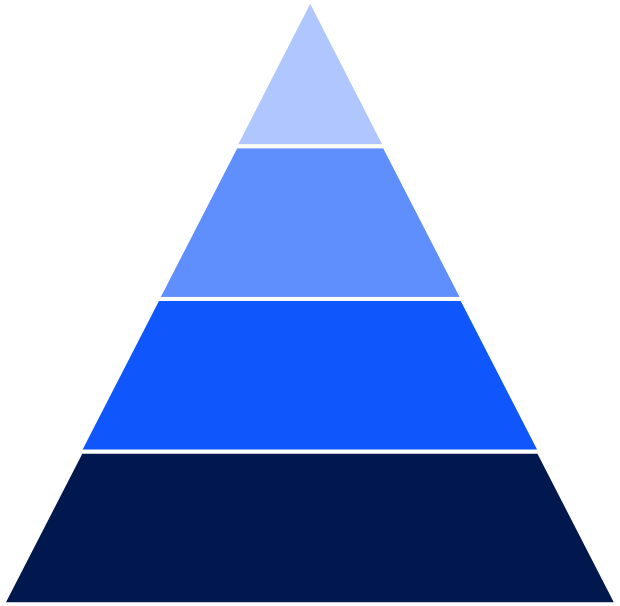
Four levels of AI



Level 2: General AI	Mimics human intelligence
Level 1: Limited-memory narrow AI	“Machine learning” today
Level 0: Reactive narrow AI	Signature-based decisions

CYCON

Four levels of AI

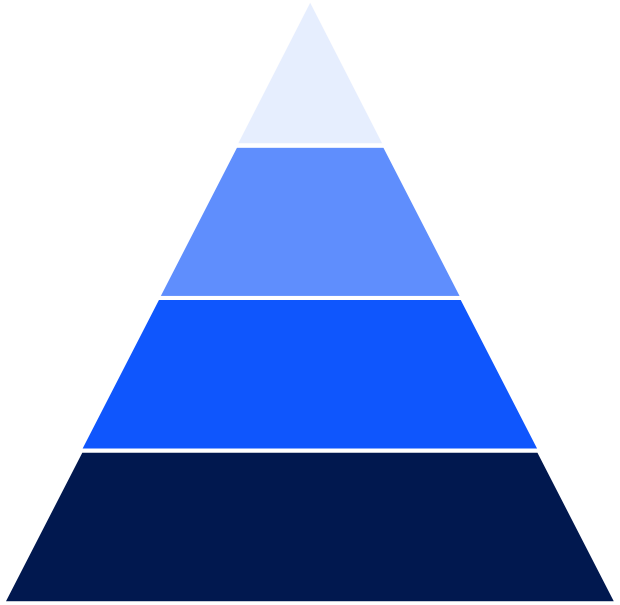


Level 3: Super AI	Surpasses human intelligence
Level 2: General AI	Mimics human intelligence
Level 1: Limited-memory narrow AI	“Machine learning” today
Level 0: Reactive narrow AI	Signature-based decisions

CYCON

~~Only level 0 and level 1 exist today~~

Levels 0 – 2 exist today



Level 3: Super AI	Surpasses human intelligence
Level 2: General AI	Mimics human intelligence
Level 1: Limited-memory narrow AI	“Machine learning” today
Level 0: Reactive narrow AI	Signature-based decisions

CYCON

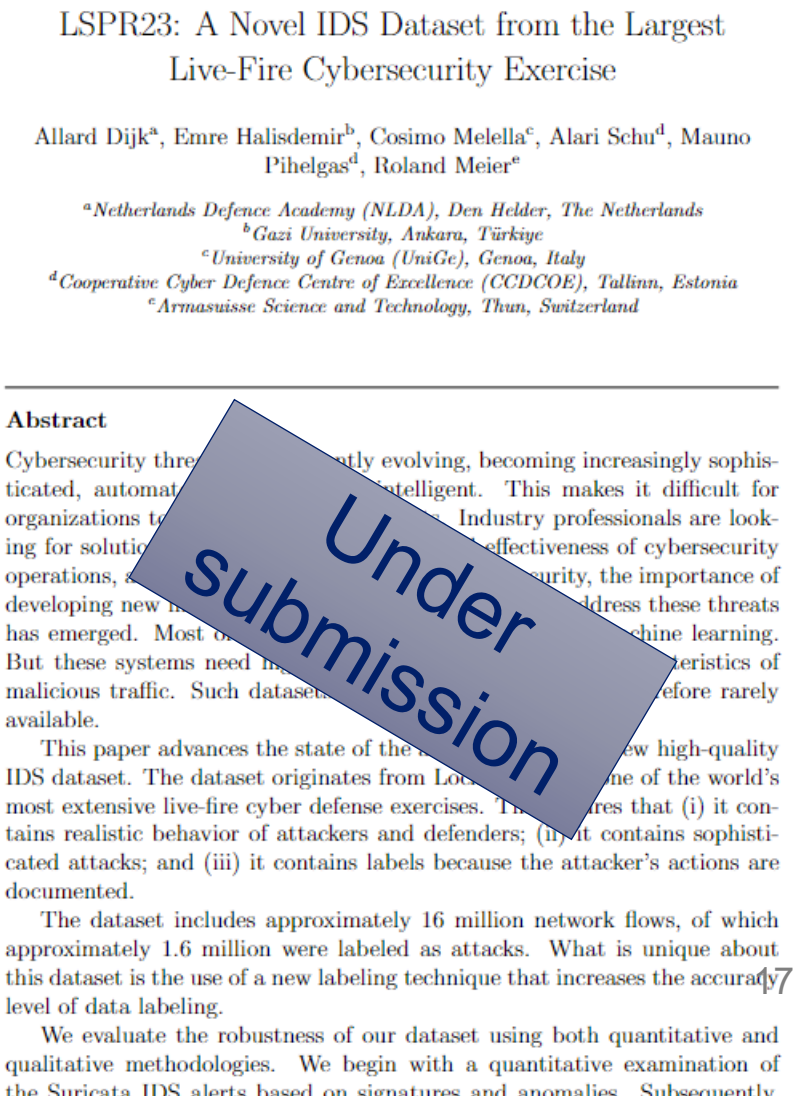
Five tasks for AI

Identification / classification	What is it?
Categorisation	What belongs together?
Assessment	What is important?
Recommendation	What should be done?
Prediction	What will happen?

CYCON

Locked Shields 2023 and 2024: Data collection during the partners run

- We participated as a blue team during the partners run
- Blue team was passive
- Goal: Collect data for future developments
- Result: Paper with public dataset



LSPR23: A Novel IDS Dataset from the Largest Live-Fire Cybersecurity Exercise

Allard Dijk[a], Emre Halisdemir[b], Cosimo Melella[c], Alari Schu[d], Mauno Pihelgas[d], Roland Meier[e]

[a]Netherlands Defence Academy (NLDA), Den Helder, The Netherlands
[b]Gazi University, Ankara, Türkiye
[c]University of Genoa (UniGe), Genoa, Italy
[d]Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia
[e]Armasuisse Science and Technology, Thun, Switzerland

Abstract

Cybersecurity thre…tly evolving, becoming increasingly sophisticated, automat…telligent. This makes it difficult for organizations t… Industry professionals are looking for solutio… effectiveness of cybersecurity operations, …urity, the importance of developing new …ddress these threats has emerged. Most o…chine learning. But these systems need h…teristics of malicious traffic. Such dataset…efore rarely available.

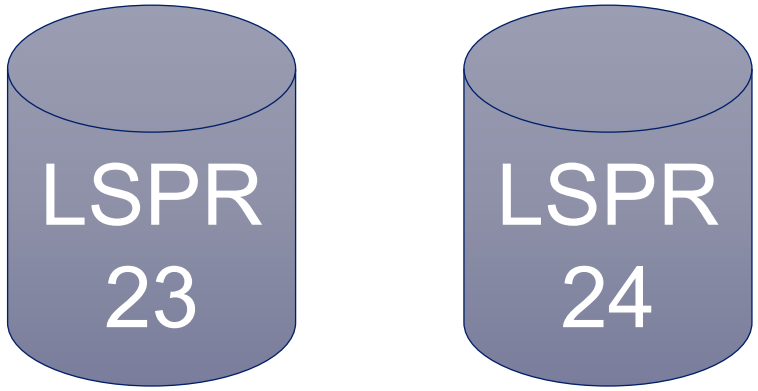
This paper advances the state of the …ew high-quality IDS dataset. The dataset originates from Loc…ne of the world's most extensive live-fire cyber defense exercises. Th…res that (i) it contains realistic behavior of attackers and defenders; (ii) it contains sophisticated attacks; and (iii) it contains labels because the attacker's actions are documented.

The dataset includes approximately 16 million network flows, of which approximately 1.6 million were labeled as attacks. What is unique about this dataset is the use of a new labeling technique that increases the accuracy level of data labeling.

We evaluate the robustness of our dataset using both quantitative and qualitative methodologies. We begin with a quantitative examination of

Under submission

And after the Locked Shields 2024?



- Automated detection and response to some types of attacks (Cobalt Strike)
- Evaluation in a simulated environment during the next 12 months
- Evaluation in LS 2025 with other Blue Teams

CYCON

Towards a fully automated Blue Team at Locked Shields

Thanks for your attention!

Dr. Roland Meier

armasuisse

roland.meier@ar.admin.ch

CYCON