CYLCOMED

AI BEHAVIOURAL ANALYSIS TOOL

Esteban Armas (EVIDEN)

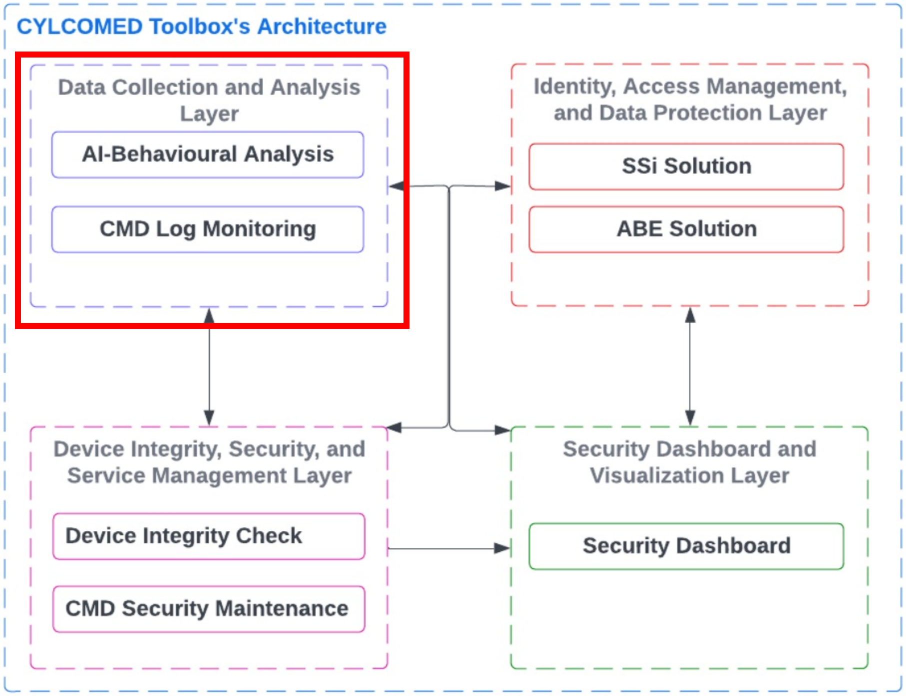
January 2025

TASK AND OBJECTIVES

Task T5.1 - AI-based CMD Behavioural Analysis & Log Monitoring

- AI-Behavioural Analysis tool: make use of unsupervised ML technologies for modelling the normal behaviour of CMDs on the network. Once modelled, the network activity is compared with the normal modelled behaviour for detecting potential attacks or malfunctioning of CMDs.

Architecture of the CYLCOMED toolbox


CYLCOMED Toolbox's Architecture
Data Collection and Analysis Layer
AI-Behavioural Analysis
CMD Log Monitoring
Identity, Access Management, and Data Protection Layer
SSi Solution
ABE Solution
Device Integrity, Security, and Service Management Layer
Device Integrity Check
CMD Security Maintenance
Security Dashboard and Visualization Layer
Security Dashboard

Part of Data Collection and Analysis Layer

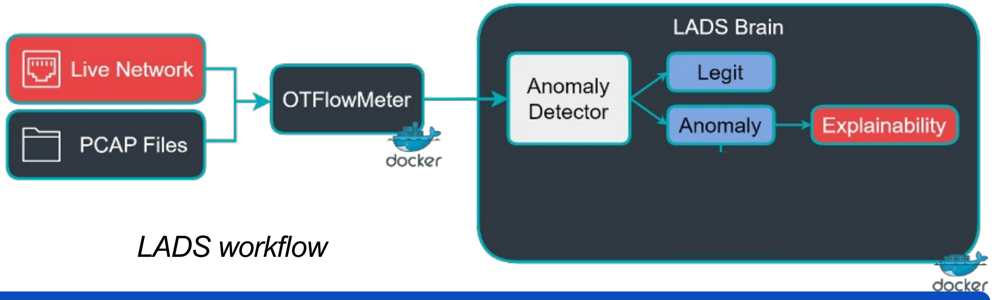
Focus on gathering, monitoring, and analysing data from various sources within the CYLCOMED ecosystem to identify potential cybersecurity threats or anomalies.

AI-BEHAVIOURAL ANALYSIS TOOL

Functionalities of Live Anomaly Detection System (LADS)

- LADS is a soft, real-time anomaly-based network intrusion detection system.
- Based on a deep learning algorithm that models patterns of benign traffic and identifies anomalous behaviour based on deviations from normal behaviour.
- LADS identifies deviations across usage of protocols and services in terms of number of packets, frequency of packets, size of packets, bytes/s, network session duration, unusual communications with internal or external hosts (IP addresses), etc.
- LADS provides anomaly *explainability* based on what features of network traffic are root cause (critical) of anomaly.
- It offers zero-touch configuration so that during a training process LADS auto-configures with the relevant assets, protocols, services, communication topology, etc.
- LADS can detect cyber-attacks:

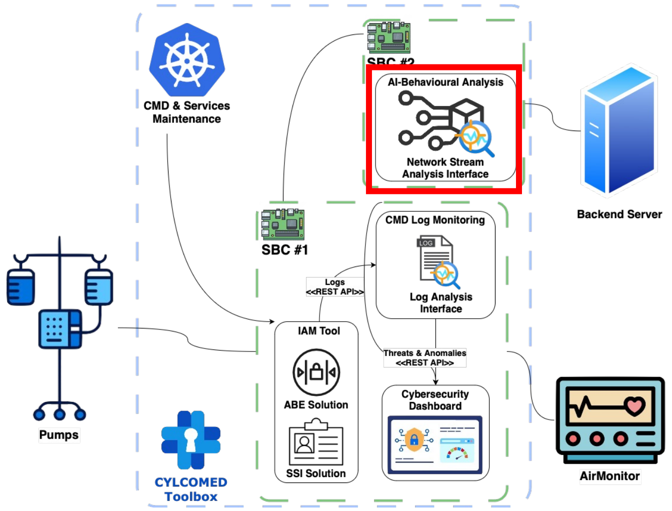
Man in the Middle (MitM)	
Packet Injection (forging/spoofing)	
Unauthorised Host Access	
Reconnaissance	Network Scanning, Port Scanning
Denial of Service (DoS/DDoS)	TCP SYN Flood, ICMP Ping Flood, Blackholing



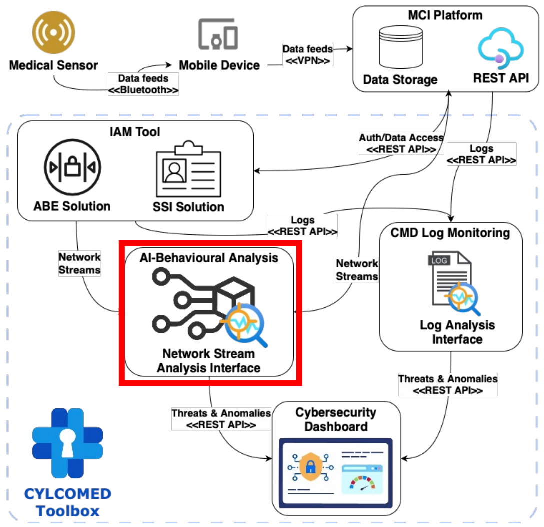
LADS workflow

CONTRIBUTION TO TOOLBOX AND PILOTS

- In both pilots, LADS continuously monitors and analyzes internal network traffic as well as incoming connections.
- LADS provides a comprehensive security status, detecting potential attacks and emerging threats.



Pilot 1 architecture overview



Pilot 2 architecture overview

PROJECT CONSORTIUM

CYLCOMED

CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

EVIDEN
an atos business

MEDIACLINICS
Wearable Health Applications

MARTEL
innovate

XLAB

Fundación para la Investigación Biomédica
Hospital Infantil Universitario
Niño Jesús

OSPEDALE PEDIATRICO
Bambino Gesù

RGB
medical devices

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

INOV inesc

CYLCOMED

THANK YOU FOR YOUR ATTENTION

cylcomed.eu

Co-funded by
the European Union

CYLCOMED project has received funding from the Horizon Europe research and innovation programme under grant agreement N° 101095542