CYLCOMED

CMD LOG MONITORING TOOL

Hrvoje Ratkajec (XLAB)

January 2025

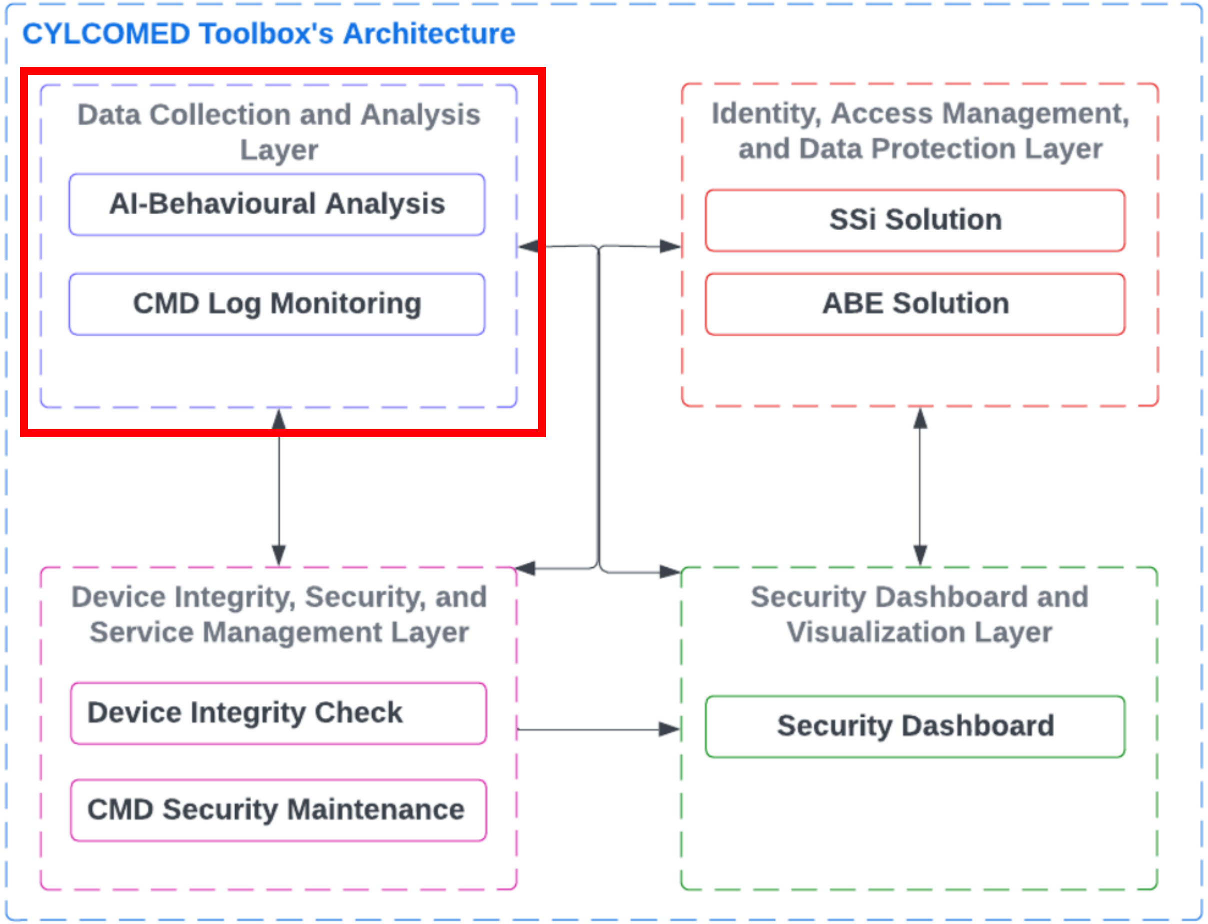
TASK AND OBJECTIVES

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

- CMD Log monitoring tool: develop novel, robust, state-of-the-art AI-based log monitoring methods and implement an AI-based log monitoring tool for the detection of different anomalies in logs generated (due to attacks or failures) by CMDs or by the platform that manages CMDs.

ARCHITECTURE

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.

Tool LOMOS - Log Monitoring System

- Monitoring system capable of detecting security-related events and incidents in the deployed application's environment
- Automatically detect deviations that would represent any kind of abnormal situations, including potential security threats

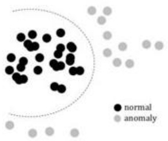
Uses state-of-the-art Natural Language Processing architectures to model log streams and understand their normal operating conditions

- Use of Masked Language Modeling (MLM)
  - Common in self-supervised NLP

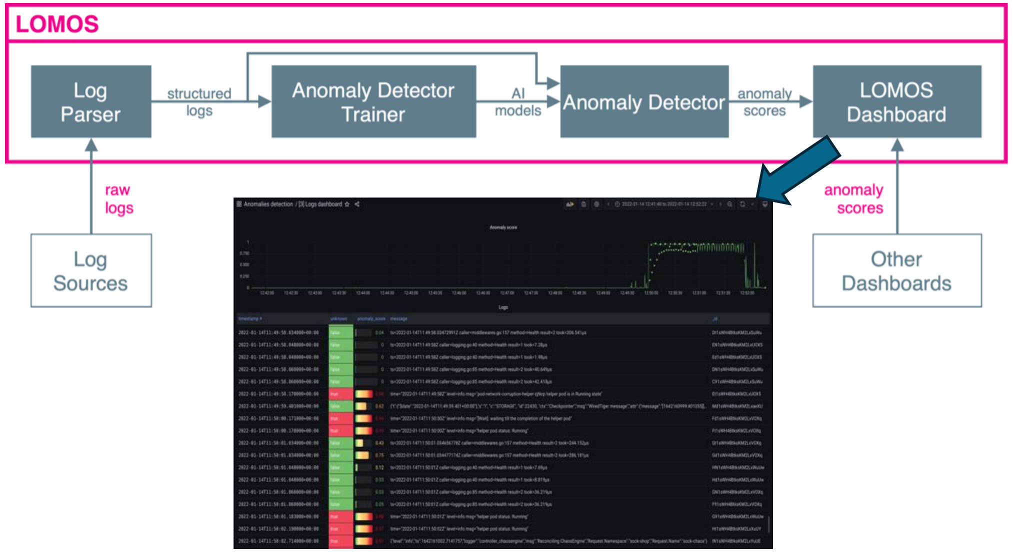
Randomly masked A quick [MASK] fox jumps over the [MASK] dog

Predict A quick brown fox jumps over the lazy dog

- Hypersphere Volume Minimization (HVM)
  - Hypothesis that 'normal' samples can be mapped to close representations.

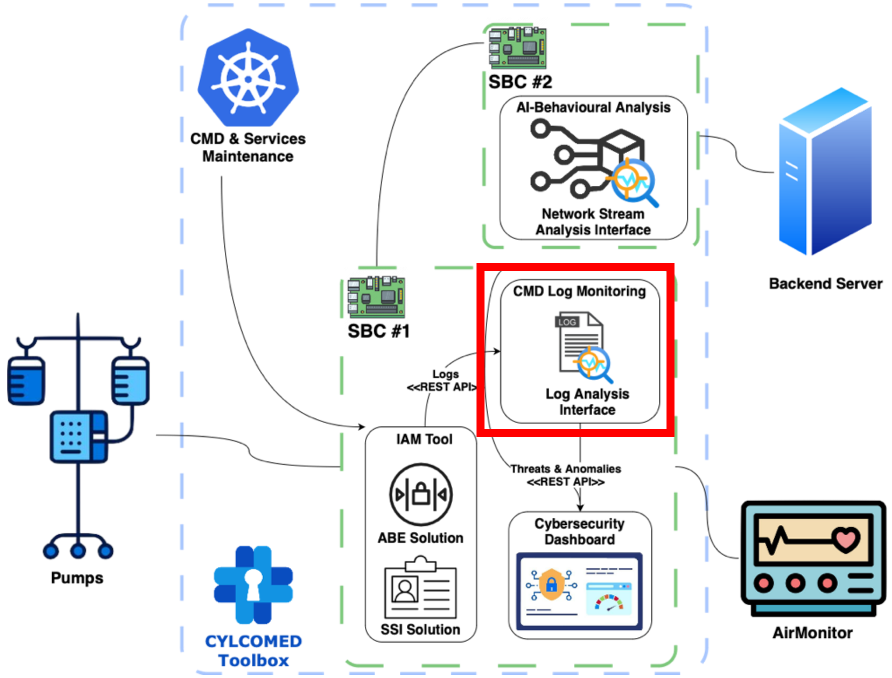


LOMOS workflow and anomaly score visualisation

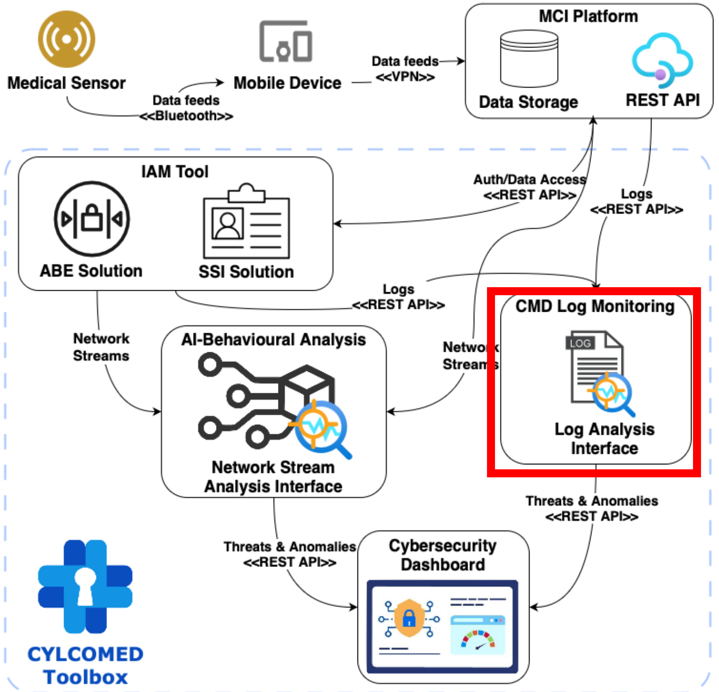


CONTRIBUTION TO TOOLBOX AND PILOTS

- Consums logs from other toolbox components (e.g. FE4MED and LuS4MED) and pilot applications
- Provides status about the security threats and anomalies



Pilot 1 architecture overview



Pilot 2 architecture overview

PROJECT CONSORTIUM

CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

EVIDEN
an atos business

MC MEDIACLINICS
Wearable Health Applications

MARTEL
innovate

XLAB

fib
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