Predictive Analytics-based Strategies for Cyber-Security Provisioning in complex ICT systems

Author: Ayaz Hussain

Advisor: Dr Xavier Masip-Bruin

Dr. Eva Marín-Tordera

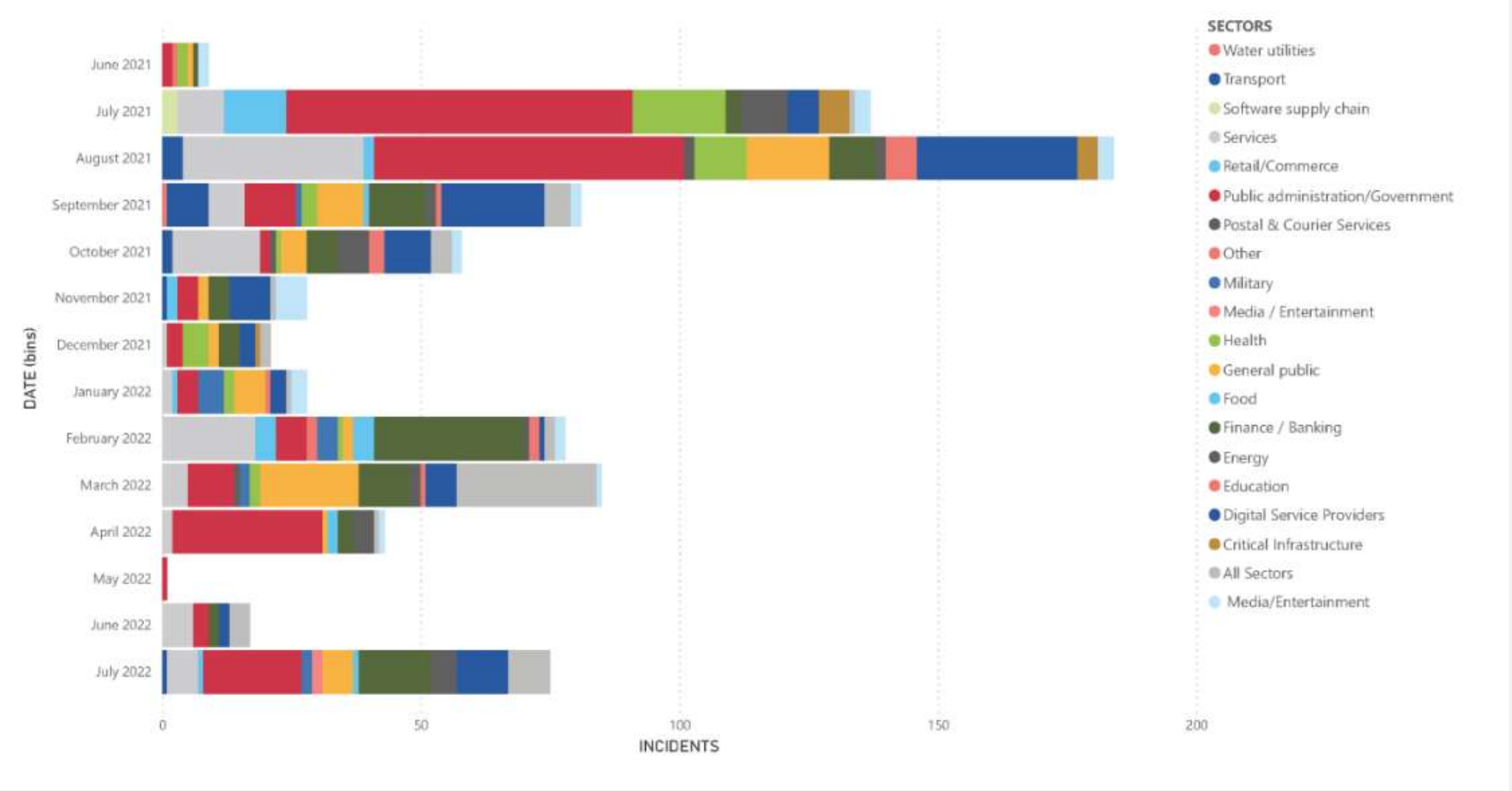
Agenda

- Introduction
- Motivation
- Problem to solve
- Thesis Objective
- Fishy Architecture
- Publications

Introduction

- Industry 4.0 revolution automates the industrial infrastructure where different sectors are connected. It results in increasing the complexity of the of the overall infrastructure.
- The complex infrastructure of ICT systems makes them difficult to detect to prevent them from cyber attacks.
- The use of cyber security standards and classical protection strategies are inadequate to handle the diverse nature of the attacks.
- Predictive analytics involves data mining, and statistical algorithms such as Machine Learning (ML) approaches to make predictions and identify the pattern of future outcomes.
- In cybersecurity, predictive analytics can be applied to a wide range of data, including network logs, security events, user behavior, and external threat intelligence.

Motivation



Observed incidents based on OSINT (Open Source Intelligence) to prime ENISA THREAT LANDSCAPE(ETL) 2022 threats in terms of the affected sector

Motivation

- Rapid development in the network infrastructure has resulted in sophisticated attacks that are hard to detect.
- Detection and prediction of attacks using a single data source and classical approaches are problematic.
- To maintain confidentiality and integrity, organizations must detect and respond the cyber threats proactively without compromising their privacy.
- There is a strong need for efficient predictive analytics-based approaches that utilize AI strategies to detect and predict known attacks along with ever-emerging exploits which can happen in the ICT scenarios.

Problem to solve

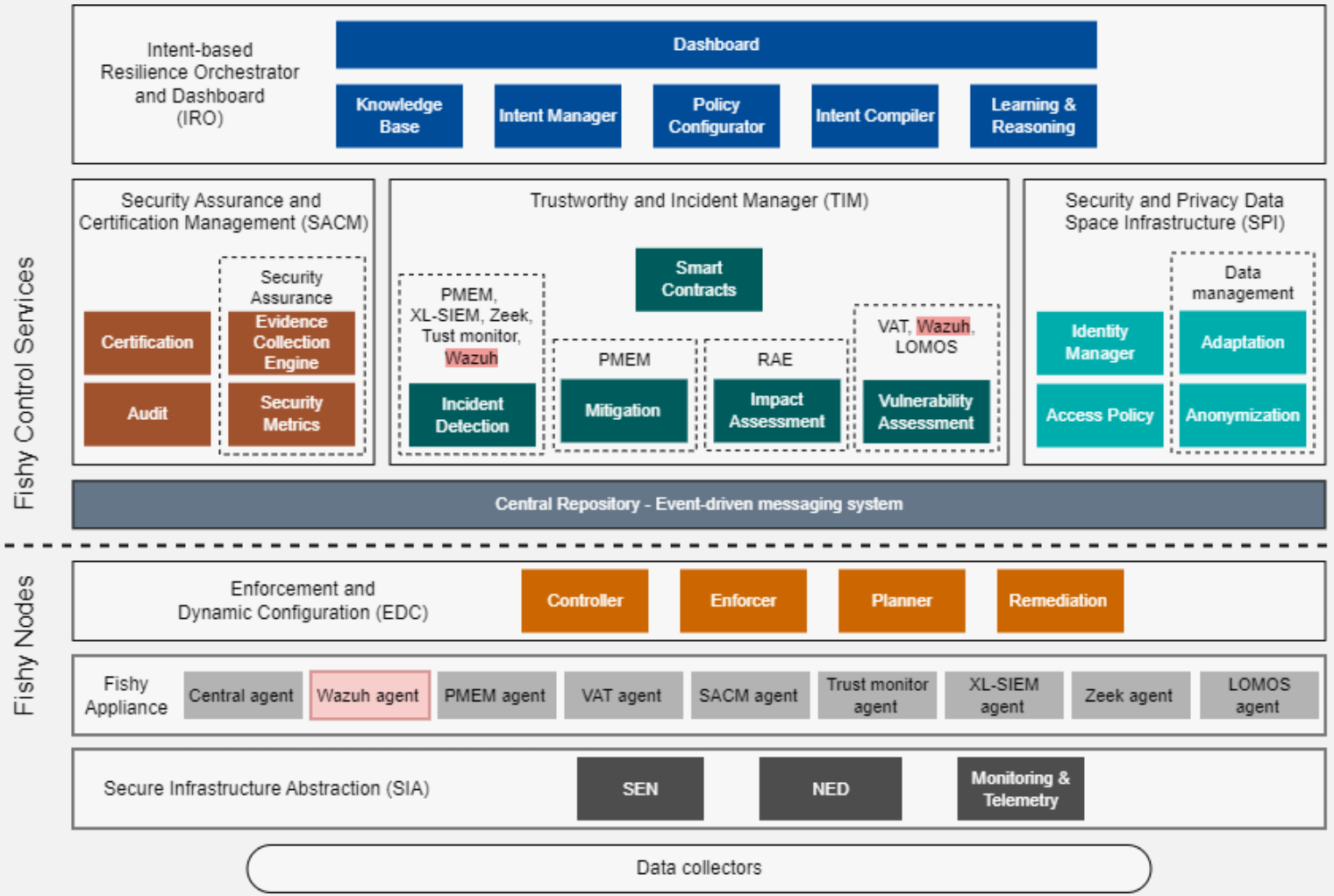
- Issue associated with the classical protection strategies e.g Rule based detection(Snort, Suricata), not able to handle the new attacks patterns.
- Protection strategies based on single input format. e.g network packet based anomalies detection. Single input format is not sufficient in ICT systems.
- Existing approaches have been more biased toward the detection and predictions using supervised Machine Learning(ML) approaches.
- Validations of the strategies with real-time scenarios.
- Actions to be taken after the detection of attack.

Thesis Objective

The thesis aims to design, develop and validate AI-based predictive analytics strategies to achieve the Cyber-Security Provisioning in ICT system. The proposed system will include a well-defined set of sub-objectives as discussed below:

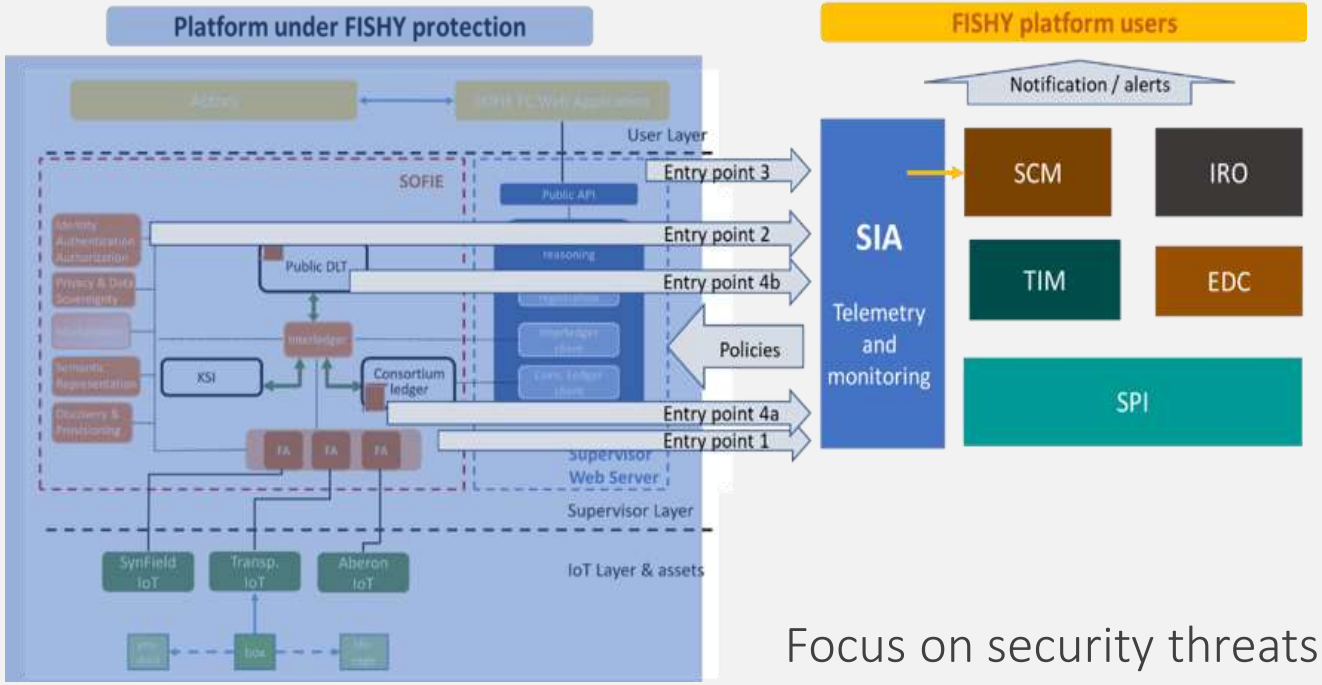
- To design and develop data collectors for data acquisitions.
- Leveraging a detailed literature review to build a taxonomy of attacks and correlated features.
- To design and develop predictive analytics strategies to handle multiple inputs for data modelling.
- To design and execute predictive analytic models for detecting and predicting known and zero-day attacks.
- To deploy and test the proposed strategies in both domain-specific and generic environments.
- To validate the proposed strategy with real-time data and public datasets

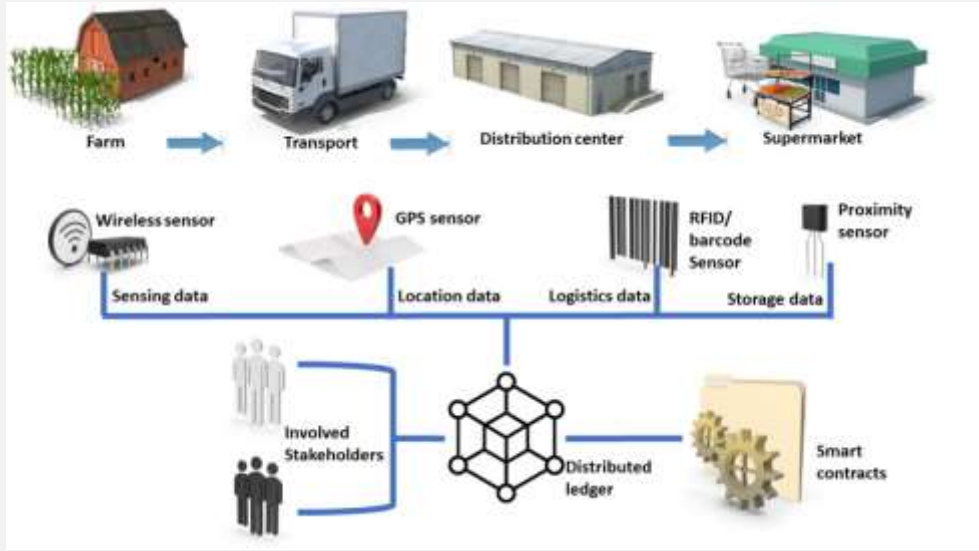
FISHY ARCHITECTURE



Source: [FISHY] - D2.4 Final Architectural design and technology radar, Admela Jukan, Jasenka Dizdarević, Francisco Carpio. 2023

FOOD SECTOR SCENARIO(FARM TO FORK)

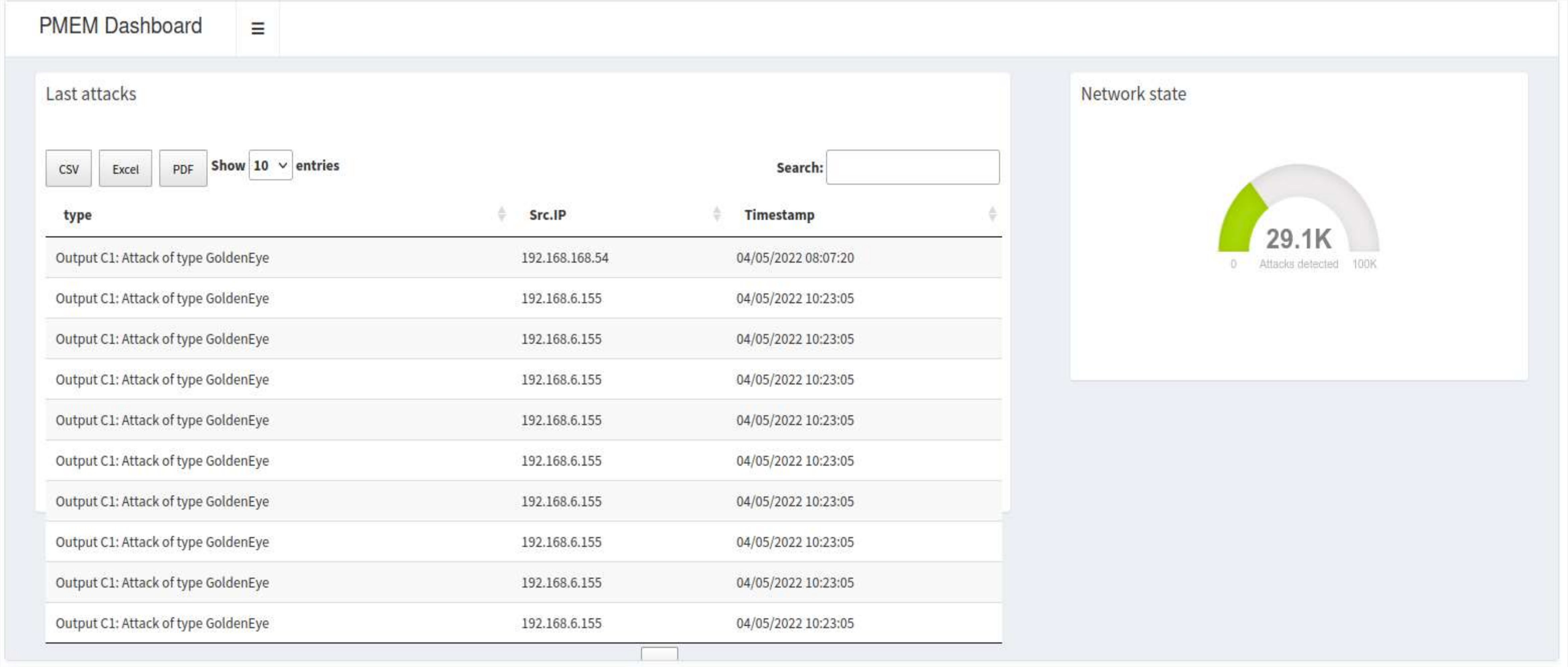




Focus on security threats and attacks for the supply chain:

- Identification of the Malicious and Normal Logs
- Specifically protection against Mirai DDOS attack

First Draft:



PMEM Dashboard

Last attacks

CSV Excel PDF Show 10 entries

Search:

type	Src.IP	Timestamp
Output C1: Attack of type GoldenEye	192.168.168.54	04/05/2022 08:07:20
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05
Output C1: Attack of type GoldenEye	192.168.6.155	04/05/2022 10:23:05

Network state

29.1K

0 Attacks detected 100K

THANK YOU
Any Query?

Ayaz Hussain

Ayaz.hussain@upc.edu