

# CyberSuite | HACKATHON26

**Edgardo Montes de Oca**  
Montimage



**ACAS: Advanced Cybersecurity Analytics Service**

2nd CyberSuite hackathon  
October 2026 | Paris, France



Co-funded by  
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.



01

Context & Motivation

02

ACAS Solution & Architecture

03

Tool Overview

04

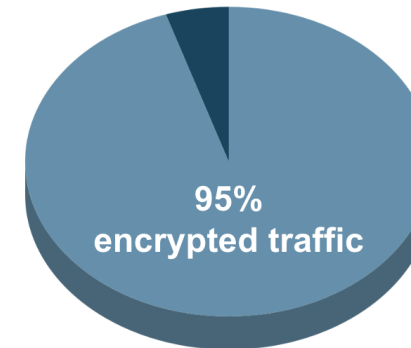
What Can You Explore?



montimage

- Encryption is rapidly becoming the norm
- Challenge for traditional security tools
  - Signature-based and rule-driven systems **struggle to inspect encrypted payloads**
  - **Decryption for inspection is resource-intensive**, often impractical, and can raise **privacy concerns**
- Need for **AI-driven solutions**:
  - Analyze metadata, traffic patterns, and behavioral signals without decrypting the content
  - Enable real-time, scalable, and privacy-preserving detection of threats

**As of 2022**

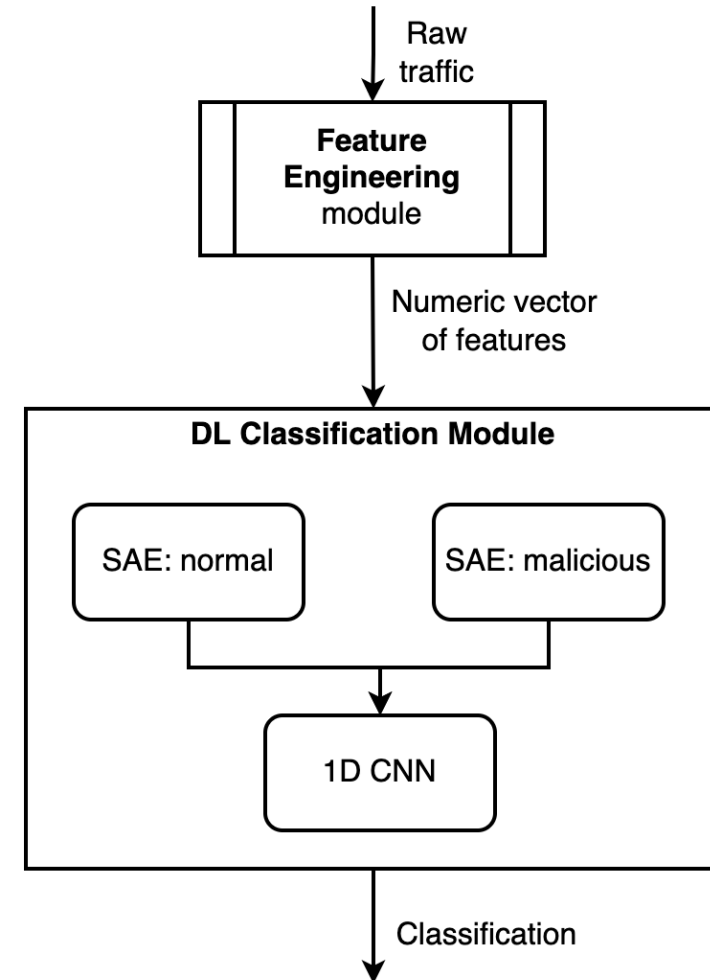


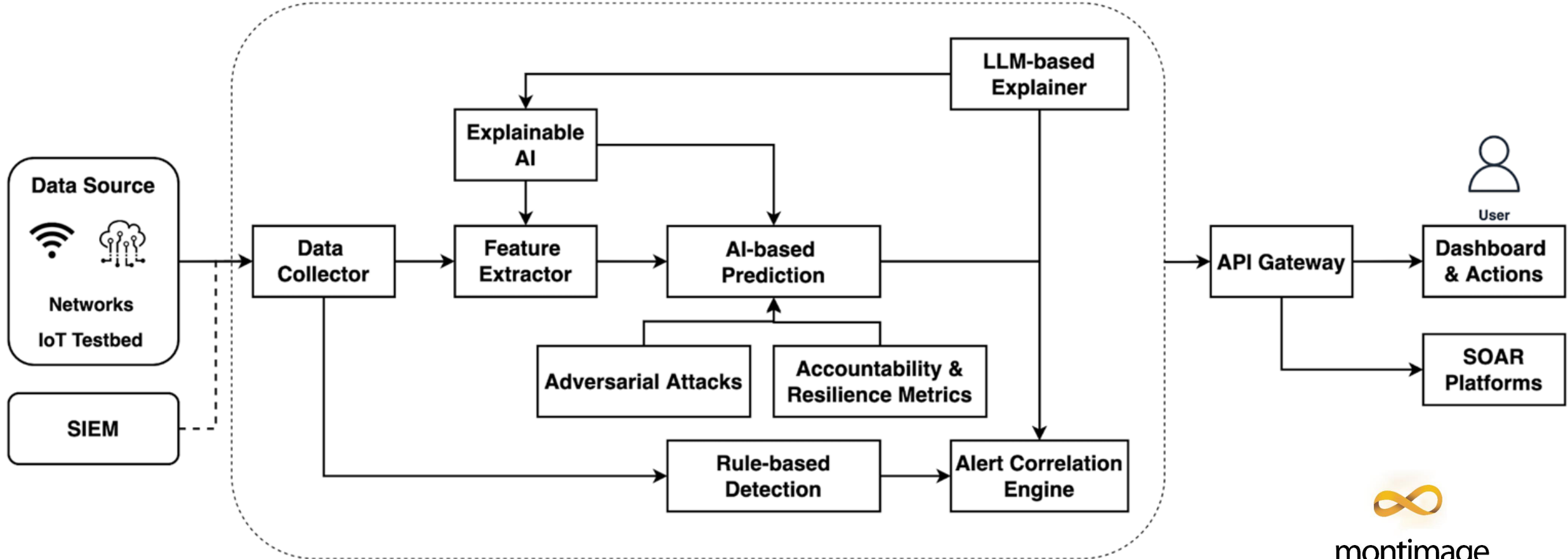
*Source: State of Encrypted Attacks 2022 by Zscaler*



montimage

- Monitor and detect anomalies (e.g., botnet, DDOS, ransomware) in encrypted network traffic
- Useful for network administrators, security analysts, AI developers and testers.
- Main functions:
  - **Traffic Feature Extraction**: 60+ flow-based features (protocol field values & statistical metrics) using MMT
  - **Deep Learning-Based Anomaly Detection**: combining Convolutional Neural Networks (CNN) and Stacked Auto-Encoders (SAE)
  - **Flexible Architecture**
- Datasets: public (CSE-CIC-IDS2018: 99% in botnet detection) and private (normal user activity & honeypot data)





montimage

## 70+ Swagger-based APIs

|         |                                                                                |                                                  |   |
|---------|--------------------------------------------------------------------------------|--------------------------------------------------|---|
| mmt     | Everything relates to manipulating the MMT Tool                                | <a href="#">Find out more</a>                    | ^ |
| GET     | /mmt/ Get the status of MMT Tool                                               |                                                  |   |
| GET     | /mmt/stop Stop analyzing                                                       |                                                  |   |
| POST    | /mmt/offline Start analysing a pcap file                                       |                                                  |   |
| POST    | /mmt/dataset Analyzing a dataset                                               |                                                  |   |
| POST    | /mmt/online Start monitor a network interface in real-time                     |                                                  |   |
| reports | Access to reports which are the output of analysing a pcap file                | <a href="#">More detail on the report format</a> | ^ |
| GET     | /reports/ Get reports list                                                     |                                                  |   |
| DELETE  | /reports/ Delete all reports                                                   |                                                  |   |
| GET     | /reports/{reportId} Get list csv of a report                                   |                                                  |   |
| GET     | /reports/{reportId}/{fileName}/download Download a raw report file             |                                                  |   |
| GET     | /reports/{reportId}/{fileName} Get detail of a csv file of a report            |                                                  |   |
| pcaps   | List/upload trace file for analysing                                           |                                                  | ^ |
| GET     | /pcaps/ Get the list of all pcap files                                         |                                                  |   |
| POST    | /pcaps/ Upload a pcap file                                                     |                                                  |   |
| DELETE  | /pcaps/ Delete all pcaps                                                       |                                                  |   |
| GET     | /pcaps/datasets Get all datasets containing pcap files                         |                                                  |   |
| GET     | /pcaps/dataset/{datasetName} Get the list of all pcap files of a given dataset |                                                  |   |
| POST    | /pcaps/dataset/{datasetName} Upload a list of pcap files to a dataset          |                                                  |   |
| DELETE  | /pcaps/dataset/{datasetName} Delete the dataset and its pcap files             |                                                  |   |
| logs    | Access to the log of MMT Tools                                                 |                                                  | ^ |

- Manipulate the MMT tool
- Access reports and logs
- Upload trace file for analysis
- Manipulate models and the building model process
- Get the stats of the building model process
- Manipulate the prediction process and obtain results
- ...



## 70+ Swagger-based APIs

|         |                                                                                |
|---------|--------------------------------------------------------------------------------|
| mmt     | Everything relates to manipulating the MMT Tool                                |
| GET     | /mmt/ Get the status of MMT Tool                                               |
| GET     | /mmt/stop Stop analyzing                                                       |
| POST    | /mmt/offline Start analysing a pcap file                                       |
| POST    | /mmt/dataset Analyzing a dataset                                               |
| POST    | /mmt/online Start monitor a network interface in real-time                     |
| reports | Access to reports which are the output of analysing a pcap file                |
| GET     | /reports/ Get reports list                                                     |
| DELETE  | /reports/ Delete all reports                                                   |
| GET     | /reports/{reportId} Get list csv of a report                                   |
| GET     | /reports/{reportId}/{fileName}/download Download a raw report file             |
| GET     | /reports/{reportId}/{fileName} Get detail of a csv file of a report            |
| pcaps   | List/upload trace file for analysing                                           |
| GET     | /pcaps/ Get the list of all pcap files                                         |
| POST    | /pcaps/ Upload a pcap file                                                     |
| DELETE  | /pcaps/ Delete all pcaps                                                       |
| GET     | /pcaps/datasets Get all datasets containing pcap files                         |
| GET     | /pcaps/dataset/{datasetName} Get the list of all pcap files of a given dataset |
| POST    | /pcaps/dataset/{datasetName} Upload a list of pcap files to a dataset          |
| DELETE  | /pcaps/dataset/{datasetName} Delete the dataset and its pcap files             |
| logs    | Access to the log of MMT Tools                                                 |

Network Detection and Response

Traffic Analysis

- Deep Packet Inspection
- Network Analysis
- Feature Extraction

Build

- Models

All Models

Models Comparison

Models Retraining

Detect

- Rule-based Detection
- Anomaly Prediction
- Early Prediction

Attacks

- XAI

SHAP

LIME

Metrics

- Accountability Metrics
- Resilience Metrics

About

Welcome, Manh-Dung

# Network Detection & Response

AI-Powered Network Anomaly Detection with Explainable Intelligence

Advanced Cybersecurity Analytics Service (ACAS) for AI-based analysis of network events captured by the Montimage Monitoring Tools (MMT). Protect your network infrastructure with advanced machine learning models that detect and respond to network threats and anomalies in real-time. Get early warnings, understand root causes, and automate responses.

Try Traffic Analysis

Explore Models

Try Prediction

Login

Documentation

Video Demo

Key Features

Comprehensive network security powered by cutting-edge AI technology



### Deep Packet Inspection (DPI)

Analyze encrypted network traffic without decryption using advanced DPI techniques and protocol analysis.



### Real-Time Detection

Advanced ML models detect network anomalies and security threats in real-time with high accuracy and minimal false positives.



### Rule-Based Detection

Flexible rule engine for custom detection logic, threshold-based alerts, and compliance monitoring.

NDR©2025 developed by Montimage. Version 1.0

Projects: <https://ndr.montimage.eu/>  
<https://ndr.montimage.eu/docs/>

CyberSuite | 2nd CyberSuite hackathon | October 2026 | Paris, France – Page 7

- Analyze normal and malicious network traffic using Deep Packet Inspection
- Explore extracted flow-based features
- Test both rule-based and AI-based detection of network attacks
- Explore different AI model metrics, like accuracy, explainability and robustness
- **Tutorial:** <https://strongcourage.notion.site/Hands-On-ACAS-Tool-Testing-2991f0954df88047a537e2a585e857f8>



**Thank you for your attention!**



Montimage



Edgardo Montes de Oca



edgardo.montesdeoca@montimage.eu



<https://montimage.eu/>



Co-funded by  
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.