

Challenge Title: Advanced Cybersecurity Analytics Service for Network Threat Detection and Response

Challenge Context and Purpose: This challenge evaluates the Advanced Cybersecurity Analytics Service (ACAS) within the Network Detection and Response (NDR) platform, an AI-driven cybersecurity system designed for near real-time anomaly detection, anomaly prediction, and explainable analysis of encrypted network traffic. The platform combines traditional rule-based detection with advanced deep learning models (such as CNNs and Autoencoders) to identify malicious activities. Additionally, its Explainable AI (XAI) module leverages methods like SHAP and LIME, along with Large Language Models (LLMs), to provide root-cause insights that help security analysts understand why specific traffic is flagged as suspicious and to recommend appropriate mitigation actions.

Participants will test key features including deep packet inspection, feature extraction, model evaluation, rule-based detection, threat prediction, and XAI-driven incident analysis. The goal is to assess detection accuracy, usability, and performance under realistic network scenarios, gather participant feedback, and identify areas for improvement. The results will determine the platform's readiness for Security Operations Center (SOC) deployment and its potential to enhance analysts' threat detection and response workflows in SMEs.

Goals of the Challenge: *What do you aim to achieve by including this challenge?*

- Gather user feedback on the tested key features.
- Assess the platform's usability, effectiveness, scalability, and mitigation recommendations.
- Identify potential areas for improvement to enhance readiness and adoption in SMEs.

Key Tasks for Participants: *List the main tasks participants will perform to test and evaluate the solution.*

Phase 1: Registration and Setup (2 minutes)

- Register a new user account on the platform. *(It is recommended to log in to access all available features)*
- Review the user guide and documentation to become familiar with the platform.

Phase 2: Task Perform (10 minutes)

For each task, logged-in users are encouraged to experiment with the provided sample PCAP files or upload their own (maximum size: 10 MB).

- **Deep Packet Inspection:** Explore traffic statistics, protocol hierarchies, and bidirectional flow visualizations.

CyberSuite Hackathon Challenges Template

- **Feature Extraction:** Examine over 80 flow-based features extracted from PCAP files for model training and testing.
- **Anomaly Detection:** Compare detection results from both rule-based and deep learning-based approaches.
- **Adversarial Attacks:** Execute three data poisoning attacks against the models and analyze their impact metrics.
- **Explainable AI (XAI):** Apply LIME and SHAP methods to interpret model predictions and identify key influencing features.

Phase 3: Feedback Collection (3 minutes)

- Complete a structured feedback form assessing usability, engagement, and feature effectiveness.
- Provide immediate suggestions and recommendations for improving the platform.

Feedback and Evaluation Requirements: *Describe the feedback participants are expected to provide.*

- A detailed evaluation form or report outlining strengths, weaknesses, and suggestions for improvement.
- Document any issues encountered during the challenge.

Deliverables: *Clearly state what participants are expected to submit.*

- Completed the challenges.
- A completed evaluation form with specific recommendations for refining the solution.

Resources and Tools Provided: *List any tools, documentation, datasets, or other resources participants will need to effectively test and evaluate the solution.*

- Access to the platform via URL
- Documentation about challenges

Estimated Time Requirement: *Provide an estimated amount of time participants will need to complete the challenge (e.g., hours, days).*

15 minutes

Contact Point (Optional): *Provide a point of contact for any questions related to this challenge (name, email, etc.).*

Primary Contact: Manh NGUYEN, manhdung.nguyen@montimage.eu