# Deliverable D6.4
# Demonstration of AI-assisted security monitoring and enforcement

## Document Summary Information

| | | | |
|---|---|---|---|
| **Grant Agreement No** | 871780 | **Acronym** | MonB5G |
| **Full Title** | Distributed Management of Network Slices in beyond 5G | | |
| **Start Date** | 01/11/2019 | **Duration** | 42 months |
| **Project URL** | https://www.monb5g.eu/ | | |
| **Deliverable** | D6.4 – Demonstration of AI-assisted security monitoring and enforcement | | |
| **Work Package** | WP6 | | |
| **Contractual due date** | M42 | **Actual submission date** | 07/06/2023 |
| **Nature** | Report | **Dissemination Level** | Public |
| **Lead Beneficiary** | EUR | | |

***Disclaimer***



***Copyright message***

## TABLE OF CONTENTS

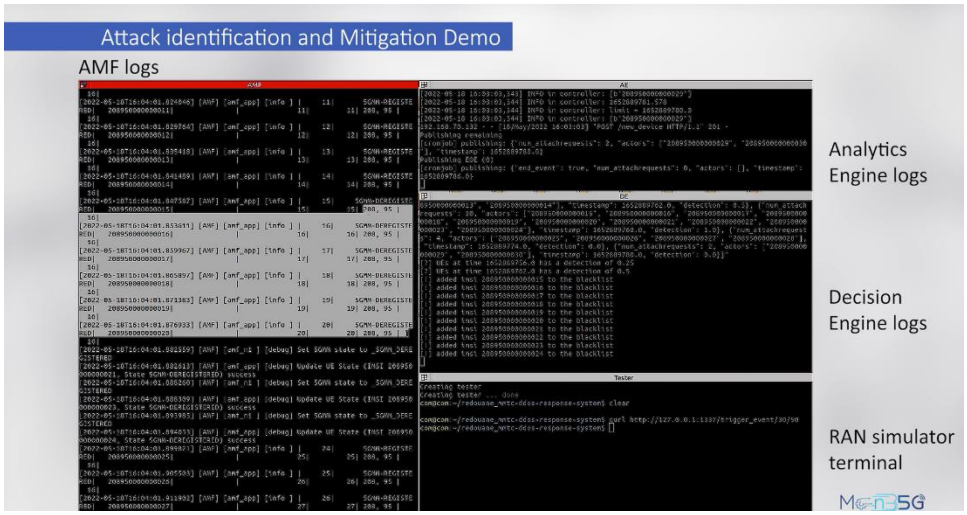
# 1 Video Release and PoC-2 Summary

## 1.1 PoC-2- Scenario 1 and 2

The MonB5G architecture consists of management and orchestration layers, which include the Monitoring System, Analysis Engine, and Decision Engine. The system detects and mitigates attacks within and between network slices. The Monitoring System collects User Equipment attach requests from the 5G Core Network, and the Analytics Engine computes a detection rate using the Gradient Boosting algorithm. The Decision Engine uses the detection rate to blacklist users if it exceeds a defined threshold, effectively mitigating distributed denial of service attacks. The demo showcases the system's ability to detect and blacklist attacking users, with visualizations displaying normal and abnormal traffic.

In the scenario presented, each network slice is managed by a Domain Slice Manager, including a Monitoring System and Analytic Engine. An Inter-Domain Slice Manager handles the management and orchestration of network slices. The system ensures privacy by sharing only model parameters with the central Inter-Domain Slice Manager, which aggregates them to build a global model. To mitigate poisoning attacks in Federated Learning, MonB5G proposes a framework that utilizes deep reinforcement learning and unsupervised machine learning to detect malicious participants. The demo demonstrates the effectiveness of this approach in detecting and mitigating poisoning attacks during the federated learning process.

During Federated Learning rounds, the Monitoring System collects the weights matrix and sends it to the Analytic Engine. Dimensionality reduction is applied to the weights matrix, reducing it to two dimensions. The Analytic Engine clusters the weights matrix using the K-means clustering algorithm, resulting in two lists of trusted and untrusted Federated Learning clients. The training continues with only the trusted clients, improving the accuracy of the global Federated Learning model. MonB5G's detection scheme not only identifies malicious Domain Slice Managers but also enhances the model's accuracy. The proposed zero-touch management enables the system to detect and mitigate attacks without human intervention.



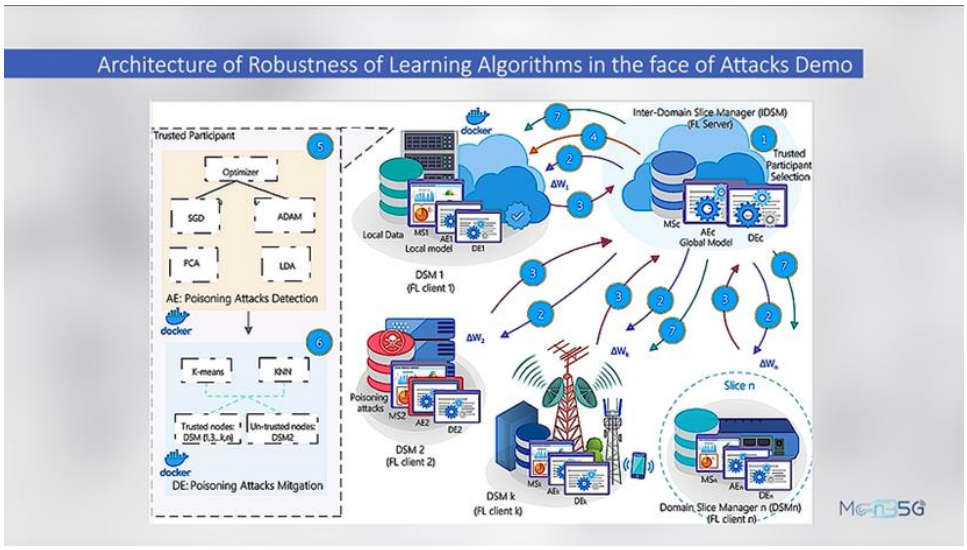



*Figure 1-1: PoC2 Scenario 1&2 Screen shots*

The video can be found on the following link at MonB5G YouTube Channel:

https://www.youtube.com/watch?v=rjG6VXFPsEQ

## 1.2 PoC-2- Scenario 3

The MonB5G system incorporates an autonomous security orchestrator architecture, automating the handling of security incidents for faster and more effective reactions to minimize the impact of security threats. Countermeasures are deployed on-demand through the Cloud Native Function Orchestrator, allowing for reconfiguration and changes in security functions. The demo focuses on responding to the aLTEr attack, a man-in-the-middle attack that manipulates DNS queries to redirect user traffic to malicious servers. Native cloud and virtual network functions are utilized for software components, including devices, the 5G system, security tools, MonB5G components, and malicious servers.

In the demo, UERANSIM simulates the terminal and base station while also simulating the attack by redirecting DNS requests to the malicious server. The 5G core network and the MonB5G Security Orchestrator are deployed on Kubernetes cluster and OpenStack project. Malicious DNS and HTTP servers are set up on virtual machines to process the redirected user requests. The Monitoring System continuously monitors DNS messages on the N6 interface through port mirroring, transforming raw packets into meaningful logs. Machine Learning algorithms are implemented to detect anomalies in DNS traffic, triggering incident events that are processed by the incident response function.

The decision engine of the security orchestrator analyzes the detected threats and instructs the actuator to deploy countermeasures. In this case, the decision engine directs the deployment and configuration of a DNS over TLS server and client to eradicate the attack. Real-time user experience is showcased, starting with the DNS query sent to the malicious server and ending with the successful resolution of the incident. By automating security with AI and utilizing security tools, the time taken to identify and eliminate threats is significantly reduced, while orchestrating security functions strengthens the defense dynamics of the system.

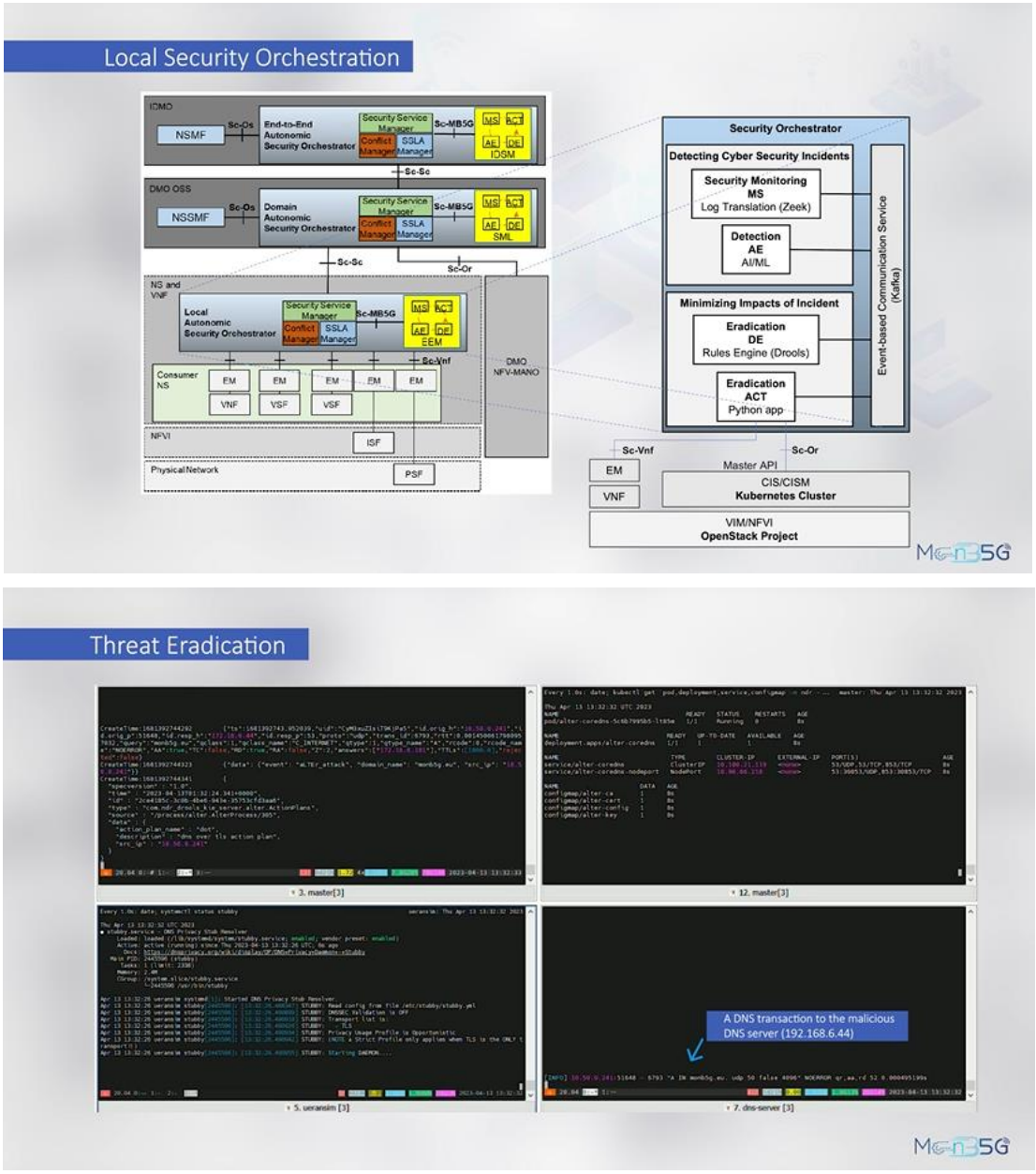



*Figure 1-2: PoC2 Scenario 3 Screen shots*

The video can be found on the following link at MonB5G YouTube Channel:

https://www.youtube.com/watch?v=zvte425HeM4