PoC Report

1. PoC Project Details

1.1. PoC Project

PoC Number:	15
PoC Project Name:	Trustworthy Zero-touch Network and Service Management in 6G Networks with NDT support
PoC Project Host:	Telefónica
Short Description:	This PoC intends to demonstrate the use of Network Digital Twins (NDTs) in a cybersecurity context, as part of a 6G network. This approach includes two different Network Digital Twins as part of a sandbox environment, working together to mitigate cyberattacks. Those NDTs are applied for prediction and prevention, and to analyse the impact of mitigation actions. The combination of both NDTs supports minimally invasive smart automated threat management.
PoC Project Status : *(Ongoing/Completed)*	Completed

1.2. PoC Team Members

#	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	Telefónica	Yes	josemanuel.manjon@telefonica.com diego.r.lopez@telefonica.com antonio.pastorperales@telefonica.com	X	Network Operator	Use case definition and architectural design of PoC. Provider of the IA-NDT
2	CNIT	No	fabrizio.granelli@unitn.it		Research center	Use case definition and architectural design of PoC. Provider of the PP-NDT
3	UPC	No	eva.rodriguez@upc.edu xavier.masip@upc.edu		University	Use case definition and architectural design of PoC.
4	TUBS	No	i.zacarias@tu-braunschweig.de a.jukan@tu-braunschweig.de		University	Use case definition and architectural design of PoC. Provider of the IBI
5	NKUA	No	pgkonis@uoa.gr		University	Use case definition and architectural design of PoC. Provider of the DTE
6	UMU	No	e.garciacaleramolina@um.es anthonyjoel.pogom@um.es skarmeta@um.es		University	Use case definition and architectural design of PoC. Supporting the development of the IA-NDT. Provider of the testbed.

(*) Identify the PoC Point of Contact with an X.
(**) The Role will be network/service provider, supplier, or other (universities, research centers, test labs, Open-Source projects, integrators, etc…).

All the PoC Team members listed above declare that the information in this report is conformant to their activities during the PoC Project.

1.3. PoC Project Scope

1.3.1. PoC Topics

Report the status of all the PoC Topics and Expected Contributions anticipated in the PoC Proposal

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
Topic 3 (Intent-driven Closed-Loop automation)	I Intent-driven operations allow the introduction of self-adapting and self-monitoring capabilities in the operations software stack. This is a key ingredient for the transition from automation into autonomous, zero-touch networks. Closed loops are key enablers for automation that have been successfully used in many industries for long, and more recently for computing and networking applications. Closed-loop automation (CLA) can self-monitor, self-evaluate and self-heal and fulfill all specified requirements. The combination of intent and closed-loop automation prides a powerful tool to capture a consumers needs and provide an intelligent feedback loop.	ZSM-011 ZSM-015 ZSM-016 ZSM-018	Demonstration of IDO-CLA for cybersecurity environments. Application of NDT technologies to enhance automation	December 2025	Completed
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

1.3.2. Other topics in scope

Report the status of all the additional PoC Topics and Contributions anticipated in the PoC Proposal.

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
Topic 2 (Automation in Multi-Stakeholder Ecosystems)	Telecom operators wanting to offer end-to-end services with potential global reach will typically require dynamic and automated interaction with other providers for enabling an open coopetitive service ecosystem	ZSM-011 ZSM-015 ZSM-016 ZSM-018	Analyse the implications of different NDT providers in providing an integrated service	December 2025	Completed
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

1.4. PoC Project Milestones

PoC Milestone	Milestone description	Target Date	Additional Info	Completion Date
P.S	PoC Project Start	April 2025	Proposal Submission	April 2025
P.D1	PoC Demo 1	June 2025	First demonstration of PoC at ZSM #32	September 2025
P.D2	PoC Demo 2	November 2025	Final demonstration of PoC at ZSM #33 and University of Granada	November 2025
P.R	PoC Report	December 2025	Final report with PoC results	December 2025

1.5. Confirmation of PoC Events Occurrences

This PoC was presented at two separate face-to-face ETSI meetings, providing opportunities to demonstrate the framework, discuss its progress, and align with ongoing ETSI activities. Also was presented at Univerisad de Granada, as an example of the current PoC of the ETSI ZSM group. The details of these events are summarized below:

Events Names and Occurrences:

- ETSI ZSM #32: Partial demonstration about the interaction between the Impact Analysis Network Digital Twin and the Intent-Based Interface, showcasing a first approach to the what-if loop for the mitigation of attacks.

- ETSI ZSM #33: Final demonstration of the PoC. It showcases the full workflow and interactions specified in the definition of the PoC.

- ETSI ZSM Event at Universidad de Granada: Overview of the ZSM Proofs of Concept to Universidad de Granada, detailing as an example the PoC #15.

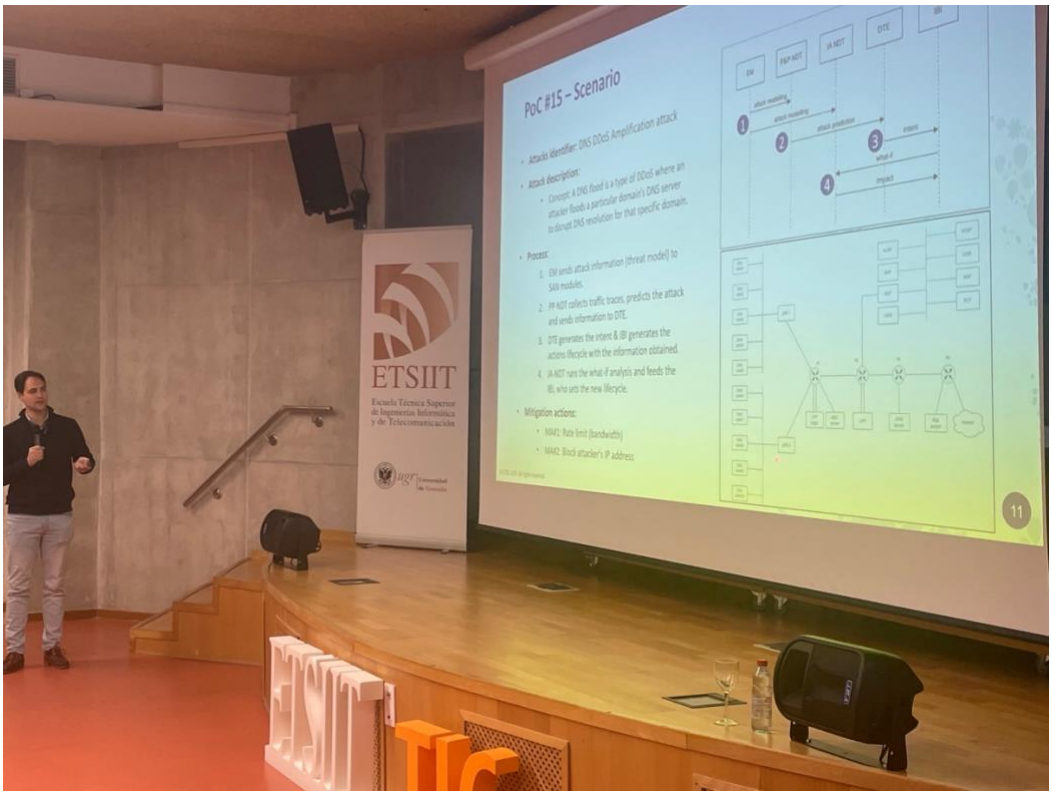

Figure 1. Presentation of the PoC at Universidad de Granada.

2. PoC Technical Details

2.1. PoC Overview

This PoC aims to validate a zero-touch management and orchestration framework for 6G networks that uses two Network Digital Twins (NDT) as a core components to enable secure and reliable decision-making. This PoC focuses on demonstrating "trustworthy" automation in complex multi-domain, multi-technology environments.

The Prediction and Prevention NDT (PP-NDT) focuses on predicting cyberattacks through replication of real network traffic and topology, enabling early detection of anomalies and threats. The Impact Analysis NDT (IA-NDT) emulates "what-if" scenarios, simulating attacks and testing mitigation strategies to assess their effectiveness before deployment in the live network.

Apart from the NDTs, the PoC integrates several components: the Early Modelling (EM) module prepares attack and mitigation models used by the NDTs; a Distributed Trustable AI Engine (DTE) processes attack information and generates mitigation intents; and an Intent-Based Interface (IBI) translates these intents into network policies, validating them iteratively through the IA-NDT to ensure compliance with security goals and QoS requirements. This closed-loop automation ensures mitigation actions are effective and do not disrupt service quality.

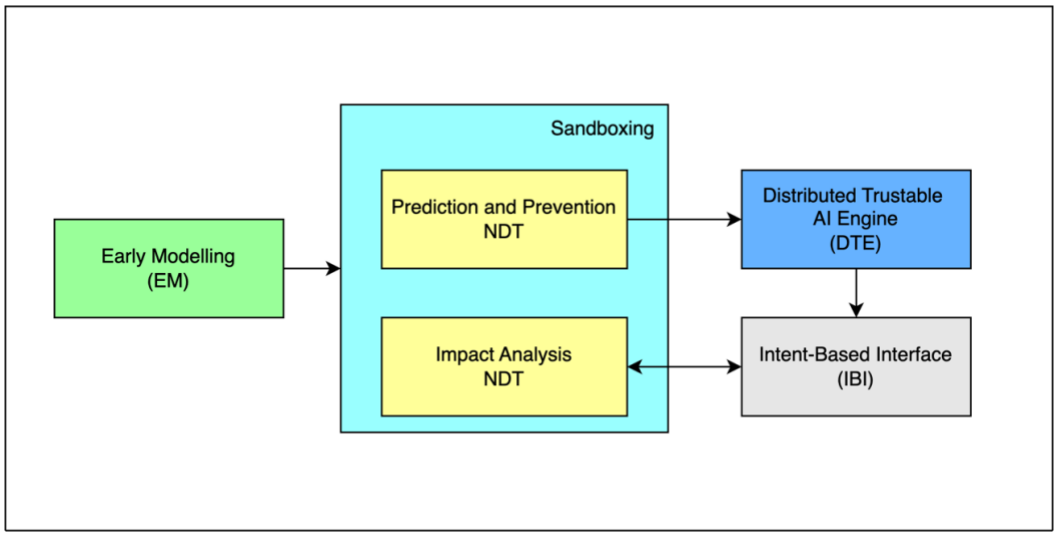

Figure 2. PoC general architecutre

2.2. PoC Infrastructure

All the PoC modules has been developed leveraging the infrastructure from the HORSE project, specifically inside the Universidad de Murcia testbed. Most of them has been deployed using a contenerized format (Docker, Kubernetes), following cloud-native principles to perform agility, speed and resilience.

2.3. PoC Workflow and Story

The PoC general workflow is the one depicted in Figure 3 and each one of the steps is further detailed below.

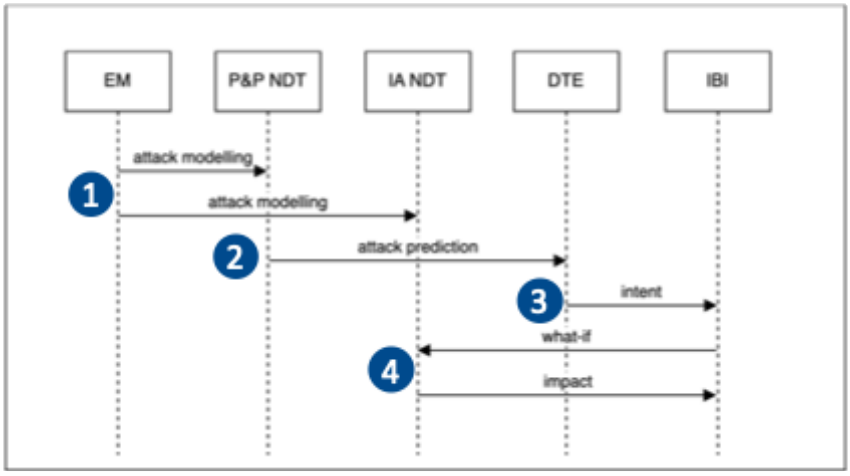

Figure 3. General workflow of the PoC

1. Early Modelling sends the threat model to the Network Digital Twins

As a fisrt step, the Early Modelly is in charge of generating an XML model with the information of the attack considered, in this case, a DNS Amplification attack. When the model is ready, the Early Modelling sends the information to both Network Digital Twins to replicate the information considered.

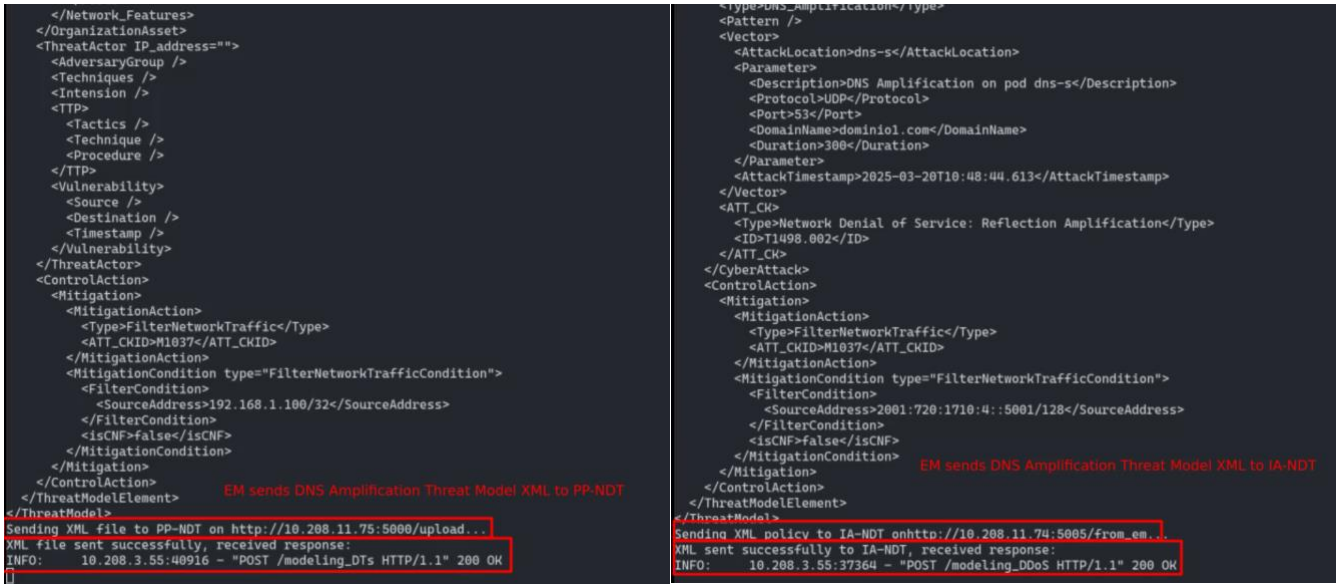

Figure 4. Early Modelling information sent to the Network Digital Twins.

2. Prediction and Prevention Network Digital Twins makes the prediction of the attack and send the information to the Distributed and Trustable AI Engine.

The Prediction and Prevention NDT maps IP addresses from the actual network to internal IP addresses and replicates the traffic flows by emulating the complete network.

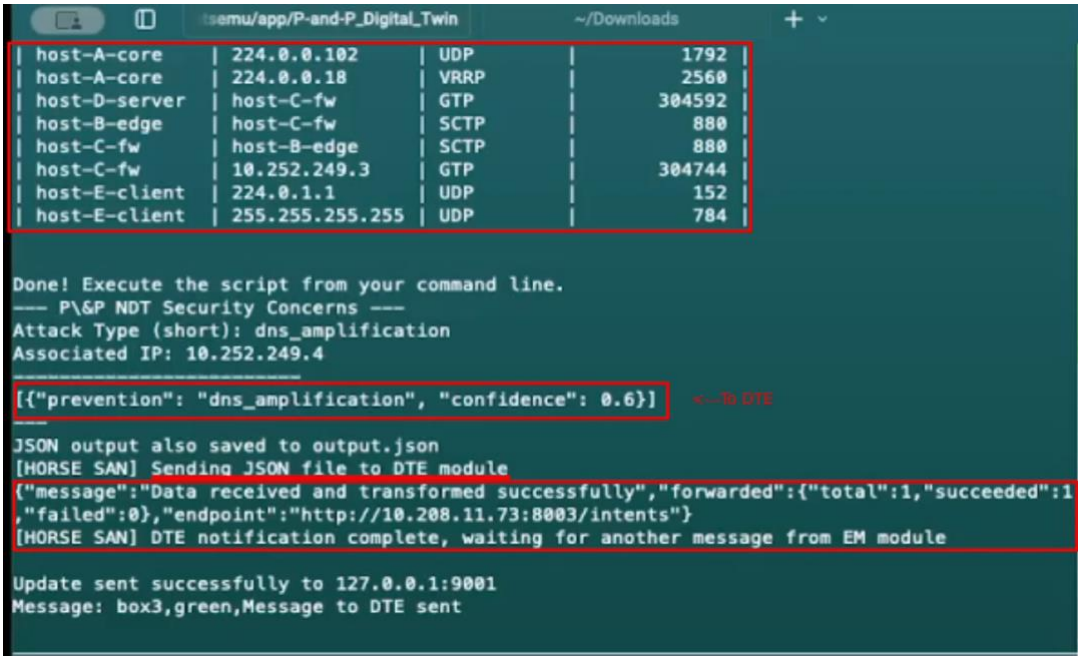

Figure 5. Prediction made from the Prediction and Prevention NDT and forwarded to the DTE.

3. Distributed and Trustable AI Engine elaborates the intent and sends it to the Intent-Based Interface.

The DTE, with the information obtained from the Prediction and Prevention NDT, elaborates a specific intent to mitigate the attack that is sent to the Intent-Based Interface. When it arrives, it can be checked in the IBI Dashboard the new intent (still not fulfilled) and the new threat pending to be mitigated.

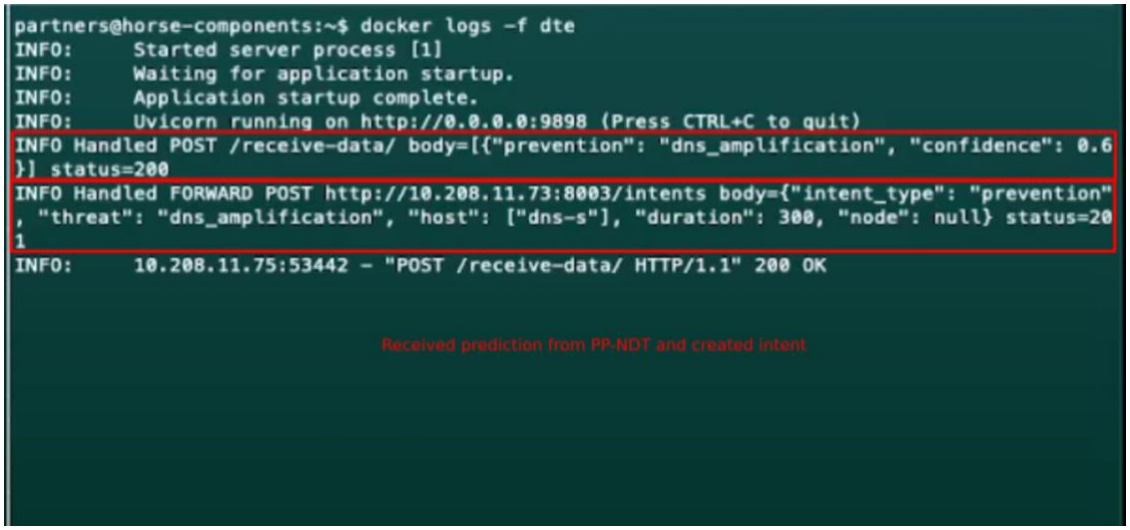

Figure 6. Intent created from the DTE and sent to the Intent-Based Interface.

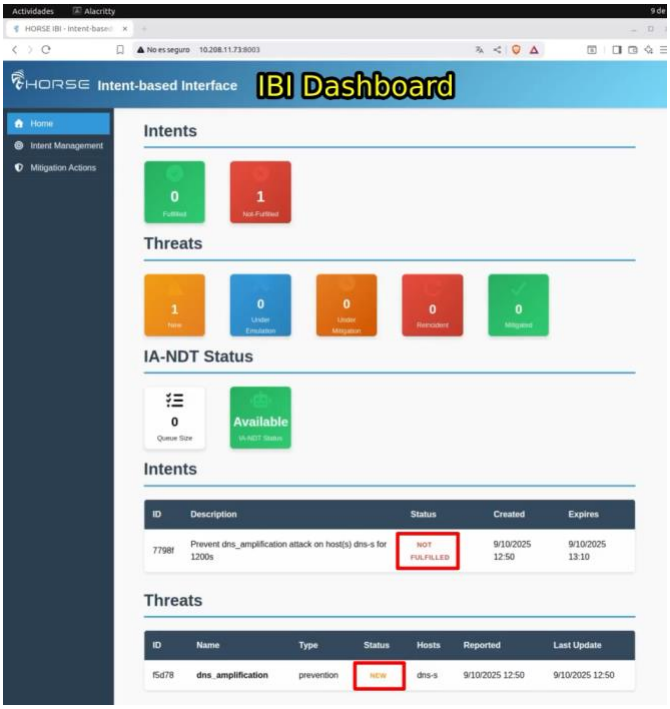

Figure 7. IBI Dashboard including the information of the new intent and attack.

4. Intent-Based interface starts the what-if loop with the Impact Analysis Network Digital Twin.
    a. First mitigation action: MONITOR

To let the IBI know the actual impact of the attack, it sends a MONITOR action, so the Impact Analysis NDT just launch the concrete attack without any mitigation. The result of a DNS Amplification attack for 30 seconds is a big amount of packets per second captured in the router interface. Meanwhile, the IBI dashboard changes the state of the threat to “UNDER EMULATION”.

```
policy-translator | INFO:werkzeug:10.208.3.55 - - [09/Oct/2025 10:49:51] "POST /from_em HTTP/1.1" 200 -
policy-translator | INFO:ibi_handler:IBI Mitigation Action (monitor):
policy-translator | {
policy-translator |     "id": "1b3287d4-441e-4da2-af09-1edf1e02c63d",
policy-translator |     "topology_name": "horse_ddos",
policy-translator |     "attack": "DNS_Amplification",
policy-translator |     "what-condition": {
policy-translator |         "KPIs": {
policy-translator |             "element": {
policy-translator |                 "node": "ceos3",
policy-translator |                 "interface": "eth2"
policy-translator |             },
policy-translator |             "metric": "packets-per-second",
policy-translator |             "duration": "30s"
policy-translator |         }
policy-translator |     },
policy-translator |     "if-condition": {
policy-translator |         "action": {
policy-translator |             "type": "monitor",
policy-translator |             "value": "*",
policy-translator |             "unit": "*",
policy-translator |             "duration": "30s"
policy-translator |         },
policy-translator |         "element": {
policy-translator |             "node": "*",
policy-translator |             "interface": "*",
policy-translator |             "network": "*",
policy-translator |             "ref": "* * *"
policy-translator |         }
policy-translator |     }
policy-translator | }
policy-translator | Read policy and removed file: /tmp/policy_cache/policy_DNS_Amplification.xml
```

Figure 8. IBI what-if request to the IA-NDT for the MONITOR action.

```
policy-translator |             "interface": "*",
policy-translator |             "network": "*",
policy-translator |             "ref": "* * *"
policy-translator |         }
policy-translator |     }
policy-translator | }
policy-translator | Read policy and removed file: /tmp/policy_cache/policy_DNS_Amplification.xml
policy-translator | INFO:ibi_handler:[IBI] Sent XML to orchestrator: 200
policy-translator | INFO:ibi_handler:EM policy sent for DNS_Amplification: 200
policy-translator | INFO:ibi_handler:Telemetry scheduled in 30s with a duration of 30s
policy-translator | INFO:werkzeug:10.208.11.73 - - [09/Oct/2025 10:50:21] "POST /from_ibi HTTP/1.1" 200 -
policy-translator | INFO:ibi_handler:Metrics obtained (packets-per-second):
policy-translator | {
policy-translator |     "id": "1b3287d4-441e-4da2-af09-1edf1e02c63d",
policy-translator |     "topology_name": "horse_ddos",
policy-translator |     "attack": "DNS_Amplification",
policy-translator |     "what": {
policy-translator |         "KPIs": {
policy-translator |             "element": {
policy-translator |                 "node": "ceos3",
policy-translator |                 "interface": "eth2"
policy-translator |             },
policy-translator |             "metric": "packets-per-second",
policy-translator |             "result": {
policy-translator |                 "value": "12848.0",
policy-translator |                 "unit": "packets-per-second"
policy-translator |             }
policy-translator |         }
policy-translator |     }
policy-translator | }
policy-translator | INFO:ibi_handler:Sent telemetry data to impact-analysis endpoint: 200
policy-translator | INFO:ibi_handler:Response: {"status":"success","job_id":"1b3287d4-441e-4da2-af09-1edf1e02c63d","value":12848.0}
```

Figure 9. IA-NDT what-if response to the IBI for the MONITOR action.

Figure 10. IBI dashboard showing the IA-NDT is emulating.

b. Second mitigation action: RATE LIMIT

Now that the IBI knows the impact that the attack has on the network, it is time to send the first mitigation action. The IBI sends a RATE LIMIT action in the router 3 of 1 Mbps. Then, the Impact Analysis NDT executes the attack and the mitigation action, sending back the values of the emulation.

```
policy-translator | INFO:ibi_handler:Sent telemetry data to impact-analysis endpoint: 200
policy-translator | INFO:ibi_handler:Response: {"status":"success","job_id":"1b3287d4-441e-4da2-af09-1edf1e02c63d","value":12848.0}
policy-translator | INFO:ibi_handler:IBI Mitigation Action (rate_limit):
policy-translator | {
policy-translator |     "id": "1b3287d4-441e-4da2-af09-1edf1e02c63d",
policy-translator |     "topology_name": "horse_ddos",
policy-translator |     "attack": "DDoS_reverse",
policy-translator |     "what-condition": {
policy-translator |         "KPIs": {
policy-translator |             "element": {
policy-translator |                 "node": "ceos3",
policy-translator |                 "interface": "eth2"
policy-translator |             },
policy-translator |             "metric": "packets-per-second"
policy-translator |             "duration": "15s"
policy-translator |         }
policy-translator |     },
policy-translator |     "if-condition": {
policy-translator |         "action": {
policy-translator |             "type": "rate_limit",
policy-translator |             "value": "1",
policy-translator |             "unit": "mbps",
policy-translator |             "duration": "30s"
policy-translator |         },
policy-translator |         "element": {
policy-translator |             "node": "ceos3",
policy-translator |             "interface": "eth2",
policy-translator |             "network": "*",
policy-translator |             "ref": "ceos3_eth2_*"
policy-translator |         }
policy-translator |     }
policy-translator | }
```

Figure 11. IBI what-if request to the IA-NDT for the RATE LIMIT action.

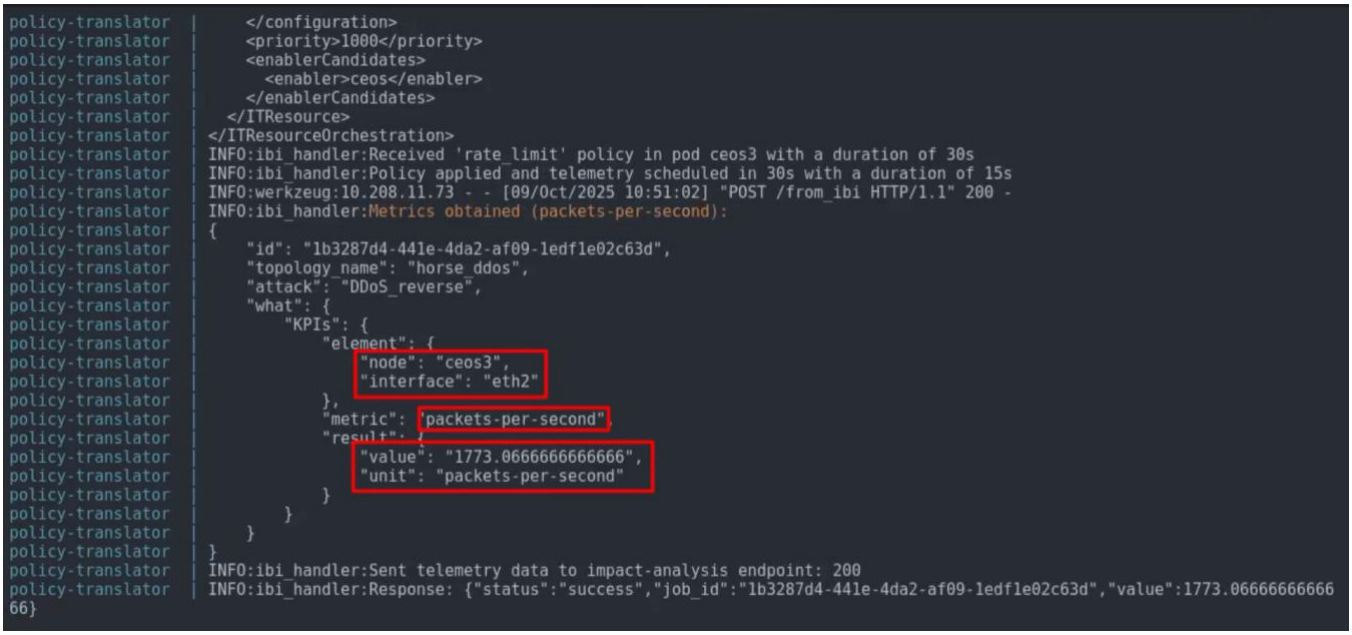

Figure 12. IA-NDT what-if response to the IBI for the RATE LIMIT action.

c. Third mitigation action: BLOCK IP

The IBI, according to its internat QoS policies, considered that the values of the rate limit action are still not enough for the mitigation of the attack. So the IBI sends the next mitigation action to properly mitigate the attack, this is the BLOCK IP of the attacker in the router 3 interface.

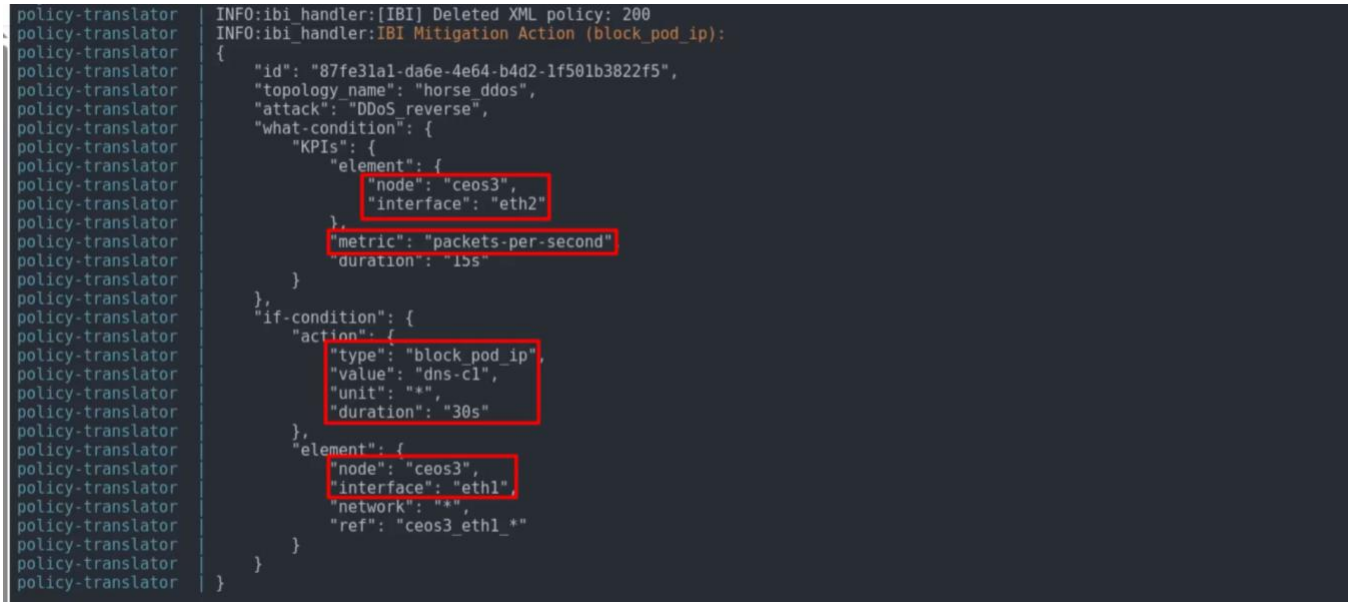

Figure 13. IBI what-if request to the IA-NDT for the BLOCK IP action.

Now, the result of this mitigation option is zero packets per second, as all the traffic has been blocked on that interface.

```
policy-translator |       <Name>Conf_87fe31a1-da6e-4e64-b4d2-1f501b3822f5</Name>
policy-translator |     </configuration>
policy-translator |     <priority>1000</priority>
policy-translator |     <enablerCandidates>
policy-translator |       <enabler>ceos</enabler>
policy-translator |     </enablerCandidates>
policy-translator |   </ITResource>
policy-translator | </ITResourceOrchestration>
policy-translator | INFO:ibi_handler:Received 'block_pod_ip' policy in pod ceos3 with a duration of 30s
policy-translator | INFO:ibi_handler:Policy applied and telemetry scheduled in 30s with a duration of 15s
policy-translator | INFO:werkzeug:10.208.11.73 - - [09/Oct/2025 10:51:56] "POST /from_ibi HTTP/1.1" 200 -
policy-translator | INFO:ibi_handler:Metrics obtained (packets-per-second):
policy-translator | {
policy-translator |     "id": "87fe31a1-da6e-4e64-b4d2-1f501b3822f5",
policy-translator |     "topology_name": "horse_ddos",
policy-translator |     "attack": "DDoS_reverse",
policy-translator |     "what": {
policy-translator |         "KPIs": {
policy-translator |             "element": {
policy-translator |                 "node": "ceos3",
policy-translator |                 "interface": "eth2"
policy-translator |             },
policy-translator |             "metric": "packets-per-second",
policy-translator |             "result": {
policy-translator |                 "value": "0.0",
policy-translator |                 "unit": "packets-per-second"
policy-translator |             }
policy-translator |         }
policy-translator |     }
policy-translator | }
policy-translator | INFO:ibi_handler:Sent telemetry data to impact-analysis endpoint: 200
policy-translator | INFO:ibi_handler:Response: {"status":"success","job_id":"87fe31a1-da6e-4e64-b4d2-1f501b3822f5","value":0.0}
```

Figure 14. IA-NDT what-if response to the IBI for the BLOCK IP action.

And the IBI dashboard shows that the state of the tread is MITIGATED and the intent has been FULFILLED.

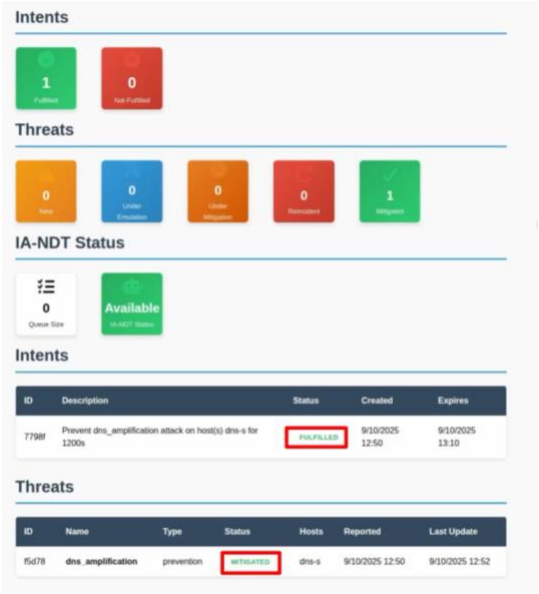

Figure 15. IBI dashboard showing the attack has been mitigated.

2.4. Gaps identified and recommendations

During the execution of PoC#15, some potential improvement areas were identified, and the team believes they will help in advancing zero-touch management in 6G environments:

- Standardization of NDT Interfaces and Models: There is a lack of standardized interfaces and data models to ensure seamless integration and interoperability among different Network Digital Twins (NDTs), management entities, and AI modules. Defining common APIs and data models would enable broader adoption and plug-and-play deployment across domains.

- Scalability and Multi-Domain Operation: While the PoC validates closed-loop automation in a controlled sandbox, larger-scale and real-world multi-domain scenarios may present new complexity. Future PoCs could include experimentation with wider, multi-stakeholder environments and guidelines for cross-domain orchestration.

2.5. Acknowledgements

This work is jointly funded by the European Commission through the HORIZON-JU-SNS-2022 HORSE project with Grant Agreement number 101096342.