

M&=<u>n</u>5G

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

Grant Agreement No	871780	Acronym	MonB5G		
Full Title	Distributed Manage	ment of Network Slices i	n beyond 5G		
Start Date	01/11/2019	Duration	42 months		
Project URL	https://www.monb5g.eu/				
Deliverable	D6.4 – Demonstratio	5.4 – Demonstration of AI-assisted security monitoring and enforcement			
Work Package	WP6				
Contractual due date	M42	Actual submission dat	e 07/06/2023		
Nature	Demonstrator	Dissemination Level	Public		
Lead Beneficiary	EUR				

Document Summary Information

Deliverable D6.4 – Demonstration of AI-assisted security monitoring and enforcement [Public]



Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the MonB5G consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the MonB5G Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the MonB5G Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© MonB5G Consortium, 2019-2023. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Deliverable D6.4 – Demonstration of Al-assisted security monitoring and enforcement [Public]



TABLE OF CONTENTS

1	Vic	deo Release and PoC-2 Summary	4
	1.1	PoC-2- Scenario 1 and 2	4
	1.2	PoC-2- Scenario 3	5

Deliverable D6.4 – Demonstration of AI-assisted security monitoring and enforcement [Public]



1 Video Release and PoC-2 Summary

PoC-2- Scenario 1 and 2 1.1

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.

AMF logs				
361	AMP		H A([2022-05-18 16:03:05,543] IN+0 in controller: (b'900366000000000)")	
[2622-05-10716:04:01.024046] [AV RED] 205950000020011] 161		11 SGAM-REGISTE 11 200, 95	[2022-05-10 16:53:03,144] [MFO in controller: 2652009761.578 [2022-05-18 16:53:03,144] [MFO in controller: limit = 1652089700.5 [2022-05-18 16:53:03,144] [MFO in controller: [b:20095000000020]	
[2022-05-10716:04:01.029764] [AM RED 20895000000012] 161	<pre>// [anf_app] [info] </pre>	12 564H-REGISTS 12 200, 95	132.138.75.132 - [15/May/2012_16:03:03] "PdSP /mew_device HTTP/L.1" 201 - Publishing remaining [ironjab] publishing: ("num_attachresuesis": 2. "actors": ["200950000000022", "20095000000000	
[2022+05+10716:04:01.035418] [AV RED] 200950000000013]	F) [anf_app] [info] 13	13 56/00-REGISTS 13 280, 95 [[], "timestamp": 1652889783.0] Publishing EDE (8)	Analytics
56 (2022-05-10716:04:01.841409) (AV RED) 20895000000014	/] [anf_app] ['info] 14	14) 56%H-REGISTE 14) 208, 95	[gromjab] publishing: ["end_event": true, "nun_attachrequests": 0, "actors": [], "timestamp": 1452089786.0}	Engine lo
16 [2022-05-1071d:04:01.007507] [AV RED] 20095000000015	f] [awf_app] [\nfe] 15	15) 5698-008161570 35] 288, 95]	(P) D2 (あらのかかかかり3*、*200950000000014*)、*でに用きてき用の**: 2052889762.の、*付きてもにていか、さ、5.3、(*nun_attach hequests': 10、*actors': (*2009500000015*、*20095000000005*、*20095400000003**、*20095400000003**、*20095400000003**	
10 [2822-85-18716:04:81.853611] [AM RED] 2089589806080016	NF) [anf_app] [info] 16	16 SGMM-DFREGISTE 16 288, 95		
16] [2022-05-18716104101.859967] [AM 800] 20895000000017] 16]) [anf_app] [lnfs] 17]	17 SGMM-DEREGISTE 17 268, 95	"tlmestang": 1652889774.0, "etrection": 0.0), ("num_sitachrequests": 2, "actors": ["200950000 010029", "200950000000030"], "trrestang": 652609708.0, ("etrection": 0.6)]" [?] WE at the 652002576.d has a detaction of 0.25	
[2022-05-18110:04:01.805897] [AM RED] 20805000000018] 20]	₩] [anf_app] [info] 18	18 SGMM-DEREGISTE 18 288, 95	[1] added this 20090000000015 to the blacklist	
[2022 03 18110:04:01.871383] [AM RED] 208950000000019]	W] [anf_app] [info] 19	19 SGAN DEREGISTE 19 288, 95	[1] added inst 2689568686666817 to the plackist [1] added inst 26855080808018 to the blackist [2] added inst 26855080080518 to the blackist	Decision
10 [2022-05-18716:04:01.876933] [AM 8LD] 20095000000020]	F] [anf_app] [info] 	201 SGMM-DEREGISTE 201 200, 95 1	added (noi 20095000000000 to the blacklist [// added (noi 20095000000000 to the blacklist [/ added (noi 2009500000000 to the blacklist	Engine lo
10 [2022-05-18716:04:01.882559] [AM CISTEMED	F] [anf_nt] [debug] Set !	GNN state to _SGNN_DERE		
[2022-05-10716:04:01.002613] [AV 000000021, State SCNM-DERECISTER	ED) success		Tester Tester	
[2022-05-10716:04:01.086260] [AV 0157ERED [2022-05-10716:04:01.086309] [AV			Creating tester Jone	
000000023, State SCHH-DEREGISTER 12022-05-10716:04:01.0939651 [AV 635770070	(D) success		compcom:~/redouane_wrtc-ddas-response-system% clear compcom:~/redouane_wrtc-ddas-response-system% gur% http://lz7.0.0.1:1337/brigger_event/30/90	
[2022+05+10716:04:01.094013] [AV 000000024, State SGNH-DEREGISTER	(ID) SUCCESS		camigcom -/redovane_mrtc-ddas-response-systems [RAN simi
[2022-05-18116:04:01.895821] [AV RED] 20895000000025]	F] [ant_app] [info] 25	24 SCAN-REGISTE 251 288, 95 1		terminal

Deliverable D6.4 – Demonstration of AI-assisted security monitoring and enforcement [Public]



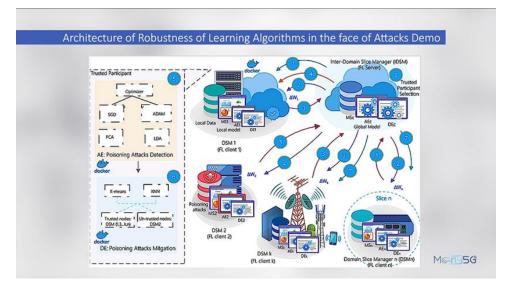


Figure 1-1: PoC2 Scenario 1&2 Screen shots

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.

Deliverable D6.4 – Demonstration of AI-assisted security monitoring and enforcement [Public]



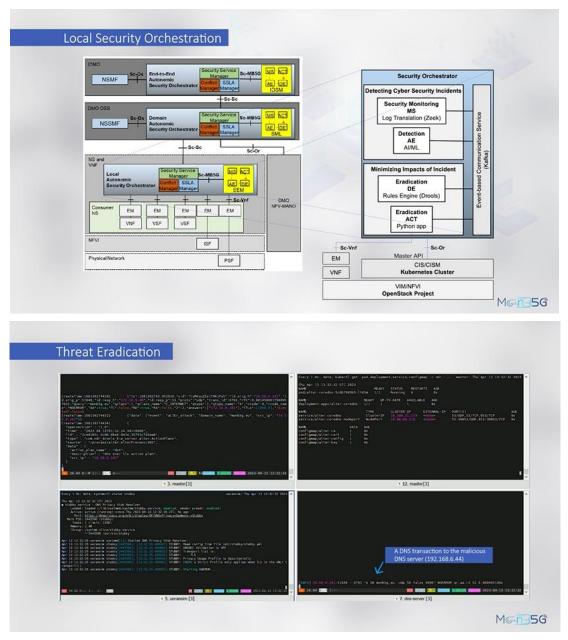


Figure 1-2: PoC2 Scenario 3 Screen shots

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

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