Data Traffic Monitoring

User Manual

SPHINX

A Universal Cyber Security Toolkit for
Health-Care Industry

Table of contents

Table of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

Data Traffic Monitoring is a SPHINX component responsible with threat identification by monitoring the network traffic and applying signature-based detection analysis. It monitors all the packets traversing the network and compares them against a database of attack signatures or attributes of known malicious threats.

DTM is a Network Intrusion Detection System (NIDS) optimized to work in the SPHINX Ecosystem by communicating with other SPHINX components and exposing alerts and relevant statistics to the users.

2 Installation/Deployment

The installation is based on docker images for deploying the DTM.

2.1 Prerequisites and hardware

Preconditions:

1. Kafka:
    - optional: kafdrop (for browser based interaction with kafka)
2. Docker image for PostgreSQL
3. Docker image for Sphinx Component ID-UI

Hardware:

1. CPU: medium CPU like Intel I7
2. GPU: no needed
3. RAM: medium Ram like 8 GB RAM
4. HDD: at least 1 terabyte(for tools (tshark, Suricata, logstash) and for files used for data analysis (pcap and json).

2.2 Deployment with Docker

1. #docker login https://sphinx-repo.intracom-telecom.com/

2. #docker pull registry.sphinx-repo.intracom-telecom.com/sphinx-project/data-traffic-monitoring/dtm-deployment:latest

3. #docker run <id imagine>

2.3 Deployment with Kubernetes

DTM can be deployed on a K8S cluster using .yml files.

3 Operation and maintenance

When the DTM is started, it starts capturing network traffic from various protocols. Packets and files that come in various formats are analyzed and alerts are issued if unusual network activity is detected.

3.1 Basic Case Examples

Case 1: Creating an instance

Objective:

The user wants to create an instance in order to identify information about network traffic.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Steps:

Access the instances and tools option: https://sphinx-kubernetes.intracom-telecom.com/id-ui/dtm/instances. In the chapter 4 "Application UI presentation", in the section "A. Instances and Tools component" are detailed and explained the steps for creating an instance.

Case 2: Asset Discovery

Objective:

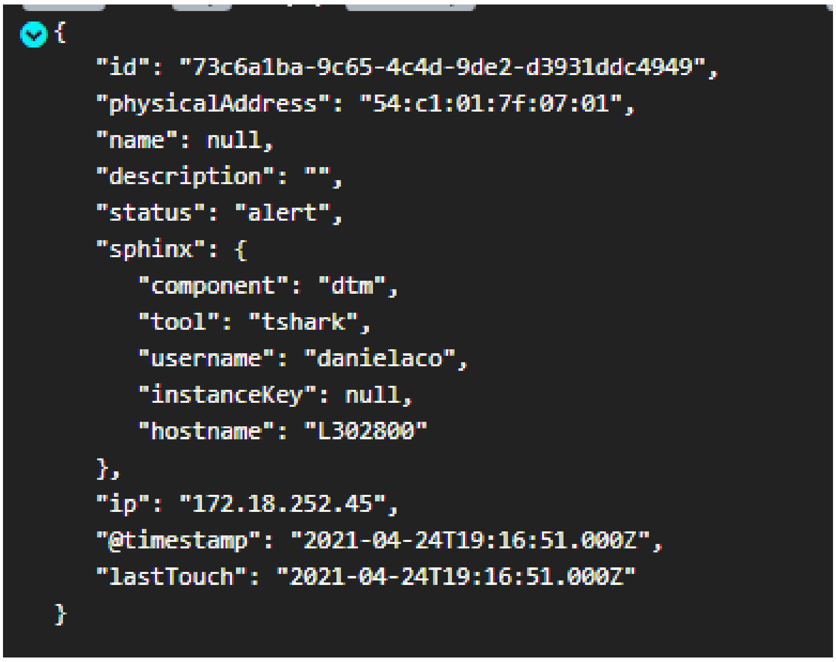
The user wants to view the list of new devices that have appeared on the network.

Steps:

Access the asset discovery option: https://sphinx-kubernetes.intracom-telecom.com/id-ui/dtm/asset-discovery.

For this component, alerts can be read from a pcap file (if there is no network traffic) or are generated in real time based on capturing network traffic at the moment a Tshark instance is started.

In **Figure 4.14** from 4 you can see the display of the list of devices in the interface, also in **Figure 3.1** it can be seen that the alerts are transferred to the dtm-asset topic .



```
{
    "id": "73c6a1ba-9c65-4c4d-9de2-d3931ddc4949",
    "physicalAddress": "54:c1:01:7f:07:01",
    "name": null,
    "description": "",
    "status": "alert",
    "sphinx": {
       "component": "dtm",
       "tool": "tshark",
       "username": "danielaco",
       "instanceKey": null,
       "hostname": "L302800"
    },
    "ip": "172.18.252.45",
    "@timestamp": "2021-04-24T19:16:51.000Z",
    "lastTouch": "2021-04-24T19:16:51.000Z"
 }
```

Figure 3.1 Sample message published to dtm-asset topic

3.2 Links with other Components

For the links to other components, DTM offers the following services:

- assetcatalogue/getAssetDiscoveryAlerts – displays an alert message when a new device appears
- tshark/persistAll – moving pcap files generated by Tshark
- alerte/grafice –provides data for graphs that are displayed in the ID component

It also publishes messages to Kafka messaging service:

- dtm-metric
- dtm-alert
- dtm-event
- dtm-package
- dtm-asset

3.3 Outcomes

Upon completion of these test cases, alerts generated when a new device appears on the network will be thrown, but also alerts generated by Suricata based on the rules configured.

4 Application UI presentation

Figure 4.1 shows the main screen that displays the components that make up the DTM. These are: Instances and Tools, Alerts and Asset Discovery.

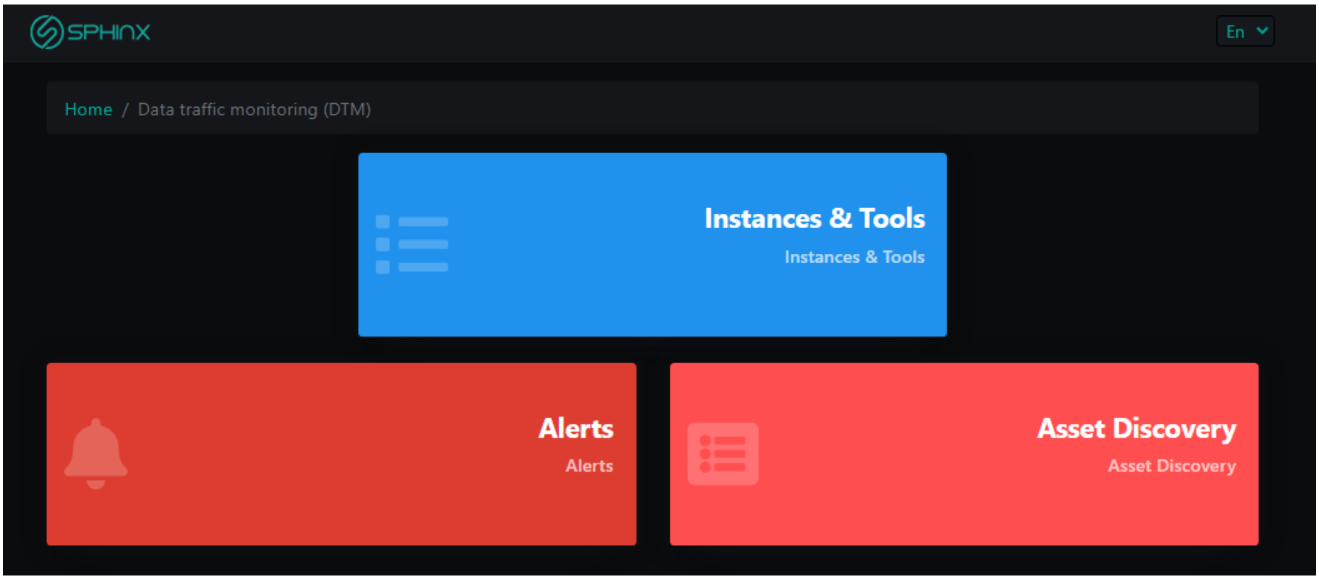
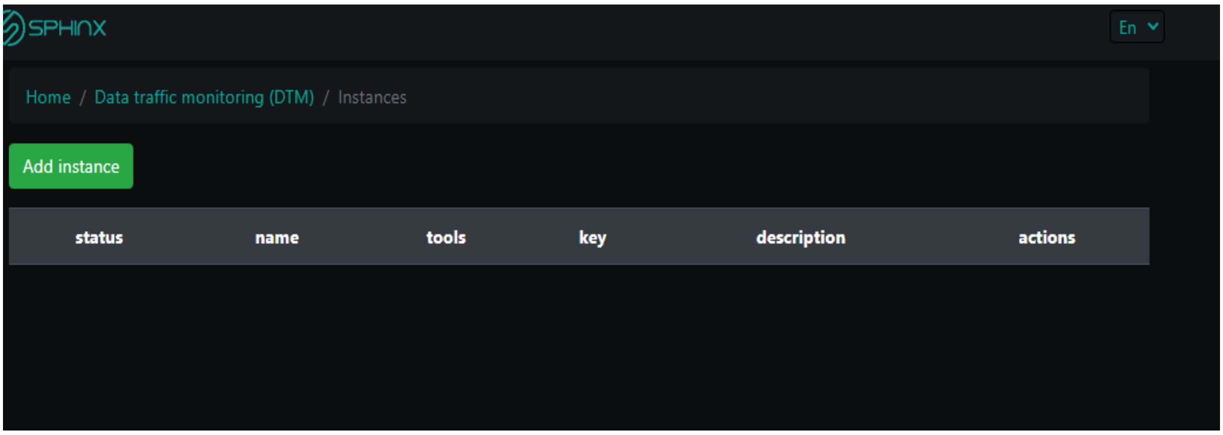


Figure 4.1 The main screen

A. Instances and Tools component:

The Instances and Tools screen (**Figure 4.2**) allows defining new agents, choosing between integration with Tshark and Suricata and configuring specific information for Tshark or Suricata.

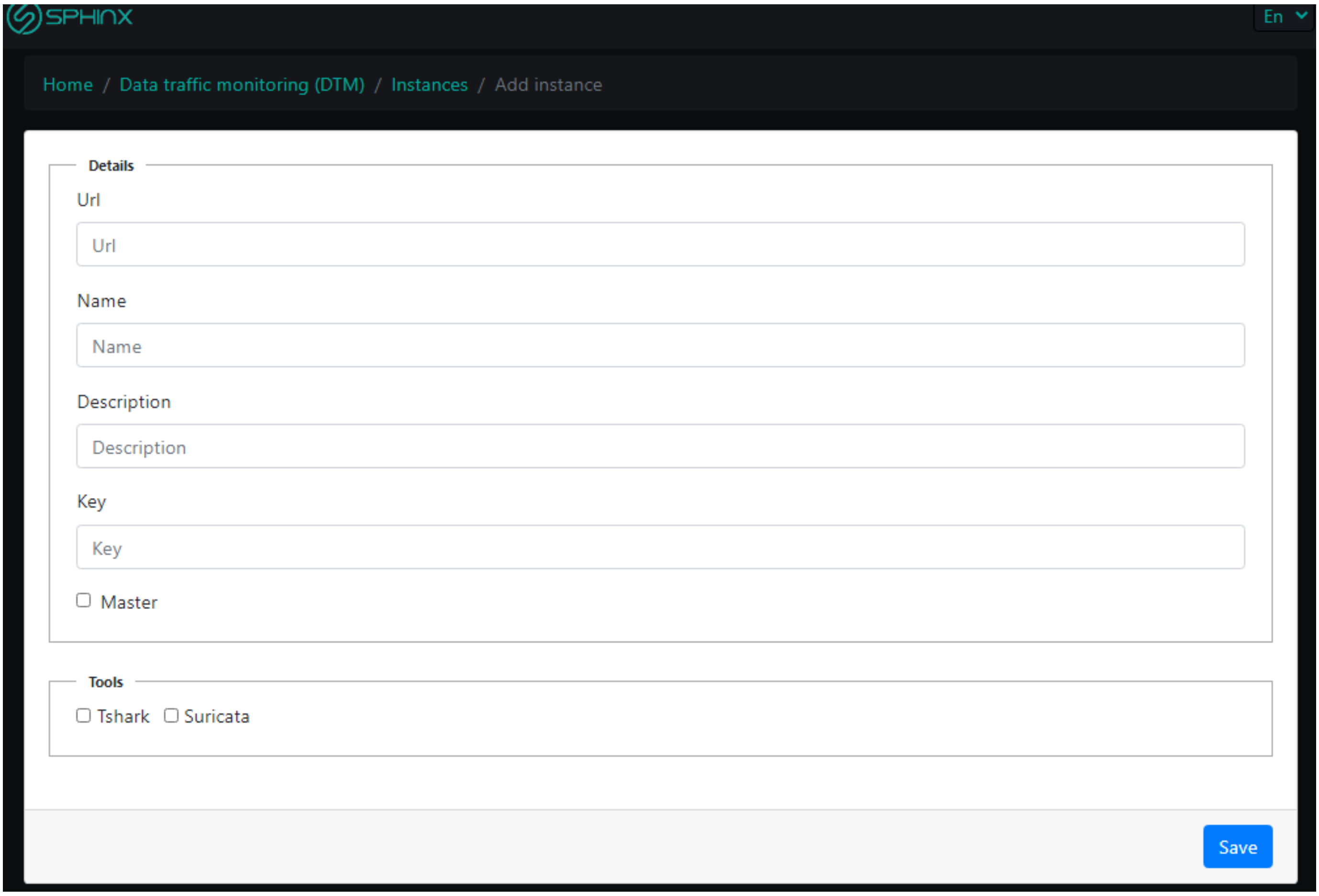


status	name	tools	key	description	actions

Figure 4.2 Instances and tools Screen

Each agent is an instance of DTM. It is managed by a primary DTM instance called the "DTM Management". The "Add instance" button allows you to add an instance. To create an instance you must specify the URL, name, description and a unique key (**Figure 4.3**). Each agent starts with a key, as a security mode, to start Tshark or Suricata and finally writes messages in kafka topics. A key can be randomly generated, recommended by an administrator. The key is sent as the parameter when starting an agent. In conclusion to start the Tshark or Suricata processes, the instance must be activated and the key must correspond to its definition.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Home / Data traffic monitoring (DTM) / Instances / Add instance

Details

Url

Url

Name

Name

Description

Description

Key

Key

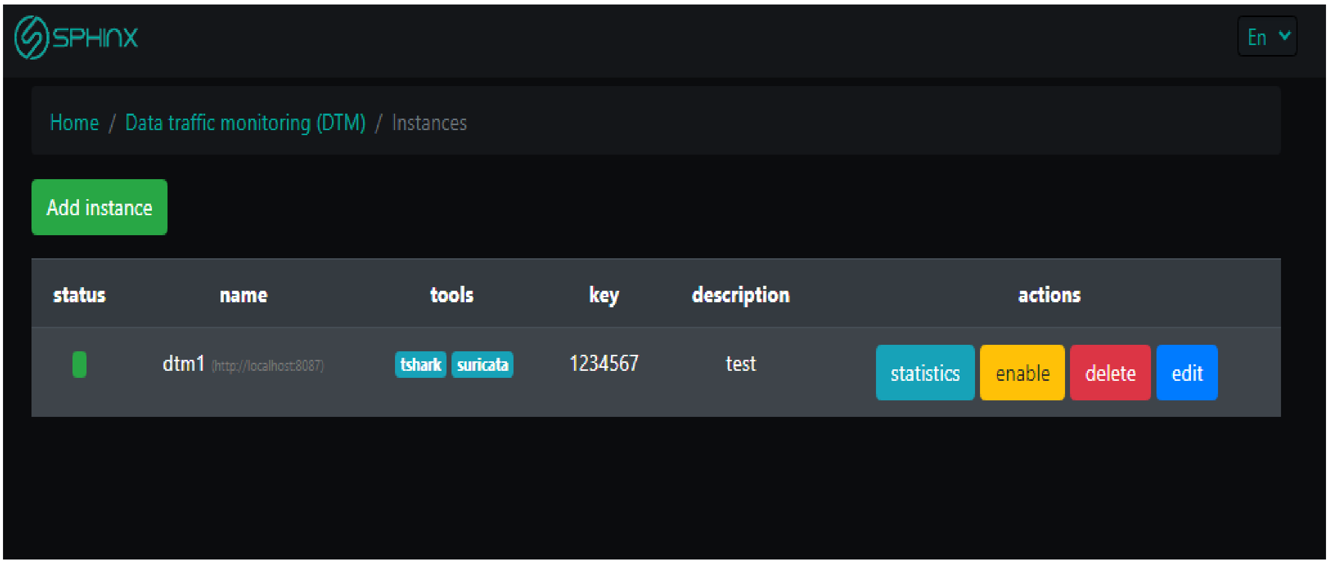
□ Master

Tools

□ Tshark □ Suricata

Figure 4.3 The screen adds the instance

Each local instance of DTM can be disabled, deleted, or certain details can be edited, except for the key. When the instance is disabled, all tshark processes on that instance are stopped. A newly created instance is disabled by default. In **Figure 4.4** it can be seen if an instance is enabled. This is marked in the status column with red, if the instance is not turned on and with green if it is enabled.

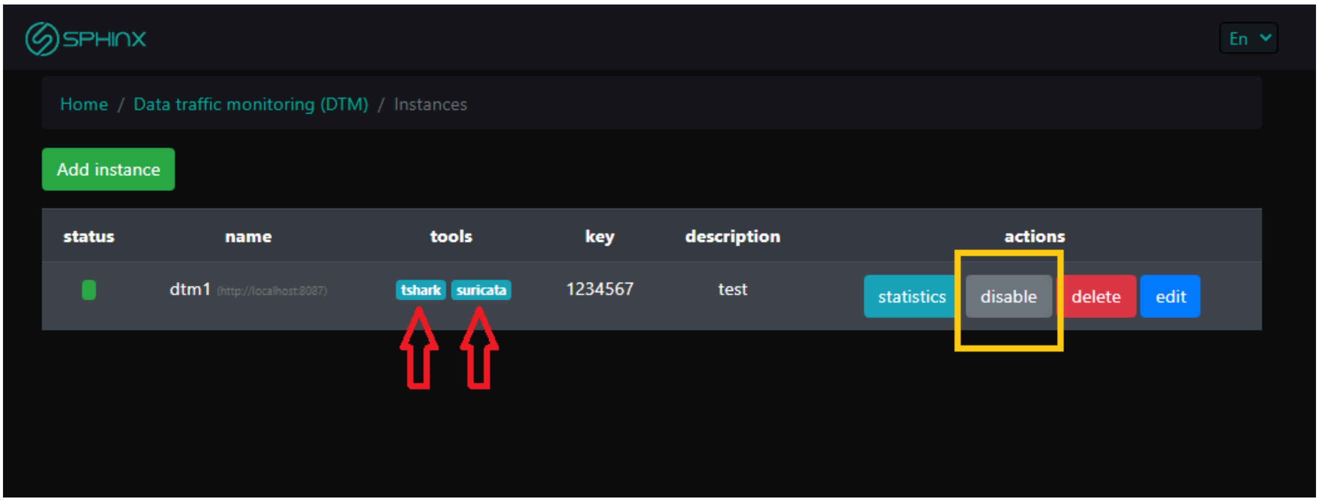


Home / Data traffic monitoring (DTM) / Instances

status	name	tools	key	description	actions
🟩	dtm1 (http://localhost:8087)	tshark suricata	1234567	test	statistics enable delete edit

Figure 4.4 The table with instances

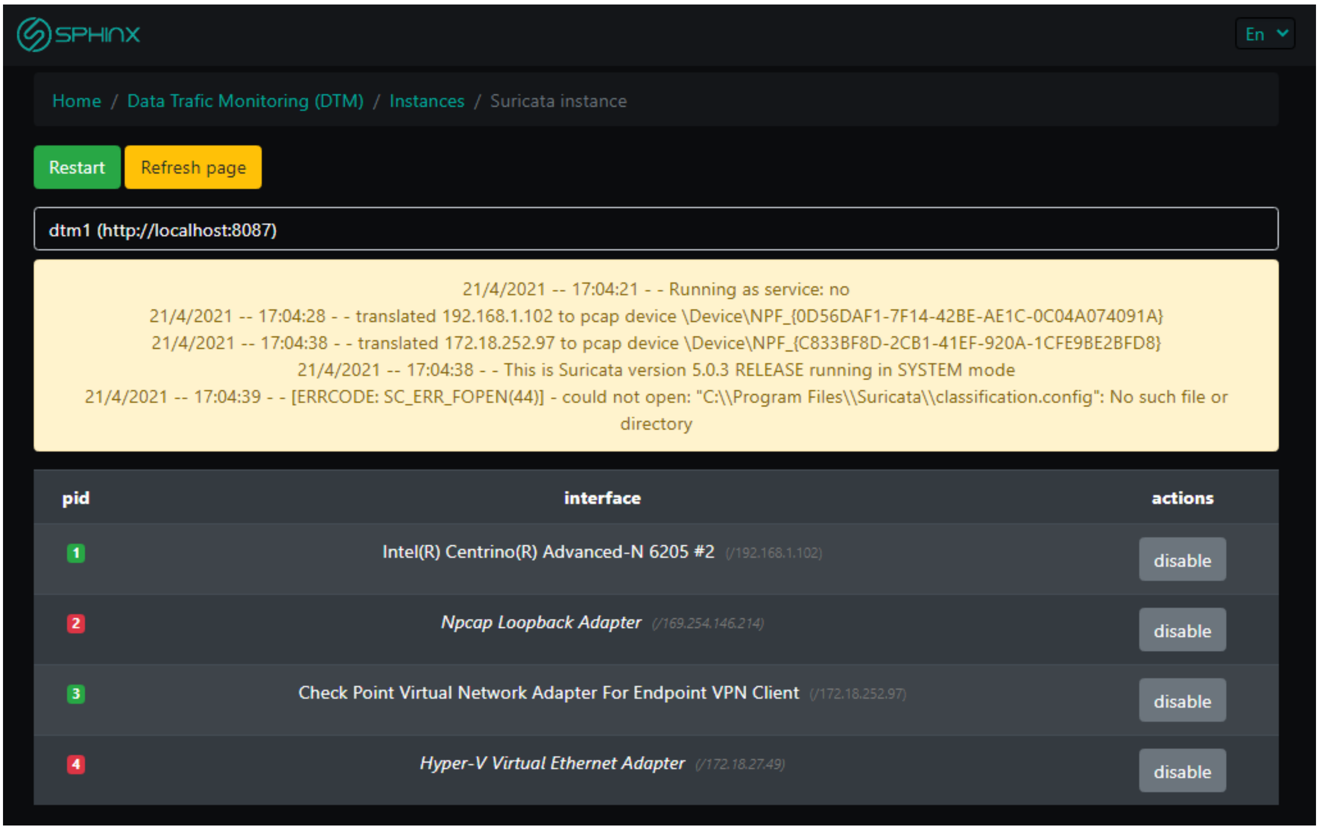
To configure the instances, press the tshark or suricata button. Make sure the instance is enabled (**Figure 4.5**).



status	name	tools	key	description	actions
🟩	dtm1 (http://localhost:8087)	tshark suricata	1234567	test	statistics disable delete edit

Figure 4.5 Select the Tshark or Suricata Button

The Suricata Instance configuration screen is in **Figure 4.6** and shows a list of network interfaces. The Suricata instance can be restarted by clicking the "Restart" button. After pressing the restart button, to update the data in the interface table, click the "Refresh page" button.


SPHINX
En
Home / Data Trafic Monitoring (DTM) / Instances / Suricata instance
Restart
Refresh page

dtm1 (http://localhost:8087)

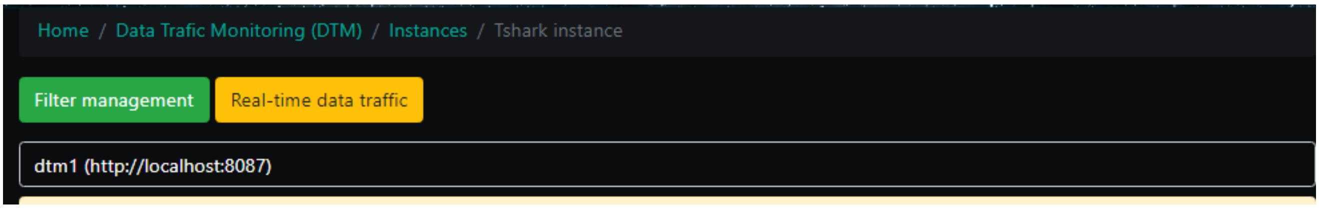
```
21/4/2021 -- 17:04:21 - - Running as service: no
21/4/2021 -- 17:04:28 - - translated 192.168.1.102 to pcap device \Device\NPF_{0D56DAF1-7F14-42BE-AE1C-0C04A074091A}
21/4/2021 -- 17:04:38 - - translated 172.18.252.97 to pcap device \Device\NPF_{C833BF8D-2CB1-41EF-920A-1CFE9BE2BFD8}
21/4/2021 -- 17:04:38 - - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
21/4/2021 -- 17:04:39 - - [ERRCODE: SC_ERR_FOPEN(44)] - could not open: "C:\\Program Files\\Suricata\\classification.config": No such file or directory
```

pid	interface	actions
1	Intel(R) Centrino(R) Advanced-N 6205 #2 (/192.168.1.102)	disable
2	*Npcap Loopback Adapter* *(/169.254.146.214)*	disable
3	Check Point Virtual Network Adapter For Endpoint VPN Client (/172.18.252.97)	disable
4	*Hyper-V Virtual Ethernet Adapter* *(/172.18.27.49)*	disable

Figure 4.6 Suricata instance

The Tshark configuration screen is in **Figure 4.7** and **Figure 4.11** and is structured in two parts. The first part of the screen contains the "Filter management" button and the "Real-time data traffic" button and the second part contains a table contains a table showing the interfaces, the filter, the number of packets and what actions can be taken on that process.

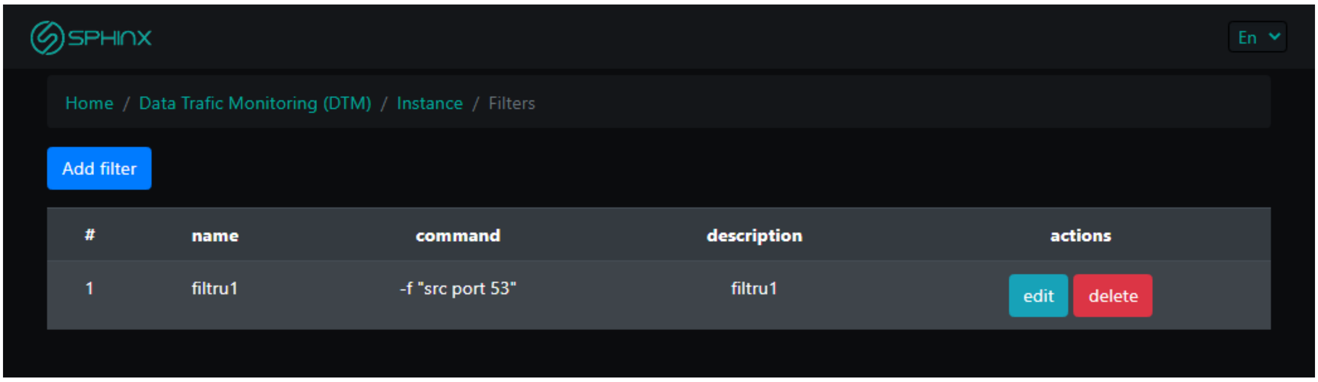
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


Home / Data Trafic Monitoring (DTM) / Instances / Tshark instance
Filter management
Real-time data traffic

dtm1 (http://localhost:8087)

Figure 4.7 Tshark's menu

When the "Filter management" button is pressed, the filter management screen opens. Within this screen, a list of filters can be displayed (**Figure 4.8**).



#	name	command	description	actions
1	filtru1	-f "src port 53"	filtru1	edit delete

Figure 4.8 Filter management screen

The "Add filter" button allows you to add a new filter. The details of a filter are: name and command that are required, and the description can be optional (**Figure 4.9**).

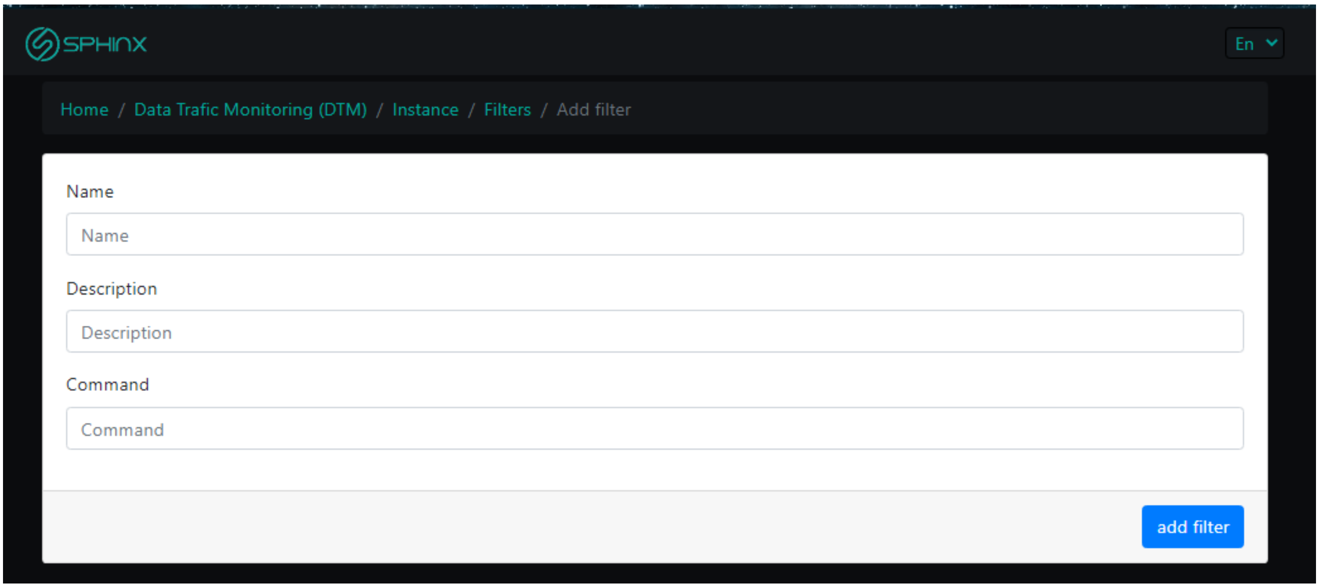
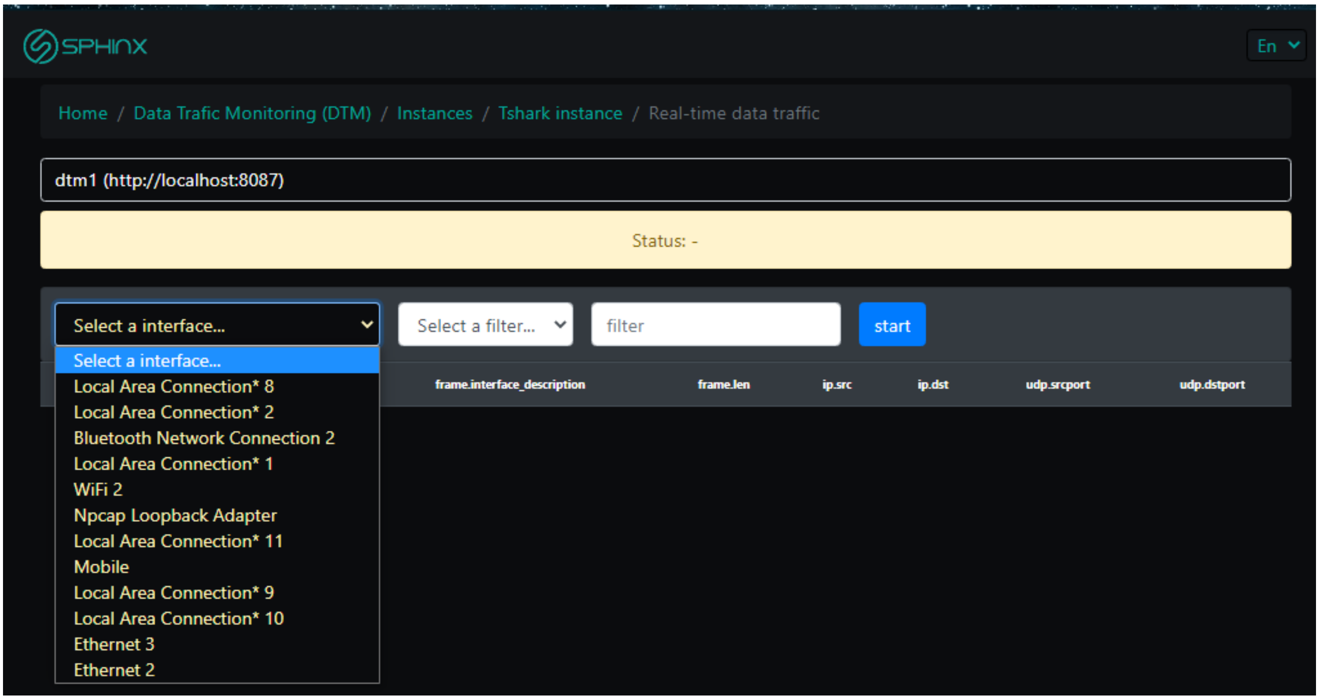

SPHINX
En
Home / Data Trafic Monitoring (DTM) / Instance / Filters / Add filter
Name
Name
Description
Description
Command
Command
add filter

Figure 4.9 Add filter screen

Pressing the "Real-time data traffic" button opens another screen where new processes can be added. The selector allows the list to be displayed on those instances (**Figure 4.10**). The interfaces are provided by Tshark.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



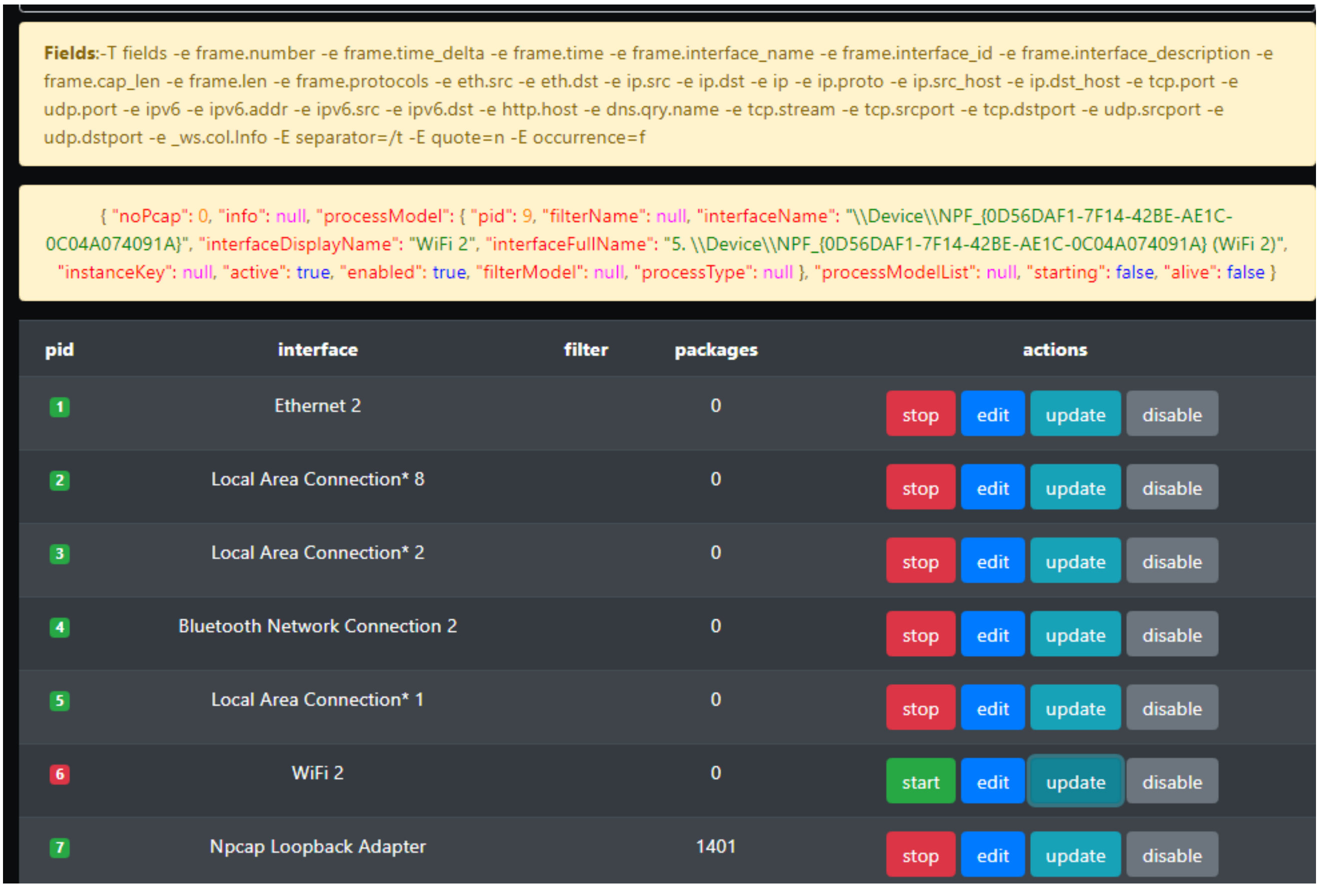
Home / Data Trafic Monitoring (DTM) / Instances / Tshark instance / Real-time data traffic

dtm1 (http://localhost:8087)

Status: -

Figure 4.10 Real-time data traffic screen

The second part of the screen contains a table with a list of processes (**Figure 4.11**). A process can be stopped, started, edited or disabled. When the update button is pressed, the number of packages and the process status are updated.



Fields:-T fields -e frame.number -e frame.time_delta -e frame.time -e frame.interface_name -e frame.interface_id -e frame.interface_description -e frame.cap_len -e frame.len -e frame.protocols -e eth.src -e eth.dst -e ip.src -e ip.dst -e ip -e ip.proto -e ip.src_host -e ip.dst_host -e tcp.port -e udp.port -e ipv6 -e ipv6.addr -e ipv6.src -e ipv6.dst -e http.host -e dns.qry.name -e tcp.stream -e tcp.srcport -e tcp.dstport -e udp.srcport -e udp.dstport -e _ws.col.Info -E separator=/t -E quote=n -E occurrence=f

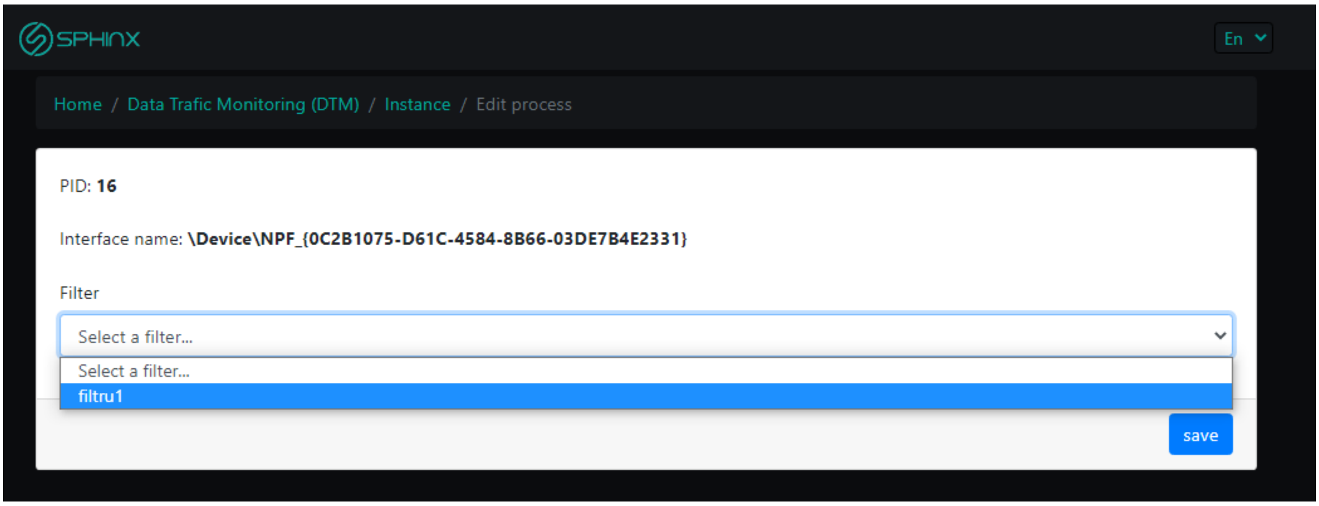
```
{ "noPcap": 0, "info": null, "processModel": { "pid": 9, "filterName": null, "interfaceName": "\\Device\\NPF_{0D56DAF1-7F14-42BE-AE1C-0C04A074091A}", "interfaceDisplayName": "WiFi 2", "interfaceFullName": "5. \\Device\\NPF_{0D56DAF1-7F14-42BE-AE1C-0C04A074091A} (WiFi 2)", "instanceKey": null, "active": true, "enabled": true, "filterModel": null, "processType": null }, "processModelList": null, "starting": false, "alive": false }
```

pid	interface	filter	packages	actions
1	Ethernet 2		0	stop edit update disable
2	Local Area Connection* 8		0	stop edit update disable
3	Local Area Connection* 2		0	stop edit update disable
4	Bluetooth Network Connection 2		0	stop edit update disable
5	Local Area Connection* 1		0	stop edit update disable
6	WiFi 2		0	start edit update disable
7	Npcap Loopback Adapter		1401	stop edit update disable

Figure 4.11 Process table

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

When editing a process, another screen opens (**Figure 4.12**) where you can see that "Interface name" can no longer be changed, but you can choose a filter for that interface (filter that was created in **Figure 4.9**).


SPHINX
En
Home / Data Trafic Monitoring (DTM) / Instance / Edit process

PID: **16**

Interface name: **\Device\NPF_{0C2B1075-D61C-4584-8B66-03DE7B4E2331}**

Filter

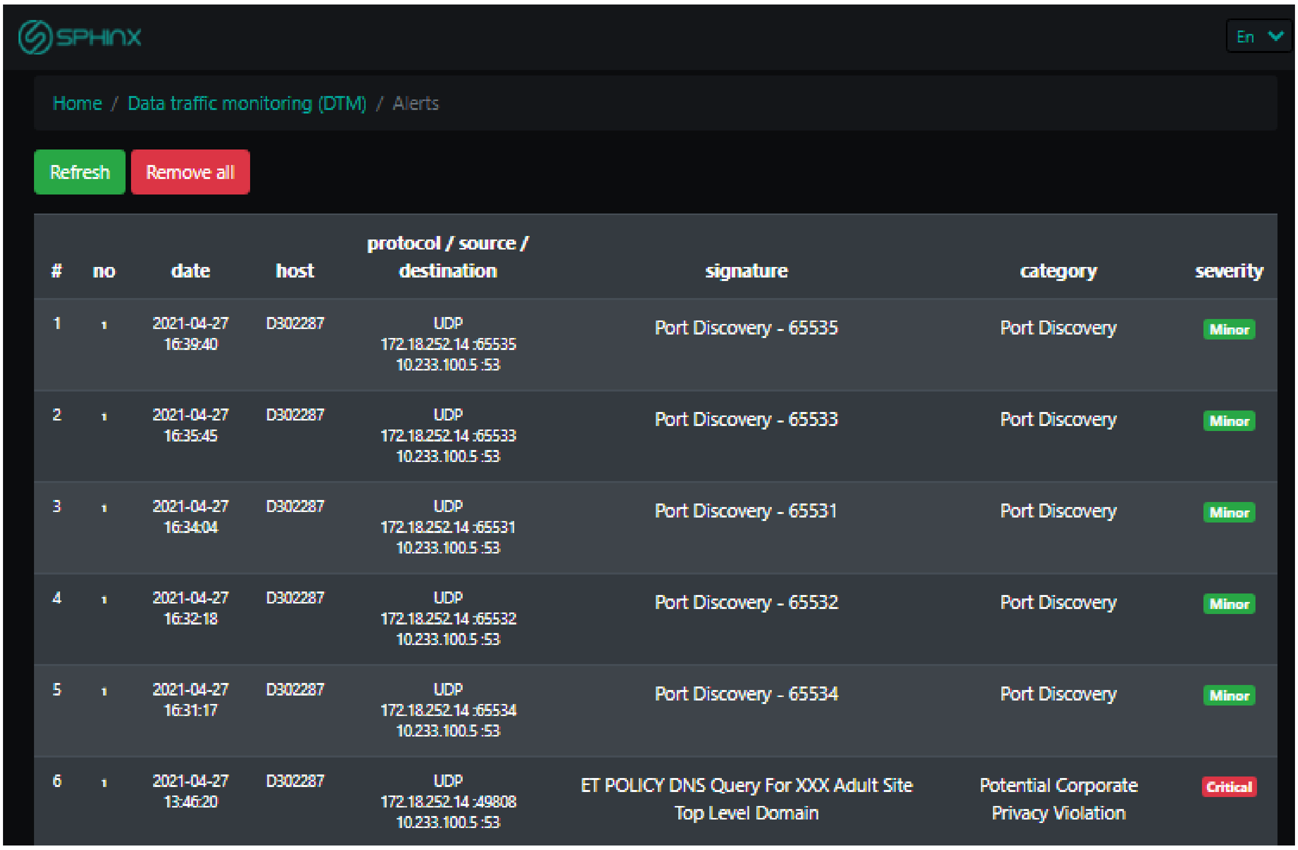
Select a filter...

Select a filter...
filtru1
save

Figure 4.12 Edit process screen

B. Alerts component:

Figure 4.13 shows the alert table that collects alerts from DTM components. The "Remove all" button allows you to delete existing alerts and the "Refresh" button allows updating the data in the alert table.



#	no	date	host	protocol / source / destination	signature	category	severity
1	1	2021-04-27 16:39:40	D302287	UDP 172.18.252.14 :65535 10.233.100.5 :53	Port Discovery - 65535	Port Discovery	Minor
2	1	2021-04-27 16:35:45	D302287	UDP 172.18.252.14 :65533 10.233.100.5 :53	Port Discovery - 65533	Port Discovery	Minor
3	1	2021-04-27 16:34:04	D302287	UDP 172.18.252.14 :65531 10.233.100.5 :53	Port Discovery - 65531	Port Discovery	Minor
4	1	2021-04-27 16:32:18	D302287	UDP 172.18.252.14 :65532 10.233.100.5 :53	Port Discovery - 65532	Port Discovery	Minor
5	1	2021-04-27 16:31:17	D302287	UDP 172.18.252.14 :65534 10.233.100.5 :53	Port Discovery - 65534	Port Discovery	Minor
6	1	2021-04-27 13:46:20	D302287	UDP 172.18.252.14 :49808 10.233.100.5 :53	ET POLICY DNS Query For XXX Adult Site Top Level Domain	Potential Corporate Privacy Violation	Critical

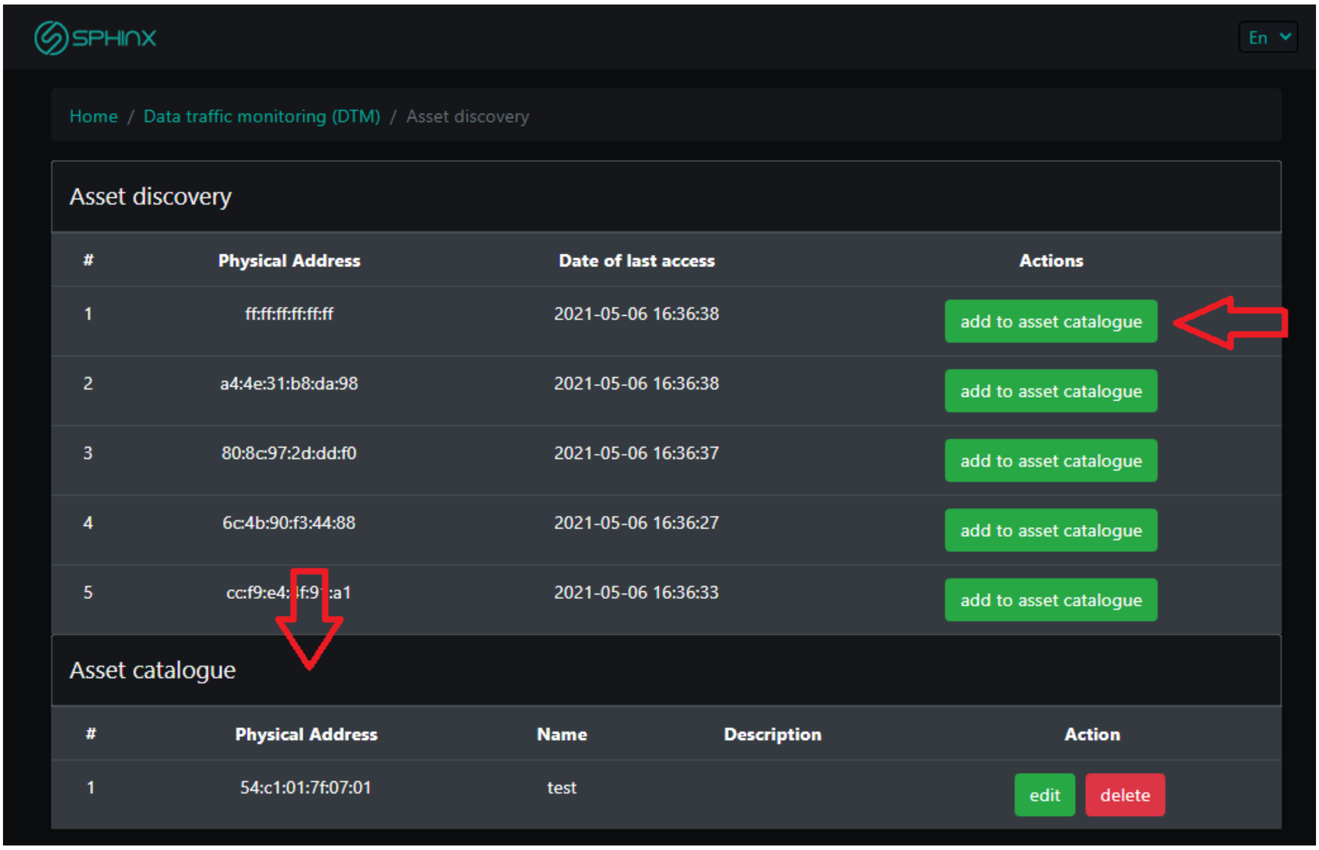
Figure 4.13 Alert table

C. Asset Discovery component:

Based on the network traffic generated at DTM startup, a series of alerts are displayed when a new device appears on the network. These alerts are generated in real time based on network traffic, obtained at the start of a Tshark instance. Asset discovery is divided into two sections (**Figure 4.14**). The first is asset

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

discovery, where the new devices are presented, more precisely their physical address, as well as the date when it was discovered. The "add to asset catalogue" button allows you to add records in the second section, Asset catalogue. Thus the Asset catalog contains a list of known devices. Each record in the table can be edited or deleted. When a record is deleted, it will be entered in the Asset discovery table.



Asset discovery

#	Physical Address	Date of last access	Actions
1	ff:ff:ff:ff:ff:ff	2021-05-06 16:36:38	add to asset catalogue
2	a4:4e:31:b8:da:98	2021-05-06 16:36:38	add to asset catalogue
3	80:8c:97:2d:dd:f0	2021-05-06 16:36:37	add to asset catalogue
4	6c:4b:90:f3:44:88	2021-05-06 16:36:27	add to asset catalogue
5	cc:f9:e4:4f:91:a1	2021-05-06 16:36:33	add to asset catalogue

Asset catalogue

#	Physical Address	Name	Description	Action
1	54:c1:01:7f:07:01	test		edit delete

Figure 4.14 Asset Discovery Screen