Decision Support System
User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

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.

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

The DSS is an essential part of the SPHINX Toolkit. Its purpose is to provide the end-user with a dedicated action plan for each event and also allow him/her to stop an ongoing attack. This component correlates the information retrieved of SPHINX's components and provides crucial information about the event, the vulnerabilities related to this event, and the affected assets. Furthermore, for each action plan, the DSS will provide a confidence level. Specifically, the user will have the ability to identify with how much confidence could implement the action plan. DSS can also distribute its information to other SPHINX Components through Kafka. Finally, the DSS's information will be displayed to the ID.

2 Installation/Deployment

2.1 Overview

The SPHINX DSS is a real-time service that depends mostly on events (alerts/reports) published in Kafka topics. In order to test the component individually some test endpoints have been created, aiming to simulate incoming traffic from the various components of the SPHINX Toolkit.

In order to deploy the DSS component in any system the following requirements should be met:

- Docker / docker-compose / kubectl and a K8S environment (eg. minikube) and kubectl
- Access to the internet
- Access to KT's container registry in Intracom's GitLab server
- Access to KT's repository in Intracom's GitLab server
- Git

2.2 Deployment using Docker

The easiest way to deploy the DSS component with docker is to clone the KT repository and use docker-compose:

- **git clone** https://sphinx-repo.intracom-telecom.com/sphinx-project/decision-support-system/sphinx_dss
- **cd sphinx_dss**
- **docker-compose up dss**

After running the above commands, the DSS API can be accessed on **<HOST IP>:3000.**

Note: If the KB component has been deployed the DSS will use it to either fetch external references related to the event being reported or search for courses of action in case an unknown event is reported. Make sure to set the value of the KB_IP in the .env file to the IP of the KB component.

2.3 Deployment using Kubernetes

The SPHINX DSS component can also be deployed in a Kubernetes cluster by applying the deployments in the **kubernetes/local** directory. The **kubernetes/local** directory contains a simplified version of the actual deployments that can be deployed with zero configuration.

2.3.1 Start a Kubernetes cluster

For the sake of simplicity, we are going to use **minikube** in this guide to quickly start a local single-node Kubernetes cluster. Feel free to skip this part if you already have a Kubernetes cluster running.

To start the Kubernetes cluster simply run:

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.

- **minikube start**

This will automatically configure the **kubectl** command-line tool to use the “minikube” cluster.

2.3.2 Create a Secret with the credentials for the container registry

First, create a Secret called **intracom-repository** with your credentials for the container registry. This will allow the Kubernetes cluster to authenticate with the container registry and pull the docker images.

You can create the secret by running the following command:

- **kubectl create secret docker-registry intracom-repository --docker-server=registry.sphinx-repo.intracom-telecom.com --docker-username=<your_username> --docker-password=<your_password> --docker-email=<your_email>**

Note: Replace **<your_username>** with your GitLab username, **<your_password>** with your GitLab password and **<your_email>** with your GitLab email address.

2.3.3 Start the DSS

Then, the DSS component can be started by executing the following commands:

- **git clone** https://sphinx-repo.intracom-telecom.com/sphinx-project/decision-support-system/sphinx_dss
- **cd sphinx_dss/kubernetes/local**
- **kubectl apply -f dss.yml**

Note: If the KB component has been deployed the DSS will use it to either fetch external references related to the event being reported or search for courses of action in case an unknown event is reported. The default value is set to http://sphinx-kb:4000 and will only work if the components are deployed in the same Kubernetes cluster. Otherwise, the value of KB_IP can be overwritten by adding an environment variable named KB_IP to the Kubernetes deployment file.

2.3.4 Access the DSS API service

You can now access the component on **<HOST IP>:3000** by running:

- **kubectl port-forward -d <pod_name> 3000:5000**

Alternatively, you can run:

- **minikube service sphinx-dss-service**

and access the component on the host port that will automatically be assigned to the sphinx-ae-service.

3 Basic Case Example

For this tutorial we have two case examples for the SPHINX DSS usage. These case examples should help familiarize the reader with the role of the SPHINX DSS. The user can use the “SPHINX KT” postman collection in order to go through the described cases and familiarize them with the component.

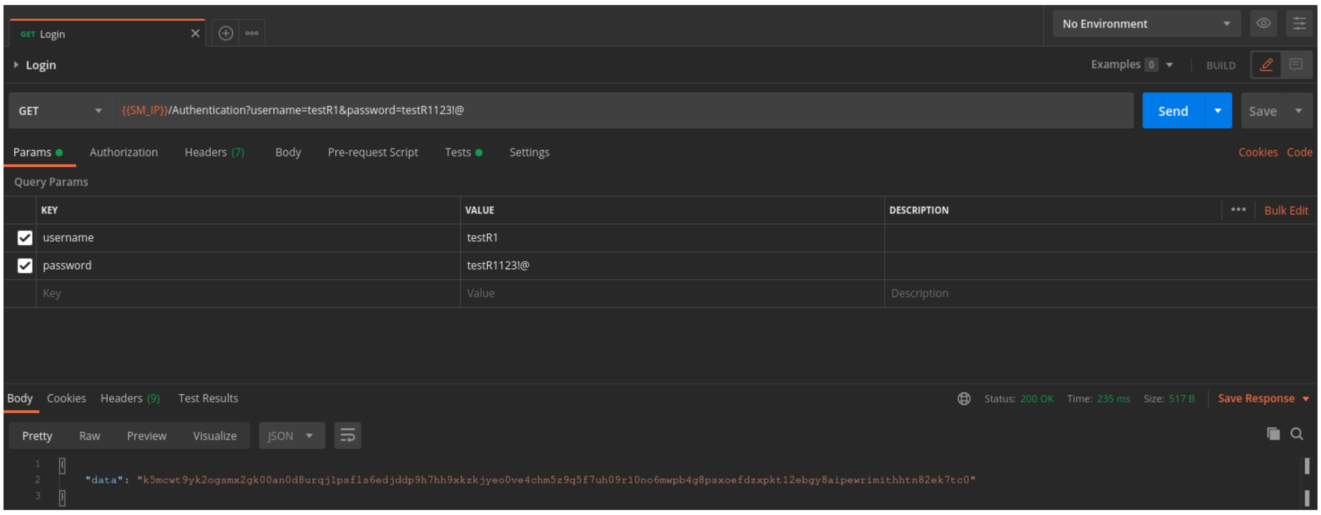
Note: The DSS is intended to be a real-time service that gets most of the data from Kafka and publishes action plans to the “**dss-suggestions**” topic. Even though the actor would only need to consume the topic in order to see the action plans (typically in the Interactive Dashboards) when there is an ongoing attack, we have created some test endpoints that simulate incoming data to test the functionality of the DSS individually.

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.

3.1 Setup

3.1.1 Login Authentication

First, the user should get a valid token from the Service Manager to authenticate their requests to the DSS API. This can be achieved by opening the "**Login**" request of the SPHINX KT postman collection and pressing "Send". This will automatically authenticate all the requests described below.



GET {{SM_IP}}/Authentication?username=testR1&password=testR1123!@

Query Params

KEY	VALUE	DESCRIPTION
username	testR1	
password	testR1123!@	

Status: 200 OK Time: 235 ms Size: 517 B

```
{
    "data": "k5mcwt9yk2ogsmx2gk00an0d8urqj1psfls6edjddp9h7hh9xkzkjyeo0ve4chm5z9q5f7uh09r10no6mwpb4g8psxoefdzxpkt12ebgy8aipewrimithhtn82ek7tc0"
}
```

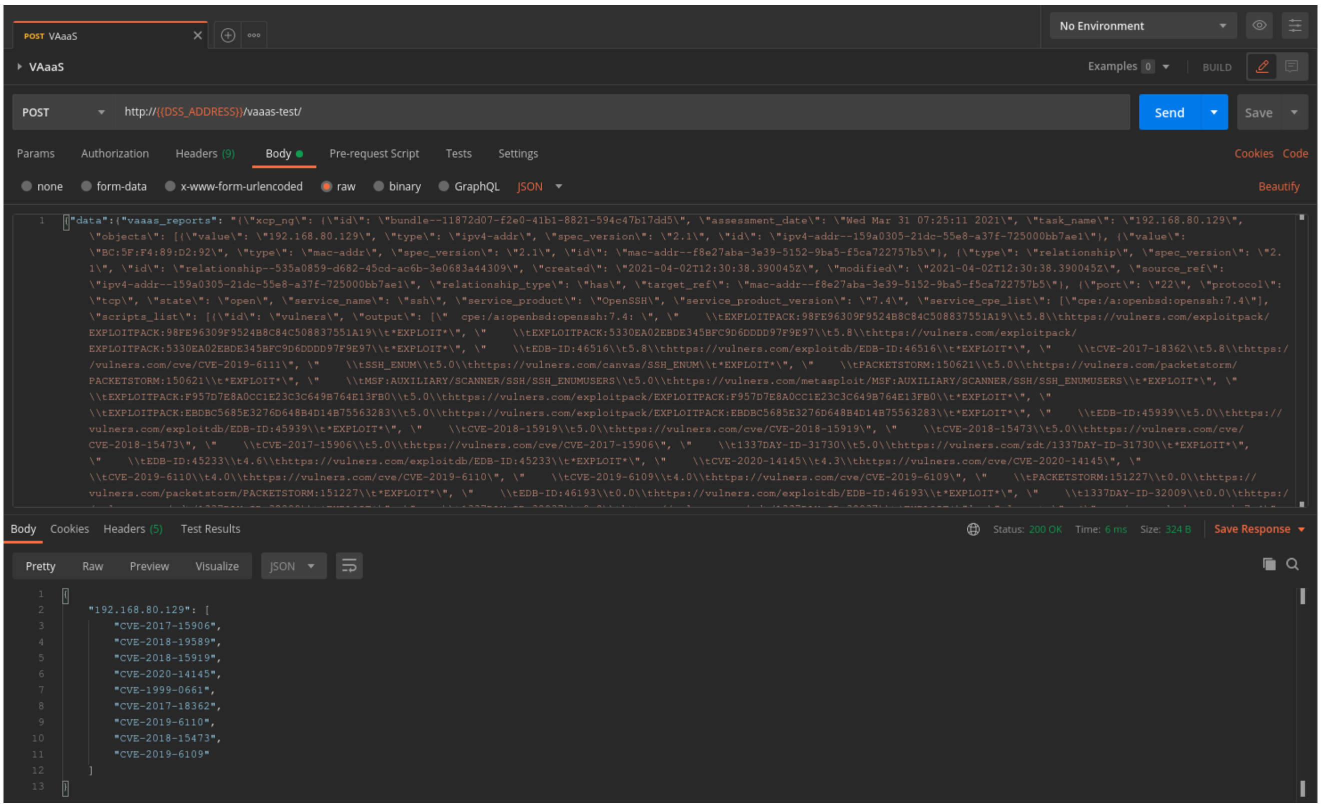
Figure 3.1 Login Request

3.1.2 VAaaS Data

The DSS stores the vulnerabilities per asset reported by the VAaaS component. Normally, this data would be consumed from the "**vaaas_reports**" topic.

In case the VAaaS component has not been deployed, the user can use the "**DSS/Test/VAaaS**" request in the SPHINX KT postman collection to simulate incoming VAaaS traffic and send some VAaaS reports to the DSS.

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.



POST http://{{DSS_ADDRESS}}/vaaas-test/

```
{"data":{"vaaas_reports": "{\"xcp_ng\": {\"id\": \"bundle--11872d07-f2e0-41b1-8821-594c47b17dd5\", \"assessment_date\": \"Wed Mar 31 07:25:11 2021\", \"task_name\": \"192.168.80.129\",
    \"objects\": [{\"value\": \"192.168.80.129\", \"type\": \"ipv4-addr\", \"spec_version\": \"2.1\", \"id\": \"ipv4-addr--159a0305-21dc-55e8-a37f-725000bb7ae1\"}, {\"value\":
    \"BC:5F:F4:89:D2:92\", \"type\": \"mac-addr\", \"spec_version\": \"2.1\", \"id\": \"mac-addr--f8e27aba-3e39-5152-9ba5-f5ca722757b5\"}, {\"type\": \"relationship\", \"spec_version\": \"2.
    1\", \"id\": \"relationship--535a0859-d682-45cd-ac6b-3e0683a44309\", \"created\": \"2021-04-02T12:30:38.390045Z\", \"modified\": \"2021-04-02T12:30:38.390045Z\", \"source_ref\":
    \"ipv4-addr--159a0305-21dc-55e8-a37f-725000bb7ae1\", \"relationship_type\": \"has\", \"target_ref\": \"mac-addr--f8e27aba-3e39-5152-9ba5-f5ca722757b5\"}, {\"port\": \"22\", \"protocol\":
    \"tcp\", \"state\": \"open\", \"service_name\": \"ssh\", \"service_product\": \"OpenSSH\", \"service_product_version\": \"7.4\", \"service_cpe_list\": [\"cpe:/a:openbsd:openssh:7.4\"],
    \"scripts_list\": [{\"id\": \"vulners\", \"output\": [\"  cpe:/a:openbsd:openssh:7.4: \", \"    \\tEXPLOITPACK:98FE96309F9524B8C84C508837551A19\\t5.8\\thttps://vulners.com/exploitpack/
    EXPLOITPACK:98FE96309F9524B8C84C508837551A19\\t*EXPLOIT*\", \"    \\tEXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97\\t5.8\\thttps://vulners.com/exploitpack/
    EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97\\t*EXPLOIT*\", \"    \\tEDB-ID:46516\\t5.8\\thttps://vulners.com/exploitdb/EDB-ID:46516\\t*EXPLOIT*\", \"    \\tCVE-2017-18362\\t5.8\\thttps:/
    /vulners.com/cve/CVE-2019-6111\", \"    \\tSSH_ENUM\\t5.0\\thttps://vulners.com/canvas/SSH_ENUM\\t*EXPLOIT*\", \"    \\tPACKETSTORM:150621\\t5.0\\thttps://vulners.com/packetstorm/
    PACKETSTORM:150621\\t*EXPLOIT*\", \"    \\tMSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS\\t5.0\\thttps://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS\\t*EXPLOIT*\", \"
    \\tEXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0\\t5.0\\thttps://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0\\t*EXPLOIT*\", \"
    \\tEXPLOITPACK:EBDBC5685E3276D648B4D14B75563283\\t5.0\\thttps://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283\\t*EXPLOIT*\", \"    \\tEDB-ID:45939\\t5.0\\thttps://
    vulners.com/exploitdb/EDB-ID:45939\\t*EXPLOIT*\", \"    \\tCVE-2018-15919\\t5.0\\thttps://vulners.com/cve/CVE-2018-15919\", \"    \\tCVE-2018-15473\\t5.0\\thttps://vulners.com/cve/
    CVE-2018-15473\", \"    \\tCVE-2017-15906\\t5.0\\thttps://vulners.com/cve/CVE-2017-15906\", \"    \\t1337DAY-ID-31730\\t5.0\\thttps://vulners.com/zdt/1337DAY-ID-31730\\t*EXPLOIT*\",
    \"    \\tEDB-ID:45233\\t4.6\\thttps://vulners.com/exploitdb/EDB-ID:45233\\t*EXPLOIT*\", \"    \\tCVE-2020-14145\\t4.3\\thttps://vulners.com/cve/CVE-2020-14145\", \"
    \\tCVE-2019-6110\\t4.0\\thttps://vulners.com/cve/CVE-2019-6110\", \"    \\tCVE-2019-6109\\t4.0\\thttps://vulners.com/cve/CVE-2019-6109\", \"    \\tPACKETSTORM:151227\\t0.0\\thttps://
    vulners.com/packetstorm/PACKETSTORM:151227\\t*EXPLOIT*\", \"    \\tEDB-ID:46193\\t0.0\\thttps://vulners.com/exploitdb/EDB-ID:46193\\t*EXPLOIT*\", \"    \\t1337DAY-ID-32009\\t0.0\\thttps:/
```

Status: 200 OK Time: 6 ms Size: 324 B

```
{
    "192.168.80.129": [
        "CVE-2017-15906",
        "CVE-2018-19589",
        "CVE-2018-15919",
        "CVE-2020-14145",
        "CVE-1999-0661",
        "CVE-2017-18362",
        "CVE-2019-6110",
        "CVE-2018-15473",
        "CVE-2019-6109"
    ]
}
```

Figure 3.2 Data for VAaaS Endpoint

3.2 Case Example 1

In this example we'll send sample DTM traffic to the DSS using the "**DSS/Test/DTM**" request in the SPHINX KT postman collection to demonstrate the behaviour of the DSS.

3.2.1 Actor for the case

The actor is the Security Expert/IT of the hospital that sees the DSS action plans in the Interactive Dashboards.

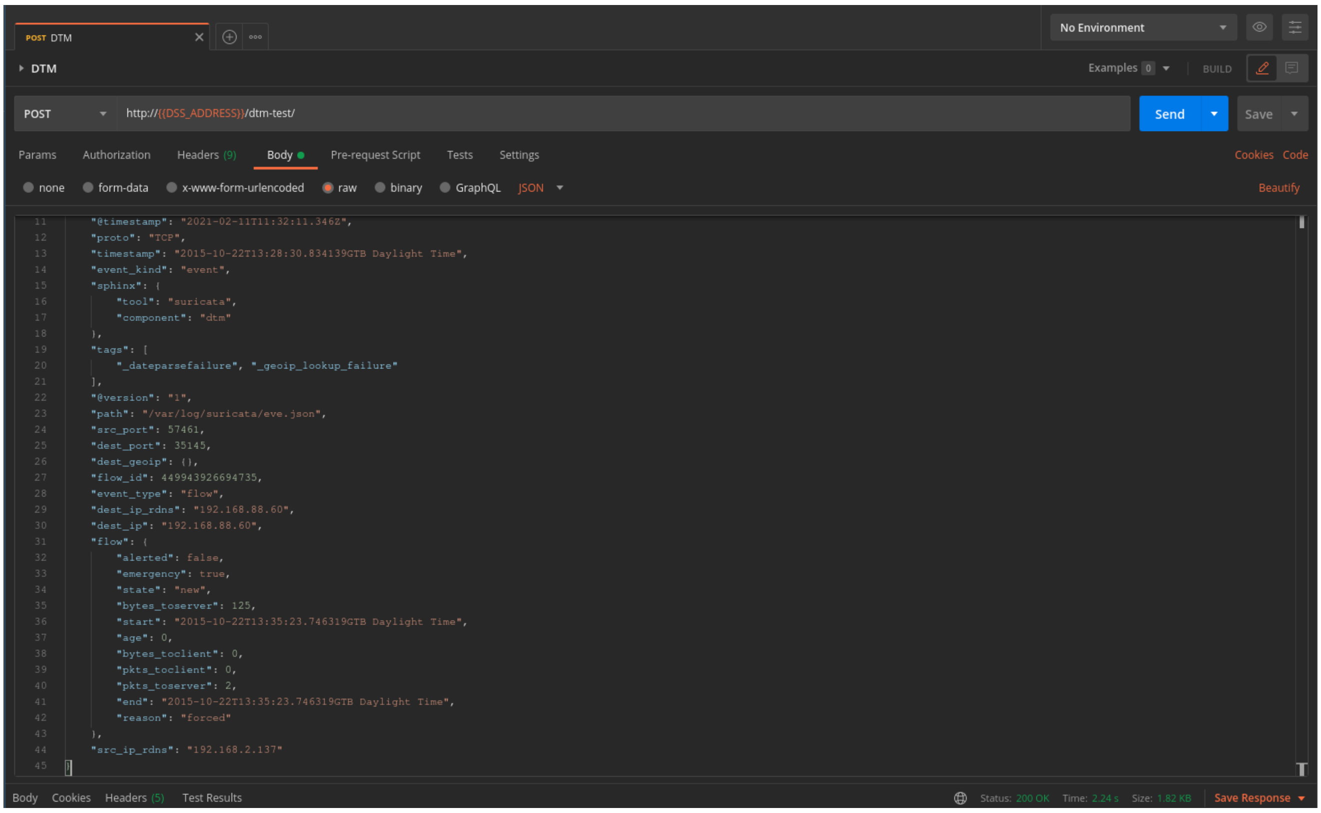
3.2.2 Instructions

The actor sees the action plans published in the "**dss-suggestions**" topic in the respective screen of the Interactive Dashboards.

3.2.3 Expected Outcome

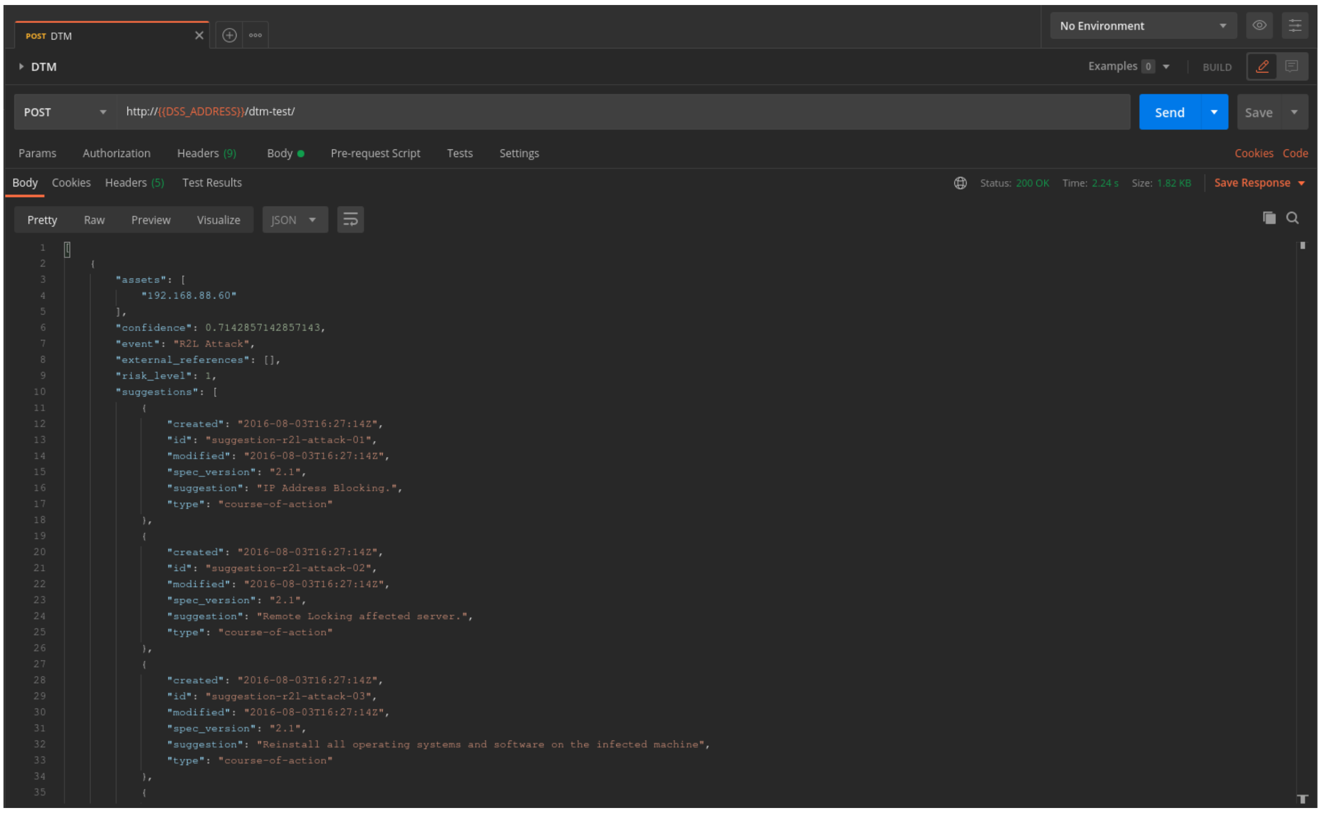
The DTM sends captured traffic data to the DSS through the "**dtm-event**" topic. The DSS analyses the last 5 received DTM events using machine learning and predicts imminent DoS or Probe attacks (Pro-active functionality). If the traffic is identified as normal a second ML model predicts whether there is an ongoing R2L or U2R attack based on the last DTM event (Active functionality).

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.



```
    "@timestamp": "2021-02-11T11:32:11.346Z",
    "proto": "TCP",
    "timestamp": "2015-10-22T13:28:30.834139GTB Daylight Time",
    "event_kind": "event",
    "sphinx": {
        "tool": "suricata",
        "component": "dtm"
    },
    "tags": [
        "_dateparsefailure", "_geoip_lookup_failure"
    ],
    "@version": "1",
    "path": "/var/log/suricata/eve.json",
    "src_port": 57461,
    "dest_port": 35145,
    "dest_geoip": {},
    "flow_id": 449943926694735,
    "event_type": "flow",
    "dest_ip_rdns": "192.168.88.60",
    "dest_ip": "192.168.88.60",
    "flow": {
        "alerted": false,
        "emergency": true,
        "state": "new",
        "bytes_toserver": 125,
        "start": "2015-10-22T13:35:23.746319GTB Daylight Time",
        "age": 0,
        "bytes_toclient": 0,
        "pkts_toclient": 0,
        "pkts_toserver": 2,
        "end": "2015-10-22T13:35:23.746319GTB Daylight Time",
        "reason": "forced"
    },
    "src_ip_rdns": "192.168.2.137"
}
```

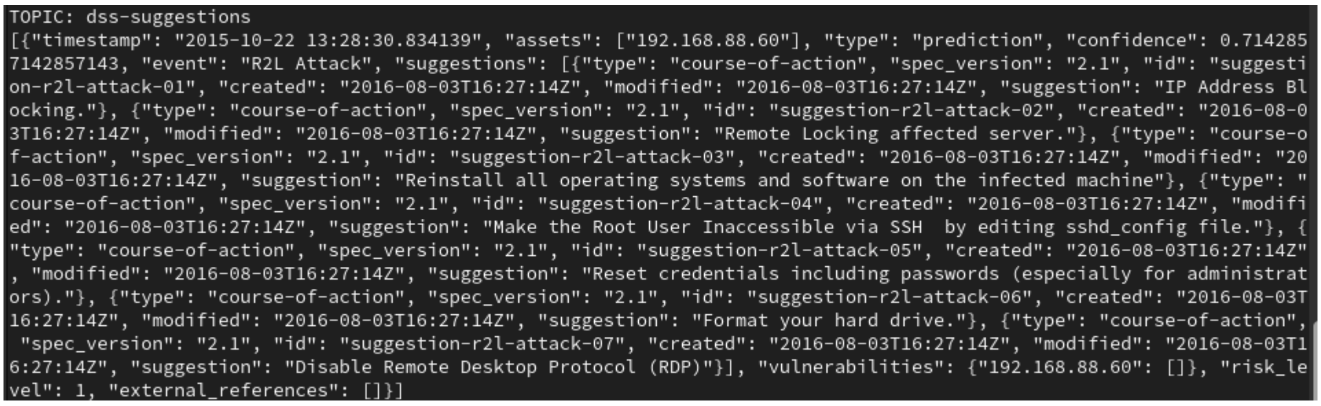
Figure 3.3 Data for DTM Endpoint



```
[
    {
        "assets": [
            "192.168.88.60"
        ],
        "confidence": 0.7142857142857143,
        "event": "R2L Attack",
        "external_references": [],
        "risk_level": 1,
        "suggestions": [
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-r2l-attack-01",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": "IP Address Blocking.",
                "type": "course-of-action"
            },
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-r2l-attack-02",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": "Remote Locking affected server.",
                "type": "course-of-action"
            },
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-r2l-attack-03",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": "Reinstall all operating systems and software on the infected machine",
                "type": "course-of-action"
            },
            {
```

Figure 3.4 Prediction from DTM Data

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.



```
TOPIC: dss-suggestions
[{"timestamp": "2015-10-22 13:28:30.834139", "assets": ["192.168.88.60"], "type": "prediction", "confidence": 0.714285
7142857143, "event": "R2L Attack", "suggestions": [{"type": "course-of-action", "spec_version": "2.1", "id": "suggesti
on-r2l-attack-01", "created": "2016-08-03T16:27:14Z", "modified": "2016-08-03T16:27:14Z", "suggestion": "IP Address Bl
ocking."}, {"type": "course-of-action", "spec_version": "2.1", "id": "suggestion-r2l-attack-02", "created": "2016-08-0
3T16:27:14Z", "modified": "2016-08-03T16:27:14Z", "suggestion": "Remote Locking affected server."}, {"type": "course-o
f-action", "spec_version": "2.1", "id": "suggestion-r2l-attack-03", "created": "2016-08-03T16:27:14Z", "modified": "20
16-08-03T16:27:14Z", "suggestion": "Reinstall all operating systems and software on the infected machine"}, {"type": "
course-of-action", "spec_version": "2.1", "id": "suggestion-r2l-attack-04", "created": "2016-08-03T16:27:14Z", "modifi
ed": "2016-08-03T16:27:14Z", "suggestion": "Make the Root User Inaccessible via SSH  by editing sshd_config file."}, {
"type": "course-of-action", "spec_version": "2.1", "id": "suggestion-r2l-attack-05", "created": "2016-08-03T16:27:14Z"
, "modified": "2016-08-03T16:27:14Z", "suggestion": "Reset credentials including passwords (especially for administrat
ors)."}, {"type": "course-of-action", "spec_version": "2.1", "id": "suggestion-r2l-attack-06", "created": "2016-08-03T
16:27:14Z", "modified": "2016-08-03T16:27:14Z", "suggestion": "Format your hard drive."}, {"type": "course-of-action",
 "spec_version": "2.1", "id": "suggestion-r2l-attack-07", "created": "2016-08-03T16:27:14Z", "modified": "2016-08-03T1
6:27:14Z", "suggestion": "Disable Remote Desktop Protocol (RDP)"}], "vulnerabilities": {"192.168.88.60": []}, "risk_le
vel": 1, "external_references": []}]
```

Figure 3.5 Kafka Topic with DSS suggestions

The generated **action plan** contains the following information:

- "**assets**" is a list containing the IPs of the affected assets eg. ["192.168.88.60", "192.168.80.129"]
- "**confidence**" is the level of confidence for the given report (how reliable the report is) eg. 0.5
- "**event**" is the name of the reported event (usually the name of an attack) eg. "Ransomware"
- "**external_references**" is a list containing external references (CWE/CAPEC) fetched from the KB that are related with the specified event
- "**risk_level**" is the risk level reported by the RCRA eg. 1.0
- "**suggestions**" is the list containing the courses of action to be performed by the end user.
- "**timestamp**" is the time when the attack was predicted/identified. eg. "2021-03-04 17:55:00.092000"
- "**type**" has two possible values. "prediction" and "reaction" (In this case it is a **prediction**)
- "**prediction**" indicates that the DSS predicted the attack being reported
- "**reaction**" indicates that the DSS reacted to an alert raised by another component of the SPHINX toolkit
- "**vulnerabilities**" is a list containing reported vulnerabilities for each affected asset (extracted from the latest VAaaS reports) that are related to the attack being reported

3.3 Case Example 2

In this example we'll send sample SIEM alerts to the DSS using the "**DSS/Test/SIEM**" request in the SPHINX KT postman collection to demonstrate the behaviour of the DSS.

3.3.1 Actor for the case

The actor is the Security Expert/IT of the hospital that sees the DSS action plans in the Interactive Dashboards.

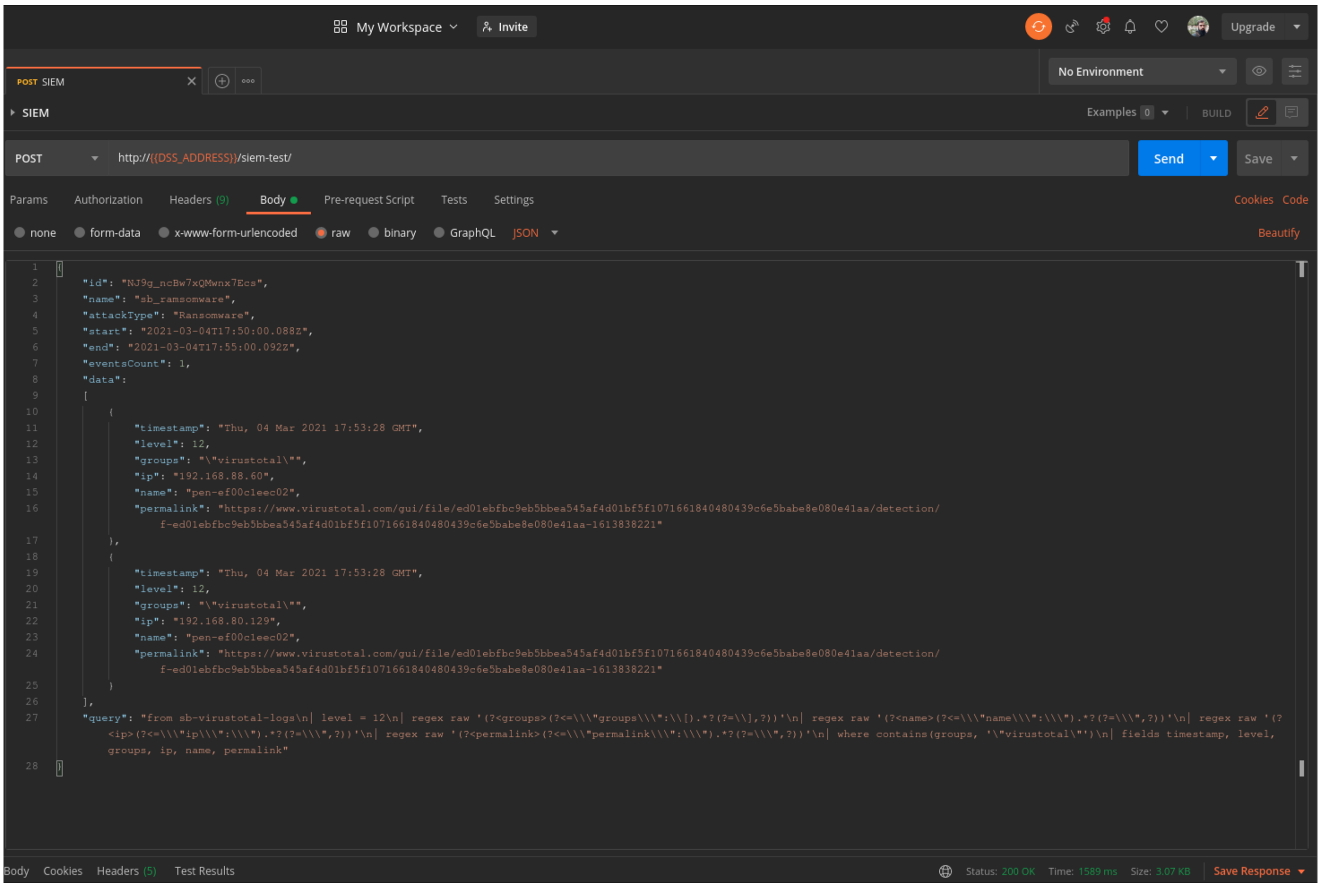
3.3.2 Instructions

The actor sees the action plans published in the "**dss-suggestions**" topic in the respective screen of the Interactive Dashboards.

3.3.3 Expected outcome

The SIEM raises an alert and the DSS consumes it from the "**siem-alert**" topic. The DSS provides an action plan based on the reported attack type. The DSS also correlates previously reported vulnerabilities with the specific attack and fetches external attack references from the KB component in order to provide a detailed and self-contained report to the end user.

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.

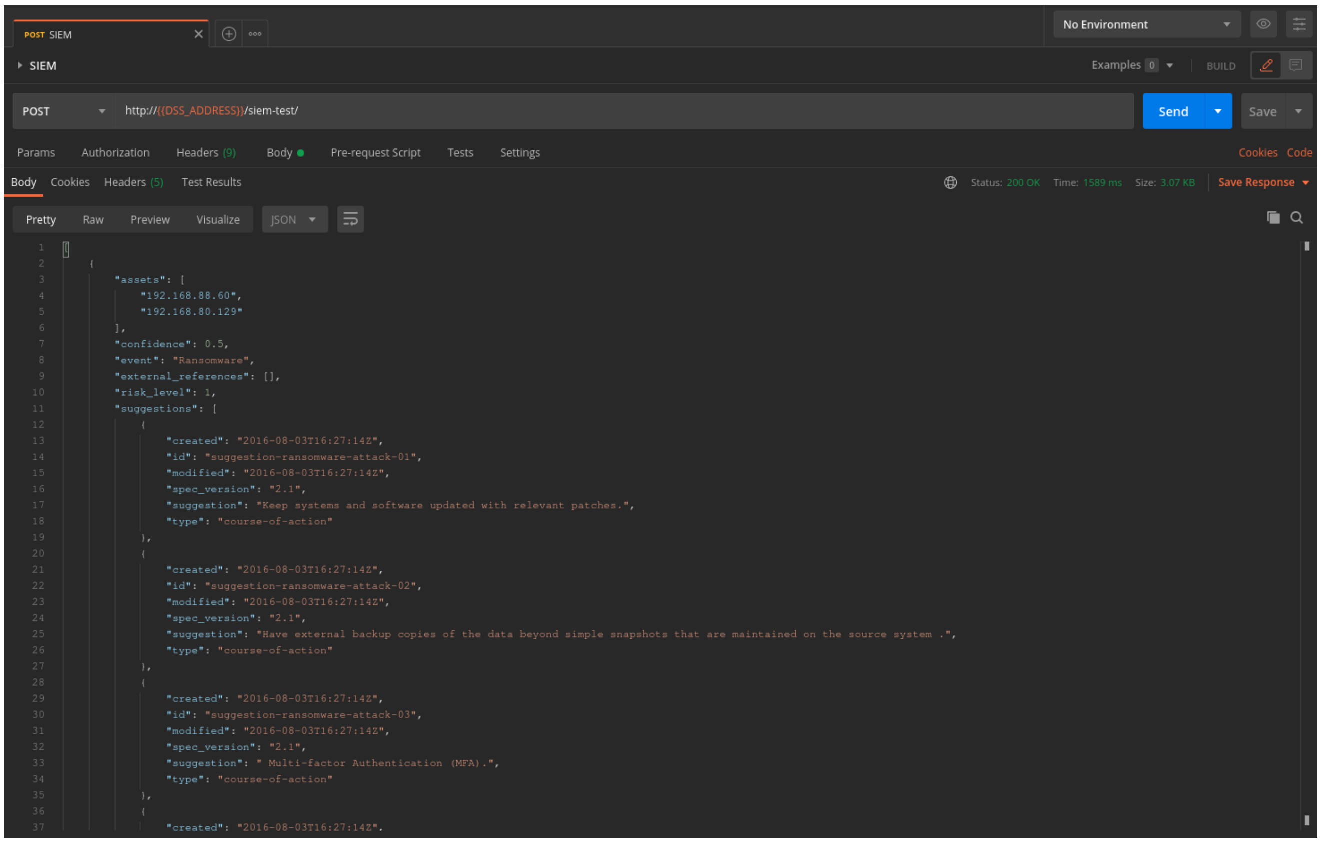


```
POST http://{{DSS_ADDRESS}}/siem-test/
```

```
{
    "id": "NJ9g_ncBw7xQMwnx7Ecs",
    "name": "sb_ramsomware",
    "attackType": "Ransomware",
    "start": "2021-03-04T17:50:00.088Z",
    "end": "2021-03-04T17:55:00.092Z",
    "eventsCount": 1,
    "data":
    [
        {
            "timestamp": "Thu, 04 Mar 2021 17:53:28 GMT",
            "level": 12,
            "groups": "\"virustotal\"",
            "ip": "192.168.88.60",
            "name": "pen-ef00c1eec02",
            "permalink": "https://www.virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/detection/
                f-ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa-1613838221"
        },
        {
            "timestamp": "Thu, 04 Mar 2021 17:53:28 GMT",
            "level": 12,
            "groups": "\"virustotal\"",
            "ip": "192.168.80.129",
            "name": "pen-ef00c1eec02",
            "permalink": "https://www.virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/detection/
                f-ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa-1613838221"
        }
    ],
    "query": "from sb-virustotal-logs\n| level = 12\n| regex raw '(?<groups>(?<=\\\"groups\\\":\\[).*?(?=\\],?))'\n| regex raw '(?<name>(?<=\\\"name\\\":\\\").*?(?=\\\",?))'\n| regex raw '(?
        <ip>(?<=\\\"ip\\\":\\\").*?(?=\\\",?))'\n| regex raw '(?<permalink>(?<=\\\"permalink\\\":\\\").*?(?=\\\",?))'\n| where contains(groups, '\"virustotal\"')\n| fields timestamp, level,
        groups, ip, name, permalink"
}
```

```
Status: 200 OK   Time: 1589 ms   Size: 3.07 KB
```

Figure 3.6 SIEM Data

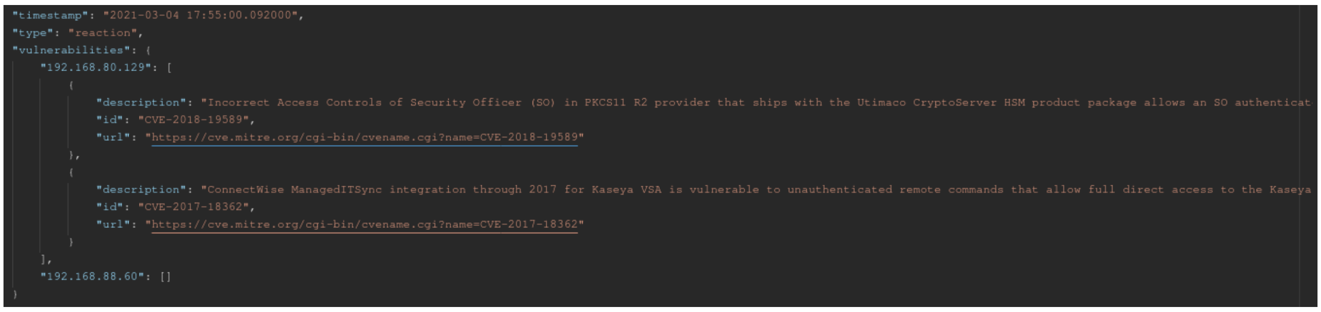


```
POST http://{{DSS_ADDRESS}}/siem-test/
Status: 200 OK   Time: 1589 ms   Size: 3.07 KB
```

```
[
    {
        "assets": [
            "192.168.88.60",
            "192.168.80.129"
        ],
        "confidence": 0.5,
        "event": "Ransomware",
        "external_references": [],
        "risk_level": 1,
        "suggestions": [
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-ransomware-attack-01",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": "Keep systems and software updated with relevant patches.",
                "type": "course-of-action"
            },
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-ransomware-attack-02",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": "Have external backup copies of the data beyond simple snapshots that are maintained on the source system .",
                "type": "course-of-action"
            },
            {
                "created": "2016-08-03T16:27:14Z",
                "id": "suggestion-ransomware-attack-03",
                "modified": "2016-08-03T16:27:14Z",
                "spec_version": "2.1",
                "suggestion": " Multi-factor Authentication (MFA).",
                "type": "course-of-action"
            },
            {
                "created": "2016-08-03T16:27:14Z".
```

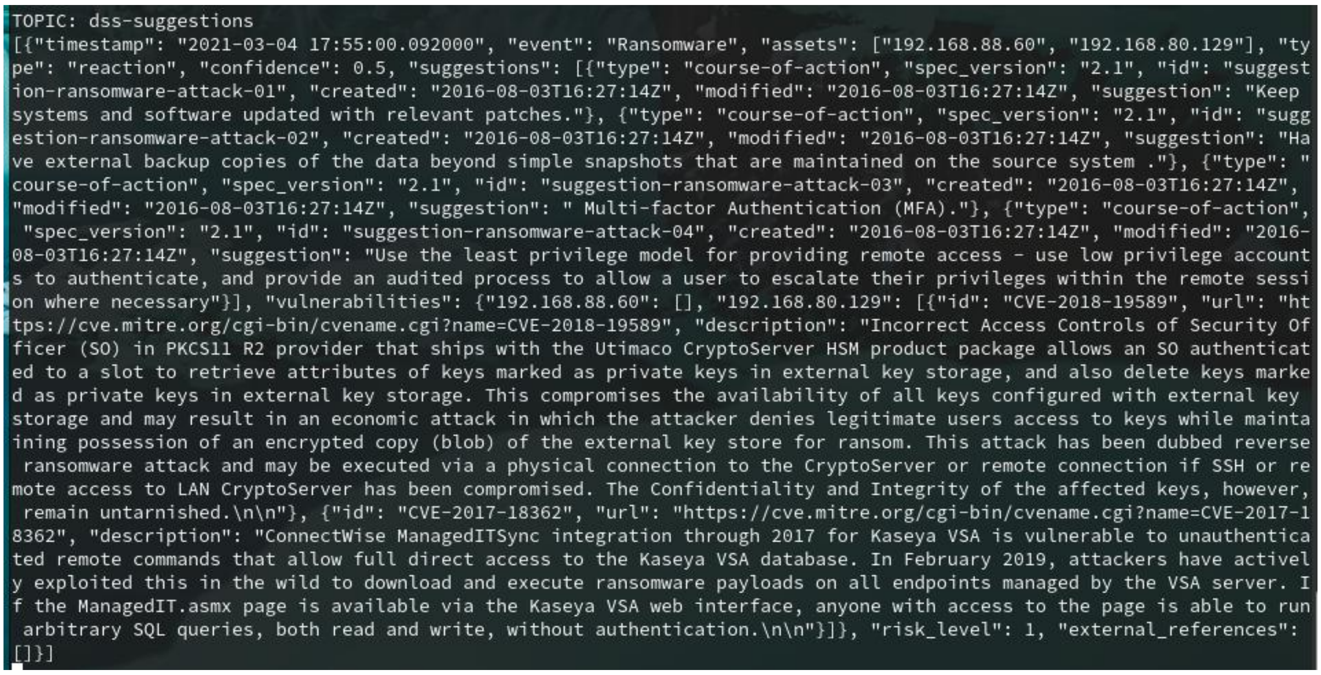
Figure 3.7 DSS Suggestions

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.



```
"timestamp": "2021-03-04 17:55:00.092000",
"type": "reaction",
"vulnerabilities": {
    "192.168.80.129": [
        {
            "description": "Incorrect Access Controls of Security Officer (SO) in PKCS11 R2 provider that ships with the Utimaco CryptoServer HSM product package allows an SO authenticat
            "id": "CVE-2018-19589",
            "url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19589"
        },
        {
            "description": "ConnectWise ManagedITSync integration through 2017 for Kaseya VSA is vulnerable to unauthenticated remote commands that allow full direct access to the Kaseya
            "id": "CVE-2017-18362",
            "url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18362"
        }
    ],
    "192.168.88.60": []
}
```

Figure 3.8 DSS suggestions continued



```
TOPIC: dss-suggestions
[{"timestamp": "2021-03-04 17:55:00.092000", "event": "Ransomware", "assets": ["192.168.88.60", "192.168.80.129"], "ty
pe": "reaction", "confidence": 0.5, "suggestions": [{"type": "course-of-action", "spec_version": "2.1", "id": "suggest
ion-ransomware-attack-01", "created": "2016-08-03T16:27:14Z", "modified": "2016-08-03T16:27:14Z", "suggestion": "Keep
systems and software updated with relevant patches."}, {"type": "course-of-action", "spec_version": "2.1", "id": "sugg
estion-ransomware-attack-02", "created": "2016-08-03T16:27:14Z", "modified": "2016-08-03T16:27:14Z", "suggestion": "Ha
ve external backup copies of the data beyond simple snapshots that are maintained on the source system ."}, {"type": "
course-of-action", "spec_version": "2.1", "id": "suggestion-ransomware-attack-03", "created": "2016-08-03T16:27:14Z",
"modified": "2016-08-03T16:27:14Z", "suggestion": " Multi-factor Authentication (MFA)."}, {"type": "course-of-action",
 "spec_version": "2.1", "id": "suggestion-ransomware-attack-04", "created": "2016-08-03T16:27:14Z", "modified": "2016-
08-03T16:27:14Z", "suggestion": "Use the least privilege model for providing remote access - use low privilege account
s to authenticate, and provide an audited process to allow a user to escalate their privileges within the remote sessi
on where necessary"}], "vulnerabilities": {"192.168.88.60": [], "192.168.80.129": [{"id": "CVE-2018-19589", "url": "ht
tps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19589", "description": "Incorrect Access Controls of Security Of
ficer (SO) in PKCS11 R2 provider that ships with the Utimaco CryptoServer HSM product package allows an SO authenticat
ed to a slot to retrieve attributes of keys marked as private keys in external key storage, and also delete keys marke
d as private keys in external key storage. This compromises the availability of all keys configured with external key
storage and may result in an economic attack in which the attacker denies legitimate users access to keys while mainta
ining possession of an encrypted copy (blob) of the external key store for ransom. This attack has been dubbed reverse
 ransomware attack and may be executed via a physical connection to the CryptoServer or remote connection if SSH or re
mote access to LAN CryptoServer has been compromised. The Confidentiality and Integrity of the affected keys, however,
 remain untarnished.\n\n"}, {"id": "CVE-2017-18362", "url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1
8362", "description": "ConnectWise ManagedITSync integration through 2017 for Kaseya VSA is vulnerable to unauthentica
ted remote commands that allow full direct access to the Kaseya VSA database. In February 2019, attackers have activel
y exploited this in the wild to download and execute ransomware payloads on all endpoints managed by the VSA server. I
f the ManagedIT.asmx page is available via the Kaseya VSA web interface, anyone with access to the page is able to run
 arbitrary SQL queries, both read and write, without authentication.\n\n"}]}, "risk_level": 1, "external_references":
[]}]
```

Figure 3.9 Kafka Topic for DSS suggestions

The generated **action plan** contains the same information as the previous case.

In this case the type is a “**reaction**” and some of the previously reported VAaaS vulnerabilities were correlated with the attack and included in the final report.

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.