Machine Learning-empowered Intrusion Detection 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

The MLID component and the HP component function together. It's basically a decision-making instrument that works from the information gathered by HP. Via the SM, the MILD accepts requests from the HP. When a request has been received by the HP, the MLID component extracts the ticket from the header of the HTTP request and authenticates it by contacting the SM. After the ticket has been accepted, the MLID component examines the JSON file for potential attacker activity parameters and makes a decision (by employing a trained ML algorithm). This decision is then incorporated as an extra part of the structure in the received JSON file, and the modified file is sent back to HP.

2 Installation requirements

The SPHINX AI MLID components are installed using Docker files, which can be used to deploy the AI MLID in any device that meets the following requirements:

- Git
- Docker and Docker-Compose
- Root Access
- Access to the Internet
- Access to Intracom's GitLab Server

3 Prerequisites and hardware

- CPU: medium CPU like Intel I7
- GPU: no needed
- RAM: medium Ram like 16 GB RAM
- HDD: for WEB backend server binary files have small size

4 Deployment inside the Kubernetes cluster

First and foremost, you must have access to the ICOM image repository.

Using the deployment file, we can create an MLID pod, with the following command:

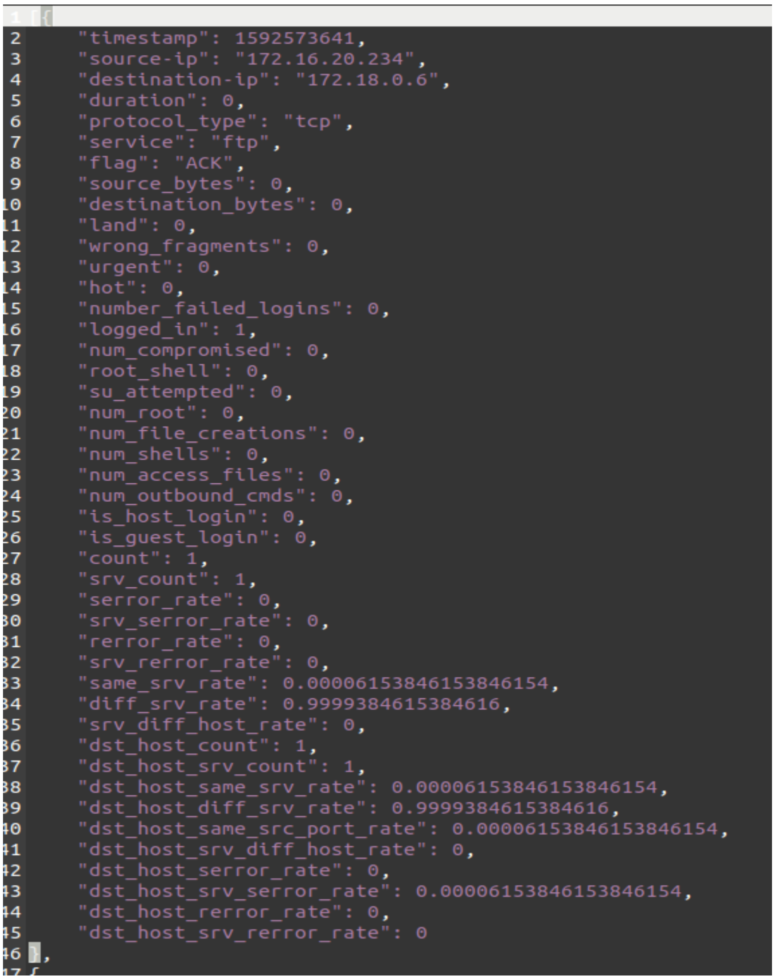
```
-kubectl apply -f Deployment.yaml
```

5 Basic Case Examples

Now, we present here a case example for the MLID usage. Two RestFul endpoints were introduced and reviewed as part of the HP and MLID integration. The first uses the HTTP POST method to send the most recent produced from the Honeypot NLVD datasets (see **Figure 1**) to the MLID component and receive the

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.

dataset's decisions, whereas the second uses the HTTP GET method to allow the MLID to request the NLVD dataset at its leisure and using several filtering criteria such as service name and time period. The integration tests were carried out by deploying the component's docker images locally and then exchanging data via the required REST endpoints.



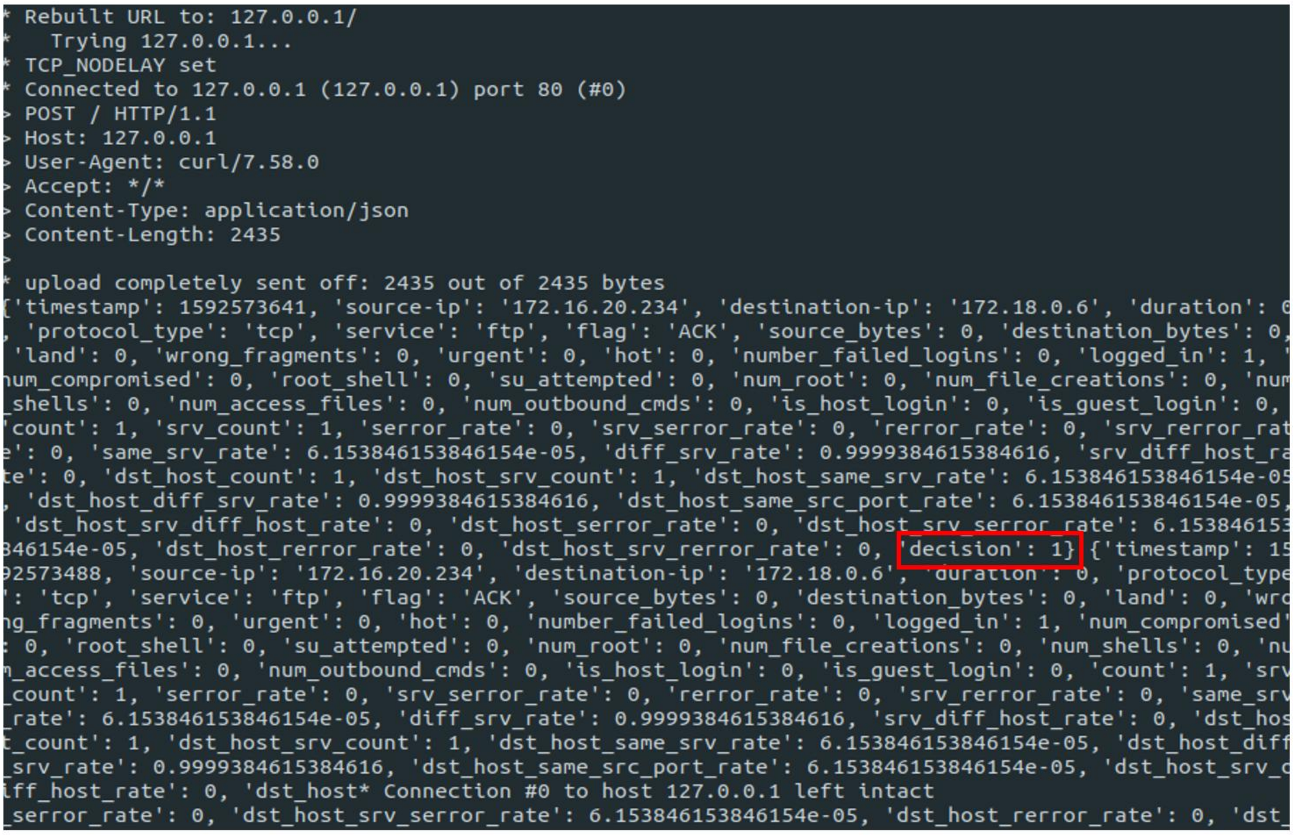
```
[{
    "timestamp": 1592573641,
    "source-ip": "172.16.20.234",
    "destination-ip": "172.18.0.6",
    "duration": 0,
    "protocol_type": "tcp",
    "service": "ftp",
    "flag": "ACK",
    "source_bytes": 0,
    "destination_bytes": 0,
    "land": 0,
    "wrong_fragments": 0,
    "urgent": 0,
    "hot": 0,
    "number_failed_logins": 0,
    "logged_in": 1,
    "num_compromised": 0,
    "root_shell": 0,
    "su_attempted": 0,
    "num_root": 0,
    "num_file_creations": 0,
    "num_shells": 0,
    "num_access_files": 0,
    "num_outbound_cmds": 0,
    "is_host_login": 0,
    "is_guest_login": 0,
    "count": 1,
    "srv_count": 1,
    "serror_rate": 0,
    "srv_serror_rate": 0,
    "rerror_rate": 0,
    "srv_rerror_rate": 0,
    "same_srv_rate": 0.000061538461538461540,
    "diff_srv_rate": 0.9999384615384616,
    "srv_diff_host_rate": 0,
    "dst_host_count": 1,
    "dst_host_srv_count": 1,
    "dst_host_same_srv_rate": 0.000061538461538461540,
    "dst_host_diff_srv_rate": 0.9999384615384616,
    "dst_host_same_src_port_rate": 0.000061538461538461540,
    "dst_host_srv_diff_host_rate": 0,
    "dst_host_serror_rate": 0,
    "dst_host_srv_serror_rate": 0.000061538461538461540,
    "dst_host_rerror_rate": 0,
    "dst_host_srv_rerror_rate": 0
},
{
```

Figure 1 The structure of the JSON file that is posted from the HP to the MLID component

6 Outcomes

In **Figure 2** we could see an example of MLID response to HP. MLID adds the response of the service in json file and returns it to HP. If the ticket is not authorized the response which MLID returns is “This service is not authorized”.

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.



```
* Rebuilt URL to: 127.0.0.1/
*   Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to 127.0.0.1 (127.0.0.1) port 80 (#0)
> POST / HTTP/1.1
> Host: 127.0.0.1
> User-Agent: curl/7.58.0
> Accept: */*
> Content-Type: application/json
> Content-Length: 2435
>
* upload completely sent off: 2435 out of 2435 bytes
{'timestamp': 1592573641, 'source-ip': '172.16.20.234', 'destination-ip': '172.18.0.6', 'duration': 0
, 'protocol_type': 'tcp', 'service': 'ftp', 'flag': 'ACK', 'source_bytes': 0, 'destination_bytes': 0,
 'land': 0, 'wrong_fragments': 0, 'urgent': 0, 'hot': 0, 'number_failed_logins': 0, 'logged_in': 1, '
num_compromised': 0, 'root_shell': 0, 'su_attempted': 0, 'num_root': 0, 'num_file_creations': 0, 'num
_shells': 0, 'num_access_files': 0, 'num_outbound_cmds': 0, 'is_host_login': 0, 'is_guest_login': 0,
'count': 1, 'srv_count': 1, 'serror_rate': 0, 'srv_serror_rate': 0, 'rerror_rate': 0, 'srv_rerror_rat
e': 0, 'same_srv_rate': 6.153846153846154e-05, 'diff_srv_rate': 0.9999384615384616, 'srv_diff_host_ra
te': 0, 'dst_host_count': 1, 'dst_host_srv_count': 1, 'dst_host_same_srv_rate': 6.153846153846154e-05
, 'dst_host_diff_srv_rate': 0.9999384615384616, 'dst_host_same_src_port_rate': 6.153846153846154e-05,
 'dst_host_srv_diff_host_rate': 0, 'dst_host_serror_rate': 0, 'dst_host_srv_serror_rate': 6.153846153
846154e-05, 'dst_host_rerror_rate': 0, 'dst_host_srv_rerror_rate': 0, 'decision': 1} {'timestamp': 15
92573488, 'source-ip': '172.16.20.234', 'destination-ip': '172.18.0.6', 'duration': 0, 'protocol_type
': 'tcp', 'service': 'ftp', 'flag': 'ACK', 'source_bytes': 0, 'destination_bytes': 0, 'land': 0, 'wro
ng_fragments': 0, 'urgent': 0, 'hot': 0, 'number_failed_logins': 0, 'logged_in': 1, 'num_compromised'
: 0, 'root_shell': 0, 'su_attempted': 0, 'num_root': 0, 'num_file_creations': 0, 'num_shells': 0, 'nu
m_access_files': 0, 'num_outbound_cmds': 0, 'is_host_login': 0, 'is_guest_login': 0, 'count': 1, 'srv
_count': 1, 'serror_rate': 0, 'srv_serror_rate': 0, 'rerror_rate': 0, 'srv_rerror_rate': 0, 'same_srv
_rate': 6.153846153846154e-05, 'diff_srv_rate': 0.9999384615384616, 'srv_diff_host_rate': 0, 'dst_hos
t_count': 1, 'dst_host_srv_count': 1, 'dst_host_same_srv_rate': 6.153846153846154e-05, 'dst_host_diff
_srv_rate': 0.9999384615384616, 'dst_host_same_src_port_rate': 6.153846153846154e-05, 'dst_host_srv_d
iff_host_rate': 0, 'dst_host* Connection #0 to host 127.0.0.1 left intact
_serror_rate': 0, 'dst_host_srv_serror_rate': 6.153846153846154e-05, 'dst_host_rerror_rate': 0, 'dst_
```

Figure 2 HP Posts data to MLID that responds by adding the ML decision into the updated JSON file

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.