Project 3 Report Part 3

IoT Security Monitoring with Suricata and Kibana

Group 8

Fozeya-Nikka Alviar

Angeline Nicole Faina

Sam Omandam

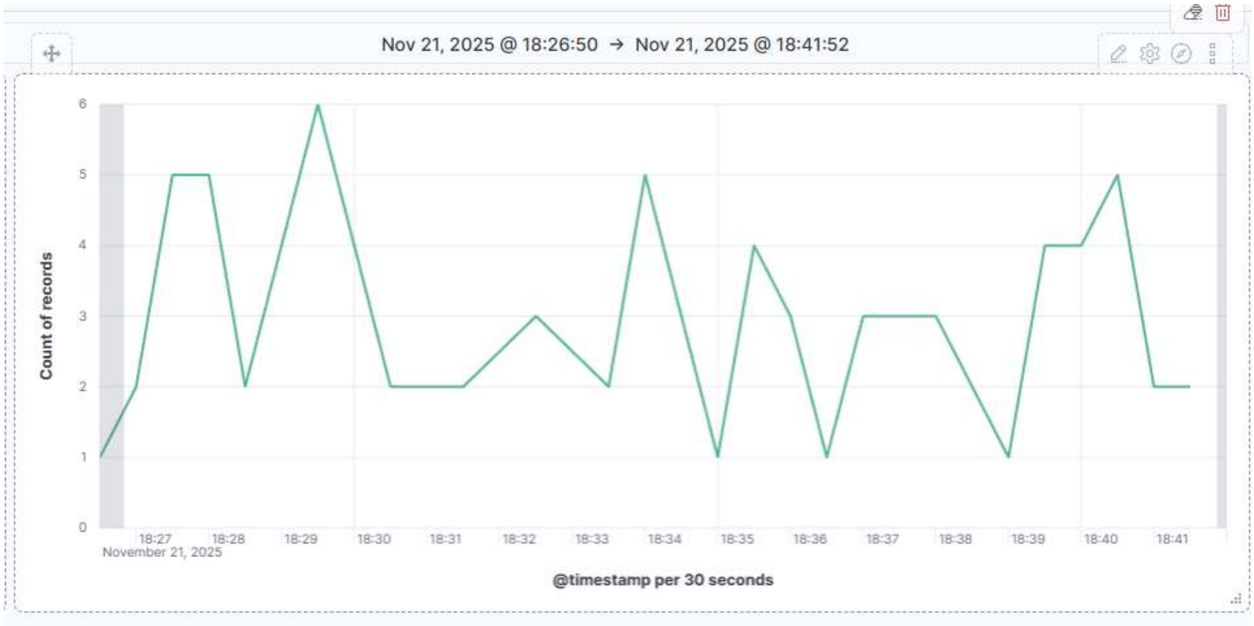
CYT160NBB

21 November 2025

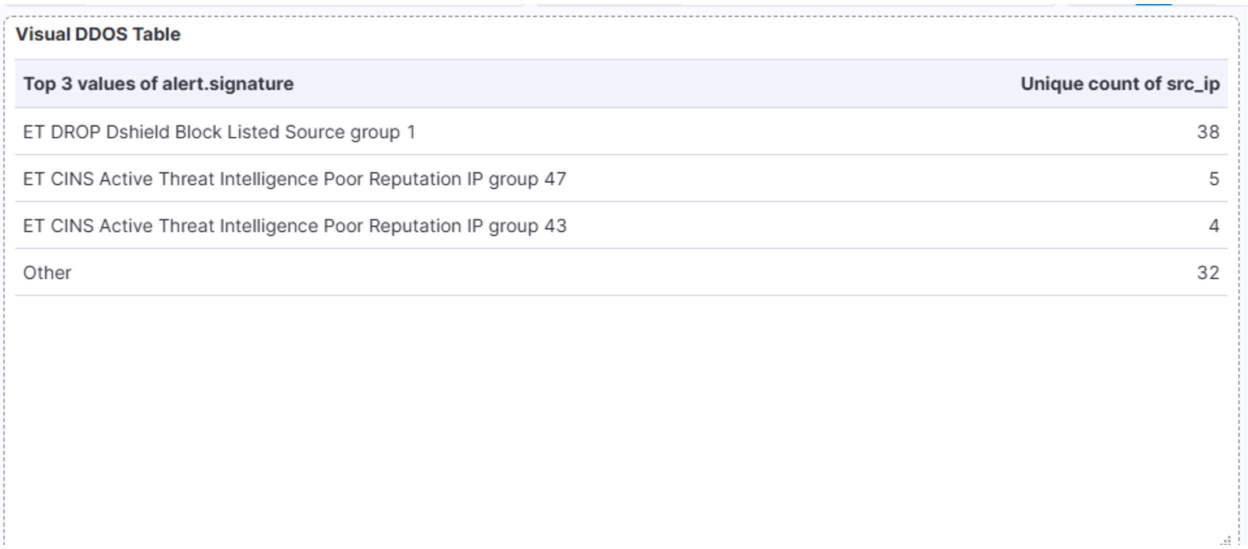
Prof. Saeed Naghizadeh Qomi

change heading for screenshots

Line Chart



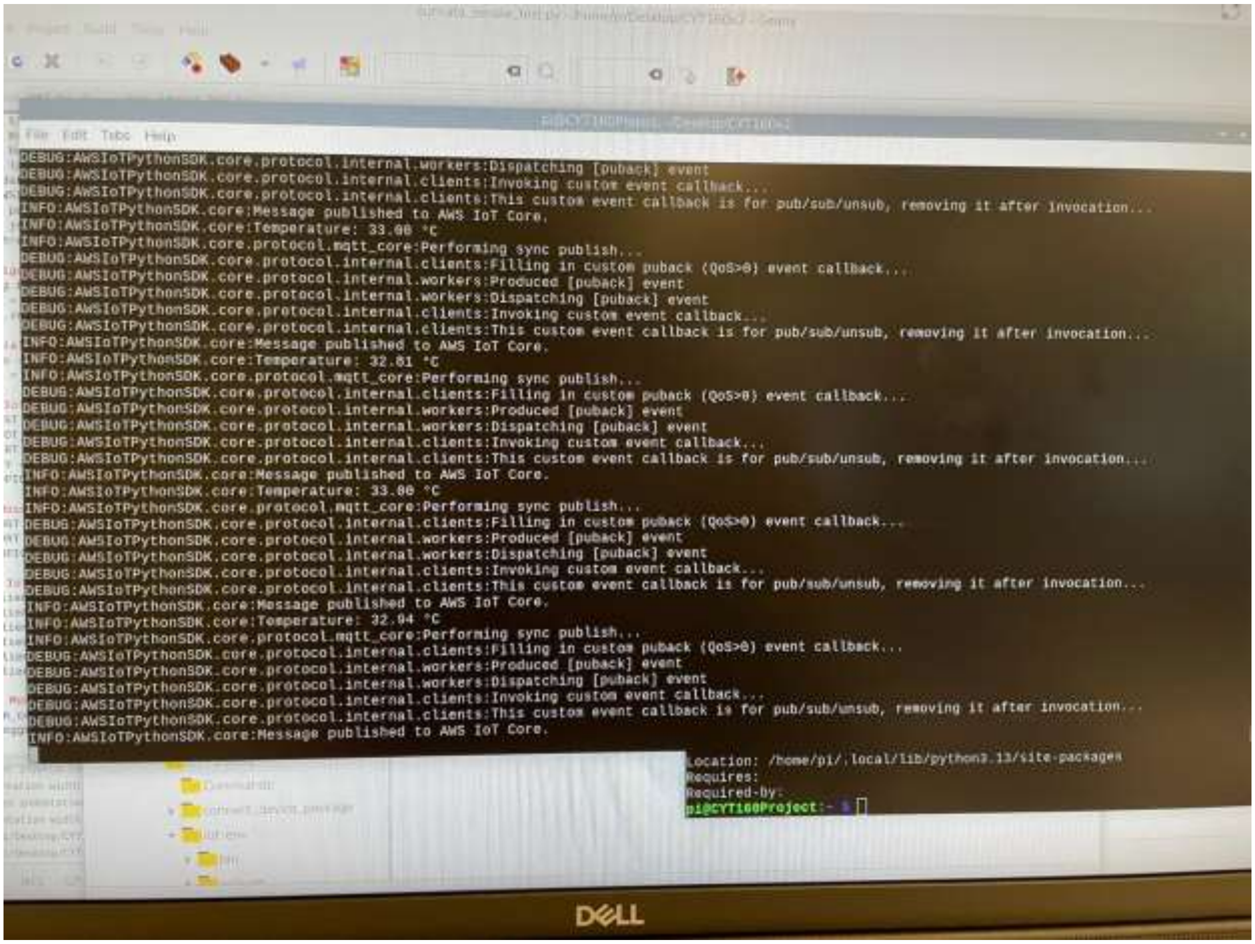
Data Table – Alert Signature and their Count



Visual DDOS Table

Top 3 values of alert.signature	Unique count of src_ip
ET DROP Dshield Block Listed Source group 1	38
ET CINS Active Threat Intelligence Poor Reputation IP group 47	5
ET CINS Active Threat Intelligence Poor Reputation IP group 43	4
Other	32

Ddos pi



```
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Dispatching [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Invoking custom event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:This custom event callback is for pub/sub/unsub, removing it after invocation...
INFO:AWSIoTPythonSDK.core:Message published to AWS IoT Core.
INFO:AWSIoTPythonSDK.core:Temperature: 33.00 °C
INFO:AWSIoTPythonSDK.core.protocol.mqtt_core:Performing sync publish...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Filling in custom puback (QoS>0) event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Produced [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Dispatching [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Invoking custom event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:This custom event callback is for pub/sub/unsub, removing it after invocation...
INFO:AWSIoTPythonSDK.core:Message published to AWS IoT Core.
INFO:AWSIoTPythonSDK.core:Temperature: 32.81 °C
INFO:AWSIoTPythonSDK.core.protocol.mqtt_core:Performing sync publish...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Filling in custom puback (QoS>0) event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Produced [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Dispatching [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Invoking custom event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:This custom event callback is for pub/sub/unsub, removing it after invocation...
INFO:AWSIoTPythonSDK.core:Message published to AWS IoT Core.
INFO:AWSIoTPythonSDK.core:Temperature: 33.00 °C
INFO:AWSIoTPythonSDK.core.protocol.mqtt_core:Performing sync publish...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Filling in custom puback (QoS>0) event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Produced [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Dispatching [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Invoking custom event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:This custom event callback is for pub/sub/unsub, removing it after invocation...
INFO:AWSIoTPythonSDK.core:Message published to AWS IoT Core.
INFO:AWSIoTPythonSDK.core:Temperature: 32.94 °C
INFO:AWSIoTPythonSDK.core.protocol.mqtt_core:Performing sync publish...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Filling in custom puback (QoS>0) event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Produced [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.workers:Dispatching [puback] event
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:Invoking custom event callback...
DEBUG:AWSIoTPythonSDK.core.protocol.internal.clients:This custom event callback is for pub/sub/unsub, removing it after invocation...
INFO:AWSIoTPythonSDK.core:Message published to AWS IoT Core.
```

```
Location: /home/pi/.local/lib/python3.13/site-packages
Requires:
Required-by:
pi@CYT160Project:~ $ 
```