Final Group Report – Part 4: IoT Attack Log Analysis Using S3 VPC Flow Logs

CYT160: Security for Cloud and Internet of Things

Professor Saeed Naghizadeh Qomi

November 24, 2025

Group 2

Jyotpal Singh

Rickie Rihal

Yash Sanjaybhai Patel

Introduction

In this part of our IoT security project, our group analyzed the network activity of our IoT setup using AWS VPC Flow Logs. Earlier, in Part 3, we used Suricata to detect attacks at the packet level. In Part 4, we focused on network-level monitoring, where only metadata like IP addresses, ports, and packet counts are visible. This helped us understand how IoT attacks look from the cloud networking side.

We enabled VPC Flow Logs, stored them in S3, downloaded the log files, and reviewed them to identify signs of the DDoS and MQTT-based attacks we previously simulated from the Raspberry Pi.

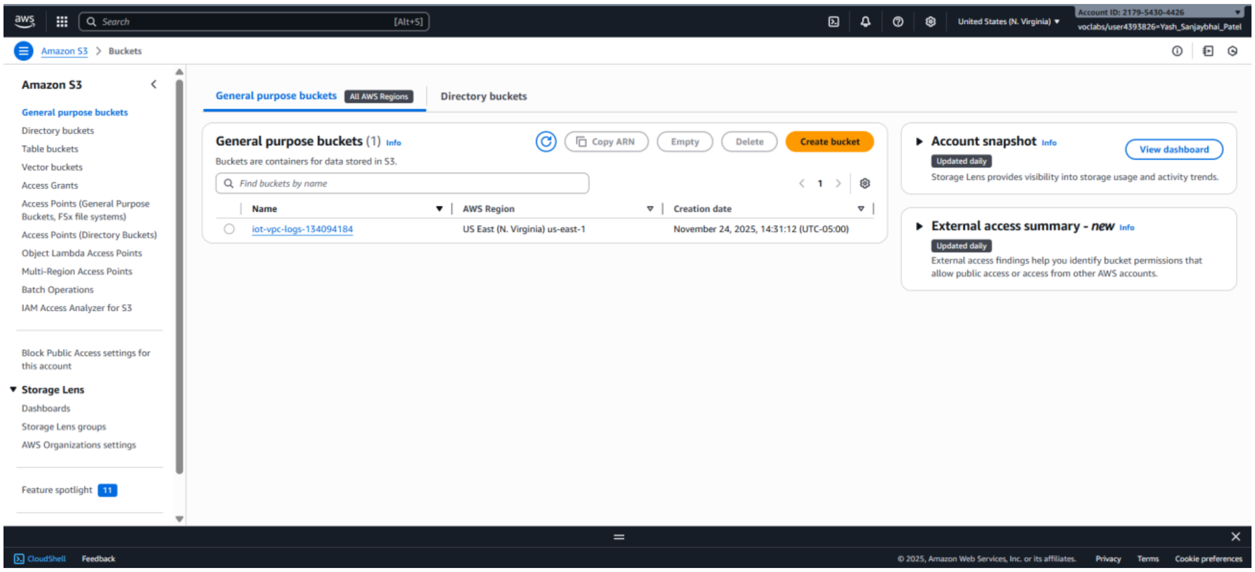
Setup and Log Collection

We first created an S3 bucket in the same region as our EC2 instance. Then we enabled VPC Flow Logs on the VPC that contains our EC2 server. The logs were configured to be delivered directly to the S3 bucket using the IAM role available in the AWS Academy environment.

After waiting for AWS to generate and deliver the logs, we found several .gz log files inside the S3 path:

We downloaded these log files and extracted them. Each log contained metadata describing who connected to our EC2 instance, which ports were used, how many packets were exchanged, and whether the traffic was allowed.

S3 Bucket



General purpose buckets (1) Info

Buckets are containers for data stored in S3.

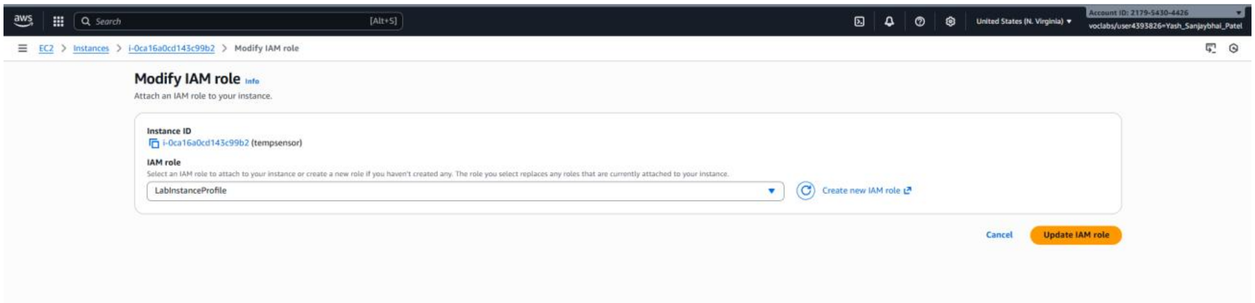
	Name	AWS Region	Creation date
○	iot-vpc-logs-134094184	US East (N. Virginia) us-east-1	November 24, 2025, 14:31:12 (UTC-05:00)

Storage Lens provides visibility into storage usage and activity trends.

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

© 2025, Amazon Web Services, Inc. or its affiliates.

Update IAM role in ec2 instance


Search [Alt+S]
United States (N. Virginia)
Account ID: 2179-5430-4426
voclabs/user4393826=Yash_Sanjaybhai_Patel
EC2 > Instances > i-0ca16a0cd143c99b2 > Modify IAM role

Modify IAM role Info

Attach an IAM role to your instance.

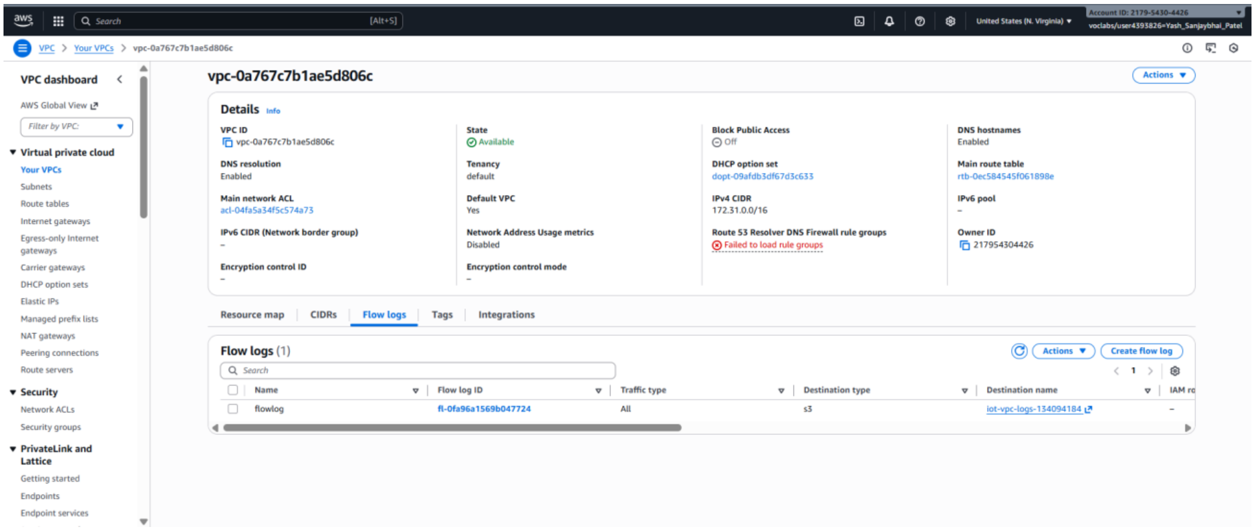
Instance ID
i-0ca16a0cd143c99b2 (tempsensor)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

LabInstanceProfile

Create new IAM role
Cancel
Update IAM role

Creation of Flowlog and Path of Gz files



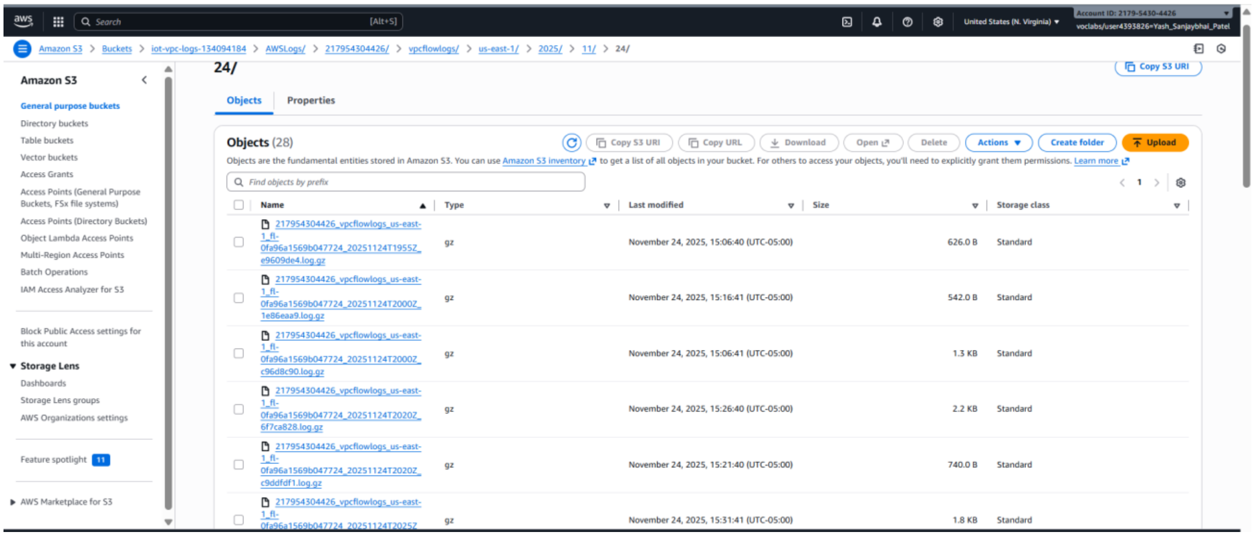
vpc-0a767c7b1ae5d806c

Details Info

VPC ID vpc-0a767c7b1ae5d806c	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-09afdb3df67d3c633	Main route table rtb-0ec584545f061898e
Main network ACL acl-04fa5a34f5c574a73	Default VPC Yes	IPv4 CIDR 172.31.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 217954304426
Encryption control ID –	Encryption control mode –		

Flow logs (1)

Name	Flow log ID	Traffic type	Destination type	Destination name	IAM ro
flowlog	fl-0fa96a1569b047724	All	s3	iot-vpc-logs-134094184	–

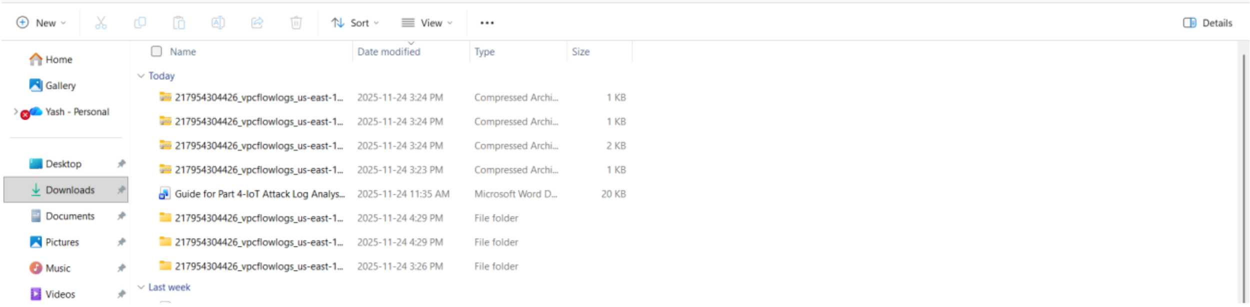

Search [Alt+S]
United States (N. Virginia)
Account ID: 2179-5430-4426
voclabs/user4393826=Yash_Sanjaybhai_Patel
Amazon S3 > Buckets > iot-vpc-logs-134094184 > AWSLogs/ > 217954304426/ > vpcflowlogs/ > us-east-1/ > 2025/ > 11/ > 24/
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
AWS Marketplace for S3
Copy S3 URI
Objects
Properties
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix

24/

Objects (28)

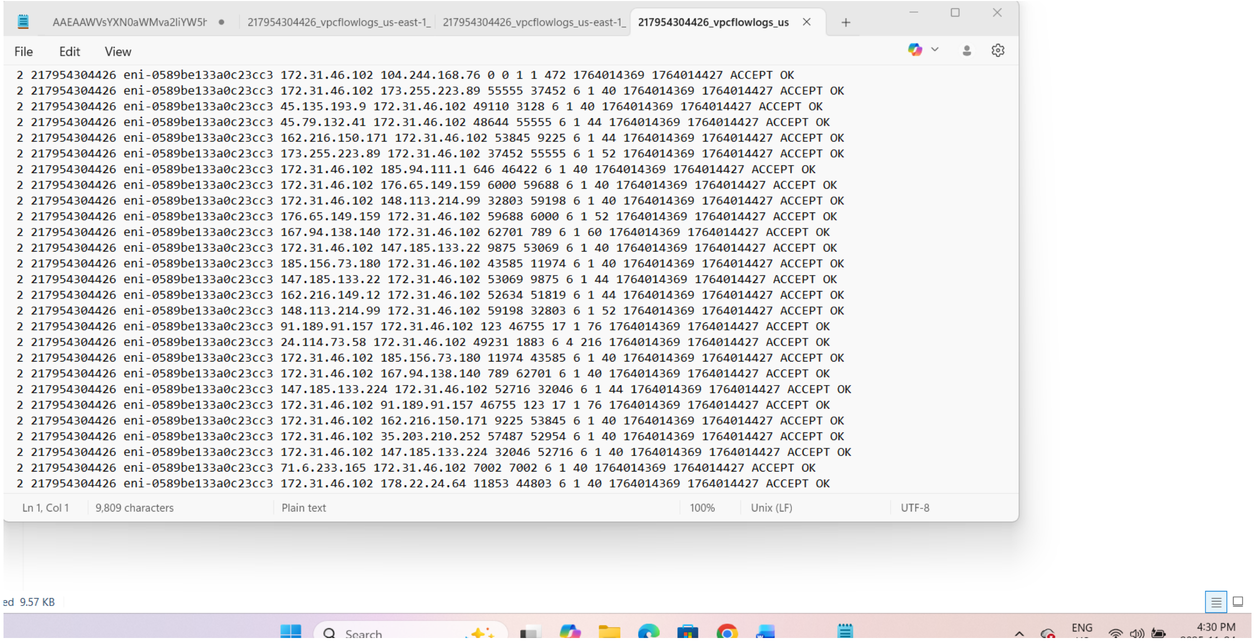
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T1955Z_e9609de4.log.gz	gz	November 24, 2025, 15:06:40 (UTC-05:00)	626.0 B	Standard
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T2000Z_1e86eaa9.log.gz	gz	November 24, 2025, 15:16:41 (UTC-05:00)	542.0 B	Standard
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T2000Z_c96d8c90.log.gz	gz	November 24, 2025, 15:06:41 (UTC-05:00)	1.3 KB	Standard
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T2020Z_6f7ca828.log.gz	gz	November 24, 2025, 15:26:40 (UTC-05:00)	2.2 KB	Standard
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T2020Z_c9ddfdf1.log.gz	gz	November 24, 2025, 15:21:40 (UTC-05:00)	740.0 B	Standard
217954304426_vpcflowlogs_us-east-1_fl-0fa96a1569b047724_20251124T2025Z	gz	November 24, 2025, 15:31:41 (UTC-05:00)	1.8 KB	Standard



Name	Date modified	Type	Size
217954304426_vpcflowlogs_us-east-1...	2025-11-24 3:24 PM	Compressed Archi...	1 KB
217954304426_vpcflowlogs_us-east-1...	2025-11-24 3:24 PM	Compressed Archi...	1 KB
217954304426_vpcflowlogs_us-east-1...	2025-11-24 3:24 PM	Compressed Archi...	2 KB
217954304426_vpcflowlogs_us-east-1...	2025-11-24 3:23 PM	Compressed Archi...	1 KB
Guide for Part 4-IoT Attack Log Analys...	2025-11-24 11:35 AM	Microsoft Word D...	20 KB
217954304426_vpcflowlogs_us-east-1...	2025-11-24 4:29 PM	File folder	
217954304426_vpcflowlogs_us-east-1...	2025-11-24 4:29 PM	File folder	
217954304426_vpcflowlogs_us-east-1...	2025-11-24 3:26 PM	File folder	

Examined the logs



```
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 104.244.168.76 0 0 1 1 472 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 173.255.223.89 55555 37452 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 45.135.193.9 172.31.46.102 49110 3128 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 45.79.132.41 172.31.46.102 48644 55555 6 1 44 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 162.216.150.171 172.31.46.102 53845 9225 6 1 44 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 173.255.223.89 172.31.46.102 37452 55555 6 1 52 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 185.94.111.1 646 46422 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 176.65.149.159 6000 59688 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 148.113.214.99 32803 59198 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 176.65.149.159 172.31.46.102 59688 6000 6 1 52 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 167.94.138.140 172.31.46.102 62701 789 6 1 60 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 147.185.133.22 9875 53069 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 185.156.73.180 172.31.46.102 43585 11974 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 147.185.133.22 172.31.46.102 53069 9875 6 1 44 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 162.216.149.12 172.31.46.102 52634 51819 6 1 44 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 148.113.214.99 172.31.46.102 59198 32803 6 1 52 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 91.189.91.157 172.31.46.102 123 46755 17 1 76 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 24.114.73.58 172.31.46.102 49231 1883 6 4 216 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 185.156.73.180 11974 43585 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 167.94.138.140 789 62701 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 147.185.133.224 172.31.46.102 52716 32046 6 1 44 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 91.189.91.157 46755 123 17 1 76 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 162.216.150.171 9225 53845 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 35.203.210.252 57487 52954 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 147.185.133.224 32046 52716 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 71.6.233.165 172.31.46.102 7002 7002 6 1 40 1764014369 1764014427 ACCEPT OK
2 217954304426 eni-0589be133a0c23cc3 172.31.46.102 178.22.24.64 11853 44803 6 1 40 1764014369 1764014427 ACCEPT OK
```

What We Observed in the Logs

When we examined the VPC Flow Logs downloaded from S3, we noticed several important patterns. The most important activity was the repeated communication with port 1883, which is the MQTT port. We confirmed this from the flow log entries that showed our EC2 instance communicating with the external IP 24.114.73.58. This is the same IP used by our Raspberry Pi during the attack. The logs contained several flows such as:

- 172.31.46.102 → 24.114.73.58 dstport=1883 packets=2 bytes=112
- 172.31.46.102 → 24.114.73.58 dstport=1883 packets=190 bytes=9892
- 24.114.73.58 → 172.31.46.102 dstport=1883 packets=192 bytes=199203

These entries show very high packet and byte counts, which match the DDoS-style MQTT flood and malformed MQTT payload attacks we performed from the Raspberry Pi. The repeated connections and large amounts of data clearly indicate abnormal and attack-like behavior.

Apart from MQTT traffic, we also noticed connections to ports that are unusual for an IoT device, such as port 465 (SMTP) and 3306 (MySQL). These appear in our logs as well:

172.31.46.102 → 193.163.125.152 dstport=465

172.31.46.102 → 109.232.218.176 dstport=3306

These ports are not normally used by temperature sensors or MQTT applications, so their presence suggests scanning, probing, or possible compromise.

All entries showed ACCEPT, meaning the traffic was allowed. This is expected because the project focuses on monitoring, not blocking. Overall, the logs confirmed both normal traffic (like DNS and HTTPS) and abnormal traffic (high-volume MQTT and strange ports), matching the attacks we simulated.

Correlating With Part 3 IDS Alerts

During Part 3, Suricata detected two types of attacks: malformed MQTT payloads and DDoS-like bursts. In Part 4, the network-level logs supported these detections. The same source IP, the same destination port (1883), and the same high-frequency connection pattern appeared in the VPC Flow Logs.

While Suricata gave deep packet alerts, the VPC logs confirmed the **traffic behavior**, showing that the same attacker IP made many repeated MQTT connections and transmitted high packet counts. Both tools, therefore, validated the same attack activity but from two different perspectives.

Conclusion

As a group, we successfully analyzed how IoT attacks appear inside AWS VPC Flow Logs. Even though these logs do not show packet contents, the repeated MQTT activity, high packet counts, and unusual port usage were enough to identify suspicious behavior. By comparing this information with our Suricata alerts from Part 3, we confirmed that the IoT device experienced the same attack patterns from both network-level and application-level viewpoints.

This part of the project helped us understand that complete IoT monitoring requires both deep-packet inspection and network-flow visibility. Together, these tools gave us a full picture of how IoT attacks behave in real environments.