Project 3 Report Part 4

IoT Attack Log Analysis with S3-Stored VPC Flow Logs

Group 8

Fozeya-Nikka Alviar

Angeline Nicole Faina

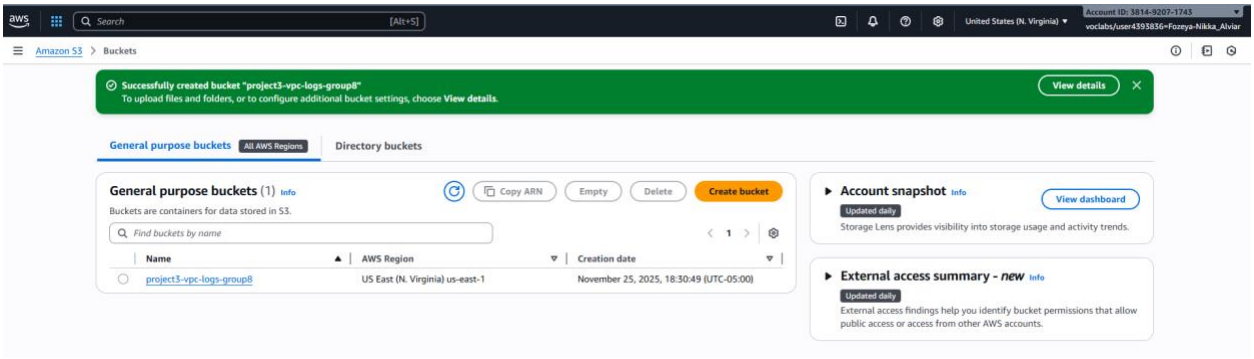
Sam Omandam

CYT160NBB

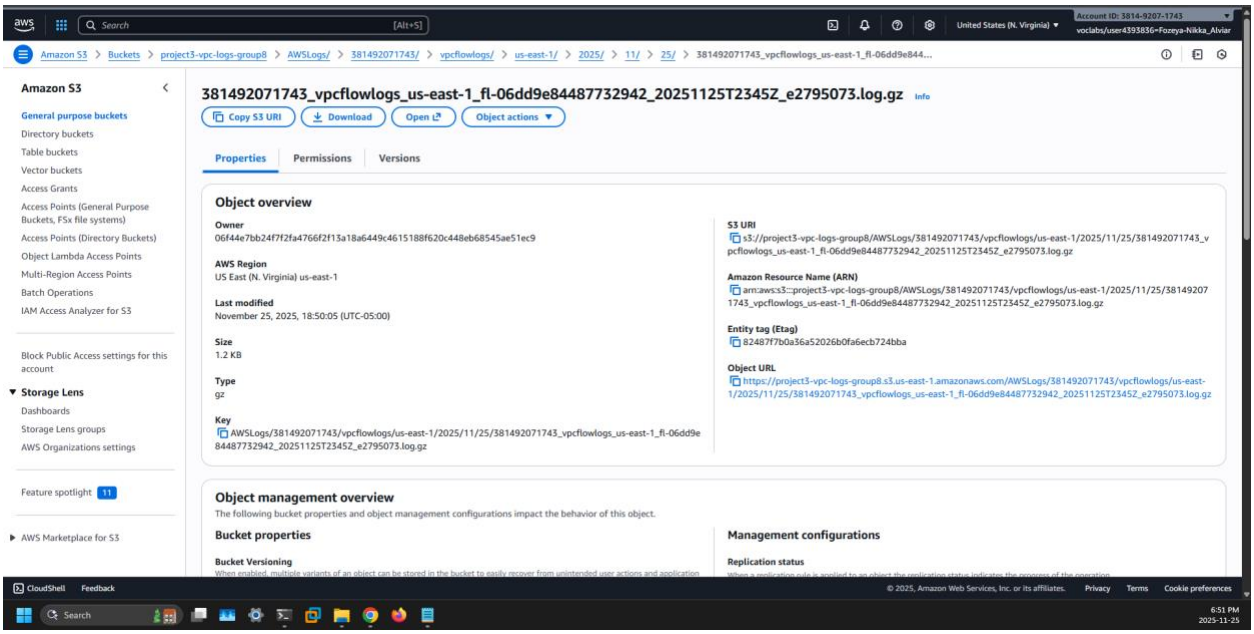
28 November 2025

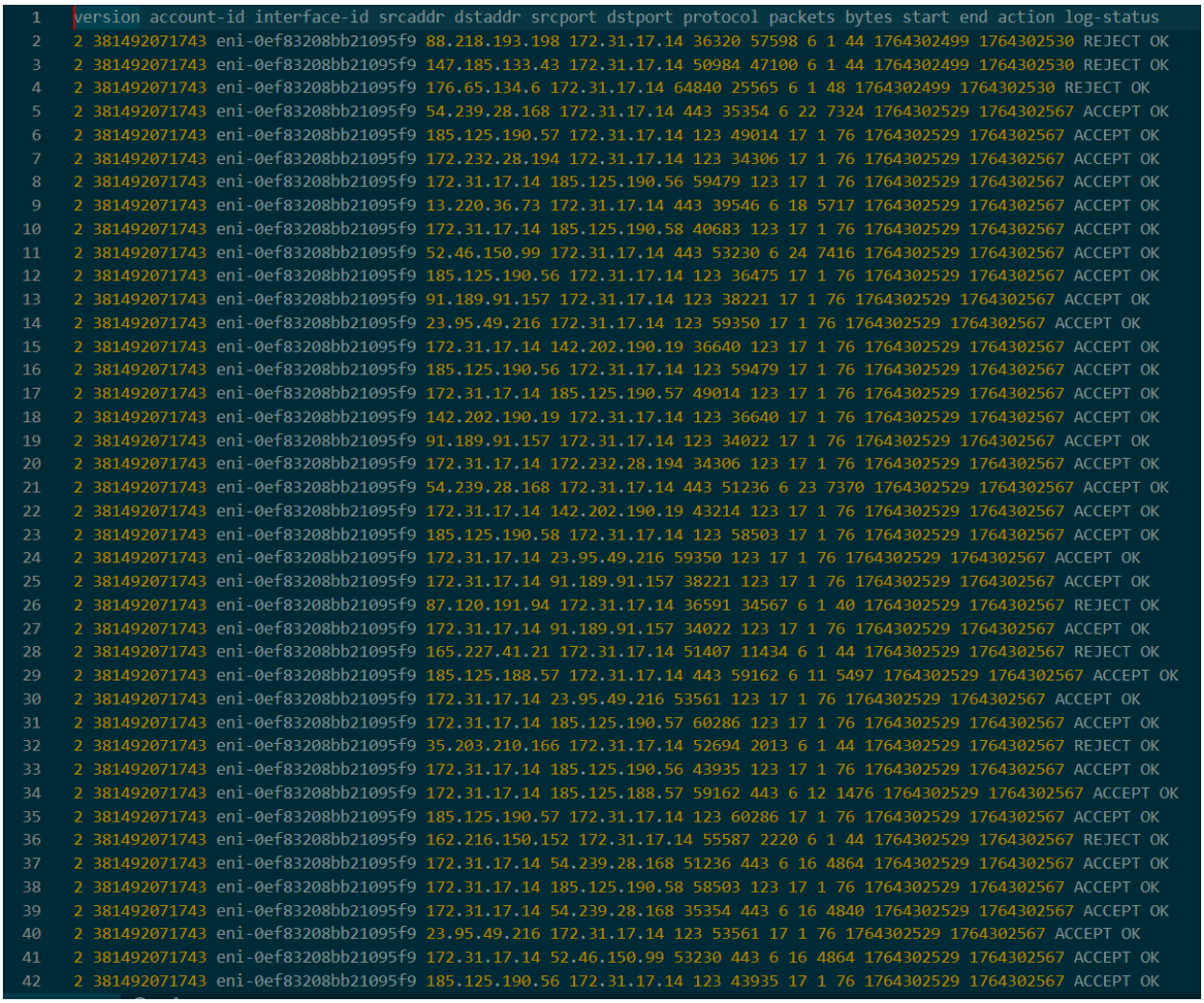
Prof. Saeed Naghizadeh Qomi

S3 Bucket Created



Log Files





```
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status
2 381492071743 eni-0ef83208bb21095f9 88.218.193.198 172.31.17.14 36320 57598 6 1 44 1764302499 1764302530 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 147.185.133.43 172.31.17.14 50984 47100 6 1 44 1764302499 1764302530 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 176.65.134.6 172.31.17.14 64840 25565 6 1 48 1764302499 1764302530 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 54.239.28.168 172.31.17.14 443 35354 6 22 7324 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.57 172.31.17.14 123 49014 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.232.28.194 172.31.17.14 123 34306 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.56 59479 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 13.220.36.73 172.31.17.14 443 39546 6 18 5717 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.58 40683 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 52.46.150.99 172.31.17.14 443 53230 6 24 7416 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.56 172.31.17.14 123 36475 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 91.189.91.157 172.31.17.14 123 38221 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 23.95.49.216 172.31.17.14 123 59350 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 142.202.190.19 36640 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.56 172.31.17.14 123 59479 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.57 49014 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 142.202.190.19 172.31.17.14 123 36640 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 91.189.91.157 172.31.17.14 123 34022 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 172.232.28.194 34306 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 54.239.28.168 172.31.17.14 443 51236 6 23 7370 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 142.202.190.19 43214 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.58 172.31.17.14 123 58503 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 23.95.49.216 59350 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 91.189.91.157 38221 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 87.120.191.94 172.31.17.14 36591 34567 6 1 40 1764302529 1764302567 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 91.189.91.157 34022 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 165.227.41.21 172.31.17.14 51407 11434 6 1 44 1764302529 1764302567 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.188.57 172.31.17.14 443 59162 6 11 5497 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 23.95.49.216 53561 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.57 60286 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 35.203.210.166 172.31.17.14 52694 2013 6 1 44 1764302529 1764302567 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.56 43935 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.188.57 59162 443 6 12 1476 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.57 172.31.17.14 123 60286 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 162.216.150.152 172.31.17.14 55587 2220 6 1 44 1764302529 1764302567 REJECT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 54.239.28.168 51236 443 6 16 4864 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 185.125.190.58 58503 123 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 54.239.28.168 35354 443 6 16 4840 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 23.95.49.216 172.31.17.14 123 53561 17 1 76 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 172.31.17.14 52.46.150.99 53230 443 6 16 4864 1764302529 1764302567 ACCEPT OK
2 381492071743 eni-0ef83208bb21095f9 185.125.190.56 172.31.17.14 123 43935 17 1 76 1764302529 1764302567 ACCEPT OK
```

Report

Excessive requests from one srcaddr: 162.216.x.x (4 IPs) and 147.185.x.x (3 IPs)

Repeated access to dstport 1883 (MQTT) or other IoT-related ports: Port 2376 (Docker), Port 25565 (Minecraft), Port 8001

High packets or bytes counts: 84,821 Bytes (67 Packets), 82,591 Bytes (70 Packets)

REJECT action status: 23 rejected connections found

Based on the vpcflowlogs file, we observed and analyzed several suspicious IPs which are scanning for open ports are 162.216.x.x (162.216.150.152, 162.216.149.224, 162.216.150.206, 162.216.150.119) and 147.185.x.x (147.185.133.43, 147.185.132.89, 147.185.133.229) (external IPs). These IPs are sending single packets to random destination ports (25565, 2376, 8001, 11434, 23107) to see what is open. Brute force attack is not explicitly observed in this sample. The traffic is horizontal (scanning many ports) rather than vertical (hammering one password prompt). The connection attempts to Port 2376 (Docker) and Port 25565 (Minecraft) are most likely reconnaissance for exploitation which is highly suspicious. Scanning is proven by 1 packet, REJECT pattern which is seen in 100% of the malicious findings. Potential botnet/C2 communication is indicated by IoT-related port targeting. The largest data transfer is from Google Cloud services (34.120.127.130) with 84,821 bytes received and 82,591 bytes received in separate sessions. While there is no massive outbound spike found (legitimate responses to cloud services), this indicates Low Risk/Legitimate traffic. The largest accepted transfers appear to be legitimate HTTPS traffic to AWS and Google Cloud infrastructure which is likely authorized cloud service communication and not data exfiltration.