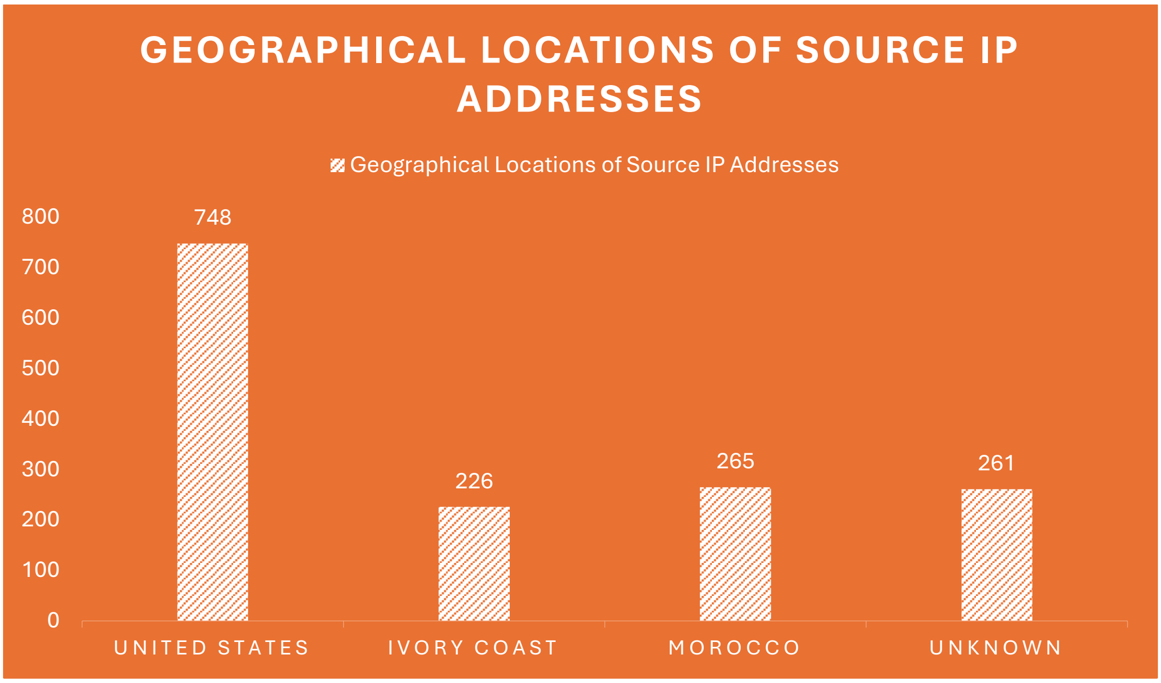
AWS Cloudtrail Executive Report – Jack Duggan

Network Security

Access to company resources is only permitted from the IP ranges *192.168.1.0/24* and *10.0.0.0/16*. The company policy states that **all** remote connections must be made via one of these approved VPN ranges.

1500 total anomalies were detected and written to *report.json*, with all 1500 originating from outside the permitted IP address ranges.

The geographical location of each of these anomaly requests was obtained from the source IP addresses and can be seen in the graph below.



AWS Usage Policies

The breakdown of events by approved AWS service are as follows: **ec2**: 426, **s3**: 442, **iam**: 452, **secretsmanager**: 180. There was no use of unapproved AWS services.

The company security policy states, “creation of IAM users is strictly forbidden”. There were, however, **242** instances of IAM *CreateUser* event.

The root account appears to be well secured as there were no events with root account usage.

TLDR/Conclusion

Quite a few anomalies were found in the logs, many of which violated the security policy in more than one way. It appeared that when high-risk events occurred, such as production EC2/S3 modification or IAM user/role modification, these events typically had source IP addresses from outside the approved VPN IP ranges. Additionally, they originated from countries outside the approved geographical zones approximately 50% of the time.