Prepared By: Gopi Gor

Date: 04/07/2024

Cloud Security Investigation

This report analyses 3 different parts of cloud security and plays a role in incident reporting. Sumologic was used to create this report, along with scripts that were created, and using saved logs. Considering a role of an SOC analyst, a report has been prepared for Public S3 Buckets, AWS Regions and Vulnerable Network ACL's along with business implications, The Appendix defines the scripts that were used during the creation of the report.

Public S3 Buckets

In my capacity as a SOC Analyst, I might initially confirm the alert by looking over the information I have, like the impacted S3 container, the kind of permission or action found, and the time it occurred. After that, I would go ahead and gather more context by going over the CloudTrail logs associated with the alert and searching for any unusual activity like an event where the public access was given. I would report the alarm to the incident response team so they may investigate it deeper if it shows that someone has accessed a public S3 bucket without authorization. This could entail checking access rights, examining the access origin, and figuring out whether any private information was revealed. The criticality assigned to this type of an alert would depend on multiple things like how much access the attacker had and what was the sensitivity of the data. If it is sensitive data, it would be a **high** criticality event. The dashboards that would be useful for this alert type would be a dashboard which monitors the ACL parameters and access permissions and logs for S3 buckets would be useful. The Amazon S3 audit would be a useful dashboard that can be used as it specifically provides details on the access logs.

These discoveries may expose confidential information to unwanted access, which might influence the company. This may result in loss of consumer trust, fines from the authorities, and harm to one's reputation. The company faces immediate short-term risks from data breaches and related expenses including incident response, forensic investigation, and notified parties. Over time, the company runs the danger of losing clients, suffering reputational harm, and facing legal repercussions. If these risks are not addressed, there may be additional weaknesses in the projected future and possible compromises.

In terms of holistic remediation, the teams should do a complete thorough investigation on the breach that took place, make changes to access control policies and procedures, and train employees on best practices. Even though it is a cloud, it is riskier as so much more data is on the cloud in the current scenario. This means ensuring that additional security measures are in place and inform the authorities and customers in case a breach has occurred. Additionally, there has to be some kind of fair compensation that should be offered, which also builds a trust back in the company.

AWS Regions

As an SOC analyst, analysing this kind of alert is a very important one. Data should always be local in the cloud and AWS allows for other regions to be included. This means if another compliance is followed and the data is another country or region, it could affect the data of another region. To analyse this alert, we need to find the logs to see if there is data from another region by using the appropriate filters. The usernames which are used to log into other regions holds another very important leg in understanding who the reason for any kind of attack may be that may occur. Additionally, the certificates and their signatures would also provide more information if the login was a legit user, and the IP address would be useful to detect further data about the login. The criticality of this kind of alert, according to me would be **high**. While AWS has a lot of cloud and region services, if a specific company only wants the data to be retained in the same country, another country login in regions can be marked as an unauthorized activity and this could be risky for anyone. This would also depend on what is the criticality of the access, and how much impact the activity has had or will have on the organization. Dashboards useful for this investigation could be the ones which show logged in locations, user activity, access logs, IP addresses. In Sumologic, some of the useful dashboards are AWS CloudTrail – User Activity and AWS WAF - Cloud Security Monitoring and Analytics one.

Businesses face serious risks from illegal entry into AWS regions, such as the loss of confidential information, possible cyberespionage, and monetary damages. Short-term consequences of such access might include operational outages and unavailability of services due to interruptions in service and the initiation of Denial of Service (DoS) assaults by foreign nations. Long-term, national-state actors and Advanced Persistent Threats (APTs) may use unlawful access as a means of cyber espionage, perhaps jeopardizing vital corporate data. Security breaches may also result in compliance and regulatory fines for firms, which would negatively affect their operations and image.

For holistic remediation of this error type, there should be constant monitored checks that take place in each region to ensure that only required people are using the different regions of the AWS. The scope of this unauthorized access and different region connections have to be analyzed to understand and safeguard the data of the individual or business that has services on the AWS Cloud. The legal and regulatory compliance policies and procedures should have clauses that make sure that there are exceptions for these logins and the authorities should be informed incase the clause has an occurrence due to any reason.

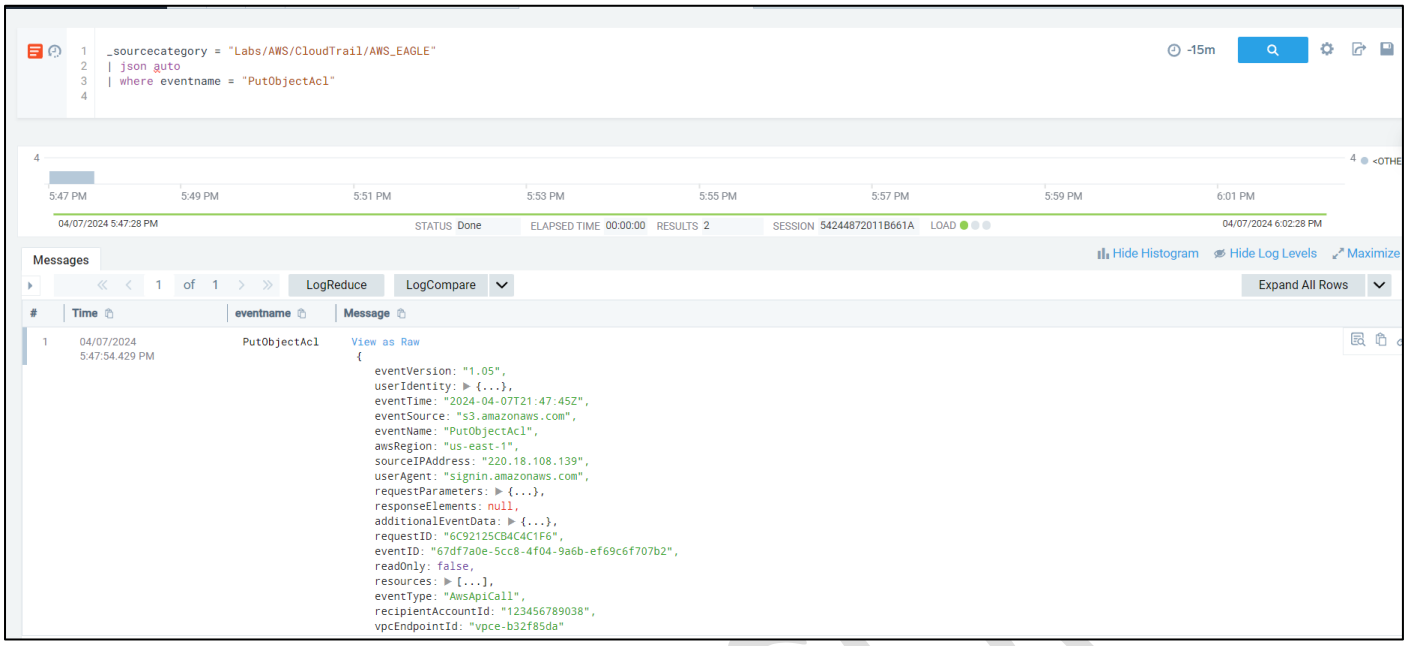
Vulnerable Network ACL's

As an SOC analyst investigating this misconfiguration of network ACL's which could lead to a potential attack, I would look at the Access control lists to check if there are any vulnerabilities in the code or the accesses given to the users. I would check if there are any permissions that are too restrictive or too permissive that allow an unauthorized person to access the cloud infrastructure. This also means looking at all rules, modifications that need to be made, and alerting the development teams of these vulnerabilities. In terms of criticality, this would definitely be a **medium to high** criticality because if the access is too permissive, as in the case with vulnerable network ACL's, it will be dangerous for the whole organization and the people concerned who use that cloud service. Dashboards that could be useful for this investigation and analysis would be ACL rule changes, network traffic patterns and unauthorized access dashboards. A good example is the Amazon S3 Audit dashboard, or Netflow optimizer, which shows security monitoring along with traffic that is using critical ports. This could specially be useful to understand what ports have been used by an outsider.

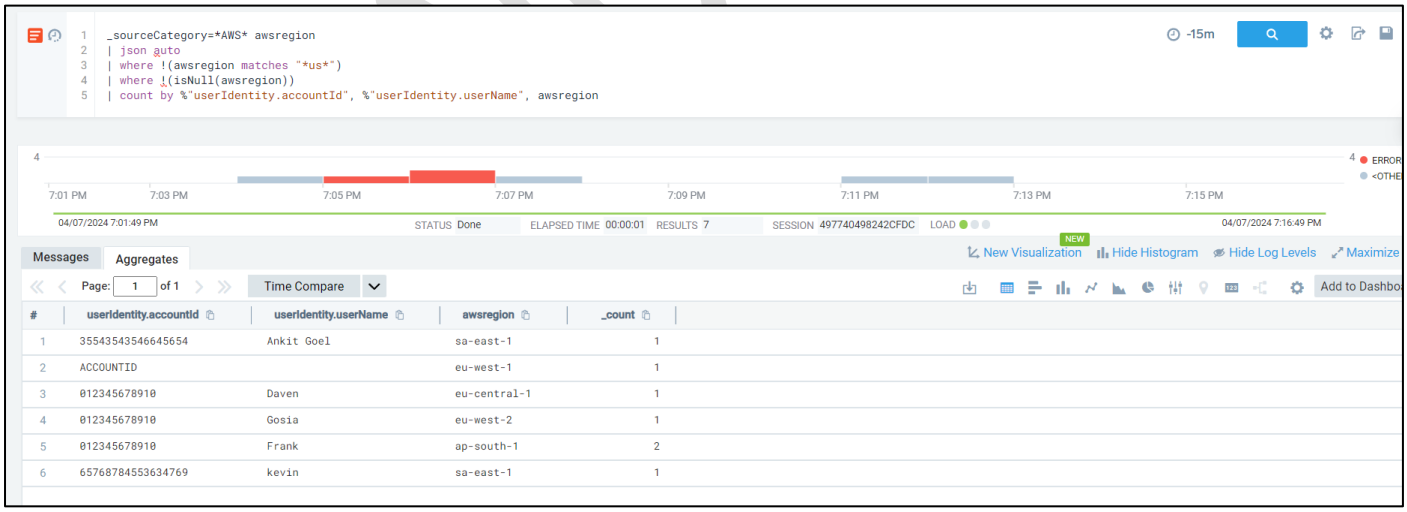
These discoveries may expose the IT infrastructure to hacker assaults and unauthorized access, which could influence the company. Security breaches that have interrupted services, and a decline in customer confidence may result from this. Because of weak networked ACLs, the company faces temporary risk to safety and possible compromises. Financial losses as well as operational problems could come from this. The company runs the long-term danger of losing clients, suffering regulatory fines, and harming its brand due to any kind of emerging attacks. Unauthorized access means anything that a hacker can do once they are in the network – malware, stealing of data, impersonation, revenge or cyber espionage. If these risks are not addressed, there may be more security breaches and weaknesses in the future.

To find and fix gaps in the ACL's, the company should thoroughly evaluate the way its computer network ACL configuration is set up. This could entail putting stronger restrictions on access in place, modifying and altering ACL rules, and keeping an eye out for unusual activities in network communication. To stop such weaknesses in the future, the company must additionally evaluate its network cybersecurity policies and processes.

Appendix




```
_sourcecategory = "Labs/AWS/CloudTrail/AWS_EAGLE"
| json auto
| where eventname = "PutObjectAcl"
| where %"requestParameters.x-amz-acl" matches "*public*"
| count by %"requestParameters.bucketName", eventname,%"requestParameters.x-amz-acl"
```




```
_sourceCategory = *AWS*
| json auto
| where eventname = "CreateNetworkAclEntry"
| where %requestParameters.ruleAction = "allow"
| where %requestParameters.portRange.from = 0 and %requestParameters.portRange.to = 5000
| count byeventname,%requestParameters.ruleAction,%requestParameters.portRange.from,%requestParameters.portRange.to, %"requestParameters.cidrBlock"
```

References

1. https://docs.aws.amazon.com/AmazonS3/latest/userguide/configuring-block-public-access-bucket.html
2. https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
3. https://www.pluralsight.com/blog/it-ops/access-control-list-concepts