Stephen Mensah

Cloud Security Monitoring

Public S3 Bucket

Screenshots

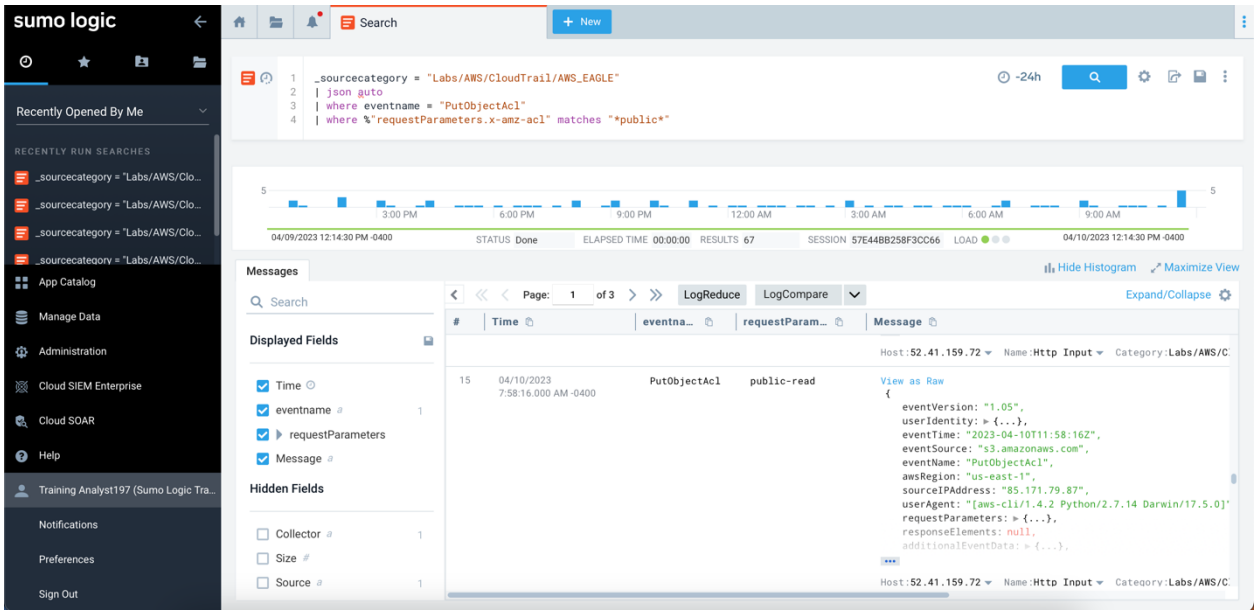

Fig 1: Logs with public access

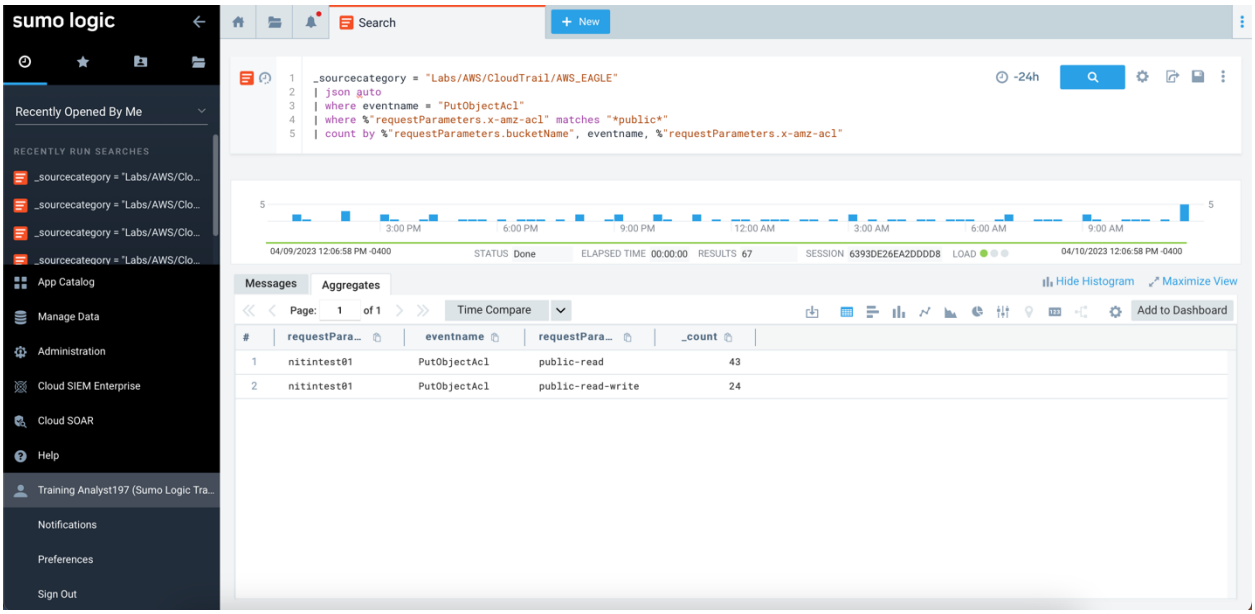

Fig 2: Aggregated results of users with public access

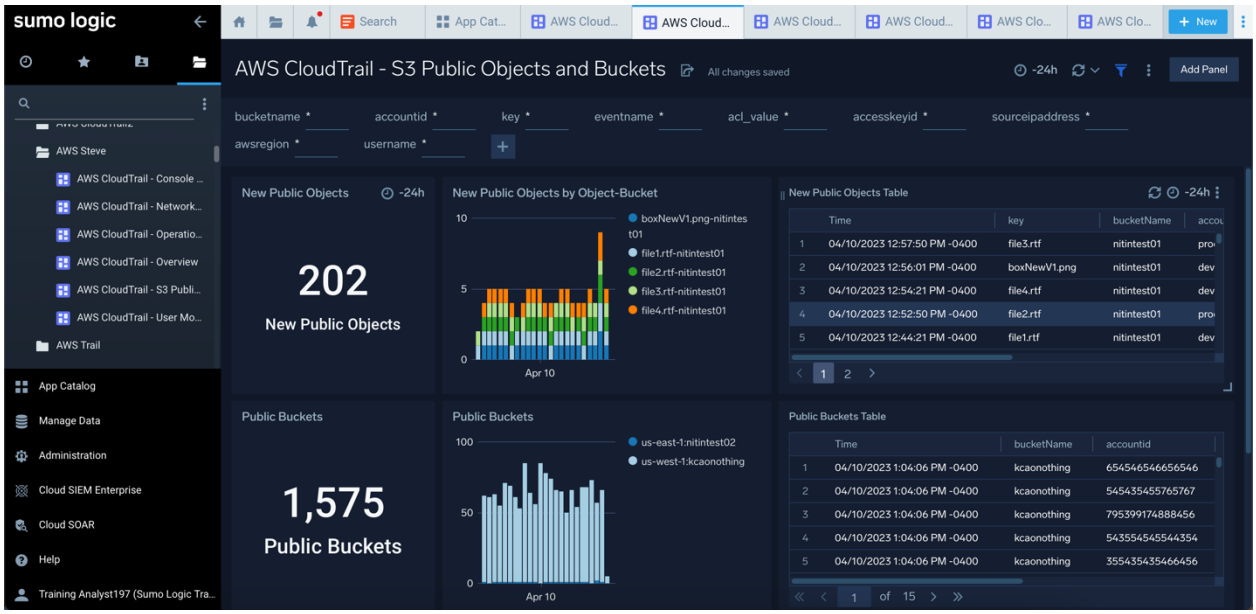

Fig. 4: S3 Public Objects and Buckets Dashboard

Fig. 4: CloudTrail Overview Dashboard

Threat Simulation

The first approach to respond to any public access to the S3 object storage service is to monitor and notify the security team when suspicious activity is detected. To this effect, an alert would be created to report any public access event that would be logged in the CloudTrail. Public write configuration is prohibited and can allow anyone on the internet to modify the objects in the S3 bucket. As such, after the alert is triggered, I would create additional search queries to filter all anonymous users who may have gained unauthorized access to the company's resources. By identifying the users, I will be able to distinguish suspicious accounts from benign ones. After filtering the users, I will monitor additional logs 7 days prior to the alert and all logs recorded after the event identify additional events that may be associated with such names. This will help me detect user actions on the bucket. These actions could be the addition, deletion, and replacement of S3 objects. Depending on the action performed by the anonymous user, the security team will take measures to remediate such modifications and occurrences. Giving public access to S3 objects can lead to data loss or exposure. As such, I will assign a high criticality level. I will use the AWS CloudTrail Overview and S3 Public Bucket and Object Dashboards.

Business Impacts

Granting public access to S3 buckets can have short-term risks of data exposure, data loss, unexpected AWS service charges, and other financial losses. The attacker can also upload malicious files to undertake other malicious activities. Long-term risks can be compliance issues and ransomware attacks on stolen data.

Remediation

Addressing such a challenge requires that CloudTrail logs are monitored in real-time for any unauthorized access. The security team must also check for S3 misconfigurations, deny public access to S3 buckets, remove anonymous users, and delete all the data uploaded to the bucket by unauthorized users.

Screenshots

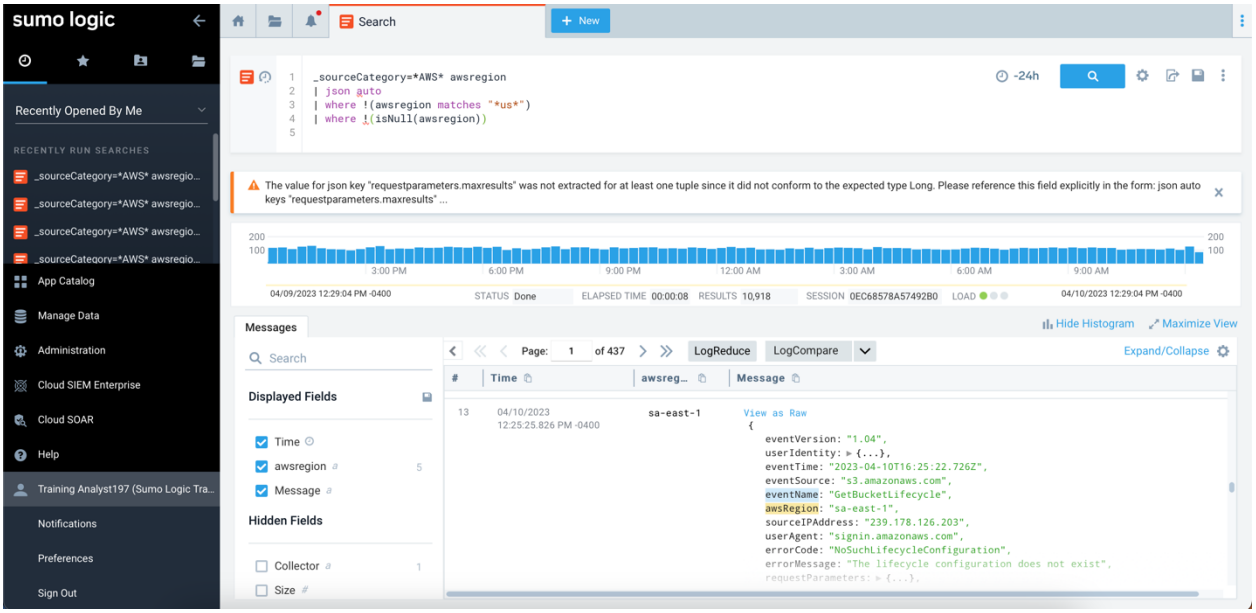

Fig. 5: Logs from non-US AWS regions

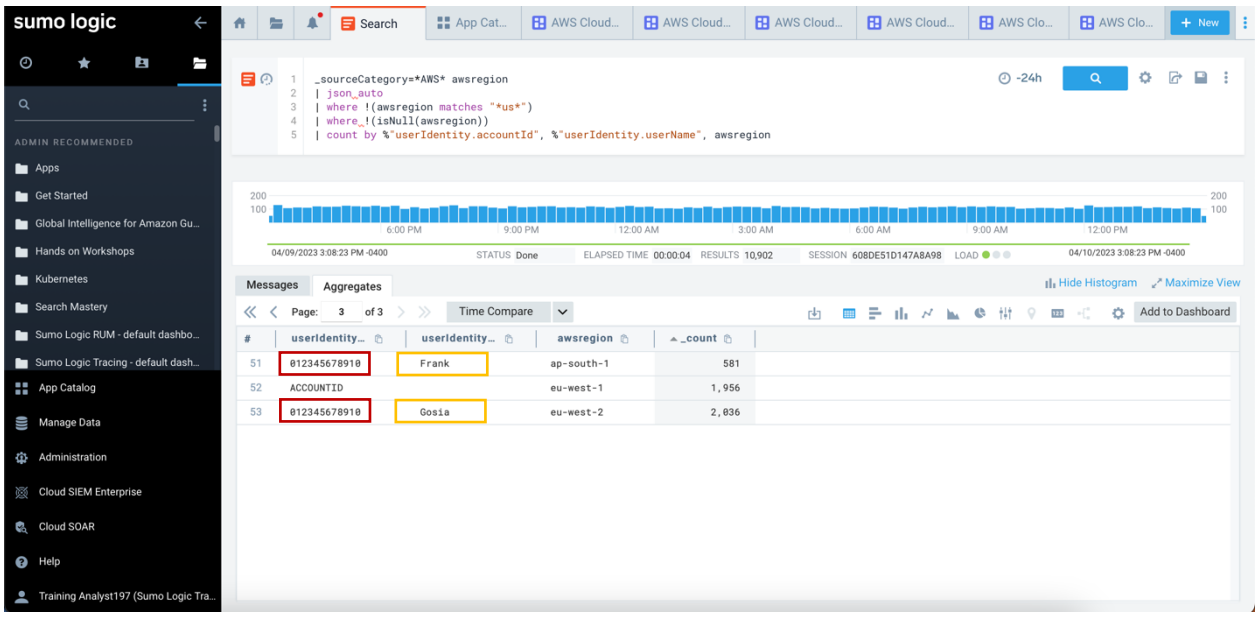

Fig. 6: Accounts with a high number of resource requests

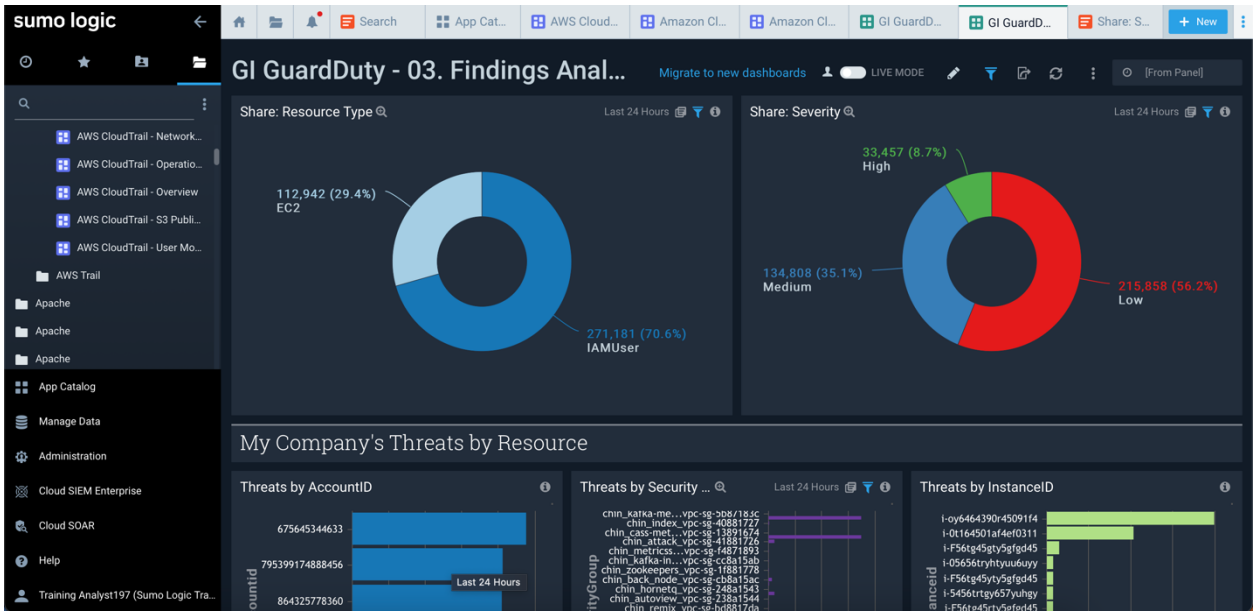

Fig. 7: Amazon GuardDuty Finding Analysis Dashboard

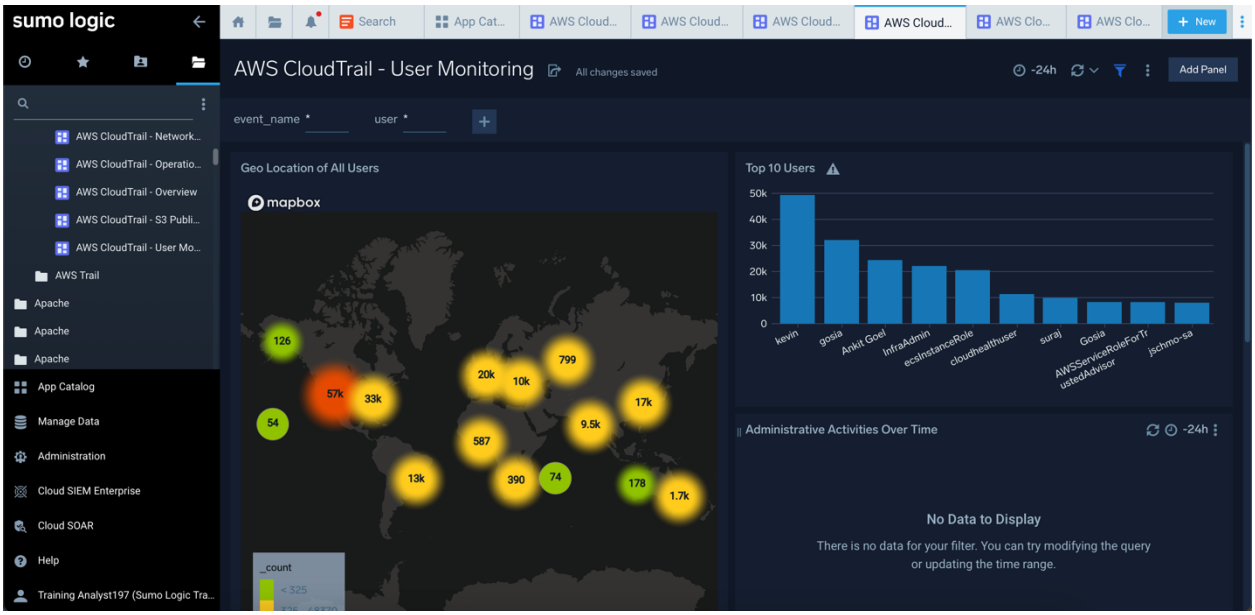

Fig. 8: User Monitoring Dashboard

AWS Regions

Threat Simulation

The first step for me to take as a SOC analyst is to create a customized alert to monitor all logged activities on CloudTrail and notify the security team when the alert is triggered. In addition, it is important to establish a baseline on how resources are used in each AWS region. By establishing the baseline activity, you will be able to detect any deviation or excessive use of resources. Accounts with suspicious usage of resources will be traced to identify any operation that may have been performed by the compromised accounts. All logs that were recorded 7 days before the alert and those logged after the alert will be analyzed to identify the operations performed to be able to track changes and additions that were made. From the query, it was identified that there was excessive use of resources in the "eu-west" region. The account id labeled as "ACCOUNTID" which had no username assigned made 1933 resource requests while the account with the ID "Gosia" made 2047 requests, about 400% times of the requests made to other regions. In addition, it was discovered that the account ID "012345678910" had two different usernames (Gosia and Frank, labelled in Fig 6.) in two different eu-regions, both with high requests. I will assign high severity to this event. And I will use the Console Login, User Monitoring, and Operation dashboards in this scenario. I will also add the Amazon GuardDuty Finding Analysis Dashboard. An incident response report will be written and communicated with stakeholders. The company's threat intel will equally be updated.

Business Impacts

Unauthorized use of resources can lead to financial losses. Compromised accounts can lead to data breaches and equally be used to create backdoors for future exploitations. Long-term risks include

fines from data breaches and potential malware attacks which can disrupt business operations. Data leaks can lead to compliance issues and damage the company's reputation.

Remediation

To address this scenario, it is important to use AWS CloudTrail to monitor all event logs. Other measures include changing the passwords for compromised accounts, rotating and deleting account access keys, and suspending compromised accounts. The business can employ Amazon GuardDuty to protect its resources from malware attacks.

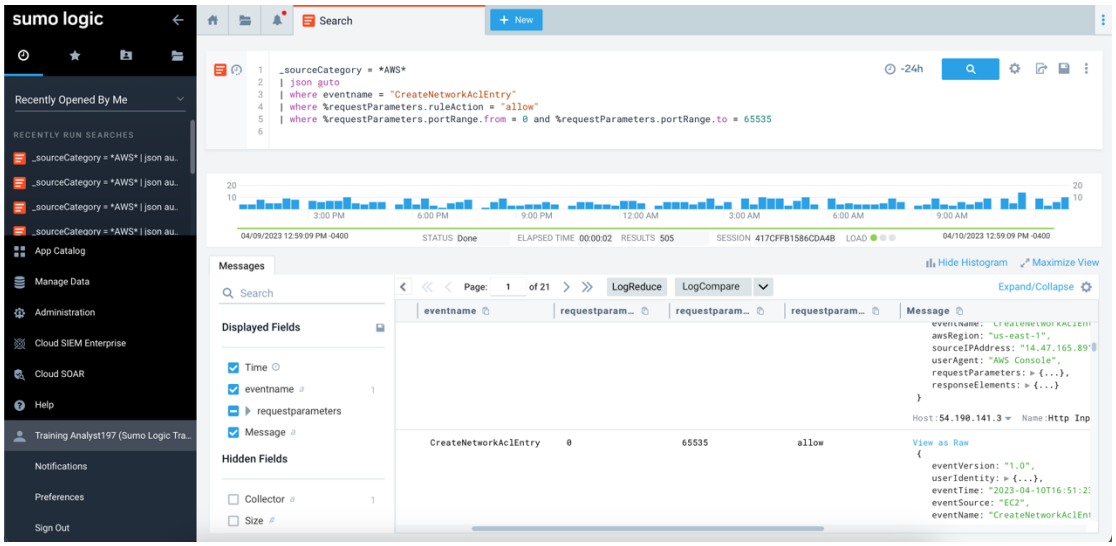

Fig. 9: ACLs that allow all ports to be open

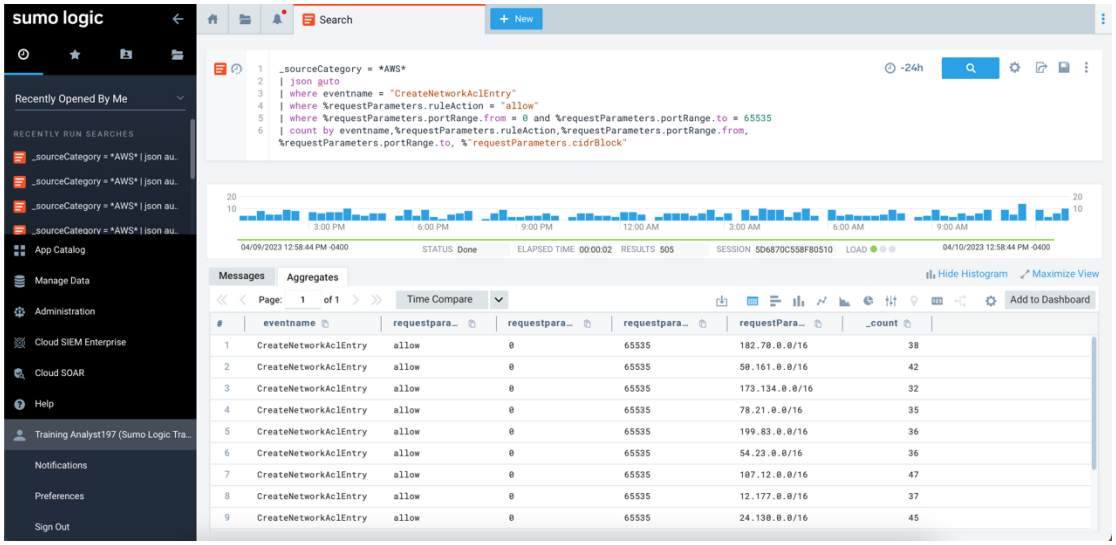

Fig. 10: Aggregates of the search results

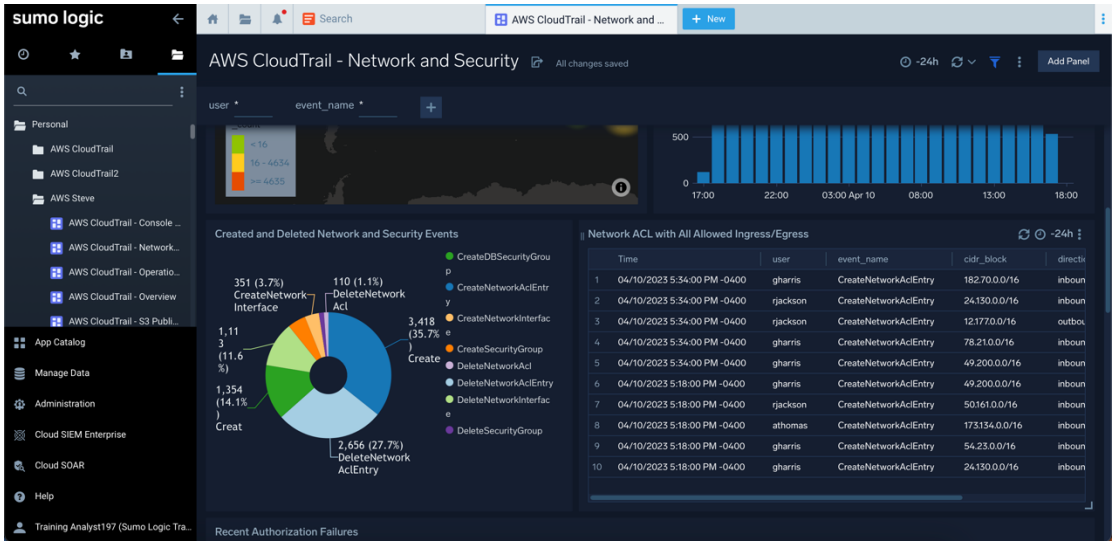

Fig: 11. Network and Security Dashboard used

Vulnerable Network ACLs

Threat Simulation

Having an unrestricted network exposes the business to a series of attacks including Distributed Denial of Service (DDoS) attacks. To respond to this kind of incident, continuously review your network policies and security control for vulnerabilities. An alert will be created to proactively notify the security team when a vulnerable ACL is detected on the network. After the alert is triggered, I will first fetch the logs and analyze them for vulnerabilities. To this effect, I will build a search to look for AWS CloudTrail events to detect if any network ACLs were created with all the ports open to a specified CIDR. After identifying such ACLs, measures will then be taken to address the weakness. I will reconfigure such Network ACL inbound rules in order to allow traffic from a specific source port or source port range only. In addition, the network will be monitored for any form of unauthorized access. Any IP address with signs of suspicious activities on the network will be traced by analyzing logs associated with such address to identify any form of malicious activity that may have been performed. I will assign a medium risk level. I will use also use the CloudTrail Network and Security Dashboard in this scenario.

Business Impacts

Short-term risks associated with this event are distributed denial of service attacks, data breaches from unauthorized access, financial losses, and disruption of business operations. Long-term risks are legal battles, regulatory compliance violations, and could damage the company's reputation.

Remediation

The first step to remediate vulnerable network ACLs is to monitor the network. Regularly audit the network and vulnerable ACLs should be reconfigured to allow traffic from a specific required source port or source port range, close unnecessary ports, and implement the principle of least privilege on the network.

References

Trend Micro (n.d). S3 Bucket Public 'WRITE' ACL Access. Accessed on April 10, 2023 from https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/S3/s3-bucket-public-write-access.html

DataDog (n.d). S3 bucket ACLs are configured to block public write actions. Accessed on April 10, 2023 from https://docs.datadoghq.com/security/default_rules/aws-s3-publicaccesscontrols/

Rosén, F (2017, July 13). A deep dive into AWS S3 access controls – taking full control over your assets. Accessed on April 10, 2023 from https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/

AWS (n.d). Malware Protection in Amazon GuardDuty. Accessed on April 10, 2023 from https://docs.aws.amazon.com/guardduty/latest/ug/malware-protection.html

Nachmani, O (2017, September 27). Prevent hacked AWS accounts from wreaking havoc. Accessed on April 10, 2023 from https://www.techtarget.com/searchaws/answer/Prevent-hacked-AWS-accounts-from-wreaking-havoc

Trendmicro (n.d). Unrestricted Network ACL Inbound Traffic. Accessed on April 10, 2023 from https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/VPC/network-acl-inbound-traffic-all-ports.html

AWS (n.d). Control traffic to subnets using Network ACLs. Accessed on April 10, 2023 from https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html?ref=wellarchitected