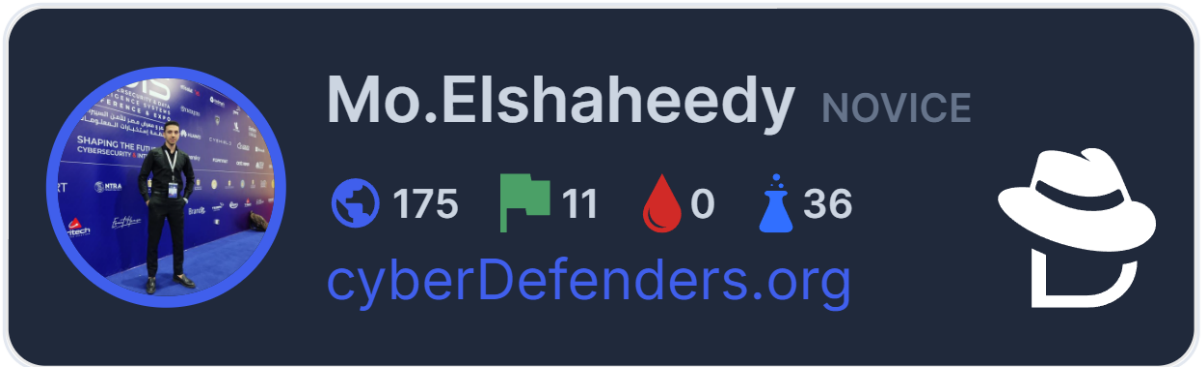
AWS RAID Challenge



https://www.linkedin.com/in/elshaheedy/

Topic: ***Cloud Forensics***

LabLink: https://cyberdefenders.org/blueteam-ctf-challenges/awsraid/

Scenario:

Your organization uses AWS for hosting critical data and applications. An incident has been reported involving unauthorized data access and potential exfiltration. The organization's security team has detected unusual activities and needs to investigate the incident to understand the scope, identify the attacker, and prevent further data breaches.

Tools:

- Splunk

Q1
Knowing which user account was compromised is essential for understanding the attacker's initial entry point into the environment. What is the username of the compromised user?

Query

index="aws_cloudtrail" eventSource="signin.amazonaws.com" responseElements.ConsoleLogin="Failure"

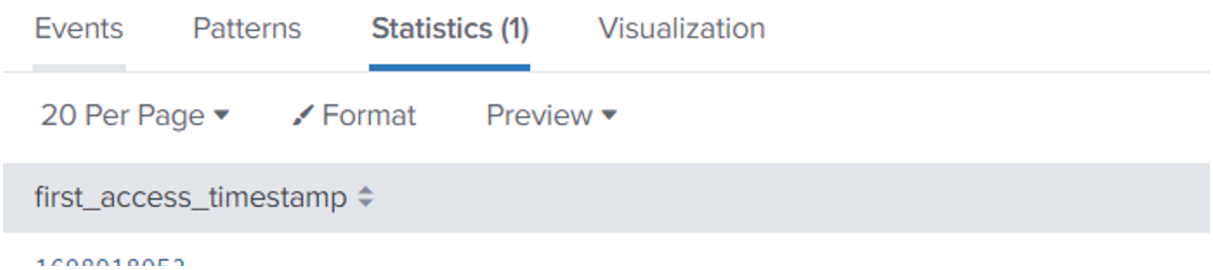
you will notice many failure authentication attempts

Q2
We must investigate the events following the initial compromise to understand

the attacker's motives. What's the UTC timestamp of the attacker's first access to an S3 object?

Query

index="aws_cloudtrail" eventName=GetObject userIdentity.userName=put it here
| stats min(_time) as first_access_timestamp

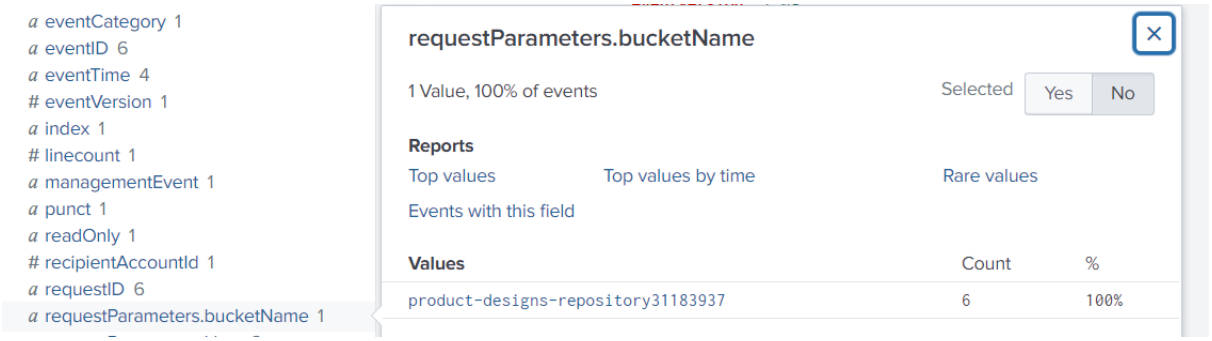


in unix
convert using
https://www.unixtimestamp.com/

Q3
Among the S3 buckets accessed by the attacker, one contains a DWG file. What is the name of this bucket?

Query

index="aws_cloudtrail" eventSource="s3.amazonaws.com"
| search requestParameters.key="*.dwg"



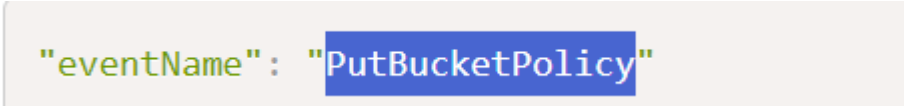
Q4

We've identified changes to a bucket's configuration that allowed public access, a significant security concern. What is the name of this particular S3 bucket?

Query

this link helped me https://community.splunk.com/t5/Splunk-Search/Splunk-query-to-check-for-S3-Buckets-in-AWS-using/m-p/571106

it gives me the EventName which i should search with



index="aws_cloudtrail" eventSource="s3.amazonaws.com" eventName=GetBucketPublicAccessBlock "userIdentity.userName"="put it here"

Q5

Creating a new user account is a common tactic attackers use to establish

persistence in a compromised environment. What is the username of the account created by the attacker?

Query

index="aws_cloudtrail" eventSource="iam.amazonaws.com" eventName="CreateUser"

Q6
Following account creation, the attacker added the account to a specific group. What is the name of the group to which the account was added?

Query

index="aws_cloudtrail" eventSource="iam.amazonaws.com" eventName="AddUserToGroup"
| search requestParameters.userName="put it here"
| stats values(requestParameters.groupName) as group_name by requestParameters.userName