Description:

-----------------

A prominent U.S.-based organization recently received an official notification from AWS alerting them to a potential security breach: one of their AWS access keys appears to have been compromised. Coincidentally, a subsequent internal security alert indicated that CloudTrail logging had been unexpectedly disabled. As a cybersecurity specialist, your task is to thoroughly investigate this series of events, and figure out the timeline of these events.

AWS CloudTrail and AWS CloudTrail Digest serve different purposes within the AWS ecosystem:

**AWS CloudTrail:**

AWS CloudTrail is a service that enables governance, compliance, and operational and risk auditing of your AWS account. It records AWS API calls and events for your account and delivers log files to an Amazon S3 bucket. CloudTrail provides visibility into user activity by recording actions taken on your account, which helps in proving compliance, improving security posture, and consolidating activity records across regions and accounts12.

**AWS CloudTrail Digest:**

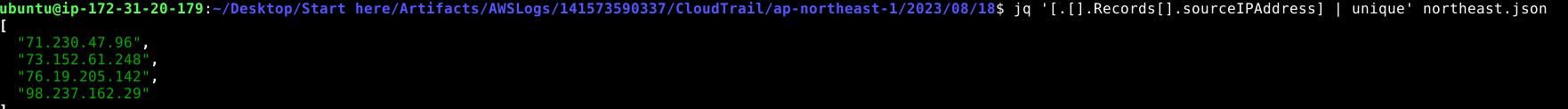
The CloudTrail Digest is a file that contains the names of the log files delivered to your Amazon S3 bucket during the last hour, the hash values for those log files, and the digital signature of the previous digest file. The digest file is used for validating the integrity of the log files and the digest file itself. It ensures that the log files have not been tampered with and provides a chain of custody for the log data3.

In summary, AWS CloudTrail records and delivers log files of API calls and events, while the CloudTrail Digest provides a mechanism to validate the integrity of those log files.



If it didn’t work go for after ungzip the files





Unique ips northeast & southeast & eu\_north & eu\_west

"71.230.47.96",

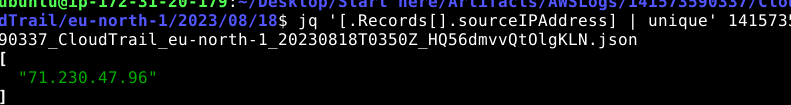
"73.152.61.248",

"76.19.205.142",

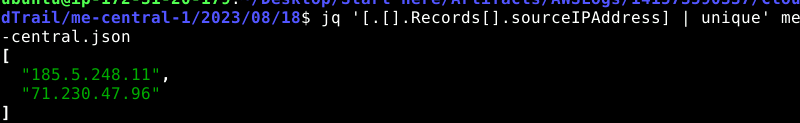
"98.237.162.29"

]

Eu\_north has only one record



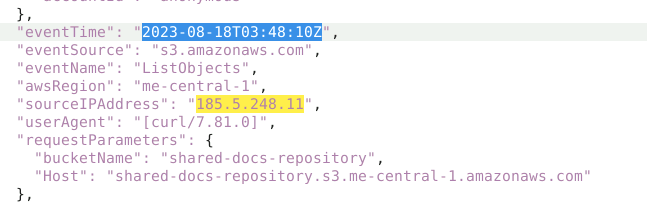
Inside the me-central trails we found the attacker’s ip address it is from Russia



1- To properly track the activities done by the attacker in the environment, you will need to determine the source of the attack. What is the attacker's IP address?

185.5.248.11

2- A timeline for the incident will help identify the gaps in your investigation. When did the attacker interact with the server for the first time?

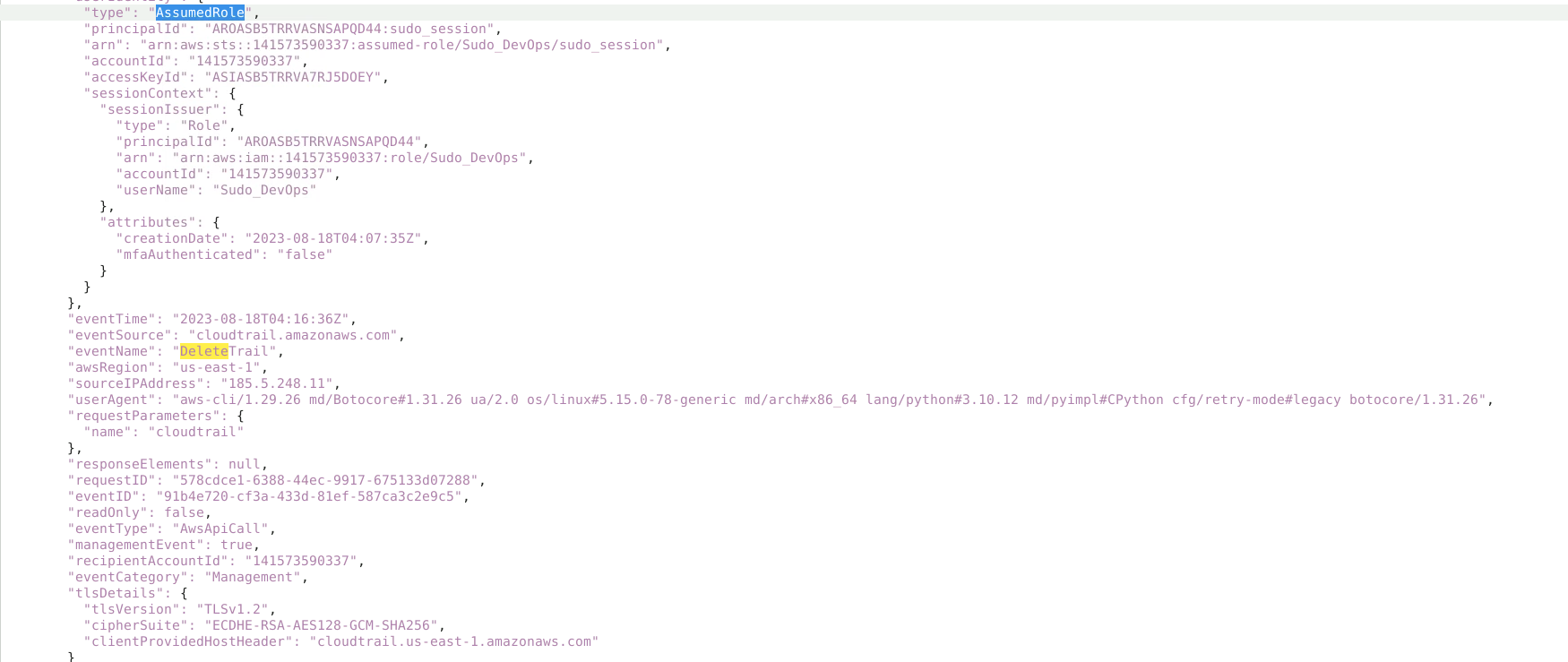


3- To ensure the environment is safe after the recent breach, identifying the attacker's entry point is essential. What is the exact file path from which the attacker retrieved the compromised user access key?



4- In a cloud environment, determining the user context can help assess the potential extent of damage based on the permissions and resources accessible to that user. What is the 'Type' of the user who disabled CloudTrail?

We will find this in the trails of us-east region



5-From the previous question, you determined the attacker's access type; now, you need to figure out what resources the attacker has access to. What is the name of the role the attacker takes advantage of to escalate his privilege in the environment?

From the previous screenshot you can notice the trail deletion was executed by username **Sudo\_DevOps**

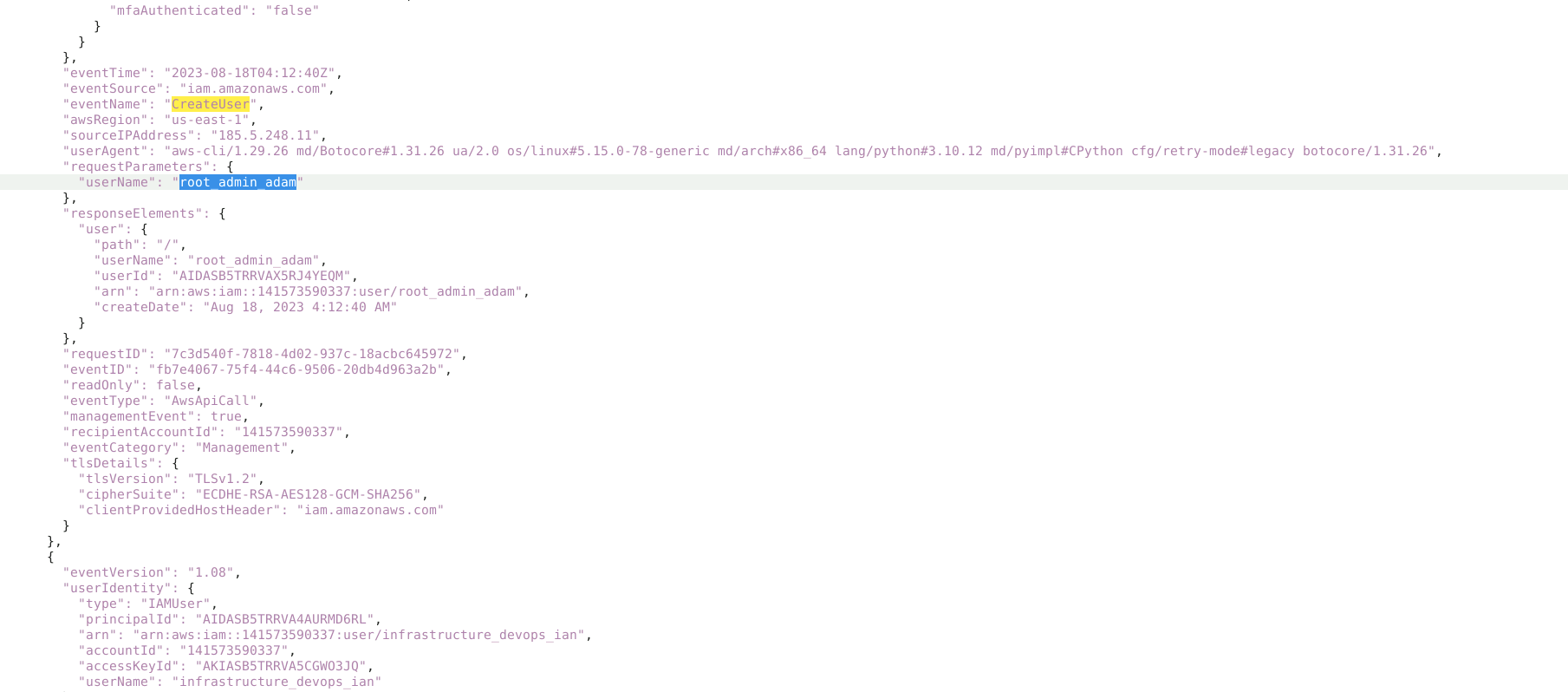
Also we have an event for AssumeRole confirms the same as well



6- In AWS, to enhance security, users are granted temporary access to specific resources when they assume a role. This action results in the creation of a session, characterized by a unique name and credentials. To trace the attacker's TTPs, can you identify the name of the session they initiated?



7- To effectively mitigate risks, it's crucial to determine whether the attacker attempted to establish persistence for ongoing access. Can you identify the name of the user the attacker created to maintain a foothold on the machine?



8- The attacker leveraged several techniques to access the account they created. What is the event name associated with their initial method?



9- What is the name of the group the attacker added the newly created user to?



10- Sophisticated threat actors often attempt to conceal their TTPs. Can you provide the exact time CloudTrail logging was disabled?

