Cloud Trail Log

We always use cloud trail log as DevOps engineers to monitor unauthorized AWS usage, such as unauthorized EC2 instances, Lambda functions or EC2 Spot bids.

CloudTrail delivers your log files to an Amazon S3 bucket that you specify when you create the trail.

CloudTrail typically delivers logs within an average of about 15 minutes of an API call. This time is not guaranteed. Review the AWS CloudTrail Service Level Agreement for more information.

Insights events are typically delivered to your bucket within 30 minutes of unusual activity.

After you enable Insights events for the first time, allow up to 36 hours to see the first Insights events, if unusual activity is detected.

The **Quarantine Policy** applied to the User protects the accounts by limiting permissions for high-risk AWS services.

Denies access to certain actions, applied by the AWS team if an IAM user's credentials have been compromised or exposed publicly. Do NOT remove this policy. Instead, please follow the instructions specified in the support case created for you regarding this event.

Application programming interfaces (APIs) are a way for one program to interact with another. API calls are the medium by which they interact. An API call, or API request, is a message sent to a server asking an API to provide a service or information.

What is an API Call? An API call is the process of a client application submitting a request to an API and that API retrieving the requested data from the external server or program and delivering it back to the client.