AWS CloudTrail announces CloudTrail Insights

Posted On: Nov 21, 2019

Today, AWS announces CloudTrail Insights, a new CloudTrail feature that helps customers identify unusual operational activity in their AWS accounts such as spikes in resource provisioning, bursts of AWS Identity and Access Management (IAM) actions, or gaps in periodic maintenance activity.

CloudTrail Insights is designed to automatically analyze management events from your CloudTrail trails to establish a baseline for normal behavior, and then raise issues by generating Insights events when it detects unusual patterns.

When CloudTrail Insights detects abnormal activity, it raises an event through dashboard views in the CloudTrail console, delivers the event to your Amazon Simple Storage Service (Amazon S3) bucket, and sends the event to Amazon CloudWatch Events. Optionally, you can send events to Amazon CloudWatch Logs. This lets you create alerts and integrate with existing event management and workflow systems.