SOFTPROM

aws partner network

Advanced Consulting Partner

Retail Competency

Solution Provider

AWS CloudTrail

Volodymyr Hryhorenko, Cloud Solutions Architect

AWS CloudTrail

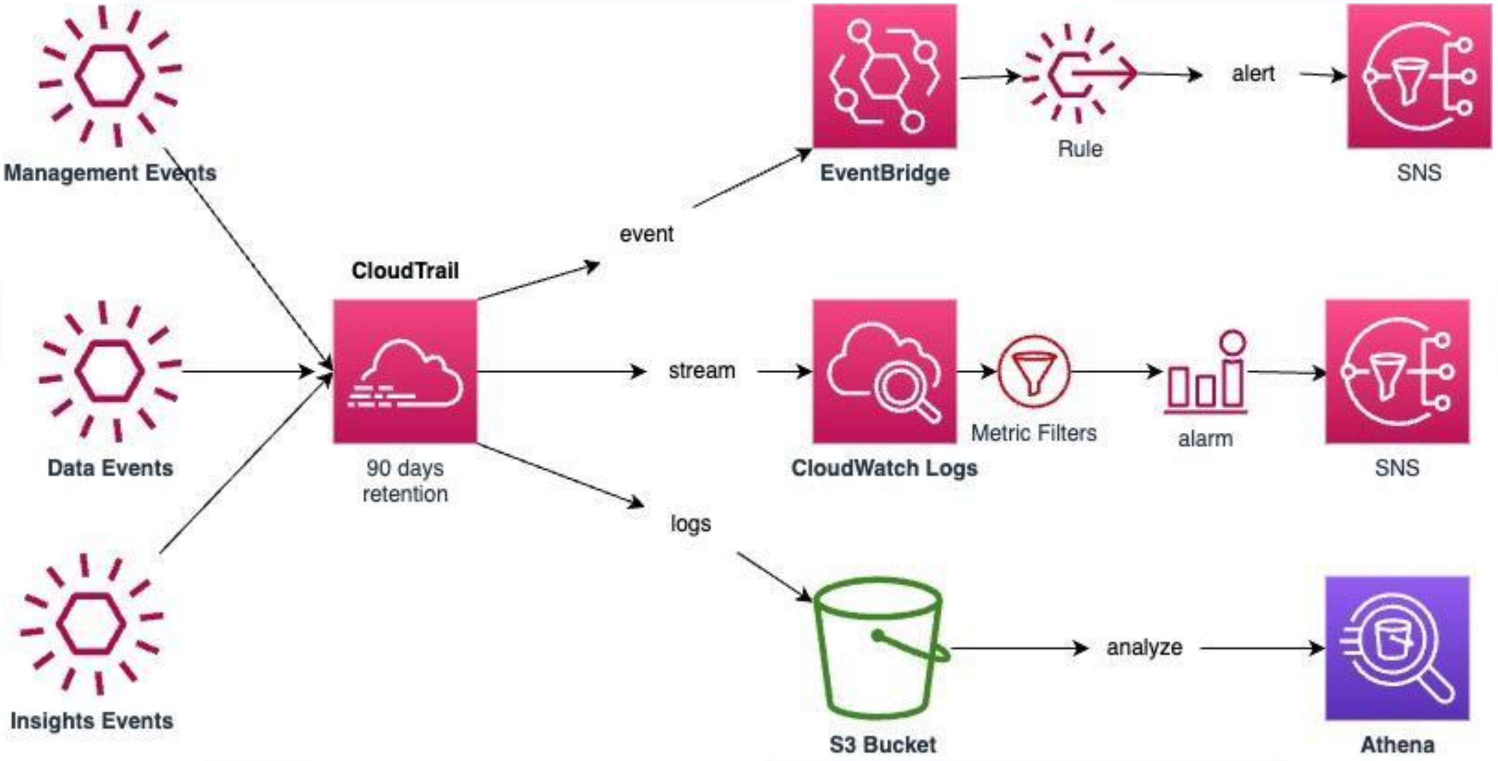
Provides governance, compliance and audit for your AWS Account

- CloudTrail is enabled by default!
- Get an history of events / API calls made within your AWS Account by:
  - Console
  - SDK
  - CLI

- Can put logs from CloudTrail into CloudWatch Logs or S3
- CloudTrail Lake
- A trail can be applied to All Regions (default) or a single Region
- If a resource is deleted in AWS, investigate CloudTrail first!

AWS CloudTrail Events

SOFTPROM | aws partner network



AWS CloudTrail Insights

Enable CloudTrail Insights to detect unusual activity in your account:

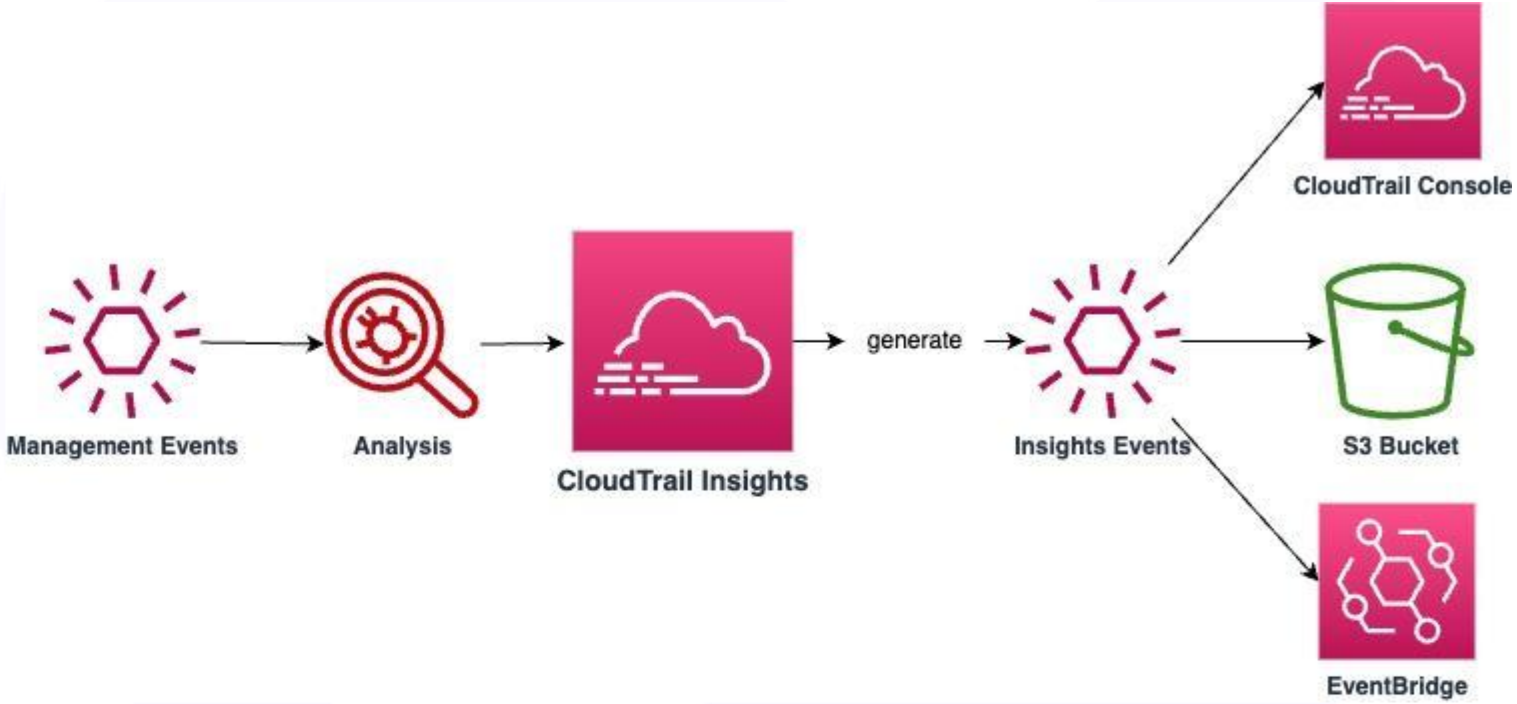
- Inaccurate resource provisioning
- Hitting service limits
- Bursts of AWS IAM actions
- Gaps in periodic maintenance activity

CloudTrail Insights analyzes normal management events to create a baseline
And then continuously analyzes write events to detect unusual patterns

- Anomalies appear in the CloudTrail console
- Event is sent to Amazon S3
- An EventBridge event is generated (for automation needs)

AWS CloudTrail Insights

SOFTPROM | aws partner network



CloudTrail:
How to react to events the fastest?

Overall, CloudTrail may take up to 15 minutes to deliver events

- EventBridge:
  - Can be triggered for any API call in CloudTrail
  - The fastest, most reactive way
- CloudTrail Delivery in CloudWatch Logs:
  - Events are streamed
  - Can perform a metric filter to analyze occurrences and detect anomalies
- CloudTrail Delivery in S3:
  - Events are delivered every 5 minutes
  - Possibility of analyzing logs integrity, deliver cross account, long-term storage

AWS CloudTrail Pricing

Free Tier

- **Event history - 90 days retention**
- **Lake -** During the 30-day free trial period, you'll have the following limits:
  - Ingest up to 5 GB of data
  - Scan up to 5 GB of data
  - Store data at no additional cost

Paid Tier

● **Trails**	
○ Management events delivered to Amazon S3	$2.00 per 100,000
○ Data events delivered to Amazon S3	$0.10 per 100,000
● **Insights**	
○ CloudTrail Insights	$0.35 per 100,000
● **Lake**	
○ Ingest and store	First 5 TB: $2.5 per GB Next 20 TB: $1 per GB Over 25 TB: $0.5 per GB