Identifying the Most Frequent AWS Events

Identifying the most frequent AWS events is important for a SOC Analyst because it helps establish a clear baseline, detect anomalies, and prioritize threat detection more effectively. To understand what the most common event types in AWS are, you need to run the following query.

Query - _sourceCategory=labs/aws/cloudtrail
| json field=_raw "eventName"
| count by eventName

#	eventName	_count
1	ReplaceNetworkAclEntry	4
2	Delete*	1
3	DescribeReservedInstancesOfferings	8
4	DescribeSnapshotTierStatus	2
5	DescribeReservedInstances	3
6	PutObjectAcl	6
7	ModifyDBCluster	73
8	CreateDBInstance	149

We can see the number of occurrences within the last 60 minutes. In order to sort the table in descending order, we have to add another line to the query. The whole query is now looking like that.

Query - _sourceCategory=labs/aws/cloudtrail
| json field=_raw "eventName"
| count by eventName
| sort by _count desc

#	eventName	_count
1	Invoke	382
2	CreateDBInstance	155
3	ListFunctions20150331	121
4	RestoreDBInstanceFromDBSnapshot	113
5	ModifyDBInstance	95
6	RebootDBInstance	89
7	ModifyDBCluster	73
8	CreateDBCluster	67
9	DeleteDBCluster	63

The most frequent AWS events now appear at the top of the table, providing instant visibility into the dominant activities occurring across your environment.

Finding the Most Active Users in AWS

Finding the most active users in AWS helps SOC analysts understand who's doing what on a daily basis. It makes it easier to spot abnormal behavior, like a normally quiet account suddenly making tons of changes. This could point to a compromised user or someone misusing their access. Keeping an eye on top users also helps you set smarter alerts and focus on accounts that really matter. To monitor users, we can use the following query.

Query - _sourceCategory=labs/aws/cloudtrail
| json field=_raw "userIdentity.userName"
| count by userIdentity.userName
| sort by _count desc

#	userIdentity.userName	_count
1	golang	140
2	michel	93
3	cloudhealthuser	90
4	kevin	69
5	James Gordon	60
6	aki	59
7	Ankit Goel	57
8	gosia	48

Operators used:

- Count by – Groups your log data by the field(s) you choose and counts how many records fall into each group. You can use it to break down and summarize activity, like the number of logins, events, users, or other key metrics, for easier analysis.
- Sort by – Sorts the results of your query based on the value of a specific field — usually _count. Use 'desc' to bring the highest values to the top, or 'asc' to highlight the smallest ones first.