Cloud Forensics Automatic Report (V3)

■ Event Summary

Total Events: 32
Average Risk Score: 30.8

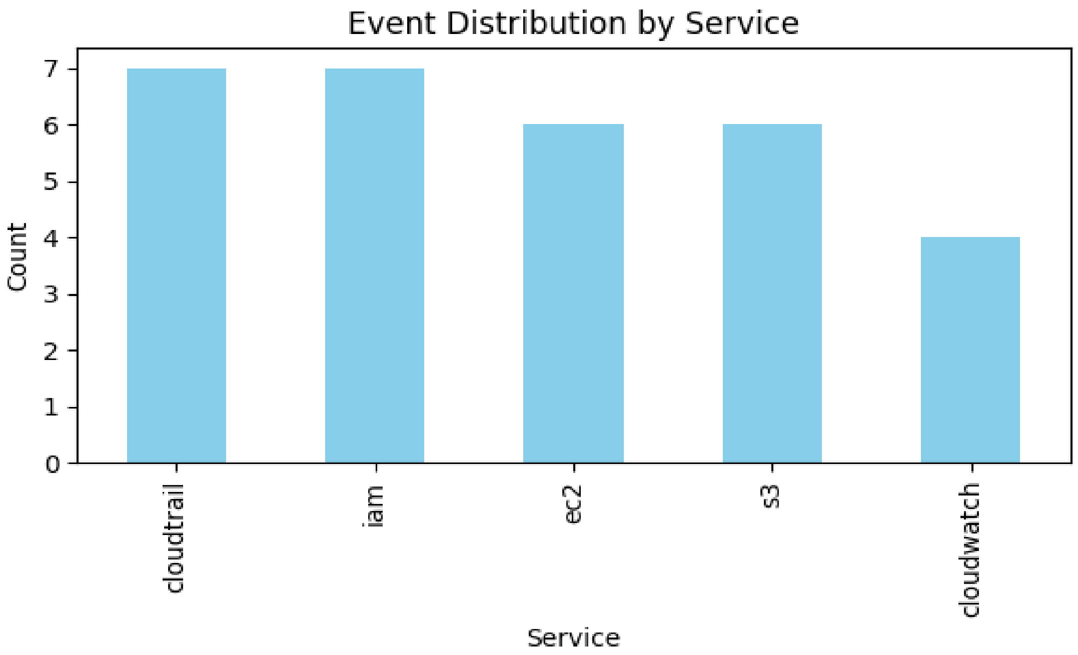
■ Anomaly Summary

Anomalous Users: cloudops (6 events), security_audit (6 events)
Anomalous Actions: StopInstances, AddUserToGroup, CreateRole, CreateUser, Unknown (High Frequency)

■ User Profiling Summary

User	Main Services	Active Hours	Total Events
Arnav	ec2	18 - 24	1
Mary	iam	18 - 24	1
Mateo	ec2	18 - 24	1
Nikki	ec2	18 - 24	1
Paulo	iam	18 - 24	1
Saanvi	iam	18 - 24	1
Terry	cloudtrail	18 - 24	1
Unknown	-	00 - 06	2
admin	iam, ec2	12 - 18	3
cloudops	cloudtrail, ec2	00 - 06	6
developer	cloudtrail, cloudwatch	00 - 06	3
security_audit	s3, cloudwatch	00 - 06	6
tester	s3, cloudwatch	06 - 12	3

■ Service-wise Event Distribution



Time	Actor	Service	Action	Result	Risk	Reason
2023-07-19T21:35:03Z	Terry	cloudtrail	UpdateTrail	TrailNotFoundException	90	CloudTrail configuration change (potential log tampering)
2025-10-28T00:19:09.291742Z	cloudops	cloudtrail	UpdateTrail	TrailNotFoundException	90	CloudTrail configuration change (potential log tampering)
2023-07-19T21:19:22Z	Arnav	ec2	CreateKeyPair	Allowed	80	EC2 SSH key creation (possible external access)
2023-07-19T21:25:09Z	Mary	iam	CreateUser	Allowed	70	IAM user created (new identity added)
2025-10-25T11:08:55.314422Z	cloudops	iam	CreateUser	Allowed	70	IAM user created (new identity added)

■ Recent 5 Events

Time	Actor	Service	Action	Result	Risk	Reason
2025-10-31T09:15:00Z	cloudops	cloudwatch	PutMetricData	Allowed	10	Normal event

Time	Actor	Service	Action	Result	Risk	Reason
2025 - 10 - 31T09:12:00 Z	tester	s3	CreateBucket	Allowed	10	Normal event
2025 - 10 - 31T02:32:55. 284323Z	security_audit	s3	CreateRole	Allowed	10	Normal event
2025 - 10 - 31T01:57:55. 282324Z	developer	cloudwatch	CreateRole	Allowed	10	Normal event
2025 - 10 - 31T01:27:55. 285333Z	cloudops	ec2	CreateRole	Allowed	10	Normal event

This report summarizes recent AWS CloudTrail events and highlights potentially risky actions based on defined detection rules.