Cloud Forensics Automatic Report (V4)

■ Event Summary

Total Events: 4693
Average Risk Score: 10.3

■ Anomaly Summary

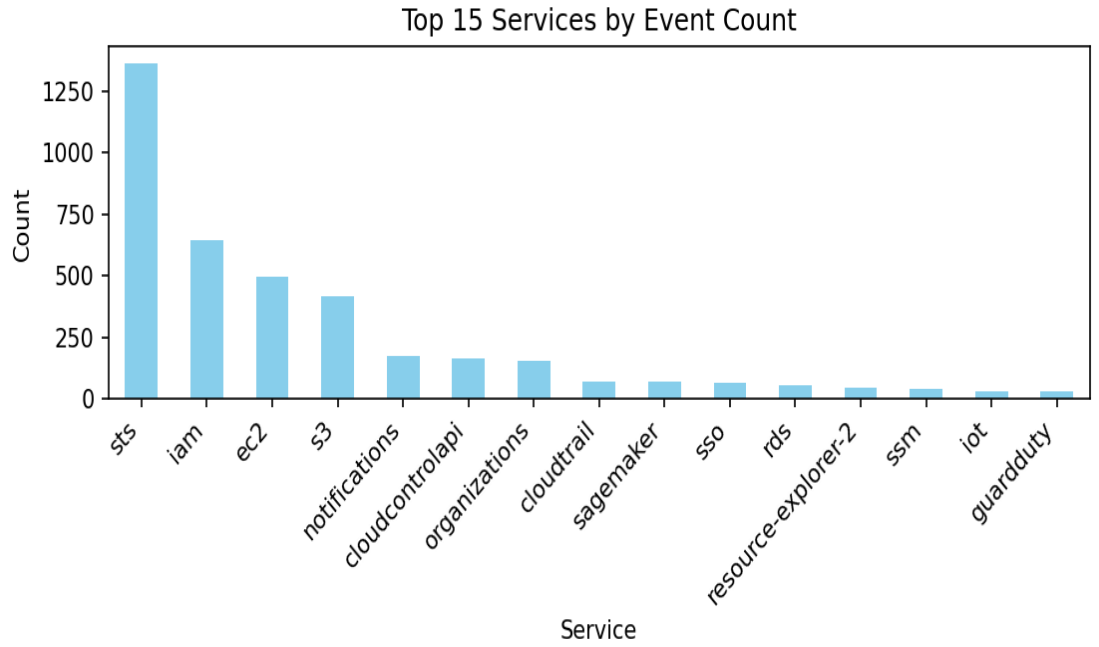
Anomalous Users: Unknown (1718 events), arn:aws:iam::518097206937:root (1679 events)
Anomalous Actions: AssumeRole, GetBucketAcl, ListResources, DescribeOrganization, ListPolicies (High Frequency)

■ 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	sts, s3	06 - 12	1718
arn:aws:iam::518097206937:root	iam, ec2	06 - 12	1679
cloudops	cloudwatch	06 - 12	1
cloudtrail - reader	sts	12 - 18	1
i - 033c2f7f2629541c5	ssm	06 - 12	1
i - 06eea5301b545340d	ssm	06 - 12	1
onboarding	resource - explorer - 2	06 - 12	3
resource - explorer - 2	cloudcontrolapi, ec2	06 - 12	1281

tester	s3	06 - 12	1

■ Service-wise Event Distribution



Time	Actor	Service	Action	Result	Risk	Reason
2023 - 07 - 19T21:35:03 Z	Terry	cloudtrail	UpdateTrail	TrailNotFoundException	90	CloudTrail configuration change (potential log tampering)
2023 - 07 - 19T21:19:22 Z	Arnav	ec2	CreateKeyPair	Allowed	80	EC2 SSH key creation (possible external access)
2025 - 11 - 20T11:21:18 Z	arn:aws:iam::518097206937:root	iam	CreateUser	Allowed	70	IAM user created (new identity added)
2025 - 11 - 20T11:09:44 Z	arn:aws:iam::518097206937:root	iam	CreateUser	Allowed	70	IAM user created (new identity added)

Time	Actor	Service	Action	Result	Risk	Reason
2025 - 11 - 20T11:43:14 Z	arn:aws:iam::518097206937:root	iam	CreateUser	Allowed	70	IAM user created (new identity added)

■ Recent 5 Events

Time	Actor	Service	Action	Result	Risk	Reason
2025 - 11 - 21T09:00:32 Z	arn:aws:iam::518097206937:root	notifications	ListManagedNotificationEvents	Allowed	10	Normal event
2025 - 11 - 21T08:58:32 Z	arn:aws:iam::518097206937:root	notifications	ListManagedNotificationEvents	Allowed	10	Normal event
2025 - 11 - 21T08:56:33 Z	arn:aws:iam::518097206937:root	organizations	DescribeOrganization	AWSOrganizationsNotInUseException	10	Normal event
2025 - 11 - 21T08:56:32 Z	arn:aws:iam::518097206937:root	notifications	ListManagedNotificationEvents	Allowed	10	Normal event
2025 - 11 - 21T08:56:32 Z	arn:aws:iam::518097206937:root	cloudtrail	ListEventDataStores	Allowed	10	Normal event

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