AWS Security Checklist Report

AWS Security Checklist - CloudTrail

Item	Description
Enable CloudTrail logging	Enable AWS CloudTrail logging to track changes made to your AWS account and resources.
Encrypt CloudTrail logs	Use server-side encryption (SSE) or client-side encryption to encrypt CloudTrail logs at rest.
Restrict access to CloudTrail logs	Limit access to CloudTrail logs to only authorized personnel, using IAM policies or bucket policies.
Monitor CloudTrail logs	Monitor CloudTrail logs for unusual activity, using services like Amazon CloudWatch or Amazon Athena.
Enable multi-factor authentication (MFA) for CloudTrail logging	Enable MFA for CloudTrail logging to prevent unauthorized changes to CloudTrail configuration.
Regularly review CloudTrail logs	Regularly review CloudTrail logs to identify and investigate any security or compliance issues.
Protect CloudTrail credentials	Protect CloudTrail credentials, including access keys and secret access keys, using best practices like rotation and secure storage.

This report has been generated by awscheck.fyi