AWS Security Checklist Report

AWS Security Checklist - Lambda

Item	Description
Use AWS Secrets Manager or AWS Systems Manager Parameter Store to store sensitive information	To prevent accidental exposure of sensitive information, use AWS Secrets Manager or AWS Systems Manager Parameter Store to store sensitive information such as passwords, API keys, and database connection strings.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Lambda functions. Restrict access to only the actions and resources that are necessary for the function to perform its intended actions.
Enable VPC access for your Lambda functions	Use Amazon Virtual Private Cloud (VPC) to isolate your Lambda functions from the public internet and to access resources in your own VPC.
Enable AWS X-Ray tracing	Enable AWS X-Ray tracing to monitor and troubleshoot your serverless application. X-Ray provides end-to-end tracing of requests and helps you identify performance bottlenecks and errors.
Use AWS Key Management Service to encrypt data in transit and at rest	Use AWS Key Management Service (KMS) to create and manage encryption keys that protect your data. Encrypt data in transit and at rest using KMS-managed keys.
Monitor and log function invocations	Use Amazon CloudWatch to monitor and log function invocations. Use CloudWatch Logs to store and analyze logs generated by your Lambda functions.
Use AWS Config to monitor resource configurations and compliance	Use AWS Config to monitor the configurations of your Lambda functions and their associated resources. Use Config rules to define compliance rules for your resources and to get notifications when they change.
Implement least privilege permissions for your Lambda functions	Use the principle of least privilege to assign permissions to your Lambda functions. Assign only the necessary permissions to access the required resources and actions.
Use environment variables to configure your Lambda functions	Use environment variables to pass configuration information to your Lambda functions. Store sensitive configuration information in AWS Secrets Manager or AWS Systems Manager Parameter Store.
Implement automated deployments for your Lambda functions	Use AWS CodeDeploy to automate the deployment of your Lambda functions. CodeDeploy can help you perform rolling deployments and automate the testing of your functions.
Test and monitor your Lambda functions	Use AWS Lambda built-in monitoring capabilities to monitor the health of your Lambda functions. Use AWS Lambda Test Events to test your functions in different scenarios.