# AWS Security Checklist Report

## AWS Security Checklist - EC2

| Item | Description |
|------|-------------|
| Use security groups | Create and configure security groups to control inbound and outbound traffic for your EC2 instances. |
| Enable monitoring | Enable CloudWatch monitoring to track the performance and status of your EC2 instances. |
| Create IAM roles | Create IAM roles to manage access to your EC2 instances and assign permissions for AWS resources and services. |
| Enable VPC Flow Logs | Enable VPC Flow Logs to monitor and capture information about IP traffic going to and from your EC2 instances in your VPC. |
| Implement Network ACLs | Use Network Access Control Lists (NACLs) to add an additional layer of security by controlling traffic at the subnet level. |
| Enable AWS Config | Enable AWS Config to continuously monitor and record your EC2 instances' configurations and evaluate them against best practices. |
| Encrypt EBS volumes | Enable encryption for your Elastic Block Store (EBS) volumes to protect your data at rest. |
| Enable instance metadata protection | Enable Instance Metadata Service Version 2 (IMDSv2) to protect against unauthorized access to the instance metadata. |
| Use dedicated tenancy | Use dedicated tenancy to launch EC2 instances on dedicated hardware for increased security and compliance. |
| Enable AWS Systems Manager | Use AWS Systems Manager to manage and automate tasks on your EC2 instances, such as patching and configuration management. |
| Regularly patch and update | Regularly apply security patches and updates to your EC2 instances and applications to reduce vulnerabilities. |
| Implement Amazon Inspector | Use Amazon Inspector to assess the security and compliance of your EC2 instances by identifying potential security issues. |
| Use Amazon GuardDuty | Enable Amazon GuardDuty to continuously monitor and detect threats to your EC2 instances and AWS accounts. |
| Enable Amazon Macie | Use Amazon Macie to discover, classify, and protect sensitive data stored in your EC2 instances. |
| Implement AWS WAF | Use AWS Web Application Firewall (WAF) to protect your web applications hosted on EC2 instances from common web exploits. |
| Enable AWS Shield | Enable AWS Shield to protect your EC2 instances from Distributed Denial of Service (DDoS) attacks. |