**AWS Security Checklist**

| **Threat** | | |  | **Mitigation** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **STRIDE** | **Potential Threat** | **Example  Threat Use Case** |  | **AWS Architectural Component and Strategies** | **AWS Tool and Service** | **Example Mitigation Use Case** |
| Spoofing | Users can access applications or AWS resources without authentication or with weak authentication  MFA is not enabled  Lack of Access Key rotation   Root account access key present | A malicious actor can break into an application that has no or weak authentication |  | AWS MFA  Credential Rotation | AWS Secret Manager | Enable MFA for Root account and IAM user  Rotate AWS User Access Key periodically  AWS Secret Manager for credential rotation,  Avoid long-term credentials  Root Account should not have/use access key |
| Public APIs are exposed with no or little authentication | A malicious actor can misuse the publicly exposed API that has no authentication |  | API Gateway  API Key  Identity provider | AWS KMS for key Management (Create, store, rotate) | Each service request should be authenticated at API Gateway with API Key and/or Token |
| Tampering | MITM- Data is eavesdropped and modified by a malicious actor during transmission | Data is eavesdropped and modified by a malicious actor during transmission and the receiver has no idea that the data has been altered. |  | TLS Certificate | Amazon Certificate Manager | Provision and deploy public and private TLS certificates using Amazon Certificate Manager |
| Server-side encryption is not enabled for S3 |  |  |  |  | S3 buckets should enforce Server-Side Encryption |
| Repudiation | No logging of important or sensitive activity | An internal or external malicious actor breaks into the system and withdraws funds but there is no record who performed that activity |  | Logging | AWS CloudWatch  VPC Flow Logs | Monitor and record network activity using AWS CloudWatch. |
| No auditing of credential modification | A malicious actor broke into the system and modified the credentials but there is no record of who performed that activity |  | Logging | AWS Config | Use AWS Config to automate credential auditing |
| No record of API or service consumption | A normal user (malicious actor ) gains access to Admin user API and consumes it but there is no record of who performed that activity |  | Logging | AWS CloudTrail | AWS CloudTrails  gives a log of API calls made against your account resources |
| Information Disclosure | Unencrypted data in transit can be stolen. | If an AWS user is malicious, the actor can eavesdrop on the data in transit. |  | Encryption | mTLS  VPN connections  HTTPS end-points | Data can be protected in transit by VPN and TLS (AWS built-in encryption).  Define VPN connections & HTTPS end-points in load balancers & CloudFront, |
| Hardcoded credentials or keys or any unsecured means of storing keys | If API keys or credentials are hardcoded in the source code then they can be exposed from the production application. |  | Use Vault | AWS KMS  AWS Secret Manager  AWS CloudHSM | Use KMS for key management (create, store, rotate)  Use Cloud HSM to store your own created keys |
| If users of lesser privilege have access to sensitive data or functionality, it can be abused. | A normal user can access data or functionality that is supposed to be for Admin only. |  | Access Control | AWS IAM | Use AWS IAM to begin with deny access for each user to each resource and then grant access as needed, based on job role.  Grant access as needed, Enforce separation of duty, |
| Sensitive data is stored in any Datastore (e.g. S3 bucket) in plain text. | S3 bucket stores the PII data such as email and Social insurance numbers of users in plain text |  | Encryption | Server-side encryption | Configure AWS services to encrypt all stored data by default |
| Unencrypted data transmitted across regions | Unencrypted data transmitted between multiple VPCs from different regions |  | VPC endpoints  AWS private link | AWS Private Link | Connecting multiple VPCs from different regions using AWS Private Link. |
| If data is transmitted, processed, and stored without any compliance consideration then sensitive data is prone to breach and exposure. | PCI DSS data is transmitted and stored in plain text |  | Compliance | AWS Artifact and AWS config | Use AWS Artifact and AWS config to detect non-compliance data transmission, processing and storage. |
| Denial of Service | DDOS attack via Brute force attack, credential stuffing, | The Network has a public subnet or end-point |  | WAF  Security Group  Network ACL | AWS Shield  AWS WAF  Amazon GuardDuty  AWS Security Hub | AWS WAF to protect Apps and APIs from attacks,  AWS Shield for DDOS protection  GuardDuty for threat detection and security visibility,  Security Hub for security best practices check & automated remediation support, |
|  |  |  | Leveraging multi-AWS account  Multiple-regions  Edge locations  Multiple VPC and data center | AWS Global Accelerator, | Use VPC to provision a logically isolated section of AWS Cloud (public and private subnets for isolation)  Use AWS Global Accelerator to direct traffic to the closest Edge location. |
| High network traffic impacts Application performance due to decreased response time and unavailable network latency | All user requests are piled up at one public end point while requests are not forwarded to other available end-points. |  | Load Balancing | Elastic load balancing  App Load Balancing  Network Load Balancing | The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application |
| An enormous number of API requests can significantly slow down the system | An application has millions of users which leads to a huge number of API requests per second. Servicing all those API requests will slow down the system and affect its performance. |  | Auto-Scaling | API Gateway | Use API Gateway to throttle requests to your APIs. |
| A large number of service requests to compute resources can significantly downgrade the performance | An application has millions of users which leads to a huge number of requests per second. Servicing all those requests will slow down the system and affect its performance. |  | Auto-Scaling,  Queues | Auto-scaling group.  Amazon Route 53 routing policies,  SQS, SNS | Elastic load balancing with EC2 and Auto-scaling group.  Bounce traffic between regions using Amazon Route 53 routing policies |
| An unfortunate security incident (accidental deletion) or hardware failure can make important data unavailable permanently. | The ISO 27000 security audit revealed the absence of a PII data back strategy. This caused non-compliance |  | Data Backup  Replication and restore | Amazon S3(cross-region replication)  AWS Backup  AWS DataSync  AWS Storage Gateway | Use AWS Backup to automate the backup process across Accounts.  Use AWS DataSync to automate moving large active data sets. |
| A Service is down or becomes unavailable | A successful brute force attack makes a service/server unavailable |  | Service backup and restore | Multi-Site (Active/Active)  Warm Stand By  Pilot light  AWS Elastic Disaster Recovery, | If Cost is not a problem and 0 downtime is an objective then choose Muti-site.  If longer downtime can be tolerated then choose Pilot-Flight.  Use AWS Elastic Disaster Recovery to replicate workload components and storage to backup across regions (disaster recovery region). |
| Retrieving frequently used data every time from the database can impact the application's performance | Delivering content to Web App users requires much of the latency for retrieving content such as images, and videos every time for each user request. |  | Caching | Redis  Amazon CloudFront  Amazon ElastiCache | Use Amazon CloudFront to cache content closer to the user  Accessing data from memory is orders of magnitude faster than accessing data from disk or SSD |
| Elevation of Privilege | Unorganized resources, policies, and responsibilities within AWS Account(s) | If there is no restriction on who can access an AWS service or resource then anybody can access any resource. |  | AWS Account  AWS Organization  Organizational Unit | Service Control Policy  AWS Control Tower | Using SCP, you can limit the AWS services, resources, and individual API operations that users and roles in each member account can access |
| Unorganized  resources, policies, and responsibilities for AWS users | Do we have proper IAM defined for the users & resources otherwise unauthorized user can perform an important action |  | IAM Users  AWS IAM identity center | Roles, Groups,  IAM policy  Identity-based policy  Bucket policy  IAM Access analyzer  Amazon Cognito  AWZ STS | Cross-account access management.  Use AWS IAM to begin with deny access for each user to each resource and then grant access as needed, based on job role.  Use Secret Access Keys and determine who can use keys with key policies. |