Security Engineering on AWS – Key Concepts

Module 1 – Security Overview

- Security engineering in the AWS Cloud
  - Responsibility varies based on AWS usage
  - MSOs and MSPs / MSO responsibility model
  - Security principles in the cloud
    - Automation / Visibility / Auditability
    - Agility / Controllability
  - Identity and accounts
    - Single AWS account / Multiple AWS accounts
    - Single sign-on (SSO) mechanisms
    - Federation and identity providers
    - Authentication, authorization, and auditing
  - Data and infrastructure protection
    - Data integrity / Encryption / VPC security
    - Denial of service / Web application security
  - Monitor, detect, and respond
    - Log / Alert / Investigate / Respond / Monitor
- Threat modeling
  - Core aspects of security
    - Confidentiality / Integrity / Availability
  - Threat modeling for your workload - STRIDE framework
  - Assess risk – Assets / Vulnerabilities / Threats

Module 2 – Access and Authorizations on AWS

- Accessing the AWS Cloud
  - Securing APIs through signing
  - IAM components and flow
    - IAM roles – Trust / Permission policy
  - Getting started with IAM
    - 1. AWS account root user
    - 2. IAM entities – user / group / role / policy
    - 3. User access keys - *for* AWS CLI and AWS SDK
- IAM Threat: Compromised long-term credentials
  - AWS Security Token Service use cases
    - Identity federation – Enterprise / Web
    - Cross-account access
    - IAM roles
  - AWS STS API calls
    - AssumeRole
    - AssumeRoleWithSAML
    - AssumeRoleWithWebIdentity
    - GetFederationToken
    - GetSessionToken – Enforce MFA for AWS CLI
  - IAM Roles Anywhere
- IAM Threat: Overly permissive and misconfigured policies
  - Policy types
    - Identity-based policies
    - Resource-based policies
    - Permission boundaries
    - Session policies
    - Organizational SCPs
  - IAM policy types
    - Managed policies – AWS / Customer
    - Inline policies
  - IAM policy operation and analysis
    - IAM policy elements
    - Testing with IAM Policy Simulator
  - Delegating and constraining permissions
    - + Permission boundaries
  - Overly permissive and misconfigured policies
    - + Session policies
- IAM Threat: Anomalous IAM entity behavior
  - API / non-API logging with CloudTrail
    - Log consolidation
    - Log file integrity
  - More visibility for non-API events
    - IAM Access Analyzer
    - Credential report

Module 3 – Account Management and Provisioning on AWS

- Managing Multiple AWS Accounts
  - Security challenges in a multi-account environment
    - Many teams
    - Isolation
    - Security controls
    - Business process
  - AWS Organizations
    - Organizational Units (OUs)
    - Service control policies (SCPs)
  - AWS Control Tower - governance at scale
    - Landing zone components
      - AWS Organizations
      - IAM Identity Center
      - CloudTrail and AWS Config
      - Preventive control (active) – SCP
      - Detective control (passive) – Config rules
      - Amazon CloudWatch alarms and events
      - GuardDuty
  - AWS Resource Access Manager (AWS RAM)
- Federation and IAM Identity Center
  - Identity federation, Federated users
  - AWS IAM Identity Center
    - AWS access through permission sets
  - AWS Directory Service
    - Simple AD
    - AD Connector
    - AWS Managed Microsoft AD
  - Amazon Cognito and web identity providers
    - User pool
      - Adaptive authentication
    - Identity pools

Module 4 – Managing Keys and Secrets on AWS

- AWS KMS
  - KMS key types
    - Symmetric keys
    - Asymmetric keys
    - HMAC keys
  - Envelope encryption
  - Protecting your keys
    - Policies (resource-based permissions)
    - Grants (temporary or more granular permissions)
  - Importing keys
  - Key rotation
  - Multi-Region keys
  - + Multi-factor authentication
- CloudHSM
  - Separation of duties – AWS vs. User
  - AWS KMS custom key stores with CloudHSM
- AWS Certificate Manager - Protecting data in transit
  - AWS Private CA
- AWS Secrets Manager
  - Rotating secrets (+ Lambda)
  - Protecting secrets with resource-based policies
  - Protecting secrets with identity-based policies
  - vs. Parameter Store

Security Engineering on AWS – Key Concepts

Module 5 – Data Security

- Protecting Data: Amazon S3
  - Amazon Macie
    - + managed / custom data identifiers
  - Data encryption for Amazon S3
    - Amazon S3 SSE
      - SSE-S3 (default) / SSE-C / SSE-KMS
  - Access control for Amazon S3
    - Legacy protection – ACLs
      - Object ACLs (resource-based)
      - Bucket ACLs (resource-based)
    - Amazon S3 resource protection with policies
      - Bucket policies (resource-based)
      - IAM policies (identity-based)
    - Amazon S3 access points
    - Amazon S3 Block Public Access
    - Access Analyzer for Amazon S3
  - Data resiliency for Amazon S3
    - Bucket replication
    - Amazon S3 versioning
    - S3 Object Lock - Write Once Read Many (WORM)
- Protecting Data: Amazon RDS
  - Protection in transit / at rest
  - Network isolation (Subnet, IP, SG, NACL)
  - Access Control
    - *to* Amazon RDS service (+ IAM)
    - *to* database
  - Cross-region encryption - Read replicas, Snapshots
- Protecting Data: DynamoDB
  - Protection in transit / at rest
  - Fine-grained access control
  - Cross-Region encryption - Global tables
- Protecting Data: EBS
  - Encryption
- Protecting Data: Amazon S3 Glacier
  - Vault Lock

Module 6 – Infrastructure and Edge Protection

- Protecting infrastructure inside the VPC
  - Security Group vs. Network Access Control List (ACL)
  - AWS Network Firewall
    - AWS Managed Threat Signatures
  - Traffic flows in your VPC
    - VPC peering / Inter-Region VPC peering
- VPC endpoints
  - Interface endpoint (powered by AWS PrivateLink)
    - *by* Security Group
    - *by* Endpoint policy
    - + Direct Connect for hybrid environments
  - Gateway endpoint (S3, DynamoDB)
    - *by* Endpoint policy
- Reliable and controlled access
  - Elastic Load Balancer
    - ELB types
      - Application Load Balancer
      - Network Load Balancer
      - Classic Load Balancer
      - Gateway Load Balancer
    - Internal and internet-facing (+ Security Group)
    - Configuring TLS offloading
  - Amazon CloudFront (+ Shield and AWS WAF)
    - Restricting access
      - origin access identities (OAIs) for S3 buckets
      - security group of origin instances
      - signed URLs or signed cookies
    - Access logs
  - Amazon Route 53
    - Anycast striping / Shuffle sharding

Module 7 – Monitoring and Collecting Logs on AWS

- Monitoring to identify threats
  - Define a baseline
  - Amazon Detective
    - *from* AWS CloudTrail logs
    - *from* VPC Flow Logs
    - *from* Amazon GuardDuty findings
    - *from* Amazon EKS audit logs (optional)
  - AWS Config
    - Configuration item relationships
    - AWS Config rules
      - AWS managed rules / Custom rules (+ Lambda)
    - AWS Config conformance pack (+ AWS Organizations)
- Monitoring using logs
  - Building a logging strategy
    - Central, secure storage / Log it all / Keep logs
  - CloudWatch Logs
  - VPC Flow logs
    - Using custom fields
  - Elastic load balancer access logs
  - Amazon S3 server access logs
  - AWS CloudTrail
- Visibility and Alarms with CloudWatch
  - Using events (event, rules, target)
  - CloudWatch Alarms
    - Metric alarms / Composite alarms
    - Using CloudWatch anomaly detection
- Log Analytics
  - Amazon Kinesis Data Streams / Firehose / Analytics
  - Amazon Security Lake
  - Amazon Athena
  - Amazon OpenSearch Service
  - The AWS Centralized Logging solution
- Mirroring Traffic for Fine-Grained Analysis
  - VPC Traffic Mirroring
    - session: source / filter / target (GWLB, NLB, ENI)

Module 8 – Responding to Threats

- Incident response
  - Security Incident Response Simulations (SIRS)
    - + penetration testing or scanning
  - Security Hub
    - insights
    - automated responses with Amazon EventBridge
    - automated response and remediation solution
- Threat detection
  - Amazon Inspector
  - GuardDuty
    - Detection categories
      - Reconnaissance
      - Instance compromise
      - Account compromise
      - Bucket compromise
    - Customize monitoring scope
      - Trusted IP list / Threat list
    - Avoiding alert fatigue
  - Detective
- Respond to security findings
  - AWS tools for incident response
    - AWS Trusted Advisor
    - AWS CloudFormation
    - AWS Service Catalog
  - Incident response domains
    - Infrastructure
      - Protect / Isolate / Preserve
      - Automated Forensics Orchestrator for EC2
    - Service
      - Exposed access keys