Cantril Review – Security, Deployment, & Operations

AWS Secrets Manager vs Parameter Store

* Primary difference is that Secrets Manager periodically triggers a Lambda function that automatically rotates secrets

AWS Secrets Manager

* It does share functionality with Parameter Store
* Designed for secrets – Passwords, API Keys
* Usable via Console, CLI, API, or SDK’s (integration)
* Supports automatic rotation – this uses Lambda
* Directly integrates with some AWS products – ex. RDS
* Encrypted at rest
* IAM access
* Auto Rotation

Application Layer (L7) Firewall

* A web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources

AWS Shield

* AWS Shield Standard & Advanced – DDOS Protection
* Shield Standard is FREE
* Shield Advanced has a cost
* Network Volumetric Attacks (L3) – Saturate Capacity
* Network Protocol Attacks (L4) – TCP SYN Flood
* In addition to protocol attacks, bad actors can leave connections open, preventing new ones
* L4 can also have a volumetric component
* Application Layer Attacks (L7) – e.g., web request floods
  + Query.php?search=all\_the\_cat\_images\_ever
* Shield Standard
  + Free for all AWS Customers
  + Protection at the perimeter
  + Region/VPC or the AWS Edge
  + Common Network (L3) or Transport (L4) layer attacks
  + Best protection using R53, CloudFront, and AWS Global Accelerator
* Shield Advanced
  + 3,000 per month (per ORG), 1 year lock-in + data (OUT) / m
  + Protects
    - CloudFront
    - R53
    - Global Accelerator
    - Anything associated with EIPs – EC2
    - ALBs
    - CLBs
    - NLBs
    - Not Automatic – must be explicitly enabled in Shield Advanced or AWS Firewall Manager Advanced Policy
    - Cost Protection – EC2 scaling for unmitigated attacks
    - Proactive engagement & AWS Shield Response Team (SRT)
    - Key Features –
      * WAF Integration – includes basic AWS WAF fees for web ACLs, rules, and web requests
      * Application Layer (L7) DDOS Protection (uses WAF)
      * Real time visibility of DDOS events and attacks
      * Health-based detection – application specific checks, used by proactive engagement team
      * Protection groups

CloudHSM vs. KMS

* KMS is AWS Managed – Shared but separated
* HSM is True “Single Tenant” Hardware Security Module (HSM(
  + AWS Provisioned – fully customer managed
  + HSM - Fully FIPS 140-2 Level 3
  + KMS is L2 Overall, some L3
* HSM uses Industry Standard APIs (KMS uses AWS)
  + PKCS#11
  + Java Cryptography Extensions (JCE)
  + Microsoft CryptoNG (CNG) Libraries
* KMS can use CloudHSM as a custom key store – CloudHSM integration with KMS
* HSMs operate in an AWS managed HSM VPC
  + ENIs are added to customer VPC
* HSMs keep keys and policies in sync when nodes are added or removed
* EC2 instances require AWS CloudHSM Client installed
* AWS Provision HSM but have NO access to secure area where key material is held
* CloudHSM Use Cases
  + By default – NO native AWS integration – e.g., no S3 SSE
  + Offload the SSL/TLS Processing for Web Servers
  + Enable Transparent Data Encryption (TDE) for Oracle Databases
  + Protect the Private Keys for an Issue Certificate Authoring (CA)

AWS Config

* Two primary functions
  + Record configuration changes over time on resources
  + Auditing of changes, compliance with standards
* Does NOT prevent changes happening – no protection
* Regional Service – supports cross-region and cross-account aggregation
* Changes can generate SNS notifications and near-realtime events via EventBridge & Lambda
* All information is stored regionally is an S3 config bucket
* Resources are evaluated against config rules – either AWS Managed or Custom (using Lambda)
* EventBridge can invoke Lambda functions based on the AWS Config events for automatic resource remediation

Amazon Macie

* Data Security and Data Privacy Service
* Discover, Monitor, and Protect Data – stored in S3 Buckets
* Automated discovery of data – PII, PHI, Finance
* Managed Data Identifiers – Built in – ML/Patterns
* Custom Data Identifiers – Proprietary – Regex Based
* Integrates – With Security Hub & “finding events” to EventBridge
* Centrally Manage – either via AWS ORG or one Macie Account Inviting
* Amazon Macie – Identifiers
  + Managed data identifiers – maintained by AWS
    - Growing list of common sensitive data types
    - Credentials, finance, Health, personal identifiers
  + Custom data identifiers – created by you
  + Regex – defines a ‘pattern’ to match in data – e.g. [A-Z]-\d{8}
  + Keywords – optional sequences that need to be in proximity to regex match
  + Maximum Match Distance – how close keywords are to regex pattern
  + Ignore Words – if regex match contains ignore words, it’s ignored
* Amazon Macie - Findings
  + Policy Findings or Sensitive Data Findings

Note –

* Shield Standard is automatically provided with the following services
  + CloudFront
  + Route53
* Shield protects against what type of attack – DDOS
* WAF Provided protections
  + Layer 7 attacks
  + SQL Injection
  + Cross-Site Scripting
* WAF can be added to
  + CloudFront
  + API Gateway
  + ALB
* The main feature which Secrets Manager provides over SSM Parameter store is Password Rotation