Well-Architected Bootcamp 2020 Taipei
Security Pillar

Bob Yeh, Solutions Architect, Amazon Web Services

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Resources:

Website:

https://aws.amazon.com/architecture/well-architected/

Whitepaper

Resources:

HTML Version of Security Pillar:

https://wa.aws.amazon.com/wat.pillar.security.en.html#sec.security

Design Principal:

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Prepare for security events

aws

Definitions:

- Identity and access management
- Detective controls
- Infrastructure protection
- Data protection
- Incident response

Identity and Access Management

- Protecting AWS credentials
  - How do you protect your Root Account?
  - How do you assign your IAM Users, Groups? How about the API/CLI access?
  - Did you create Appropriate Policies?
- Fine-grained authorization
  - Least privilege practice
  - IAM Role for resources

Identity and Access Management

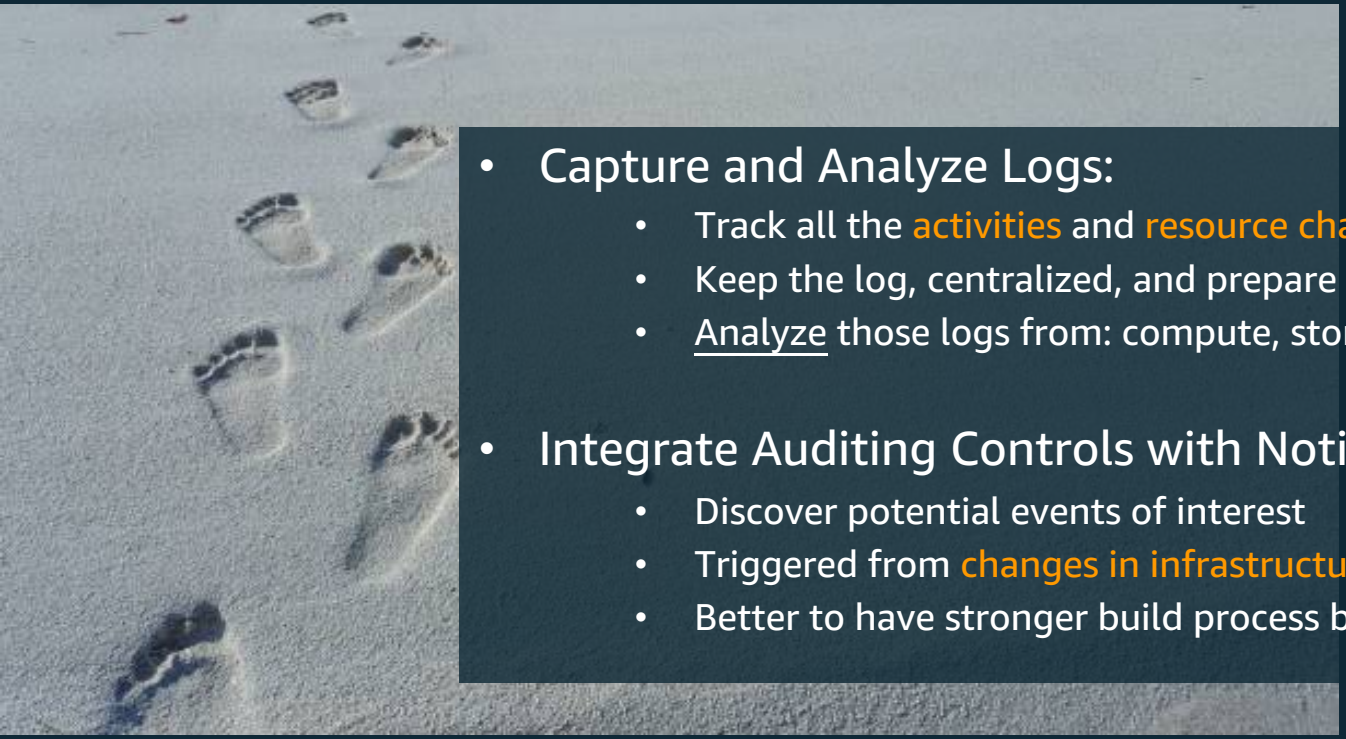
- Protecting AWS credentials
  - MFA for Root Account
  - MFA for critical API Call
  - IAM
  - IAM instance profiles for EC2 instances
  - AWS STS

- Fine-grained authorization
  - IAM, IAM Role
  - AWS Organizations

Definitions:

- Identity and access management
- Detective controls
- Infrastructure protection
- Data protection
- Incident response

Detective Controls



- Capture and Analyze Logs:
  - Track all the activities and resource changes on your cloud env
  - Keep the log, centralized, and prepare for analyze
  - Analyze those logs from: compute, storage, applications
- Integrate Auditing Controls with Notification and Workflow:
  - Discover potential events of interest
  - Triggered from changes in infrastructure
  - Better to have stronger build process before production

aws

Detective Controls

- Capture and Analyze Logs:
  - Capture: CloudTrial, AWS Config
  - Store: CloudWatch Logs, S3, Glacier
  - Analyze: Elasticsearch Service, EMR, Athena

- Integrate Auditing Controls with Notification and Workflow:
  - CloudWatch, CloudWatch Events
  - AWS Config Rules
  - CloudWatch API & AWS SDKs
  - Inspector

Definitions:

- Identity and access management
- Detective controls
- **Infrastructure protection**
- Data protection
- Incident response

Infrastructure Protection

- Protecting network and host-level boundaries:
  - How you provide isolation and boundaries for resource?
  - How to design your network topology?
  - How to protect your network access?
  - What will you do, if you have hybrid cloud?
- System(OS) security configuration and maintenance
  - How to manage your system security configuration?
  - How to make sure your system is secure?
  - Do you applied Least-privilege approach, in your system?
- Enforcing service-level protection
  - Who can access service-endpoints? And how?
  - Who can access the resource of this service? And how?
  - Did you prevent all the possible data leak?

Infrastructure Protection

- Protecting network and host-level boundaries:
  - VPC
  - Security Group
  - NetACL
  - DirectConnect
- System security configuration and maintenance
  - VPC Security Group
  - Amazon Inspector
  - Systems Manager
    (Run Command, State Manager, Inventory, Parameter Store, Patch Manager)
- Enforcing service-level protection
  - IAM
  - AWS KMS allows you to set policies on the individual key
  - Amazon S3 allows you to set bucket policies for each S3 bucket.

Definitions:

- Identity and access management
- Detective controls
- Infrastructure protection
- **Data protection**
- Incident response

Data Protection

- Data Classification
  - Categorize organizational data based on levels of sensitivity
  - Manage appropriate data classification system with different requirement level
  - Public data? Internal data? HIPPA PHI?
- Encryption/tokenization
  - Protect your content against unauthorized user and unnecessary explosure.
- Protecting data at rest
- Protecting data in transit
- Data backup/replication/recovery
  - Against the deletion or destruction of data
  - Ensure continued business operations

Data Protection

- Data Classification
  - Resource Tag
  - Detect abnormal access → Amazon Macie
  - AWS KMS
- Encryption/tokenization
  - AWS KMS
  - AWS CloudHSM
  - Amazon DynamoDB
- Protecting data at rest
  - AWS KMS
  - AWS S3, EBS, Glacier all support KMS

Data Protection

- Protecting data in transit
  - AWS Certificate Manager (ACM)
  - ELB Classic Load Balancers/ Application Load Balancers
  - Amazon CloudFront
  - AWS Shield
  - AWS WAF
- Data backup/replication/recovery
  - Amazon S3
  - Amazon S3 Cross-Region Replication
  - Amazon S3 Lifecycle polices and versioning

Definitions:

- Identity and access management
- Detective controls
- Infrastructure protection
- Data protection
- Incident response

Incident Response

Incident Response

- What is “incident”?

- Clean Room
    - Maintain situational awareness of incident
    - Describe your resource with Tag. (Whom to response?)
    - How to get access for the right people during an incident?
    - How to clean a same environment to investigate incident/reproduce defect?

Incident Response

- Clean Room
  - IAM should be used to grant appropriate authorization to incident response teams
  - AWS CloudFormation
  - EC2 APIs
  - AWS Step Functions

Q: How are you protecting access to and use of the AWS root account credentials??

No MFA on Root

Root Actively Used

MFA and Minimal Use of Root

No Use of Root

Q: How are you classifying your data?

No Data Classification Schema

Data Not Classified

Using Data Classification Schema

All Data Treated as Sensitive

Q&A

Thank you!