SECURED INFRASTRUCTURE & SECURITY CONTROLS DEMO

Presented to: Deloitte Cyber Center
Directors & Managers

Objective: Demonstrate a secure AWS environment deployed via Infrastructure as Code (IaC) in alignment with NIST CSF v1.1

Presented By Zach Almog

Goals

- DEVELOP & PRESENT:
  - SLIDE DECK DEMONSTRATING A SECURE AWS ENVIRONMENT
- PROCESS:
  - OUTLINE STEPS ALIGNING WITH NIST CSF (PROTECT FUNCTION)
- DEMO:
  - AWS-BASED SOLUTION (LAMBDA, S3, IAM)
  - IAC DEPLOYMENT (CLOUDFORMATION)
  - SECURITY CONTROLS DEMONSTRATION (LOGGING, ENCRYPTION, LEAST PRIVILEGE)

Approach & Tools

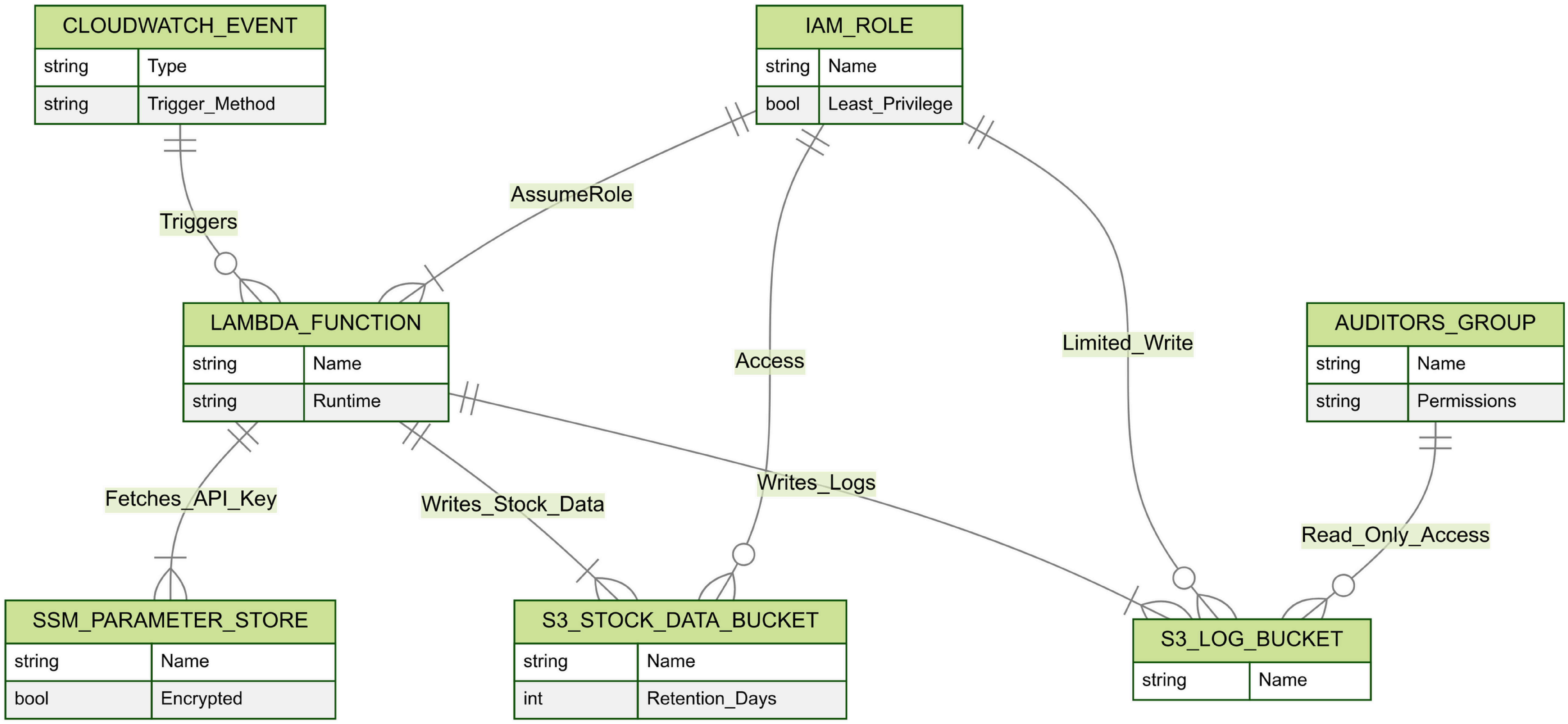
- **Framework: NIST Cybersecurity Framework v1.1**

- **Selected Subcategories:**
  - **PR.PT-1 (Audit/log records)**
  - **PR.DS-1 (Data-at-rest protection)**
  - **PR.AC-3 (Remote access management)**

- **AWS Services:**
  - **Lambda for stock data retrieval**
  - **S3 for data & log storage**
  - **IAM for least-privilege roles/groups**
  - **SSM Parameter Store for secret management**
  - **IaC: AWS CloudFormation (GitHub: almogzach/deloitte)**

Architecture & Demo Flow

- Lambda Function
- Fetches stock prices using an API key in SSM Parameter Store
- Writes data to StockDataBucket
- S3 Buckets
- StockDataBucket for fetched data
- LogBucket for Lambda logs
- IAM & Auditors
- Least-privilege role for Lambda (S3 + SSM access only)
- AuditorsGroup read-only access to LogBucket
- Encryption
- Server-side encryption (SSE-S3) for data-at-rest
- No plaintext secrets (API key in SSM Parameter Store)


CLOUDWATCH_EVENT
string Type
string Trigger_Method
IAM_ROLE
string Name
bool Least_Privilege
Triggers
AssumeRole
LAMBDA_FUNCTION
string Name
string Runtime
Access
Limited_Write
AUDITORS_GROUP
string Name
string Permissions
Fetches_API_Key
Writes_Stock_Data
Writes_Logs
Read_Only_Access
SSM_PARAMETER_STORE
string Name
bool Encrypted
S3_STOCK_DATA_BUCKET
string Name
int Retention_Days
S3_LOG_BUCKET
string Name

NIST CSF Controls Implementation

- **PR.PT-1 (Audit/Log Records)**
    - **CloudWatch triggers Lambda**
    - **Logs stored in LogBucket**
    - **AuditorsGroup can review logs regularly (segregation of duties)**
- **PR.DS-1 (Data-at-Rest Protection)**
    - **S3 server-side encryption**
    - **API key secured in SSM Parameter Store**
- **PR.AC-3 (Remote Access Management)**
    - **Least-privilege IAM role for Lambda**
    - **Read-only policy for auditors**

Results & Next Steps

- Results:
  - Secure AWS environment deployed via CloudFormation
  - Logging, encryption, and access control aligned with NIST CSF

- Next Steps:
  - Integrate with more services (e.g., EC2, VPC)
  - Add CI/CD pipelines with automated security checks
  - Expand monitoring with AWS Security Hub, GuardDuty, etc.

Q&A

- Git Repository: GitHub: almogzach/deloitte
- AWS Console Demo (S3, Lambda, IAM, CloudWatch)
- Contact: [Zach Almog / zalmog@gmail.com]

Thank you for your time!