Securing AWS Infrastructure

the Well-Architectured Way

Agenda

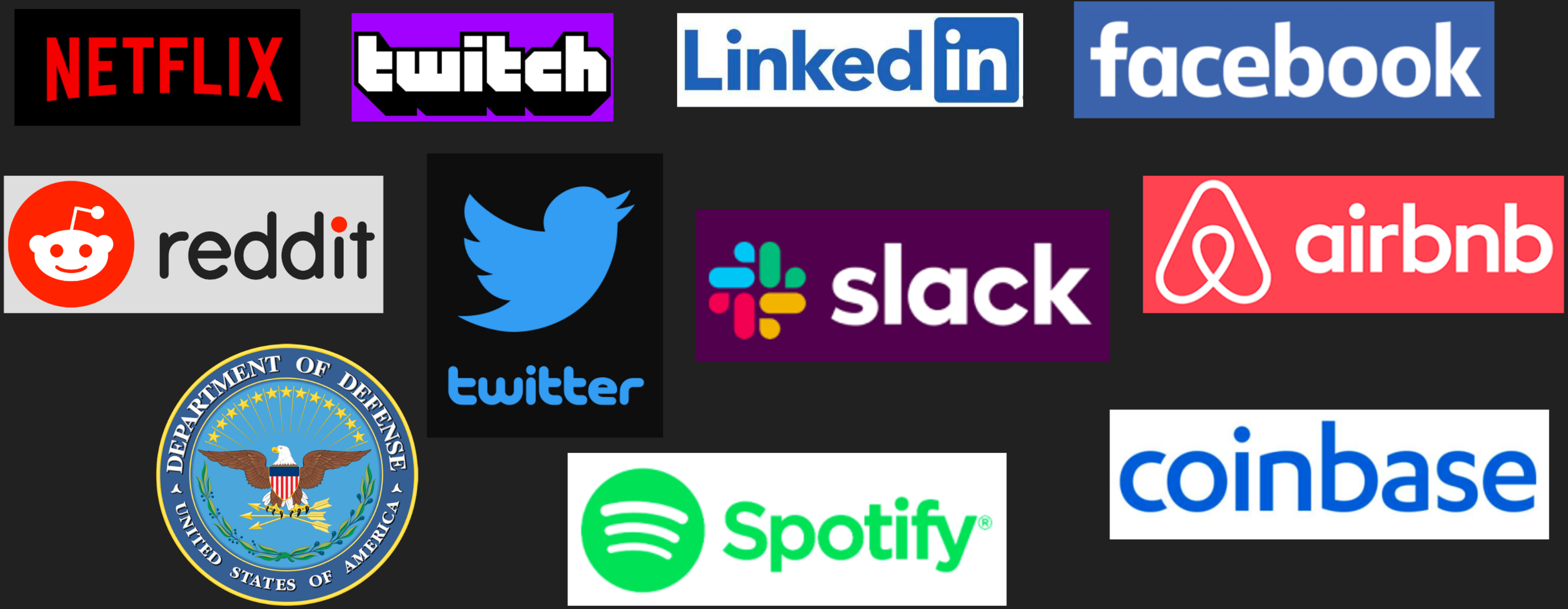
- What is AWS?
- Shared Responsibility Model
- What is AWS-Well Architected Framework?
- Design Principles for Security
- Best Practice Areas for Security
- Questions?

What is AWS?

- ➢ Cloud Computing Service
- ➢ Provides three different services
  - ○ SaaS (Software as a Service)
  - ○ PaaS (Platform as a Service)
  - ○ IaaS (Infrastructure as a Service)
- ➢ Used by many in different sectors

Reference:
https://aws.amazon.com/what-is-aws/
https://aws.amazon.com/about-aws/global-infrastructure/

Who uses AWS?



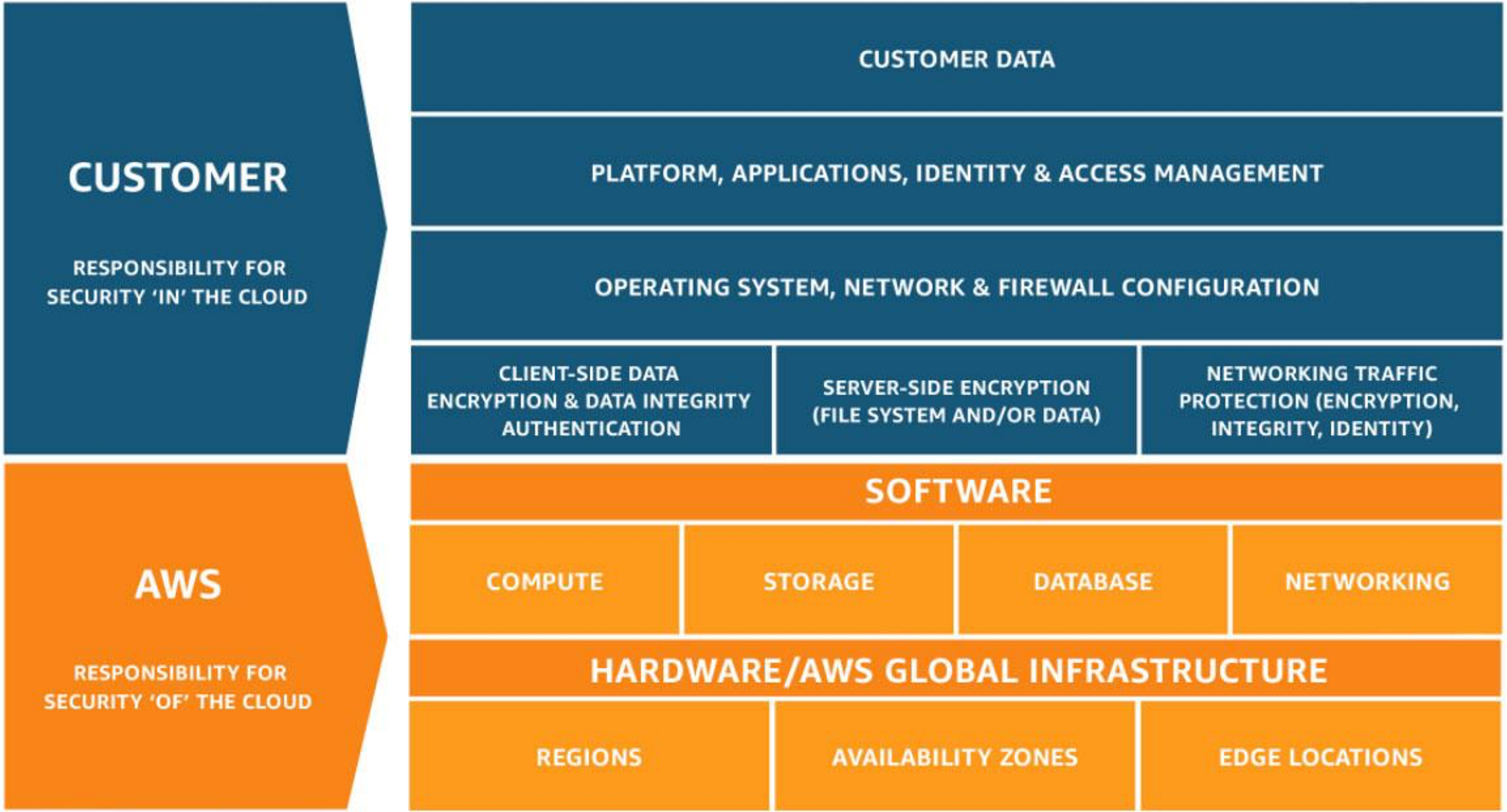
Reference:

https://aws.amazon.com/solutions/case-studies/

https://www.quora.com/Who-are-the-top-10-Amazon-AWS-customers

Shared Responsibility Model

Reference: https://aws.amazon.com/compliance/shared-responsibility-model/



CUSTOMER

RESPONSIBILITY FOR
SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR
SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

What is AWS-Well Architected Framework?

- ➢ A Framework developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure.

- ➢ The Five Pillars of the Framework
  - ➢ Operational Excellence
  - ➢ Security
  - ➢ Reliability
  - ➢ Performance Efficiency
  - ➢ Cost Optimization

Reference:
https://aws.amazon.com/architecture/well-architected/
https://wa.aws.amazon.com/index.en.html

Design Principles for Security

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

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

Best Practices Areas for Security

- ➢ Identity and Access Management
- ➢ Detective Controls
- ➢ Infrastructure Protection
- ➢ Data Protection
- ➢ Incident Response

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

Best Practices Areas for Security

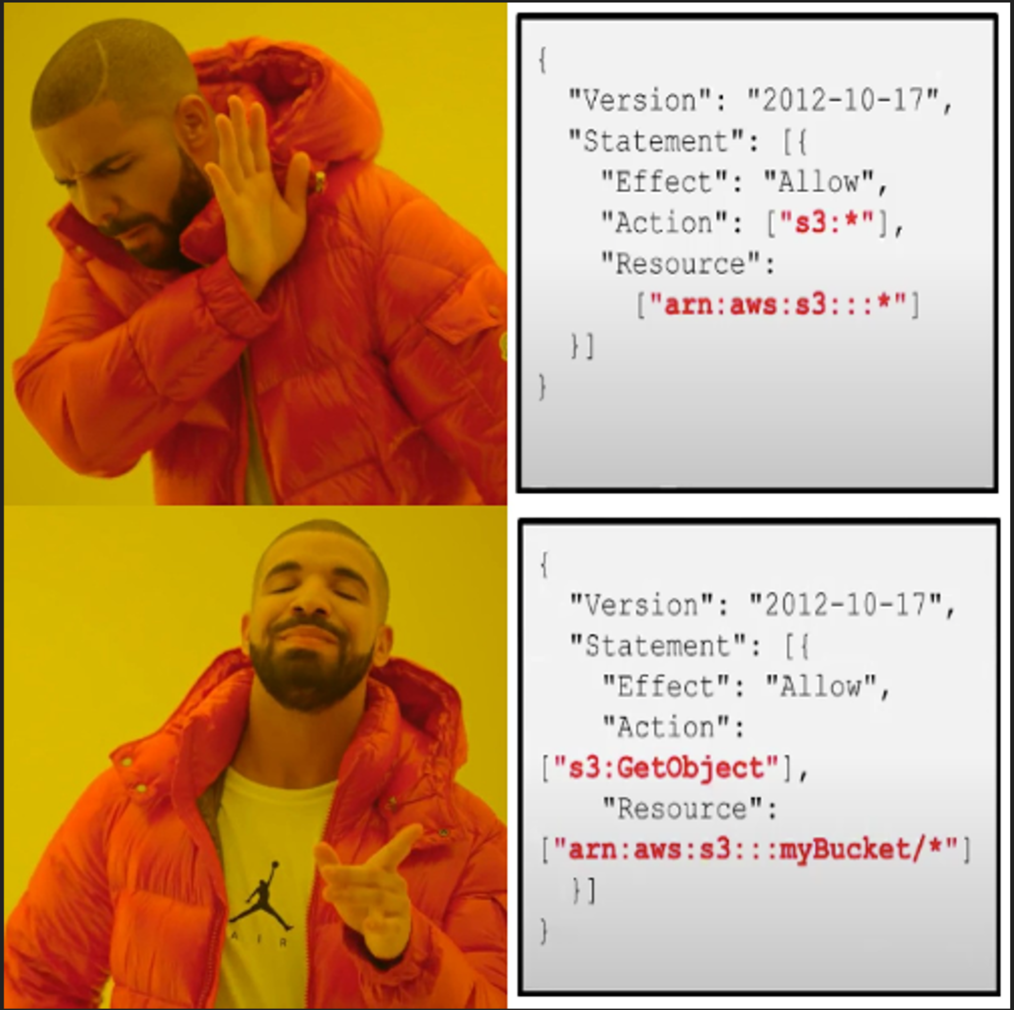
- ➢ Identity and Access Management
- ➢ Detective Controls
- ➢ Infrastructure Protection
- ➢ Data Protection
- ➢ Incident Response

Identity and Access Management (IAM)

- Ensure only authorized and authenticated user are able to access resources
- Define user, groups, service, and roles
- Protect AWS credentials
- Use fine grained authorization/access control

Reference: https://wa.aws.amazon.com/wat.question.SEC_1.en.html

IAM in action



```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource":
      ["arn:aws:s3:::*"]
  }]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action":
["s3:GetObject"],
    "Resource":
["arn:aws:s3:::myBucket/*"]
  }]
}
```

Best Practices Areas for Security

- Identity and Access Management
- Detective Controls
- Infrastructure Protection
- Data Protection
- Incident Response

Detective Controls

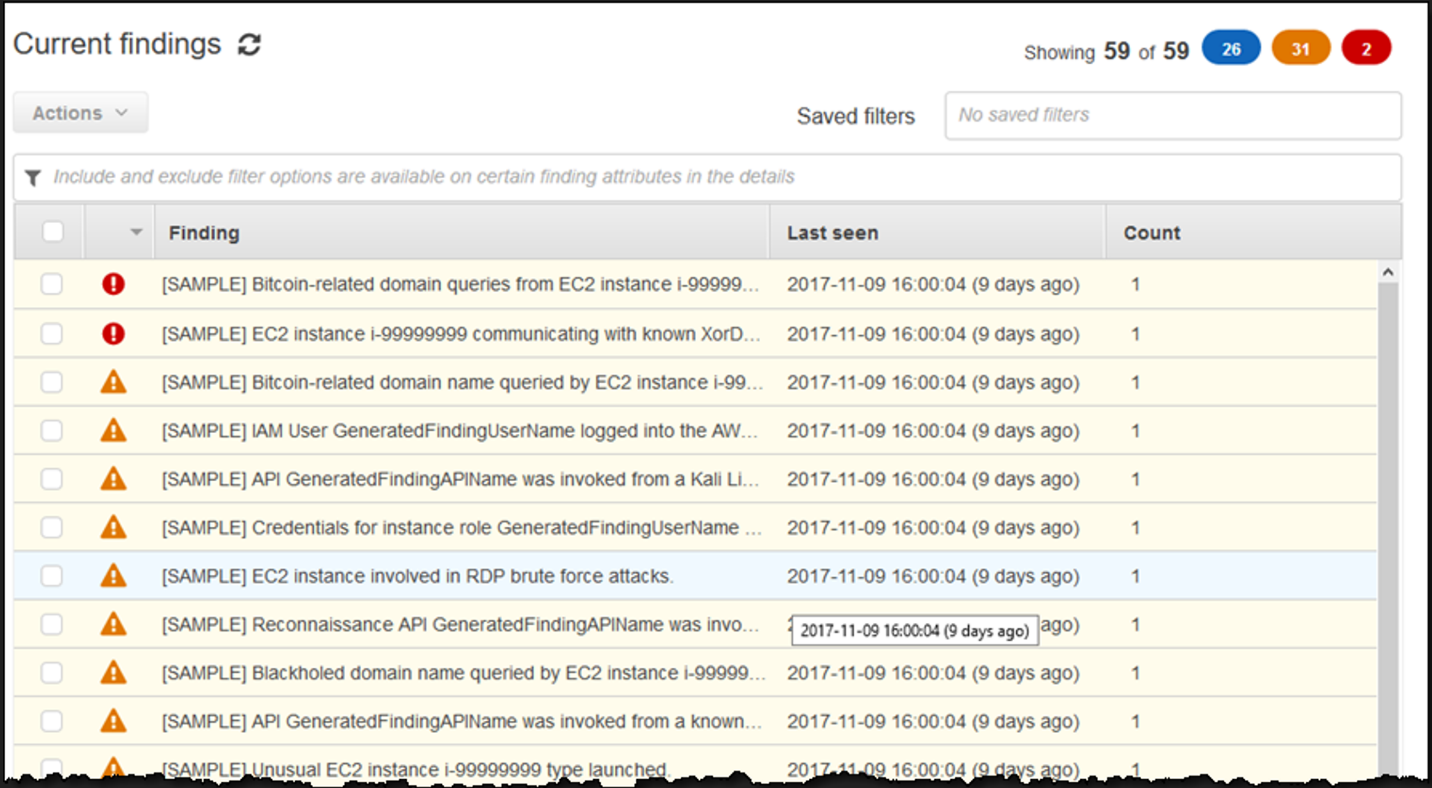
- Detection of unauthorized traffic
- Capture and analyze logs
- Integrate auditing controls with notifications and workflows
- Fine-grained audits

Reference: https://wa.aws.amazon.com/wat.question.SEC_4.en.html

Detective Controls

- ➢ GuardDuty
- ➢ CloudTrail
- ➢ CloudWatch
- ➢ AWS Config
- ➢ AWS Trusted Advisor
- ➢ VPC Flow Logs

Detective Controls in action



Current findings

Showing 59 of 59 26 31 2

Saved filters: *No saved filters*

Include and exclude filter options are available on certain finding attributes in the details

□		Finding	Last seen	Count
□	❗	[SAMPLE] Bitcoin-related domain queries from EC2 instance i-99999...	2017-11-09 16:00:04 (9 days ago)	1
□	❗	[SAMPLE] EC2 instance i-99999999 communicating with known XorD...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] Bitcoin-related domain name queried by EC2 instance i-99...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] IAM User GeneratedFindingUserName logged into the AW...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] API GeneratedFindingAPIName was invoked from a Kali Li...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] Credentials for instance role GeneratedFindingUserName ...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] EC2 instance involved in RDP brute force attacks.	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] Reconnaissance API GeneratedFindingAPIName was invo...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] Blackholed domain name queried by EC2 instance i-99999...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] API GeneratedFindingAPIName was invoked from a known...	2017-11-09 16:00:04 (9 days ago)	1
□	⚠	[SAMPLE] Unusual EC2 instance i-99999999 type launched.	2017-11-09 16:00:04 (9 days ago)	1

Best Practices Areas for Security

- ➢ Identity and Access Management
- ➢ Detective Controls
- ➢ Infrastructure Protection
- ➢ Data Protection
- ➢ Incident Response

Infrastructure Protection

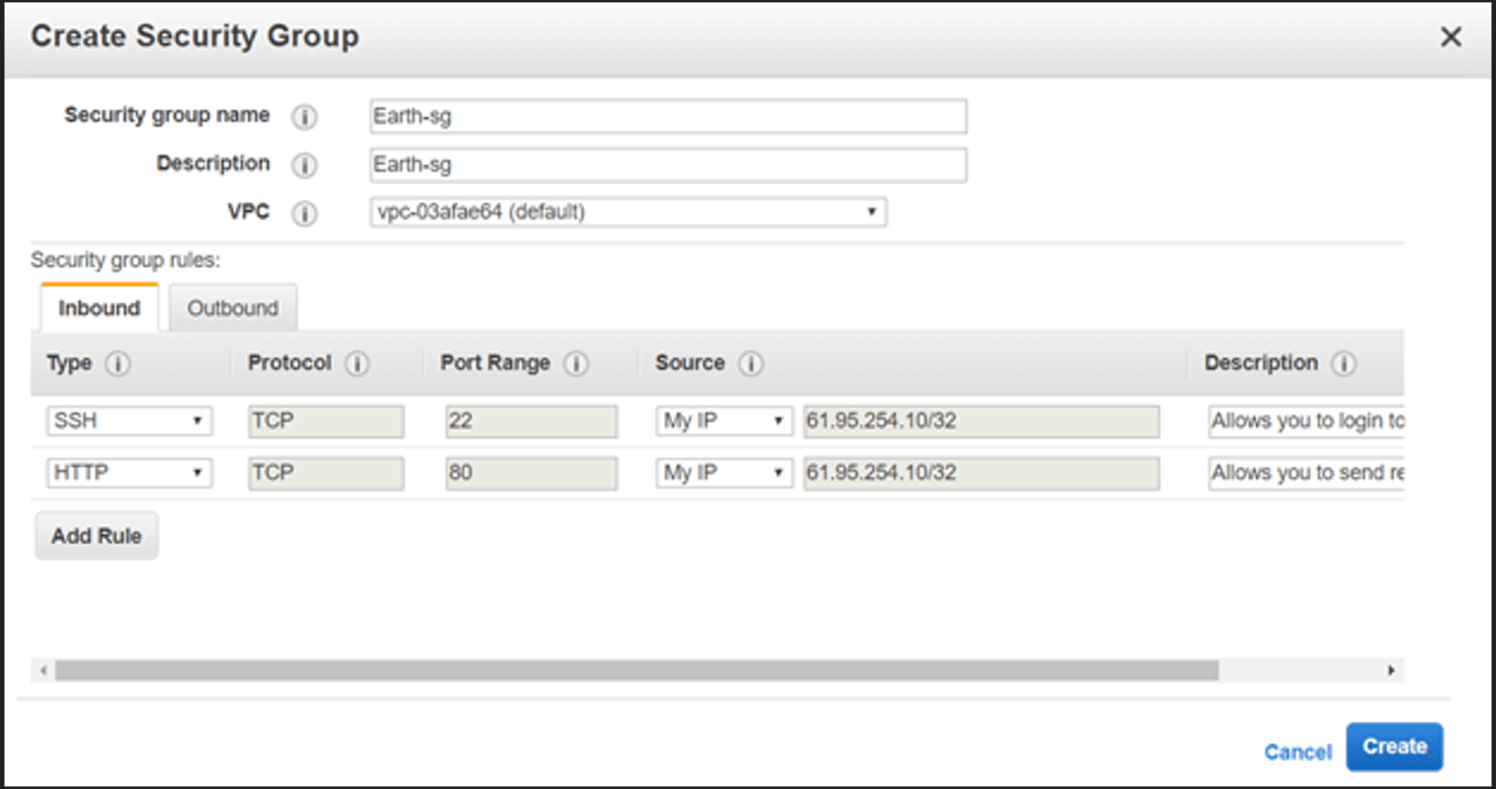
- Encompasses control methodologies
  - Defense in depth
  - Best practices
  - Organizational or Regulatory obligations
- Protecting network and host-level boundaries
- Limit exposure
- Control traffic at all layers

Reference: https://wa.aws.amazon.com/wat.question.SEC_6.en.html

Infrastructure Protection

- ➢ VPC Security Groups
- ➢ Network ACLs
- ➢ AWS WAF
- ➢ AWS Shield
- ➢ AWS Direct Connect

Infrastructure Protection in action



Create Security Group

Security group name: Earth-sg

Description: Earth-sg

VPC: vpc-03afae64 (default)

Security group rules:

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	61.95.254.10/32	Allows you to login tc
HTTP	TCP	80	My IP	61.95.254.10/32	Allows you to send re

Best Practices Areas for Security

- ➢ Identity and Access Management
- ➢ Detective Controls
- ➢ Infrastructure Protection
- ➢ Data Protection
- ➢ Incident Response

Data Protection

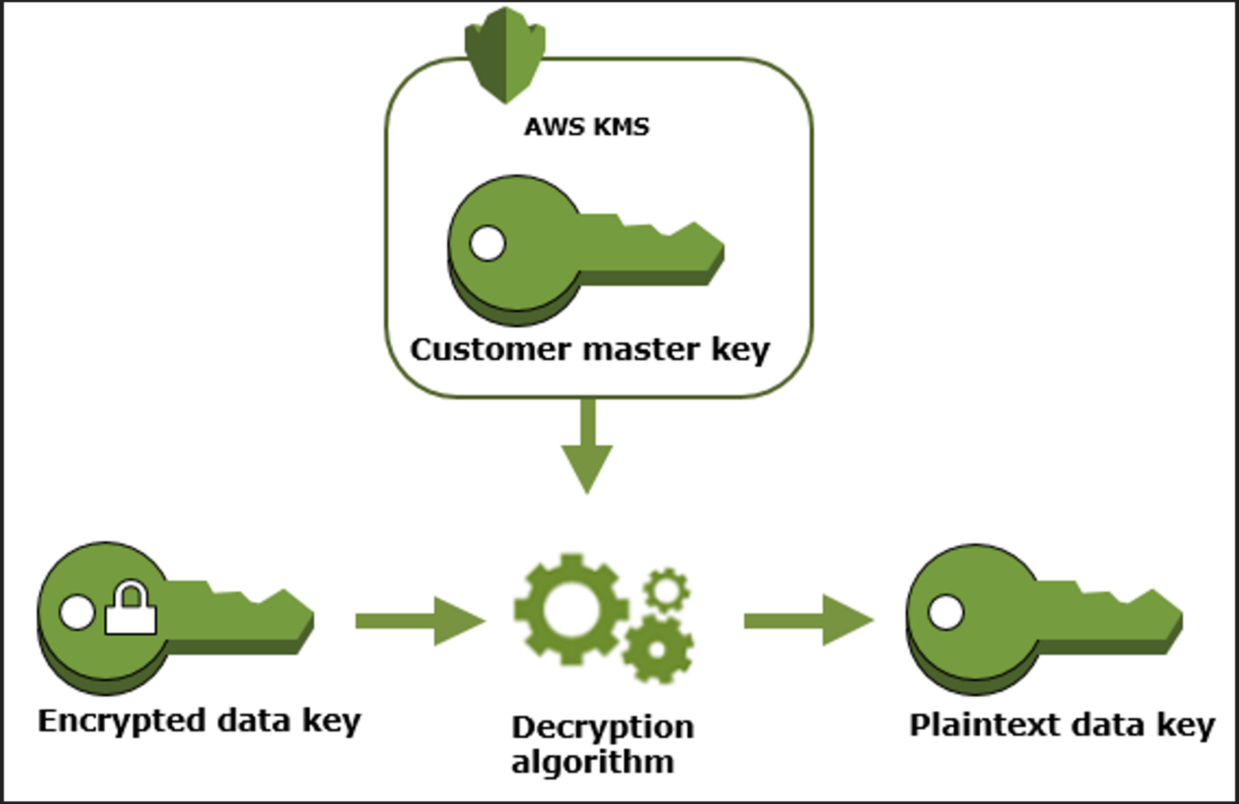
- ➢ Data Classification
- ➢ Authenticate network communication
- ➢ Encryption and Tokenization
- ➢ Protect data in transit
- ➢ Protect data at rest

Reference:
https://wa.aws.amazon.com/wat.question.SEC_9.en.html
https://wa.aws.amazon.com/wat.question.SEC_10.en.html

Data Protection

- Amazon KMS
- Amazon EBS Encryption
- VPC VPN Connections
- Amazon S3 Data Encryption

Data Protection in action



Best Practices Areas for Security

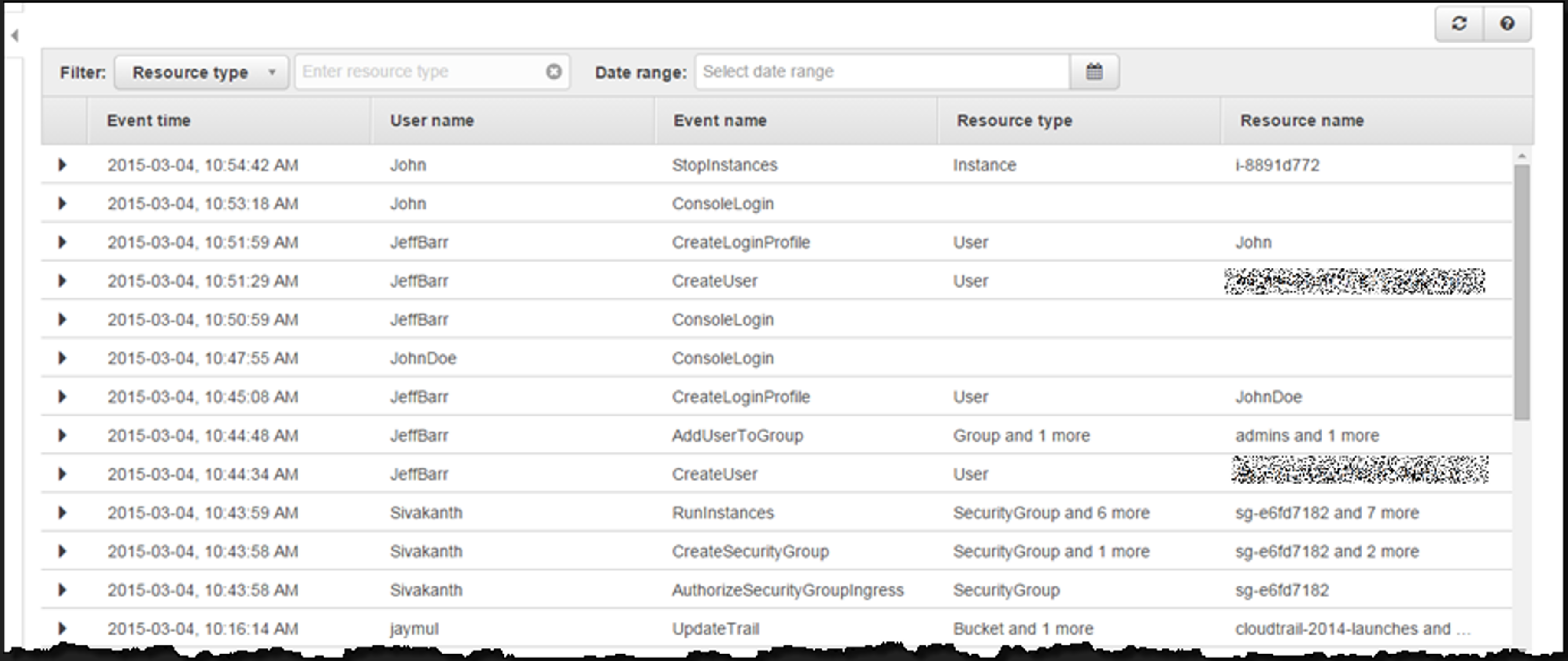
- Identity and Access Management
- Detective Controls
- Infrastructure Protection
- Data Protection
- Incident Response

Incident Response

- ➢ Identify key personnel and external resources
- ➢ Develop incident response plans
- ➢ Automate containment capability
- ➢ Pre-provision access
- ➢ Pre-deploy tools
- ➢ Run game days

Reference: https://wa.aws.amazon.com/wat.question.SEC_11.en.html

Incident Response in action



Filter: Resource type ▾ Enter resource type

Date range: Select date range

	Event time	User name	Event name	Resource type	Resource name
▸	2015-03-04, 10:54:42 AM	John	StopInstances	Instance	i-8891d772
▸	2015-03-04, 10:53:18 AM	John	ConsoleLogin		
▸	2015-03-04, 10:51:59 AM	JeffBarr	CreateLoginProfile	User	John
▸	2015-03-04, 10:51:29 AM	JeffBarr	CreateUser	User	[redacted]
▸	2015-03-04, 10:50:59 AM	JeffBarr	ConsoleLogin		
▸	2015-03-04, 10:47:55 AM	JohnDoe	ConsoleLogin		
▸	2015-03-04, 10:45:08 AM	JeffBarr	CreateLoginProfile	User	JohnDoe
▸	2015-03-04, 10:44:48 AM	JeffBarr	AddUserToGroup	Group and 1 more	admins and 1 more
▸	2015-03-04, 10:44:34 AM	JeffBarr	CreateUser	User	[redacted]
▸	2015-03-04, 10:43:59 AM	Sivakanth	RunInstances	SecurityGroup and 6 more	sg-e6fd7182 and 7 more
▸	2015-03-04, 10:43:58 AM	Sivakanth	CreateSecurityGroup	SecurityGroup and 1 more	sg-e6fd7182 and 2 more
▸	2015-03-04, 10:43:58 AM	Sivakanth	AuthorizeSecurityGroupIngress	SecurityGroup	sg-e6fd7182
▸	2015-03-04, 10:16:14 AM	jaymul	UpdateTrail	Bucket and 1 more	cloudtrail-2014-launches and ...

QUESTIONS ?

THANK YOU!