

# AWS Security Specialty

by S.Suresh

CloudSiksha

# Agenda

01

Understand the shared responsibility model of AWS for Security

02

Understand how to secure your infrastructure in AWS

03

Understand how to effectively use Identity & Access Management

04

Understand the tools provided by AWS for Security

05

Understand the Security Best practices on AWS

# AWS Security Certification (Optional)

Incident Response : 12%

Logging & Monitoring : 20%

Infrastructure Security : 26%

Identity & Access Management : 20%

Data Management : 22%

# Training Methodology



Lectures



Demos & Partial Hands On

Account wide services

Region wide services

AWS Config, WAF, AWS Organizations, CloudTrail etc



Hands On

VPC, EC2, S3, CloudWatch Logs, CloudWatch Events,  
Inspector etc

# Security Frameworks

# AWS CAF - Security Perspective

**Security Governance**

*develop and communicate security roles, responsibilities, policies, processes, and procedures*

**Security Assurance**

*monitor, evaluate, manage, and improve the effectiveness of your security and privacy programs*

**Identity and Access Mgmt**

*manage identities and permissions at scale*

**Threat Detection**

*understand and identify potential security misconfigurations, threats, or unexpected behaviors*

**Vulnerability Mgmt**

*continuously identify, classify, remediate, and mitigate security vulnerabilities*

**Infrastructure Protection**

*validate that systems and services within your workload are protected*

**Data Protection**

*maintain visibility and control over data, and how it is accessed and used in your organization*

**Application Security**

*detect and address security vulnerabilities during the software development process*

**Incident Response**

*reduce potential harm by effectively responding to security incidents*

# AWS Cloud Framework - Security Perspective (Older Version)

Directive controls establish the governance, risk, and compliance models the environment will operate within.

Preventive controls protect your workloads and mitigate threats and vulnerabilities.

Detective controls provide full visibility and transparency over the operation of your deployments in AWS.

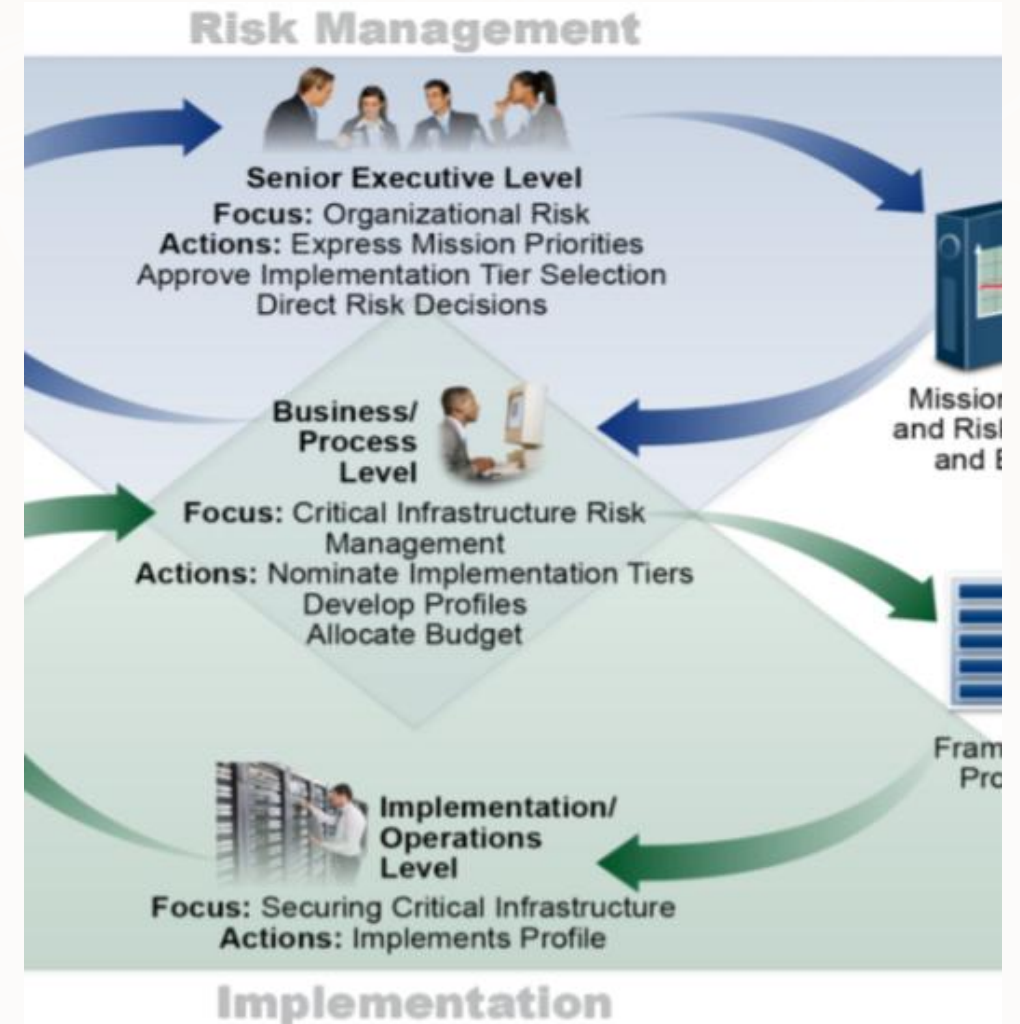
Responsive controls drive remediation of potential deviations from your security baselines.

# NIST Security Framework



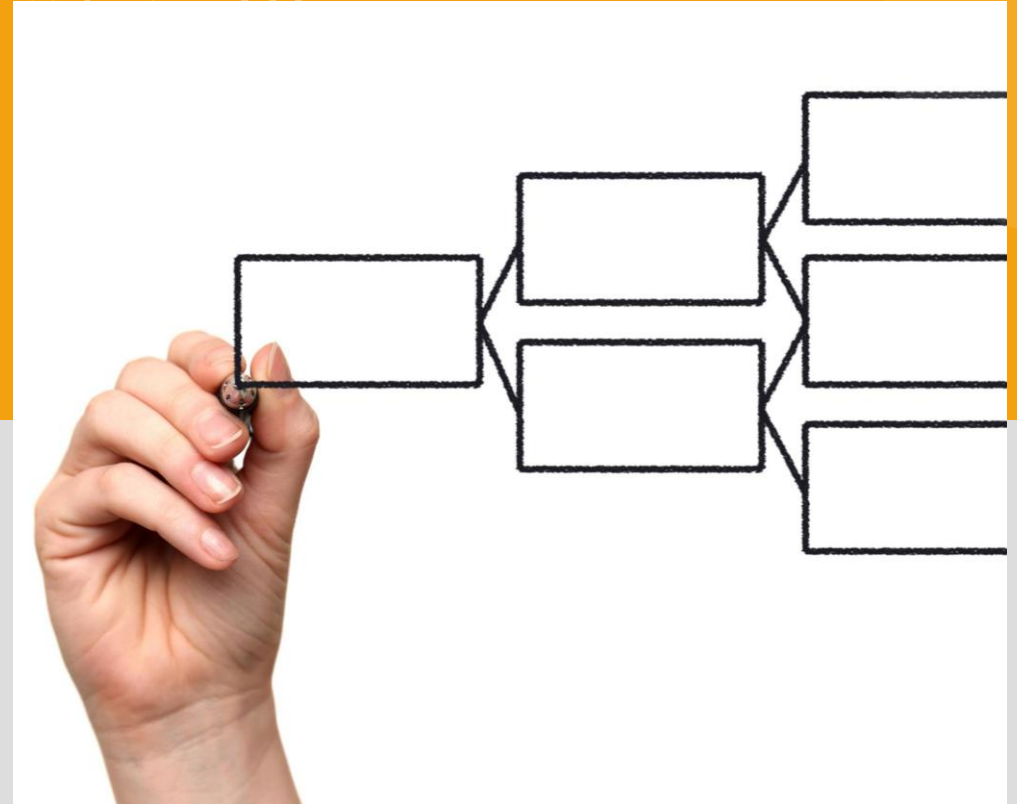


# NIST Security Framework - Organization Levels



# Understanding the MITRE ATT&CK Framework

- MITRE ATT&CK provides a comprehensive knowledge base.
- Framework helps in identifying and categorizing cyber threats.
- ATT&CK is used for threat modeling and incident response.
- It includes tactics, techniques, and procedures (TTPs) used by adversaries.
- Organizations can use ATT&CK for enhancing their security posture.

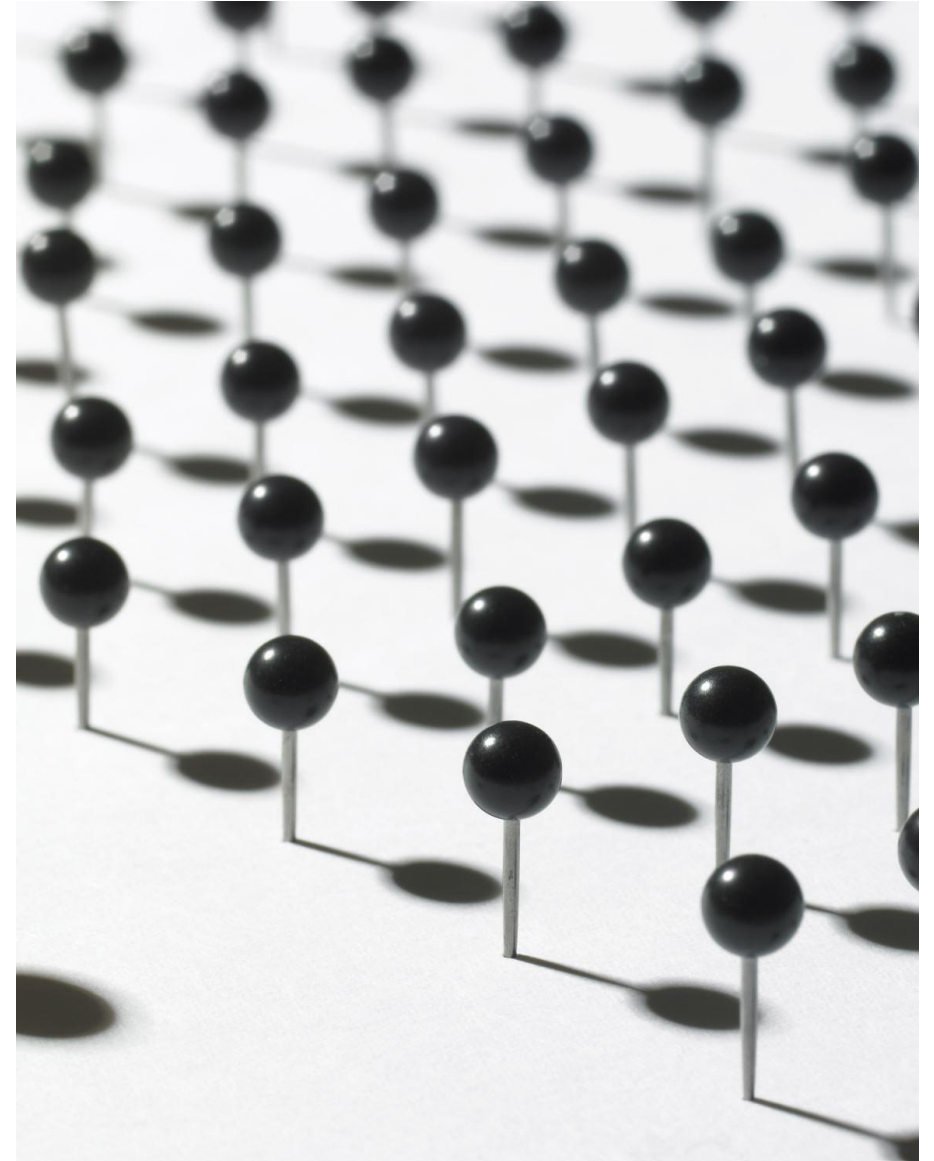


# MITRE ATT&CK FRAMEWORK

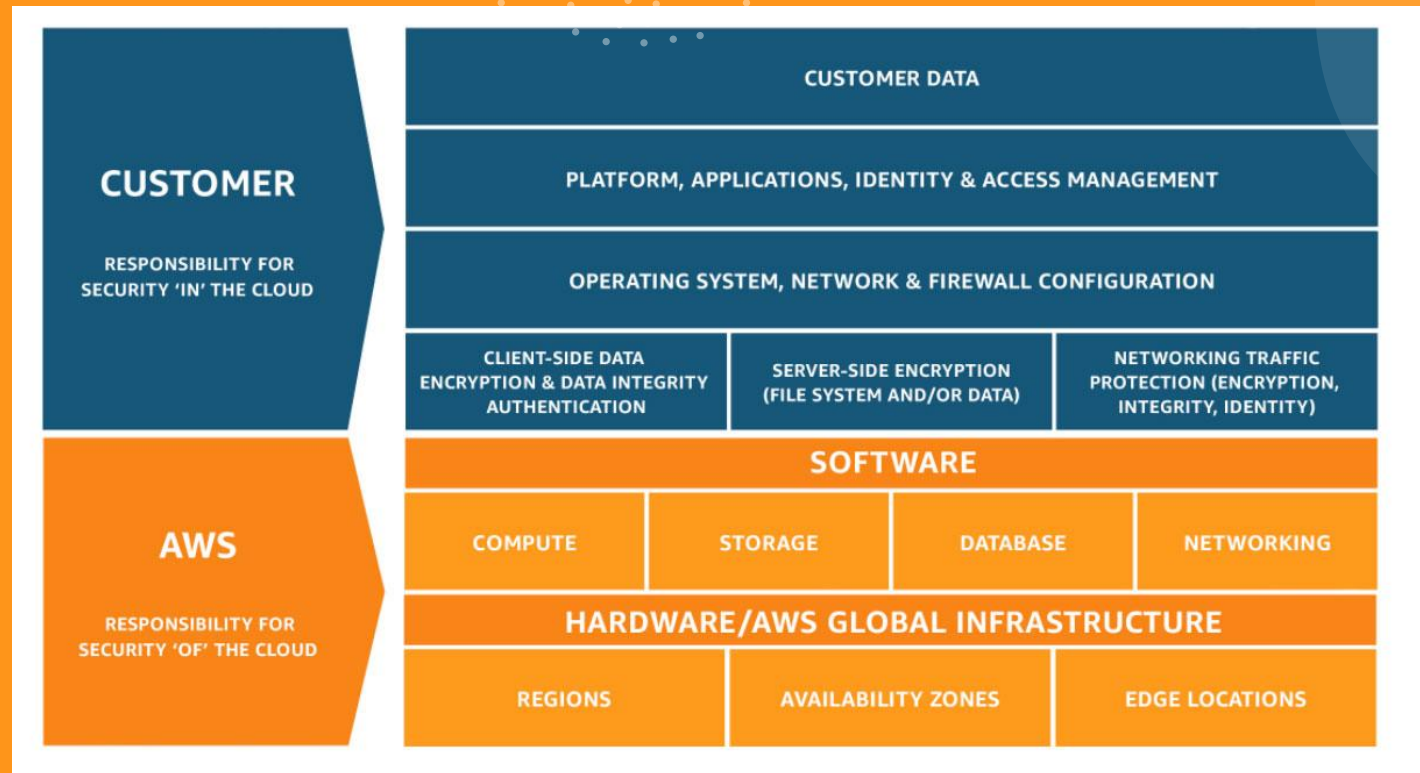
Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
<ul style="list-style-type: none"> <li>Active Scanning (0/2)</li> <li>Gather Victim Host Information (0/4)</li> <li>Gather Victim Identity Information (0/3)</li> <li>Gather Victim Network Information (0/6)</li> <li>Gather Victim Org Information (0/4)</li> <li>Phishing for Information (0/3)</li> <li>Search Closed Sources (0/2)</li> <li>Search Open Technical Databases (0/5)</li> <li>Search Open Websites/Domains (0/2)</li> <li>Search Victim-Owned Websites</li> </ul>	<ul style="list-style-type: none"> <li>Acquire Infrastructure (0/6)</li> <li>Compromise Accounts (0/2)</li> <li>Compromise Infrastructure (0/6)</li> <li>Develop Capabilities (0/4)</li> <li>Establish Accounts (0/2)</li> <li>Obtain Capabilities (0/6)</li> </ul>	<ul style="list-style-type: none"> <li>Drive-by Compromise</li> <li>Exploit Public-Facing Application</li> <li>External Remote Services</li> <li>Hardware Additions</li> <li>Phishing (0/3)</li> <li>Replication Through Removable Media</li> <li>Supply Chain Compromise (0/3)</li> <li>Trusted Relationship</li> <li>Valid Accounts (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Command and Scripting Interpreter (0/8)</li> <li>Exploitation for Client Execution</li> <li>Inter-Process Communication (0/2)</li> <li>Native API</li> <li>Scheduled Task/Job (0/6)</li> <li>Shared Modules</li> <li>Software Deployment Tools</li> <li>System Services (0/2)</li> <li>User Execution (0/2)</li> <li>Windows Management Instrumentation</li> </ul>	<ul style="list-style-type: none"> <li>Account Manipulation (0/4)</li> <li>BITS Jobs</li> <li>Boot or Logon Autostart Execution (0/12)</li> <li>Boot or Logon Initialization Scripts (0/5)</li> <li>Browser Extensions</li> <li>Compromise Client Software Binary</li> <li>Create Account (0/3)</li> <li>Create or Modify System Process (0/4)</li> <li>Event Triggered Execution (0/15)</li> <li>External Remote Services</li> <li>Hijack Execution Flow (0/11)</li> <li>Implant Container Image</li> <li>Office Application Startup (0/6)</li> <li>Pre-OS Boot (0/5)</li> <li>Scheduled Task/Job (0/6)</li> <li>Server Software Component (0/3)</li> </ul>	<ul style="list-style-type: none"> <li>Abuse Elevation Control Mechanism (0/4)</li> <li>Access Token Manipulation (0/5)</li> <li>Boot or Logon Autostart Execution (0/12)</li> <li>Boot or Logon Initialization Scripts (0/5)</li> <li>Create or Modify System Process (0/4)</li> <li>Event Triggered Execution (0/15)</li> <li>Exploitation for Privilege Escalation</li> <li>Group Policy Modification</li> <li>Hijack Execution Flow (0/11)</li> <li>Process Injection (0/11)</li> <li>Scheduled Task/Job (0/6)</li> <li>Valid Accounts (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Abuse Elevation Control Mechanism (0/4)</li> <li>Access Token Manipulation (0/5)</li> <li>BITS Jobs</li> <li>Deobfuscate/Decode Files or Information</li> <li>Direct Volume Access</li> <li>Execution Guardrails (0/1)</li> <li>Exploitation for Defense Evasion</li> <li>File and Directory Permissions Modification (0/2)</li> <li>Group Policy Modification</li> <li>Hide Artifacts (0/7)</li> <li>Hijack Execution Flow (0/11)</li> <li>Impair Defenses (0/7)</li> <li>Indicator Removal on Host (0/6)</li> <li>Indirect Command Execution</li> <li>Masquerading (0/6)</li> <li>Modify Authentication Process (0/4)</li> <li>Modify Cloud Compute Infrastructure (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Brute Force (0/4)</li> <li>Credentials from Password Stores (0/3)</li> <li>Exploitation for Credential Access</li> <li>Forced Authentication</li> <li>Input Capture (0/4)</li> <li>Man-in-the-Middle (0/2)</li> <li>Modify Authentication Process (0/4)</li> <li>Network Sniffing</li> <li>OS Credential Dumping (0/8)</li> <li>Steal Application Access Token</li> <li>Steal or Forge Kerberos Tickets (0/4)</li> <li>Steal Web Session Cookie</li> <li>Two-Factor Authentication Interception</li> <li>Unsecured Credentials (0/6)</li> </ul>	<ul style="list-style-type: none"> <li>Account Discovery (0/4)</li> <li>Application Window Discovery</li> <li>Browser Bookmark Discovery</li> <li>Cloud Infrastructure Discovery</li> <li>Cloud Service Dashboard</li> <li>Cloud Service Discovery</li> <li>Domain Trust Discovery</li> <li>File and Directory Discovery</li> <li>Network Service Scanning</li> <li>Network Share Discovery</li> <li>Network Sniffing</li> <li>Password Policy Discovery</li> <li>Peripheral Device Discovery</li> <li>Permission Groups Discovery (0/3)</li> <li>Query Registry</li> <li>Remote System Discovery</li> <li>Software Discovery (0/1)</li> </ul>	<ul style="list-style-type: none"> <li>Exploitation of Remote Services</li> <li>Internal Spearphishing</li> <li>Lateral Tool Transfer</li> <li>Remote Service Session Hijacking (0/2)</li> <li>Remote Services (0/6)</li> <li>Replication Through Removable Media</li> <li>Software Deployment Tools</li> <li>Taint Shared Content</li> <li>Use Alternate Authentication Material (0/4)</li> </ul>	<ul style="list-style-type: none"> <li>Archive Collected Data (0/3)</li> <li>Audio Capture</li> <li>Automated Collection</li> <li>Clipboard Data</li> <li>Data from Cloud Storage Object</li> <li>Data from Configuration Repository (0/2)</li> <li>Data from Information Repositories (0/2)</li> <li>Data from Local System</li> <li>Data from Network Shared Drive</li> <li>Data from Removable Media</li> <li>Data Staged (0/2)</li> <li>Email Collection (0/3)</li> <li>Input Capture (0/4)</li> <li>Man in the Browser</li> <li>Man-in-the-Middle (0/2)</li> <li>Screen Capture</li> <li>Video Capture</li> </ul>	<ul style="list-style-type: none"> <li>Application Layer Protocol (0/4)</li> <li>Communication Through Removable Media</li> <li>Data Encoding (0/2)</li> <li>Data Obfuscation (0/3)</li> <li>Dynamic Resolution (0/3)</li> <li>Encrypted Channel (0/2)</li> <li>Fallback Channels</li> <li>Ingress Tool Transfer</li> <li>Multi-Stage Channels</li> <li>Non-Application Layer Protocol</li> <li>Non-Standard Port</li> <li>Protocol Tunneling</li> <li>Proxy (0/4)</li> <li>Remote Access Software</li> <li>Traffic Signaling (0/1)</li> <li>Web Service (0/3)</li> </ul>	<ul style="list-style-type: none"> <li>Automated Exfiltration (0/1)</li> <li>Data Transfer Size Limits</li> <li>Exfiltration Over Alternative Protocol (0/3)</li> <li>Exfiltration Over C2 Channel</li> <li>Exfiltration Over Other Network Medium (0/1)</li> <li>Exfiltration Over Physical Medium (0/1)</li> <li>Exfiltration Over Web Service (0/2)</li> <li>Scheduled Transfer</li> <li>Transfer Data to Cloud Account</li> </ul>	<ul style="list-style-type: none"> <li>Account Access Removal</li> <li>Data Destruction</li> <li>Data Encrypted for Impact</li> <li>Data Manipulation (0/3)</li> <li>Defacement (0/2)</li> <li>Disk Wipe (0/2)</li> <li>Endpoint Denial of Service (0/4)</li> <li>Firmware Corruption</li> <li>Inhibit System Recovery</li> <li>Network Denial of Service (0/2)</li> <li>Resource Hijacking</li> <li>Service Stop</li> <li>System Shutdown/Reboot</li> </ul>

# Security by Design

- Principle of Least Privilege
- Defence in Depth
- Failsafe
- Keep It Simple, Simple (KISS)
- Separation of Duties
- Open Design
- Segmentation
- Usability
- Minimize the attack surface
- Secure by Default



# AWS Shared Responsibility Model



# Cloud Specific Security Risks

- Shared Responsibility
- Multi-Tenancy
- Misconfigured Resources
- Complexity of IAM
- Data Security
- Denial of Service Attacks
- Insider Threats
- Supply Chain and Dependency Risks
- Compliance and Legal Issues
- API Security
- Shadow IT and Uncontrolled usage



# AWS Introduction



# Security Resources

- AWS Site for Security, Identity and Compliance:
  - <https://aws.amazon.com/architecture/security-identity-compliance>
- AWS Security Reference Architecture
  - <https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html>
- AWS Security Documentation
  - <https://docs.aws.amazon.com/security/>
- Cloud Adoption Framework Document
  - <https://dl.awsstatic.com/whitepapers/aws-caf-ebook.pdf>
- All images taken from the Amazon unless specified otherwise



# AWS Regions and Availability Zones

## Regions

Geographical areas

Multiple regions across the globe

New regions keep getting added regularly



## Availability Zones (AZ)

Isolated data centers

Used for designing High Availability

At least two AZ per regions

Number of AZ per region will depend on the region



# Our Agenda

# Our Agenda

- Day 1: Introduction and Infrastructure Protection
  - Introduction to Security Specialization and Security Frameworks
  - Introduction to AWS
  - Basics of AWS (Networking and EC2)
  - Lab: Creating VPC and Protecting Subnets
- Afternoon
  - Protecting Storage (S3)
  - CloudFront and Web Application Delivery
  - Protecting Web Applications
  - Lab: S3, CloudFront and Web Application Firewall

# Our Agenda

- Day 2: Data Security and Monitoring
  - Introduction to Data Security
  - Introduction to Cryptography
  - Hardware Security Modules (HSM)
  - Key Management System
  - Digital Certificates
  - Logging and Monitoring in AWS
  - FlowLogs and CloudTrail Logs
  - Application Protection
  - Labs: KMS, AWS Inspector, Guard Duty, AWS Config, SSM Parameter Store, VPC Flow Logs



# Our Agenda

- Day 3: IAM, Federation, Organizations, Control Tower
  - Identity and Access Management
  - Role Based Policies
  - Attribute Based Policies
  - Roles
  - Cross Account Access
  - Federated Access
  - AWS Organizations
  - AWS Control Tower
  - Lab: Role Based Policies, Access Based Policies, Roles, Cross Account Access & AWS Organization



# Pre-requisite

- Basic understanding of AWS services
  - **EC2, S3, VPC at a minimum**
- Important:
  - **Some of the services are CLI only services**
  - **To install CLI you will require your personal laptop**
  - **If you do not have a personal laptop, you will not be able to perform some of lab exercises**

Thanks



CloudSiksha

# STRIDE Framework

- Developed by Praerit Garg and Loren Kohnfelder at Microsoft
- STRIDE is a model for threats
- STRIDE stands for
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service
  - Elevation of privilege



# STRIDE

- Spoofing
  - **Spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data**
- Tampering
  - **Intentional modification of products in a way that would make them harmful to the consumer**
- Repudiation
  - **Non-repudiation refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract**
- Information Disclosure
- Denial of Service
  - **A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users**
- Elevation of Privilege
  - **Act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources**

# Threats & Mitigation

Threat	Mitigation
Spoofing	Authentication
Tampering	Integrity
Repudiation	Confirmation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

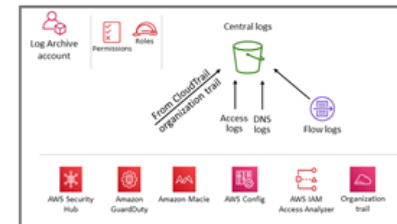
# AWS Security Reference Architecture (SRA)

- Value of AWS SRA
- Security Foundations Review
- AWS Organizations, Accounts and IAM GuardRails
- AWS Security Reference Architecture
- IAM Resources
- Code repository for AWS SRA examples

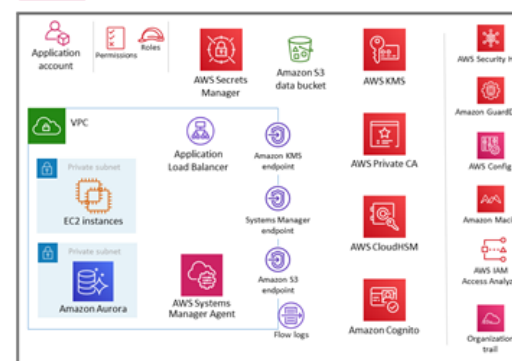
# SRA Reference Architecture



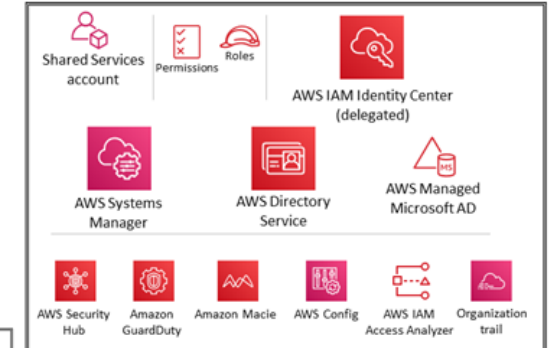
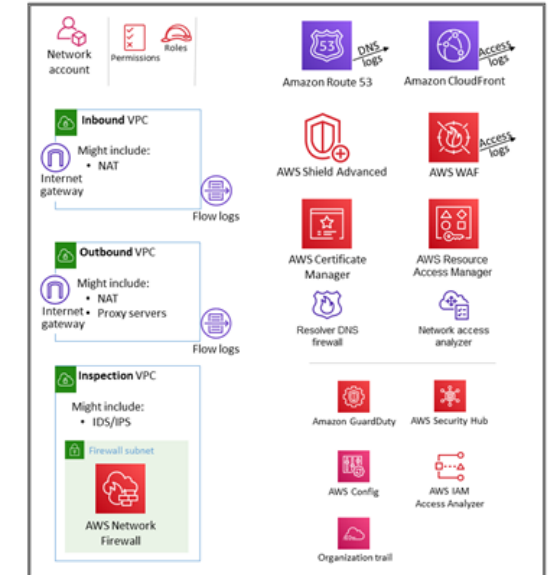
## OU – Security



## OU – Workloads



## OU – Infrastructure



# AWS Security Services - Data Protection

Amazon  
Macie

AWS KMS

AWS HSM

AWS  
Certificate  
Manager

AWS Secrets  
Manager

# AWS Security Services - IAM

IAM

IAM Identity Center

Amazon Cognito

AWS Directory Service

AWS Resource Access Manager

AWS Organizations

# AWS Security Services - Networking & App Protection

AWS Shield

AWS WAF

AWS Firewall Manager

AWS Systems Manager

VPC

AWS Network Firewall

AWS Route53 DNS Firewall

# AWS Security Services - Threat Detection & Continuous Monitoring

Security Hub

Guard Duty

Inspector

Config

CloudTrail

Detective



# AWS Security Services - Compliance & Data Privacy

AWS  
Audit  
Manager

AWS  
Artifacts