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

AWS Cloud Framework - Security Perspective (Older Version)

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

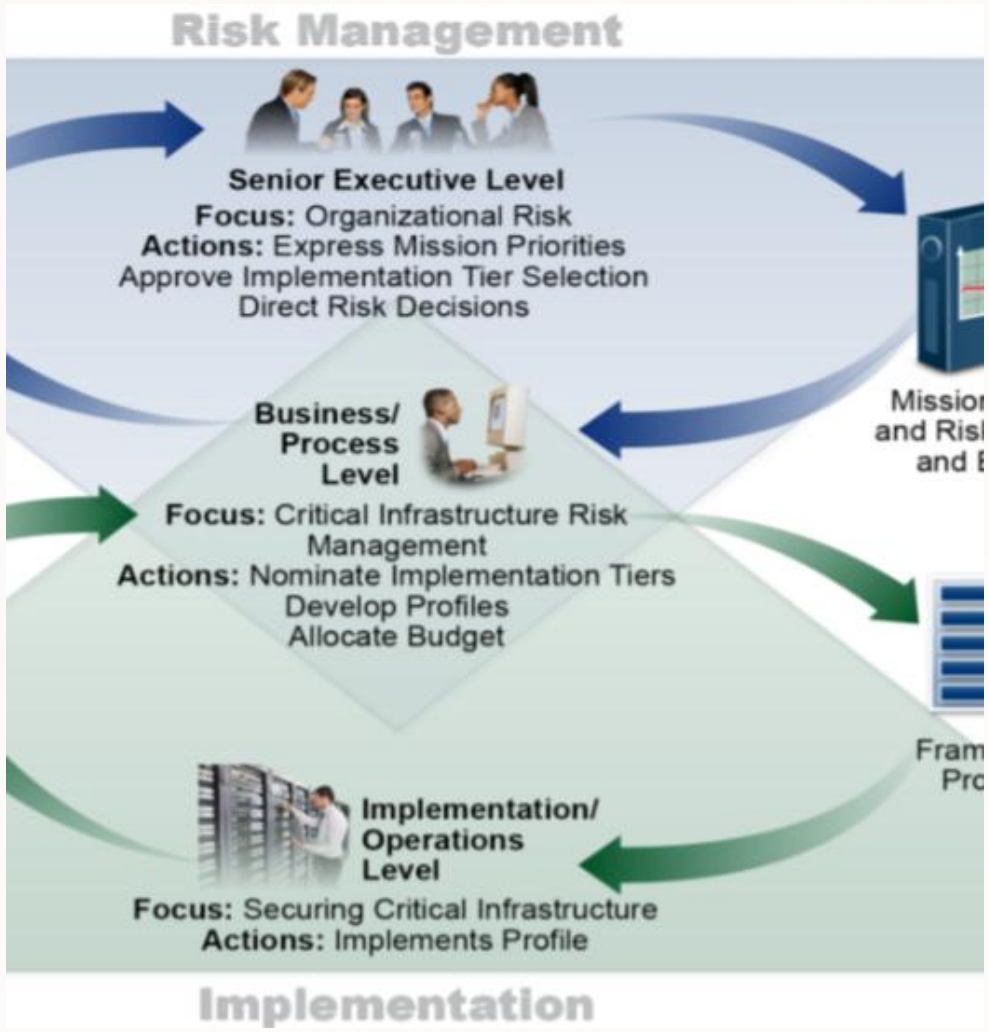
Preventive controls protect your workloads and mitigate threats and vulnerabilities.

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.

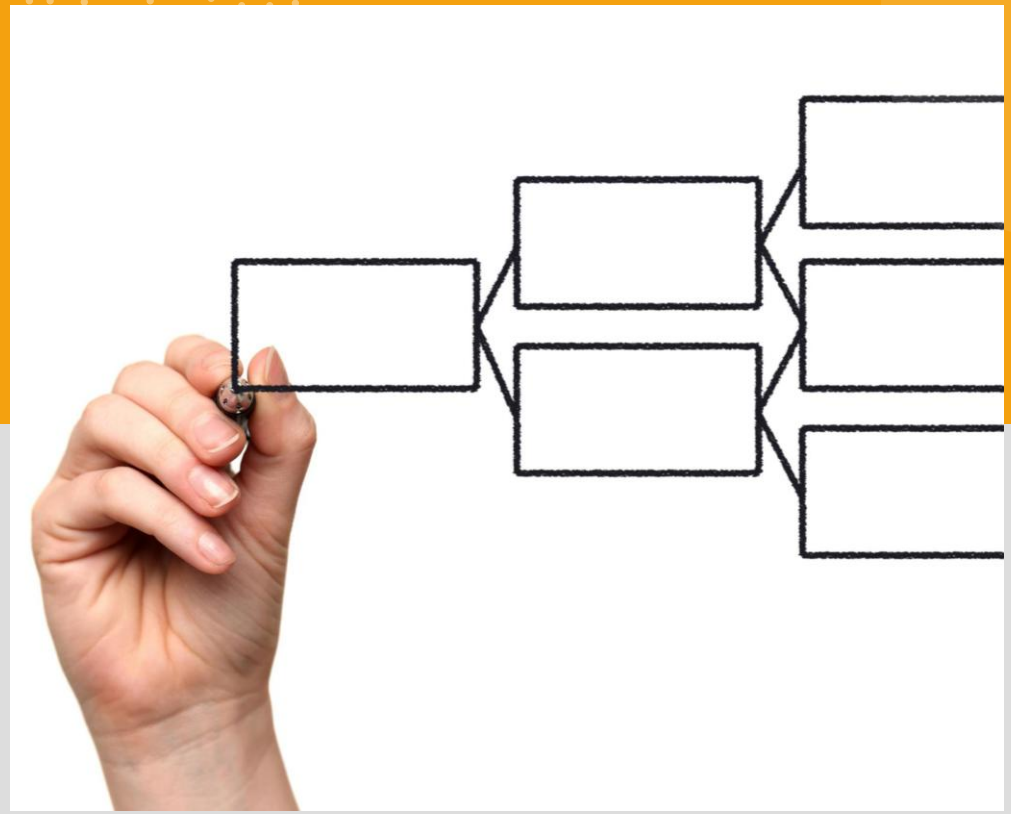
NIST Security Framework

NIST Security Framework - Organization Levels

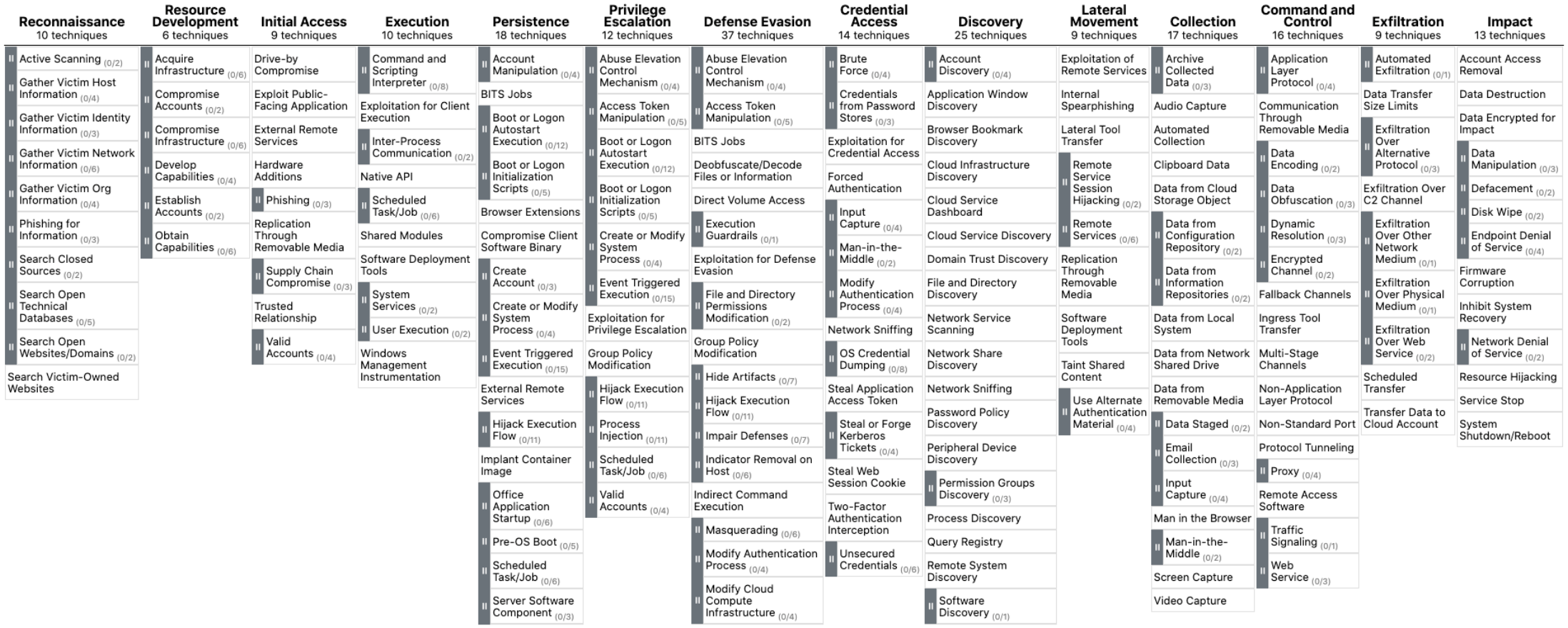


Understanding the MITRE ATT&CK Framework

- 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.

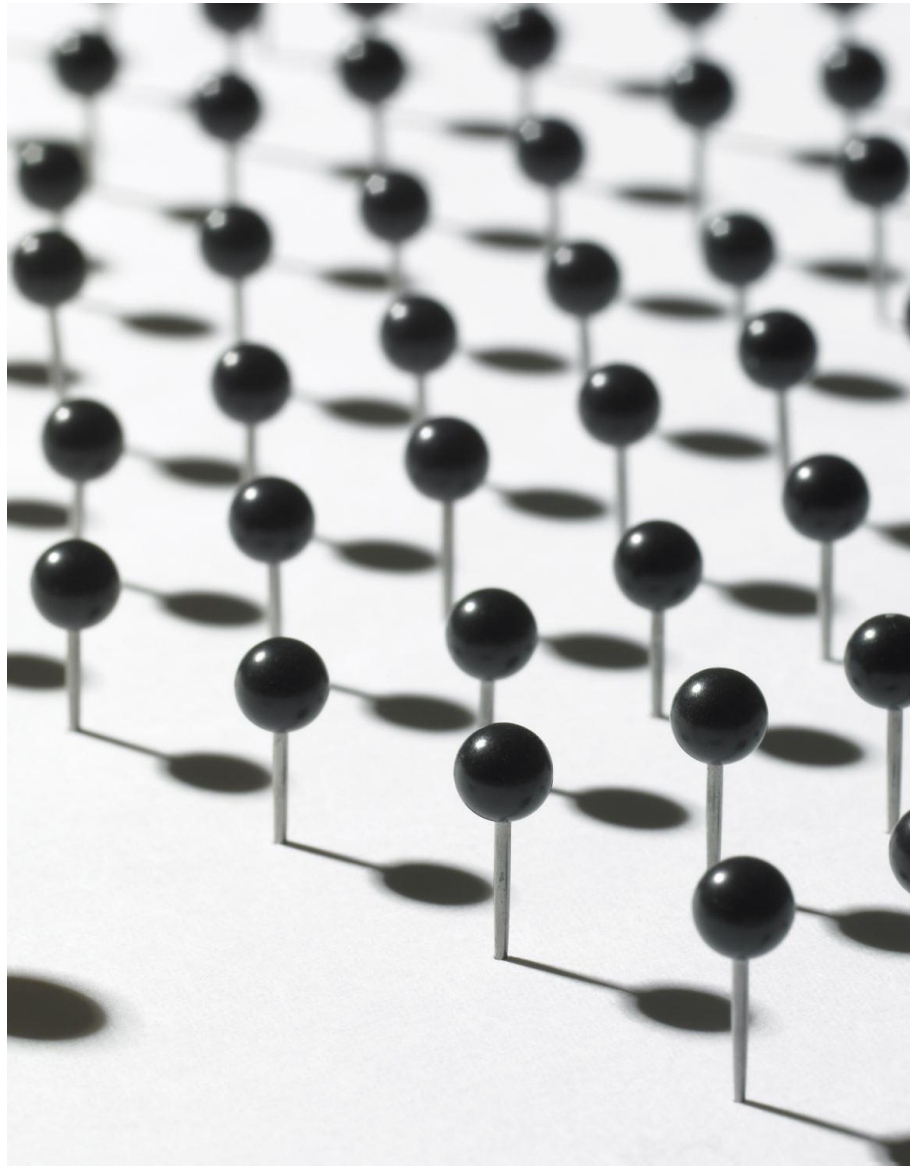


MITRE ATT&CK FRAMEWORK

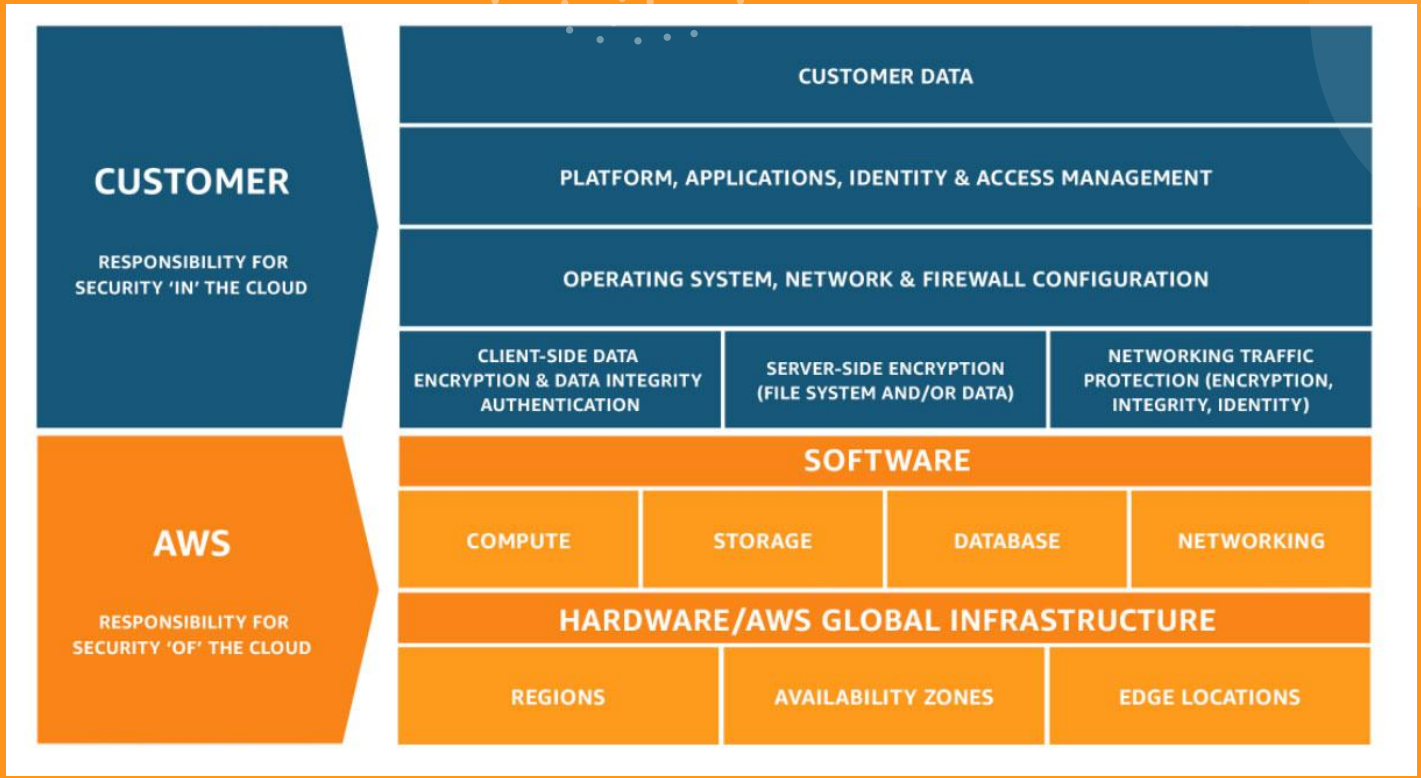


Security by Design

- 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://d1.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
- Atleast two AZ per regions
- Number of AZ per region will depend on the region

Our Agenda

Our Agenda

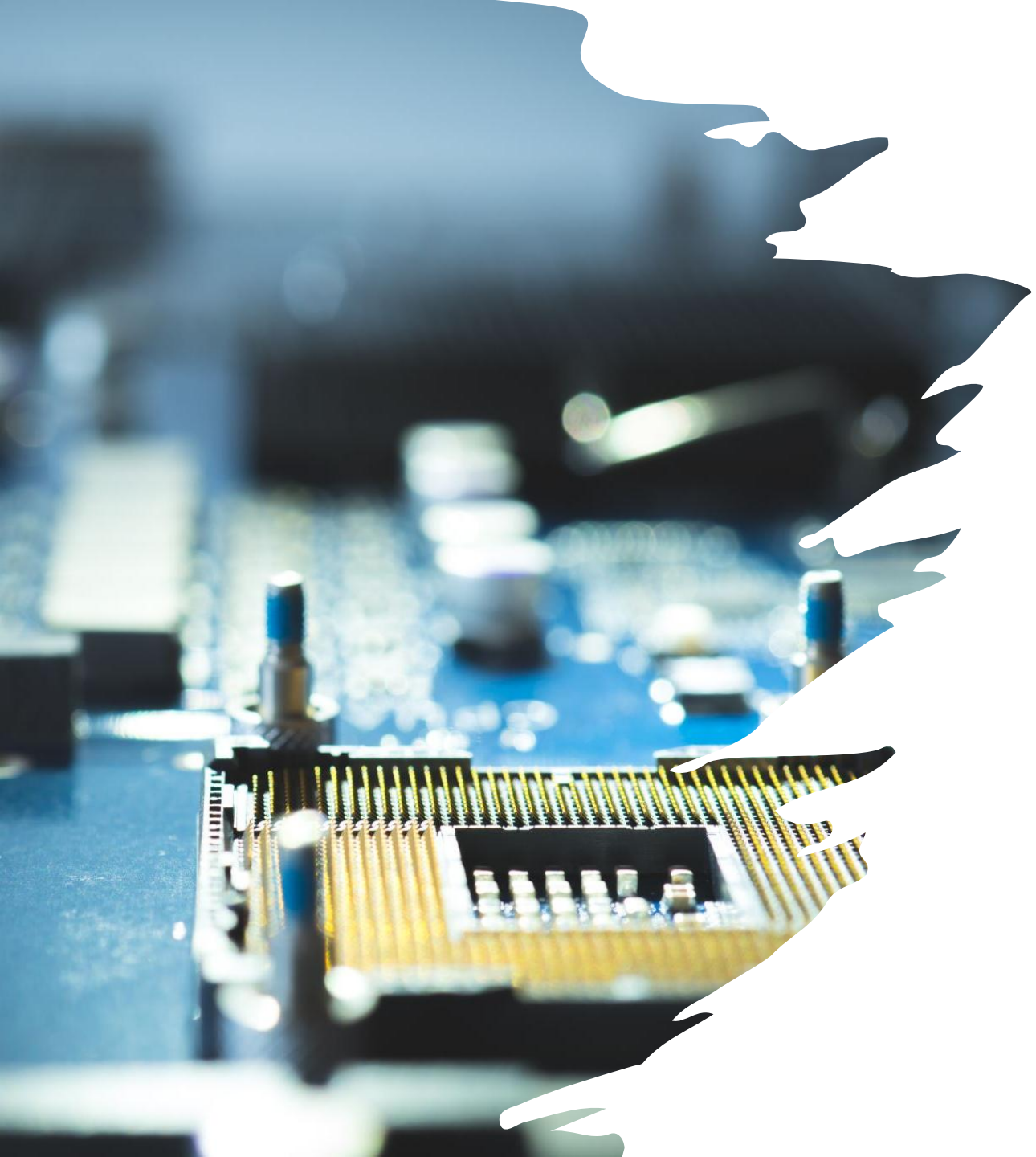
- Day 1: Introduction and Infrastructure Protection
  - Introduction to Security Specialization and Security Frameworks
  - Introduction to AWS
  - Basics of AWS (Networking and EC2)
  - Lab: Creating VPC and Protecting Subnets
- Afternoon
  - Protecting Storage (S3)
  - CloudFront and Web Application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

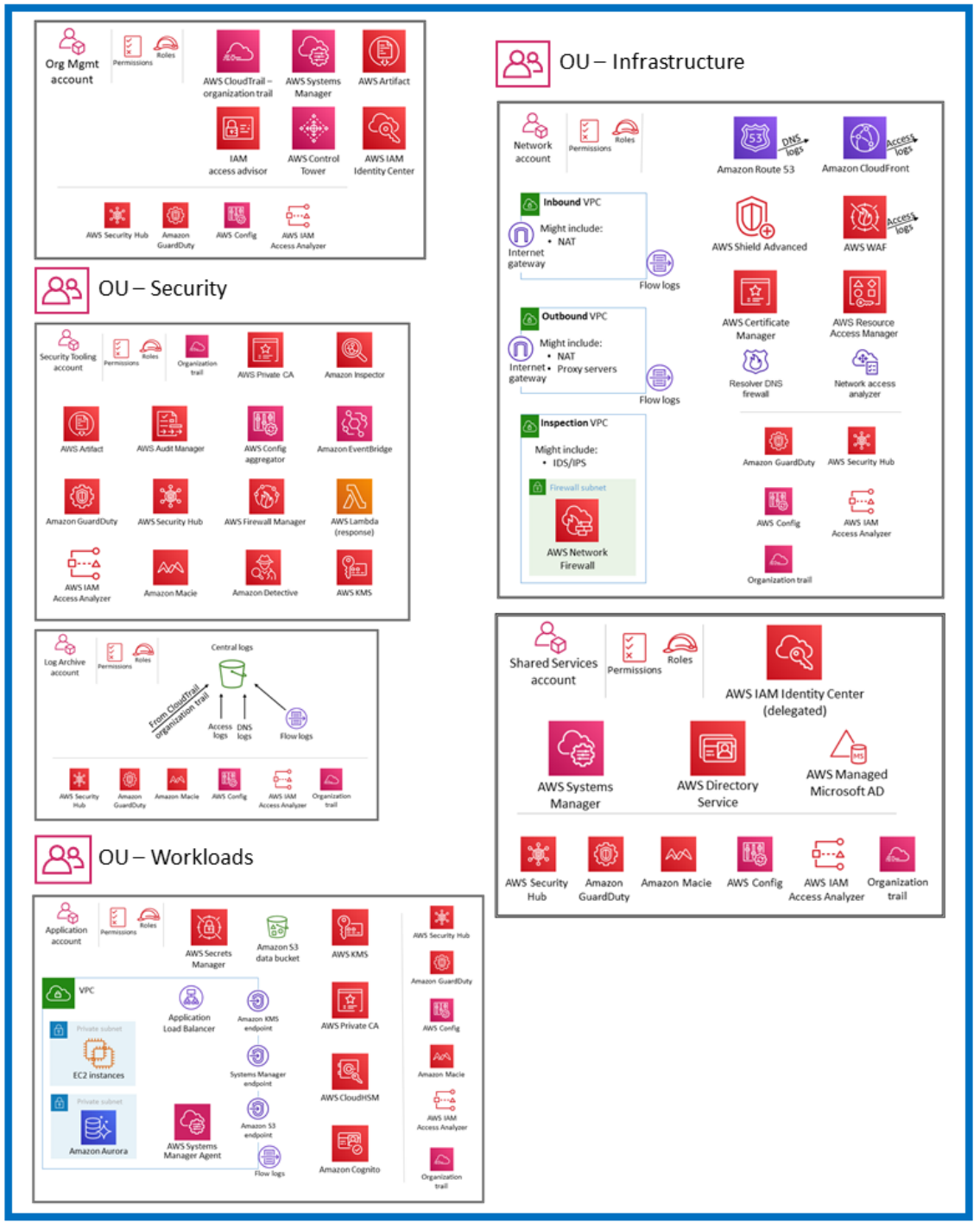
Threats & Mitigation

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



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