


CloudSiksha

Security Specialty

by S.Suresh




Topics to be covered

- Introduction
 - AWS Entry Points
 - Securing Web Apps
 - Securing Network Communication
 - Hybrid Environment Security
 - Monitoring, Log Collection & Log Processing
 - Data Security
 - Hybrid Network security
- 



Topics to be covered

- Account Management
 - Threat Detection and Monitoring Sensitive Data
 - Incident Response
 - Secrets Management
 - Serverless Security
- 

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

Pre-requisite

- Basic understanding of AWS services
 - **EC2, S3, VPC** at a minimum
- Well versed in Linux
 - **Lot of work will be done in Linux. Should know Linux commands and how to edit files in Linux**

Security WhitePaper

- Based on Security WhitePaper of AWS
- Available at
 - <https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>
 - **August 2016 version**
- All images taken from the Amazon Whitepapers unless specified otherwise

AWS Cloud Framework - Security Perspective

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.

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

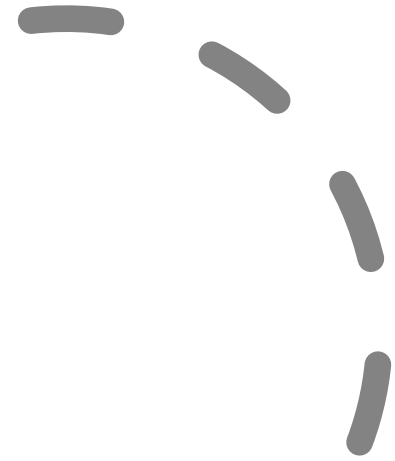
Number of AZ per region will depend on the region

Threats & Mitigation

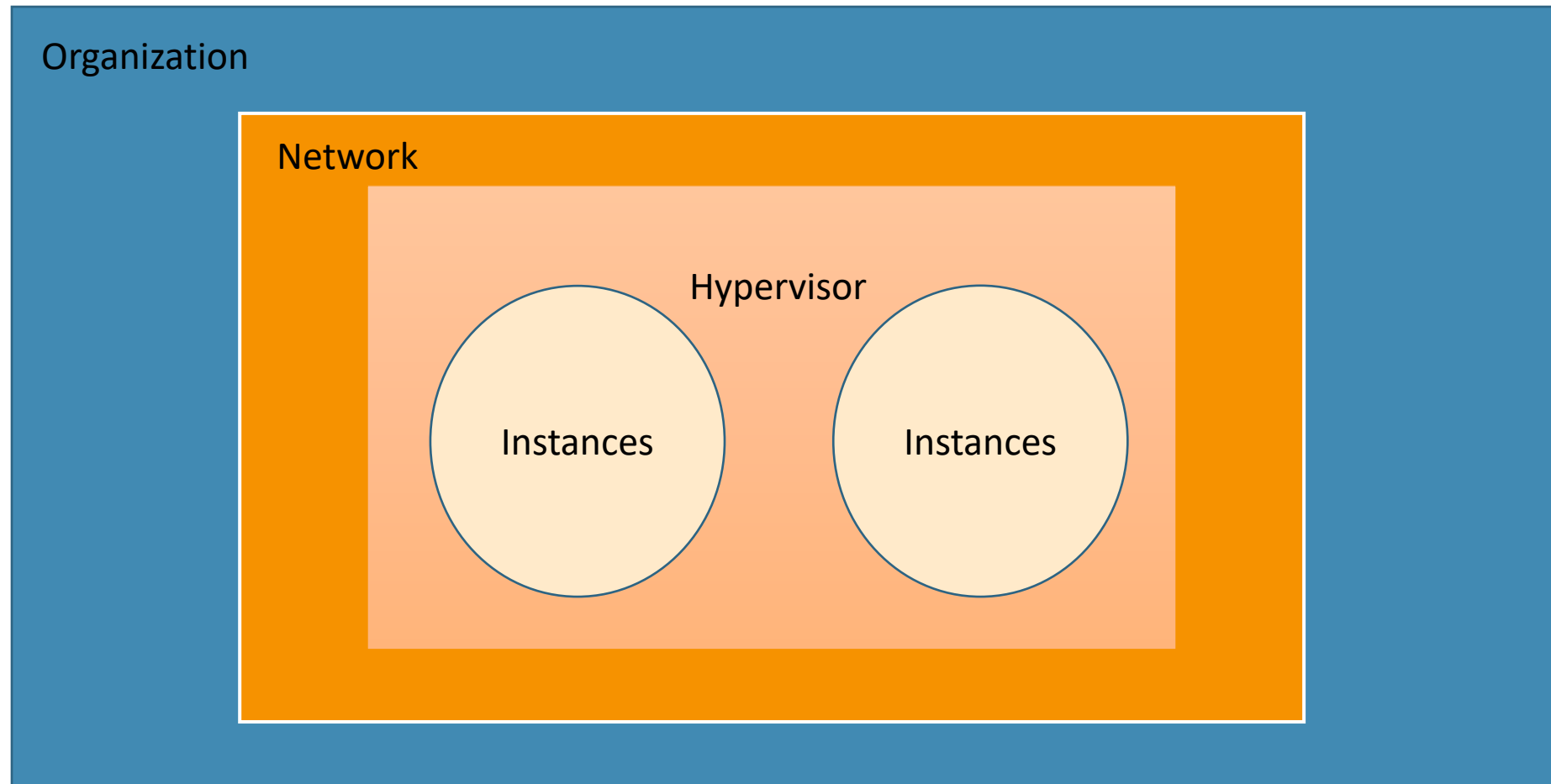
Threat	Mitigation
Spoofing	Authentication
Tampering	Integrity
Repudiation	Confirmation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Entry Points

- Console
- CLI
- SDK
- Other AWS Services
- Secure your APIs via signing
- Automatically signed if using Console/CLI/SDK

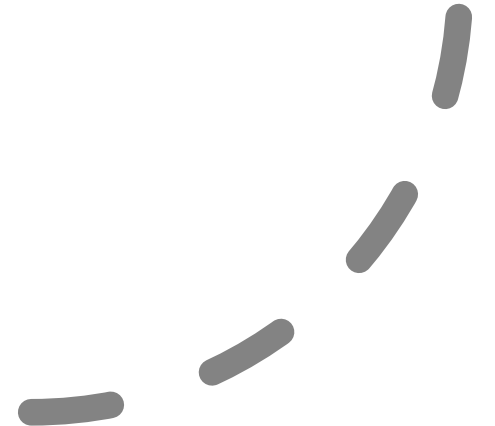


Levels of Security



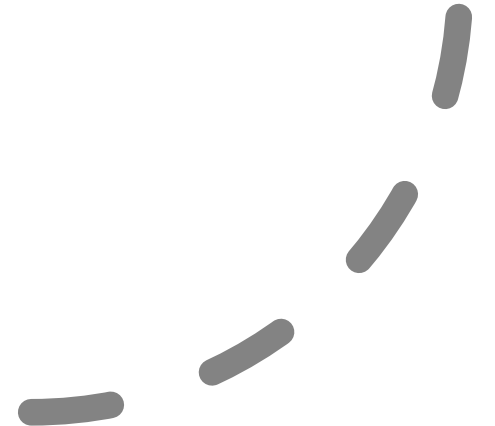
Organization Level Security

- Compliance
 - **AWS Config**
 - **SSM Patching**
- Identity & Access Management
 - **AWS Organizations**
 - **Federation**
 - **IAM Roles**
- Audit
 - **CloudTrail**
 - **CloudWatch Logs**



Network Security & Hypervisor Security

- Network Security
 - VPC
 - Private Subnets
 - Endpoints
 - NACL
 - WAFL
 - AWS Shield
- Hypervisor Security
 - Isolation of instances
 - Security Groups



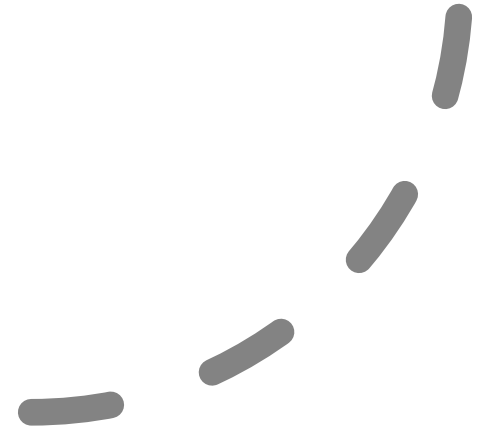
Instance Security & Logging

- Instance Security & Compliance
 - AWS Inspector
 - Security Groups
 - IDS/IPS
- Logging
 - CloudWatch Logs
 - CloudWatch Events
 - VPC FlowLogs
 - CloudWatch Metrics & Alarm



Data Security & AWS Services

- Encryption
 - KMS
 - CloudHSM
 - S3, EBS, DynameDB, RDS etc
- Certificates
 - AWS Certificate Manager
- Protecting S3
 - CloudFront
 - WAF
 - Signed URLs



Thanks



CloudSiksha