Shared Responsibility Model in Cloud Security

The Shared Responsibility Model explains how security responsibilities are divided between the cloud service provider and the customer.

Core Principle:
Cloud Provider is responsible for security OF the cloud.
Customer is responsible for security IN the cloud.

Why This Model Exists:
Cloud providers manage physical infrastructure and core services, while customers control configurations, identities, applications, and data.

Cloud Provider Responsibilities (Security OF the Cloud):

- Physical data center security
- Hardware lifecycle management
- Networking backbone
- Hypervisor and host OS
- Availability and redundancy of cloud infrastructure

Customer Responsibilities (Security IN the Cloud):

- Identity and Access Management (IAM)
- Operating system patching (IaaS)
- Application security and secure coding
- Network configuration (firewalls, security groups)
- Data protection and encryption
- Logging, monitoring, and incident response

Responsibility by Service Model:

- **IaaS:** Customer manages OS, apps, data, IAM
- **PaaS:** Customer manages apps, data, IAM
- **SaaS:** Customer manages users, access, and data

SOC & Incident Response Perspective:
Most cloud incidents occur due to customer misconfiguration, not cloud provider failures. SOC analysts use the Shared Responsibility Model to identify accountability during investigations.

Key Takeaway:
Understanding the Shared Responsibility Model is critical for cloud security roles, audits, and incident response. It helps clearly define accountability and prevent common security failures.