**Day 3**





**“CLOUD SECURITY”**

**Cloud Security vs Traditional IT security:**

* **Built-in tools** like encryption and AI-based threat detection.
* **Auto-scaling & patching** ensure faster updates than manual IT.
* **24/7 monitoring** by expert teams for quicker response.
* **Global compliance** with industry standards.
* **Disaster recovery** is more reliable with backups and redundancy.
* **Shared responsibility** improves focus on security at all levels.

**Cloud Security: Shared Responsibility**

* In cloud security, responsibilities are shared between the cloud provider and the cloud consumer.
* Provider secures the infrastructure (hardware, network, storage).
* Consumer is responsible for securing data, user access, and application settings.
* Responsibility varies by service model: SaaS < PaaS < IaaS (consumer has more control in IaaS).

**Elements of Cloud Security:**

1. **Identity Access Management (IAM)**

* IAM provides role-based access control to users based on their responsibilities.
* It includes policies, processes, and technologies to manage digital identities securely.
* Supports Single Sign-On (SSO), Identity Federation, and Multi-Factor Authentication (MFA) for enhanced access security.
* Helps monitor, create, and revoke user access efficiently across cloud systems.

1. **Data Storage Security**

* Always back up data locally to avoid loss and ensure business continuity.
* Avoid storing sensitive data (e.g., IP, legal documents) directly on the cloud.
* Use encryption (local or cloud-provided) before uploading data.
* Ensure strong key management practices and regular password updates.
* Use two-step verification, antivirus, and admin controls for extra protection.
* Periodically test cloud data security to identify and fix vulnerabilities.

1. **Network Security**

* Main Challenge: Cloud consumers face limited network visibility, making it hard to detect suspicious activity.
* Key Features: Requires encryption, MFA, firewalls, and data loss prevention beyond traditional security.
* Protection Methods: Use DMZs, subnet isolation, IDS/IPS, and secure traffic control (ACLs, NSGs, IPsec).

1. **Monitoring**

* **Purpose**: Cloud monitoring manages cloud infrastructure, detects threats, and safeguards data and services.
* **Key Activities to Monitor**: Track **data replication**, **file name changes**, **classification changes**, and **ownership changes** to detect unauthorized access.
* **Monitoring Plan**: Define **thresholds**, set **alert rules**, and identify **key metrics/events** critical to business operations.

1. **Logging**

* Purpose: Security logs help in threat detection, compliance audits, and root cause analysis in cloud environments.
* Best Practices:
  + Aggregate all logs into SIEM/log analytics tools for centralized visibility.
  + Capture key data (who, what, when, where, and why) for actionable insights.
  + Ensure scalability and avoid overloading applications with excessive logging.
* Challenge: With many cloud servers, managing log volume and granularity is complex and requires optimized configuration.

**--The End--**