



**Day 30**



## **“CLOUD SECURITY”**

### **Amazon CloudFront**

- A secure CDN that delivers data, apps, video, and APIs globally with low latency & high speed.
- Security Features:
  - HTTPS & field-level encryption.
  - Prevents network & application layer DDoS attacks.
  - Integrates with AWS WAF, AWS Shield, Route 53 for extra defense.
- Integration: Works with EC2, S3, ELB to boost performance and availability.
- Compliance: PCI DSS, HIPAA, SOC 1/2/3 certified.
- Key Point: Must prevent users from bypassing CDN to access origin directly.

### **AWS Shield (DDoS Protection)**

- Purpose: Protects applications from DDoS attacks with always-on detection & auto-mitigation.
- Shield Standard:
  - Free, built-in with AWS.
  - Protects against Layer 3 & 4 attacks (network & transport).
  - Works with CloudFront, Route 53, ELB, EC2.
- Shield Advanced:
  - Paid, stronger defense for complex/large-scale DDoS.
  - Includes 24/7 AWS DDoS Response Team (DRT).
  - Extra protection for EC2, Route 53, CloudFront.
  - Detailed DDoS attack logs & reports

### **Amazon Inspector**

- Automated security assessment tool.
- Checks apps before & during deployment for vulnerabilities, deviations, and network issues.
- Uses a rule database updated by security researchers.
- Provides findings with severity levels to prioritize fixes.
- Ensures compliance with best practices & policies.

### **Amazon CloudWatch**

- Monitoring & observability service for AWS apps.
- Collects logs, metrics, events for analysis.
- Detects abnormal behavior & security issues.
- Enables performance monitoring, troubleshooting, and health checks.
- Ensures smooth application performance by correlating real-time data

--The End--