Day 18: AWS CloudTrail and ELK Stack

AWS CloudTrail – Overview

CloudTrail tracks API activity and stores logs securely.

Monitors AWS Console, CLI, SDK usage

Logs sent to S3

Supports multi-region logging

Integrates with CloudWatch for alerting

CloudTrail Use Cases

Security Auditing: Detect unauthorized access

Operational Monitoring: Track changes to EC2, etc.

Compliance: Audit trails for governance

Automation: Trigger events using Lambda

Introduction to ELK Stack

ELK = Elasticsearch + Logstash + Kibana

Elasticsearch: Stores and indexes logs

Logstash: Collects, processes, and forwards logs

Kibana: Visualizes logs and metrics in dashboards

DevOps Use Cases for ELK

Why ELK is used in DevOps:

Debug EC2, Lambda, ECS logs

Visualize system health and metrics

Detect anomalies or failed logins

Create alerting based on log patterns