Day 10/13 -Module 10

·Monitoring, compliance, and Governance in the AWS cloud

Secure - Protect data, systems and infrastructure from unauthorised access, use, disclosure, disruption, modification or destruction.

Monitor - continuously observe and analyze system activity, network traffic, and security events to detect potential threats or anomalies.

Audit - periodically review and assess the effectivenes of security controls and check that all requirements are met and security policies and procedures are adhered to.

Compliance - Help ensure that an organization's security practices and controls meet the requiremen of relevant regulations, industry standards and contractual obligations.

1. ~~Monitoring~~ Monitoring

→ observing systems, collecting metrics and then using data to make decisions.

Benefits:

(I) maintain security (II) Respond proactively
(III) ensure reliability (IV) Monitor costs
(V) Improve performance.

EF2 Amazon Cloudwatch

Metrics : variables tied to your resources

Amazon Cloudwatch Alarm : Monitors a metric and automatically triggers an action (like notification or scaling) when it crosses a defined threshold.

Dashboard - A customizable visual panel that displays real-time metrics, logs and alarms from multiple AWS resources in one centralized view

Logs - Cloud watch Logs centralize the logs from all of the systems, applications, and AWS services that you use.

Benefits:

→ Access all your metrics from a central location

→ Gain visibility into your applications, infrastructure, and services.

→ Reduces Mean Time to Repair (MTTR) and Improve Total cost of ownership (TCO)

→ Drive insights to optimize applications and operational resources.

#3 AWS Cloud Trail

- → Every request gets logged in Cloud Trail
- → Audit logs of AWS API calls.
- → Save logs indefinitely
- → Store in secure S3 buckets
- → Tamper-proof

Events - Records API activity and account actions (who did what, when, from where)

Cloud Trail logs: Stores detailed event history in log files (usually in S3) for auditing and compliance.

CloudTrail Insights: Detects [illegible] unusual API activity patterns (e.g. sudden spike in calls) using anomaly detection.

API calls, user activity, auditing, compliance - Cloud Trail
Metrics, CPU usage, monitoring performance, alarms
→ Cloudwatch

#4 compliance

compliance - Adhering to legal, regulatory, and industry security standards and requirements.

AWS compliance center: A central portal that provides information about AWS compliance programs, certifications and security standards. (FAQ | stories)

AWS Artifacts: A self-service portal to download AWS compliance reports and agreements (like SOC Reports, ISO Certificates, NDA)

#5 Auditing AWS Resources for compliance

AWS config

AWS Config is a service that you can use to asses, audit and evaluate the configurations of your AWS resources.

→ continuously track changes
→ create custom Rules
→ Generate compliance Reports.

AWS Audit Manager

→ It continually audits your AWS usage to simplify risk and compliance assessment. It helps collect evidence and manage audit data

→ Assess your policies
→ Mange reviews of stakeholder
→ Build audit-ready reports
→ provides prebuilt frameworks

#6. AWS Organisations

→ A central location to manage multiple AWS accounts.

Organisational Unit (OU) - A logical container used to group multiple AWS accounts so you can apply policies (like SCPs) to them collectively.

SCP (Service control Policy) → A policy in AWS Organisations that sets maximum permission boundaries for accounts within an OU or the entire org (It restricts what IAM users/roles can do, but does not grant permissions)
→ It applie to OU and individual member account

#7 Governance

A framework to manage your IT goals with policies, processes, and structures to ensure adherence

AWS Control Tower- A service you can use to set up and govern a secure, compliant, multi-account AWS environment based on best practices.

Service Catalog: A service you can use to create, share, organise AWS services and resources from a curated catalog that you define.

Licence Manager: A service that helps you manage your Software licences and fine-tune ~~licenticing~~ licensing costs.

initial setup + governance + guardrails → control Tower
Restricted provisoning from predefined list → Service Catalog.
licence compliance or cost control → Licence Manager.

#8 AWS Health Dashboard provids personalized, real-time information about AWS service events and how they impact your specific resources.

#9 AWS Trusted Advisor : provides real-time best recommendations for cost optimization, performance, security, fault tolerance and Service Limits.

IAM Access Analyzer : Identifies external and unused access by analyzing IAM policies to enforce least privilege and validate permissions against security standards.