AWS

Security

VPC and GuardDuty

Key things to know

- **Network Access Control Lists** - control inbound and outbound traffic at the subnet level
- **Security Groups** - act as a firewall at the EC2 level to control inbound and outbound traffic
- **VPC Flow logs** - capture information about how traffic is flowing
- **GuardDuty** - analyses data from VPC Flow Logs, and profiles them for anomaly detection. This service can detect a brute force attack on an EC2, suspicious API calls, or unauthorised behaviour

S3 and Macie

Key things to know

- **IAM policies** - control access to S3, and bucket policies to make sure buckets are kept private
- **MFA Delete and Versioning** - stops accidental deletion of objects and allow objects to be recovered using Cross-region replication
- **Amazon S3 Object Lock** - locks objects to prevent them being deleted during a fixed term or indefinitely
- **KMS or S3-Managed Keys** - for Server Side Encryption
- **Macie** - identifies personally identifiable information, API keys, and credentials

AWS

Security

EC2 and Inspector

Key things to know

- **Security Groups** - control inbound and outbound traffic to instances
- **Elastic Block Store (EBS) Encryption** - adds an extra layer of security
- **Inspector** - checks for access to your instances from the internet, remote root login being enabled, or vulnerable software versions installed

RDS and Redshift

Key things to know

- Encrypt data using AES-256 level encryption
- Encrypt data in transit using SSL. This creates and installs the certificate when the instance is provisioned
- When using Redshift, enable cluster encryption to encrypt user-created tables

CloudTrail

Key things to know

- Enable CloudTrail to provide a history of API calls made across your account
- Integrate with CloudWatch and SNS to support compliance and monitoring by setting up logs, metrics and alarms