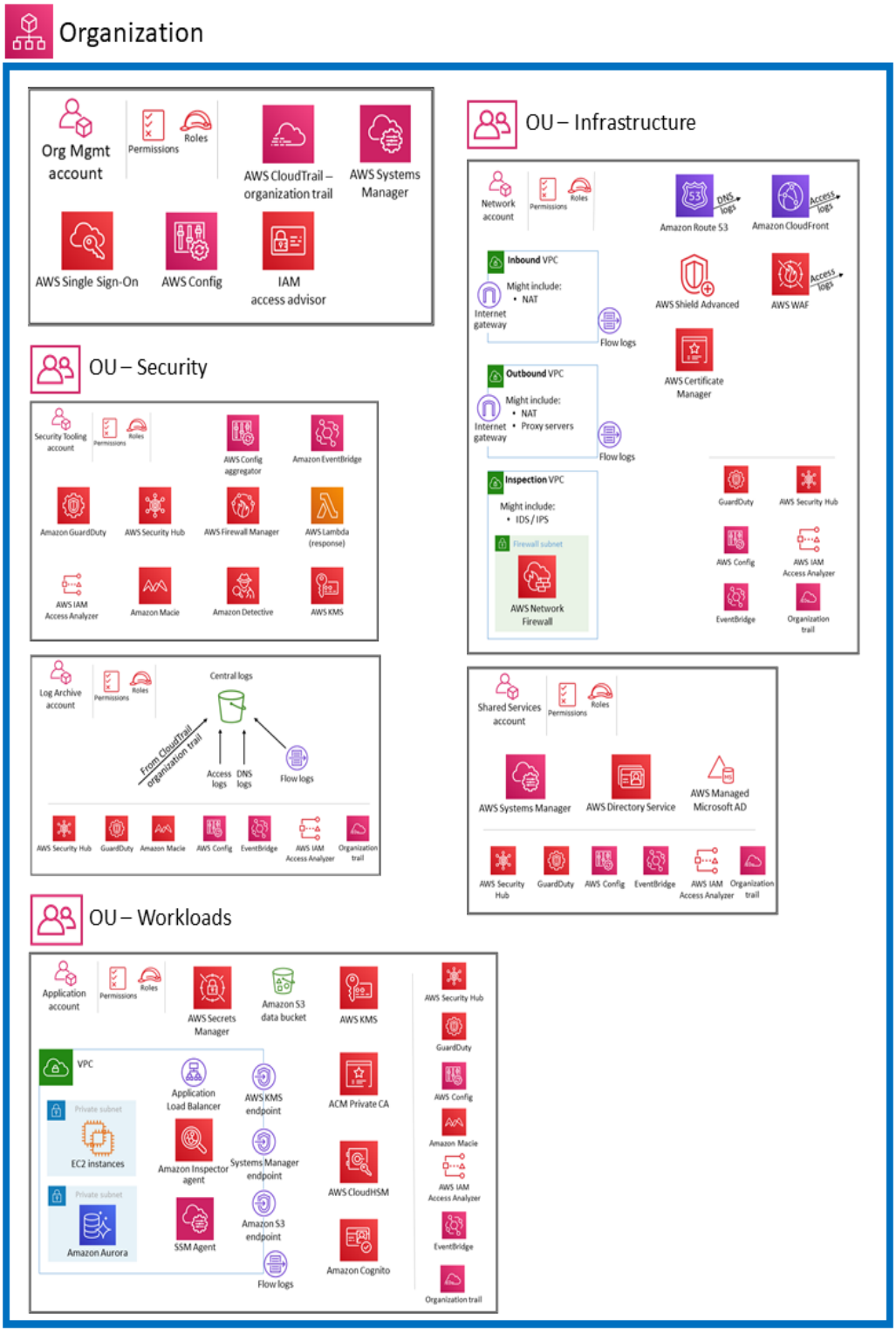
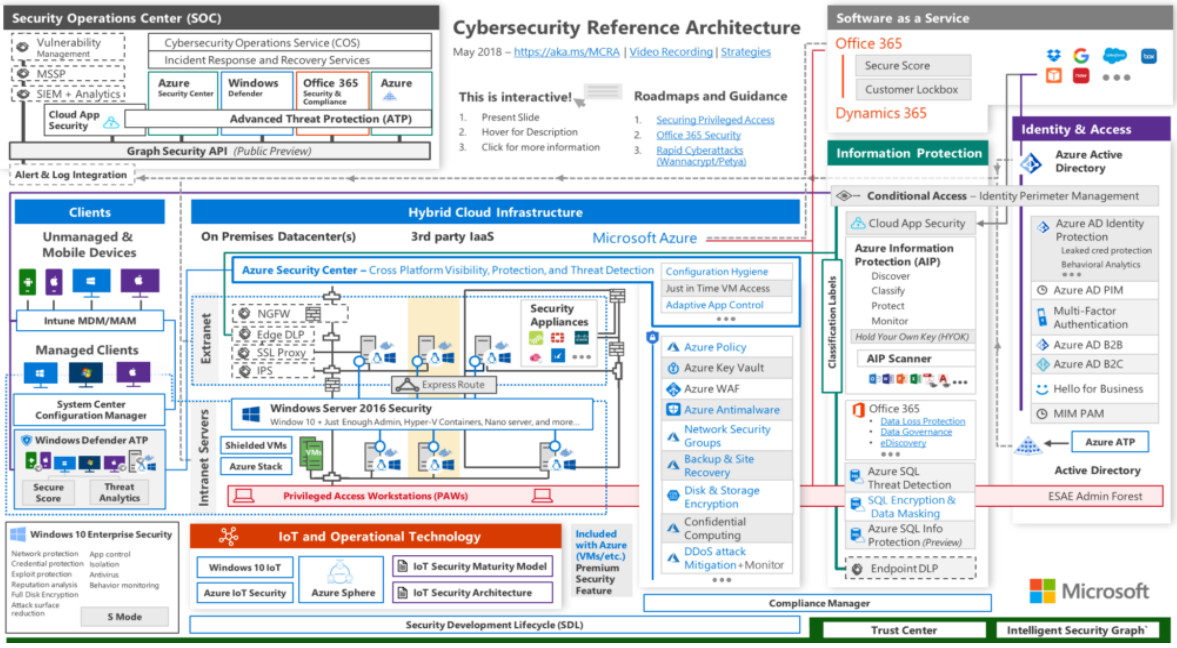
Multi cloud security operation knowledge base

CSP security reference architecture

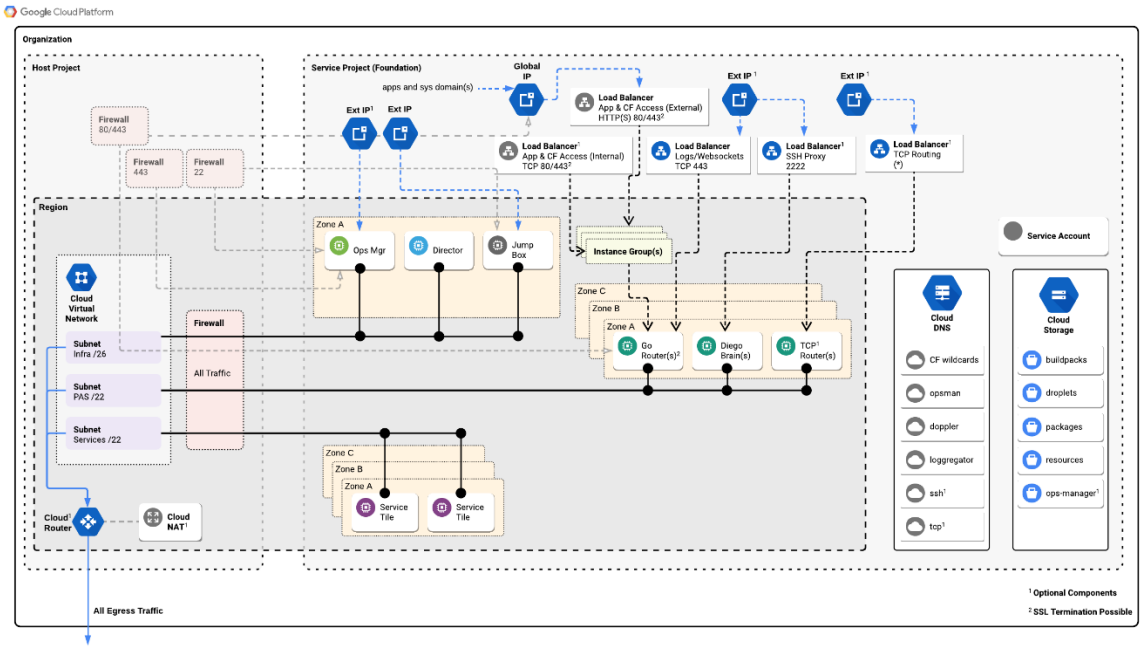
a. AWS security reference architecture



b. Azure security reference architecture



c. GCP security reference architecture



1. Multi cloud security essential knowledge base

- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by AWS, Azure, GCP
- Evaluate the trustworthiness of AWS, Azure, GCP based on their security documentation, service features, third-party attestations, and position in the global cloud ecosystem
- Create accounts and use the services of AWS, Azure, GCP and be comfortable with the self-service nature of the public cloud, including finding documentation, tutorials, pricing, and security features
- Articulate the business and security implications of a multi-cloud strategy
- Secure access to the consoles used to access the AWS, Azure, GCP environments
- Use command line interfaces to query assets and identities in the cloud environment
- Use hardening benchmarks, patching, and configuration management to achieve and maintain an engineered state of security for the cloud environment
- Evaluate the logging services of AWS, Azure and use those logs to provide the necessary accountability for events that occur in the cloud environment

Practice guide

- Configure the command line interface (CLI) and properly protect the access keys to minimize the risk of compromised credentials in AWS/Azure
- Use basic Bash and Python scripts to automate tasks in the AWS/Azure cloud
- Implement network security controls that are native to both AWS and Azure
- Employ an architectural pattern to automatically create and provision patched and hardened virtual machine images to multiple AWS and Azure accounts
- Use Azure Security Center to audit the configuration in an Azure deployment and identify security issues
- Use AWS security hub to audit the configuration in an AWS deployment
- Use HashiCorp’s Terraform to deploy a complete "infrastructure as code" environment to multiple cloud providers(AWS, Azure, GCP)
- Leverage the Cloud Security Alliance Cloud Controls Matrix to select the appropriate security controls for a given cloud network security architecture and assess a CSP's implementation of those controls using audit reports and the CSP's shared responsibility model
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your "inner red teamer" to compromise a full stack cloud application
- Use logs from AWS and virtual machines hosted in the Azure to detect a security incident and take appropriate steps as a first responder according to a recommended incident response methodology
- Perform a preliminary forensic file system analysis of a compromised virtual machine to identify indicators of compromise and create a file system timeline

2. Multi cloud security (AWS, Azure, GCP)

- Practice Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth
- Practice the intricacies of Identity and Access Management(AWS, AZURE,GCP), one of the most fundamental concepts in the cloud and yet one of the last understood
- Understand how AWS, Azure, GCP cloud networking and how locking it down is a critical aspect of defense in depth in the cloud
- Analyze how AWS, Azure, GCP handle encryption at rest and in transit in order to prevent sensitive data loss

- Explore the service offering landscape of AWS, Azure, GCP to discover what is driving the adoption of multiple cloud platforms and to assess the security of services at the bleeding edge
- Understand the complex connections between cloud accounts, providers, and on-premise systems and the cloud amongs AWS, Azure, GCP
- Perform secure data migration to and from the AWS cloud to Azure, GCP
- Use open source Terraform Infrastructure-as-Code well enough to share it with your engineering team as a starting point for implementing the controls discussed in the course
- Use HashiCorp language configuration(HCL) to configure the infrastructure-as-code for AWS, Azure, GCP VM and containers.

3. Application security defender (securing Web applications, API, microservice and serverless)

4. Cloud Penetration Testing

- Conduct cloud-based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments

5. Cloud Security Automation

using enterprise tools such as Jenkins, GitLab, Puppet, Vault, and Grafana to automate Configuration Management ("Infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), cloud infrastructure, containerization, micro-segmentation, Functions as a Service (FaaS), Compliance as Code, and Continuous Monitoring.

- Recognize how DevOps works and identify keys to success
- Utilize Continuous Integration, Continuous Delivery, and Continuous Deployment workflows, patterns, and tools
- Identify the security risks and issues associated with DevOps and Continuous Delivery
- Use DevOps practices to secure DevOps tools and workflows
- Conduct effective risk assessments and threat modeling in a rapidly changing environment
- Design and write automated security tests and checks in CI/CD
- Understand the strengths and weaknesses of different automated testing approaches in Continuous Delivery
- Implement self-serve security services for developers
- Inventory and patch your software dependencies
- Threat model and secure your build and deployment environment
- Automate configuration management using Infrastructure as Code
- Secure container technologies (such as Docker and Kubernetes)
- Build continuous monitoring feedback loops from production to engineering
- Securely manage secrets for continuous integration servers and applications
- Automate compliance and security policy scanning
- Understand how to automate cloud architecture components

- Use CloudFormation and Terraform to create Infrastructure as Code
- Build CI/CD pipelines using Jenkins and CodePipeline
- Wire security scanning into Jenkins and CodePipeline workflows
- Containerize applications with Elastic Container Service and Azure Kubernetes Service
- Integrate cloud logging and metrics with Grafana
- Create Slack alerts from CloudWatch metrics
- Manage secrets with Vault, KMS, and the SSM Parameter store
- Protect static content with CloudFront Signatures
- Leverage Elastic Container Service for blue/green deployments
- Secure REST APIs with API Gateway
- Implement an API Gateway custom authorization Lambda function
- Deploy the AWS WAF and build custom WAF rules
- Perform continuous compliance scans with CloudMapper
- Enforce cloud configuration policies with Cloud Custodian