

Common Cloud Security Controls

4.5 Given a scenario, apply security controls in the cloud

Description

- In this episode, we will look over common security controls used in cloud environments, such as Endpoint Protection, Data Loss Prevention(DLP), Intrusion Detection/Prevention Systems(IDS/IPS), Distributed Denial-of-Service(DDoS) Protection, Identity and Access Management(IAM) Policies, and Firewalls.

Resources

- <https://aws.amazon.com/mp/scenarios/security/ids/>
- <https://www.cloudflare.com/ddos/>
- AWS-IAM-S3-UserAccess-Policy.txt

Learning Objectives

- Describe common cloud security controls such as Endpoint Protection, Data Loss Prevention(DLP), Intrusion Detection/Prevention Systems(IDS/IPS), Distributed Denial-of-Service(DDoS) Protection, Identity and Access Management(IAM) Policies, and Firewalls.

Notes

- Endpoint protection
- Data loss prevention (DLP)
 - Protects systems from leaking sensitive data
 - Regulated data
 - Financial data
 - PII
 - Intellectual Property
- Intrusion prevention system/intrusion detection system (IPS/IDS)
 - <https://aws.amazon.com/mp/scenarios/security/ids/>
- Distributed denial-of-service (DDoS) protection
 - <https://www.cloudflare.com/ddos/>
- Identity and access management (IAM) policies
 - AWS-IAM-S3-UserAccess-Policy.txt
- Firewall
 - Network access control list (ACL)
 - Web application firewall (WAF)
 - Network security group