Module 7
Fundamental Cloud Security

STRIDE
- spoofing
- tampering
- repudiation
- information disclosure
- denial-of-service
- elevation of privilege

Threats
- data-oriented
  - denial-of-service
  - insufficient authorization
  - virtualization attack
  - overlapping trust boundary
- access-oriented
  - buffer overrun
  - information leakage
  - XML parser attack
  - malicious intermediary

Trust Assurance Patterns
- Cloud Key Management
- Trust Attestation Service
- Collaborative Monitoring and Logging
- Independent Cloud Auditing
- Threat Intelligence Processing

Network Protection Patterns
- Cloud Denial-of-Service Protection
- Cloud Traffic Hijacking Protection
- Automatically Defined Perimeter

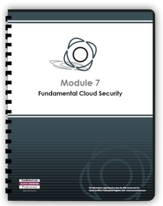
Secure Network Connection Patterns
- Secure On-Premise Internet Access
- Secure External Cloud Connection
- Secure Connection for Scaled VMs

Cloud Identity and Access Management Patterns
- Cloud Authentication (compound)
- Cloud Authentication Gateway
- Federated Cloud Authentication

Threat Agents
- external attacker
- malicious service agent
- malicious tenant
- malicious insider

Foundations
- cryptography
  - user/consumer management
  - credential management
  - authentication
  - authorization
- trust assurance
- identity and access management (IAM)
- AIC triad
  - availability
  - integrity
  - confidentiality

Mechanisms
- application delivery controller (ADC)
- domain name service (DNS)
- intrusion detection and prevention system (IDPS)
- certificate
- virtual private network (VPN)
- cloud consumer gateway (CCG)
- virtual private cloud (VPC)
- VPN cloud hub
- live VM migration
- virtual firewall
- traffic monitor
- traffic filter
- automatically defined perimeter (ADP) controller
- identity and access management (IAM)
- certificate authority (CA)
- certificate revocation list (CRL)
- public key infrastructure (PKI)
- authentication gateway service (AGS)
- certificate validation service (CVS)
- cryptographic key management system (CKMS)
- trusted platform module (TPM)
- attestation service
- orchestration engine
- security information and event management (SIEM) system
- endpoint threat detection and response (ETDR)
- honeypot
- network forensics monitor
- malware hash
- sandbox
- threat intelligence system



Certified Cloud Security (CCA) Program
Module 7: Fundamental Cloud Security
Official Mind Map Supplement
www.cloudselfstudy.com

CloudSchool.com™
CLOUD CERTIFIED
Professional

CloudSchool.com™ Cloud Certified Professional (CCP) Program
www.arcitura.com • www.cloudschool.com
Copyright © Arcitura Education Inc.