

CCP MODULE 08

Advanced Cloud Security

This advanced course covers cloud security mechanisms and architectural design patterns that address data and access control security for virtual machines, as well as trust boundaries, geotagging and BIOS security.

The course also explains common methods used by attackers to breach organizational resources and provides a methodology for countering such attacks. The course concludes by demonstrating the relationship between threats, attacks, and risks via threat modeling.

The following primary topics are covered:

- Cloud Service Security Patterns and Supporting Mechanisms
- Virtual Machine Platform Protection Patterns
- Considerations for Setting Up Secure Ephemeral Perimeters
- Trusted Cloud Resource Pools and Cloud Resource Access Control
- Permanent Data Access Loss Protection
- Cloud Data Breach Protection
- Isolated Trust Boundaries
- The Attack Lifecycle and the Security Lifecycle
- Proactive Mitigation vs. Incidence Response
- Threats, Vulnerabilities, Impacts from Exploitation
- Threat Modeling, Threats and Mitigations

Duration: 1 Day

Arcitura®
CERTIFIED
Cloud Security
Specialist

CERTIFICATION

This course is part of an accreditation curriculum through which one or more official certifications can be achieved.



EXAM C90.08

Exams are generally available at Pearson VUE testing centers worldwide, via Pearson VUE online proctoring and on-site delivery as part of private workshops.



STUDY KIT CONTENTS

This course is available as part of an Arcitura Study Kit that includes the contents listed below. In addition to the base course materials used during training workshops, additional materials designed for self-study purposes are also included.

- Presentation Booklet
- Workbook
- Self-Study Guide
- Mind Map Poster
- Flashcards
- Audio Tutor Recordings (usb)

