CompTIA Cloud+, Part 7 of 8: Security in the Cloud

Meet the expert: Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

Prerequisites: This course assumes you are familiar with the basic concepts of cloud computing, either from completing CompTIA Cloud+ Parts 1-6 or through outside study.

Runtime: 01:28:31

Course description: Learn about implementing security in cloud computing models by examining the best practices for network security and how to utilize them to secure data and resources, both on-premise as well as in the cloud. This includes the need to assess and audit the network, using established frameworks, using a layered security approach, and more. Discover concepts of data security and how to use simple forms including authentication and authorization to determine resource access authorizations, and examine security mechanisms to ensure data confidentiality through encryption and data integrity using digital signatures. Finally, take a look at concepts including single sign-on and multi-factor authentication to help you better understand data security in various environments, as well as various access control methods utilized in cloud computing environments to maintain data security.

Course outline:

Best Practices For Network Security
- Introduction
- Bests Practices for Network Security
- Assess and Audit the Network
- Established Industry Frameworks
- Layered Security Approach
- DMZ
- Third Party Audits
- Host and Guest Hardening
- Host and Guest Hardening Concepts
- Penetration Testing
- Vulnerability Assessment
- Storage Resources
- Summary

Understanding Data Security
- Introduction
- Understanding Data Security
- Additional Mechanisms
- Public Key Infrastructure
- Encryption Concepts
- Symmetric Encryption
- Asymmetric Encryption
- Digital Signatures
- Ciphers
- Encryption Protocols
- Summary

Understanding Access Controls
- Introduction
- Understanding Access Controls
- Role Based Access Control
- Mandatory Access Control
- Discretionary Access Control
- Multifactor Authentication
- Single Sign On (SSO)
- Federation
- Summary