# LESSON: Cloud Security Architecture

## Before you Begin

This is the very last lesson of this course. Instructors should not spend any time explaining how to access TDX Arena or how to navigate canvas. Note that if, for some reason, you are behind in the slides or labs in terms of pacing or timing, you absolutely must finish up in this module.

For this lesson, instructors are required to ensure the following activities are completed:

- Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
- Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
- Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them if needed.
- For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
- Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
- At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.

## Summary

In this lesson, learners will explore identity and access management (IAM) principles, emphasizing its crucial role in managing digital identities and ensuring secure access in cloud environments. This lesson covers IAM scalability, data protection, and auditability, including role-based access control (RBAC) and cloud multi-factor authentication (MFA). Learners delve into cloud networking, understanding virtual private clouds (VPCs), security groups, network segmentation, and tools for network traffic analysis. Data security topics, including encryption strategies, data loss prevention (DLP) tools, and best practices for AWS Simple Storage Service (S3), will be covered. The lesson extends to cloud database security,

SDLC security integration, serverless computing challenges, and Application Programming Interface (API) security, concluding with cloud application security best practices, ensuring a comprehensive understanding of security measures in diverse cloud scenarios.

## Objectives

- Define identity and access management (IAM) and recognize its importance in cloud security.
- Compare and contrast between traditional and cloud IAM.
- Identify the benefits of cloud IAM.
- Explain the mechanisms of role-based access control (RBAC) and multi-factor authentication (MFA).
- Recognize the importance of implementing security measures in cloud networking.
- Explain the role of security groups in virtual private clouds (VPCs).
- Identify different cloud networking security strategies, including network segmentation, monitoring, and logging.
- List tools used for network traffic analysis.
- Explain how to avoid common pitfalls in cloud networking.
- Describe the role of encryption in cloud data security and its integration with IAM policies.
- Identify cloud-native encryption services.
- Explain the role of data loss prevention (DLP) tools.
- Define the concept of cloud database security within IAM.
- Identify Amazon Web Services (AWS) storage systems, such as simple storage service (S3).
- Describe cloud data security best practices.
- Recognize the importance of security within the software development life cycle (SDLC).
- Describe the role of security checks within continuous integration/continuous deployment (CI/CD) pipelines.
- Explain the security considerations involved in cloud containerization.
- Describe the role of Kubernetes in cloud container orchestration.
- List the specific security challenges associated with serverless computing.
- Recognize the importance of APIs in cloud architectures and the role of the OAuth authorization mechanism.

## Lesson Activities and Teaching Strategies

| Estimated Time | Lesson Portion | Directions |
|---|---|---|
| < 2 min | **Lesson Opener:** Cloud Security Architecture | ● Introduce learners to the importance of cloud security architecture in cybersecurity. |
| < 5 min | **Real World Scenario:** Cloud Security Architecture | ● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |

| | | |
|---|---|---|
| 25 min | **Cyber Uncovered:** Cloud Identity and Access Management (IAM) | ● Emphasize the importance of IAM in managing digital identities and access rights.<br>● Discuss the three pivotal questions IAM answers regarding user identity, access, and operations.<br>● Highlight the benefits of IAM in addressing scalability, data protection, compliance, efficiency, and auditability in the cloud environment.<br>● Explore the differences between traditional IAM and cloud IAM in terms of infrastructure, deployment speed, cost model, integration, maintenance, and scalability.<br>● Break down the advantages of cloud IAM, focusing on dynamic scalability, geographical flexibility, customizability, and elastic costing.<br>● Explain the concept of RBAC and how it differs from traditional permission management.<br>● Use examples to illustrate how roles, like "Engineer" and "Manager," determine access rights.<br>● Discuss how RBAC simplifies permission management by centralizing adjustments at the role level, thereby reducing errors and enhancing scalability.<br>● Explore the granular control, dynamic adjustments, unified framework, and transparency aspects of RBAC for ensuring security.<br>● Introduce MFA as a pivotal security strategy in cloud IAM, requiring multiple forms of identification.<br>● Explain its integration with cloud IAM policies, support for access audits, and enhancement of security through key rotations.<br>● Detail the integration of Microsoft Authenticator with AWS cloud IAM, highlighting its role in providing a secure and user-friendly system.<br>● Emphasize the benefits for organizations leveraging Microsoft's ecosystem in ensuring streamlined and secure user access in the cloud.<br>● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 25 min | **Lab:** Secure AWS IAM | ● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day.<br>● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| **5 min Break** | | |
| 25 min | **Cyber Uncovered:** Secure Cloud Networking | ● Emphasize the critical role of cloud networking in connecting virtual and physical cloud infrastructure components.<br>● Highlight its significance as the foundation for data movement and application accessibility in diverse cloud environments. |

| | | |
|---|---|---|
| | | ● Discuss key security measures, including encryption during transit, stringent access control, deployment of intrusion detection systems (IDS), and the use of advanced firewalls.<br>● Introduce VPCs as a crucial component, providing a private, isolated cloud segment with the scalability and efficiency of the cloud and the security and control of a private network.<br>● Explain key features, such as isolation, customizable network configuration, security groups, and network access control lists (ACLs).<br>● Describe how security groups function as virtual firewalls, controlling inbound and outbound traffic to resources within a VPC.<br>● Use a diagram to illustrate a VPC with a subnet, an internet gateway, and a security group assigned to an instance.<br>● Explain the role of ACLs as an alternative to security groups, providing broader traffic control at the subnet level.<br>● Utilize a diagram to showcase a two-subnet VPC with ACLs controlling traffic entry and exit for enhanced security.<br>● Provide insights into how ACLs in AWS operate, controlling traffic in and out of a network subnet within a VPC.<br>● Emphasize their effectiveness for broad network-level traffic control, complementing the granularity of security groups.<br>● Define network segmentation and its significance in dividing a network into subnets for enhanced security and optimized performance.<br>● Discuss use cases, including protecting sensitive data, regulatory compliance, and threat containment.<br>● Illustrate the concept of software-defined networking (SDN), which divides control and data planes, managing networking operations through software.<br>● Demonstrate how SDN facilitates functions like load balancing, routing, and switching entirely through software.<br>● Stress the importance of constant monitoring in maintaining a secure cloud network, enabling timely threat detection and response.<br>● Explain the role of logging in providing real-time visibility into network activities and aiding in proactive threat detection.<br>● Introduce tools for network traffic analysis, including VPC Flow Logs by AWS, Azure Network Watcher, and VPC Flow Logs by Google Cloud.<br>● Address common pitfalls, such as relying solely on default settings, incomplete documentation, and the lack of testing.<br>● Emphasize the need to tailor configurations to the organization's needs, maintain clear documentation for troubleshooting, and always test configurations in a sandbox environment before applying them live.<br>● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. |

| | | |
|---|---|---|
| | | There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 25 min | **Lab:** Setting up Secure Cloud Networking and Monitoring | ● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day.<br>● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| **5 min Pulse Check** (wait for ~75% respondent rate then close the poll) | | |
| **5 min Break** | | |
| 25 min | **Cyber Uncovered:** Cloud Data Security | ● Explain the symbiotic relationship between data encryption and IAM policies in the cloud.<br>● Emphasize the role of encryption in maintaining data confidentiality and integrity, coupled with IAM's role in controlling authorized access.<br>● Present the comparison table highlighting aspects of data at rest and in transit.<br>● Discuss how data encryption aligns with IAM principles in securing stored data and protecting data during transmission.<br>● Introduce cloud-native encryption services like AWS KMS, Azure Key Vault, and Google Cloud KMS.<br>● Discuss best practices for encryption, emphasizing the importance of trusted algorithms and effective key management in alignment with IAM principles.<br>● Explore the pivotal role of data encryption in AWS for both data at rest and in transit.<br>● Detail the use of Amazon S3 for server-side encryption and the central role of AWS Key Management Service (KMS) in managing encryption keys.<br>● Explain how AWS Certificate Manager contributes to securing data in transit.<br>● Discuss the collaboration between DLP tools and IAM strategies in preventing unauthorized data access or transfers.<br>● Highlight key features of DLP in IAM, such as pattern recognition, predefined policies, and real-time alerts, supporting IAM in monitoring and controlling data access.<br>● Explain practices for securing databases in alignment with IAM strategies.<br>● Discuss security features in IAM related to database security, including encryption, automated backups, access controls, and threat detection.<br>● Explore the role of Amazon RDS in cloud database security in AWS.<br>● Detail key security features when setting up an RDS instance, such as encryption with KMS keys, automated backups, restricted public access, and logging/monitoring.<br>● Discuss vital best practices for securing data in AWS S3, focusing on access permissions guided by the principle of least privilege.<br>● Emphasize the role of S3's object lifecycle policies in automating tasks and reinforcing data governance and security. |

| | | |
|---|---|---|
| | | ● Highlight the importance of regular data audits in IAM for reviewing access patterns and permissions.<br>● Stress the need for robust security measures—including strong encryption and effective DLP solutions—in cloud IAM for protection against potential threats.<br>● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 25 min | **Lab:** Enhancing Data Security in the Cloud on AW | ● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day.<br>● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| **5 min Break** | | |
| 25 min | **Cyber Uncovered:** Cloud Application Security | ● Explain the significance of the software development life cycle (SDLC) on the creation and evolution of software applications.<br>● Highlight how SDLC integrates with cloud resources, services, and deployment models.<br>● Emphasize the importance of incorporating security throughout the SDLC, particularly in cloud environments.<br>● Discuss the benefits, including early vulnerability detection and the use of cloud-native tools for enhanced application and data protection.<br>● Introduce the concept of continuous integration/continuous deployment (CI/CD) and its relevance in cloud deployments.<br>● Discuss the necessity of integrating security checks into CI/CD pipelines to ensure secure cloud configurations and resources.<br>● Present cloud-centric tools such as AWS Inspector, Azure Security Center, and Google Cloud Security Command Center.<br>● Explain how these tools contribute to real-time vulnerability detection, enhancing overall cloud application and infrastructure security.<br>● Define cloud containerization and its efficiency in packaging and deploying applications with dependencies.<br>● Discuss the security considerations and risks associated with cloud containerization.<br>● Outline container security best practices, including using verified container images, regular updates, and strong configuration management.<br>● Emphasize the importance of container scanning, least privilege principles, network segmentation, and regular security audits.<br>● Introduce Kubernetes as an open-source container orchestration system.<br>● Highlight how Kubernetes automates deployment and scaling, working seamlessly with cloud services. |

| | | |
|---|---|---|
| | | ● Discuss effective security measures in cloud container orchestration, utilizing managed network policies, secrets management, and IAM roles.<br>● Explain how these strategies contribute to a robust security framework for containerized applications in the cloud.<br>● Introduce serverless computing as a shift in cloud technology, allowing developers to build and deploy applications without server management.<br>● Explain the advantage of automatic scaling in response to triggers and highlight potential risks associated with serverless computing.<br>● Emphasize the crucial role of APIs in cloud architectures and the need for robust security measures.<br>● Discuss the implementation of OAuth for authorization, focusing on accurate callback URLs, scope and permission control, token security, and proactive monitoring.<br>● Discuss the importance of cloud vulnerability assessments using cloud-native or third-party tools.<br>● Emphasize the need to maintain up-to-date cloud configurations, following the principle of least privilege for all configurations.<br>● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10 min | **Lesson Closure** | ● For this last lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson. The take-aways discussion should include key concepts such as IAM and cloud security integration as well as SDLC and data security. Students should review this information prior to moving to the next course.<br>● Q&A |
| < 2 min | **End-of-Course Survey** | ● Allocate 5 minutes to facilitate the completion of the End-of-Course Survey.<br>● Encourage learners to provide honest and constructive feedback about their learning experience. |
| | **Additional Time Filler (if needed)** | ● Kahoot<br>● Discuss interview prep and questioning<br>● Use breakout rooms for additional lab practice<br>● Continue Real World Scenario Conversation |