LESSON: Secure Network Architecture

Before you Begin

This is the last week of this course. Instructors should not spend 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 must catch up during these last two modules.

For this lesson and upcoming lessons, 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 discuss essential aspects of network architecture and security. Learners will understand the alignment of network architecture with organizational requirements and explore the role of host devices, including computers and IoT, in ensuring security. The mitigation of TCP/IP vulnerabilities through innovative technologies is discussed, along with the importance of online diagram-making tools like diagrams.net. This lesson emphasizes the integration of people, processes, and technologies for effective security, addressing key points such as patch management and the least

privilege model. Network segmentation, DMZ, network access control (NAC), and air-gapped environments are explained for enhanced security. The lesson also covers the categorization of network threats into active and passive, effective surveying techniques, and advanced security measures, providing a comprehensive defense against physical and digital cyberthreats within a multi-layered security strategy.

Objectives

- Recognize the importance of a secure network architecture.
- List security considerations that must be taken into account when managing host devices.
- Explain how to create network diagrams.
- Analyze the concept of people, processes, and technologies in cybersecurity.
- Describe cybersecurity essential strategies.
- Explain the role of patch management in network architecture security.
- Recognize the importance of secure architecture technologies within network security.
- Define different secure architecture solutions, including network segmentation, demilitarized zones (DMZs), and air-gapped environments.
- Analyze the key features of network access control (NAC).
- Explain how network threats are classified.
- Identify passive and active threat countermeasures.
- Recognize the benefits of implementing a multi-layered network defense.
- Compare and contrast tangible and digital network security.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Secure Network Architecture	● Introduce learners to the importance of secure network architecture in cybersecurity.
< 5 min	**Real World Scenario:** Secure Network 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.
30 min	**Cyber Uncovered:** Security Considerations	● Emphasize the definition of network architecture, covering hardware, software, connectivity, communication protocols, and data transmission. ● Highlight the significance of well-planned network architecture in identifying and mitigating all kinds of vulnerabilities. ● Discuss the concept of "hosts" in a network, including traditional computers and IoT devices. ● Explore security posture assessment, network management, monitoring, incident response, and compliance within host device considerations.

		● Provide an overview of TCP/IP as the fundamental suite of protocols in internet and network communication. ● Emphasize the importance of understanding TCP/IP security and countermeasures, such as firewalls and encryption technologies. ● Introduce diagrams.net as an online tool for creating network diagrams. ● Walk through the step-by-step guide for using diagrams.net, including creating, customizing, arranging, and exporting diagrams. ● Present use cases that illustrate home networks, small business networks, and corporate networks. ● Break down the three components (people, processes, and technologies) of cybersecurity strategy. ● Discuss the role of each component, focusing on implementation, enforcement, training, awareness, guidance, decision-making, compliance, and the role of technologies in protection, defense, automation, and adaptation. ● Cover essential cybersecurity strategies, such as identifying low-hanging fruit, securing the weakest link, and implementing the least privilege model. ● Emphasize the importance of understanding these concepts in fortifying an organization's cybersecurity structure. ● Define patch management and its significance in managing software and firmware updates. ● Discuss how effective patch management contributes to maintaining the security and stability of systems. ● 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.
5 min Break		
30 min	**Cyber Uncovered:** Secure Architecture Technologies	● Emphasize the integration of advanced tools and systems into network architectures for cybersecurity enhancement. ● Highlight key technologies such as firewalls, intrusion detection and prevention systems, encryption protocols, and secure access controls. ● Stress the pivotal role of these technologies in safeguarding data integrity, ensuring confidentiality, and maintaining network resilience against evolving cyber risks. ● Define network segmentation as the practice of dividing a network into smaller subnets for security enhancement and improved performance. ● Discuss the factors influencing segmentation, such as device type, user role, and applications. ● Explain the role of network segmentation in preventing breach spread, utilizing zero-trust principles, and limiting access to sensitive network areas.

		• Introduce the concept of a DMZ as a buffer zone between internal and external networks, providing an additional layer of security. • Discuss the critical role of DMZs in hosting public-facing services while safeguarding the internal network from external threats. • Define an air-gapped environment as a physically isolated network, eliminating remote access for high-level security. • Discuss the critical importance of air-gapped environments in scenarios with an exceptionally high risk of cyber infiltration. • Introduce NAC as a security solution that enforces policy-based access control to network resources. • Highlight that NAC restricts network access to authorized users and devices based on predefined security rules. • Clarify that subsequent analysis will focus on NAC's functionality, applicable to other discussed tools. • Detail key NAC features, including network access regulation, rule-based enforcement, organizational policies, and network integrity and security. • Emphasize NAC's primary function in regulating and controlling access to the network, preventing unauthorized entry and security incidents. • Discuss rule-based enforcement as a mechanism for consistent and automated decision-making, reducing the risk of human error. • Highlight the role of organizational policies in aligning network access decisions with the organization's security strategy and compliance requirements. • Emphasize NAC's critical role in maintaining network integrity and security by preventing potential threats and ensuring compliance with security standards. • 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.
30 min	**Lab:** Drawing a Secure Topology	• Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. • 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		
30 min	**Cyber Uncovered:** Design Considerations	• Outline the two core types of network threats: Active threats and passive threats. • Discuss the nature of active threats, involving intentional manipulation or theft of data, and passive threats, focusing on scrutinizing and scanning without direct alteration. • Emphasize the critical role of network surveying in secure network design. • Explain how precision and detail in the surveying phase contribute to the network's resilience against potential vulnerabilities.

		● Cover passive threats like data interception and deceptive data gathering. ● Discuss countermeasures, including end-to-end encryption, stringent network access controls, and training sessions for personnel. ● Examine active threats such as network overload attacks and data exfiltration. ● Explore countermeasures like strategic backup infrastructure, failover mechanisms, network compartmentalization, and the principle of minimal access rights. ● Break down advanced countermeasures for both passive and active threats. ● Discuss the integration of network anomaly detection systems, stringent access control protocols, multi-factor authentication, and advanced network packet inspection tools. ● Introduce the concept of a multi-layered defense strategy. ● Explain varied defense protocols and collaborative defense, highlighting how each layer supports the others for a robust shield against a spectrum of threats. ● Define tangible network security and its focus on physical aspects. ● Provide examples such as alarm systems, motion detectors, locked server rooms, biometric scanners, and surveillance systems. ● Define digital network security and its focus on protecting network assets from cyberthreats. ● Provide examples such as antivirus programs, firewalls, encryption protocols, and intrusion detection systems. ● Compare and contrast tangible and digital network security. ● Explore aspects like perceptibility, entry management, symbiosis, scope, and examples of each security type. ● 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.
5 min Break		
30 min	**Lab:** High-Level Analysis	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
10 min	**Lesson Closure**	● For this lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as secure network architecture, comprehensive defense strategies and the Integration of people, processes, and technologies. Students should review this information prior to moving to the next module.

		● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation