Your grade: 90%

Your latest: **90%** • Your highest: **90%** • To pass you need at least 80%. We keep your highest score.

1. What is the purpose of network monitoring? **1 / 1 point**

● Continuously observe and analyze the performance, availability, and security of a computer network

○ Oversee and control a computer network

○ Monitor and optimize the performance of network components and services

○ Maintain a secure and resilient network infrastructure

✓ **Correct**
Correct! Network monitoring is the process of continuously observing and analyzing the performance, availability, and security of a computer network. For more information, please review the Introduction to Network Monitoring lecture in Module 3 Lesson 1.

2. Which network management tool is cloud-based and provides intuitive monitoring and configuration features? **1 / 1 point**

○ Cisco SD WAN

○ Cisco DNA Center

● Cisco Meraki Dashboard

○ Cisco Prime Infrastructure

✓ **Correct**
Correct! Cisco Meraki Dashboard is a cloud-based management platform specifically designed for Cisco Meraki networking devices. It provides intuitive monitoring and configuration features, allowing you to manage switches, access points, security appliances, and cameras from a single interface. For more information, please review the Overview of Network Management lecture in Module 3 Lesson 1.

3. Your company has been having challenges with network management. They are having difficulty with the initial setup and arrangement of network devices. Which key component of network management do they need help with? **1 / 1 point**

○ Security management

● Configuration management

○ Performance management

○ Fault management

✓ **Correct**
Correct! Configuration management involves the initial setup and ongoing configuration of network devices, including routers, switches, firewalls, and servers. For more information, please review the Overview of Network Management lecture in Module 3 Lesson 1.

4. Which of the following scenarios best describes the network security threat of social engineering? **1 / 1 point**

○ Mark, a marketing manager, notices multiple failed login attempts on his company email account over the past few days. Concerned about security, he decides to change his password to a stronger one.

● John receives a call from someone posing as an IT support representative from his credit card company, asking for personal details and email password to secure his account due to a supposed security breach. Trusting the caller's authority, John provides the information.

○ Lisa, a disgruntled employee, decides to take revenge on her company for not promoting her. She uses her authorized access to the company's network to steal confidential customer data and company strategies, intending to sell the information to a competitor.

○ Sophia, an employee at a financial institution, receives an email that appears to be from her company's IT department, requesting her to update her login credentials urgently. Trusting the sender's familiar email address and the urgent tone of the message, she clicks on the provided link and enters her username and password.

✓ **Correct**
Correct! The caller is not a legitimate representative from the credit card company, but a skilled social engineer seeking to exploit his trust and cooperation. Armed with personal information and email password, the social engineer gains unauthorized access to John's email account and begins to infiltrate the company's network by exploiting weak security practices.

5. Educating users is an important strategy for mitigating security threats. One way to do this is to:

1 / 1 point

○ Have users develop a Security Incident Response Plan.

○ Conduct regular vulnerability assessments.

● Conduct regular training sessions about common threats.

○ Keep your systems and software up to date.

Correct
Correct! Educating and raising awareness among employees about cybersecurity best practices is essential. One way to educate users is to have Security Awareness Training to conduct regular training sessions to educate users about common threats, such as phishing, social engineering, and password security. For more information, please review the Mitigating Security Threats lecture in Module 3 Lesson 2.

6. The function of access control lists (ACLs) in network security is to:

1 / 1 point

○ Identify and respond to security incidents.

○ Contain the impact of security breaches.

● Prevent unauthorized access and protect sensitive information.

○ Secure the configurations and minimize vulnerabilities on your routers and switches.

Correct
Correct! The function of access control lists (ACLs) in network security is to prevent unauthorized access and protect sensitive information. For more information, please review the Best Practices for Securing Cisco Routers and Switches lecture in Module 3 Lesson 2.

7. One of the best ways to secure Cisco routers and switches involves disabling unnecessary services and changing default passwords. Which best practice does this describe?

1 / 1 point

○ Network segmentation

○ Monitoring and logging

● Device hardening

○ Physical security

Correct
Correct! Changing default passwords and using strong, unique passwords for administrative access is one of the best practices in device hardening. For more information, please review the Best Practices for Securing Cisco Routers and Switches lecture in Module 3 Lesson 2.

8. The purpose of network management is to:

0 / 1 point

● Continuously observe and analyze the performance, availability and security of a computer network.

○ Maintain a secure and resilient network infrastructure.

○ Provide proactive issue detection and enhanced security.

○ Oversee and control a computer network.

Incorrect
Incorrect. For more information, please the Overview of Network Management lecture in Module 3 Lesson 1.

9. Which of these strategies is a part of the monitoring and incident response to mitigate threats for Cisco devices?

1 / 1 point

○ Security Awareness Training

○ Endpoint protection

○ Perimeter defense

● Regular testing and simulation

Correct
Correct! Regular testing and simulation is a strategy that is part of the monitoring and incident response to mitigate threats for Cisco devices. For more information, please review the Mitigating Security Threats lecture in Module 3 Lesson 2.

10. Why is it important to have proactive issue detection when monitoring networks?

1 / 1 point

○ Analyze network trends and usage patterns over time

○ Detect and mitigate potential security threats

● Identify problems before they escalate

○ Help optimize network performance

✓ **Correct**

Correct! Proactive Issue Detection is a key benefit in network monitoring which allows you to identify problems before they escalate. For more information, please review the Introduction to Network Monitoring lecture in Module 3 Lesson 1.