

UTS KEAMANAN SISTEM INFORMASI

Checkpoint Exam : Vulnerability Assessment and Risk Management



Oleh :

Moh. Samsul Hadi

2141762133

KELAS SIB – 4C

PROGRAM STUDI
D-IV SISTEM INFORMASI BISNIS
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG

Jl. Soekarno Hatta No.9, Jatimulyo, Kec, Lowokwaru, Kota Malang, Jawa Timur

65141

Checkpoint Exam : Vulnerability Assessment and Risk Management

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy | Cyber Threat Management

Course Outline | Resources

Search course outline

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response 100%

Checkpoint Exam: Incident Response 100%

Checkpoint Exam

You've scored 100%.
Congratulations, you have passed the quiz.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Module: Governance and Compliance	100%
Module: Network Security Testing	100%
Module: Threat Intelligence	100%
Module: Endpoint Vulnerability Assessment	100%
Module: Risk Management and Security Controls	100%
Skill: Select security controls based on organizational relevance.	100%
Skill: Explain why organizations must conform with specific compliance frameworks.	100%
Skill: Create a personal code of conduct based on ethical and legal standards.	100%

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy | Cyber Threat Management

Course Outline | Resources

Search course outline

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response 100%

Checkpoint Exam: Incident Response 100%

Checkpoint Exam

You've scored 100%.
Congratulations, you have passed the quiz.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Module: Governance and Compliance	100%
Module: Network Security Testing	100%
Module: Threat Intelligence	100%
Module: Endpoint Vulnerability Assessment	100%
Module: Risk Management and Security Controls	100%
Skill: Select security controls based on organizational relevance.	100%
Skill: Explain why organizations must conform with specific compliance frameworks.	100%
Skill: Create a personal code of conduct based on ethical and legal standards.	100%
Skill: Create a risk management plan.	100%
Skill: Evaluate network and systems vulnerability.	100%
Skill: Explain how IT systems vulnerability is assessed.	100%
Skill: Create a vulnerability assessment plan by identifying and describing relevant threats.	100%

Cisco Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 1

A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?

SOX

ECPA

GLBA

PCI DSS

Question 2

A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)

Use content filtering.

Disable CD and USB access.

Monitor all activity by the users.

Change to thin clients.

Implement disciplinary action.

Provide security awareness training.

Question 3

Which threat is mitigated through user awareness training and tying security awareness to performance reviews?

device-related threats

cloud-related threats

user-related threats

physical threats

Question 4

The image displays three sequential screenshots of the Cisco Academy Cyber Threat Management course exam interface. Each screenshot shows the course outline on the left and a question on the right.

Question 4: As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?

Options: physical threats, FIRPA, GLBA (selected), SOX, PCI.

Question 5: What is the workforce framework category that includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence?

Options: Protect and Defend, Securely Provision, Oversight and Development, Analyze (selected).

Question 6: A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?

Options: packet analyzer, malware, pentest, vulnerability scanner (selected).

Question 7: (Partially visible at the bottom of the third screenshot).

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd5b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 7

What information does the SIEM network security management tool provide to network administrators?

☐ detection of open TCP and UDP ports
☒ real time reporting and analysis of security events
☐ assessment of system security configurations
☐ a map of network systems and services

Question 8

What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd5b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 8

What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?

☒ Tripwire
☐ Nessus
☐ L0phtcrack
☐ Metasploit

Question 9

What type of network security test can detect and report changes made to network systems?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd5b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 9

What type of network security test can detect and report changes made to network systems?

☐ network scanning
☐ vulnerability scanning
☐ penetration testing
☒ integrity checking

Question 10

What type of network security test uses simulated attacks to determine the feasibility of an attack as well as the results.

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-3b6d68b07a2f&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c62d976e4

Networking CISCO Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: network security testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 10

What type of network security test uses simulated attacks to determine the feasibility of an attack as well as the possible consequences if the attack occurs?

penetration testing

integrity checking

network scanning

vulnerability scanning

Question 11

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-3b6d68b07a2f&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c62d976e4

Networking CISCO Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: network security testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 11

Which organization defines unique CVE identifiers for publicly known information-security vulnerabilities that make it easier to share data?

MITRE

DHS

Cisco Talos

FireEye

Question 12

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-3b6d68b07a2f&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c62d976e4

Networking CISCO Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: network security testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 12

Which statement describes Trusted Automated Exchange of Indicator Information (TAXII)?

It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.

It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

It is a dynamic database of real-time vulnerabilities.

It is a set of specifications for exchanging cyber threat information between organizations.

Question 13

How does AIS address a newly discovered threat?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd6b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 13

How does AIS address a newly discovered threat?

by mitigating the attack with active response defense mechanisms

by advising the U.S. Federal Government to publish internal response strategies

by creating response strategies against the new threat

by enabling real-time exchange of cyberthreat indicators with U.S. Federal Government and the private sector

Question 14

Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd6b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 14

Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

assess

verify

discover

prioritize assets

Question 15

In addressing an identified risk, which strategy aims to decrease the risk by taking measures to reduce vulnerability?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd6b07a2f8&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

prioritize assets

Question 15

In addressing an identified risk, which strategy aims to decrease the risk by taking measures to reduce vulnerability?

risk reduction

risk retention

risk avoidance

risk sharing

Question 16

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d86b07a2f0&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 16

What are the steps in the vulnerability management life cycle?

detect, analyze, recover, respond

discover, prioritize assets, assess, report, remediate, verify

plan, do, act, check

identify, protect, detect, respond, recover

Question 17

What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d86b07a2f0&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 17

What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

exploit

integrity

remediation level

confidentiality

attack vector

availability

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d86b07a2f0&tab=curriculum&view=fa2ad388-b6f6-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 18

Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?

risk management

patch management

vulnerability management

asset management

Question 19

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd8b07a2f8&tab=curriculum&view=fa2ad388-b686-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 19

Match the security management function with the description.

Categories:

- A the security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization
- B the comprehensive analysis of impacts of attacks on core company assets and functioning
- C the inventory and control of hardware and software configurations of systems
- D the implementation of systems that track the location and configuration of networked devices and software across an enterprise

Options:

- A vulnerability management
- B risk management
- C configuration management
- D asset management

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd8b07a2f8&tab=curriculum&view=fa2ad388-b686-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 20

Why would an organization perform a quantitative risk analysis for network security threats?

- so that the organization can focus resources where they are most needed
- so that management has documentation about the number of security attacks that have occurred within a particular time period
- so that the organization knows the top areas where network security holes exist
- so that management can determine the number of network devices needed to inspect, analyze, and protect the corporate resources

Question 21

In which situation would a detective control be warranted?

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38dd8b07a2f8&tab=curriculum&view=fa2ad388-b686-586d-8990-d1c6c2d976e4

Networking Academy Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response

Checkpoint Exam

Question 21

In which situation would a detective control be warranted?

- when the organization needs to repair damage
- when the organization needs to look for prohibited activity
- after the organization has experienced a breach in order to restore everything back to a normal state
- when the organization cannot use a guard dog, so it is necessary to consider an alternative

Question 22

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d4d8b07a2f&tab=curriculum&view=f62ad388-b6f6-586d-8990-d1dc2d976e4

Networking
Cisco Academy

Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Response and Response

Checkpoint Exam

Question 22

Which two values are required to calculate annual loss expectancy? (Choose two.)

quantitative loss value

single loss expectancy

exposure factor

asset value

frequency factor

annual rate of occurrence

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d4d8b07a2f&tab=curriculum&view=f62ad388-b6f6-586d-8990-d1dc2d976e4

Networking
Cisco Academy

Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Response and Response

Checkpoint Exam

Question 23

The team is in the process of performing a risk analysis on the database services. The information collected includes the initial value of these assets, the threats to the assets and the impact of the threats. What type of risk analysis is the team performing by calculating the annual loss expectancy?

protection analysis

loss analysis

qualitative analysis

quantitative analysis

Question 24

netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38d4d8b07a2f&tab=curriculum&view=f62ad388-b6f6-586d-8990-d1dc2d976e4

Networking
Cisco Academy

Cyber Threat Management

Course Outline Resources

Search course outline

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Checkpoint Exam

Module 6: Digital Forensics and Incident Response and Response

Checkpoint Exam

quantitative analysis

Question 24

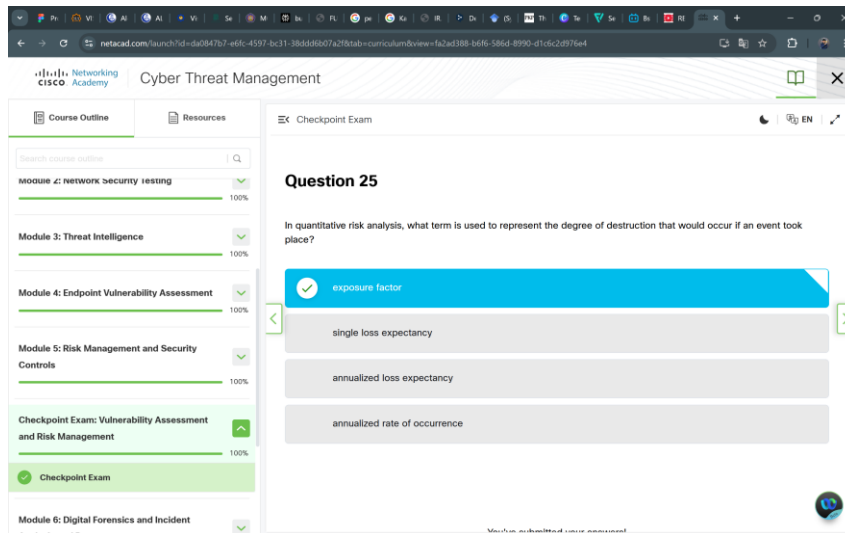
Based on the risk management process, what should the cybersecurity team do as the next step when a cybersecurity risk is identified?

Monitor the risk.

Assess the risk.

Respond to the risk.

Frame the risk.



The screenshot shows the Cisco Academy interface for the 'Cyber Threat Management' course. On the left, the 'Course Outline' sidebar lists several modules, each with a 100% completion status: 'Module 1: Network Security Testing', 'Module 3: Threat Intelligence', 'Module 4: Endpoint Vulnerability Assessment', 'Module 5: Risk Management and Security Controls', 'Checkpoint Exam: Vulnerability Assessment and Risk Management', 'Checkpoint Exam', and 'Module 6: Digital Forensics and Incident Response'. The 'Checkpoint Exam' is currently selected and highlighted in green. The main content area is titled 'Checkpoint Exam' and displays 'Question 25'. The question text is: 'In quantitative risk analysis, what term is used to represent the degree of destruction that would occur if an event took place?'. Below the question, there are four answer options in a scrollable list: 'exposure factor' (which is selected and highlighted in blue with a checkmark icon), 'single loss expectancy', 'annualized loss expectancy', and 'annualized rate of occurrence'. The interface also includes a search bar, a language selector (EN), and a small chat icon in the bottom right corner.