KEAMANAN SISTEM INFORMASI

Checkpoint Exam : Incident Response

Oleh :

Moh. Samsul Hadi

2141762133

KELAS SIB – 4C

PROGRAM STUDI

D-IV SISTEM INFORMASI BISNIS

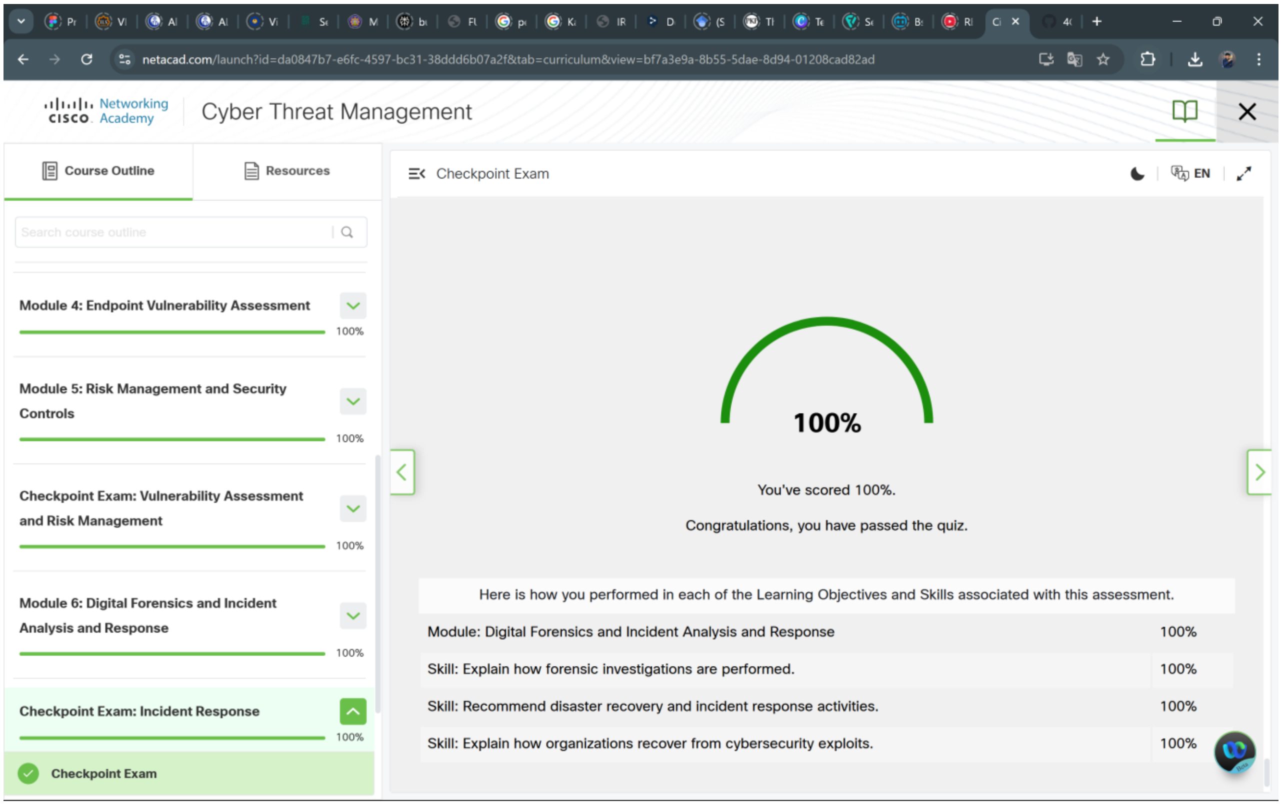
JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

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

65141

Checkpoint Exam : Incident Response (Result)



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Networking Academy

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

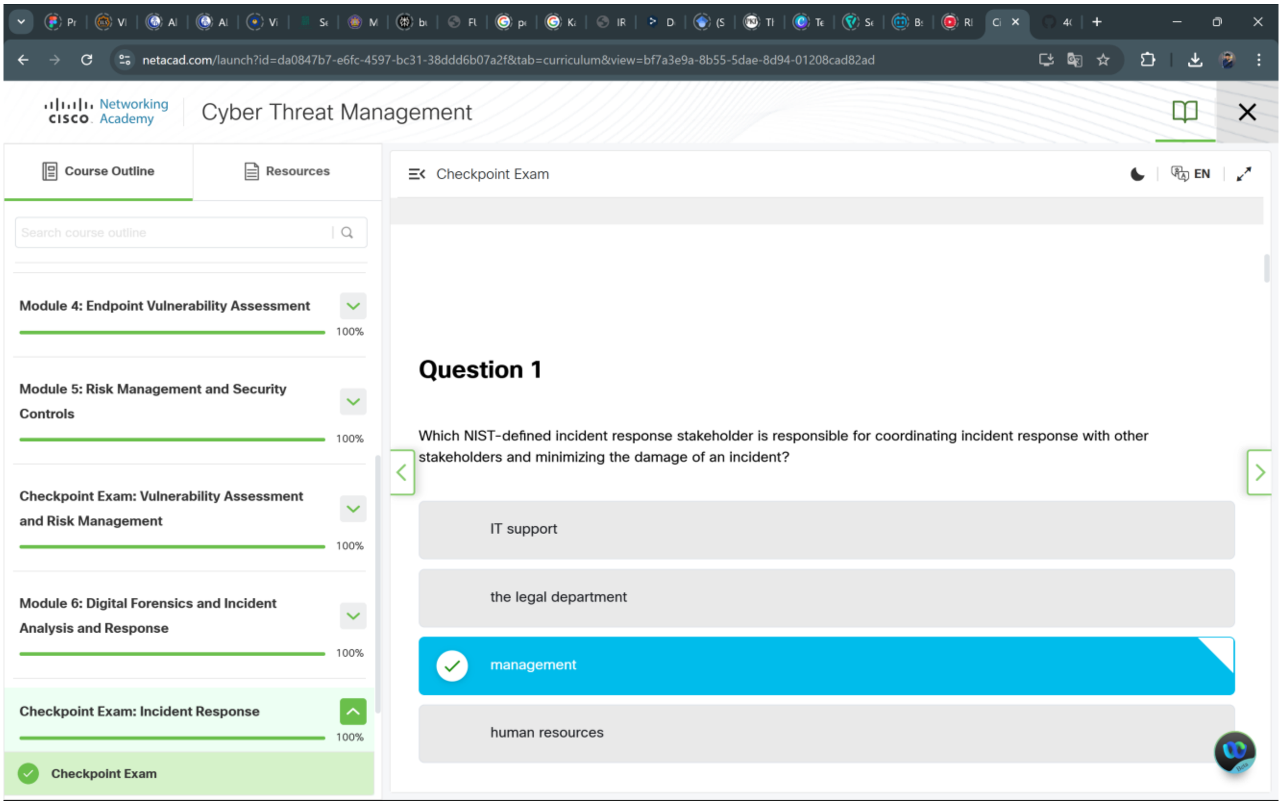
100%

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: Digital Forensics and Incident Analysis and Response	100%
Skill: Explain how forensic investigations are performed.	100%
Skill: Recommend disaster recovery and incident response activities.	100%
Skill: Explain how organizations recover from cybersecurity exploits.	100%

Checkpoint Exam : Incident Response



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Networking Academy

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

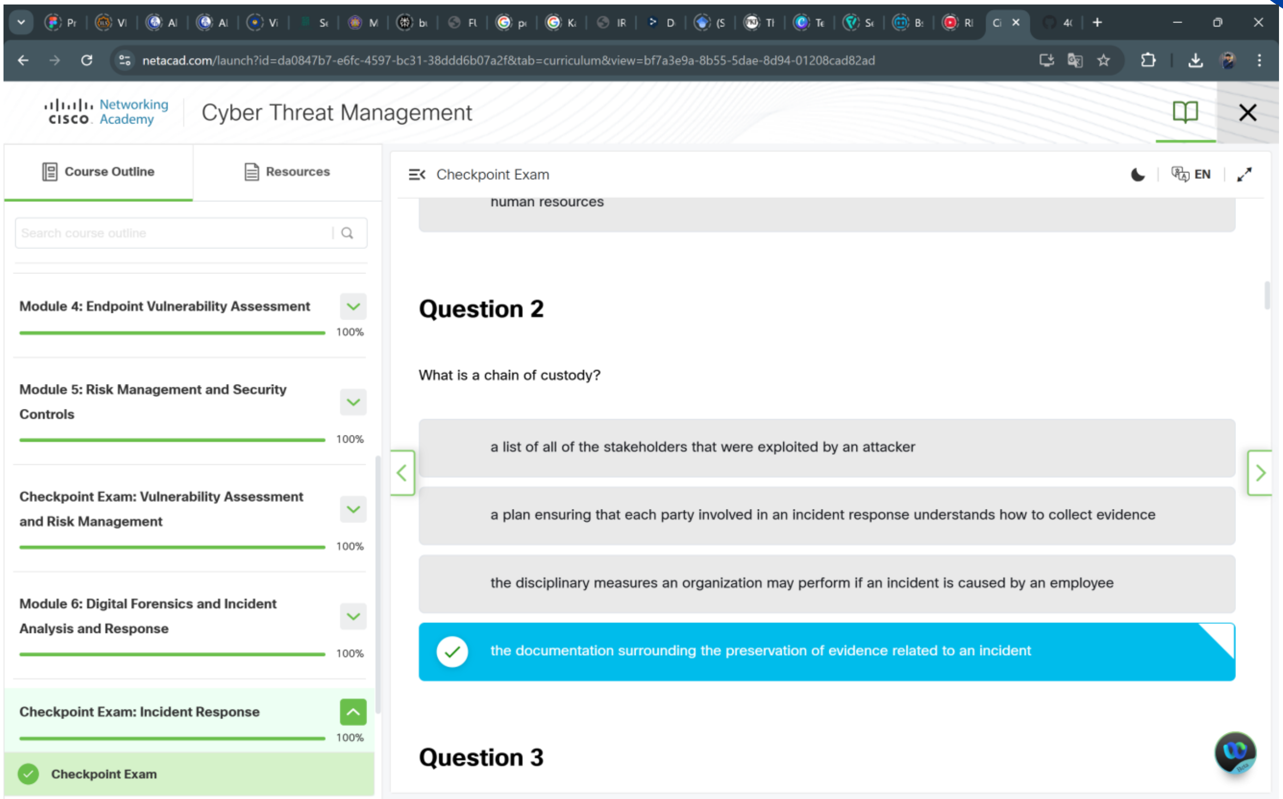
Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

Question 1

Which NIST-defined incident response stakeholder is responsible for coordinating incident response with other stakeholders and minimizing the damage of an incident?

- IT support
- the legal department
- ✓ management
- human resources



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment — 100%

Module 5: Risk Management and Security Controls — 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management — 100%

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

Checkpoint Exam: Incident Response — 100%

✓ Checkpoint Exam

Checkpoint Exam

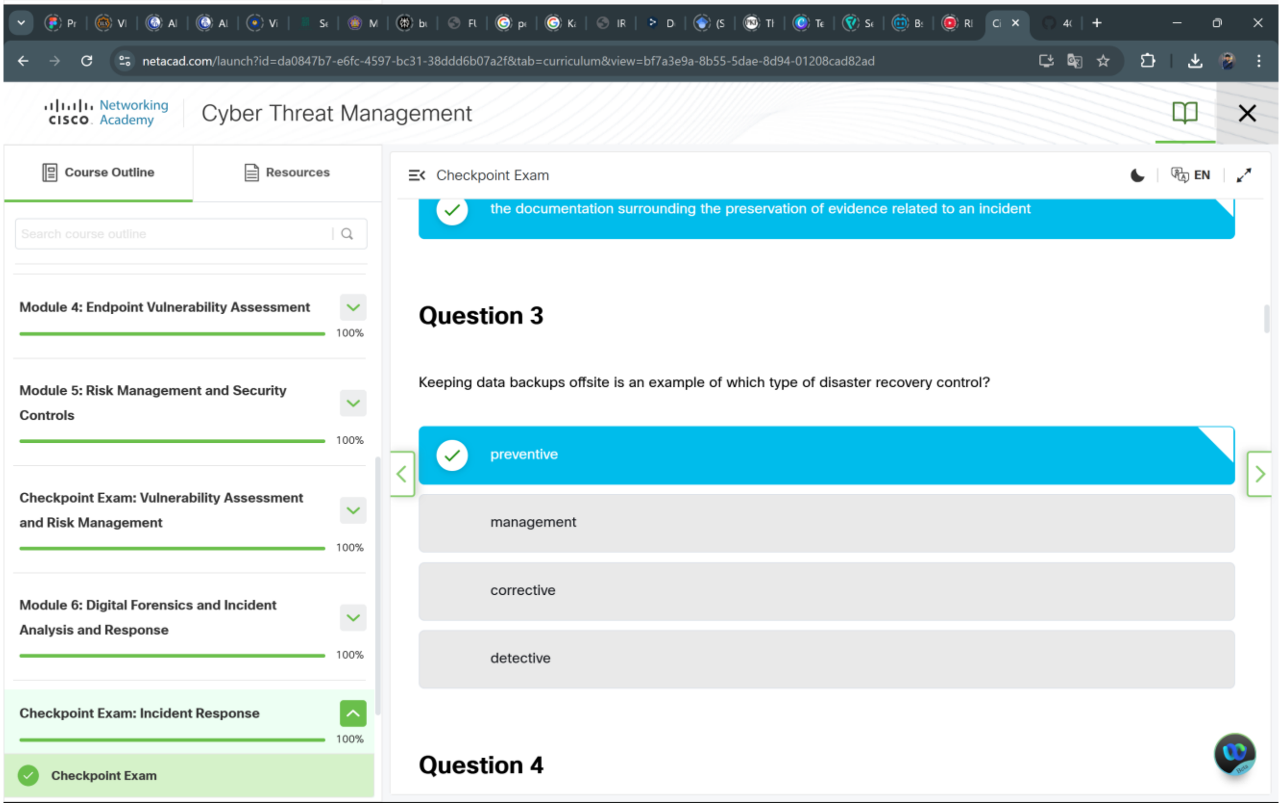
human resources

Question 2

What is a chain of custody?

- a list of all of the stakeholders that were exploited by an attacker
- a plan ensuring that each party involved in an incident response understands how to collect evidence
- the disciplinary measures an organization may perform if an incident is caused by an employee
- ✓ the documentation surrounding the preservation of evidence related to an incident

Question 3



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment — 100%

Module 5: Risk Management and Security Controls — 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management — 100%

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

Checkpoint Exam: Incident Response — 100%

✓ Checkpoint Exam

Checkpoint Exam

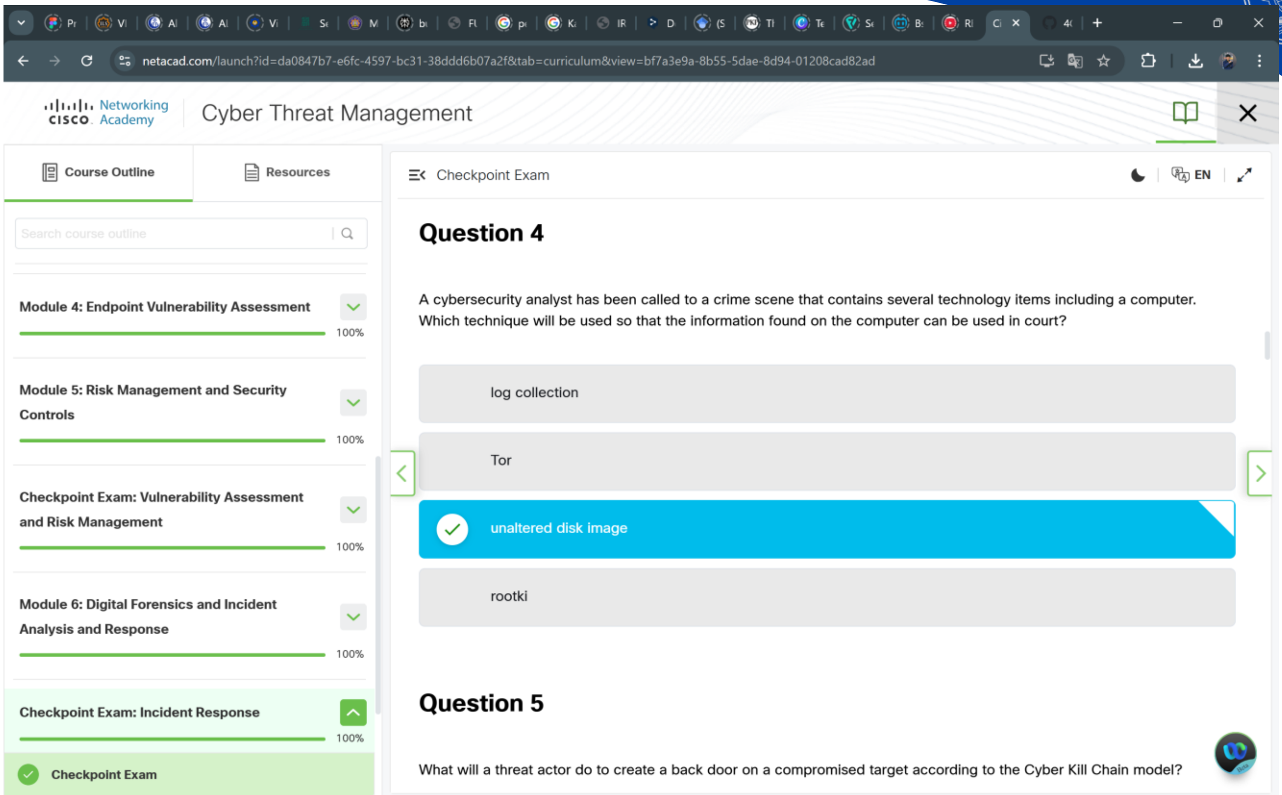
✓ the documentation surrounding the preservation of evidence related to an incident

Question 3

Keeping data backups offsite is an example of which type of disaster recovery control?

- ✓ preventive
- management
- corrective
- detective

Question 4



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

Checkpoint Exam

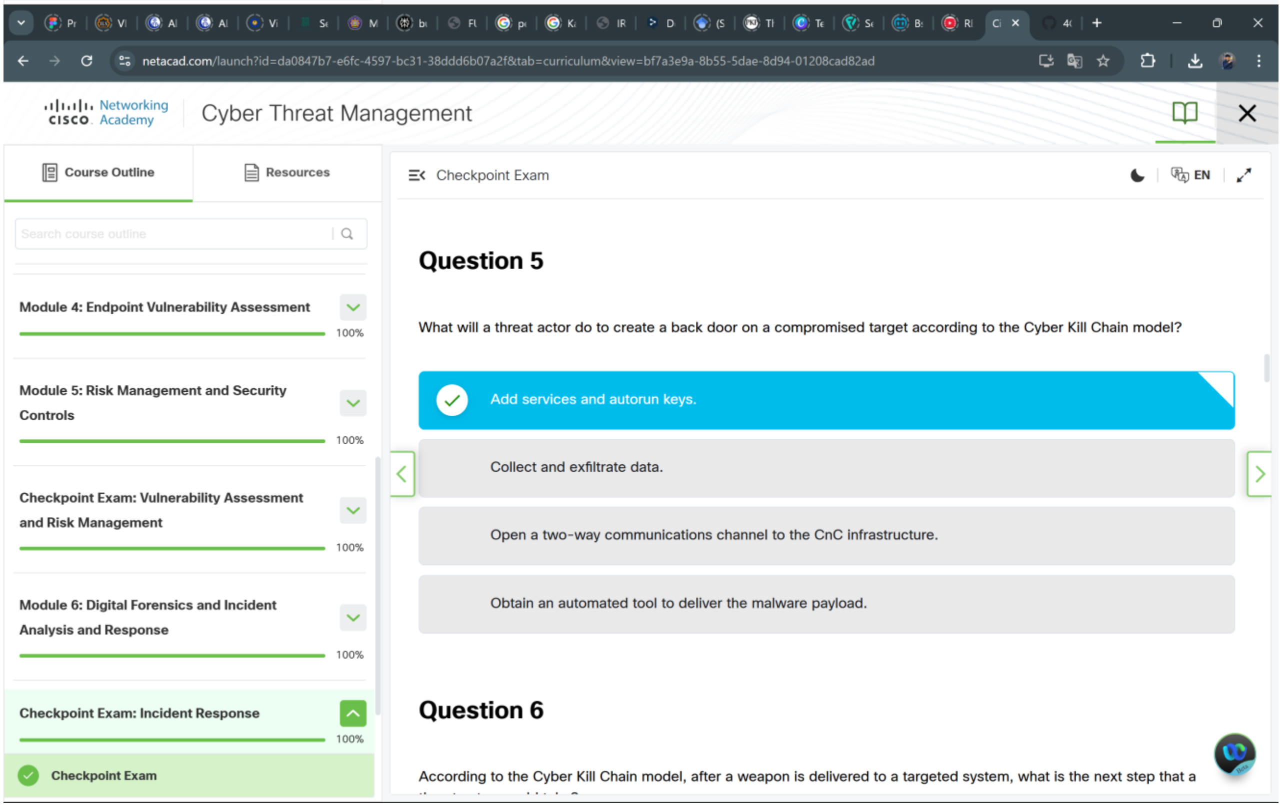
Question 4

A cybersecurity analyst has been called to a crime scene that contains several technology items including a computer. Which technique will be used so that the information found on the computer can be used in court?

- log collection
- Tor
- ✓ unaltered disk image
- rootki

Question 5

What will a threat actor do to create a back door on a compromised target according to the Cyber Kill Chain model?



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

Checkpoint Exam

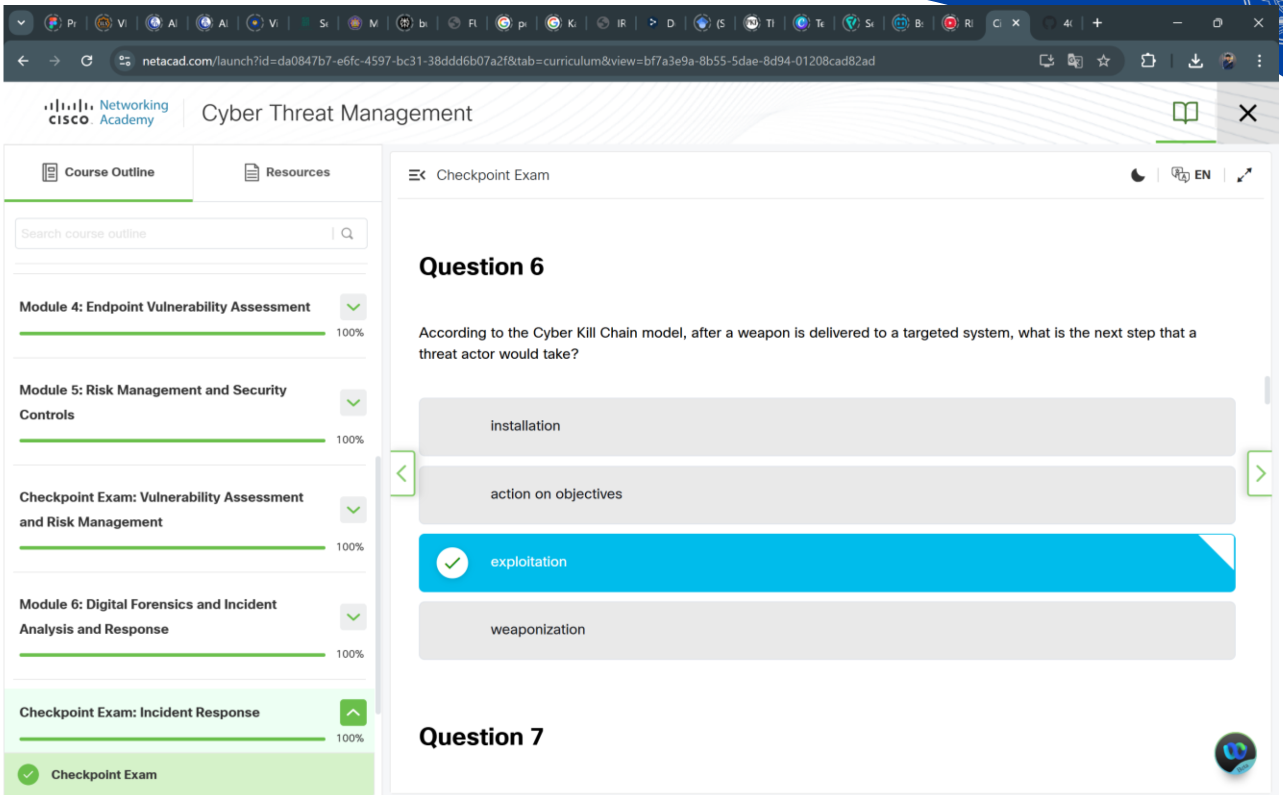
Question 5

What will a threat actor do to create a back door on a compromised target according to the Cyber Kill Chain model?

- ✓ Add services and autorun keys.
- Collect and exfiltrate data.
- Open a two-way communications channel to the CnC infrastructure.
- Obtain an automated tool to deliver the malware payload.

Question 6

According to the Cyber Kill Chain model, after a weapon is delivered to a targeted system, what is the next step that a



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Networking Academy

Cyber Threat Management

Course Outline | Resources

Search course outline

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

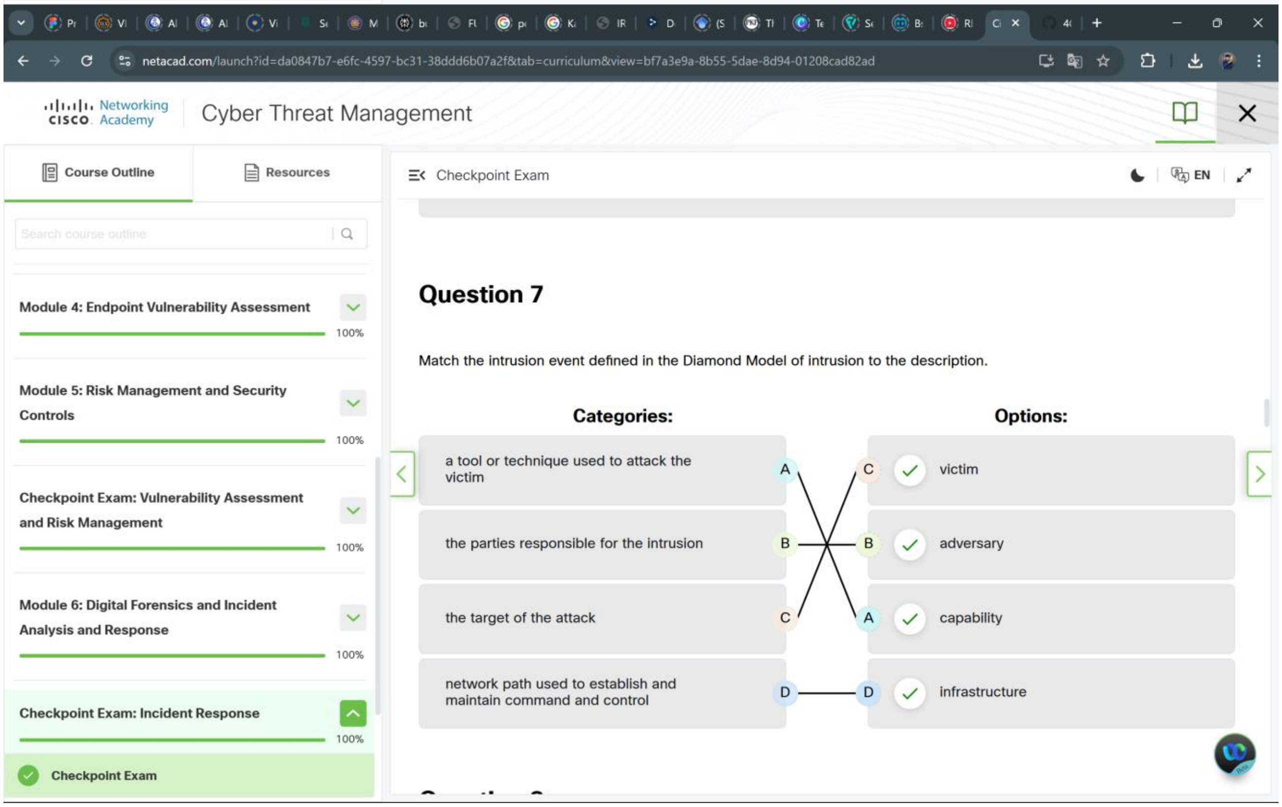
Checkpoint Exam EN

Question 6

According to the Cyber Kill Chain model, after a weapon is delivered to a targeted system, what is the next step that a threat actor would take?

- installation
- action on objectives
- ✓ exploitation
- weaponization

Question 7



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Networking Academy

Cyber Threat Management

Course Outline | Resources

Search course outline

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

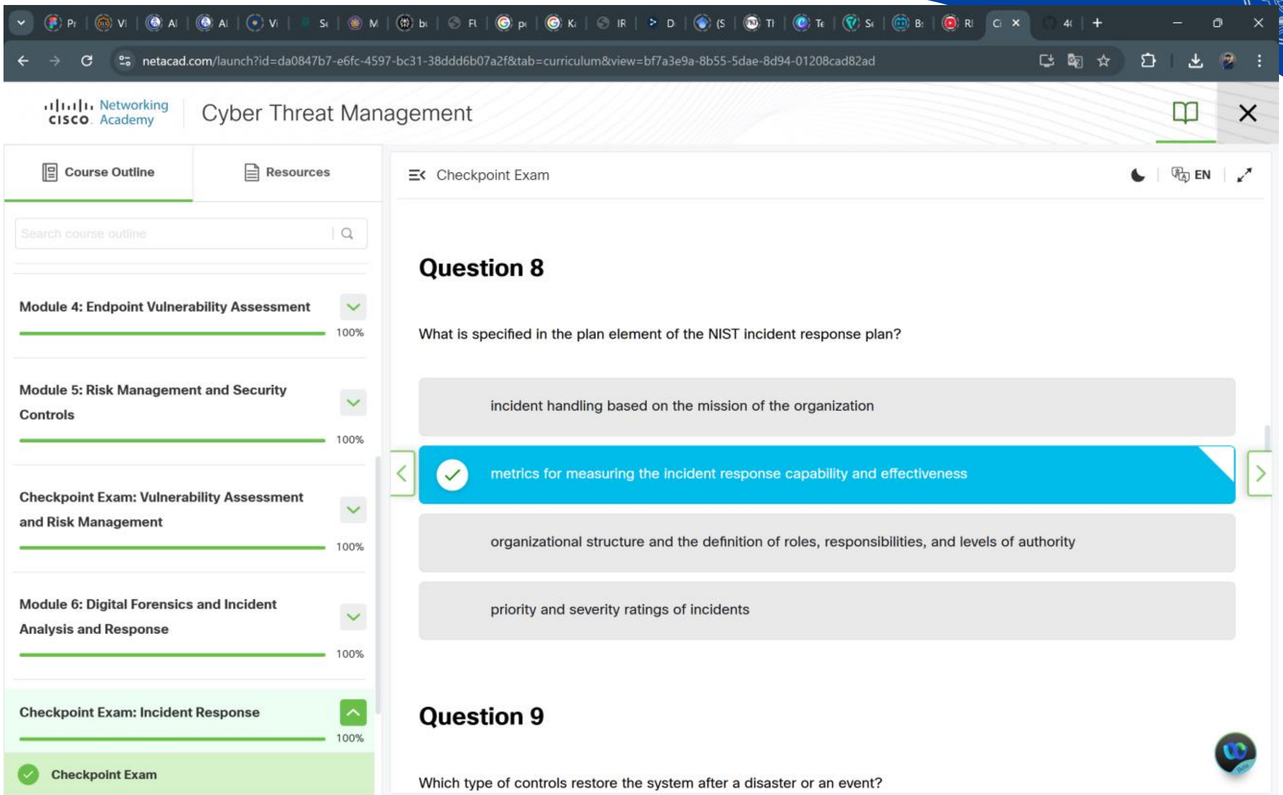
✓ Checkpoint Exam

Checkpoint Exam EN

Question 7

Match the intrusion event defined in the Diamond Model of intrusion to the description.

Categories:			Options:
a tool or technique used to attack the victim	A	C	✓ victim
the parties responsible for the intrusion	B	B	✓ adversary
the target of the attack	C	A	✓ capability
network path used to establish and maintain command and control	D	D	✓ infrastructure


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline
Module 4: Endpoint Vulnerability Assessment 100%
Module 5: Risk Management and Security Controls 100%
Checkpoint Exam: Vulnerability Assessment and Risk Management 100%
Module 6: Digital Forensics and Incident Analysis and Response 100%
Checkpoint Exam: Incident Response 100%
Checkpoint Exam
Checkpoint Exam
EN

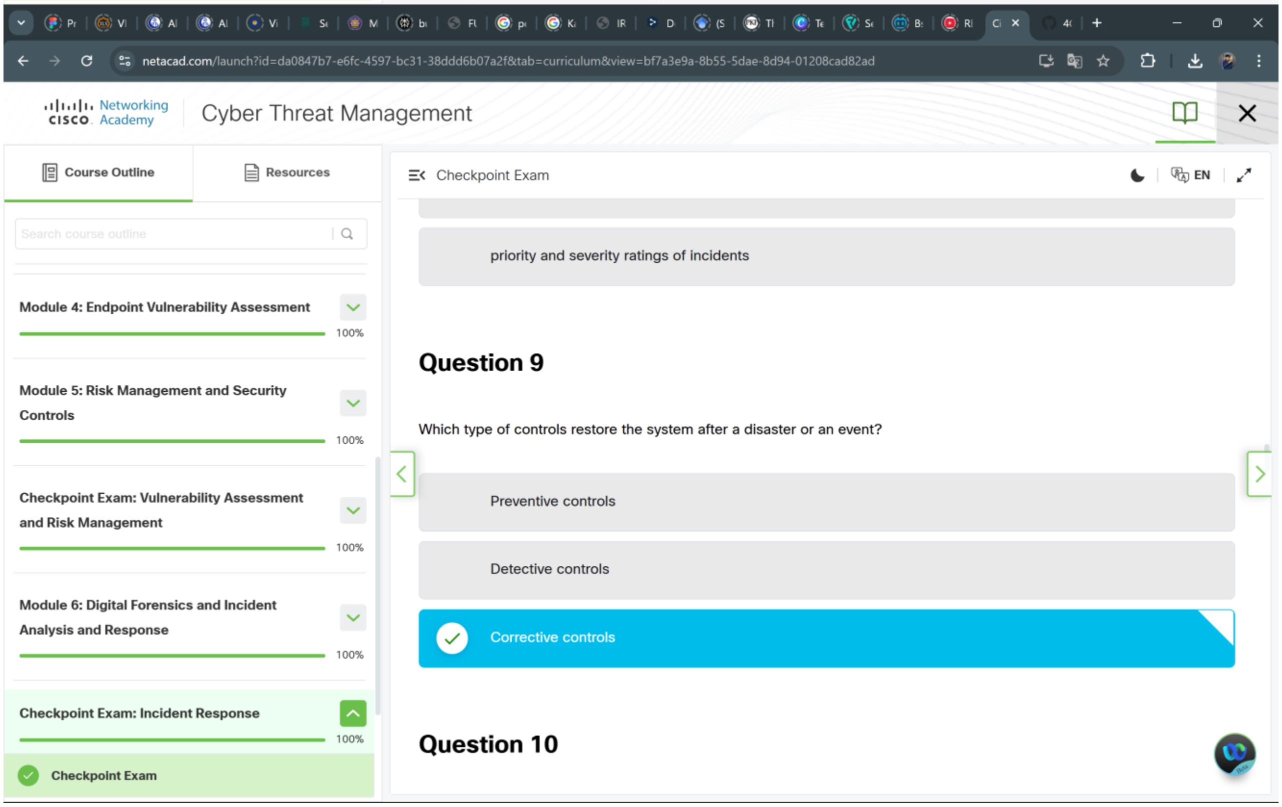
Question 8

What is specified in the plan element of the NIST incident response plan?

- incident handling based on the mission of the organization
- ✓ metrics for measuring the incident response capability and effectiveness
- organizational structure and the definition of roles, responsibilities, and levels of authority
- priority and severity ratings of incidents

Question 9

Which type of controls restore the system after a disaster or an event?


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline
Module 4: Endpoint Vulnerability Assessment 100%
Module 5: Risk Management and Security Controls 100%
Checkpoint Exam: Vulnerability Assessment and Risk Management 100%
Module 6: Digital Forensics and Incident Analysis and Response 100%
Checkpoint Exam: Incident Response 100%
Checkpoint Exam
Checkpoint Exam
EN

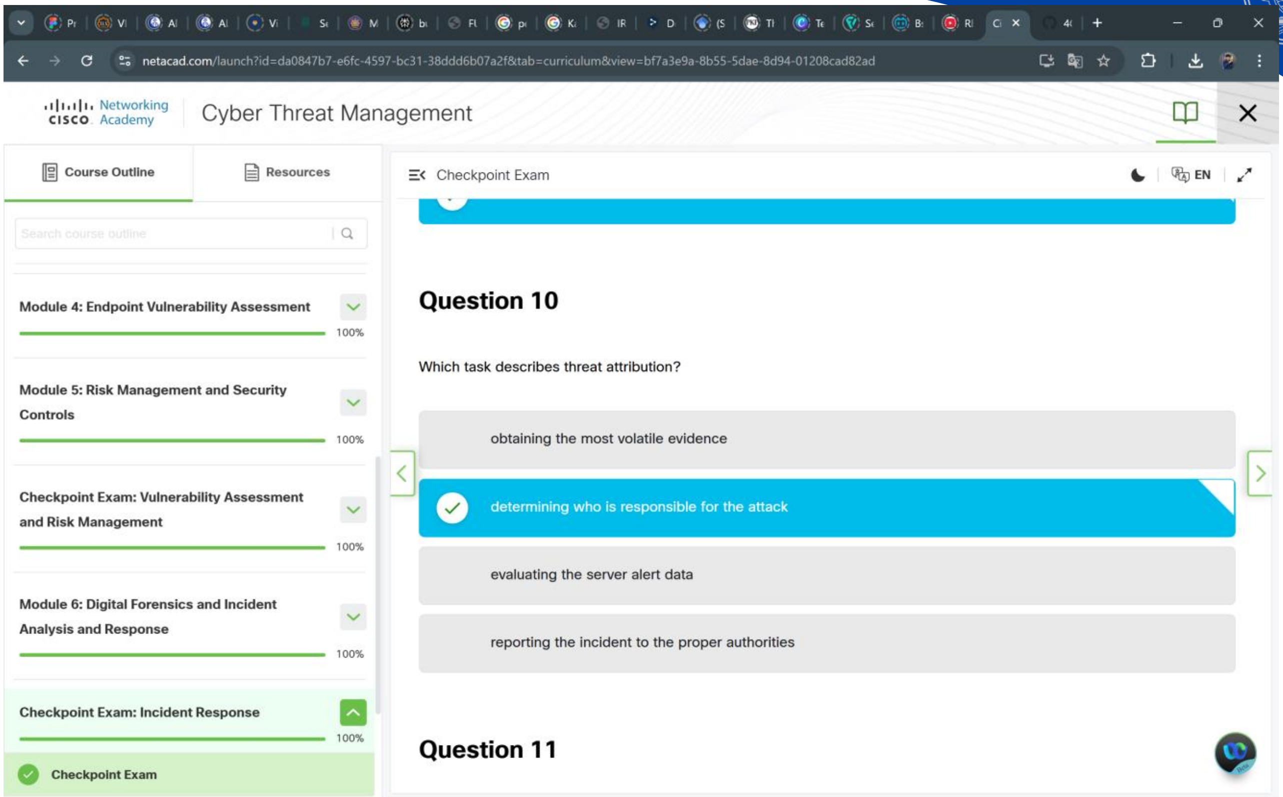
- priority and severity ratings of incidents

Question 9

Which type of controls restore the system after a disaster or an event?

- Preventive controls
- Detective controls
- ✓ Corrective controls

Question 10



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

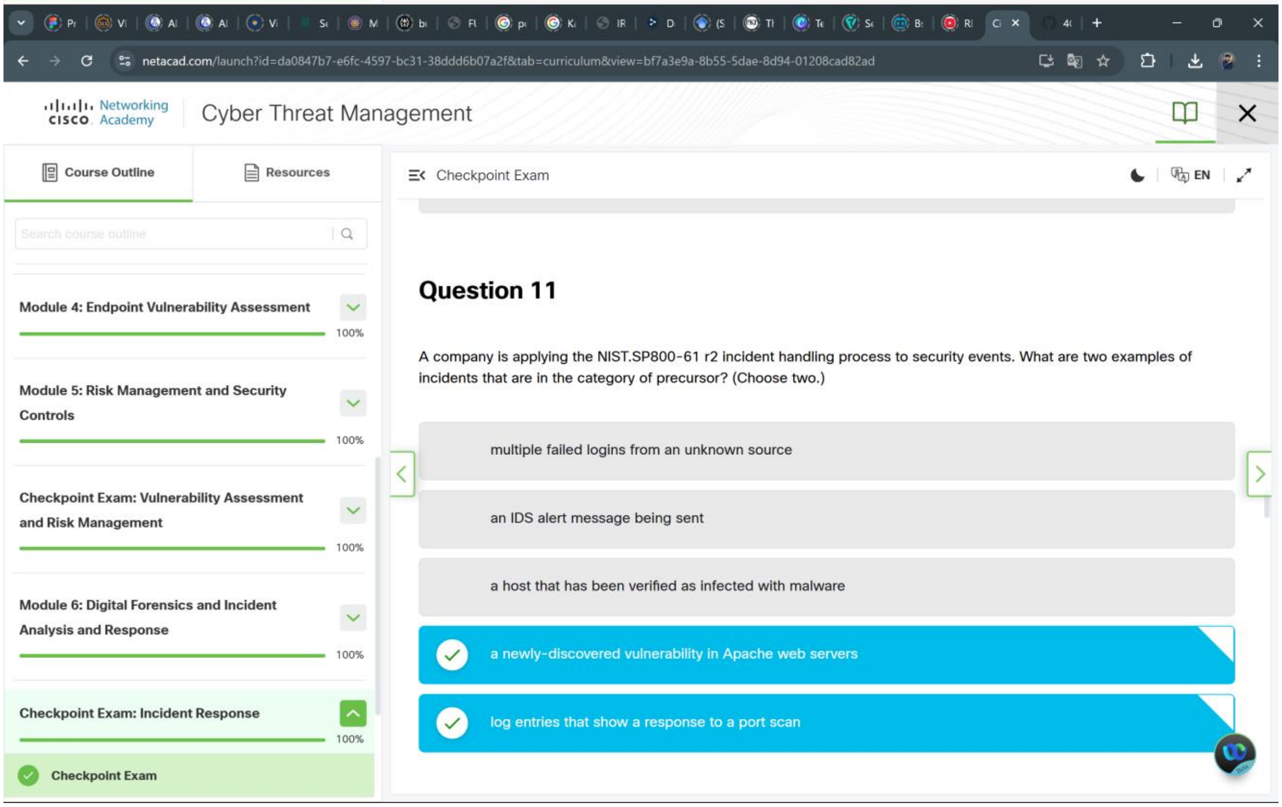
✓ Checkpoint Exam

Question 10

Which task describes threat attribution?

- obtaining the most volatile evidence
- ✓ determining who is responsible for the attack
- evaluating the server alert data
- reporting the incident to the proper authorities

Question 11



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

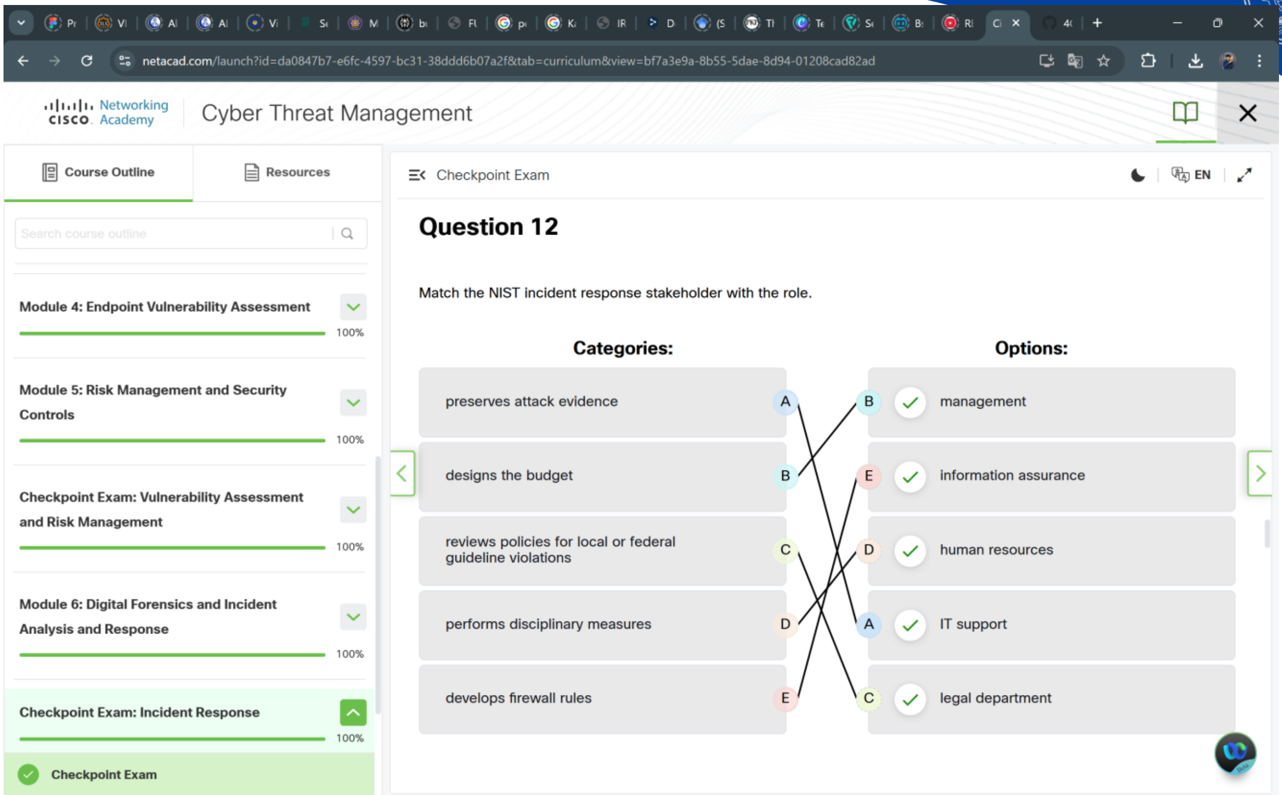
Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

Question 11

A company is applying the NIST.SP800-61 r2 incident handling process to security events. What are two examples of incidents that are in the category of precursor? (Choose two.)

- multiple failed logins from an unknown source
- an IDS alert message being sent
- a host that has been verified as infected with malware
- ✓ a newly-discovered vulnerability in Apache web servers
- ✓ log entries that show a response to a port scan


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cisco Networking Academy — Cyber Threat Management

Course Outline | Resources

Search course outline

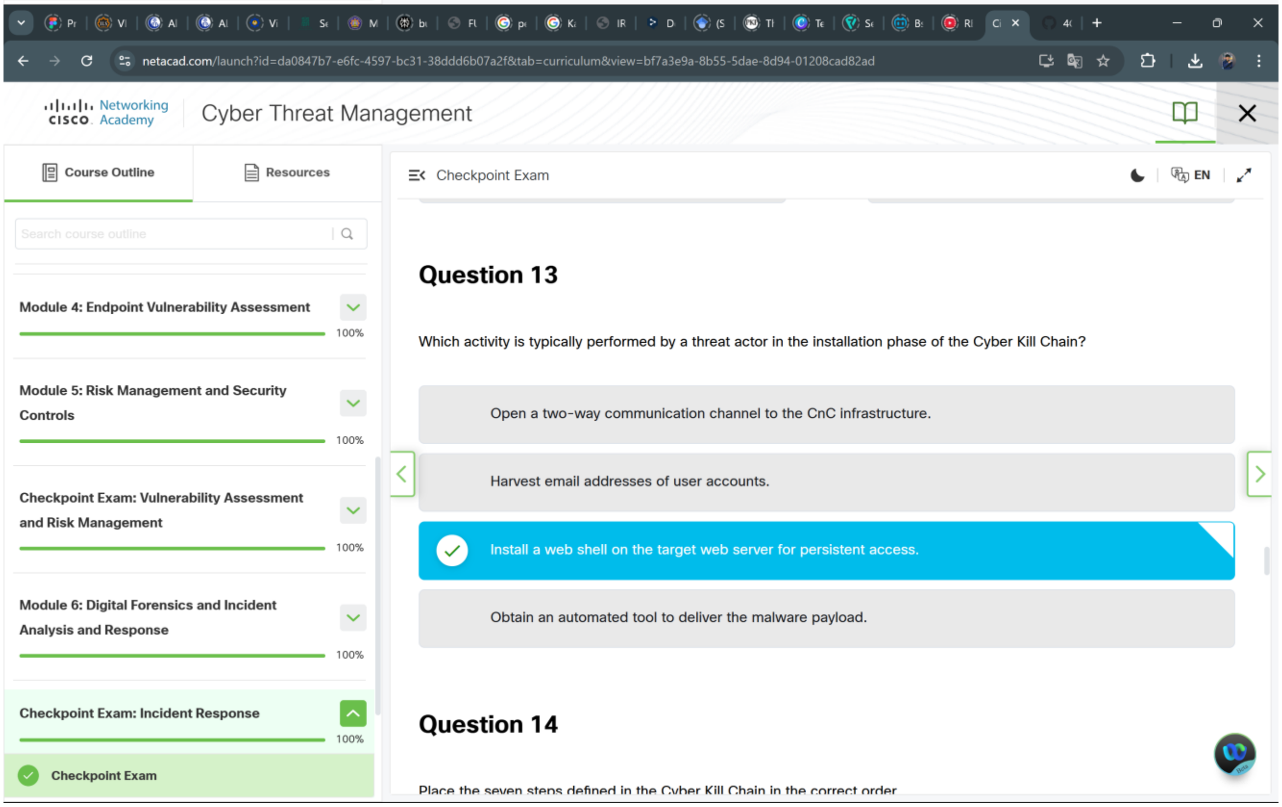
- Module 4: Endpoint Vulnerability Assessment — 100%
- Module 5: Risk Management and Security Controls — 100%
- Checkpoint Exam: Vulnerability Assessment and Risk Management — 100%
- Module 6: Digital Forensics and Incident Analysis and Response — 100%
- Checkpoint Exam: Incident Response — 100%
  - ✓ Checkpoint Exam

Checkpoint Exam | EN

Question 12

Match the NIST incident response stakeholder with the role.

Categories:			Options:
preserves attack evidence	A	B	✓ management
designs the budget	B	E	✓ information assurance
reviews policies for local or federal guideline violations	C	D	✓ human resources
performs disciplinary measures	D	A	✓ IT support
develops firewall rules	E	C	✓ legal department


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cisco Networking Academy — Cyber Threat Management

Course Outline | Resources

Search course outline

- Module 4: Endpoint Vulnerability Assessment — 100%
- Module 5: Risk Management and Security Controls — 100%
- Checkpoint Exam: Vulnerability Assessment and Risk Management — 100%
- Module 6: Digital Forensics and Incident Analysis and Response — 100%
- Checkpoint Exam: Incident Response — 100%
  - ✓ Checkpoint Exam

Checkpoint Exam | EN

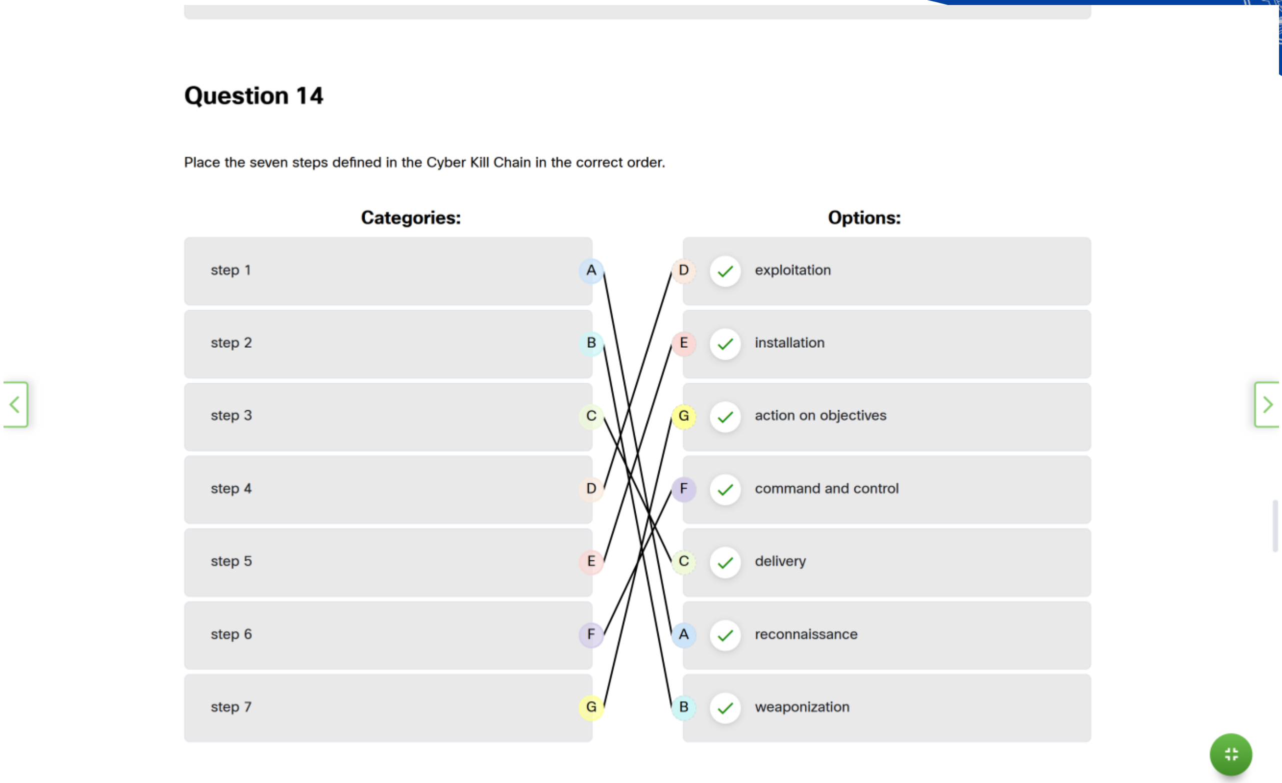
Question 13

Which activity is typically performed by a threat actor in the installation phase of the Cyber Kill Chain?

- Open a two-way communication channel to the CnC infrastructure.
- Harvest email addresses of user accounts.
- ✓ Install a web shell on the target web server for persistent access.
- Obtain an automated tool to deliver the malware payload.

Question 14

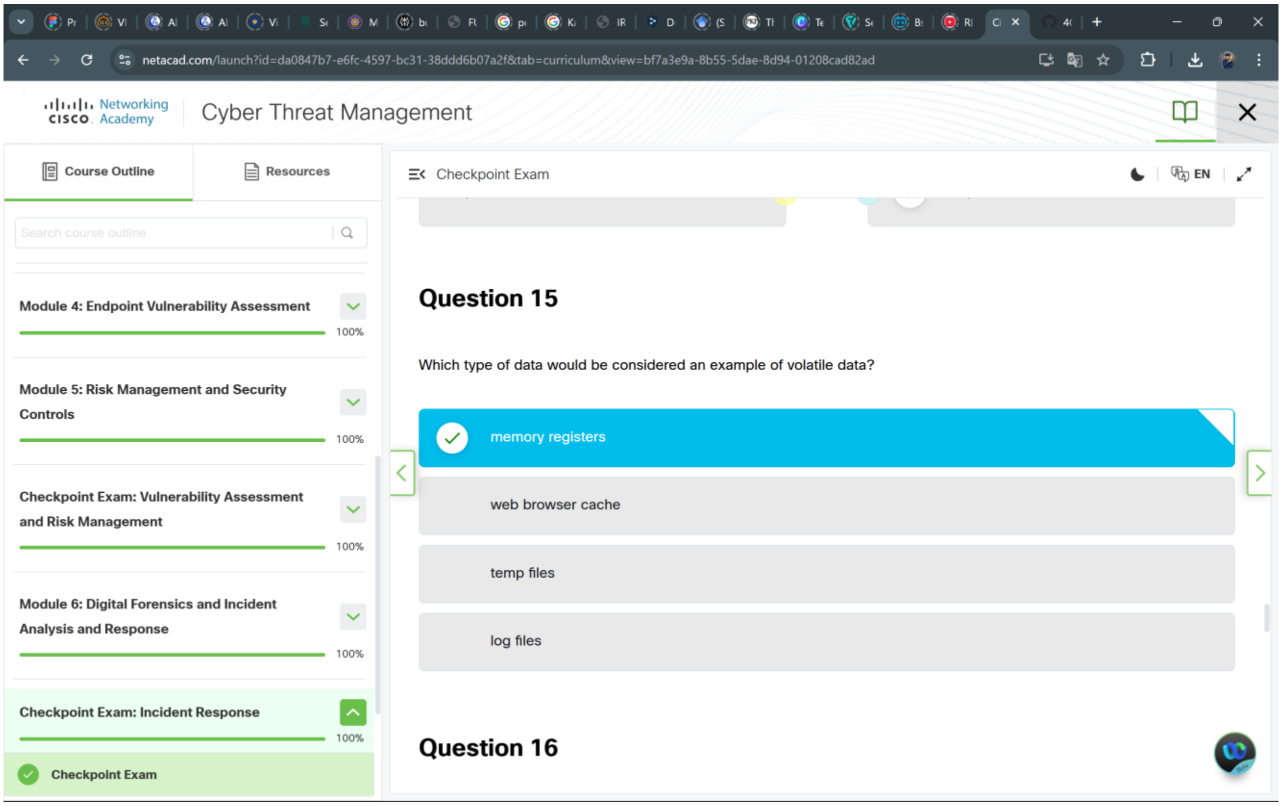
Place the seven steps defined in the Cyber Kill Chain in the correct order.



Question 14

Place the seven steps defined in the Cyber Kill Chain in the correct order.

Categories:			Options:
step 1	A	D	✓ exploitation
step 2	B	E	✓ installation
step 3	C	G	✓ action on objectives
step 4	D	F	✓ command and control
step 5	E	C	✓ delivery
step 6	F	A	✓ reconnaissance
step 7	G	B	✓ weaponization



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

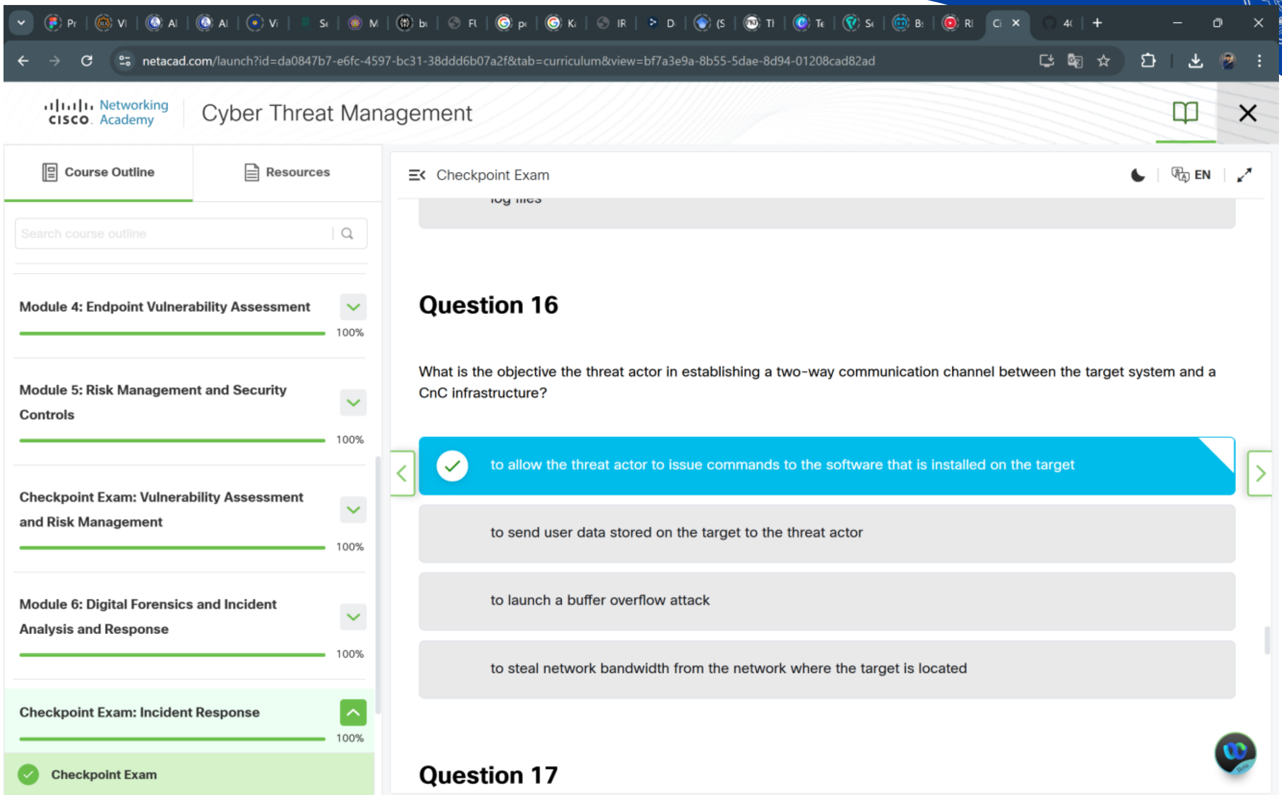
✓ Checkpoint Exam

Question 15

Which type of data would be considered an example of volatile data?

- ✓ memory registers
- web browser cache
- temp files
- log files

Question 16


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline
Checkpoint Exam
EN

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

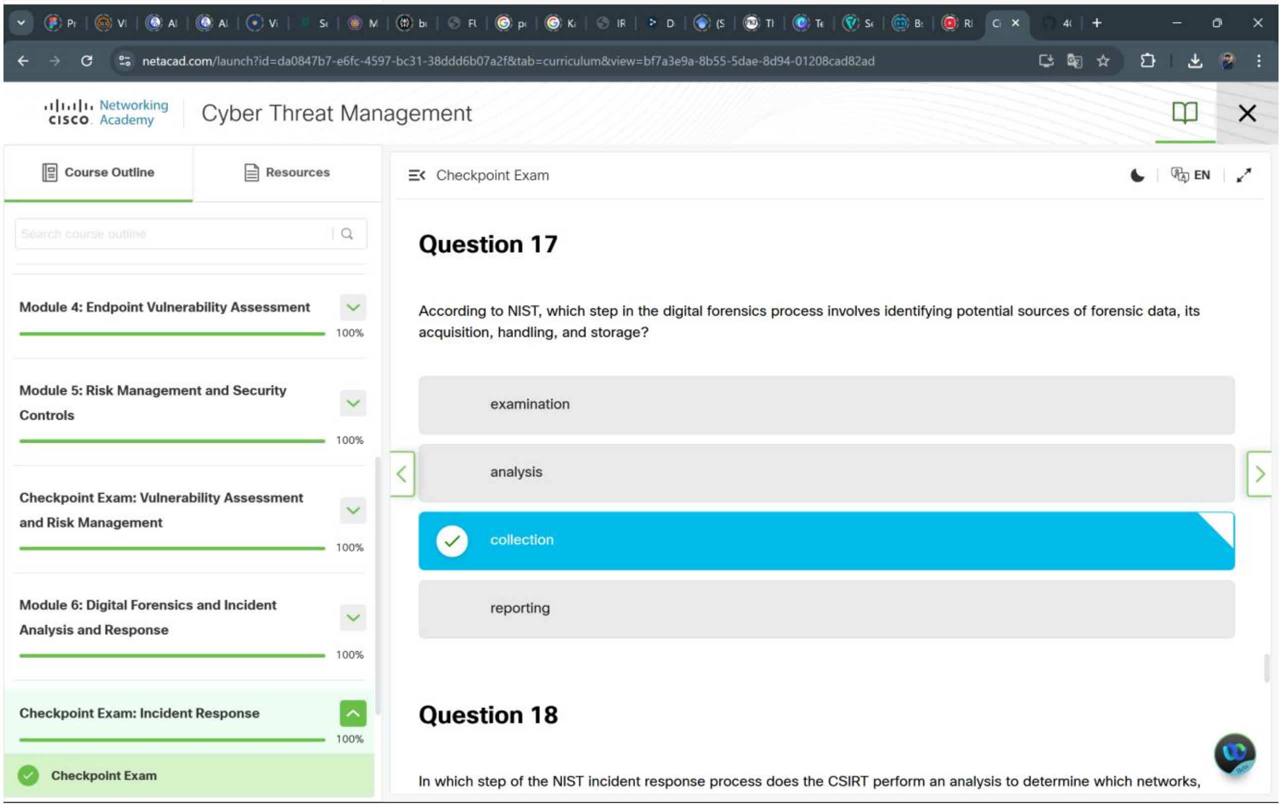
log files

Question 16

What is the objective the threat actor in establishing a two-way communication channel between the target system and a CnC infrastructure?

- ✓ to allow the threat actor to issue commands to the software that is installed on the target
- to send user data stored on the target to the threat actor
- to launch a buffer overflow attack
- to steal network bandwidth from the network where the target is located

Question 17


netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline
Checkpoint Exam
EN

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

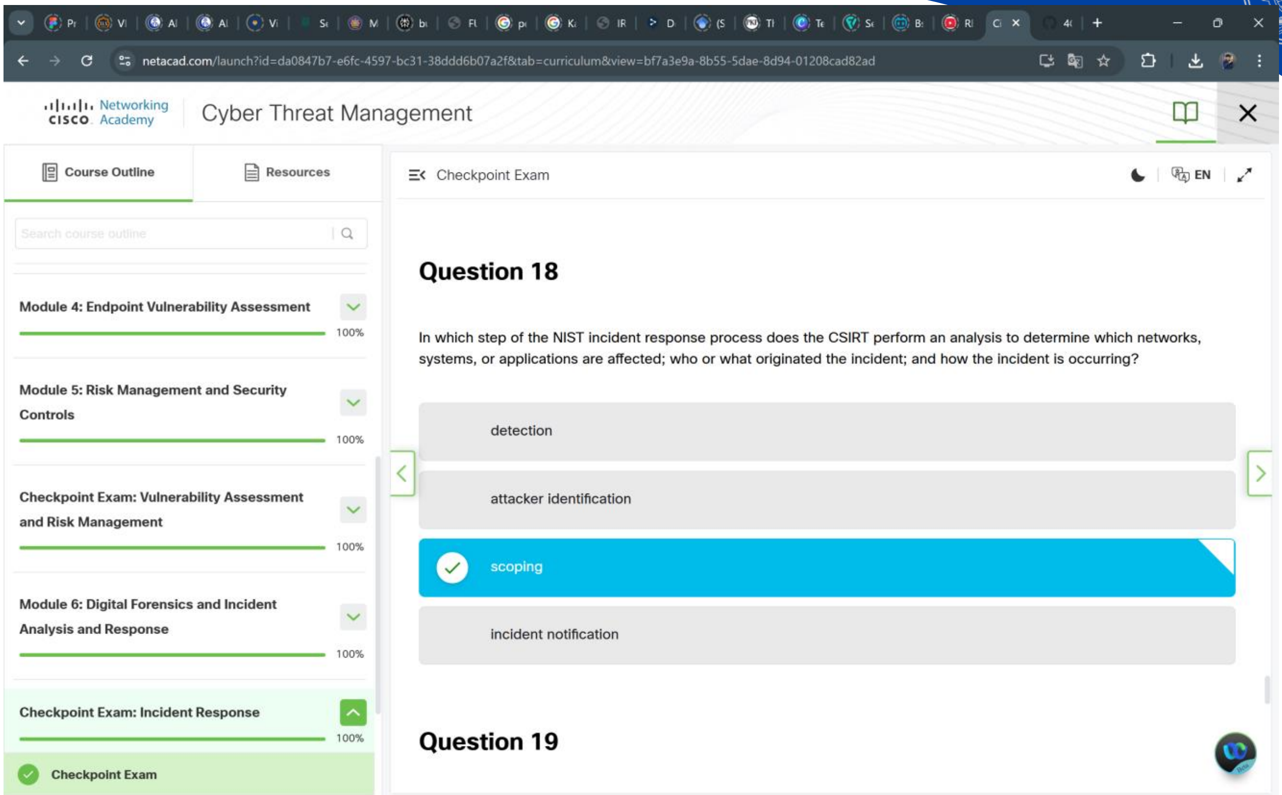
Question 17

According to NIST, which step in the digital forensics process involves identifying potential sources of forensic data, its acquisition, handling, and storage?

- examination
- analysis
- ✓ collection
- reporting

Question 18

In which step of the NIST incident response process does the CSIRT perform an analysis to determine which networks,



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cisco Networking Academy Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

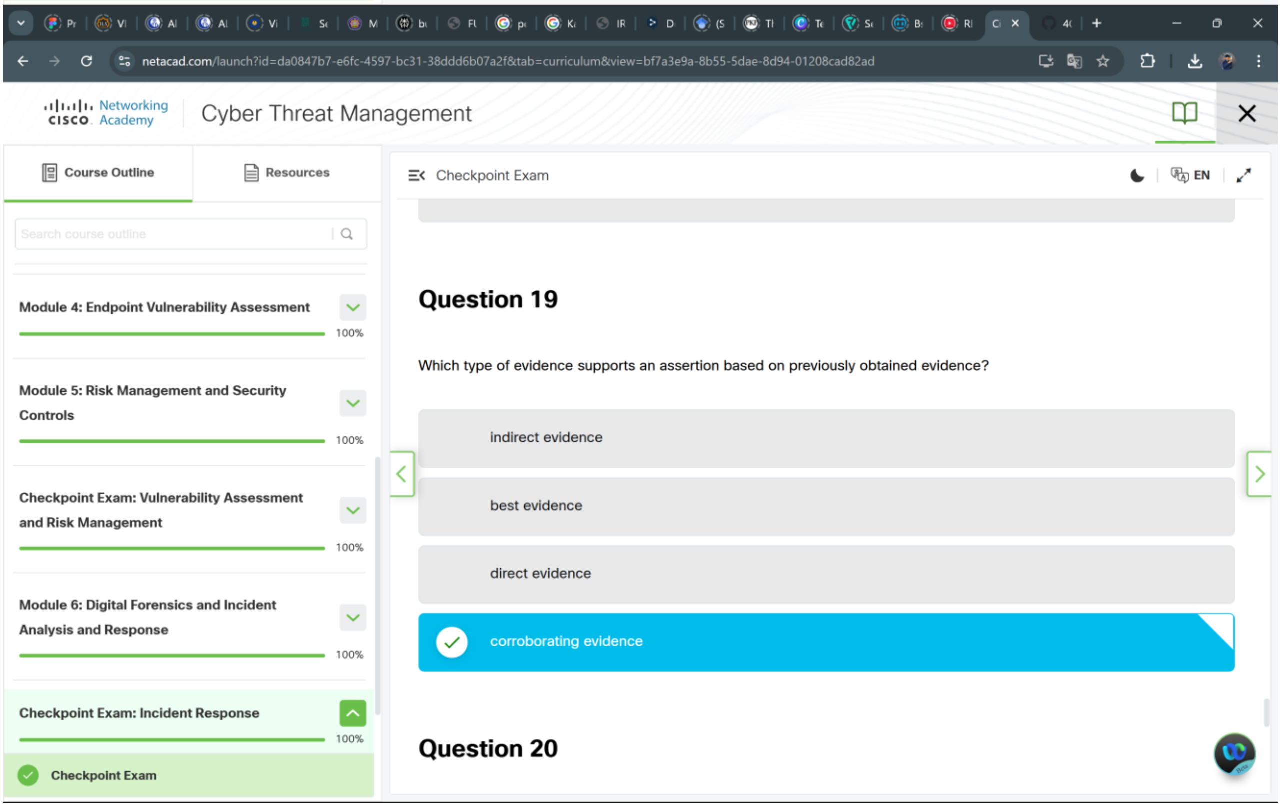
Checkpoint Exam

Question 18

In which step of the NIST incident response process does the CSIRT perform an analysis to determine which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring?

- detection
- attacker identification
- ✓ scoping
- incident notification

Question 19



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad

Cisco Networking Academy Cyber Threat Management

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

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

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

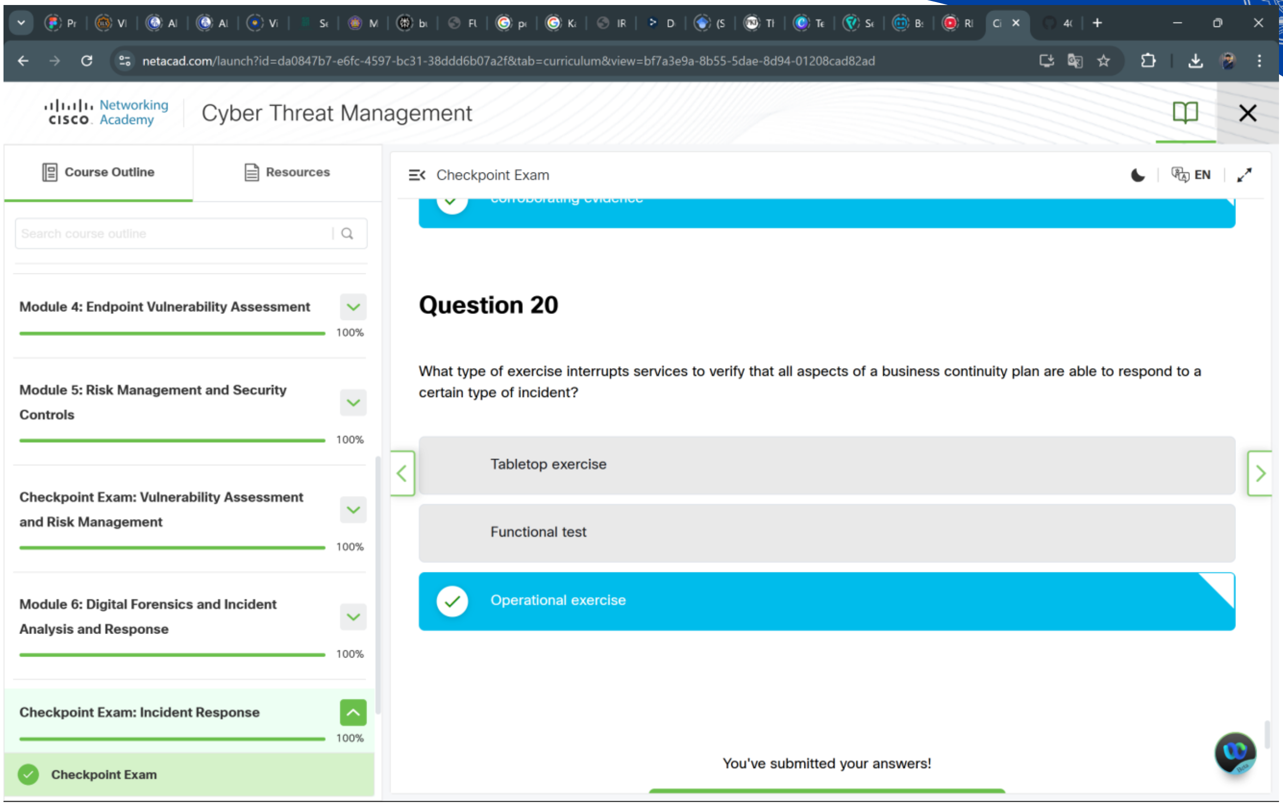
Checkpoint Exam

Question 19

Which type of evidence supports an assertion based on previously obtained evidence?

- indirect evidence
- best evidence
- direct evidence
- ✓ corroborating evidence

Question 20



netacad.com/launch?id=da0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=bf7a3e9a-8b55-5dae-8d94-01208cad82ad
Networking Academy
Cyber Threat Management
Course Outline
Resources
Search course outline
Module 4: Endpoint Vulnerability Assessment
100%
Module 5: Risk Management and Security Controls
100%
Checkpoint Exam: Vulnerability Assessment and Risk Management
100%
Module 6: Digital Forensics and Incident Analysis and Response
100%
Checkpoint Exam: Incident Response
100%
Checkpoint Exam
Checkpoint Exam
EN

corroborating evidence

Question 20

What type of exercise interrupts services to verify that all aspects of a business continuity plan are able to respond to a certain type of incident?

- Tabletop exercise
- Functional test
- ✓ Operational exercise

You've submitted your answers!