

Question Completion Status:

T

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----

Test Information

Description The midterm exam covers all of the material (including videos) from Weeks One and Two. It consists of multiple choice, True/False, Ordering, short answer, and essay questions.

Instructions This is a timed test. You will have 75 minutes to take the test and it must be completed in one sitting.

Multiple Attempts Not allowed. This test can only be taken once.

Force Completion This test can be saved and resumed later.

QUESTION 1**6 points**

Saved

Senior leadership support is required in order to have a successful incident response program.

- ☒ True
☐ False

QUESTION 2**6 points**

Saved

A _____ is an incident that is expected to cause significant damage, corruption, or loss of critical and/or strategic company or customer information. A high-level incident may involve widespread or extended loss of system or network resources.

- ☐ Low-level incident
☐ Moderate-level incident
☒ High-level incident
☐ Defcon-2

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Question Completion Status:

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

QUESTION 4**6 points**

Saved

A playbook and checklist are the same thing.

- ☐ True
- ☒ False

QUESTION 5**6 points**

Saved

Recovery activities are very closely aligned with those that may be found in an organization's _____.

- ☐ Pentest plan
- ☒ Business continuity or disaster recovery plans
- ☐ Network policy
- ☐ Business plan

QUESTION 6**6 points**

Saved

Any organization that collects log data should have a policy that covers the following areas (select all that apply):

- ☒ Logging of network activity is part of the normal business activity.
- ☐ Log data will be publicly available.
- ☐ Users do not have a reasonable expectation of privacy when using the network.
- ☐ Log data will not be protected.

QUESTION 7**6 points**

Save Answer

In which phase of incident response does an organization create and

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

🚩 Question Completion Status:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----

QUESTION 8**6 points**

Save Answer

When using tcpdump, the timestamp for the packet will be the original timestamp from the pcap file.

- ☐ True
- ☐ False

QUESTION 9**6 points**

Save Answer

What does this regular expression 246* match to from the following expression 246436:

- ☐ 24636
- ☐ 246
- ☐ 246*
- ☐ 2464

QUESTION 10**6 points**

Save Answer

A routing table is a key piece of evidentiary information that contains _____.

- ☐ switches
- ☐ firewalls
- ☐ routers
- ☐ hubs

QUESTION 11**6 points**

Save Answer

A CSIRT that provides reactive services gives training for non-CSIRT staff, gives briefs emerging security threats, supports the deployment of security tools, and provides assistance before an incident occurs.

- ☐ True
- ☐ False

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

🚩 Question Completion Status:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----

☐ False

QUESTION 13**6 points**[Save Answer](#)

In which phase of incident response does an organization take actions to limit the ability for attackers to continue compromising other network resources, communicating with command and control infrastructures, or exfiltrating confidential data?

- ☐ Preparation
- ☐ Detection
- ☐ Containment
- ☐ Eradication and Recovery

QUESTION 14**6 points**[Save Answer](#)

A _____ is an incident that may cause damage, corruption, or loss of replaceable information without compromise (there has been no misuse of sensitive customer information). This type of event may involve significant disruption to a system or network resource.

- ☐ Low-level incident
- ☐ Moderate-level incident
- ☐ High-level incident
- ☐ Defcon-2

QUESTION 15**6 points**[Save Answer](#)

A/An _____ allows for the dynamic assignment of IP addresses to systems on the LAN and is useful for tracking down workstations or other devices connected to the network.

- ☐ DHCP server
- ☐ authentication server
- ☐ web proxy server
- ☐ domain controller

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18



Save Answer

Save Answer



Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Question Completion Status:

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18



Analysis



Containment

QUESTION 19**40 points**

Save Answer

Define regular expressions and how they can be used for incident response.

				Paragraph		Arial		3 (12pt)											

QUESTION 20**40 points**

Save Answer

You are developing an incident response program and your CIO wants to know what type of log data you should collect. Provide your recommendations on three different types of log data you would collect and how it can be used for incident response. Your answer should explain why you chose each type of log data and should also explain how each type of data can be used.

				Paragraph		Arial		3 (12pt)											

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

🚩 Question Completion Status:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	--

Click Save and Submit to save and submit. Click Save All Answers to save all answers.