210-255 Q&As

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which example of a precursor is true?

A. A notification that a host is infected with malware.

B. An admin finds their password has been changed.

C. A log indicating a port scan was run against a host

D. A device configuration changed from the baseline without an audit log entry.

Correct Answer: C

QUESTION 2

Which compliance framework applies to safeguarding a patient prescription list?

A. PCI

B. SOX

C. HIPAA

D. COBIT

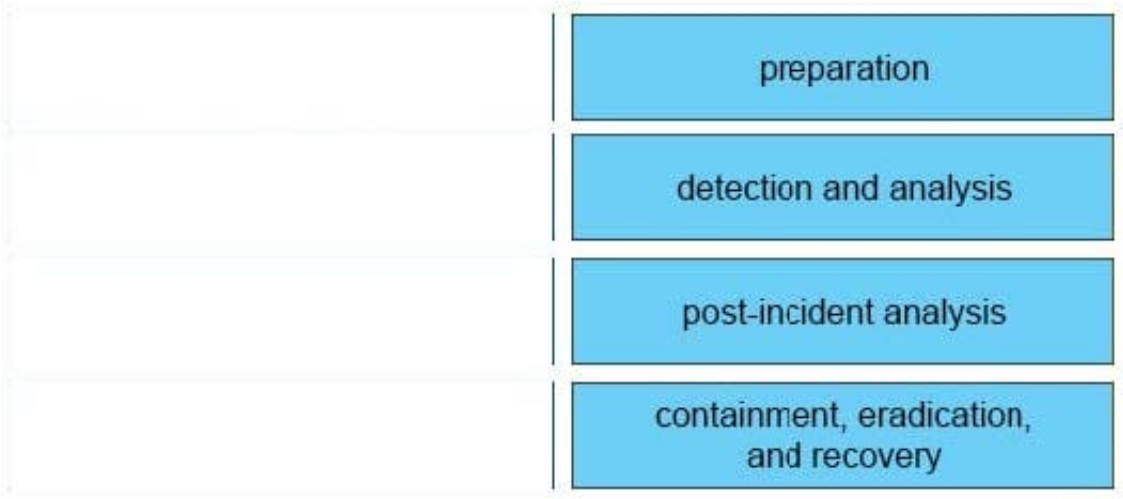
Correct Answer: C

QUESTION 3

Drag and drop the elements of incident handling from the left into the correct order on the right.

Select and Place:

Correct Answer:



QUESTION 4

Which data element must be protected with regards to PCI?

A. past health condition

B. geographic location

C. full name / full account number

D. recent payment amount

Correct Answer: C

QUESTION 5

What does 5-typle refer to?

A. set of five different values that comprise a SSL connection

B. set of five different values that comprise a HTTPS connection

C. set of five different values that comprise a UDP connection

D. set of five different values that comprise a TCP/IP connection

Correct Answer: D

QUESTION 6

What is the common artifact that is used to uniquely identify a detected file?

A. Hash

B. Timestamp

C. File size

Correct Answer: A

QUESTION 7

Which of the following are not components of the 5-tuple of a flow in NetFlow? (Select all that apply.)

A. Source IP address

B. Flow record ID

C. Gateway

D. Source port

E. Destination port

Correct Answer: BC

QUESTION 8

Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?

A. The website has been marked benign on all 68 checks.

B. The threat detection needs to run again.

C. The website has 68 open threats.

D. The website has been marked benign on 0 checks.

Correct Answer: A

QUESTION 9

What protocol is related to NAC?

A. 802.1Q

B. 802.1X

C. 802.1E

D. 802.1F

Correct Answer: B

QUESTION 10

Which incident handling phase is focused on minimizing the impact of the incident?

A. reporting

B. remediation

C. containment

D. scoping

Correct Answer: C

QUESTION 11

In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model\\'?

A. victim demographics, incident description, incident details, discovery and response

B. victim demographics, incident details, indicators of compromise, impact assessment

C. actors, attributes, impact, remediation

D. actors, actions, assets, attributes

Correct Answer: D

QUESTION 12

Drag and drop the type of evidence from the left onto the correct descnption(s) of that evidence on the right.

Select and Place:

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

Correct Answer:

	indirect evidence
	direct evidence
	corroborative evidence

QUESTION 13

Refer to the exhibit.

```
Mar 07 2018 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?

A. NetFlow

B. IDS

C. web proxy

D. firewall

Correct Answer: D

QUESTION 14

Which option is missing a malware variety per VERIS enumerations?

A. backdoor, command and control, denial or service attack

B. adware, brute force, client-side attack

C. packet sniffer, password dumper, scan network

D. abuse of functionality, cache poisoning, remote file inclusion

Correct Answer: D

QUESTION 15

Which process is being utilized when IPS events are removed to improve data integrity?

A. data normalization

B. data availability

C. data protection

D. data signature

Correct Answer: A