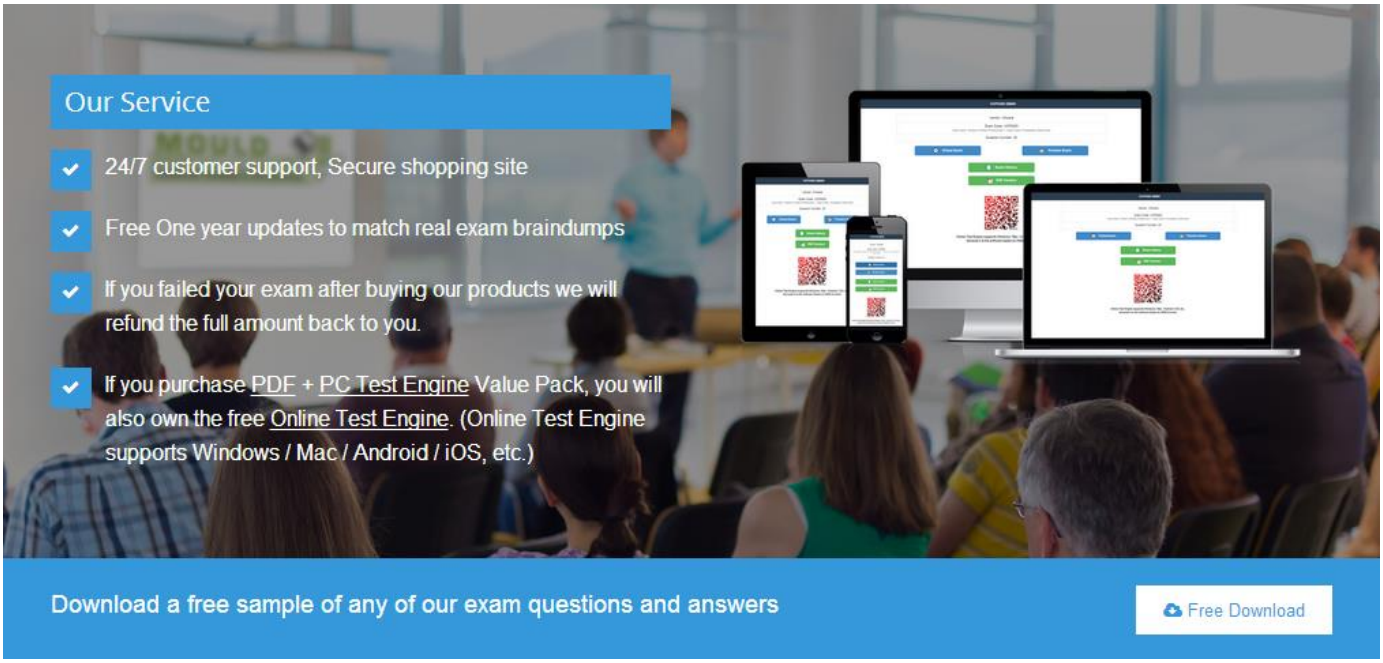
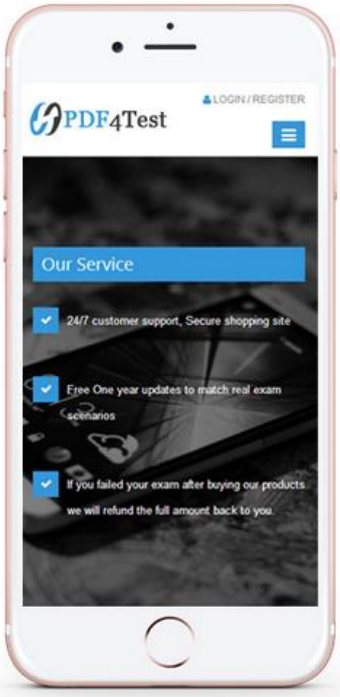
PDF4Test



QUALITY AND VALUE

PDF4Test Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our PDF4Test testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

PDF4Test offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.pdf4test.com

Free valid test questions and dumps pdf for certification test prep

Exam : **210-255**

Title : Implementing Cisco Cybersecurity Operations

Vendor : Cisco

Version : DEMO

NO.1 Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a security operations center (SOC)?

A. Cisco Managed Firepower Service

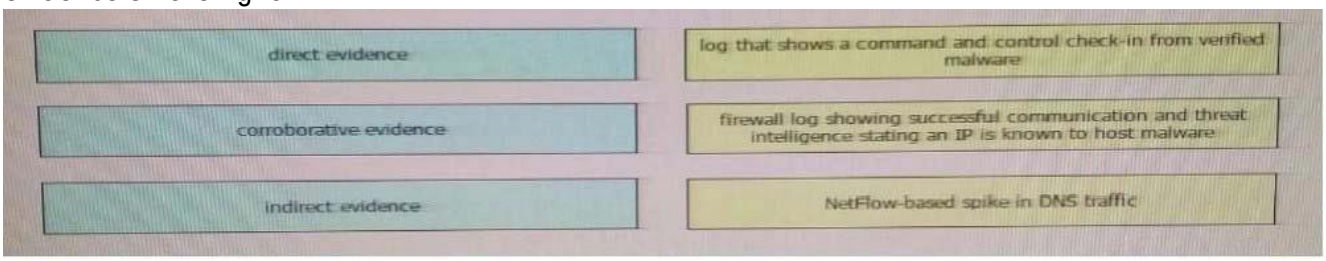
B. Cisco's Active Threat Analytics (ATA)

C. Cisco Jasper

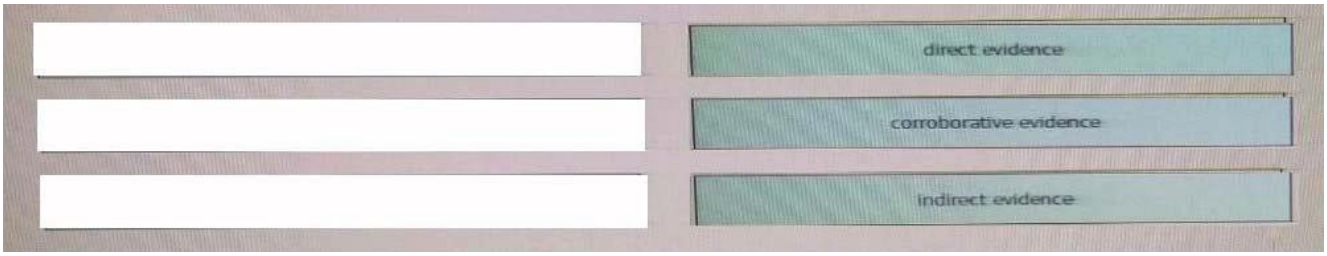
D. Cisco CloudLock

Answer: B

NO.2 Drag and drop the type of evidence from the left onto the correct deception(s) of that evidence on the right.



Answer:



NO.3 Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

A. URL

B. destination port

C. hash

D. IP address

Answer: C

NO.4 Which Security Operations Center's goal is to provide incident handling to a country?

A. Coordination Center

B. National CSIRT

C. Analysis Center

D. Internal CSIRT

Answer: B

NO.5 Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. detection and analysis

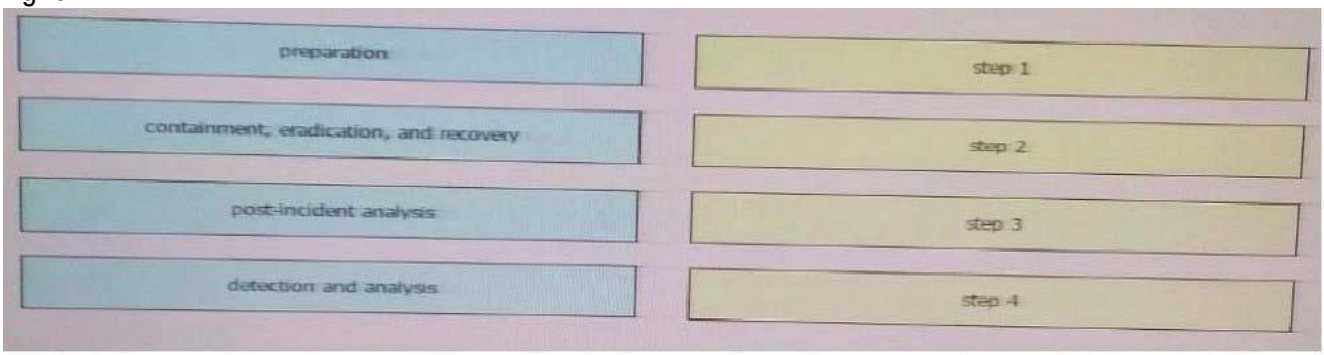
B. post-incident analysis

C. containment, eradication, and recovery

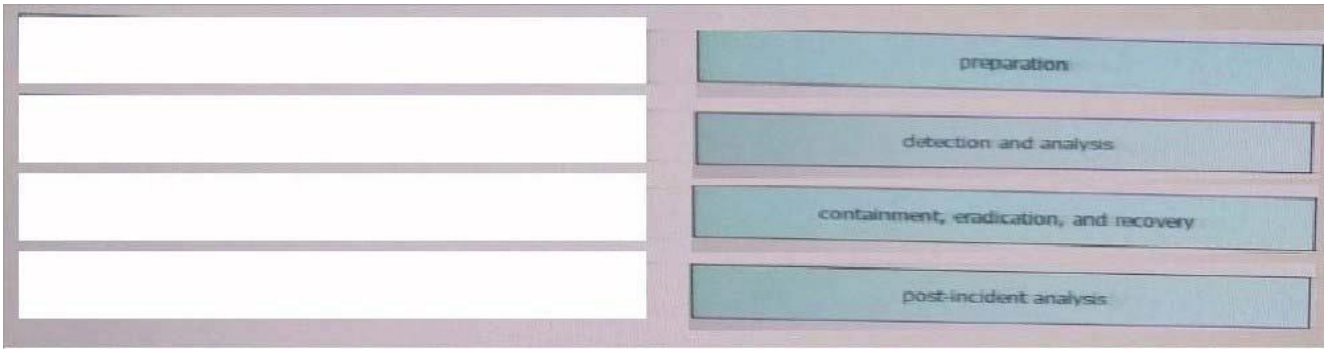
D. preparation

Answer: B
Explanation
3.4.2 Using Collected Incident Data (which falls under post incident analysis in the aforementioned document)Lessons learned activities should produce a set of objective and subjective data regarding each incident.Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as wellas changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (e.g., improvements in efficiency, reductions in costs).

NO.6 Drag and drop the elements of incident handling from the left into the correct order on the right.



Answer:



Explanation
Preparation
Detection and analysis
Containment, eradication and recovery
Post incident analysis

NO.7 Which of the following are the three broad categories of cybersecurity investigations?
A. Public, private, and corporate investigations
B. Public, private, and individual investigations
C. Government, corporate, and private investigations
D. Judiciary, private, and individual investigations

Answer: B

NO.8 You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. weaponization

B. action on objectives

C. delivery

D. reconnaissance

Answer: B

Explanation

It is an Advanced Persistent Threat group that being exfiltrated confidential data, and Action and Objectives says that adversary is inside the network and starting to achieve his or her objective for launching the attack.

An adversary could use this opportunity to steal data.

NO.9 Choose the option that best describes NIST data integrity

A. use only sha-1

B. no need to hash data & backup and compare hashes

C. you must hash data & backup and compare hashes

D. use only md5

Answer: C

NO.10 From a security perspective, why is it important to employ a clock synchronization protocol on a network?

A. so that everyone knows the local time

B. to construct an accurate timeline of events when responding to an incident

C. to guarantee that updates are pushed out according to schedule

D. to ensure employees adhere to work schedule

Answer: B

Explanation

The Importance of Time Synchronization for Your NetworkIn modern computer networks time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events happen. Time also provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating log files between these devices is difficult, even impossible. Following are just a few specific reasons:Tracking security breaches, network usage, or problems affecting a large number of components can be nearly impossible if timestamps in logs are inaccurate. Time is often the critical factor that allows an event on one network node to be mapped to a corresponding event on another.To reduce confusion in shared filesystems, it is important for the modification times to be consistent, regardless of what machine the filesystems are on.