

1.

Select the missing phase of Incident Response: Preparation, _____, Containment, Eradication & Recovery, Post Incident Activity.

1 point
- ☐

Root Cause Analysis

☒

Detection and Analysis

☐

Execution

☐

Acquire Data
2.
- Which statement is true about an incident?
- 1 point

☐

An incident becomes an event if a threat is identified.

☐

Incidents involved external actors while events involved internal actors.

☒

An incident is an event that negatively affects IT systems.

☐

An incident is any collection of 3 or more related events.

3.

True or False: A Coordinating Incidents Response Team provides advice and guidance to the Distributed IR teams in each department, but generally does not have specific authority over those teams.

1 point

☒

True

☐

False

4.

Which Incident Response Team model describes a team that has authority over all aspects of IR within the entire organization?

1 point

☐

Distributed

☐

Coordinating

☐

Control

☒

Central

5.

In what way will having a set of predefined baseline questions will help you in the event of an incident?

1 point

☒

Coordinate with other teams and the media.

☐

Avoid events turning into Incidents.

☐

Interrogate suspects.

☐

Trap the bad actors.

6.

Incident Response team resources can be divided into which three (3) of the following categories?

1 point

☒

Incident Analysis Resources

☒

Incident Handler Communications and Facilities

☒

Incident Analysis Hardware and Software

☐

Incident Post-Analysis Resources

7.

Port lists, Documentation, and Cryptographic hashes all belong to which Incident Response resource category?

1 point

☐

Incident Post-Analysis Resources

☐

Incident Analysis Hardware and Software

☒

Incident Analysis Resources

☐

Incident Handler Communications and Facilities

8.

Which three (3) of the following would be considered an incident detection indicator?

1 point

☒

An application log showing numerous failed login attempts from an unknown remote system.

☒

The discovery of a file containing unusual characters by a system administrator.

☒

A significant deviation from typical network traffic flow patterns.

☐

Detecting the use of a vulnerability scanner.

9.

Which type of monitoring system analyzes logs and events in real time?

1 point

☐

IDS

☐

DLP

☒

SIEM

☐

IPS

10.

True or False: Highly detailed and thorough documentation is needed to support the analysis of current and future incidents.

1 point

☒

True

☐

False

11.

What is the proper classification for a breach that results in sensitive or proprietary information being changed or deleted.

1 point

☒

Integrity Loss

☐

Proprietary Breach

☐

Privacy Breach

☐

None

12.

What is the proper classification for the recovery effort from a breach if sensitive data was stolen and posted on a public web site?

1 point

☐

Extended

☐

Supplemented

☒

Not Recoverable

☐

Regular

13.

During which stage of a comprehensive Containment, Eradication & Recovery strategy does NIST recommend considering the following: Eliminate components of the incident, Disable compromised accounts, and Identify and mitigate vulnerabilities?

1 point

☐

Containment

☒

Eradication

☐

Recovery

☐

None of these.

14.

Which Post Incident activity would include reviewing response times, which systems were impacted and other metrics associated with the incident?

1 point

☐

Evidence retention

☐


Lessons learned meeting

☐

Documentation review & update

☒

Utilizing collected data

Coursera Honor Code [Learn more](#) 

☒

I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit

Save draft