1. Which two (2) key components are part of incident response? (Select 2) **1 point**

- [ ] Threat
- [x] Response team
- [ ] Attack
- [x] Investigation

2. Which is **not** part of the Sans Institutes Audit process? **1 point**

- (•) Help to translate the business needs into technical or operational needs.
- ( ) Define the audit scope and limitations.
- ( ) Feedback based on the findings.
- ( ) Deliver a report.

3. Which key concept to understand incident response is defined as "*data inventory, helps to understand the current tech status, data classification, data management, we could use automated systems. Understand how you control data retention and backup.*" **1 point**

- ( ) Post-Incident
- ( ) Automated Systems
- ( ) BCP & Disaster Recovery
- (•) E-Discovery

4. Which is **not** included as part of the IT Governance process? **1 point**

- ( ) Procedures
- ( ) Tactical Plans
- (•) Audits
- ( ) Policies

5. Trudy reading Alice's message to Bob is a violation of which aspect of the CIA Triad? **1 point**

- (•) Confidentiality
- ( ) Integrity
- ( ) Availability

6. A hash is a mathematical algorithm that helps assure which aspect of the CIA Triad? **1 point**

- ( ) Confidentiality
- (•) Integrity
- ( ) Availability

7. A successful DOS attack against your company's servers is a violation of which aspect of the CIA Triad? **1 point**

- ( ) Confidentiality
- ( ) Integrity
- (•) Availability

8. Which of these is an example of the concept of non-repudiation? **1 point**

- (•) Alice sends a message to Bob and Bob knows for a certainty that it came from Alice and no one else.
- ( ) Alice sends a message to Bob with certainty that it will be delivered.
- ( ) Alice sends a message to Bob with certainty that it was not altered while in route by Trudy.
- ( ) Alice sends a message to Bob and Alice is certain that it was not read by Trudy.

9. You have been asked to establish access to corporate documents in such a way that they can be read from anywhere, but only modified while the employees are in the office. Which 2 access criteria types were likely involved in setting this up? **1 point**

- [x] Physical location
- [x] Transaction type
- [ ] Timeframe
- [ ] Groups

10. In incident management, an observed change to the normal behavior of a system, environment or process is called what? **1 point**

- ( ) Incident
- ( ) Threat
- (•) Event
- ( ) Attack

11. In incident management, tools like SIEM, SOA and UBA are part of which key concept? **1 point**

- ( ) E-Discovery
- ( ) BCP & Disaster Recovery
- ( ) Post-Incident Activities
- (•) Automated system

12. Which phase of the Incident Response Process do steps like *Carry out a post incident review* and *Communicate and build on lessons learned* fall into? **1 point**

- ( ) Respond
- (•) Follow Up
- ( ) Prepare

13. In the context of security standards and compliance, which two (2) of these are considered normative and compliance items? **1 point**

- [ ] They seek to improve performance, controls and metrics.
- [x] They serve as an enforcement mechanism for government, industry or clients.
- [ ] They help translate the business needs into technical or operational needs.
- [x] They are rules to follow for a specific industry.

14. A company document that details how an employee should request Internet access for her computer would be which of the following? **1 point**

- ( ) Strategic Plan
- (•) Procedure
- ( ) Policy
- ( ) Tactical Plan

15. Which of these is a methodology by which to conduct audits? **1 point**

- ( ) SOX
- ( ) HIPPA
- ( ) PCI/DSS
- (•) OCTAVE

16. Mile 2 CPTE Training teaches you how to do what? **1 point**

- (•) Conduct a pentest
- ( ) Conduct a Ransomware attack
- ( ) Construct a botnet
- ( ) Advanced network management tasks

17. Which three (3) statements about OWASP are True? **1 point**

- [x] OWASP stands for Open Web Application Security Project
- [ ] OWASP Top 10 only lists the top 10 web application vulnerabilities but you must engage an OWASP certified partner to learn how to fix them.
- [x] OWASP provides guidance and tools to help you address web application vulnerabilities on their Top 10 list.
- [x] OWASP provides tools and guidance for mobile applications.

Coursera Honor Code Learn more

- [x] 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**