1. In creating an incident response capability in your organization, NIST recommends taking 6 actions. Which three (3) actions that are a included on that list? (Select 3) **1 point**

- [x] Considering the relevant factors when selecting an incident response team model
- [ ] Secure executive sponsorship for the incident response plan
- [x] Establish policies and procedures regarding incident-related information sharing
- [x] Develop incident response procedures

2. Which incident response team model would best fit the needs of a the field offices of a large distributed organizations? **1 point**

- ( ) Coordinating incident response team
- (•) Distributed incident response team
- ( ) Hybrid incident response team
- ( ) Central incident response team

3. Which incident response team staffing model would be appropriate for a small retail store that has just launched an online selling platform and finds it is now under attack? The platform was put together by its very small IT department who has no experience in managing incident response. **1 point**

- ( ) Use internal IT staff only, forcing them to come up to speed as quickly as possible
- (•) Completely outsource the incident response work to an onsite contractor with expertise in monitoring and responding to incidents
- ( ) Outsource the monitoring of intrusion detection systems and firewalls to an offsite managed security service provider while leaving the response to detected incidents to current IT staff
- ( ) Migrate all online operations to a cloud service provider so you will not have to worry about further attacks

4. Which three (3) technical skills are important to have in an organization's incident response team? (Select 3) **1 point**

- [ ] Encryption
- [x] System administration
- [x] Programming
- [x] Network administration

5. Identifying incident precursors and indicators is part of which phase of the incident response lifecycle? **1 point**

- ( ) Preparation
- (•) Detection & Analysis
- ( ) Post-Incident Activity
- ( ) Containment, Eradication & Recovery

6. Automatically isolating a system from the network when malware is detected on that system is part of which phase of the incident response lifecycle? **1 point**

- ( ) Post-Incident Activity
- (•) Containment, Eradication & Recovery
- ( ) Detection & Analysis
- ( ) Preparation

7. According to the IRIS Framework, during which stage of an attack would the attacker send phishing email, steal credentials and establish a foothold in the target network? **1 point**

- ( ) Continue the attack, expand network access
- ( ) Continuous phases occur
- ( ) Attack beginnings
- (•) Launch and execute the attack
- ( ) Attack objective execution

8. According to the IRIS Framework, during which stage of an attack would the attacker execute their final objectives? **1 point**

- ( ) Attack beginnings
- ( ) Launch and execute the attack
- ( ) Continue the attack, expand network access
- ( ) Continuous phases occur
- (•) Attack objective execution

9. According to the IRIS framework, during the first stage of an attack, when the bad actors are conducting external reconnaissance and aligning their tactics, techniques and procedures, what should the IR team be doing as a countermeasure? **1 point**

- ( ) Analyze all network traffic and endpoints, searching for anomalous behavior
- ( ) Implement strong endpoint detection and mitigation strategies
- (•) Build a threat profile of adversarial actors who are likely to target the company
- ( ) Enforce strong user password policies by enabling multi-factor authentication and restricting the ability to use the same password across systems
- ( ) Thoroughly examine available forensics to understand attack details, establish mitigation priorities, provide data to law enforcement, and plan risk reduction strategies

10. According to the IRIS framework, during the fourth phase of an attack, the attackers will attempt to evade detection. What should the IR team be doing as a countermeasure? **1 point**

- ( ) Enforce strong user password policies by enabling multi-factor authentication and restricting the ability to use the same password across systems
- ( ) Build a threat profile of adversarial actors who are likely to target the company
- (•) Analyze all network traffic and endpoints, searching for anomalous behavior
- ( ) Implement strong endpoint detection and mitigation strategies
- ( ) Thoroughly examine available forensics to understand attack details, establish mitigation priorities, provide data to law enforcement, and plan risk reduction strategies

11. True or False. A data breach always has to be reported to law enforcement agencies. **1 point**

- ( ) True
- (•) False

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