UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL ASSIGNMENT
MARCH 2026 SEMESTER

COURSE CODE	:	IKB42003
COURSE NAME	:	INCIDENT HANDLING AND RESPONSE
PROGRAMME NAME	:	BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	24 JUNE 2026
TIME	:	9:00 AM – 11:00 AM
DURATION	:	2 HOURS

INSTRUCTIONS TO CANDIDATES

1. Candidates are required to read all instructions carefully before answering the questions.
2. This question paper contains printed information on both sides of the paper.
3. This question paper consists of TWO (2) sections, namely Section A and Section B.
4. Candidates must answer ALL questions in English ONLY.
5. Write your answers in the Answer Booklet provided.

THERE ARE 11 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

TOTAL: 80 MARKS

SECTION A (30 marks)

INSTRUCTION: Answer all questions.

Please use the answer booklet provided.

1. A financial organization recently experienced a ransomware attack that temporarily disrupted access to employee workstations. During an internal review, the cybersecurity manager discovered that the organization had no formal incident response procedures, employees were unfamiliar with reporting suspicious activities, and backups had not been tested for several months. Based on the incident handling preparation phase, which of the following actions should have been prioritized before the incident occurred to improve the organization's readiness?
   A. Disconnecting all employee computers from the internet permanently
   B. Creating incident response procedures, conducting staff training, and preparing recovery resources
   C. Waiting for a cyberattack to happen before deciding the best response strategy
   D. Replacing all employees involved in the incident with new personnel

2. A university's cybersecurity team is preparing to improve its incident handling capabilities after several phishing attempts targeted staff and students. The Chief Information Security Officer (CISO) wants to ensure that everyone involved understands their responsibilities during a cybersecurity incident. Which preparation activity would be the MOST appropriate to achieve this objective?
   A. Defining roles and responsibilities for the incident response team and conducting simulation exercises
   B. Allowing every employee to independently decide how to respond to incidents
   C. Purchasing additional office computers for administrative staff only
   D. Ignoring phishing awareness because technical controls alone are sufficient

3. A healthcare company experienced a malware infection after an employee unknowingly clicked a malicious email attachment. During the post-incident investigation, the IT manager concluded that employees had never attended cybersecurity awareness training and many systems had outdated security patches. Which preventive measures could MOST effectively reduce the likelihood of similar incidents in the future?
   A. Disabling all internet access permanently for employees
   B. Conducting security awareness training and regularly updating systems with security patches
   C. Replacing all employee laptops every month
   D. Allowing employees to install any software they prefer to improve flexibility

4. A security analyst notices unusual login activities occurring at 2:30 AM involving privileged administrator accounts. To determine whether unauthorized access occurred, the analyst reviews records showing login timestamps, user authentication attempts, and system configuration changes. Which type of data source is MOST useful for this investigation?
   A. Network logs
   B. Application logs
   C. Security logs
   D. Social media monitoring logs

5. A multinational company detects unusually large amounts of outgoing traffic from an internal workstation to an unknown external IP address. The incident response team wants to determine whether sensitive company data is being exfiltrated through the network. Which source of incident data would provide the MOST relevant information?
   A. Physical attendance logs
   B. Printed audit reports stored in cabinets
   C. Network logs showing communication between systems
   D. Employee salary records

6. During an internal audit, a cybersecurity consultant discovers that system event logs are stored in unsecured folders where any employee can modify or delete them. The consultant warns management that this practice could seriously affect future digital investigations. Which requirement of event log storage is being violated?
   A. Time synchronization
   B. Regular backup of logs
   C. Protection from unauthorized modification
   D. Correlation of events

7. A Security Operations Centre (SOC) analyst is investigating suspicious login attempts across multiple servers. However, the analyst realizes that different systems show inconsistent timestamps because some devices are using different time zones and inaccurate clock settings. Which event log storage practice would BEST solve this issue?
   A. Event correlation
   B. Time synchronization using a centralized time source
   C. Disabling logs on unnecessary systems
   D. Reducing the number of devices connected to the network

8. A cybersecurity analyst is reviewing logs from several systems and notices multiple failed logins attempts from the same IP address followed by unusual file access activities on a company server. After combining these related events, the analyst suspects that an attacker may have successfully compromised user credentials. Which event log processing activity is MOST likely being applied?
   A. Data backup
   B. Correlation of events
   C. Password rotation
   D. Software patch deployment

9. A large enterprise uses a Security Information and Event Management (SIEM) platform to automatically collect logs from firewalls, antivirus systems, and servers. The platform immediately alerts administrators whenever suspicious malware-related activities are detected. Which concept BEST describes this approach?
   A. Manual forensic examination
   B. Event normalization
   C. Automation in log processing
   D. Incident eradication

10. A company's cybersecurity team receives reports that several employees suddenly cannot access important files stored on a shared server. At the same time, the incident response team notices files being renamed with unusual extensions and ransom notes appearing in multiple folders. Based on these observations, which of the following BEST represents indicators or signs of a cybersecurity incident?
    A. Employees requesting annual leave at the same time
    B. Unexpected file encryption, ransom notes, and restricted access to files
    C. Routine operating system updates occurring overnight
    D. Employees changing desktop wallpapers frequently

11. During an investigation, a cybersecurity analyst attempts to identify the possible attack vector used by attackers after discovering malicious software on an employee's workstation. Email logs reveal that the employee recently opened an attachment from an unknown sender disguised as an invoice document. Which attack vector was MOST likely used in this incident?
    A. Insider sabotage
    B. Distributed Denial-of-Service (DDoS) attack
    C. Phishing email attachment
    D. Hardware failure

12. A cybersecurity team is overwhelmed by thousands of daily log entries and decides to apply data analytics techniques to identify suspicious patterns more efficiently. The team discovers repeated failed login attempts followed by successful access from the same source IP. What is the PRIMARY benefit of using data analytics in incident analysis?
    A. Eliminating the need for cybersecurity staff entirely
    B. Detecting suspicious patterns and improving investigation efficiency
    C. Replacing all network devices automatically
    D. Preventing organizations from collecting future logs

13. An organization experiences two cybersecurity incidents simultaneously. The first incident involves a minor website display error affecting a few users, while the second incident involves unauthorized access to customer financial information. Due to limited resources, management must decide which incident to handle first. Which factor should MOST influence incident prioritisation?
    A. The number of employees currently on leave
    B. The severity and potential business impact of the incident
    C. Which department complains the loudest
    D. The age of the affected computer systems

14. A hospital network detects ransomware spreading rapidly across several departments. The incident response team decides to immediately disconnect infected systems from the network to prevent additional devices from becoming compromised while further investigation takes place. Which incident handling activity is being applied?
    A. Recovery
    B. Post-incident activity
    C. Containment
    D. Incident prevention

15. During a cybersecurity investigation, a forensic investigator discovers suspicious files stored on a compromised server. To ensure the files can later be presented as reliable digital evidence, the investigator carefully documents collection procedures, preserves file integrity, and limits access to authorized personnel only. What is the PRIMARY purpose of proper evidence gathering and handling?
    A. To speed up internet performance during investigations
    B. To ensure evidence remains trustworthy and admissible during investigations
    C. To permanently delete all suspicious files immediately
    D. To prevent employees from reporting future incidents

16. Following a malware infection, a company removes malicious files, patches vulnerable systems, and resets compromised administrator credentials. The IT department then restores critical services using verified clean backups and closely monitors systems for abnormal behaviour. Which sequence of incident response activities is MOST accurately represented?
    A. Detection → Preparation → Prevention
    B. Notification → Monitoring → Prevention
    C. Eradication → Recovery
    D. Event storage → Log normalization

17. A cybersecurity team discovers that a company server was compromised due to an unpatched vulnerability. Before reconnecting the server to the production environment, the team applies security updates, scans for remaining malicious activity, and verifies system functionality. Why is this step important during recovery?
    A. To ensure systems are safely restored without reintroducing threats
    B. To permanently disconnect the server from the organization
    C. To avoid documenting the incident for management review
    D. To prevent users from accessing systems indefinitely

18. After successfully responding to a phishing incident, a company organizes a meeting involving technical staff, management, and incident responders to discuss what happened, identify weaknesses, and improve response strategies for future incidents. Which post-incident activity is being performed?
    A. Threat eradication
    B. Event normalization
    C. Lessons learned session
    D. Malware deployment testing

19. A financial institution decides to retain all incident-related logs and digital evidence for several years, even after incidents have been resolved. Senior management explains that some attacks may only be discovered much later or may require legal investigation. Which post-incident activity BEST supports this decision?
    A. Evidence retention
    B. Event filtering
    C. Log normalization
    D. Network segmentation

20. A manufacturing company experienced a cyberattack caused by delayed incident reporting and poor communication among IT staff. As a result, management introduces a formal incident handling checklist with reporting procedures, escalation paths, and communication guidelines. What is the MOST important benefit of implementing an incident handling checklist?
    A. It guarantees that cyberattacks will never happen again
    B. It ensures consistent, organized, and efficient incident response activities
    C. It removes the need for cybersecurity professionals
    D. It prevents organizations from using digital evidence in investigations

21. A security analyst needs to contain a malware outbreak on a critical production server that runs the company's main website. The analyst can choose between a "fast isolation" strategy (pulling the network cable) or a "delayed isolation" strategy (waiting to harvest volatile memory data first). What primary factor should guide this containment decision?
    A. The brand and age of the server hardware being used
    B. The trade-off between immediate damage control and the need to gather forensic evidence
    C. Whether the security analyst is scheduled to work the next shift
    D. The total storage capacity of the company's offsite backup drives

22. While collecting evidence from a compromised laptop, a digital forensics investigator creates an exact, bit-by-bit copy of the hard drive and calculates a unique cryptographic hash value (like SHA-256) for both the original drive and the copy. Why is calculating this hash value necessary?
    A. To compress the file size so the evidence is easier to transfer over the internet
    B. To encrypt the data so that nobody, including the court, can read the files
    C. To prove that the data in the forensic copy is identical to the original and has not been altered
    D. To automatically delete any malware hidden in the deep sectors of the drive

23. A company's cloud-hosted email service begins sending thousands of spam messages to external partners because an administrative account was hijacked. The incident response team changes the administrative password and revokes all active login sessions to stop the unauthorized access. Which phase of the incident response lifecycle does this action represent?
    A. Post-Incident Activity
    B. Eradication
    C. Detection and Analysis
    D. Preparation

24. A business continuity manager is setting security policies and needs to establish the Maximum Tolerable Downtime (MTD) and Recovery Time Objective (RTO) for the company's billing system. What do these metrics primarily help the organization determine?
    A. The maximum amount of money the company is willing to pay as a ransom fee
    B. How long the organization can tolerate system downtime and how quickly systems must be restored after a failure
    C. The number of external security consultants needed to fix a network bug
    D. The total number of characters required for a secure administrative password

25. An incident responder discovers that an attacker gained access to an internal network by exploiting a vulnerability that was publicly disclosed only two hours prior, giving the IT team no time to patch it. What is the standard term used to describe this type of security vulnerability?
    A. A phishing exploit
    B. A distributed denial-of-service weakness
    C. A zero-day vulnerability
    D. An insider threat anomaly

26. A security operations team subscribes to a trusted third-party threat intelligence feed that provides updated lists of known malicious IP addresses, domain names, and file signatures used by active hacker groups. How does this data primarily assist the team during an investigation?
    A. It completely automates the recovery of deleted database files
    B. It provides contextual data that helps analysts quickly identify and validate known indicators of compromise (IoCs)
    C. It eliminates the need for the company to use local firewalls or endpoint antivirus software
    D. It automatically drafts the legal paperwork required to prosecute external attackers

27. During an active data breach investigation, a security manager ensures that every person who handles, transfers, or analyzes a piece of digital evidence signs a tracking document detailing the exact date, time, and reason for possession. What is this document called?
    A. A business impact analysis
    B. An incident handling playbook
    C. A chain of custody record
    D. A vulnerability scan report

28. A Software-as-a-Service (SaaS) provider experiences a system breach that exposes data belonging to several corporate clients. Based on standard incident reporting obligations, the SaaS provider notifies the affected client organizations. Who is generally responsible for notifying affected end-users and relevant regulatory bodies, depending on privacy laws and service agreements?
    A. The local internet service provider that routes data to the cloud servers
    B. The hardware manufacturer that built the physical servers used by the SaaS provider
    C. The impacted client organizations acting as data controllers
    D. The individual employees who first noticed that the cloud service was slow

29. A large retail firm wants to verify how effectively its incident response team handles a high-stress corporate espionage scenario. They hire an external group to simulate attackers while the internal security staff defends the network. After the exercise, both teams collaborate to review findings and improve defences. What is this exercise called?
    A. A code regression review
    B. A purple-team simulation exercise
    C. A passive vulnerability baseline assessment
    D. A static configuration desk audit

30. Following a major database breach, an organization establishes a "lessons learned" task force. The executive team insists that the final report must include an analysis of why the incident happened, how the response team performed, and structural recommendations for the company's future security architecture. What is the primary long-term goal of this report?
    A. To find and punish individual employees who made mistakes during the crisis
    B. To justify lowering the overall budget allocated to information technology operations
    C. To continuously improve the organization's security posture and prevent similar failures
    D. To satisfy public curiosity by publishing confidential network maps online

SECTION B (50 marks)

INSTRUCTION: Answer all questions. Please use the answer booklet provided.

Case Study: Big Data, AI, and Digital Rights.

BioAegis Insurance leverages a cloud-based Big Data analytics platform containing the historical, sensitive medical and biometric data of 5 million policyholders. To optimize claims processing, BioAegis feeds this Big Data into an internal generative AI model called *DeepTrust*, which predicts health risk profiles. Employees access the platform and the AI interface via a Single Sign-On (SSO) portal at bioaegis-analytics.com.

The Incident:

On a Wednesday morning, the Data Privacy Officer (DPO) discovers that a large 50-gigabyte database export containing AI-generated policyholder health-risk profiles was accessed and downloaded from an unusual external IP address using valid administrative credentials.

An investigation by the Incident Response Team (IRT) reveals the following sequence of events:

- **Phase 1 (The Trigger):** A senior data scientist received a spear-phishing email containing a link to a **typosquatting domain**: bioaegis-analytrics. Believing it was a system update notice, the scientist logged into the look-alike page, unknowingly surrendering their administrative corporate SSO credentials.
- **Phase 2 (The Abuse of Big Data & AI):** The threat actor used the stolen credentials to log into the legitimate Big Data repository. Instead of downloading raw files, the actor used the administrative account to query the *DeepTrust* AI model. They ran automated prompts to consolidate, extract, and exfiltrate millions of synthesized customer health risk profiles.
- **Phase 3 (The Digital Rights Crisis):** The threat actor published a snippet of the stolen AI-generated data on a public forum. They threatened to sell the entire dataset to the highest bidder unless a ransom is paid, directly violating the **Digital Rights** (privacy, data protection, and automated decision-making transparency) of millions of citizens.

(a) Evaluate the technical flaws and exploitation mechanisms involved in the incident.

(i) Identify and explain **TWO (2)** attack concepts that were used to deceive the engineer.

(ii) Explain how the internal AI model was leveraged to maximize the efficiency of the data theft.

(15 marks)

(b) Discuss whether the digital rights of citizens were compromised by the exposure of AI-generated health profiles rather than raw files. Your discussion should include:

(i) Explaining at least **THREE (3) distinct Digital Rights** or regulatory implications that are violated by the exposure of predictive AI profiling data.

(6 marks)

(ii) Explaining at least **THREE (3) compliance obligations** triggered immediately following the discovery.

(6 marks)

(iii) Providing an overall evaluation of organization's liability.

(2 marks)

(c) Suggest **THREE (3) technical remediation** actions to immediately contain this incident, and **THREE (3) advanced controls** to prevent future automated AI data scraping.

(21 Marks)

END OF QUESTIONS