DUMPSARENA

EC Council Certified Incident Handler (ECIH v3)

ECCouncil 212-89

Version Demo

Total Demo Questions: 50

Total Premium Questions: 509

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Incident Handling and Response	131
Topic 2, Incident Handling and Response Process	90
Topic 3, Forensic Readiness and First Response	98
Topic 4, Handling and Responding to Malware Incidents	60
Topic 5, Handling and Responding to Email Security Incidents	42
Topic 6, Handling and Responding to Web Application Security Incidents	34
Topic 7, Handling and Responding to Insider Threats	49
Topic 8, Mix Questions	5
Total	509

QUESTION NO: 1

The state of incident response preparedness that enables an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation is called:

A. Computer Forensics

B. Digital Forensic Analysis

C. Forensic Readiness

D. Digital Forensic Policy

ANSWER: C

Explanation:

Forensic Readiness is correct because it describes an organization's ability to prepare for, identify, preserve, collect, and use digital evidence efficiently before a specific incident occurs. Its purpose is to ensure that potentially relevant evidence is available, reliable, and handled in a way that supports internal investigations, incident response, legal requirements, and possible proceedings. By establishing appropriate logging, time synchronization, evidence-retention procedures, chain-of-custody practices, responsibilities, and technical collection capabilities in advance, an organization reduces the time, disruption, and expense involved when an investigation is required.

This directly matches the recognized definition of forensic readiness: maximizing the use of digital evidence while minimizing the cost of an investigation. It is therefore an incident-response preparedness state rather than merely the technical activity of examining evidence after an event. The UK National Police Chiefs' Council's good-practice guide describes forensic readiness as preparation to maximize the potential use of digital evidence while minimizing investigation costs. NIST also emphasizes that organizations should establish policies and procedures for collecting and preserving digital evidence as part of incident-handling capability. See the Digital Forensics Good Practice Guide and NIST SP 800-61 Rev. 2.

QUESTION NO: 2

In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:

A. Honey Pots

B. Relays

C. Zombies

D. Handlers

ANSWER: C

Explanation:

In a distributed denial-of-service attack, the compromised computers or devices that carry out the attacker's commands are called **zombies**. Each zombie is a system that has been infected with malicious software or otherwise brought under the attacker's control, often without its legitimate owner's knowledge. A collection of these compromised systems is commonly known as a botnet. The attacker can instruct many zombies to send traffic, connection requests, or other resource-consuming activity to the same victim at the same time. This distributed source set can overwhelm available bandwidth, processing capacity, or connection tables and thereby disrupt legitimate access to the targeted service. The term accurately describes the affected hosts because they operate under remote command rather than for their owners' intended purposes. DDoS incident response therefore commonly includes identifying coordinated traffic patterns, filtering malicious sources where feasible, and coordinating with network providers and affected device owners to reduce botnet-driven traffic. The U.S. Cybersecurity and Infrastructure Security Agency describes DDoS attacks as attempts to make systems unavailable by overwhelming them with traffic from multiple sources, while NIST's glossary defines a botnet as a collection of compromised computers connected to a network. See CISA's overview of denial-of-service attacks and the NIST botnet glossary entry.

QUESTION NO: 3

Which of the following processes is referred to as an approach to respond to the

security incidents that occurred in an organization and enables the response team by

ensuring that they know exactly what process to follow in case of security incidents?

A. Risk assessment

B. Incident response orchestration

C. Vulnerability management

D. Threat assessment

ANSWER: B

Explanation:

Incident response orchestration is the correct answer because it coordinates people, processes, and security technologies into a consistent, repeatable workflow for handling security incidents. Its central purpose is to ensure that responders know what actions to take, in what sequence, and with which tools when an alert is validated as an incident. Orchestration can connect telemetry, case-management systems, endpoint tools, identity systems, and threat-intelligence sources so that investigation and containment steps are performed according to predefined procedures. Where appropriate, it can also automate routine actions, while retaining analyst approval for higher-impact decisions.

This structured approach supports timely and consistent incident handling by operationalizing documented playbooks. It helps a response team collect relevant evidence, assign ownership, coordinate communications, contain affected assets, eradicate the cause, recover services, and record lessons learned. These outcomes align with the incident-response lifecycle described in NIST guidance, which emphasizes preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. EC-Council's Certified Incident Handler program likewise focuses on planning and conducting incident-response processes and managing incidents effectively. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and EC-Council Certified Incident Handler.

QUESTION NO: 4

Which of the following is a characteristic of adware?

A. Gathering information

B. Displaying popups

C. Intimidating users

D. Replicating

ANSWER: B

Explanation:

Displaying popups is a defining characteristic of adware. Adware is software that automatically presents advertising material to a user, commonly through pop-up windows, injected advertisements in browsers, banners, redirects, or notifications. While some ad-supported software may be installed with user consent, malicious or potentially unwanted adware often displays ads excessively, interferes with normal browser behavior, and may be difficult to remove. From an incident-handling perspective, an unexpected surge in pop-ups, browser redirects, altered search results, or advertisements appearing outside the expected website context are useful indicators that a system may be affected by adware. These symptoms should prompt responders to identify suspicious browser extensions and recently installed applications, review persistence mechanisms, and perform approved endpoint scanning and remediation. The U.S. Federal Trade Commission describes adware as software that displays advertisements and may be bundled with other programs, while Microsoft identifies unwanted advertising and pop-up behavior as common effects of potentially unwanted applications. See the Federal Trade Commission malware guidance and Microsoft criteria for potentially unwanted applications.

QUESTION NO: 5

DeltaCorp, a global e-commerce company, received an email sent to the financial department claiming to be from the CEO, requesting an urgent transfer of funds. To determine the legitimacy of this potentially deceptive email, which of the following should be the primary focus of the investigation?

A. Inspect the email headers for spoofing or sender IP irregularities.

B. Contact the vendor mentioned in the email.

C. Review past emails for similar language.

D. Scan the email server for malware.

ANSWER: A

Explanation:

Inspect the email headers for spoofing or sender IP irregularities. Header analysis provides the most direct forensic evidence for assessing whether a purported CEO email actually originated through authorized infrastructure. Investigators should preserve the message in its original form and examine the full headers, particularly the chain of `Received` fields, the envelope sender or `Return-Path`, the visible `From` address, reply-to address, and message identifiers. This information can reveal routing anomalies, mismatches between claimed and actual sending domains, unexpected originating IP addresses, and signs that an external system relayed the message.

Authentication results in the headers are especially valuable. SPF indicates whether the sending IP was authorized by the envelope-sender domain, DKIM validates whether signed message content was altered and identifies the signing domain, and DMARC shows how domain-alignment and authentication checks were evaluated. These results, combined with the routing trail and organizational knowledge of the CEO's normal email systems, support a defensible conclusion about impersonation or spoofing. This approach aligns with email-security best practices because it relies on technical artifacts retained with the message rather than only its wording or business context. For detailed header fields and authentication analysis, see Google Workspace: Trace an email with its full headers and RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

QUESTION NO: 6

Which one of the following is the correct sequence of flow of the stages in an incident response:

A. Containment - Identification - Preparation - Recovery - Follow-up - Eradication

B. Preparation - Identification - Containment - Eradication - Recovery - Follow-up

C. Eradication - Containment - Identification - Preparation - Recovery - Follow-up

D. Identification - Preparation - Containment - Recovery - Follow-up - Eradication

ANSWER: B

Explanation:

The correct incident-response lifecycle sequence is **Preparation - Identification - Containment - Eradication - Recovery - Follow-up**. Preparation occurs before an incident and establishes the people, procedures, tools, communication plans, baselines, and training needed to respond effectively. Identification then involves detecting, validating, and analyzing a suspected security event to determine whether it is an incident and to establish its scope and impact. Once confirmed, containment limits the incident's spread and protects systems and evidence while the response team plans the next steps. Eradication removes the underlying cause, such as malicious files, compromised accounts, persistence mechanisms, or exploited vulnerabilities. Recovery safely returns affected systems and business services to normal operation, with appropriate validation and monitoring to ensure the threat does not reappear. Finally, follow-up, often called post-incident activity or lessons learned, documents findings, assesses the response, and drives improvements to controls, playbooks, and organizational readiness. This lifecycle aligns with the incident-handling process described by NIST and is consistent with the structured incident-response approach tested in EC-Council incident-handling training. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and EC-Council Certified Incident Handler (E|CIH).

QUESTION NO: 7 - (SIMULATION)

A global retail enterprise operating across multiple e-commerce platforms and physical locations has recently been targeted by a well-orchestrated cyberattack that disrupted transaction processing systems and led to a temporary shutdown of online services. Following the incident, customer confidence dropped, and the board demanded immediate corrective and preventive measures to strengthen cybersecurity resilience. The Chief Information Security Officer (CISO) directed the incident response team to establish a forward-looking approach that not only mitigates such incidents but also ensures that all stakeholders are trained in advance. This includes defining clear roles and responsibilities, creating and training a dedicated response team, conducting simulation exercises, reviewing existing IR tools, auditing organizational assets, and developing a comprehensive set of policies and playbooks. Which phase of the IH&R process should the organization focus on to achieve this?

ANSWER: See the explanation for the answer

Explanation:

Correct phase: Preparation.

The organization should focus on the **Preparation** phase of the Incident Handling and Response (IH&R) process. This proactive phase occurs before another incident and is intended to ensure the organization is ready to respond effectively.

Define incident-response roles, responsibilities, and escalation procedures.
Establish and train a dedicated incident response team (IRT/CSIRT).
Conduct tabletop exercises and incident-response simulations.
Review, acquire, and maintain incident response tools.
Identify and audit organizational assets and critical systems.
Create, update, and test incident-response policies, procedures, and playbooks.
Provide security awareness and incident-response training to relevant stakeholders.

These activities directly match the scenario's requirement for advance planning, readiness, training, and preventive resilience.

QUESTION NO: 8

Which test is conducted to determine the incident recovery procedures effectiveness?

A. Live walk-throughs of procedures

B. Scenario testing

C. Department-level test

D. Facility-level test

ANSWER: A

Explanation:

Live walk-throughs of procedures are conducted to validate the practical effectiveness of incident recovery procedures. This type of exercise takes the documented recovery process and steps through its execution in a realistic, operational manner. Personnel responsible for recovery perform or demonstrate their assigned activities, such as activating recovery resources, restoring systems or data, validating service availability, coordinating communications, and documenting results. Observing the process in action provides evidence of whether the procedure can be followed as written, whether responsibilities are clear, whether required resources are available, and whether recovery objectives can be achieved within expected time frames.

This validation is essential because a recovery plan is only useful when the organization can execute it under incident conditions. The exercise also produces actionable findings that can be used to update procedures, contact information, technical runbooks, dependencies, and training. NIST guidance emphasizes testing, training, and exercises as necessary activities for verifying contingency capabilities and maintaining recovery readiness. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 9

Noah, a physical security officer, reviewed entry logs after a breach was reported in the data center. Surveillance showed a contract worker accessing restricted areas using another employee's badge. The access control system lacked biometric verification. Which physical security control could have best prevented this incident?

A. Scheduled patch management

B. Dual authentication

C. Role-based firewall segmentation

D. Encrypted file systems

ANSWER: B

Explanation:

Dual authentication is the appropriate physical security control because it requires a person seeking entry to present more than one independent form of authentication. In this situation, the employee badge establishes possession of an authorized credential, while biometric verification establishes that the person presenting that credential is its legitimate holder. Requiring both a badge and a fingerprint, iris scan, or comparable biometric would have prevented a contract worker from successfully using a borrowed, stolen, or shared badge to enter a restricted data-center area.

This control also improves attribution and incident-handling readiness. Physical access records become more reliable because an entry event is tied not merely to a transferable card, but to an individual whose biometric characteristic was verified at the point of entry. That stronger identity assurance supports investigation, containment, and evidence review after a physical-security event. NIST describes personal identity verification systems as using credentials and authentication mechanisms to establish identity and control facility access, including biometric capabilities where required. See NIST FIPS 201-3. NIST's guidance on electronic physical access-control systems further addresses identity authentication and access-control requirements for facilities: NIST SP 800-116 Revision 1.

QUESTION NO: 10

During monitoring, a security analyst observes several failed login attempts from an external IP address. The analyst has not yet determined whether the activity violates the organization's security policy. How should this activity be classified?

A. Event

B. Incident

C. Vulnerability

D. Threat

ANSWER: A

Explanation:

Event is correct because an event is any observable occurrence in a system, application, network, or service. Failed authentication attempts may be benign, caused by user error, or may represent reconnaissance or an attempted compromise. The activity becomes an incident only after analysis determines that it has violated, or imminently threatens to violate, security policies or controls.

Incident handlers should collect and correlate relevant authentication records, source information, affected accounts, and the frequency of attempts before deciding whether escalation or containment is necessary. NIST distinguishes security events from incidents during detection and analysis activities. See NIST SP 800-61 Rev. 3.

QUESTION NO: 11

Tibson works as an incident responder for MNC based in Singapore. He is investigating a web application security incident recently faced by the company. The attack is performed on a MS SQL Server hosted by the company. In the detection and analysis phase, he used regular expressions to analyze and detect SQL meta-characters that led to SQL injection attack.

Identify the regular expression used by Tibson to detect SQL injection attack on MS SQL Server.

A. /exec(\s|\+)+(s|x)p\w+/ix

B. ((\.\.\\)|(\.\.\/))

C. ((\.|%2E)(\.|%2E)(\/|%2F|\\|%5C))

D. ((\%3C)|<)((\%2F)|\/)*(script)((\%3E)|>)

ANSWER: A

Explanation:

`/exec(\s|\+)+(s|x)p\w+/ix` is the appropriate regular expression for identifying a common Microsoft SQL Server injection pattern involving execution of stored procedures or extended stored procedures. It searches for the `exec` keyword, followed by one or more whitespace characters or plus signs. Including plus signs is important because attackers may use string concatenation or simple obfuscation when constructing injected SQL input. The next portion, `(s|x)p\w+`, identifies procedure names beginning with `sp` or `xp`, followed by one or more word characters. These prefixes are significant in SQL Server investigations because system and extended stored procedures are frequently relevant to malicious execution attempts; for example, attackers have historically attempted to invoke extended procedures through injected statements. The `i` modifier makes matching case-insensitive, helping detect variations such as `EXEC` or mixed-case input. This pattern is therefore useful for triaging web-server logs, application logs, WAF events, and captured request parameters for suspicious SQL Server-oriented payloads. Microsoft documents the security implications of extended stored procedures such as `xp_cmdshell` at Microsoft Learn; broader SQL injection detection and prevention guidance is available from OWASP.

QUESTION NO: 12

A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

A. The risk must be urgently mitigated

B. The risk must be transferred immediately

C. The risk is not present at this time

D. The risk is accepted

ANSWER: C

Explanation:

The risk is not present at this time is correct because risk depends on more than the existence of a vulnerability. It also requires a realistic threat event and a feasible means of exploitation that could produce an adverse impact. In this scenario, the weakness exists, but current technology cannot exploit it. Therefore, there is no presently realizable threat path through which the vulnerability can cause harm, so the organization does not have an active risk from that vulnerability at this time.

This conclusion should be time-bound and documented rather than treated as a permanent condition. Technology, attacker capabilities, tools, and research can change; an exploitation method that is infeasible today may become practical later. The incident-handling and risk-management team should retain awareness of the vulnerability, monitor relevant threat

intelligence and technical developments, and reassess the risk when the environment or available attack capabilities change. NIST describes risk as a function of threats, vulnerabilities, likelihood, and impact, supporting the need for a feasible threat/vulnerability path before a current risk is realized. See NIST SP 800-30 Rev. 1 and NIST SP 800-37 Rev. 2.

QUESTION NO: 13

Alice is a disgruntled employee. She decided to acquire critical information from her organization for financial benefit. To acccomplish this, Alice started running a virtual machine on the same physical host as her victim ' s virtual machine and took advantage of shared physical resources (processor cache) to steal data (cryptographic key/plain text secrets) from the victim machine. Identify the type of attack Alice is performing in the above scenario.

A. Side channel attack

B. Service hijacking

C. SQL injection attack

D. Man-in-the-cloud attack

ANSWER: A

Explanation:

Side channel attack is correct because Alice obtains sensitive information by observing effects created by the victim virtual machine's use of a shared hardware resource rather than by directly accessing its files, memory, or credentials. In a multitenant virtualized environment, colocating an attacker-controlled virtual machine with a target VM can make processor-cache behavior observable. Cache timing and contention patterns may reveal information about operations performed by the target, including cryptographic computations. This is commonly described as a cross-VM cache side-channel attack. The relevant "channel" is the indirect information leakage arising from the physical implementation and shared-resource behavior of the platform. Such attacks can expose secrets, including cryptographic keys or plaintext-related information, even where logical isolation between virtual machines is intended to prevent direct access. NIST describes side-channel attacks as attacks that exploit information unintentionally revealed by a system's implementation, and its cloud-computing guidance identifies shared technology and multitenancy as security considerations requiring appropriate isolation and risk management. In incident handling, evidence such as suspicious VM placement, high-resolution timing activity, unusual cache-monitoring behavior, and workloads designed to induce cache contention should therefore be assessed as possible indicators of this attack category. See NIST's side-channel attack definition and NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.

QUESTION NO: 14

Elena, a first responder at a multinational firm, receives multiple reports from employees claiming they were asked to update their payroll information through an email that appears to be from HR. The email includes a URL directing users to a login page identical to the company's intranet but hosted on an unfamiliar domain. Elena immediately informs the IH&R team, preserves the email headers, captures screenshots of the spoofed page, and blocks the domain at the network level. What type of email security incident is Elena handling?

A. DNS cache poisoning

B. Mail storm attack

C. Email spamming

D. Deceptive phishing attack

ANSWER: D

Explanation:

Deceptive phishing attack is the correct classification because the message impersonates a trusted internal business function, HR, and uses a payroll-update pretext to persuade employees to visit a fraudulent credential-collection site. This is

the defining mechanism of phishing: an attacker uses a seemingly legitimate communication and a spoofed or look-alike destination to obtain sensitive information or access. The unfamiliar domain is particularly significant, even though the login page visually resembles the organization's intranet, because it identifies that the authentication page is not under the company's legitimate control.

Elena's response supports this classification and follows sound incident-handling practice. Preserving the full email headers retains technical evidence that can help identify sending infrastructure, routing details, authentication results, and indicators of compromise. Capturing the spoofed page documents the attacker's social-engineering content and credential-harvesting infrastructure. Blocking the malicious domain contains the incident by preventing additional users from reaching the fraudulent site. These artifacts also support threat hunting, user notification, takedown requests, and reporting. CISA describes phishing as the use of deceptive emails or websites to induce users to disclose information or take unsafe actions; its guidance is available at CISA Phishing Guidance. Additional practical detection and response guidance is provided by NCSC phishing guidance.

QUESTION NO: 15

Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user's information and system. These

programs may unleash dangerous programs that may erase the unsuspecting user's disk and send the victim's credit card numbers and passwords to a stranger.

A. Worm

B. Adware

C. Virus

D. Trojan

ANSWER: D

Explanation:

Trojan is correct because a Trojan horse is malware that deliberately presents itself as a legitimate, useful, or harmless application, file, or attachment in order to persuade a user to execute it. Its defining characteristic is deception: the malicious code is concealed behind an apparently trustworthy program rather than openly identifying itself as harmful. After execution, a Trojan can provide an attacker with unauthorized remote access, commonly through backdoor functionality, enabling the attacker to control the host and access data or system resources.

This access can be used to steal sensitive information such as stored credentials, payment-card information, and passwords, as well as to download and run additional malicious payloads. Those payloads may alter or delete files, disable security controls, or otherwise damage the system. Trojans are therefore particularly significant in incident handling because their apparent legitimacy can help them bypass a user's initial suspicion and establish a foothold for broader compromise. The U.S. Cybersecurity and Infrastructure Security Agency describes Trojan malware as malicious software disguised as legitimate software, while NIST's malware guidance recognizes Trojans as a major category of malicious code requiring prevention, detection, and response measures. See CISA guidance on social engineering and phishing and NIST SP 800-83 Rev. 1.

QUESTION NO: 16

Which of the following risk mitigation strategies involves execution of controls to

reduce the risk factor and brings it to an acceptable level or accepts the potential risk

and continues operating the IT system?

A. Risk assumption

B. Risk avoidance

C. Risk planning

D. Risk transference

ANSWER: A

Explanation:

Risk assumption is the appropriate strategy because it represents the deliberate decision to continue operating a system while accepting the residual risk that remains after reasonable safeguards are applied. In practice, an organization identifies the risk, implements cost-effective administrative, technical, or physical controls where needed, evaluates the resulting residual risk, and formally accepts that remaining exposure when it falls within the organization's established risk tolerance. This is a business and governance decision: the system's mission value and operational need justify continued use, while management acknowledges accountability for the remaining risk.

This approach does not require risk to be eliminated. Rather, it requires that the risk be understood, documented, monitored, and brought to a level that authorized decision-makers consider acceptable. NIST describes risk acceptance as accepting the potential risk and continuing to operate the information system, and its risk-management guidance emphasizes that risk responses are selected in accordance with organizational risk tolerance. See the NIST glossary definition of risk acceptance and NIST SP 800-39.

QUESTION NO: 17

The sign of incident that may happen in the future is called:

A. A Precursor

B. An Indication

C. A Proactive

D. A Reactive

ANSWER: A

Explanation:

A Precursor is correct because incident-handling terminology uses "precursor" to describe a sign that an incident may occur in the future. Precursors are observable conditions or events that can provide advance warning, allowing an incident response team to investigate, increase monitoring, and apply preventive or containment measures before a security event fully develops. For example, public disclosure of a vulnerability affecting an organization's deployed software, or reconnaissance activity against systems, can serve as a precursor because either condition may precede exploitation or another incident. This concept is central to proactive incident detection and preparation: recognizing precursor activity helps the organization reduce exposure and respond earlier, rather than waiting for confirmed harm. NIST's Computer Security Incident Handling Guide distinguishes incident precursors from indicators and defines a precursor as a sign that an incident may occur in the future. EC-Council incident-handling training follows this widely used incident-response terminology when discussing detection and analysis. See the NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and NIST's published PDF of SP 800-61 Rev. 2.

QUESTION NO: 18

An estimation of the expected losses after an incident helps organization in prioritizing and formulating their incident response. The cost of an incident can be categorized as a tangible and intangible cost. Identify the tangible cost associated with virus outbreak?

A. Loss of goodwill

B. Damage to corporate reputation

C. Psychological damage

D. Lost productivity damage

ANSWER: D

Explanation:

Lost productivity damage is a tangible cost because a virus outbreak can directly prevent employees, systems, and business processes from performing productive work. For example, personnel may be unable to access endpoints or applications while malware containment, eradication, restoration, patching, and validation are underway. The organization can estimate this loss using measurable inputs such as affected staff hours, employee labor rates, system downtime, delayed transaction volume, missed operational output, and overtime required for recovery. This produces a quantifiable financial impact that can be included in incident-impact estimates and used to prioritize response actions.

Incident handlers should document the scope and duration of affected services, identify the business functions dependent on those services, and work with business owners to calculate the operational cost of unavailable or degraded systems. This supports evidence-based escalation and recovery decisions. NIST's incident-handling guidance emphasizes analyzing incident impact and prioritizing handling activities according to the effect on organizational operations. CISA also describes malware as a threat that can disrupt systems and operations, making operational downtime and lost work a practical, measurable consequence of an outbreak. See NIST SP 800-61 Rev. 2 and CISA Malware guidance.

QUESTION NO: 19

Finn is working in the eradication phase, wherein he is eliminating the root cause of an incident that occurred in the Windows operating system installed in a system. He ran a tool that can detect missing security patches and install the latest patches on the system and networks. Which of the following tools did he use to detect the missing security patches?

A. Microsoft Cloud App Security

B. Offico360 Advanced Throat Protection

C. Microsoft Advanced Threat Analytics

D. Microsoft Baseline Security Analyzer

ANSWER: D

Explanation:

Microsoft Baseline Security Analyzer is the correct tool because it was designed by Microsoft to assess the security configuration of Windows computers and identify missing security updates. In an incident-eradication workflow, identifying unpatched vulnerabilities is essential: an omitted update may be the root cause that enabled compromise, and applying the relevant updates helps remove that exposure before the system is returned to normal operation. MBSA evaluates Windows update status and selected security configuration settings, then produces a report that administrators can use to prioritize remediation. Its update-assessment capability historically relied on the same Microsoft security-update detection technologies used for update deployment and management, enabling it to determine which applicable security updates were absent on scanned hosts. This makes it directly aligned with the scenario's need to find missing patches across Windows systems or a network. Although MBSA is a legacy product and Microsoft has retired it, it remains the tool described in this exam-style question. For modern environments, Microsoft recommends supported update-management and vulnerability-management services, but the underlying incident-handling practice remains the same: validate patch status, remediate the identified gap, and confirm that the vulnerable condition is no longer present. See Microsoft's Windows security baselines documentation and Windows Update management guidance.

QUESTION NO: 20

Eric works as a system administrator at ABC organization and previously granted several users with access privileges to the organizations systems with unlimited permissions. These privileged users could prospectively misuse their rights unintentionally, maliciously, or could be deceived by attackers that could trick them to perform malicious activities. Which of the following guidelines would help incident handlers eradicate insider attacks by privileged users?

A. Do not allow administrators to use unique accounts during the installation process

B. Do not enable default administrative accounts to ensure accountability

C. Do not control the access to administrator ano privileged users

D. Do not use encryption methods to prevent, administrators and privileged users from accessing backup tapes and sensitive information

ANSWER: B

Explanation:

Do not enable default administrative accounts to ensure accountability is the appropriate guideline because shared, built-in, or default administrator identities weaken attribution. When a default account is used, multiple people may be able to perform sensitive actions under the same identity, making it difficult for incident handlers to determine who performed an action, whether the activity was authorized, and whether credentials were abused. Disabling default administrative accounts where feasible, or tightly controlling and renaming them when they must exist, supports use of distinct, individually assigned privileged accounts. This provides reliable audit trails that link administrative activity to a specific person and makes investigation, containment, and remediation of suspected insider misuse more effective.

This practice should be implemented as part of privileged-access management: grant administrative permissions only when needed, require strong authentication, log privileged actions, and regularly review account status and access assignments. NIST Special Publication 800-53 identifies account management and auditing controls as foundational safeguards for controlling privileged access and maintaining accountability. NIST's guidance on digital identity also emphasizes unique, managed identities and authentication assurance. See NIST SP 800-53 Rev. 5 and NIST SP 800-63B.

QUESTION NO: 21

TechStream, a rising tech start-up, developed an AI-powered chatbot for its clients' websites. Shortly after deployment, users reported receiving malicious links and phishing messages from the chatbot. Preliminary investigation traced the issue to an attacker exploiting the chatbot's AI training module. Which of the following steps would be the most efficient in addressing this vulnerability?

A. Introducing CAPTCHA challenges before users can interact with the chatbot.

B. Implementing strict input validation for any data fed to the chatbot.

C. Disabling the chatbot until a complete security review is done.

D. Limiting the chatbot's ability to share links or external content.

ANSWER: B

Explanation:

Implementing strict input validation for any data fed to the chatbot is the most efficient corrective action because the incident originates in the AI training module's handling of attacker-controlled content. Training, fine-tuning, retrieval, feedback, and other ingestion pipelines are trust boundaries: unvalidated data can introduce malicious instructions, poisoned examples, unsafe links, or content that influences later chatbot responses. Strong validation should enforce expected schemas and data types, sanitize and normalize text, reject or quarantine suspicious URLs and phishing indicators, verify data provenance, and require review or approval before untrusted material enters a production training corpus. This directly reduces the opportunity for data poisoning and indirect prompt-injection-style attacks while allowing the service to continue operating under controlled conditions. It should be paired operationally with logging, monitoring, versioning of training data, and the ability to roll back to a known-good model or dataset. OWASP identifies training-data poisoning and insufficient validation as important risks in machine-learning systems, and its guidance emphasizes validating, sanitizing, and controlling data inputs throughout the ML lifecycle. See the OWASP Machine Learning Security Top Ten and the OWASP guidance on training data poisoning.

QUESTION NO: 22

A multinational law firm suffered a sophisticated malware attack that encrypted critical legal documents. During recovery, there is concern that some archived backups may already be compromised. Which recovery-focused action should the organization prioritize to ensure safe restoration?

A. Perform comprehensive scans of all backup data using updated antivirus and heuristics.

B. Deploy host-based firewalls and restrict outbound traffic.

C. Restore services from live file shares synchronized with other offices.

D. Wipe all endpoints completely before restoring files.

ANSWER: A

Explanation:

Perform comprehensive scans of all backup data using updated antivirus and heuristics is the priority because recovery must restore systems and information to a known-good, trustworthy state without reintroducing the malware that caused the incident. When archived backups might have been exposed before the attack was detected, they may contain dormant malware, malicious scripts, altered files, or persistence mechanisms. Scanning backup content with current detection signatures improves identification of known threats, while heuristic and behavior-oriented analysis can help identify suspicious or previously unknown malware characteristics. The organization should validate backup integrity and provenance, scan recovery media in an isolated environment where practical, and restore only data that has passed validation. This approach supports a controlled recovery sequence: preserve clean recovery points, verify that the threat has been eradicated from the restoration environment, and monitor restored assets for signs of recurrence. NIST incident-recovery guidance similarly emphasizes restoring systems from known-clean backups and validating that restored systems operate normally and securely. This directly addresses the central recovery risk: an unvalidated restoration can recreate the compromise and undermine containment and eradication work. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and CISA Ransomware Guide.

QUESTION NO: 23

EduTech University noticed unauthorized access to student records, including academic and financial details. As the semester's examinations approached, there were concerns about potential leaks or manipulations of question papers. In this complex digital scenario, what is the optimal step for the first responder?

A. Capture logs from the academic servers, focusing on recent access and modifications.

B. Collaborate with faculty to develop alternative exam papers as a backup.

C. Isolate the academic systems, ensuring the integrity of upcoming examinations.

D. Notify students and staff, urging them to change their university portal passwords.

ANSWER: C

Explanation:

“Isolate the academic systems, ensuring the integrity of upcoming examinations.” is the appropriate first-responder action because the scenario indicates an active or recent unauthorized-access event involving highly sensitive information and a time-critical risk to examination materials. Immediate, carefully controlled containment limits an intruder’s ability to continue accessing records, exfiltrate question papers, alter academic content, or use compromised systems to move laterally. The isolation should be scoped to affected systems and performed in a manner that retains the systems’ evidentiary value—for example, removing them from normal network access while maintaining the ability to preserve relevant logs, memory, and system state under the incident-response process. This directly protects confidentiality and integrity at the point of greatest operational risk: the imminent examinations. Incident handling guidance treats containment as a central activity for stopping ongoing harm while the organization coordinates forensic collection, eradication, recovery, and communications. NIST describes containment as an incident-response activity used to prevent further damage and spread; see NIST SP 800-61 Rev. 2. EC-Council’s ECIH program likewise emphasizes structured incident handling and response capabilities; see EC-Council Certified Incident Handler.

QUESTION NO: 24

Which of the following is the BEST method to prevent email incidents?

A. Installing antivirus rule updates

B. Disabling HTML in email content fields

C. Web proxy filtering

D. End-user training

ANSWER: D

Explanation:

End-user training is the best method because email incidents frequently depend on a recipient making a decision that bypasses otherwise effective technical controls. Phishing, business email compromise, malicious attachments, credential-harvesting links, and social-engineering messages are designed to persuade users to disclose information, open content, approve requests, or enter credentials on fraudulent sites. Practical, recurring training helps personnel recognize suspicious sender addresses, unexpected attachments, urgent payment requests, credential prompts, and misleading links. It should also teach users how to verify unusual requests through an independent channel and how to promptly report suspected phishing so the incident-response team can contain similar messages across the organization. Training is most effective when reinforced with phishing simulations, clear reporting mechanisms, and role-appropriate examples, making users an active layer of defense rather than passive recipients of email. The U.S. Cybersecurity and Infrastructure Security Agency identifies user awareness and reporting as key phishing-resistance practices, while NIST emphasizes awareness and training as an organizational security-control family. See CISA phishing guidance and NIST SP 800-53 Awareness and Training controls.

QUESTION NO: 25

A global logistics company recently experienced a targeted ransomware attack that began through a deceptive email campaign. The malicious software encrypted critical files on several systems tied to dispatch and finance operations. Fortunately, the organization had deployed an advanced security setup that could swiftly recognize abnormal behaviors, isolate compromised devices, and alert both the technical support desk and the security operations team.

In parallel, system logs were captured and analyzed using integrated threat detection tools, and a detailed file was automatically created with relevant data such as affected assets, user activity, and potential entry points. Security analysts then assessed the case, adapted containment measures based on the affected departments, and continued tracking suspicious activity across the network. Additional countermeasures were executed based on a mix of pre-approved workflows and expert decisions, ensuring the issue was contained without major disruption. Which combination of technologies is MOST likely supporting this workflow?

A. A manual log management tool integrated with a physical ticketing desk for report creation

B. A legacy antivirus solution configured to detect known malware only

C. A cloud storage backup system with no direct link to detection or containment mechanisms

D. A coordinated system combining incident response automation with orchestration capabilities

ANSWER: D

Explanation:

A coordinated system combining incident response automation with orchestration capabilities is correct because the described workflow matches a Security Orchestration, Automation, and Response (SOAR) capability. SOAR connects security tools and operational teams, allowing alerts and telemetry from detection platforms to be enriched with contextual information such as asset details, user activity, and likely attack vectors. It can automatically open and populate an incident case, notify relevant teams, and execute established response playbooks.

In this ransomware scenario, rapid isolation of affected endpoints, cross-team alerting, and centralized case creation reduce the time between detection and containment. Orchestration is especially important because it coordinates actions across endpoint, log-analysis, ticketing, and threat-detection systems rather than treating each tool as an isolated control. Automation supports repeatable, pre-authorized actions, while analyst-driven decisions remain available for department-

specific containment and investigation. This combined human-and-automated response model enables an organization to limit operational disruption while continuing to monitor for related malicious activity.

This aligns with incident-handling practices that emphasize detection, analysis, containment, and coordinated response. See EC-Council's Certified Incident Handler program and NIST's Computer Security Incident Handling Guide.

QUESTION NO: 26

What is the most recent NIST standard for incident response?

A. 800-61r2

B. 800-61r3

C. 800-53r3

D. 800-171r2

ANSWER: B

Explanation:

800-61r3 is the most recent NIST publication specifically addressing incident response. NIST released Special Publication 800-61 Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, in April 2025. It supersedes Revision 2 and updates NIST's incident-response guidance to align with the Cybersecurity Framework 2.0 and modern cybersecurity risk-management practices.

The publication emphasizes integrating incident-response capabilities throughout an organization's cybersecurity risk-management activities, rather than treating response as an isolated sequence of technical steps. It provides recommendations for preparing for incidents, reducing their impact, improving detection and response activities, and using lessons learned to strengthen organizational risk management. This makes 800-61r3 the appropriate current reference for an incident handler seeking the latest NIST guidance on building, operating, and continuously improving an incident-response capability. NIST's official publication page identifies Revision 3 as the current version and provides the final document for use by security and incident-response teams.

References: NIST SP 800-61 Rev. 3 publication page; NIST SP 800-61 Rev. 3 PDF.

QUESTION NO: 27

Which of the following types of digital evidence is temporarily stored in a digital device that requires constant power supply and is deleted if the power supply is interrupted?

A. Slack space

B. Process memory

C. Event logs

D. Swap file

ANSWER: B

Explanation:

Process memory is correct because it is held in volatile random-access memory (RAM), which requires continuous electrical power to preserve its contents. While a computer is operating, process memory can contain highly valuable incident-response evidence, including running processes, loaded modules, active network connections, command-line arguments, authentication material, encryption keys, clipboard contents, and data associated with malware that may never be written to persistent storage. When power is removed, or when the device is shut down or restarted, this volatile information is ordinarily lost. For this reason, responders should consider collecting a memory image early in an investigation, provided doing so is authorized and consistent with the incident-handling plan. Memory acquisition enables subsequent forensic

analysis of the system's live state and can reveal artifacts that are unavailable in disk-based evidence alone. The National Institute of Standards and Technology describes volatile data collection as part of forensic data acquisition and emphasizes collecting data in an appropriate order of volatility. Guidance on preserving and analyzing volatile information is available in NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and the CISA Incident Response resources.

QUESTION NO: 28

A user reports receiving an email that appears to be from the organization's cloud-service provider. The email requests immediate password verification through a link to an unfamiliar domain. Which type of attack does this incident most likely represent?

A. Phishing

B. Shoulder surfing

C. Wardriving

D. Tailgating

ANSWER: A

Explanation:

Phishing is correct because the message impersonates a trusted service and attempts to persuade the recipient to disclose credentials through a deceptive link. Attackers commonly use urgency, familiar branding, and account-related warnings to make a malicious request appear legitimate. The unfamiliar destination domain is an important indicator that the link may lead to a credential-harvesting site.

Incident handlers should preserve the message, including headers and URLs, identify other recipients, block confirmed malicious indicators where appropriate, and reset credentials if users submitted them. CISA provides guidance on recognizing and reporting phishing activity at Recognize and Report Phishing.

QUESTION NO: 29

AlphaTech, a cloud-based storage company, recently suffered data leakage. Investigation revealed an employee sent sensitive client data to a personal email. AlphaTech wants to implement a solution to monitor and prevent such incidents. What should they prioritize?

A. Mandate employees to attend cyber hygiene workshops every month.

B. Implement a Data Loss Prevention (DLP) tool to monitor sensitive data movement.

C. Limit email attachments to SMB for all employees.

D. Block all personal email domains on the company network.

ANSWER: B

Explanation:

Implement a Data Loss Prevention (DLP) tool to monitor sensitive data movement. is the appropriate priority because the incident involves sensitive information leaving an approved business environment through email. DLP provides a technical control that can identify and classify protected content, inspect it while it is being used or transmitted, and apply policy-driven actions such as alerting, requiring justification, encrypting content, or blocking delivery. For this scenario, policies can recognize client records through classifications, labels, patterns, or fingerprints and prevent their transmission to external or personal email recipients.

An effective deployment should begin by defining the sensitive data categories AlphaTech must protect, mapping permitted business flows, and implementing email DLP policies in a monitoring mode before enforcing blocks. Alerts should feed the incident-response process so the security team can investigate activity, preserve relevant evidence, validate whether a

policy exception is needed, and refine detection rules. DLP should also cover other likely outbound paths, including cloud applications, endpoint copying, and web uploads, because insider exfiltration can occur through more than one channel. Microsoft describes how DLP policies detect and protect sensitive items across locations in its Purview DLP overview, and NIST outlines controls for preventing unauthorized information flow in SP 800-53 Rev. 5.

QUESTION NO: 30

Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-profile executives of the company. What type of phishing attack is this?

A. Pharming

B. Whaling

C. Puddle phishing

D. Spear phishing

ANSWER: B

Explanation:

Whaling is the correct classification because it is a highly targeted form of phishing directed at senior, high-profile individuals, such as executives, directors, and other organizational leaders. Attackers choose these recipients because they often have authority to approve payments, access sensitive corporate data, influence employees, or authorize changes to business processes. The scenario specifically identifies that most targets are company executives, which is the defining indicator of a whaling campaign. Such attacks commonly use carefully tailored messages that appear to concern urgent financial, legal, personnel, or business matters, increasing the chance that a busy executive will act before independently verifying the request. Incident handlers should treat this targeting pattern as high risk: an executive compromise can enable business email compromise, credential theft, fraudulent wire transfers, or access to confidential information. CISA describes phishing as the use of deceptive communications to induce recipients to reveal information or take harmful actions, and notes that targeted phishing campaigns can impersonate trusted parties. Guidance on protecting senior personnel from these tailored attacks is available from CISA's Phishing Guidance and the UK National Cyber Security Centre's phishing guidance.

QUESTION NO: 31

Which of the following is NOT one of the Computer Forensic types:

A. USB Forensics

B. Email Forensics

C. Forensic Archaeology

D. Image Forensics

ANSWER: C

Explanation:

Forensic Archaeology is the correct selection because it is a physical-forensic discipline concerned with applying archaeological methods to legal investigations. Its practitioners may locate, document, excavate, and interpret buried or surface evidence, including clandestine graves, human remains, artifacts, and disturbed soil. The discipline's core evidence sources and examination methods are therefore physical and environmental rather than data stored, transmitted, or processed by computer systems.

Computer forensics, also commonly called digital forensics, is concerned with the identification, preservation, collection, examination, analysis, and reporting of digital evidence in a manner that maintains evidentiary integrity. Incident handlers

use these practices to establish what occurred on an endpoint or within a digital environment, reconstruct relevant activity, and support a defensible investigation. NIST describes digital-forensics work as involving data acquisition and examination from digital systems and media, while the National Institute of Justice recognizes forensic archaeology as a distinct forensic-science specialty focused on archaeological recovery and interpretation. These distinct investigative domains make Forensic Archaeology the appropriate answer. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and the National Institute of Justice overview of forensic anthropology and archaeology.

QUESTION NO: 32

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

A. Configuring firewall to default settings

B. Inspecting the process running on the system

C. Browsing particular government websites

D. Sending mails to only group of friends

ANSWER: B

Explanation:

Inspecting the process running on the system is the appropriate activity because active processes provide direct evidence of what a host is executing at the time of investigation. Incident handlers can review process names, paths, parent-child relationships, command-line arguments, associated users, network connections, hashes, and persistence-related behavior to identify suspicious or malicious execution. This information helps distinguish an actually compromised endpoint from unaffected systems and supports an informed containment decision, such as placing the identified host in network isolation while preserving relevant volatile evidence. Process inspection is particularly valuable because many incidents involve malware, unauthorized remote-access tools, scripts, or injected processes that are observable through endpoint telemetry and memory/process analysis. NIST's incident-handling guidance describes analysis as determining the scope and impact of an incident so that containment actions can be selected appropriately. Similarly, CISA recommends isolating affected systems as a containment action after signs of compromise are identified. Reviewing running processes therefore supports both recognition of infected hosts and their safe separation from the broader information system. See NIST SP 800-61 Rev. 2 and CISA ransomware response guidance.

QUESTION NO: 33

Which of the following is not a countermeasure to eradicate inappropriate usage

incidents?

A. Avoid VPN and other secure network channels

B. Register the user activity logs and keep monitoring them regularly

C. Install firewall and IDS/IPS to block services that violate the organization's policy

D. Always store the sensitive data in far located servers and restrict its access

ANSWER: A

Explanation:

Avoid VPN and other secure network channels is the measure that is not a countermeasure for inappropriate-usage incidents. A virtual private network provides an authenticated, encrypted communications channel over an untrusted network. Using such protected channels helps an organization enforce secure remote access and reduces the exposure of credentials, sessions, and sensitive information to interception. Avoiding them would remove a valuable security control rather than contain, eradicate, or prevent policy-violating activity.

Incident handling for inappropriate usage should preserve and strengthen controls that support authorized, accountable access. Secure remote-access technologies can be combined with centralized authentication, authorization rules, logging, and monitoring to identify the user responsible for activity and to apply organizational policy consistently. Encryption in transit is also a foundational protection for sensitive data moving across networks, particularly where remote users or third-party networks are involved. NIST's guidance on remote access emphasizes protecting remote-access communications and controlling access paths, while CISA identifies VPNs as a means of creating encrypted connections for remote users. Therefore, the appropriate response is to use secure network channels under managed policy—not to avoid them. See NIST SP 800-46 Rev. 2 and CISA: Understanding VPNs.

QUESTION NO: 34

In which of the following stages of incident handling and response (IH & R) process do

the incident handlers try to find out the root cause of the incident along with the threat

actors behind the incidents, threat vectors, etc.?

A. Post-incident activities

B. Incident triage

C. Evidence gathering and forensics analysis

D. Incident recording and assignment

ANSWER: C

Explanation:

Evidence gathering and forensics analysis is the correct stage because responders must collect, preserve, and examine relevant digital artifacts to establish what happened and how it happened. This work commonly includes reviewing endpoint and server logs, network telemetry, memory captures, disk images, authentication records, malicious files, and indicators of compromise. Correlating those artifacts enables the team to reconstruct the incident timeline, identify the initial access path and affected assets, determine the techniques and threat vectors used, and develop evidence-based findings regarding the likely root cause and threat-actor activity. Proper forensic handling also protects the integrity and evidentiary value of collected material through documented acquisition, hashing, secure storage, and chain-of-custody practices. These findings directly support informed remediation and recovery decisions, while also producing intelligence that can be used to prevent recurrence. NIST describes incident analysis as examining incident data and determining its scope, impact, and characteristics, and its digital-forensics guidance emphasizes collecting and analyzing data while preserving its integrity. See NIST SP 800-61 Rev. 2 and NIST SP 800-86.

QUESTION NO: 35

A malicious, security-breaking program is disguised as a useful program. Such executable programs, which are installed when a file is opened, allow others to control a user's system. What is this type of program called?

A. Trojan

B. Worm

C. Virus

D. Spyware

ANSWER: A

Explanation:

Trojan is the correct term for malware that presents itself as a legitimate, useful, or desirable program in order to persuade a user to open or install it. The defining characteristic is deception: the program's apparent function conceals its malicious purpose. Once the user executes the disguised file, a Trojan may install a remote-access component or backdoor, enabling

an attacker to control the affected system, run commands, steal data, download additional malware, or monitor activity. This behavior directly matches the scenario's description of an executable installed when a file is opened and subsequently allowing another party to control the user's system. Trojans commonly rely on social engineering and may be delivered through email attachments, software downloads, or files shared through compromised websites. The U.S. Cybersecurity and Infrastructure Security Agency describes Trojan malware as software that appears legitimate but carries out hidden malicious actions after execution. MITRE's ATT&CK knowledge base also documents remote-access software and command-and-control behavior that attackers use after gaining execution on a host. See CISA: Understanding Malware and MITRE ATT&CK: Command and Control.

QUESTION NO: 36

Your company holds a large amount of customer PH. and you want to protect those data from theft or unauthorized modification. Among other actions, you classify and encrypt the data. In this process, which of the following OWASP security risks are you guarding against?

A. Insecure deserialization

B. Security misconfiguration

C. Broken authentication

D. Sensitive data exposure

ANSWER: D

Explanation:

Sensitive data exposure is the applicable OWASP risk because the organization is handling customer protected health information and is applying controls specifically intended to preserve its confidentiality and integrity. Data classification identifies information that requires heightened handling, allowing the organization to consistently apply appropriate protection requirements throughout storage, transmission, processing, retention, and disposal. Encryption then makes protected data unreadable to a party that obtains it without authorization, provided encryption is implemented correctly and the cryptographic keys are properly protected. This substantially reduces the impact of theft of a database, backup, endpoint, or intercepted transmission, because possession of encrypted records alone does not reveal their contents. Encryption and classification also support governance by making it possible to define access, handling, monitoring, and retention controls according to the sensitivity of the information. In the OWASP Top 10 2017 edition, this category was named "Sensitive Data Exposure"; OWASP Top 10 2021 reframed the closely related concern as "Cryptographic Failures," emphasizing failures to protect sensitive data through appropriate cryptography. See the OWASP Top 10 2017 Sensitive Data Exposure page and the OWASP Top 10 2021 Cryptographic Failures page.

QUESTION NO: 37

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

A. An Adware

B. Mail bomb

C. A Virus Hoax

D. Spear Phishing

ANSWER: C

Explanation:

A Virus Hoax is correct. A virus hoax is a false warning, commonly distributed through email or messaging, that claims a dangerous virus is present and pressures recipients to take immediate action. Typical instructions include deleting legitimate files that are alleged to be malicious, forwarding the warning to everyone in the recipient's contacts, or urgently sharing it

with colleagues. The social-engineering element is central: the message uses fear, urgency, and an apparent public-service purpose to cause disruptive actions without an actual malware infection being present.

For an incident handler, identifying a suspected virus hoax requires validating the claimed threat through reliable security-vendor advisories, endpoint telemetry, and organizational incident procedures before users are instructed to delete files or redistribute a warning. Users should be directed to report suspicious messages through established channels rather than forwarding them. CISA describes how malicious actors use social-engineering techniques, including urgent messaging, to manipulate recipients, while the FTC provides guidance on recognizing and handling deceptive messages. See CISA's malware guidance and the FTC guidance on recognizing deceptive messages.

QUESTION NO: 38

An AWS user notices unusual activity in their EC2 instances, including unexpected outbound traffic. When suspecting a security compromise, what is the most effective immediate step to take to contain the incident?

A. Increase logging levels and monitor traffic for anomalies.

B. Terminate all affected EC2 instances.

C. Reboot the affected instances to disrupt unauthorized processes.

D. Snapshot the affected instances for forensic analysis and then isolate them using network ACLs.

ANSWER: D

Explanation:

Snapshot the affected instances for forensic analysis and then isolate them using network ACLs is the strongest immediate containment action because it addresses both essential incident-response priorities: stopping potential attacker communications and preserving evidence for investigation. An Amazon EBS snapshot creates a point-in-time copy of the instance's attached EBS volumes, allowing responders to retain disk artifacts such as malware binaries, persistence mechanisms, logs, command history, and configuration details. Capturing that evidence before making disruptive changes helps maintain a defensible basis for later forensic analysis and recovery decisions.

After evidence capture, restricting the affected workload's network connectivity prevents continued command-and-control traffic, lateral movement, data exfiltration, or other unauthorized outbound activity. In AWS, responders can rapidly apply restrictive security-group rules, adjust network ACLs, or otherwise remove the instance's communication paths according to the environment's architecture. This containment should be coordinated to preserve authorized responder access where needed for live acquisition. AWS incident-response guidance emphasizes isolating affected resources while preserving relevant evidence and collecting forensic data. See the AWS Security Incident Response Guide and the Amazon EBS snapshot documentation.

QUESTION NO: 39

Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?

A. ISO/IEC 27002

B. ISO/IEC 27035

C. PCI DSS

D. RFC 219G

ANSWER: A

Explanation:

ISO/IEC 27002 is correct because it supplies guidance and recommendations for selecting, implementing, and managing information security controls within an information security management system. It is designed for organizations establishing

or improving an ISMS and for personnel responsible for implementing, operating, monitoring, reviewing, and maintaining information-security controls. The standard organizes a comprehensive control set into themes such as organizational, people, physical, and technological controls. Its guidance supports a risk-based approach: an organization identifies its relevant information-security risks and then uses the control guidance to determine and tailor appropriate safeguards. ISO/IEC 27002 therefore complements ISO/IEC 27001, which defines requirements for an ISMS, by providing practical control guidance rather than merely stating management-system requirements. The International Organization for Standardization describes ISO/IEC 27002 as guidance for information-security controls and notes its applicability to organizations of all types and sizes. This makes ISO/IEC 27002 the standard framework directly matching the question's focus on recommendations for organizations that initiate, implement, or maintain ISMSs. See the ISO/IEC 27002:2022 standard page and ISO's ISO/IEC 27001 information-security overview.

QUESTION NO: 40

Bonney's system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware

incident from spreading?

A. Turn off the infected machine

B. Leave it to the network administrators to handle

C. Complaint to police in a formal way regarding the incident

D. Call the legal department in the organization and inform about the incident

ANSWER: A

Explanation:

Turn off the infected machine is the appropriate immediate action in the context of this question because it promptly stops the compromised host from communicating with other systems, services, or attackers. Malware commonly spreads through network shares, remote connections, credential reuse, exploit traffic, and command-and-control communications. Removing power prevents the host from continuing those activities and therefore provides rapid containment when no more targeted isolation procedure is stated. Containment is a priority early in incident handling because it limits the scope of compromise, reduces the chance of additional data loss or service disruption, and gives responders a stable environment in which to assess the incident. Once the system is no longer active, the incident-response team can follow established procedures to preserve available evidence, identify affected assets, determine the malware's persistence and propagation mechanisms, eradicate it, and restore the device safely. NIST's incident-response guidance describes containment as an essential response phase and emphasizes selecting actions that limit damage and prevent further spread. CISA likewise advises organizations to isolate affected systems as part of responding to malware and ransomware incidents. See NIST SP 800-61 Rev. 2 and CISA StopRansomware Guide.

QUESTION NO: 41

Jason, a cybersecurity analyst in the incident response team, begins investigating several complaints from employees who received emails urgently requesting wire transfers to an overseas account. The emails appeared to come from the company's CEO, using a tone of authority and pressure to bypass standard procedures. Upon closer inspection, Jason identifies that the sender ' s email address includes a minor alteration in the domain name—a form of domain spoofing. He examines the email headers, confirms the falsified sender identity, and cross-checks with the actual CEO's activity logs to ensure there was no internal compromise. Immediately, Jason blocks the sender's IP address at the firewall level, alerts the finance department to prevent any unauthorized transactions, and issues a company-wide advisory about the impersonation attempt. What type of phishing is Jason handling?

A. Whaling

B. Mail bombing

C. Credential stuffing

D. Spimming

ANSWER: A

Explanation:

Whaling is the correct classification because this is an executive-impersonation phishing campaign intended to exploit the authority associated with a senior leader. The messages claim to originate from the CEO and use urgency and pressure to induce employees to bypass established financial controls and transfer money to an external account. This type of business email compromise commonly relies on a look-alike or slightly altered sender domain, rather than malware or a generic mass-mailing lure, to make the fraudulent request appear credible at a glance.

The requested wire transfer is especially significant: executive impersonation and payment-redirection requests are core indicators of whaling-style fraud. Jason's validation of the actual CEO's activity helps establish that the message is spoofed rather than sent from a legitimately compromised internal executive account. His immediate containment and notification actions appropriately focus on preventing financial loss, preserving evidence in the email headers, and warning personnel who may receive equivalent requests. The U.S. Cybersecurity and Infrastructure Security Agency describes business email compromise as fraud that often uses impersonation and social engineering to cause unauthorized payments, while the FBI identifies executive impersonation and fraudulent wire-transfer instructions as common BEC patterns. See CISA's Business Email Compromise guidance and the FBI IC3 public service announcement on BEC.

QUESTION NO: 42

After experiencing a large-scale distributed denial-of-service (DDoS) attack that caused service outages, a national telecom provider recovered its web platform. The IH & R team must now implement post-recovery measures to enhance resilience against future DDoS attempts. Which action would be most effective?

A. Remove antivirus to speed up application response

B. Configure a CDN and implement blackhole routing

C. Add guest user accounts for remote diagnostics

D. Increase FTP access for easier maintenance

ANSWER: B

Explanation:

Configure a CDN and implement blackhole routing is the most effective post-recovery action because it directly improves the provider's ability to sustain availability during a future DDoS event. A content delivery network distributes web content and traffic-handling capacity across geographically dispersed edge locations. This reduces pressure on the origin platform, provides scalable capacity for legitimate users, and enables traffic filtering and rate controls closer to where requests enter the network. For a national telecom provider, this distributed architecture is especially valuable because an attack may target multiple services or network regions simultaneously.

Blackhole routing is an upstream network-response capability used when harmful traffic toward a destination must be discarded before it can consume the organization's links or infrastructure. When coordinated with the telecom provider's backbone, transit providers, and established incident-response procedures, it can contain severe volumetric attacks and protect unaffected services. The organization should define activation criteria, authorization, communication paths, monitoring, and rollback procedures so the control is applied deliberately during an incident. Together, CDN-based traffic absorption and upstream blackholing provide layered DDoS resilience aligned with post-incident improvement practices. See CISA guidance on denial-of-service attacks and Cloudflare's explanation of blackhole routing.

QUESTION NO: 43

Jason, a cybersecurity analyst in the incident response team, begins investigating several complaints from employees who received emails urgently requesting wire transfers to an overseas account. The emails appeared to come from the companyâ€™s CEO, using a tone of authority and pressure to bypass standard procedures. Upon closer inspection, Jason identifies that the sender's email address includes a minor alteration in the domain nameâ€”a form of domain spoofing. He

examines the email headers, confirms the falsified sender identity, and cross-checks with the actual CEOâ€™s activity logs to ensure there was no internal compromise. Immediately, Jason blocks the senderâ€™s IP address at the firewall level, alerts the finance department to prevent any unauthorized transactions, and issues a company-wide advisory about the impersonation attempt. What type of phishing is Jason handling?

A. Whaling

B. Mail bombing

C. Credential stuffing

D. Spimming

ANSWER: A

Explanation:

Whaling is the correct classification because the attack exploits the authority, trust, and urgency associated with a senior executive—here, the CEO—to induce employees to make a high-value financial transfer. Whaling is a targeted phishing technique involving executives or executive identities and commonly supports business email compromise-style payment fraud. The altered lookalike domain is especially significant: it enables the attacker to make the sender address resemble a legitimate executive address while avoiding use of the company's actual mail infrastructure. The urgent wire-transfer demand is intended to override ordinary verification and approval processes, a defining social-engineering pattern in executive impersonation scams. Jason's validation of message headers and the real CEO's activity helps establish that the request is fraudulent rather than an authorized internal communication. Alerting finance before a transfer occurs is an essential containment action because payment-diversion attacks can result in immediate and difficult-to-recover losses. CISA describes business email compromise as fraud that uses compromised or spoofed email accounts to request transfers, and it specifically identifies executive impersonation as a common scenario. See CISA's Business Email Compromise guidance and the FBI IC3 public service announcement on BEC.

QUESTION NO: 44

Eric is an incident responder and is working on developing incident-handling plans and procedures. As part of this process, he is performing an analysis on the organizational network to generate a report and develop policies based on the acquired results. Which of the following tools will help him in analyzing his network and the related traffic?

A. Whois

B. Burp Suite

C. FaceNiff

D. Wireshark

ANSWER: D

Explanation:

Wireshark is the appropriate tool because it is a network protocol analyzer designed to capture and inspect traffic traversing an interface. An incident responder can use it to examine packet-level communications, identify the hosts and protocols active on an organizational network, review connection patterns, and investigate suspicious activity such as unusual DNS queries, unexpected outbound connections, or clear-text credentials. Its display filters, protocol dissection, statistics views, and follow-stream capabilities support the detailed traffic analysis needed to establish a network baseline and produce evidence-based incident-handling procedures and policies. Packet captures can also provide useful indicators and context during later incident investigations, helping responders determine what systems communicated, when the communication occurred, and what data was transmitted. Wireshark documentation describes the software as a network protocol analyzer and provides guidance on capturing and analyzing packets; see the Wireshark User's Guide. This use also aligns with NIST incident-response guidance, which emphasizes collecting and analyzing relevant network-event information to support detection, analysis, containment, and recovery activities; see NIST SP 800-61 Rev. 2.

QUESTION NO: 45

Which of the following risk management processes identifies the risks, estimates the impact, and determines sources to recommend proper mitigation measures?

A. Risk assessment

B. Risk assumption

C. Risk mitigation

D. Risk avoidance

ANSWER: A

Explanation:

Risk assessment is correct because it is the structured risk-management activity used to identify potential risks, analyze their sources and relevant threat events, evaluate vulnerabilities and existing controls, and estimate the likely impact on organizational operations, assets, and individuals. Its results give incident-handling and security teams an evidence-based understanding of which conditions could cause harm, how significant that harm could be, and where treatment should be focused. This information is then used to prioritize risks and recommend proportionate safeguards or other treatment measures. NIST describes risk assessment as a process for identifying threats and vulnerabilities, determining likelihood and impact, and informing risk-response decisions. In an incident-handling context, this supports selecting protections and preparedness measures that address the organization's most meaningful exposures before an incident occurs, while also improving the basis for response planning. The assessment is therefore the analytical stage that produces the risk information needed to recommend proper mitigation measures, rather than the implementation of those measures itself. See NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments and NIST Risk Management Framework.

QUESTION NO: 46

Based on the some statistics; what is the typical number one top incident?

A. Phishing

B. Policy violation

C. Un-authorized access

D. Malware

ANSWER: A

Explanation:

Phishing is the best answer because it is consistently one of the most frequently reported and operationally significant incident types. A phishing incident begins when an attacker uses deceptive email, messaging, websites, or other communications to induce a target to disclose credentials, open malicious content, approve a fraudulent transaction, or otherwise take an unsafe action. Incident-handling teams commonly receive phishing reports at high volume and must rapidly triage messages, identify affected users, remove malicious artifacts, reset compromised credentials where appropriate, and assess whether the activity led to account takeover or malware deployment.

This prominence is supported by widely used incident and cybercrime reporting data. The FBI Internet Crime Complaint Center's annual reporting identifies phishing/spoofing among the most commonly reported cybercrime categories, reflecting its broad reach and low barrier to attacker use. Verizon's Data Breach Investigations Report also documents the continuing importance of social-engineering techniques in real-world breaches. Therefore, when the question asks for the typical leading incident based on general statistics, phishing is the most appropriate selection. See the FBI IC3 2023 Annual Report and the Verizon Data Breach Investigations Report.

QUESTION NO: 47

ClobalTech, an avant-garde tech giant, became victim to a massive data breach. The perpetrator was identified as an inside employee who had been with the company for over a decade. The breach unveiled sensitive client data that severely tarnished the company's reputation. ClobalTech is now revamping its security strategy. What should be its primary emphasis?

A. Monitor and restrict internet access for employees.

B. Rotate employees between departments every year.

C. Mandate monthly cybersecurity training for all employees.

D. Implement behavioral analytics to scrutinize and detect abnormal employee activities.

ANSWER: D

Explanation:

Implement behavioral analytics to scrutinize and detect abnormal employee activities is the primary emphasis because the incident was caused by a trusted, long-tenured insider. Insider threats frequently involve valid accounts and authorized access, meaning traditional perimeter-focused monitoring may not identify misuse of sensitive data. Behavioral analytics establishes a baseline of normal activity for each user or role, then detects meaningful deviations such as unusual access times, atypical data volumes, access to systems outside normal job responsibilities, or suspicious file transfers. These alerts give incident handlers an opportunity to investigate potentially harmful activity early, contain the event, and preserve relevant evidence before substantial exfiltration occurs. This capability is commonly implemented through user and entity behavior analytics, integrated with centralized logging, identity controls, and security monitoring. NIST's insider-threat guidance emphasizes monitoring and analysis as important elements of an insider-threat program, while CISA identifies anomalous user behavior and unauthorized data access as important indicators requiring attention. Making behavioral analytics central to the revised strategy directly addresses the organization's demonstrated risk: abuse of legitimate internal access. See NIST SP 800-53 security and privacy controls and CISA Insider Threat Mitigation.

QUESTION NO: 48

An incident handler arrives at a compromised server that is still powered on and connected to the network. Which of the following should be collected first because it may be lost when the system is shut down or rebooted?

A. Volatile memory contents

B. Archived backup tapes

C. Printed system documentation

D. Inactive user account records

ANSWER: A

Explanation:

Volatile memory contents is correct because RAM contains information that normally disappears when power is removed or the operating system is restarted. This information can include running processes, active network connections, logged-on users, command history, encryption keys, injected code, and other indicators that may not be available from disk evidence alone. The incident handler should carefully collect volatile data using approved procedures before performing actions that could alter or destroy it.

Nonvolatile evidence, such as disk contents, can generally be acquired after volatile evidence has been preserved. NIST forensic guidance emphasizes that responders should consider the volatility of evidence and preserve data that is most likely to change or disappear first. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 49

Performing Vulnerability Assessment is an example of a:

A. Incident Response

B. Incident Handling

C. Pre-Incident Preparation

D. Post Incident Management

ANSWER: C

Explanation:

Performing Vulnerability Assessment is an example of **Pre-Incident Preparation**. Vulnerability assessment is a proactive activity performed before a security event is identified or declared. It systematically identifies, inventories, validates, and prioritizes weaknesses in systems, applications, configurations, and network services so the organization can remediate or mitigate those weaknesses before they are exploited. Its results support essential preparedness activities, including risk-based patching, hardening, control selection, asset-risk awareness, and the creation of detection and response priorities.

This aligns with incident-handling guidance that places vulnerability management, security assessments, and preventive safeguards within organizational preparation. Effective preparation reduces both the likelihood that an incident will occur and the potential impact if an attacker attempts to exploit an exposed weakness. NIST describes vulnerability monitoring and scanning as activities used to identify vulnerabilities and inform remediation, while its incident-handling guidance identifies preparation as a foundational capability for managing incidents effectively. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and NIST SP 800-40 Rev. 4, Enterprise Patch Management Planning.

QUESTION NO: 50

One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

A. Protection

B. Preparation

C. Detection

D. Triage

ANSWER: A

Explanation:

Protection is correct because this CERT incident-management activity uses lessons learned from completed incident handling to reduce the likelihood and impact of future incidents. Postmortem reviews identify gaps such as inadequate physical safeguards, weak network segmentation, insufficient logging, unpatched systems, unclear procedures, or missing defensive controls. The resulting improvements are then implemented as protective measures across the environment. This makes incident management a continuous improvement discipline rather than a process that ends when an individual incident is closed.

Infrastructure improvements can include strengthening facility access controls, hardening systems, improving monitoring coverage, revising backup and recovery capabilities, and introducing technical or administrative controls that address the root causes and contributing conditions found during review. These actions feed operational experience back into the organization's security posture, helping it prevent recurrence and improve resilience. This aligns with the incident-response lifecycle guidance that emphasizes lessons learned and using incident findings to improve security controls and response capabilities. See the CISA incident response resources and the CERT/SEI cybersecurity resources for incident-management and continuous-improvement guidance.