Eccouncil

(212-89)

EC-Council Certified Incident Handler

Total: **163 Questions**

Link:

MYEXAM.FR

Evaluation of Other Options:

A: High level incident
Labeling this incident as high level would imply a critical breach that has far-reaching consequences across multiple organizational domains, potentially jeopardizing essential operations or leading to substantial regulatory penalties. Given that the incident is contained to competitive information and can be resolved within hours, it does not justify the high level classification.

C: Ultra-High level incident
An ultra-high level incident would typically encompass scenarios involving catastrophic failures, such as extensive data breaches affecting thousands of stakeholders or long-term system disruptions. The promptness and specific nature of the incident at hand do not exhibit these characteristics. The employee's actions, while significant, are more contained and manageable.

D: Low level incident
This classification would be inappropriate as it underestimates the severity of passing sensitive access control information to a competitor. Such actions can pose a serious threat to market position and are intrinsically linked to organizational security, necessitating immediate attention and response.

For authoritative references:

1. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
2. https://www.oecd.org/sti/ieconomy/38500804.pdf
3. https://www.isaca.org/resources/itaf/what-is-incident-response

Question: 5

Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a business continuity plan?

A. Forensics Procedure Plan
B. Business Recovery Plan
C. Sales and Marketing plan
D. New business strategy plan

Answer: B

Explanation:

The correct answer is B: Business Recovery Plan, as it is essential for ensuring organizational resilience post-disaster.

A Business Recovery Plan (BRP) is critical within a Business Continuity Plan (BCP) because it outlines the procedures and resources necessary to restore operations and minimize downtime following a disruptive event. The plan encompasses strategies for both immediate recovery and restoration of business functions, thus directly correlating to the core definition of business continuity.

Evaluation of Other Options:

A. **Forensics Procedure Plan**: While important for investigating breaches and understanding incidents, it focuses primarily on post-incident analysis rather than operational continuity. Its role is supplementary,

Answer: A

Explanation:

A is correct because the procedure to identify security funds to hedge risk does not directly correlate with operational procedures found in a computer risk policy.

Justification:

1. **Scope of a Risk Policy**: A computer risk policy is designed primarily to outline operational procedures, responsibilities, and guidelines to manage and mitigate security incidents effectively. It encompasses monitoring, training, and contingency planning rather than financial considerations.
2. **Operational Focus**: Options B, C, and D all emphasize the operational aspects necessary to maintain robust security frameworks. Monitoring the efficiency of security controls (B) ensures that current measures are effective, while ongoing training for authorized employees (C) is crucial for vigilance and awareness of potential threats. Provisions for continued support during incidents (D) are essential for maintaining system integrity and customer trust.
3. **Financial Initiatives**: Option A introduces a financial component by suggesting that identifying security funds to hedge risk is an integral aspect of the risk management process. While funding is important, it does not fit the procedural actions typically embedded in a risk policy aimed at incident management. This reflects a broader organizational strategy rather than a specific incident response procedure.

Evaluation of Other Options:

B (Monitoring Efficiency): This is a critical component of risk management, allowing organizations to assess the effectiveness of existing security measures and implementing necessary adjustments. Efficient monitoring correlates directly with successful incident management.

C (Training of Employees): Employee training is vital as human error often constitutes a significant vulnerability in security frameworks. A well-informed staff can identify and mitigate potential threats, reinforcing the organization's security posture.

D (Support Provisions): These are essential for business continuity, establishing a clear direction for responding to system interruptions or failures, ensuring minimal downtime and maintaining operational integrity.

References:

https://www.isc2.org/News-and-Events/Blog/PostID/14486/What-is-an-Information-Security-Risk-Management-Policy
https://csrc.nist.gov/publications/detail/sp/800-39/final
https://www.sans.org/white-papers/1957/

Question: 9

Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation
B. XSS Attack
C. SQL Injection
D. Denial of Service Attack

software, where their effects can be devastating.

Evaluation of Other Options:

A. **Cookie Tracker:** Cookie trackers are primarily used for user behavior analysis and advertising. They do not possess inherent malicious capabilities to access or manipulate systems, and their purpose is less nefarious compared to Trojans.

B. **Worm:** Worms self-replicate across networks without needing user intervention, unlike Trojans, which rely on users executing them willingly. Worms generally target vulnerabilities for propagation rather than disguising themselves as benign applications to gain access.

D. **Virus:** While viruses attach themselves to legitimate programs and can cause harm, they differ significantly from Trojans as they require a host file to replicate. Trojans do not replicate and instead rely on deception and user action to compromise the system.

In conclusion, Trojans represent a sophisticated method of attack by exploiting user trust and effectively compromising system integrity, thereby aligning them closely with the attributes described in the question.

References:

https://www.cyber.gov.au/acsc/view-all-content/publications/malware
https://www.cisa.gov/publications-library/blog/what-trojan-horse-malware
https://www.varonis.com/blog/trojans

Question: 12

Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

A. (Probability of Loss) X (Loss)
B. (Loss) / (Probability of Loss)
C. (Probability of Loss) / (Loss)
D. Significant Risks X Probability of Loss X Loss

Answer: A

Explanation:

The correct answer is A. (Probability of Loss) X (Loss) as it encapsulates the fundamental principle of quantitative risk assessment.

In quantitative risk assessment, the focus is on quantifying risk in numerical terms where the risk is defined as the potential for loss or gain. Option A accurately captures this definition by multiplying the probability of an adverse event by the potential loss associated with that event, thus providing a concrete measure of risk exposure. This calculation allows organizations to prioritize risks based on their financial impact, facilitating informed decision-making regarding resource allocation and risk mitigation strategies.

Critique of Other Options:

B. (Loss) / (Probability of Loss): This formulation wrongly suggests that one could derive an actionable risk value by inversely relating loss to the probability, which lacks an intuitive or practical application in calculating risk impact.

Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a course of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

A. Examination> Analysis > Preparation > Collection > Reporting
B. Preparation > Analysis > Collection > Examination > Reporting
C. Analysis > Preparation > Collection > Reporting > Examination
D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

Explanation:

D is correct because it follows a systematic approach essential for ensuring the integrity and admissibility of digital evidence.

The computer forensics process begins with Preparation, where strategies for evidence collection are developed, ensuring compliance with legal requirements and the preservation of data integrity. Next is Collection, which involves the acquisition of digital evidence from various sources, using techniques that prevent alteration or loss. The Examination phase employs specific methodologies to analyze the gathered data, identifying relevant information and ensuring that no data is overlooked. This leads to the Analysis stage, which synthesizes findings and interprets the implications within a legal context. Finally, Reporting documents the entire process and presents conclusions in a format suitable for court proceedings, which is critical for legal validation.

Other options are incorrect for the following reasons:

A incorrectly sequences the steps, starting with Examination, which cannot occur until Collection has been performed.
B places Analysis before Collection, which disallows the foundational evidence-gathering step and compromises the integrity of findings.
C erroneously sequences Analysis before Reporting, which could lead to presenting unverified conclusions without prior Examination of the evidence.

Thus, the order in D not only reflects logical progression but also adheres to best practices within the field.

References:

https://www.ncjrs.gov/pdffiles1/nij/226686.pdf
https://www.coursera.org/learn/computer-forensics
https://www.forensicscolleges.com/faq/what-is-computer-forensics

Question: 17

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

A. An insider intentionally deleting files from a workstation
B. An attacker redirecting user to a malicious website and infects his system with Trojan
C. An attacker infecting a machine to launch a DDoS attack
D. An attacker using email with malicious code to infect internal workstation

D. CAT 6: This category encompasses incidents regarding policy violations or noncompliance, which does not apply here since the incident is technical in nature, primarily focused on disrupted services rather than policy breaches.

References:

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
https://www.dhs.gov/publication/cybersecurity-incident-reporting-guidelines
https://www.cisa.gov/publications-library/guides/federal-information-security-modernization-act-fisma

Question: 21

US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?

A. Weekly

B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to successfully mitigate activity

C. Within two (2) hours of discovery/detection

D. Monthly

Answer: A

Explanation:

A is correct because the CAT 4 Federal Agency category necessitates incidents to be reported weekly, reflecting a lower severity compared to other categories.

The U.S. Computer Emergency Readiness Team (US-CERT) classifies incidents based on their potential impact and urgency, with CAT 4 representing incidents that pose minimal immediate danger but may still have significant operational implications. Reporting weekly allows for a systematic update on ongoing incidents and facilitates more thorough analyses without overwhelming resources.

Critical Evaluation of Other Options:

B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity: This timeframe pertains to CAT 1 incidents, which involve severe threats requiring urgent reporting. CAT 4 incidents do not demand such immediate actions due to their lower impact level.

C. Within two (2) hours of discovery/detection: This timeframe is applicable to CAT 2 incidents, which require expedited response mechanisms for moderate threats. CAT 4's specification for weekly reporting establishes a less urgent requirement that aligns with its categorization.

D. Monthly: This option underestimates the frequency required, as CAT 4 dictates a more proactive approach, necessitating weekly updates instead of a more lenient monthly obligation.

Ultimately, adhering to the established reporting timelines enables federal agencies to balance resource allocation with incident management effectively.

References:

https://www.us-cert.cisa.gov/incident-handling-guide
https://www.cisa.gov/publications-library

D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

Answer: A

Explanation:

The correct answer is A: "All access rights of the employee to physical locations, networks, systems, applications, and data should be disabled."

Disabling all access rights immediately upon termination is critical for mitigating potential security risks. This action serves to prevent unauthorized access to sensitive organizational data and systems—a foundational aspect of incident response management. The principle of least privilege dictates that individuals should only have access necessary for their roles; thus, revoking access upon termination ensures compliance with this principle and reduces the risk of insider threats (East, 2020). Furthermore, timely access termination is mandated by various regulations governing data protection, highlighting its importance in maintaining the integrity and confidentiality of information (Nyskohus, 2023).

Evaluation of Other Options:

B. The organization should enforce separation of duties: While enforcing separation of duties is a best practice for security management, it is more strategic and preventive rather than an immediate action post-termination. This option does not address the immediate risk posed by terminated employees.

C. The access requests granted to an employee should be documented and vetted by the supervisor: Though documentation and vetting are important to prevent unauthorized access at the outset of employment, they do not address the critical issue of removing access post-termination. This step is reactive rather than proactive.

D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information: Monitoring is essential for ongoing security but does not directly address the risks associated with a recently terminated employee. This option delays necessary action and does not resolve the immediate vulnerability created by terminated access.

In summary, while all options reflect important aspects of security management, prompt revocation of access (Option A) remains the most urgent action necessary to mitigate risks associated with employee termination.

References:

https://www.csoonline.com/article/2115969/the-importance-of-disabling-access-rights-immediately-upon-employee-termination.html
https://www.securitymagazine.com/articles/91180-why-separation-of-duties-is-vital-for-incident-handling
https://www.privacycompliance.global/importance-of-documenting-access-requests-in-the-workplace

Question: 25

A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:



C. Containment
D. Identification

Answer: D

Explanation:

D is correct because the identification stage is crucial for understanding the specifics of an incident, which includes analyzing system and network log files for clues about its nature and impact.

The identification phase involves a comprehensive examination of logs, alerts, and other data to ascertain the characteristics of the incident. This initial assessment is vital for categorizing the incident and determining its potential severity. By reviewing system and network logs, incident handlers can identify indicators of compromise (IoCs), track user activities, and pinpoint entry points exploited by attackers. Such meticulous analysis lays the groundwork for informed decision-making in subsequent response stages.

Critical Evaluation of Other Options:

A. Incident Recording: This stage focuses on documenting the incident and relevant details such as time and nature, but it does not involve in-depth log analysis. Recording is foundational but not diagnostic.

B. Reporting: Reporting occurs after the incident is understood and mitigated, summarizing findings for stakeholders. This step communicates outcomes rather than analyzes root causes or current impacts.

C. Containment: Containment involves measures taken to limit the incident's spread and impact once it has been identified. It does not typically include log analysis but rather focuses on mitigating damage.

In summary, D is distinctly positioned as the stage where log audits occur, enabling the identification and understanding of incidents.

References:

https://www.eccouncil.org/
https://www.csoonline.com/article/3532926/what-is-the-cybersecurity-incident-response-plan.html
https://www.ncsc.gov.uk/guidance/incident-management

Question: 29

Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

A. NET-CERT
B. DFN-CERT
C. Funet CERT
D. SURFnet-CERT

Answer: D

Explanation:

D is correct because SURFnet-CERT is specifically dedicated to addressing computer security incidents involving higher education institutions in the Netherlands, serving as an essential resource in both victim and

Question: 33

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

A. To restore the original site, tests systems to prevent the incident and terminates operations
B. To define the notification procedures, damage assessments and offers the plan activation
C. To provide the introduction and detailed concept of the contingency plan
D. To provide a sequence of recovery activities with the help of recovery procedures

Answer: A

Explanation:

The main purpose of the reconstitution plan is to restore the original site, test systems to prevent future incidents, and terminate operations.

Reconstitution is crucial in the incident handling lifecycle, as it ensures that fundamental systems and operations are restored to a secure state post-incident, allowing businesses to resume normal functionality while minimizing future risks. This process focuses on not just recovering but enhancing the resilience of the infrastructure.

Evaluation of Options:

B. To define the notification procedures, damage assessments and offers the plan activation: While notification and assessment are critical components of the initial response to an incident, they are not specific to reconstitution. Instead, these elements fall under the notification activation component of an IT contingency plan.

C. To provide the introduction and detailed concept of the contingency plan: This option relates more to the plan's preamble than to any operational phase like reconstitution. The introduction primarily serves to set the context and objectives rather than addressing the nuanced processes involved in recovery.

D. To provide a sequence of recovery activities with the help of recovery procedures: Although recovery activities are instrumental in reestablishing normal operations, the option does not encapsulate the broader scope of reconstitution, which also emphasizes testing and ensuring resilience against recurrence of incidents.

In summary, A distinctly captures the essence of reconstitution by linking operational recovery with future incident preventive measures, reinforcing its critical role within the overall IT contingency strategy.

References:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7827223/
https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-new-it-contingency-planning-handbook

Question: 34

The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the

legal standards for evidence preservation.

C. Forensic analysis report: This report summarizes findings from an investigation and evaluates the evidence; however, it does not provide a systematic way to maintain the evidence itself. Without a Chain-of-Custody, the integrity of evidence may still be questioned despite the conclusions drawn in the analysis.

D. Chain-of-Precedence: This term often refers to the hierarchy of evidence reliability rather than the documentation of evidence handling. It lacks the procedural rigor necessary for safeguarding evidence and fails to establish a documented path of evidence management required in legal settings.

In conclusion, B is the only option that serves to preserve and protect evidence effectively, ensuring legal compliance and maintaining its integrity throughout any investigation.

References:

https://www.courts.ca.gov/documents/ChainofCustody.pdf
https://www.ncjrs.gov/pdffiles1/nij/185560.pdf
https://www.sans.org/media/209234/home/chain-of-custody.pdf

Question: 38

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

A. Links the appropriate technology to the incident to ensure that the foundation's offices are returned to normal operations as quickly as possible

B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management

C. Applies the appropriate technology and tries to eradicate and recover from the incident

D. Focuses on the incident and handles it from management and technical point of view

Answer: B

Explanation:

B is correct because the Incident Coordinator facilitates communication and coordination among various affected groups such as legal, human resources, management, and other business areas during an incident.

The role of the Incident Coordinator is essential in the Incident Response Team (IRT) as it ensures that stakeholders across different domains are aligned and informed throughout the incident lifecycle. By linking these groups, the Incident Coordinator plays a critical role in managing the incident's broader implications, encompassing legal, ethical, and operational concerns. Effective communication enhances coordination and aids in timely decision-making, ultimately leading to a more efficient incident resolution.

Evaluation of Other Options:

A. The assertion that the Incident Coordinator links technology to the incident is misleading. While technical resources are vital, it is not the primary responsibility of the Incident Coordinator to manage technology directly. This task is usually assigned to technical specialists within the IRT who focus on the technological aspects of incident management, such as system recovery or data integrity.

C. The function of applying technology and eradicating incidents aligns more with the roles of technical team members, such as cybersecurity analysts or incident handlers. The Incident Coordinator's role is more strategic and communicative, rather than operational or technical in nature, making this option inaccurate in

Question: 41

A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so

B. The message from a known email id is caught by SPAM filters due to change of filter settings

C. The message warns to delete certain files if the user does not take appropriate action

D. The message prompts the user to install Anti-Virus

Answer: B

Explanation:

B is correct as it describes a symptom unrelated to virus hoax messages, which typically lack legitimate concerns about spam filters.

Virus hoaxes primarily rely on instilling fear or urgency without promoting genuine response mechanisms. They characteristically prompt forwarding to amplify reach (A), threaten action (C), or suggest downloads (D). Each of these actions manipulates user behavior under false pretenses, aligning closely with the psychological strategy of hoax dissemination.

Option A is incorrect as it explicitly incentivizes users to forward the hoax for monetary gain, a hallmark of such scams. This technique exploits social connections, leveraging the urgency to enhance credibility and proliferation.

Option C is incorrect since it typically involves directives that can incite fear or panic among users, pushing them to take unnecessary actions based on fabricated information about file deletions. Such strategies effectively amplify the hoax's reach.

Option D is incorrect because persuading users to install purported antivirus software is a common tactic in virus hoaxes. This not only propagates the misinformation but can also lead to malicious software installation under the guise of security.

In summary, while options A, C, and D align with the characteristics of virus hoaxes, option B does not reflect the typical attributes of such messages.

https://www.cisecurity.org/white-papers/the-truth-about-email-hoaxes/
https://www.webroot.com/us/en/resources/tips/article/how-to-spot-an-email-hoax
https://www.kaspersky.com/resource-center/preemptive-safety/hoaxes

Question: 42

In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

A. Likelihood Determination

B. Control recommendation

Evaluation of Other Options:

Option A: This statement is true as enforceability through both technical controls and organizational sanctions is vital in ensuring compliance and effectiveness. A policy that cannot be enforced is merely aspirational and lacks operational relevance.

Option C: This option is also true; effective implementation through administrative procedures and acceptable use guidelines ensures that employees understand their roles and responsibilities, fostering a security-aware culture within the organization.

Option D: True as well, since a clearly defined delineation of responsibilities helps in accountability and promotes adherence to the policy. It establishes a framework for who is responsible for various aspects of security, aiding in the efficient execution of security measures.

In summary, while enforceability and clarity in an organization's security policy are crucial, legal approval is not a fundamental requirement.

References:

1. https://www.nist.gov/publications/introduction-information-security
2. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. https://www.sans.org/white-papers/401/

Question: 45

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:

B is correct as inspecting the processes running on the system is crucial for recognizing infected hosts and mitigating potential threats.

In incident response, the ability to detect malicious processes is integral to distinguishing between normal and abnormal behavior in an information system. When an incident occurs, automated or manual inspection of running processes enables cybersecurity professionals to identify unauthorized applications or malware directly affecting the system. This process scrutiny allows for the isolation of infected hosts, which is essential for containing the incident and preventing further spread within the network.

Evaluation of Incorrect Options:

A. Configuring firewall to default settings - While reverting firewalls to default settings can enhance protection against unintentional rule changes, it does not actively identify infected hosts. Firewall configurations primarily control traffic rather than analyze running processes for criminal activity.

C. Browsing particular government websites - This action is largely irrelevant in terms of incident handling. It

A. SAM file
B. Web serve log
C. Routing table list
D. Web browser history

Answer: D

Explanation:

D is correct because web browser history provides direct evidence of the websites visited, which can link the suspect to child pornography.

In cyber-crime investigations, digital evidence must establish a clear connection between the suspect and illegal activities. Web browser history serves as a crucial artifact, showing specific URLs accessed, search terms used, and timestamps of activity. This direct correlation can help ascertain the suspect's online behavior related to child pornography, supporting evidence for both prosecution and understanding the extent of the crime.

Evaluation of Other Options:

A. SAM file: The Security Account Manager (SAM) file is primarily concerned with user account management on Windows systems. While it contains hashed passwords and user authentication data, it does not directly indicate web activity related to child pornography, and thus is less relevant in this investigation.

B. Web server log: While web server logs can contain useful information about data traffic to and from websites, they typically lack specific user context, such as exact IP addresses associated with particular users, especially if the evidence is gathered from a shared or public server. This makes them less reliable than direct user browser history.

C. Routing table list: A routing table provides information about the paths data takes to reach destinations across networks and does not contain user-level data or specifics about the criminal's online activities. Its utility in the context of proving individual access to child pornography is minimal.

In conclusion, web browser history provides the most pertinent and direct evidence linking the criminal to the offense, thereby making it the optimal choice for John's investigation.

References:

https://www.ncjrs.gov/pdffiles1/Digitization/203778NCJRS.pdf
https://www.us-cert.cisa.gov/ncas/white-papers/digital-evidence-law-enforcement-investigations
https://www.forensicscolleges.com/blog/digital-evidence-in-cyber-crime-investigations