7. Amanda's organization does not currently have an incident response plan. Which of the following reasons is not one she should present to management in support of creating one?

a. It will prevent incidents from occurring.

b. It will help responders react appropriately under stress.

c. It will prepare the organization for incidents.

d. It may be required for legal or compliance reasons.

Correct Answer: a. It will prevent incidents from occurring.

**Detailed Explanation of the Correct Answer:**

Option a is the correct answer because an incident response plan (IRP) does not prevent incidents from occurring; rather, it prepares an organization to handle incidents effectively when they do occur. The purpose of an IRP is to ensure a coordinated and structured approach to responding to cybersecurity incidents, minimizing the impact and facilitating a swift recovery. Although an IRP helps manage incidents, it does not act as a preventive measure, which would involve tools and practices focused on detecting and mitigating risks before they become incidents.

**Explanations for Why Each of the Other Options Is Incorrect:**

b. It will help responders react appropriately under stress:

This is a correct reason to support the creation of an incident response plan. During a cybersecurity incident, stress levels can be high, and a well-structured IRP provides clear guidelines and procedures for responders to follow, helping them act decisively and consistently. Having a predefined plan reduces uncertainty and supports better decision-making, which is especially valuable under pressure.

c. It will prepare the organization for incidents:

This is also a correct reason to advocate for an IRP. An incident response plan allows an organization to anticipate potential threats and defines specific actions to take if an incident occurs. This preparation includes identifying incident response teams, defining roles and responsibilities, establishing communication protocols, and planning recovery steps, all of which make the organization better equipped to respond to incidents.

d. It may be required for legal or compliance reasons:

This is another valid reason to support the development of an IRP. Many industries and regulatory bodies require organizations to have an incident response plan in place as part of compliance with cybersecurity standards, such as the GDPR, HIPAA, or PCI-DSS. Failing to meet these requirements could result in fines, legal repercussions, or loss of customer trust, making compliance a compelling reason for implementing an IRP.

21. Elle is conducting an exercise for her organization and wants to run an exercise that is as close to an actual event as possible. What type of event should she run to help her organization get this type of real-world practice?

\*a. A simulation

b. A tabletop exercise

c. A walk-through

d. A wargame

**Correct Answer: a. A simulation**

Detailed Explanation of the Correct Answer:

Option a (A simulation) is the best choice because a simulation closely replicates a real-world event, providing participants with a hands-on, realistic experience. In a simulation exercise, participants respond to a mock incident using actual tools, procedures, and communication channels, giving them the chance to practice their roles in a scenario that mirrors real events. This type of exercise is highly effective for preparing an organization for actual incidents, as it involves real-time decision-making and response actions.

**Explanations for Why Each of the Other Options Is Incorrect:**

b. A tabletop exercise:

A tabletop exercise is a discussion-based exercise where participants talk through their responses to a hypothetical scenario rather than acting them out. While tabletop exercises are valuable for identifying potential gaps in response plans and enhancing team coordination, they do not provide the same level of realism as a simulation because they lack the hands-on, immersive experience.

c. A walk-through:

A walk-through is a low-intensity exercise in which team members review response plans and procedures step-by-step in a non-realistic setting. This type of exercise is helpful for introducing participants to the plan and ensuring everyone understands their roles, but it lacks the urgency and realism that a simulation offers.

d. A wargame:

A wargame is a strategic exercise often used to explore decision-making processes and test strategic plans in hypothetical scenarios. While wargames are useful for high-level planning and testing different strategies, they are not typically conducted in a hands-on, realistic environment, making them less suited for practical, real-world incident response training.

85. Wiping a drive and reinstalling from known good media is an example of what incident

response option?

a. Recovery

b. Containment

\*c. Eradication

d. Root cause elimination

**Correct Answer: c. Eradication**

Detailed Explanation of the Correct Answer:

Option c (Eradication) is the correct answer because wiping a drive and reinstalling from known good media is a method used to completely remove any malicious software or compromised files from a system. Eradication involves ensuring that any traces of the malware, vulnerabilities, or compromised files are thoroughly removed to prevent further exploitation or re-infection of the system. This step is crucial after containing an incident but before moving to recovery, as it removes the root cause of the incident from the affected systems.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. Recovery:

Recovery involves restoring systems to normal operation after an incident has been contained and eradicated. While wiping and reinstalling can support the recovery process, the primary purpose of this action in the context given is to remove the threat, which falls under eradication rather than recovery.

b. Containment:

Containment involves stopping the spread of an incident and limiting its impact on other systems or networks. Wiping and reinstalling is not a containment action; it is an eradication measure taken to ensure that the threat is fully removed from the system. Containment typically involves temporary measures like isolating the infected system, not permanently removing data and applications.

d. Root cause elimination:

Root cause elimination generally refers to addressing the underlying vulnerability or issue that allowed the incident to occur in the first place. While wiping and reinstalling can remove the malware, it does not necessarily address the root cause of how the malware infected the system initially (e.g., a software vulnerability or weak password). Additional steps would be required to fully address and eliminate the root cause.

62. What phase of the incident response process often involves adding firewall rules and patching systems to address the incident?

a. Preparation

b. Eradication

\*c. Recovery

d. Containment

**Correct Answer: c. Recovery**

Detailed Explanation of the Correct Answer:

Option c (Recovery) is correct because this phase of the incident response process involves actions to restore systems to normal operations and strengthen defenses to prevent similar incidents in the future. During the recovery phase, teams often apply patches, update firewall rules, and make configuration changes to mitigate vulnerabilities exploited in the incident. These steps are essential to ensure that the systems are secure and resilient before they are fully brought back online.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. Preparation:

The preparation phase involves proactive planning, setting up incident response tools, training, and establishing protocols for handling potential incidents. While adding firewall rules and patching systems are important security measures, they are usually performed reactively in response to an incident rather than during preparation, which is more about readiness than response.

b. Eradication:

The eradication phase focuses on removing the threat from the affected systems, such as by deleting malicious files or reinstalling compromised software. While this phase may involve actions to clear the immediate issue, adding firewall rules and patching typically occurs afterward, during recovery, to secure the system long-term.

d. Containment:

Containment is about stopping the spread of an incident and limiting its impact on other systems. Actions in this phase are usually temporary and aimed at controlling the immediate situation, such as isolating infected systems. Permanent security enhancements, like adding firewall rules and patching, are not typically part of containment and are instead applied during the recovery phase.

4. Alaina has completed the eradication and recovery steps of the incident response process. What step commonly comes after these two phases?

\*a. A lessons learned session

b. Detection

c. Training

d. A tabletop exercise

**Correct Answer: a. A lessons learned session**

Detailed Explanation of the Correct Answer:

Option a (A lessons learned session) is the correct answer because, after the eradication and recovery steps, incident response teams typically hold a "lessons learned" session to review the incident. This step is crucial for analyzing the effectiveness of the response, identifying areas for improvement, and implementing any necessary adjustments to policies, procedures, or tools. By conducting this session, the organization can improve its incident response process and better prepare for future incidents.

**Explanations for Why Each of the Other Options Is Incorrect:**

b. Detection:

Detection is an early phase in the incident response process, focused on identifying potential incidents through monitoring and alerts. Since Alaina has already completed eradication and recovery, detection would not be the next step in this sequence.

c. Training:

Training is an important part of the preparation phase but is not typically the immediate next step after an incident has been resolved. While training might be recommended based on insights from the lessons learned session, it is not a direct follow-up step to eradication and recovery.

d. A tabletop exercise:

A tabletop exercise is a type of practice exercise where team members discuss their response to a simulated incident. It’s often used as a training tool to prepare for future incidents but is not the immediate step following an actual incident response process. The tabletop exercise may be recommended in the lessons learned session but would not directly follow eradication and recovery.

13. Brent wants to use a tool to help him analyze malware and attacks and wants to cover a broad range of tactics and tools that are used by adversaries. Which of the following is broadly implemented in technical tools and covers techniques and tactics without requiring a specific order of operations?

a. The Diamond Model of Intrusion Analysis

b. The Cyber Kill Chain

\*c. The MITRE ATT&CK framework

d. The CVSS (Common Vulnerability Scoring System) standard

**Correct Answer: c. The MITRE ATT&CK framework**

Detailed Explanation of the Correct Answer:

Option c (The MITRE ATT&CK framework) is the correct answer because it provides a comprehensive matrix of tactics, techniques, and procedures (TTPs) used by adversaries, organized in a way that allows analysts to understand and track various attack methods without a specific sequence. This framework is widely used in technical tools for malware and attack analysis and covers a broad spectrum of adversary behaviors, making it suitable for Brent’s needs. MITRE ATT&CK’s flexibility allows users to analyze attacks and malware across various stages without requiring a linear order, enabling a more dynamic analysis process.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. The Diamond Model of Intrusion Analysis:

The Diamond Model of Intrusion Analysis is a framework that focuses on understanding adversaries and their relationships to victims, capabilities, and infrastructure. It is useful for high-level threat analysis but does not provide the detailed, tactic-focused breakdown that MITRE ATT&CK offers. It is less commonly implemented in technical tools for directly analyzing malware and specific attack techniques.

b. The Cyber Kill Chain:

The Cyber Kill Chain, developed by Lockheed Martin, outlines a linear sequence of stages in an attack, from reconnaissance to exfiltration. While it’s useful for understanding the general flow of an attack, it is not as flexible as the MITRE ATT&CK framework for covering a wide range of tactics and techniques without following a specific order. The Kill Chain’s structured sequence makes it less ideal for analyzing non-linear attacks.

d. The CVSS standard:

The Common Vulnerability Scoring System (CVSS) is used for rating the severity of security vulnerabilities rather than analyzing adversary tactics or techniques. It does not provide a structure for understanding or analyzing specific malware or attack techniques and is not typically implemented in tools for threat analysis in the same way MITRE ATT&CK is.

42. Jack wants to ensure that files have not changed. What technique can he use to compare current versions of the files to an original copy?

a. Encryption

b. Check the file size

c. Check the file metadata

\*d. Compare hashes of the files

**Correct Answer: d. Compare hashes of the files**

Detailed Explanation of the Correct Answer:

Option d (Compare hashes of the files) is the correct answer because hashing generates a unique fixed-length string based on the contents of a file. By comparing the hash of the current version of a file to the hash of the original version, Jack can verify whether the file has been altered. If the hashes match, the file is unchanged; if they differ, the file has been modified. Hash functions like MD5, SHA-1, or SHA-256 are commonly used for this purpose because even a small change in file content results in a completely different hash.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. Encryption:

Encryption secures data by encoding it so that only authorized parties can access it. However, encryption does not provide a method to verify if a file has changed; it only protects the file’s contents from unauthorized access. Comparing files for changes requires a method like hashing, not encryption.

b. Check the file size:

Checking the file size may indicate if a file has been modified in a way that changes its size, but it is not a reliable method. Small changes that don’t affect the file size would not be detected. Hashing provides a more precise way to detect any modifications, regardless of size.

c. Check the file metadata:

File metadata (such as timestamps, author information, or file permissions) might offer clues about recent modifications, but it does not confirm if the content of the file has changed. Metadata can be altered independently of file content, making it an unreliable method for verifying file integrity compared to hashing.

51. Troy wants to review metadata about an email he has received to determine what system or server the email was sent from. Where can he find this information?

a. In the email message's footer

b. In the to: field

\*c. In the email message's headers

d. In the from: field

**Correct Answer: c. In the email message's headers**

Detailed Explanation of the Correct Answer:

Option c (In the email message's headers) is correct because email headers contain metadata about the message, including information about the servers and systems it passed through on its way to the recipient. By reviewing the email headers, Troy can trace the "Received" fields, which show the path the email took, including IP addresses, domain names, and timestamps for each mail server involved. This information can help determine the origin of the email and assess whether it might be legitimate or suspicious.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. In the email message's footer:

The footer of an email typically contains information added by the sender, such as contact details or disclaimers. It does not contain technical metadata about the email's origin or the servers involved in its transmission. Headers, not footers, provide this critical routing information.

b. In the to: field:

The "To" field only shows the intended recipient(s) of the email. It does not include metadata or information about the servers or systems that handled the email on its way to the recipient.

d. In the from: field:

The "From" field indicates the purported sender of the email, but it can easily be spoofed or altered and does not provide technical information about the actual server or system that sent the email. The headers are necessary to get accurate, detailed information about the email’s path.

48. Theresa's organization has received a legal hold notice for their files and documents. Which of the following is not an action she needs to take?

a. Ensure that changes to existing documents related to the case are tracked and that originals can be provided.

b. Preserve all existing documents relevant to the case.

\*c. Delete all sensitive documents related to the case.

d. Prevent backups that contain files related to the case from being overwritten on their normal schedule.

**Correct Answer: c. Delete all sensitive documents related to the case**

Detailed Explanation of the Correct Answer:

Option c (Delete all sensitive documents related to the case) is correct because deleting documents related to the case directly violates the legal hold notice. A legal hold requires that all relevant documents be preserved for potential review or use in legal proceedings. Deleting documents could be considered spoliation of evidence and might result in legal consequences for the organization. Instead, the organization should focus on retaining and safeguarding all pertinent files and data.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. Ensure that changes to existing documents related to the case are tracked and that originals can be provided:

Tracking changes to documents and retaining original versions are essential steps in a legal hold process. This ensures that any modifications made to documents after the hold was issued can be accounted for, and original documents can be provided if needed.

b. Preserve all existing documents relevant to the case:

Preserving all relevant documents is one of the main requirements of a legal hold. This action ensures that all evidence is intact and available for legal proceedings, aligning with the purpose of the legal hold notice.

d. Prevent backups that contain files related to the case from being overwritten on their normal schedule:

Preventing backups from being overwritten is necessary to ensure that historical versions of files are available if required. This step helps maintain a comprehensive record of all documents and files related to the case, in compliance with the legal hold.

55. What forensic concept is key to establishing provenance for a forensic artifact?

a. Right to audit

b. Preservation

\*c. Chain of custody

d. Timelines

**Correct Answer: c. Chain of custody**

Detailed Explanation of the Correct Answer:

Option c (Chain of custody) is the correct answer because the chain of custody is essential for establishing the provenance and integrity of a forensic artifact. It involves documenting each step in the handling, transfer, and storage of evidence from the moment it is collected to its presentation in court. Maintaining a clear chain of custody ensures that the artifact has not been altered or tampered with, which is critical for proving its authenticity and reliability as evidence.

Explanations for Why Each of the Other Options Is Incorrect:

a. Right to audit:

The right to audit is a legal or contractual right that allows a party to examine the practices, records, and compliance of another party. While important in legal and compliance contexts, it does not relate directly to the forensic process of proving the authenticity or origin of evidence.

b. Preservation:

Preservation involves protecting and safeguarding forensic artifacts from alteration or destruction, which is vital in forensic analysis. However, preservation alone does not establish provenance or the documented history of the artifact’s handling and custody. Chain of custody specifically addresses the artifact’s documented journey.

d. Timelines:

Timelines can help reconstruct the sequence of events in an investigation, but they do not establish the provenance of an artifact. Timelines may be derived from evidence, but they do not replace the need for a documented chain of custody to prove the artifact’s integrity.

60. What legal concept determines the law enforcement agency or agencies that will be involved in a case based on location?

a. Nexus

b. Nonrepudiation

\*c. Jurisdiction

d. Admissibility

**Correct Answer: c. Jurisdiction**

Detailed Explanation of the Correct Answer:

Option c (Jurisdiction) is correct because jurisdiction is the legal authority granted to a law enforcement agency or court to operate within a specific geographic area or over certain types of cases. In a legal context, jurisdiction determines which agencies have the authority to investigate, enforce laws, and prosecute cases based on the location where the crime or incident occurred. Jurisdictional boundaries help clarify which agency or agencies will lead or participate in the investigation.

**Explanations for Why Each of the Other Options Is Incorrect:**

a. Nexus:

Nexus refers to a connection or link, particularly between an entity and a location or activity, but it does not define which law enforcement agencies have authority over a case. While nexus can influence jurisdiction, it is not the legal concept that directly determines the involved agencies.

b. Nonrepudiation:

Nonrepudiation is a security principle ensuring that a person or entity cannot deny the validity of their actions or communications, commonly used in digital security contexts. It does not relate to the legal authority or jurisdiction of law enforcement agencies.

d. Admissibility:

Admissibility refers to whether evidence can be accepted in a court of law based on its relevance, reliability, and compliance with legal standards. While admissibility is important in legal proceedings, it does not determine which law enforcement agencies have jurisdiction in a case.