Free Questions for Lead-Cybersecurity-Manager by vceexamstest

Shared by Klein on 12-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is NOT a component of the ISO/IEC 27032 framework?

Options:

A- Cyber incident management

B- Business strategy formulation

C- Cybersecurity controls and best practices

D- Stakeholder cooperation

Answer:

B

Explanation:

ISO/IEC 27032 focuses on cybersecurity aspects such as cyber incident management, cybersecurity controls and best practices, and stakeholder cooperation. It does not cover business strategy formulation, which is outside its scope.

Question 2

Question Type: MultipleChoice

What is a key objective of the ISO/IEC 27032 standard?

Options:

A- To establish a framework for managing financial audits

B- To provide guidelines for protecting information systems from cyber threats

C- To define protocols for environmental management systems

D- To outline procedures for software development lifecycle

Answer:

B

Explanation:

The ISO/IEC 27032 standard aims to provide guidelines and best practices for protecting information systems and cyberspace from cyber threats, enhancing overall cybersecurity.

Question 3

Question Type: MultipleChoice

Which of the following best describes the primary focus of ISO/IEC 27032?

Options:

A- Financial management

B- Business continuity planning

C- Information security risk management

D- Cybersecurity

Answer:

D

Explanation:

ISO/IEC 27032 specifically focuses on cybersecurity, providing guidelines for improving the state of cybersecurity by addressing the protection of information systems and the broader internet ecosystem.

Question 4

Question Type: MultipleChoice

Which of the following activities does not ensure the ongoing security of an Intrusion Detection System (IDS)?

Options:

A- Encrypting IDS management communications

B- Creating unique user and administrator account for every IDS system

C- Reporting IDS alerts of malicious transactions to interested parties

Answer:

C

Explanation:

Reporting IDS alerts of malicious transactions to interested parties does not ensure the ongoing security of an Intrusion Detection System (IDS). While it is important for situational awareness and incident response, it does not directly contribute to the security and maintenance of the IDS itself. Ensuring ongoing security of an IDS involves activities such as encrypting IDS management communications and creating unique user and administrator accounts for every IDS system, which help protect the IDS from being compromised. Reference include NIST SP 800-94, which provides guidelines for securing IDS systems.

Top of Form

Bottom of Form

Question 5

Question Type: **MultipleChoice**

Why is proper maintenance of documented information important in a cybersecurity program?

Options:

A- It limns the possibility of taking spontaneous decisions

B- li ensures that actors are ready to act when needed

C- Both A and B

Answer:

B

Explanation:

Proper maintenance of documented information in a cybersecurity program is important because it ensures that actors are ready to act when needed. Up-to-date documentation provides clear guidelines and procedures for handling incidents, implementing security measures, and maintaining compliance with policies. This readiness is critical for effective and timely response to cybersecurity threats. Reference include ISO/IEC 27001, which emphasizes the importance of maintaining accurate and current documentation for effective information security management.

Question 6

Question Type: MultipleChoice

What is the main objective of end point monitoring in cyber security?

Options:

A- To respond to security threats in computer networks

B- To resolve network performance issues

C- To protect laptops, mobile devices, and servers

Answer:

C

Explanation:

The main objective of endpoint monitoring in cybersecurity is to protect laptops, mobile devices, and servers. Endpoint monitoring involves continuously monitoring and managing the security of devices that connect to the network, ensuring they are not compromised and do not become entry points for attacks. This practice helps maintain the security and integrity of the network by detecting and responding to threats targeting endpoints. Reference include NIST SP 800-137, which covers continuous monitoring and provides guidelines for protecting endpoint devices.

Top of Form

Bottom of Form

Question 7

Question Type: MultipleChoice

What information should be included in The vulnerability assessment report for vulnerabilities categorized as medium to high risk?

Options:

A- The plan and effort required to fix the vulnerability

B- The recommendations for enhancing access control and security requirements

C- The individuals responsible for addressing the vulnerability

Answer:

A

Explanation:

For vulnerabilities categorized as medium to high risk, the vulnerability assessment report should include the plan and effort required to fix the vulnerability. This information is crucial for prioritizing remediation efforts and allocating the necessary resources to address the vulnerabilities effectively. It helps ensure that high-risk issues are resolved promptly to minimize potential security impacts. Reference include NIST SP 800-115, which provides guidance on technical aspects of security testing and vulnerability assessments.

Question 8

Question Type: MultipleChoice

Which of the following statements regarding best describes vulnerability assessment?

Options:

A- Vulnerability assessment focuses on minimizing network downtime

B- Vulnerability assessment exploits vulnerabilities in multiple assets

C- Vulnerability assessment combines automated testing with expert analysis

Answer:

C

Explanation:

Vulnerability assessment best describes the process of combining automated testing with expert analysis. This approach helps identify, evaluate, and prioritize vulnerabilities in an organization's systems and networks. Automated tools can quickly scan for known vulnerabilities, while expert analysis can provide context, validate findings, and offer remediation recommendations. This comprehensive method ensures a thorough assessment of security weaknesses. Reference include NIST SP 800-30, which provides guidance on risk assessments, including vulnerability assessments.

Question 9

Question Type: MultipleChoice

EuroDart considers factors such as modems and faulty operations when maintaining documented Information regarding its cybersecurity practices. Is this a good practice?

Options:

A- Yes. because adapting lo changing threats and circumstances is crucial for effective cybersecurity

B- No. because it is more cost-effective to maintain a static cybersecurity program

C- It can be both a good and a bad practice, depending on EuroDart's mission and goals

Answer:

A

Explanation:

Considering factors such as modern threats and faulty operations when maintaining documented information regarding cybersecurity practices is a good practice. Cybersecurity is a dynamic field where threats and technologies continuously evolve. Regularly updating cybersecurity documentation ensures that the organization can adapt to new threats and changes in its operational environment, maintaining an effective defense posture. This practice is in line with ISO/IEC 27001, which emphasizes the need for continuous improvement and adaptation in information security management systems.