Cybersecurity for Marine Safety Personnel Training Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which document is NOT typically used to guide response actions after a cyber incident?

A. MCAAG

B. Incident Response Plan

C. System Recovery Procedure

D. Business Continuity Plan

2. Which term describes a group of computers located physically close to one another?

A. WAN

B. LAN

C. MAN

D. Enterprise Network

3. Which factor is multiplied by vulnerability and consequence to assess risk?

A. Impact

B. Threat

C. Probability

D. Exposure

4. Which two characteristics typically apply to Information Technology (IT)?

A. Strong security culture and frequently updated

B. Data availability critical and globally connected network

C. Limited access and rarely updated

D. Strong security culture and rarely updated

5. A DMZ in network security is used for what purpose?

A. To store sensitive data

B. To provide a buffer zone for external access

C. To monitor internal traffic

D. To back up public data

6. Which of the following is considered a risk to security in a facility?

A. Unauthorized access

B. Insider threats

C. Cyber incidents

D. All of the above

7. What describes the reporting requirement for increased network scanning?

A. Must be reported to the FBI

B. Always requires a COTP report

C. No report is necessary

D. Requires internal review

8. In the context of Industrial Control Systems (ICS), what is the primary purpose of a Supervisory Control and Data Acquisition (SCADA) system?

A. Connect users to the internet

B. Monitor and control processes in real time

C. Store data securely

D. Create backup copies of data

9. What does a Programmable Logic Controller (PLC) primarily control in industrial processes?

A. Network traffic

B. Electrical grids

C. Input/Output devices

D. Data storage

10. What is the difference between an Intrusion Detection System and an Intrusion Prevention System?

A. Both are the same

B. Only the latter blocks intrusions

C. Only the former detects intrusions

D. Both serve to enhance password security

Answers

1. A
2. B
3. B
4. A
5. B
6. D
7. C
8. B
9. C
10. B

Explanations

1. Which document is NOT typically used to guide response actions after a cyber incident?

A. MCAAG

B. Incident Response Plan

C. System Recovery Procedure

D. Business Continuity Plan

The Marine Cybersecurity Assessment Guidance (MCAAG) is primarily used as a framework to assess cybersecurity risks and vulnerabilities within maritime operations, rather than providing direct guidance for response actions after a cyber incident. Its focus is on evaluation and preparedness, which ensures that organizations understand their cyber posture and can take preventative measures. On the other hand, the Incident Response Plan outlines the specific actions and procedures to be followed in the event of a cyber incident, ensuring a structured and efficient response to minimize damage. The System Recovery Procedure details the steps necessary to restore systems to operational status after a breach, and the Business Continuity Plan addresses how an organization will continue to operate during and after a cyber incident, detailing recovery strategies for critical functions. Each of these documents plays a crucial role in managing and mitigating the impact of cybersecurity incidents, distinctly highlighting the MCAAG's role as more of an assessment tool rather than a response guide.

2. Which term describes a group of computers located physically close to one another?

A. WAN

B. LAN

C. MAN

D. Enterprise Network

The term that describes a group of computers located physically close to one another is "LAN," which stands for Local Area Network. A LAN typically covers a small geographic area, such as a single building or a campus, allowing devices within this proximity to communicate and share resources efficiently. This type of network enables high-speed connections and low latency, which is crucial for applications requiring quick data exchange, such as collaboration tools and file sharing. In contrast, other types of networks mentioned have different characteristics. A WAN, or Wide Area Network, covers larger geographical areas and connects multiple LANs, while a MAN, or Metropolitan Area Network, spans a city or a large campus, but still is broader than a LAN. An enterprise network generally refers to the entirety of networks operated by an organization, which may encompass multiple LANs, WANs, and other network types, but does not specifically denote a close physical arrangement of computers.

3. Which factor is multiplied by vulnerability and consequence to assess risk?

A. Impact

B. Threat

C. Probability

D. Exposure

The correct answer is that the factor multiplied by vulnerability and consequence to assess risk is the threat. In risk assessment, the calculation typically involves three primary components: vulnerability, consequence, and threat. Vulnerability represents the weaknesses in a system that could be exploited. Consequence is the potential impact or damage caused by an incident if it occurs. Threat, on the other hand, refers to any potential event or action that could exploit the vulnerability and lead to consequences. By multiplying vulnerability and consequence by the threat, you can derive the overall risk associated with a given scenario. This understanding is crucial because it emphasizes the dynamic nature of risk, where simply having vulnerabilities and consequences is not enough; the potential for a threat to exploit that situation must also be considered in order to accurately assess risk. The other options, while relevant to discussions about risk, do not perform the necessary role in this particular calculation. Impact, which relates closely but is not a direct factor in this formula, instead describes the effect of an event rather than contributing to the assessment framework. Probability might refer to the likelihood of a threat occurring, but it is not included in the primary formula where threat directly correlates with the assessment of risk alongside vulnerability and consequence. Exposure indicates the extent to

4. Which two characteristics typically apply to Information Technology (IT)?

A. Strong security culture and frequently updated

B. Data availability critical and globally connected network

C. Limited access and rarely updated

D. Strong security culture and rarely updated

The correct choice highlights the importance of a strong security culture and the need for frequent updates within Information Technology (IT) environments. A strong security culture is pivotal in IT as it fosters an environment where cybersecurity measures are prioritized, enabling organizations to proactively mitigate threats, educate employees about security practices, and maintain vigilance against potential breaches. Additionally, the frequency of updates is crucial because IT systems must regularly adopt patches, enhancements, and security measures to protect against evolving cyber threats. Regular updates ensure that software and systems remain resilient against vulnerabilities and exploits that can be targeted by malicious actors. This dynamic approach to cybersecurity practices reinforces the integrity and safety of the information systems, ultimately leading to a more secure IT environment. The other options do not accurately reflect the typical characteristics associated with IT. Characteristics like limited access and rarely updated systems would hinder operational efficiency and increase security risks, which contradicts the necessity for a proactive and robust security posture in modern IT infrastructure.

5. A DMZ in network security is used for what purpose?

A. To store sensitive data

B. To provide a buffer zone for external access

C. To monitor internal traffic

D. To back up public data

A DMZ, or Demilitarized Zone, in network security serves as a buffer zone between an internal network and external networks, like the internet. This configuration is strategically important because it allows organizations to expose certain services to the internet while keeping the more sensitive parts of the network protected. The DMZ typically hosts services that need to be accessible by external users, such as web servers, email servers, or DNS servers, separating them from the internal network where sensitive data resides. By having a DMZ, organizations can establish better control over traffic entering and leaving their networks. Any attack or breach originating from the internet is contained within the DMZ, preventing direct access to the internal systems and data. This way, even if an attacker successfully compromises a service in the DMZ, they encounter further barriers before reaching critical internal resources. This setup allows for heightened security measures, including monitoring and filtering traffic entering and leaving both the DMZ and the internal network, ensuring that potential threats are mitigated while still providing necessary access to specific functions. Thus, the role of a DMZ in providing a buffer zone for external access is essential in maintaining an organization's overall cybersecurity posture.

6. Which of the following is considered a risk to security in a facility?

A. Unauthorized access

B. Insider threats

C. Cyber incidents

D. All of the above

A comprehensive understanding of security risks in a facility necessitates recognizing various threats that could compromise safety and integrity. Unauthorized access is a critical risk as it involves individuals gaining entry to restricted areas without permission, which can lead to theft, vandalism, or data breaches. Insider threats represent another significant concern since they originate from employees or individuals within the organization who have legitimate access. These insiders may potentially exploit their privileges for malicious purposes, posing a notable risk to security. Cyber incidents encompass a wide array of threats, including hacking, phishing, and malware attacks, which can disrupt operations, compromise sensitive data, and threaten overall safety. The inclusion of all these elements highlights the multifaceted nature of security risks in a facility. Recognizing that each of these areas poses distinct challenges allows organizations to better prepare and implement a comprehensive security strategy that addresses unauthorized access, insider threats, and cyber incidents simultaneously.

7. What describes the reporting requirement for increased network scanning?

A. Must be reported to the FBI

B. Always requires a COTP report

C. No report is necessary

D. Requires internal review

The correct answer reflects that no report is necessary for increased network scanning in certain contexts. This is grounded in the fact that routine network scanning is often a standard operational procedure within cybersecurity practices for monitoring the health and security of systems. Increased scanning may merely indicate heightened awareness or proactive measures rather than a security incident requiring formal reporting. In many scenarios, organizations characterize such activities as regular maintenance or vulnerability assessments. Therefore, unless these scans lead to a discovery of a security breach or other actionable incident, there typically is no obligation to report these actions to external entities. Understanding this helps marine safety personnel focus on real threats and incidents that truly require escalated alerts and official reporting, rather than overburdening reporting mechanisms with routine activities. While other options suggest various reporting obligations, the specific nature of routine network scanning does not inherently necessitate external or internal reporting unless it uncovers significant concerns.

8. In the context of Industrial Control Systems (ICS), what is the primary purpose of a Supervisory Control and Data Acquisition (SCADA) system?

A. Connect users to the internet

B. Monitor and control processes in real time

C. Store data securely

D. Create backup copies of data

The primary purpose of a Supervisory Control and Data Acquisition (SCADA) system is to monitor and control processes in real time. SCADA systems play a critical role in various industrial sectors, including energy, water management, manufacturing, and transportation. They collect data from sensors and devices located in the field, which allows operators to oversee operations, respond to conditions promptly, and make informed decisions. Real-time monitoring facilitates immediate awareness of system performance, potential issues, and alarms. This capability is essential for maintaining efficiency, safety, and stability in operations. By enabling operators to control processes directly from a centralized location, SCADA systems help to streamline operations and enhance decision-making, thereby reducing risks and improving overall system reliability. While aspects such as connecting users to the internet, securely storing data, and creating backup copies of data are important components of overall cybersecurity and data management strategies, they do not capture the fundamental operational focus of SCADA systems in the context of Industrial Control Systems. Thus, the emphasis on monitoring and controlling processes in real time distinguishes the core function of SCADA from the other options.

9. What does a Programmable Logic Controller (PLC) primarily control in industrial processes?

A. Network traffic

B. Electrical grids

C. Input/Output devices

D. Data storage

A Programmable Logic Controller (PLC) primarily controls input and output devices in industrial processes, making it essential for automation systems in manufacturing and production environments. The PLC acts as the brain of the control system, receiving signals from various input devices such as sensors and switches, processing this information based on pre-programmed logic, and then sending commands to output devices like motors, valves, or alarms. This capability enables real-time monitoring and management of industrial operations, allowing for precise control over machinery and processes. Hence, the distinction of PLCs lies in their ability to interface with and regulate the physical components of industrial settings, making them critical for maintaining efficiency, safety, and reliability in operations. Other options pertain to different areas of technology. Network traffic management deals primarily with data transmission over networks, while electrical grids focus on the distribution and management of electrical power. Data storage refers to the collection and preservation of digital information, but these aspects do not encapsulate the main functions of a PLC in the context of industrial process control.

10. What is the difference between an Intrusion Detection System and an Intrusion Prevention System?

A. Both are the same

B. Only the latter blocks intrusions

C. Only the former detects intrusions

D. Both serve to enhance password security

An Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) are distinct components of network security, each serving unique roles in protecting data and systems from unauthorized access or attacks. The key difference lies in their functionality: an IDS focuses on monitoring and analyzing network traffic for suspicious activity and potential threats. It generates alerts when it detects anomalies, allowing security personnel to investigate and respond appropriately. In contrast, an IPS goes a step further by not only detecting threats but also actively preventing them from causing harm. When an IPS detects a potential intrusion, it can automatically take actions such as blocking traffic from the suspicious source or dropping malicious packets, effectively thwarting attacks in real time. Understanding this distinction is crucial for effective cybersecurity management. While both systems work to enhance overall security, the IPS provides a proactive layer by taking immediate action against identified threats, thereby offering a more comprehensive defense strategy. The other options either suggest that IDS and IPS are the same, misrepresent their functionalities, or incorrectly imply that they are focused solely on enhancing password security, which is not their primary function.