Free Questions for D-SF-A-24 by certsinside

Shared by Spence on 25-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

Dell Services team cannot eliminate all risks, but they can continually evaluate the resilience and preparedness of A .R.T.I.E. by using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Match the core NIST CSF component functions with the description that the Dell Services team would have recommended to A .R.T.I.E.

Source Area	Description	
Recover	Cultivate the organizational understanding of cybersecurity risks.	
Detect	Develop ways to identify cybersecurity breaches.	
Respond	Plan and implement appropriate safeguards.	
Protect	Quickly mitigate damage if a cybersecurity incident is detected.	
Identify	Restore capabilities that were impaired due to a cyberattack.	

Answer:

Question 2

Question Type: DragDrop

Match the security hardening type with the hardening techniques.

Source Area	Description	
Operating System	Implements Intrusion Prevention System.	
Database	Implements Role Base Access Control and removes unnecessary database services.	
Network	Encrypts the host device using hardware trusted privilege.	
Server	Enables secure boot and removes unnecessary drivers.	

Question 3

Question Type: MultipleChoice

To minimize the cost and damage of ransomware attacks the cybersecurity team provided static analysis of files in an environment and compare a ransomware sample hash to known data.

Which detection mechanism is used to detect data theft techniques to access valuable information and hold ransom?

Options:

A- Signature based

B- Behavior based

C- Deception based

Answer:

A

Explanation:

Signature-Based Detection: This method relies on known signatures or patterns of data that match known malware or ransomware samples1.

Static Analysis: Involves analyzing files without executing them to compare their hashes against a database of known threats1.

Ransomware Sample Hash: A unique identifier for a ransomware sample that can be matched against a database to identify known ransomware1.

Dell Security Foundations Achievement: The Dell Security Foundations Achievement documents likely cover the importance of signature-based detection as part of a comprehensive cybersecurity strategy1.

Effectiveness: While signature-based detection is effective against known threats, it may not detect new, unknown (zero-day) ransomware variants1.

Signature-based detection is a fundamental component of many cybersecurity defenses, particularly for identifying and preventing known ransomware attacks1.

Question 4

Question Type: MultipleChoice

Based on the information in the case study, which security team should be the most suitable to perform root cause analysis of the attack and present the proposal to solve the challenges faced by the A .R.T.I.E. organization?

Options:

A- Identity and Assess Management

B- Threat intelligence

C- Ethical hackers

D- Business advisory

Answer:

B

Explanation:

Role of Threat Intelligence: The threat intelligence team is specialized in investigating methodologies and technologies to detect, understand, and deflect advanced cybersecurity threats1.

Root Cause Analysis: They have the expertise to analyze security events, uncover advanced threats, and provide insights into the root causes of cyberattacks1.

Solution Proposal: Based on their analysis, the threat intelligence team can propose solutions to tackle the identified vulnerabilities and enhance the security posture of A .R.T.I.E.1.

Preventive Measures: Their knowledge of the latest developments in the security landscape allows them to recommend proactive measures to prevent future attacks1.

Dell Security Foundations Achievement: The Dell Security Foundations Achievement documents emphasize the importance of threat intelligence in understanding and responding to cybersecurity incidents1.

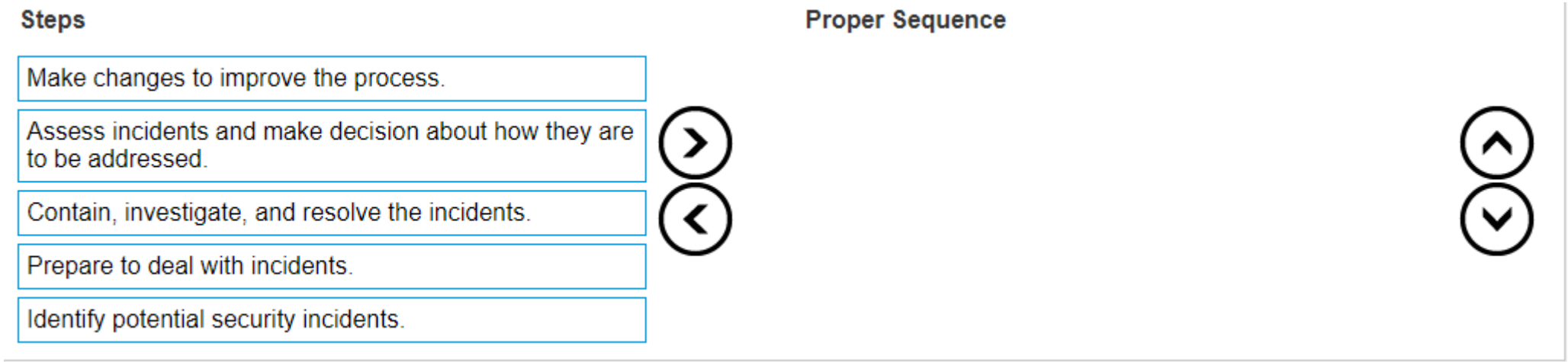
The threat intelligence team's capabilities align with the requirements of A .R.T.I.E. to address their cybersecurity challenges effectively1.

Question 5

Question Type: **OrderList**

The cybersecurity team created a detailed security incident management procedures training program to manage any probable incidents at A .R.T.I.E.

Arrange the steps in the proper sequence to best manage cybersecurity incidents.



Answer:

Prepare to deal with incidents. Identify potential security incidents. Assess

Question 6

Question Type: MultipleChoice

An A .R.T.I.E. employee received an email with an invoice that looks official for $200 for a one-year subscription. It clearly states: "Please do not reply to this email," but provides a Help and Contact button along with a phone number.

What is the type of risk if the employee clicks the Help and Contact button?

Options:

A- People

B- Technology

C- Operational

D- Strategic

Answer:

A

Explanation:

People Risk Definition: People risk involves the potential for human error or intentional actions that can lead to security incidents1.

Phishing and Social Engineering: The scenario described is typical of phishing, where attackers use seemingly official communications to trick individuals into revealing sensitive information or accessing malicious links1.

Employee Actions: Clicking on the button could potentially lead to the employee inadvertently providing access to the company's systems or revealing personal or company information1.

Dell's Security Foundations Achievement: Dell's Security Foundations Achievement emphasizes the importance of recognizing and minimizing phishing exploits as part of managing people risk21.

Mitigation Measures: Training employees to recognize and respond appropriately to phishing attempts is a key strategy in mitigating people risk1.

In this context, the risk is categorized as 'people' because it directly involves the potential actions of an individual employee that could compromise security1.

Question 7

Question Type: MultipleChoice

The security team recommends the use of User Entity and Behavior Analytics (UEBA) in order to monitor and detect unusual traffic patterns, unauthorized data access, and malicious activity of A .R.T.I.E. The monitored entities include A .R.T.I.E. processes, applications, and network devices Besides the use of UEBA, the security team suggests a customized and thorough implementation plan for the organization.

What are the key attributes that define UEBA?

Options:

A- User analytics, threat detection, and data.

B- User analytics, encryption, and data.

C- Encryption, automation, and data.

D- Automation, user analytics, and data.

Answer:

A

Explanation:

User Analytics: UEBA systems analyze user behavior to establish a baseline of normal activities and detect anomalies12.

Threat Detection: By monitoring for deviations from the baseline, UEBA can detect potential security threats, such as compromised accounts or insider threats12.

Data Analysis: UEBA solutions ingest and analyze large volumes of data from various sources within the organization to identify suspicious activities12.

Behavioral Analytics: UEBA uses behavioral analytics to understand how users typically interact with the organization's systems and data12.

Machine Learning and Automation: Advanced machine learning algorithms and automation are employed to refine the analysis and improve the accuracy of anomaly detection over time12.

UEBA is essential for A .R.T.I.E. as it provides a comprehensive approach to security monitoring, which is critical given the diverse and dynamic nature of their user base and the complexity of their IT environment12.

Question 8

Question Type: MultipleChoice

The cybersecurity team must create a resilient security plan to address threats. To accomplish this, the threat intelligence team performed a thorough analysis of the A .R.T.I.E. threat landscape. The result was a list of vulnerabilities such as social engineering, zero-day exploits, ransomware, phishing emails, outsourced infrastructure, and insider threats.

Using the information in the case study and the scenario for this question, which vulnerability type exposes the data and infrastructure of A.R.T.I.E .?

Options:

A- Malicious insider

B- Zero day exploit

C- Ransomware

D- Social engineering

Answer:

D

Question 9

Question Type: MultipleChoice

During analysis, the Dell Services team found outdated applications and operating systems with missing security patches. To avert potential cyberattacks, Dell recommends application and operating system hardening measures.

Why is security hardening important for A.R.T.I.E .?

Options:

A- Enhance operational cost.

B- Decrease attack surface.

C- Enhance productivity.

D- Remove redundancy.

Answer:

B

Explanation:

Security Hardening Definition: Security hardening involves implementing measures to reduce vulnerabilities in applications and operating systems1.

Reducing Attack Surface: By updating and patching outdated applications and operating systems, A .R.T.I.E. can minimize the number of potential entry points for attackers1.

Preventing Cyberattacks: Hardening is a proactive measure to protect against potential cyberattacks by eliminating as many security risks as possible1.

Compliance with Best Practices: Security hardening aligns with industry best practices and regulatory requirements, which is essential for A .R.T.I.E.'s operations in the public cloud1.

Dell's Recommendation: Dell's Security Foundations Achievement emphasizes the importance of security hardening as a fundamental aspect of an organization's cybersecurity strategy1.

Security hardening is crucial for A .R.T.I.E. because it directly contributes to the robustness of their cybersecurity posture, ensuring that their systems are less susceptible to attacks and breaches1.