Number: D-SF-A-24
Passing Score: 800
Time Limit: 120
File Version: 3.0

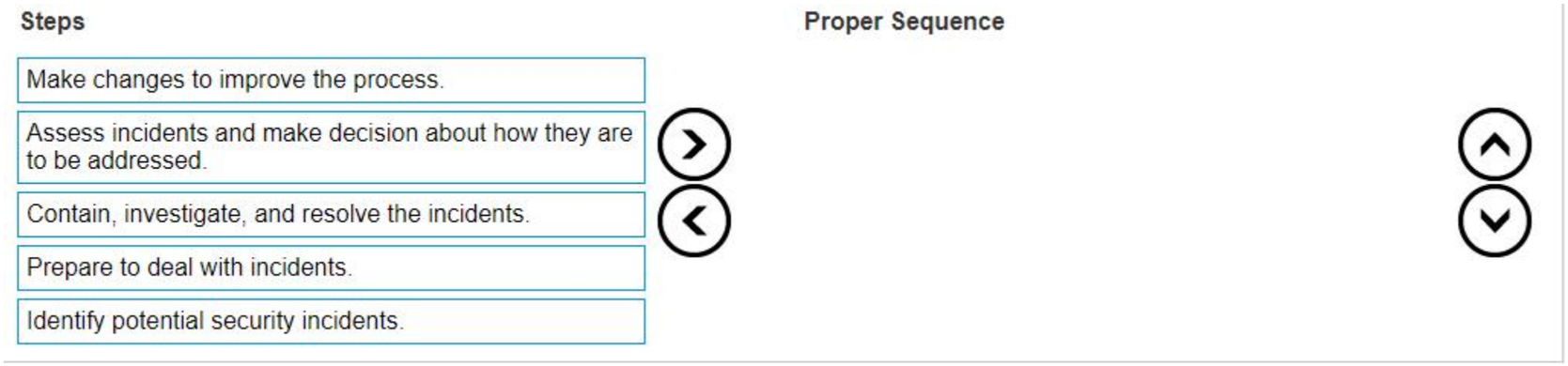
Exam Code: D-SF-A-24

Exam Name: Dell Security Foundations Achievement

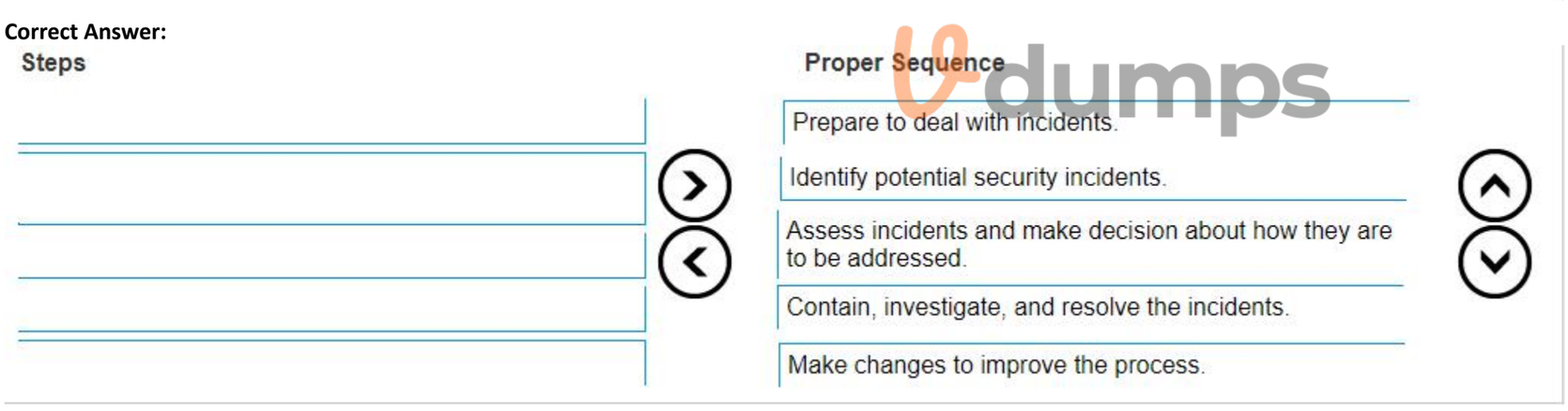
Exam A

QUESTION 1
DRAG DROP
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.

Select and Place:



Correct Answer:



Section:
Explanation:
Prepare to deal with incidents.
Identify potential security incidents.
Assess incidents and make decisions about...
Contain, investigate, and resolve the incidents.
Make changes to improve the process.

QUESTION 2
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?

A. Identity and Assess Management

B. Threat intelligence
C. Ethical hackers
D. Business advisory

Correct Answer: B
Section:
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 3
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?

A. Signature based
B. Behavior based
C. Deception based

Correct Answer: A
Section:
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
The cybersecurity team performed a quantitative risk analysis on A .R.T.I.E.'s IT systems during the risk management process.
What is the focus of a quantitative risk analysis?

A. Rank and handle risk to use time and resources more wisely.
B. Evaluators discretion for resources.
C. Knowledge and experience to determine risk likelihood.
D. Objective and mathematical models to provide risk acumens.

Correct Answer: D
Section:
Explanation:
Quantitative risk analysis in cybersecurity is a method that uses objective and mathematical models to assess and understand the potential impact of risks. It involves assigning numerical values to the likelihood of a threat occurring, the potential impact of the threat, and the cost of mitigating the risk. This approach allows for a more precise measurement of risk, which can then be used to make informed decisions about where to allocate resources and how to prioritize security measures.
The focus of a quantitative risk analysis is to provide risk acumens, which are insights into the level of risk associated with different threats. This is achieved by calculating the potential loss in terms of monetary value and the

probability of occurrence. The result is a risk score that can be compared across different threats, enabling an organization to prioritize its responses and resource allocation.
For example, if a particular vulnerability in the IT system has a high likelihood of being exploited and the potential impact is significant, the quantitative risk analysis would assign a high-risk score to this vulnerability. This would signal to the organization that they need to address this issue promptly.
Quantitative risk analysis is particularly useful in scenarios where organizations need to justify security investments or when making decisions about risk management strategies. It provides a clear and objective way to communicate the potential impact of risks to stakeholders.
In the context of the Dell Security Foundations Achievement, understanding the principles of quantitative risk analysis is crucial for IT staff and application administrators. It aligns with the topics covered in the assessment, such as security hardening, identity and access management, and security in the cloud, which are all areas where risk analysis plays a key role123.

QUESTION 5
A R.T.I.E.'s business is forecast to grow tremendously in the next year, the organization will not only need to hire new employees but also requires contracting with third-party vendors to continue seamless operations. A .R.T.I.E. uses a VPN to support its employees on the corporate network, but the organization is facing a security challenge in supporting the third-party business vendors.
To better meet A .R.T.I.E.'s security needs, the cybersecurity team suggested adopting a Zero Trust architecture (ZTA). The main aim was to move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero Trust continuously ensures that a user is authentic and the request for resources is also valid. ZTA also helps to secure the attack surface while supporting vendor access.
What is the main challenge that ZTA addresses?

A. Authorization of A .R.T.I.E. employees.
B. Malware attacks.
C. Access to the corporate network for third-party vendors.
D. Proactive defense in-depth strategy.

Correct Answer: C
Section:
Explanation:
The main challenge that Zero Trust Architecture (ZTA) addresses is the access to the corporate network for third-party vendors. ZTA is a security model that assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)12. It mandates that any attempt to access resources be authenticated and authorized within a dynamic policy context.
A .R.T.I.E.'s business model involves contracting with third-party vendors to continue seamless operations, which presents a security challenge. The traditional VPN-based approach to network security is not sufficient for this scenario because it does not provide granular control over user access and does not verify the trustworthiness of devices and users continuously2.
Implementing ZTA would address this challenge by:
Ensuring that all users, even those within the network perimeter, must be authenticated and authorized to access any corporate resources.
Providing continuous validation of the security posture of both the user and the device before granting access to resources.
Enabling the organization to apply more granular security controls, which is particularly important when dealing with third-party vendors who require access to certain parts of the network31.
This approach aligns with the case study's emphasis on securing the attack surface while supporting vendor access, as it allows A .R.T.I.E. to grant access based on the principle of least privilege, reducing the risk of unauthorized access to sensitive data and systems4.

QUESTION 6
During the analysis, the threat intelligence team disclosed a possible threat which went unnoticed when an A .R.T.I.E. employee sent their friend a slide deck containing the personal information of a colleague. The exposed information included employee first and last names, date of birth and employee ID.
What kind of attack occurred?

A. Ransomware
B. Data breach
C. Advance Persistent Threat
D. Supply chain attack

Correct Answer: B
Section:
Explanation:
A data breach occurs when confidential information is accessed or disclosed without authorization. In the scenario described, an employee unintentionally sent out a slide deck containing personal information of a colleague.

This incident falls under the category of a data breach because it involves the exposure of personal data.
The Dell Security Foundations Achievement covers a broad range of topics, including the NIST Cybersecurity Framework, ransomware, and security hardening. It aims to validate knowledge on various risks and attack vectors, as well as the techniques and frameworks used to prevent and respond to possible attacks, focusing on people, process, and technology1.
In the context of the Dell Security Foundations Achievement, understanding the nature of different types of cyber threats is crucial. A data breach, as mentioned, is an incident where information is accessed without authorization. This differs from:
A ransomware attack (A), which involves malware that encrypts the victim's files and demands a ransom for the decryption key.
An advanced persistent threat , which is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.
A supply chain attack (D), which occurs when a malicious party infiltrates a system through an outside partner or provider with access to the system and its data.
Therefore, based on the information provided and the context of the Dell Security Foundations Achievement, the correct answer is B. Data breach.

QUESTION 7
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?

A. User analytics, threat detection, and data.
B. User analytics, encryption, and data.
C. Encryption, automation, and data.
D. Automation, user analytics, and data.

Correct Answer: A
Section:
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.

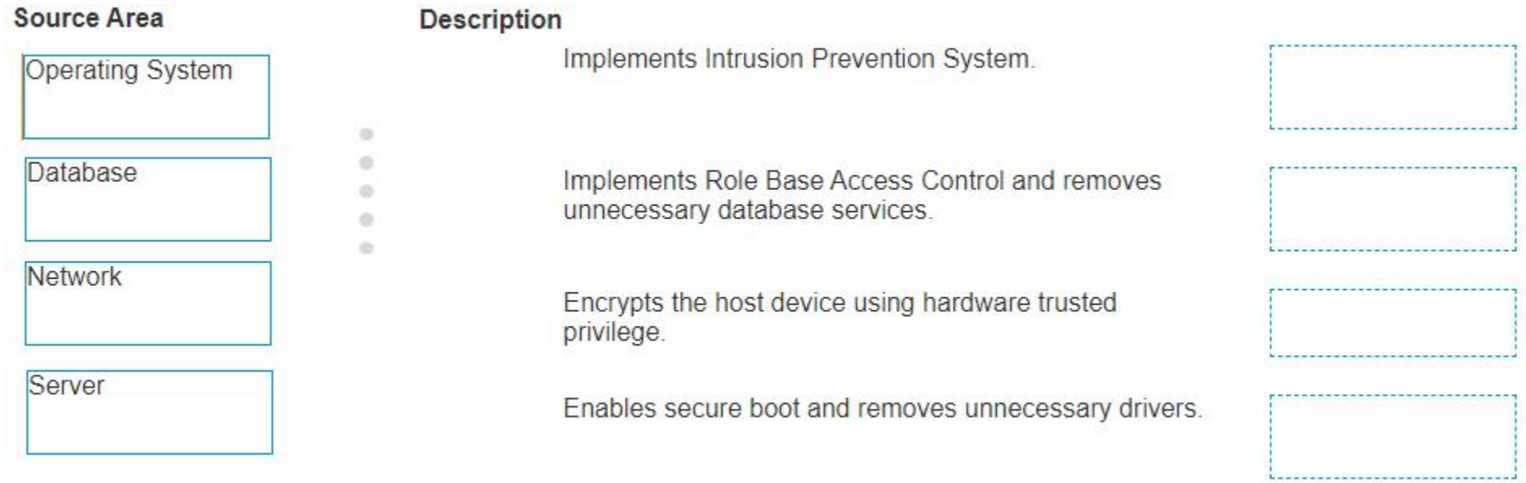
QUESTION 8
An A .R.T.I.E. employee received an email with an invoice that looks official for $200 for a one-year subscription. It clearly states: 'Please do not reply to this email,' but provides a Help and Contact button along with a phone number.
What is the type of risk if the employee clicks the Help and Contact button?

A. People
B. Technology
C. Operational
D. Strategic

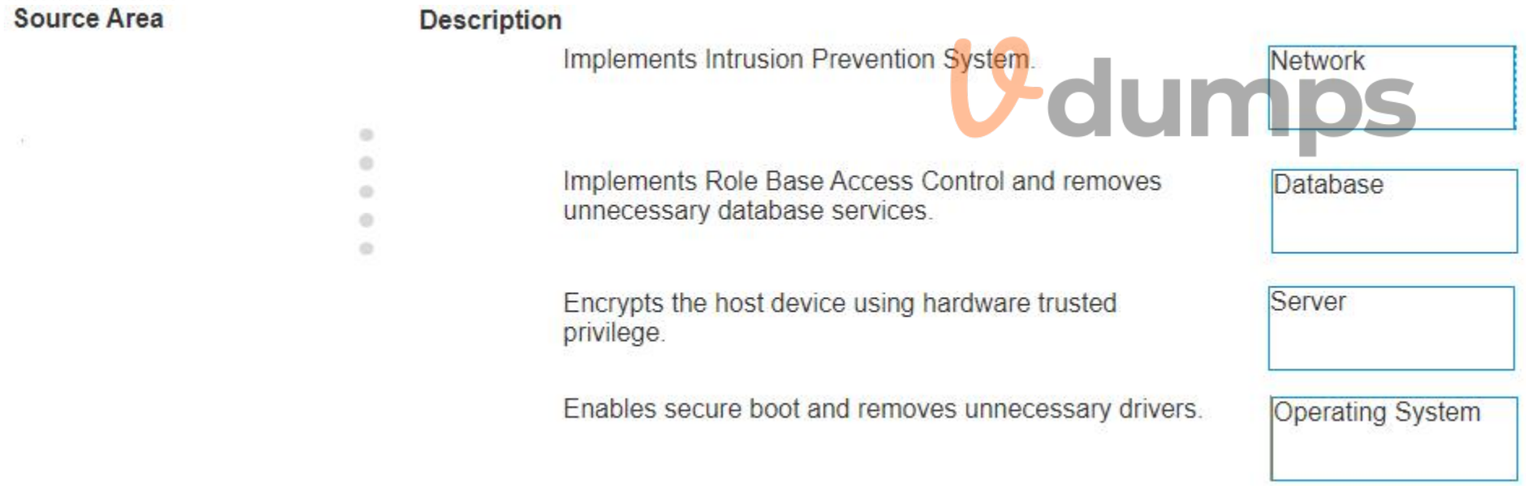
Correct Answer: A
Section:
Explanation:
People Risk Definition: People risk involves the potential for human error or intentional actions that can lead to security incidents1.
Phishing and Social Engineering: The scenario described is typical of phishing, where attackers use seemingly official communications 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 9
DRAG DROP
Match the security hardening type with the hardening techniques.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 10
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 .?

A. Malicious insider
B. Zero day exploit
C. Ransomware

D. Social engineering

Correct Answer: D
Section:

QUESTION 11
A .R.T.I.E. has an evolving need, which was amplified during the incidents. Their complex and dispersed IT environments have thousands of users, applications, and resources to manage. Dell found that the existing Identity and Access Management was limited in its ability to apply expanding IAM protection to applications beyond the core financial and human resource management application. A .R.T.I.E. also did not have many options for protecting their access especially in the cloud. A .R.T.I.E. were also not comfortable exposing their applications for remote access.
Dell recommended adopting robust IAM techniques like mapping out connections between privileged users and admin accounts, and the use multifactor authentication.

Authentication Attribute	Authentication Type	Unauthorized Use Exposure	Relative Validation Value
Password	Something you know.	May be easily stolen or guessed.	Weak. Strong if part of multi-factor authentication.
Driver's License/Passport	Something you have.	High probability that public/government issued IDs may be stolen, copied, or replicated.	Weak-Strong. Very Strong if part of multi-factor authentication.
Access card with magnetic stripe and/or IC chip	Something you have.	Privately issued/controlled ID that also contains a physical/electronic feature that cannot be easily copied or replicated. May be stolen, possibly replicated.	Strong. Very Strong if part of multi-factor authentication.
Fingerprint	Something you are.	May be easily copied and replicated.	Weak-Strong. Very Strong if part of multi-factor authentication.
Eye Retina pattern	Something you are.	Almost impossible to copy, reproduce or replicate.	Very Strong. Extremely Strong if part of multi-factor authentication.

The Dell Services team suggest implementing a system that requires individuals to provide a PIN and biometric information to access their device.
Which type of multifactor authentication should be suggested?

A. Something you have and something you are.
B. Something you have and something you know.
C. Something you know and something you are.

Correct Answer: A
Section:
Explanation:
The recommended multifactor authentication (MFA) type for A .R.T.I.E., as suggested by Dell Services, is A. Something you have and something you are. This type of MFA requires two distinct forms of identification: one that the user possesses (something you have) and one that is inherent to the user (something you are).
Something you have could be a physical token, a security key, or a mobile device that generates time-based one-time passwords (TOTPs).
Something you are refers to biometric identifiers, such as fingerprints, facial recognition, or iris scans, which are unique to each individual.
By combining these two factors, the authentication process becomes significantly more secure than using any single factor alone. The physical token or device provides proof of possession, which is difficult for an attacker to replicate, especially without physical access. The biometric identifier ensures that even if the physical token is stolen, it cannot be used without the matching biometric input.
The use of MFA is supported by security best practices and standards, including those outlined by the National Institute of Standards and Technology (NIST).
Dell's own security framework likely aligns with these standards, advocating for robust authentication mechanisms to protect against unauthorized access, especially in cloud environments where the attack surface is broader.
In the context of A .R.T.I.E.'s case, where employees access sensitive applications and data remotely, implementing MFA with these two factors will help mitigate the risk of unauthorized access and potential data breaches. It is a proactive step towards enhancing the organization's security posture in line with Dell's strategic advice.

QUESTION 12
A Zero Trust security strategy is defined by which of the primary approaches?

A. IAM and security awareness training

B. VPNs and IAM
C. Network segmenting and access control
D. Micro-segmenting and Multi-factor authentication

Correct Answer: D
Section: