ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Dell EMC

Code: D-SF-A-24

Exam: Dell Security Foundations Achievement

https://www.examsnest.com/exam/d-sf-a-24/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

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.

Answer: A

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).
Explanation:
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.
Reference:
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: 2

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

Answer: D

Explanation:

Question: 3

To optimize network performance and reliability, low latency network path for customer traffic, A.R.T.I.E created a modern edge solution. The edge solution helped the organization to analyze and process diverse data and identify related business opportunities. Edge computing also helped them to create and distribute content and determine how the users consume it. But as compute and data creation becomes more decentralized and distributed, A .R.T.I.E. was exposed to various risks and security challenges inevitably became more complex. Unlike the cloud in a data center, it is physically impossible to wall off the edge.

Which type of edge security risk A .R.T.I.E. is primarily exposed?

A. Data risk
B. Internet of Things risk
C. Protection risk
D. Hardware risk

Answer: A

Explanation:

For the question regarding the type of edge security risk A .R.T.I.E. is primarily exposed to, let's analyze the options:
Data risk: This refers to the risk associated with the storage, processing, and transmission of data. Given that A .R.T.I.E. is a social media company with a platform for sharing content and making in-app purchases, there is a significant amount of data being handled, which could be at risk if not properly secured.
Internet of Things (IoT) risk: This involves risks associated with IoT devices, which may not be applicable in this context as A .R.T.I.E. is described as a social media company rather than one that specializes in IoT devices.
Protection risk: This could refer to the overall security measures in place to protect the company's assets. Since A .R.T.I.E. has moved some applications to the public cloud and operates an internal network accessible via VPN, the protection of these assets is crucial.
Hardware risk: This involves risks related to the physical components of the network. The case study does not provide specific details about hardware vulnerabilities, so this may not be the primary concern.
Considering the case study's focus on data handling, cloud migration, and the need for secure solutions, Data risk seems to be the most relevant edge security risk A .R.T.I.E. is exposed to. The decentralization of compute and data creation, along with the inability to physically secure the edge as one would with a data center, increases the risk to the data being processed and stored at the edge.
Remember, when preparing for assessments like the Dell Security Foundations Achievement, it's important to thoroughly review the study materials provided, understand the key concepts, and apply them to the scenarios presented in the case studies. Good luck with your preparation!

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.

Answer: D

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.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Dell EMC

Code: D-SF-A-24

Exam: Dell Security Foundations Achievement

https://www.examsnest.com/exam/d-sf-a-24/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation