PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **D-SF-A-24**

Title : Dell Security Foundations Achievement

Vendor : EMC

Version : DEMO

NO.1 AnA .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
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.
==========
Topic 1, Case Study Scenario
It is recommended that you read through the case study before answering any questions. You can always return to the case study while viewing any of the twenty questions.
Introduction
As the threat landscape has grown over past years and continues to evolve unpredictably, cyber-attacks on organizations are now unavoidable. Security is no longer about averting attacks; it is all about preparing for them.
In recent years, large corporate data breaches have impacted millions of customers and revealed personal information that can be used in follow-on crimes. The longer a cyber-attack goes unnoticed, the more damage it does to the business and the more money and time it will cost to recover. Hackers steal financial, medical, and other sensitive information to sell online or use in cybercrimes. This unpredictable security threat landscape has resulted in a challenging scenario for all organizations.
Business Description

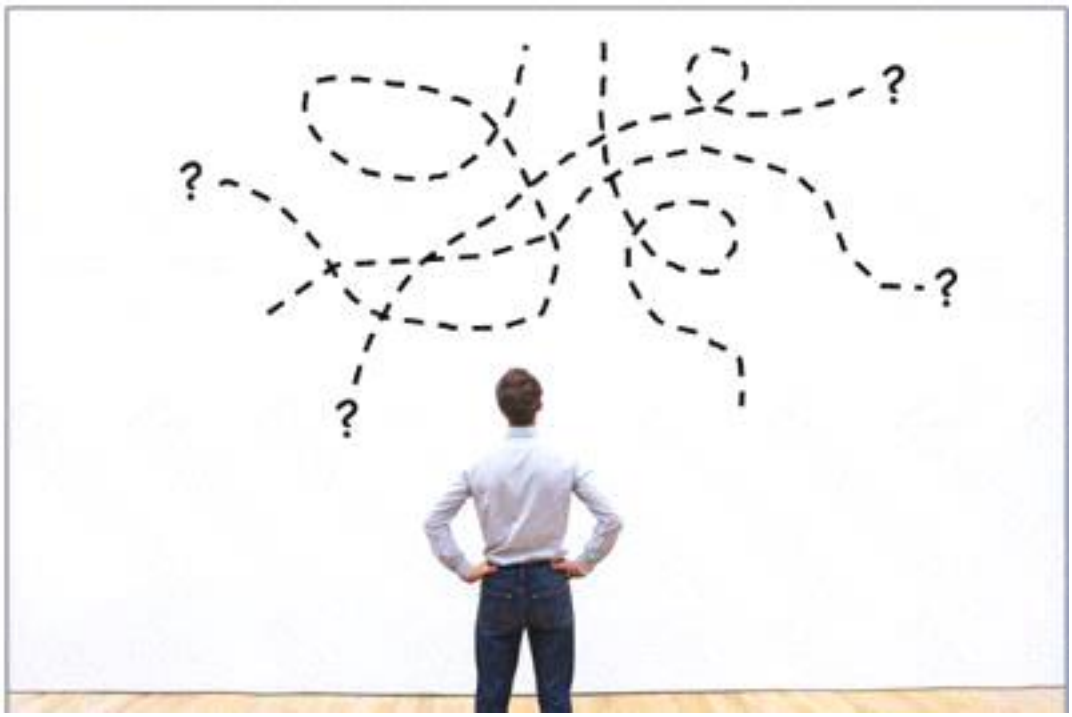
A:R.T.I.E.is a midsize social media company whose key customers are 18- to 28-year-olds. Using the organization's platform, customers can share content such as photos, videos and post status updates and views.

The organization has a in-built messenger app that helps users to interact. The platform also has an option to make in-app purchases and play games with other users.

One key characteristic ofA .R.T.I.E.is that it supports social influencers and has attracted large firms as advertisers.

With 450 employees, who work from different locations, the main goal ofA .R.T.I.E.is to provide high quality of services to a user base of 15K individuals and associates. The employees have access to the apps, platform, data, and systems through an internal network that uses a virtual private network (VPN) to secure access from remote locations.

Business Problem



Senior management ofA .R.T.I.E.expects the core business to continue to grow rapidly due to an

increase in user traffic and increased demand of its advertising platform especially by big organizations.
Based on their current business-critical needs for their solutions and client base, the organization is planning to move towards a global operational geography and have migrated some of its key applications to the public cloud. Deployment of the applications to the public cloud provides:
. Ability to scale.
. Higher data transfer speeds and more efficient access management.
. Faster time-to-market and better control of IT costs.
However, with progress comes new challenges as public cloud environments broaden the attack surface from which attackers can try to gain unauthorized access to an organization's resources.A .R.T.I.E.also must comply with various regulations and cloud security controls and have to come up with holistic security capabilities that ensure security across the organization, core-to-edge-to-cloud.
Even though the IT team of the organization constantly monitor their IT environment and assets along with watching for unauthorized profiles, information disclosure, fake accounts, and other threats, the CIO of A.R.I.T.E. is aware that the nature of their business being an open platform makes them a prime target for attackers and other cybercriminals.
Due to the growing business and untrained employees, the organization is constantly under the fear of threat.
This fear increased tenfold when they had discovered two back-to-back cyberattacks resulting in unauthorized access to databases containing user information.
In the first attack, the attackers performed data theft techniques to exfiltrate vulnerable information and held internal systems for ransom. This incident led to the company negotiating a ransom payment to recover data.
Also, an unexplained surge in requests to a single webpage occurred along with unusual network traffic patterns which indicated a second attack. These attacks were concerning not only for the financial impact but also for the amount of data exposed.
Requirements
The key requirements to address the primary challenges to the business includes:
. Understanding the cyber threat landscape specific to the organizational risk tolerance.
. Secure migration of applications to the public cloud.
. Implement a suitable security framework to tackle current and emerging threats.
. Identify possible vulnerabilities and threats.
. Create an incident management plan based on knowledge, experience, and real-time information to prevent future attacks.
. Learn about the tools and technologies used to avert the attacks and determine which tools will be appropriate for them.
. Take measures to implement secure solutions and control: Zero Trust, Security hardening, IAM techniques.
Dell Services Team

To improve the overall cyber security posture and implement better security policies as the company grows,A.R.T.I.E.contacted Dell Services.

Dell clients use their services and solutions to collectively monitor thousands of devices, systems, and applications. Some clients have a significant workforce with minimal IT knowledge, which opens greater security risks and technological gaps.

Strategic advisory team

. Commonly known as the core security team which has a global presence.

. Helps organizations to evaluate and gauge their exposure to cybersecurity risk.

. Supports various organizations in developing a vision and strategy for handling cyberattacks.

. Provides advice on the implementation of standard cybersecurity frameworks.

Ethical hackers

. Works within the defined boundaries to legally infiltrate the organization's network environment with their permission.

. Exposes vulnerabilities in customers IT systems.

Threat intelligence and incident management team

. The team help to keep the organization apprised of the latest developments in the security landscape.

. The cyber security intelligence team investigates methodologies and technologies to help organizations detect, understand, and deflect advanced cybersecurity threats and attacks on their IT infrastructure, and in the cloud.

. The incident management team helps consider what they would do when under attack. The team may simulate an attack to ensure that non-technical staff members know how to respond.

. The simulated attack is managed by the incident management team. This team also helps to prevent future attacks based on the information gathered.

Identity and Access Management team

. Reviews and accesses the access rights for each member and user.

. During their analysis the Dell cyber team did a thorough analysis to help create a secure environment for A.R.T.I.E.and mitigate potential attacks.

Outcomes

With the rapid and thorough analysis of security events originating from both internal and external sources to A.R.T.I.E.complete, the Dell Services team could detect anomalies, uncover advanced

threats and remove false positives. The Threat Intelligence team was also able to provide a list of potentially malicious IP addresses, malware, and threat actors.
Along with this, the team also implemented methods that helped determine what is being attacked and how to stop an attack providingA .R.T.I.E.with real time threat detection mechanisms, knowledge on cyber security.
The common outcomes after implementation of the Dell recommendations were:
. Prioritization of threat and impact - Determine threat intelligence, vulnerability status and network communications to evaluate accurate vulnerability risk.
. Secure workforce and educate employees about best practices to be adopted to mitigate attacks, security frameworks and policies.
. Implementation of incident management plan and build an organization-wide security strategy to avert future attacks.
. Identification of at-risk users and authorized users, account takeover, disgruntled employees, malware actions.
. Streamlining of security solutions while reducing operational costs and staffing requirements.
. Increased effectiveness to address the continual growth of IT environments, along with the sharp rise in the number of threats and attacks.
The objective was to consolidate data from the organization's multiple sources such as: networks, servers, databases, applications, and so on; thus, supports centralized monitoring.

NO.2 The cybersecurity team must create a resilient security plan to address threats. To accomplish this, the threat intelligence team performed a thorough analysis of theA .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
Answer: D

NO.3 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 forA .R.T.I.E., as suggested by Dell Services, isA.
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 havecould be a physical token, a security key, or a mobile device that generates time-based one-time passwords (TOTPs).
* Something you arerefers 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.
References:
* 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 ofA .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.