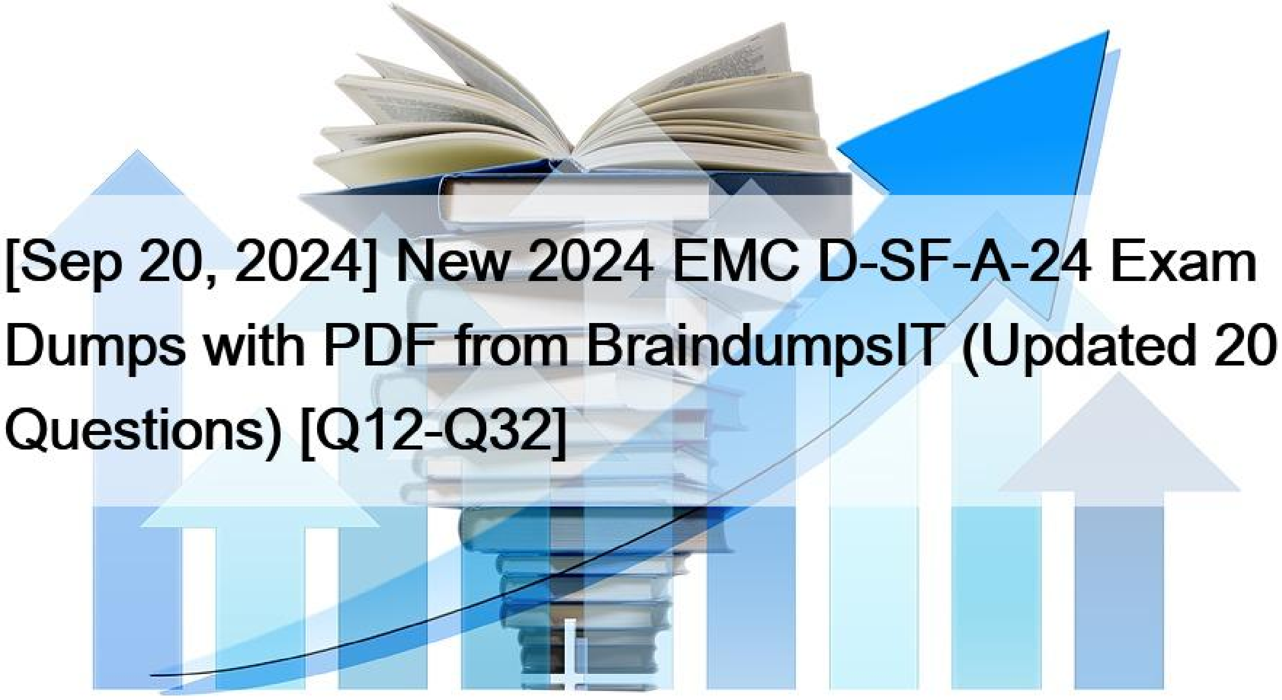
[Sep 20, 2024 New 2024 EMC D-SF-A-24 Exam Dumps with PDF from BraindumpsIT (Updated 20 Questions) [Q12-Q32



New 2024 D-SF-A-24 exam questions Welcome to download the newest BraindumpsIT D-SF-A-24 PDF dumps (20 Q&As) P.S. Free 2024 Dell Security D-SF-A-24 dumps are available on Google Drive shared by BraindumpsIT NO.12 In the cloud, there are numerous configuration options for the services provided. If not properly set, these configurations can leave the environment in an unsecure state where an attacker can read and modify the transmitted data packets and send their own requests to the client.

Which types of attack enable an attacker to read and modify the transmitted data packets and send their own requests to the client?
* Data loss
* Shared technology
* TCP hijacking
* Dumpster diving
Verified answer:The type of attack that enables an attacker to read and modify the transmitted data packets and send their own requests to the client is:C. TCP hijacking

* TCP Hijacking Definition:TCP hijacking is a type of cyber attack where an attacker takes control of a communication session

between two entities12.

* Attack Mechanism:The attacker intercepts and manipulates data packets being sent over the network, allowing them to read, modify, and insert their own packets into the communication stream1.

* Impact on Security:This attack can lead to unauthorized access to sensitive data and systems, and it can

* be used to impersonate the victim, resulting in data breaches and other security incidents1.

* Prevention Measures:Implementing security measures such as encryption, using secure protocols, and monitoring network traffic can help prevent TCP hijacking attacks1.

TCP hijacking is particularly relevant to cloud environments where misconfigurations can leave systems vulnerable. It is crucial forA .R.T.I.E.to ensure proper security configurations and adopt measures to protect against such attacks as part of their migration to the public cloud and overall cybersecurity strategy12.

NO.13 The cybersecurity team performed a quantitative risk analysis onA .R.T.I.E.&#8217;s IT systems during the risk management process.

What is the focus of a quantitative risk analysis?
* Rank and handle risk to use time and resources more wisely.
* Evaluators discretion for resources.
* Knowledge and experience to determine risk likelihood.
* Objective and mathematical models to provide risk acumens.
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-riskscore 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.

NO.14 A Zero Trust security strategy is defined by which of the primary approaches?
* IAM and security awareness training
* VPNs and IAM
* Network segmenting and access control

* Micro-segmenting and Multi-factor authentication
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&#8217;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&#8217;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&#8217;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 &#8211; 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&#8217;s multiple sources such as: networks, servers, databases, applications, and so on; thus, supports centralized monitoring.

NO.15 An externalA .R.T.I.E.user requires access to sensitive resources and data.

Which authentication technique should be best recommended to provide access to this business user?
* Two-factor
* Privileged Access Management
* Multifactor
* Single Sign-On
* Multifactor Authentication (MFA) Definition:MFA requires users to provide multiple forms of identification before gaining access to a resource1.

* Security Enhancement:MFA enhances security by combining something the user knows (like a password), something the user has (like a smartphone), and something the user is (like a fingerprint)1.

* Protection Against Unauthorized Access:This method protects against unauthorized access by ensuring that even if one factor (like a password) is compromised, the attacker still needs the other factors to gain access1.

* Compliance with Regulations:MFA helps organizations comply with various regulations and cloud security controls, which is essential forA .R.T.I.E.as they move to the public cloud1.

* Dell&#8217;s Commitment to MFA:Dell&#8217;s own security guidelines emphasize the importance of MFA, reflecting their commitment to safeguarding data integrity and providing an additional layer of security during the sign-in process1.

MFA is particularly suitable forA .R.T.I.E.&#8217;s scenario because it provides robust security for accessing sensitive resources and data, which is crucial for external users who may not be within the secure internal network1.

NO.16 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 ofA .R.T.I.E.The monitored entities includeA .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?
* User analytics, threat detection, and data.
* User analytics, encryption, and data.
* Encryption, automation, and data.
* Automation, user analytics, and data.
* 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.

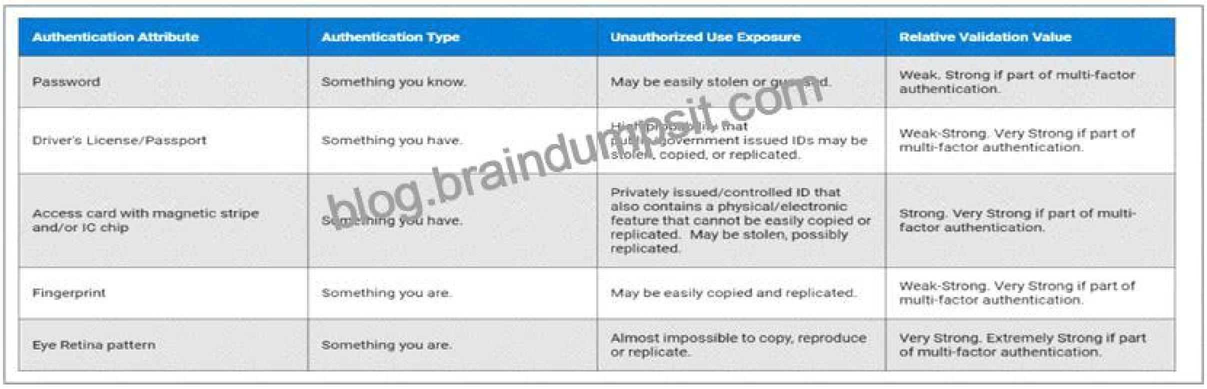
* Behavioral Analytics:UEBA uses behavioral analytics to understand how users typically interact with the organization&#8217;s systems and data12.

* 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 forA .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.

NO.17 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?
* Something you have and something you are.
* Something you have and something you know.
* Something you know and something you are.
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&#8217;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.&#8217;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&#8217;s security posture in line with Dell&#8217;s strategic advice.

NO.18 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 .?
* Malicious insider
* Zero day exploit
* Ransomware
* Social engineering

NO.19 Which framework should be recommended toA .R.T.I.E.to enhance the overall security and resilience of their critical infrastructure, and outline methods to reduce their cybersecurity risk?
* NIST CSF
* COBIT
* PCIDSS
* HIPAA
Based on the case study provided and the requirements forA .R.T.I.E., the most suitable framework to enhance the overall security and resilience of their critical infrastructure, and to outline methods to reduce their cybersecurity risk would be:A. NIST CSF TheNIST Cybersecurity Framework (CSF)is recommended forA .R.T.I.E.to enhance security and resilience.The NIST CSF provides guidelines for organizations to manage cybersecurity risks in a structured and prioritized manner12.

* Identify:A .R.T.I.E.can use the NIST CSF to identify its digital assets, cybersecurity policies, and the current threat landscape1.

* Protect:Implement protective technology to ensure that critical infrastructure services are not disrupted1.

* Detect:Use the framework to implement advanced detection processes to quickly identify cybersecurity events1.

* Respond:Develop and implement appropriate activities to take action regarding a detected cybersecurity incident1.

* Recover:Plan for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident1.

The NIST CSF aligns withA .R.T.I.E.&#8217;s need for a secure migration to the public cloud and addresses the need for a holistic security capability that ensures security across the organization2.It also supports the Zero Trust model, which is crucial forA .R.T.I.E.&#8217;s open platform nature1.

D-SF-A-24 exam questions from BraindumpsIT dumps: https://www.braindumpsit.com/D-SF-A-24_real-exam.html (20 Q&As)]