IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

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

Title : Dell Security Foundations Achievement

Version : DEMO

1. Topic 1, Case Study Scenario

Overview

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.

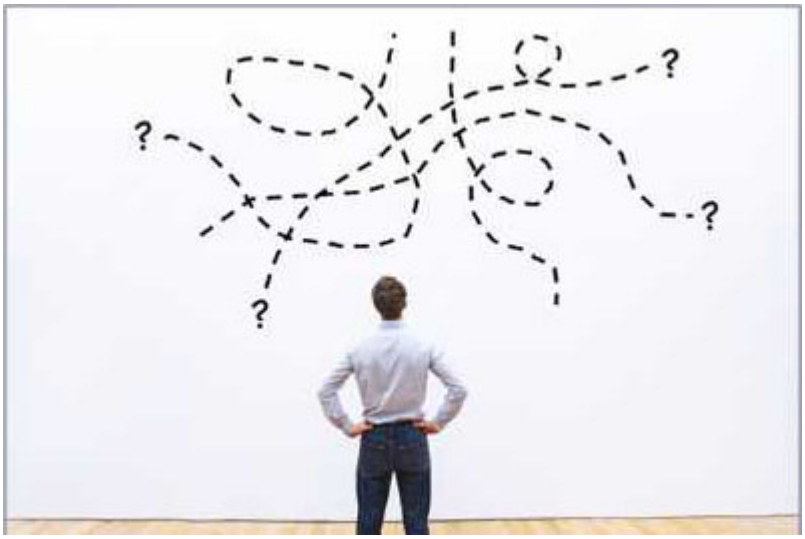
Business Description

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 of A.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 of A.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 of A.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 providing A.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.

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).
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.

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

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!

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.

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.

Answer: C

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.