PassQueen
a.k.a dumpsqueen.com

Dell Security Foundations Achievement

EMC D-SF-A-24

Version Demo

Total Demo Questions: 4

Total Premium Questions: 44

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A.R.T.I.E. has limited historical loss data for a newly deployed service. The risk team uses workshops with technical and business stakeholders to rate the likelihood of an incident as High, Medium, or Low and to rate the expected business impact using the same scale.

Which type of risk analysis is being performed?

A. Quantitative risk analysis

B. Qualitative risk analysis

C. Vulnerability assessment

D. Business impact analysis

ANSWER: B

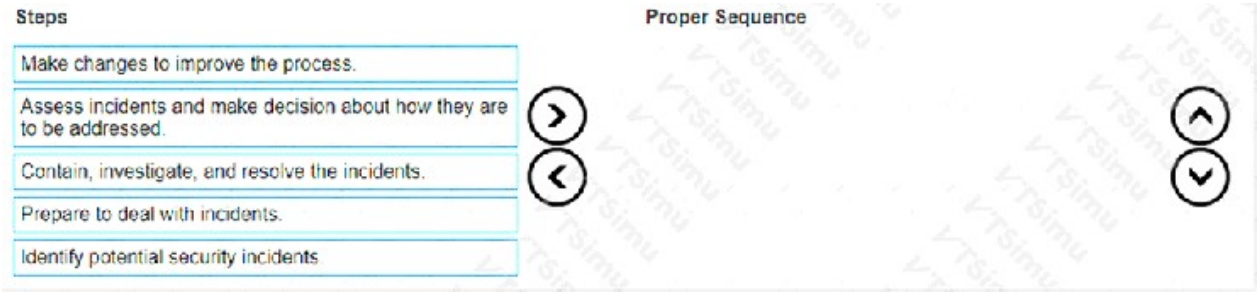
Explanation:

Qualitative risk analysis is correct because the organization is using descriptive ratings and stakeholder judgment to evaluate likelihood and impact. This approach is useful when reliable financial-loss figures, event frequencies, or other numerical data are unavailable. Quantitative analysis uses measurable values and mathematical models, such as estimated financial loss and annual rate of occurrence.

QUESTION NO: 2 - (SIMULATION)

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.



ANSWER: Check the explanation for the answer

Explanation:

Arrange the incident-management steps in this order:

This follows the incident response lifecycle: preparation, detection/identification, assessment and decision, containment/investigation/resolution, then post-incident improvement.

QUESTION NO: 3

A.R.T.I.E. requires multifactor authentication for remote access. An attacker obtains an employee's password through a phishing email and then repeatedly sends authentication approval prompts to the employee's mobile device. The employee eventually approves one prompt to stop the notifications.

Which control would most directly reduce the risk of this attack succeeding?

A. Require password changes at shorter intervals

B. Use phishing-resistant MFA that requires user verification of the sign-in request

C. Allow push approvals without displaying sign-in context

D. Disable logging for failed authentication requests

ANSWER: B

Explanation:

Phishing-resistant MFA that requires user verification of the sign-in request is correct because it reduces reliance on a user approving an unsolicited push notification. Methods such as FIDO2 security keys use cryptographic authentication and are designed to resist credential phishing. Password-expiration policies do not stop an attacker who already has a current password, and additional push prompts can increase the opportunity for approval fatigue rather than reduce it.

QUESTION NO: 4

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

Explanation:

Social engineering is the vulnerability type that exposes an organization’s data and infrastructure because it targets the human element that protects technical systems. An attacker may manipulate an employee, contractor, or trusted partner into revealing credentials, approving a fraudulent request, opening a malicious attachment, or disclosing sensitive operational information. Once the attacker obtains legitimate access or persuades a user to perform an unsafe action, the attacker can move beyond the initial interaction and reach organizational data, cloud resources, applications, and infrastructure-management systems. This makes social engineering especially significant in a resilient security plan: technical controls must be paired with security awareness, identity verification processes, multifactor authentication, least-privilege access, and procedures for reporting suspicious communications. The Cybersecurity and Infrastructure Security Agency describes social-engineering attacks as efforts to exploit human behavior to gain access to information or systems, and emphasizes awareness and verification as defenses. Guidance from the National Institute of Standards and Technology also identifies awareness and training as an essential component of managing cybersecurity risk. See CISA guidance on avoiding social engineering and phishing attacks and NIST Cybersecurity Framework.