CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication

Which of the following is the best way for the security officer to restrict MI~A notifications\\'\\'

A. Provisioning FID02 devices

B. Deploying a text message based on MFA

C. Enabling OTP via email

D. Configuring prompt-driven MFA

Correct Answer: D

Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:

A. Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication, they may not be practical for all users and do not directly address the issue of excessive push notifications.

B. Deploying a text message-based MFA: SMS-based MFA can still be vulnerable to similar spamming attacks and phishing.

C. Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications. D. Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner,

often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts. Configuring prompt-driven MFA is

the best solution to restrict unnecessary MFA notifications and improve security.

References:

CompTIA Security+ Study Guide

NIST SP 800-63B, "Digital Identity Guidelines"

"Multi-Factor Authentication: Best Practices" by Microsoft

QUESTION 2

Which of the following industrial protocols is most likely to be found in public utility applications, such as water or electric?

A. CIP

B. Zigbee

C. Modbus

D. DNP3

Correct Answer: D

DNP3 (Distributed Network Protocol 3) is specifically designed for use in SCADA (Supervisory Control and Data Acquisition) systems, which are commonly employed in public utility sectors such as water and electric utilities. DNP3 is known for its robustness in handling communication over long distances and in noisy environments typical of utility operations. It supports features essential for reliable and secure communication, including time synchronization, data integrity checks, and error recovery mechanisms. These capabilities make DNP3 highly suitable for monitoring and controlling remote devices and systems critical to public utilities.

QUESTION 3

Company A and Company D ate merging Company A\\'s compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed.

Which of the following should me analyst cons