CompTIA

SY0-701 Exam

CompTIA Security+ Certification Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

ZTA utilizes which of the following to improve the network's security posture?

A. Micro-segmentation and encryption
B. Compliance analytics and network communication
C. Network communication and micro-segmentation
D. Encryption and compliance analytics

Answer: A

Explanation:

Verified Answer =

A) Micro-segmentation and encryption Very Short Explanation = ZTA uses micro-segmentation to divide the network into smaller, isolated segments that can prevent unauthorized access and contain lateral movement. ZTA also uses encryption to protect data in transit and at rest from eavesdropping and tampering. Reference = 1, 2, 3, 4

Question: 2

Scenario: A multinational org uses ZTA to enhance security. They collaborate with third-party service providers for remote access to specific resources. How can ZTA policies authenticate third-party users and devices for accessing resources?

A. ZTA policies can implement robust encryption and secure access controls to prevent access to services from stolen devices, ensuring that only legitimate users can access mobile services.
B. ZTA policies should prioritize securing remote users through technologies like virtual desktop infrastructure (VDI) and corporate cloud workstation resources to reduce the risk of lateral movement via compromised access controls.
C. ZTA policies can be configured to authenticate third-party users and their devices, determining the necessary access privileges for resources while concealing all other assets to minimize the attack surface.
D. ZTA policies should primarily educate users about secure practices

and promote strong authentication for services accessed via mobile devices to prevent data compromise.

Answer: C

Explanation:

ZTA is based on the principle of never trusting any user or device by default, regardless of their location or ownership. ZTA policies can use various methods to verify the identity and context of third-party users and devices, such as tokens, certificates, multifactor authentication, device posture assessment, etc. ZTA policies can also enforce granular and dynamic access policies that grant the minimum necessary privileges to third-party users and devices for accessing specific resources, while hiding all other assets from their view. This reduces the attack surface and prevents unauthorized access and lateral movement within the network.

Question: 3

Which ZT tenet is based on the notion that malicious actors reside inside and outside the network?

A. Assume breach
B. Assume a hostile environment
C. Scrutinize explicitly
D. Requiring continuous monitoring

Answer: A

Explanation:

The ZT tenet of assume breach is based on the notion that malicious actors reside inside and outside the network, and that any user, device, or service can be compromised at any time. Therefore, ZT requires continuous verification and validation of all entities and transactions, and does not rely on implicit trust or perimeter-based defenses

Question: 4

During ZT planning, which of the following determines the scope of the target state definition? Select the best answer.

A. Risk appetite
B. Risk assessment
C. Service level agreements
D. Risk register

Answer: B

Explanation:

Risk assessment is the process of identifying, analyzing, and evaluating the risks that an organization faces in achieving its objectives. Risk assessment helps to determine the scope of the target state definition for ZT planning, as it identifies the critical assets, threats, vulnerabilities, and impacts that need to be addressed by ZT capabilities and activities. Risk assessment also helps to prioritize and align the ZT planning with the organization's risk appetite and tolerance levels.

Question: 5

Of the following options, which risk/threat does SDP mitigate by mandating micro-segmentation and implementing least privilege?

A. Identification and authentication failures
B. Injection
C. Security logging and monitoring failures
D. Broken access control

Answer: D

Explanation:

SDP mitigates the risk of broken access control by mandating micro-segmentation and implementing least privilege. Micro-segmentation divides the network into smaller, isolated segments that can prevent unauthorized access and contain lateral movement. Least privilege grants the minimum necessary access to users and devices for specific resources, while hiding all other assets from their view. This reduces the attack surface and prevents attackers from exploiting weak or misconfigured access controls