CCZT$^{Q\&As}$

Certificate of Competence in Zero Trust (CCZT)

Pass Cloud Security Alliance CCZT Exam with 100% Guarantee

QUESTION 1

Network architects should consider__________ before selecting an SDP model.

Select the best answer.

A. leadership buy-in

B. gateways

C. their use case

D. cost

Correct Answer: C

Different SDP deployment models have different advantages and disadvantages depending on the organization\\'s use case, such as the type of resources to be protected, the location of the clients and servers, the network topology, the

scalability, the performance, and the security requirements. Network architects should consider their use case before selecting an SDP model that best suits their needs and goals.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 21, section 3.1.2 6 SDP Deployment Models to Achieve Zero Trust | CSA, section "Deployment Models Explained"

Software-Defined Perimeter (SDP) and Zero Trust | CSA, page 7, section 3.1 Why SDP Matters in Zero Trust | SonicWall, section "SDP Deployment Models"

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.

Correct Answer: C

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

For ZTA, what should be used to validate the identity of an entity?

A. Password management system

B. Multifactor authentication

C. Single sign-on

D. Bio-metric authentication

Correct Answer: B

Multifactor authentication is a method of validating the identity of an entity by requiring two or more factors, such as something the entity knows (e.g., password, PIN), something the entity has (e.g., token, smart card), or something the entity is (e.g., biometric, behavioral). Multifactor authentication enhances the security of Zero Trust Architecture (ZTA) by reducing the risk of identity compromise and unauthorized access. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 4: Identity and Access Management

QUESTION 4

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

Correct Answer: D

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

QUESTION 5

What should an organization\\'s data and asset classification be based on?

A. Location of data

B. History of data

C. Sensitivity of data

D. Recovery of data

Correct Answer: C

Data and asset classification should be based on the sensitivity of data, which is the degree to which the data requires protection from unauthorized access, modification, or disclosure. Data sensitivity is determined by the potential impact of data loss, theft, or corruption on the organization, its customers, and its partners. Data sensitivity can also be influenced by legal, regulatory, and contractual obligations. References: Certificate of Competence in Zero Trust (CCZT) prepkit, page 10, section 2.1.1 Identify and protect sensitive business data with Zero Trust, section 1 Secure data with Zero Trust, section 1 SP 800-207, Zero Trust Architecture, page 9, section 3.2.1