Vendor: Cloud Security Alliance

Exam Code:CCZT

Exam Name: Certificate of Competence in Zero Trust (CCZT)

Version: Demo

QUESTION 1

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 2

How can we use ZT to ensure that only legitimate users can access a SaaS or PaaS? Select the best answer.

A. Implementing micro-segmentation and mutual Transport Layer Security (mTLS)

B. Configuring the security assertion markup language (SAML) service provider only to accept requests from the designated ZT gateway

C. Integrating behavior analysis and geofencing as part of ZT controls

D. Enforcing multi-factor authentication (MFA) and single-sign on (SSO)

Correct Answer: B

(Configuring the security assertion markup language (SAML) service provider only to accept requests from the designated ZT gateway) Explanation: Configuring SAML to accept requests only from the designated ZT gateway ensures that all access requests are authenticated and authorized appropriately. References: Zero Trust Architecture related sources including NIST

QUESTION 3

When kicking off ZT planning, what is the first step for an organization in defining priorities?

A. Determine current state

B. Define the scope

C. Define a business case

D. Identifying the data and assets

Correct Answer: A

The first step for an organization in defining priorities for ZT planning is to determine the current state of its network, security, and business environment. This involves conducting a comprehensive assessment of the existing IT infrastructure, systems, applications, data, and assets, as well as the threats, risks, and vulnerabilities that affect them. The current state analysis also involves identifying the gaps, challenges, and opportunities for improvement in the current security posture, as well as the business goals, objectives, and requirements for ZT implementation12. By determining the current state, the organization can establish a baseline for measuring the progress and impact of ZT, as well as prioritize the most critical and urgent areas for ZT adoption. References: Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators | CSRC Publications NIST Zero Trust Architecture Explained: A Step-by-Step Approach - Comparitech

---

QUESTION 4

Which vital ZTA component enhances network security and simplifies management by creating boundaries between resources in the same network zone?

A. Micro-segmentation

B. Session establishment or termination

C. Decision transmission

D. Authentication request/validation request (AR/VR)

Correct Answer: A

Micro-segmentation is a vital ZTA component that enhances network security and simplifies management by creating boundaries between resources in the same network zone. Micro-segmentation divides the network into smaller segments or zones based on the attributes and context of the resources, such as data sensitivity, application functionality, user roles, etc. Micro-segmentation helps to isolate and protect the resources from unauthorized access and lateral movement of attackers within the same network zone. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 6: Micro-segmentation

---

QUESTION 5

How can device impersonation attacks be effectively prevented in a ZTA?

A. Strict access control

B. Micro-segmentation

C. Organizational asset management

D. Single packet authorization (SPA)

Correct Answer: D

SPA is a security protocol that prevents device impersonation attacks in a ZTA by hiding the network infrastructure from unauthorized and unauthenticated users. SPA uses a single encrypted packet to convey the user\\'s identity and request access to a resource. The SPA packet must be digitally signed and authenticated by the SPA server before granting access. This ensures that only authorized devices can send valid SPA packets and prevents spoofing, replay, or brute-force attacks12.

References:

Zero Trust: Single Packet Authorization | Passive authorization Single Packet Authorization | Linux Journal

---

QUESTION 6

When planning for a ZTA, a critical product of the gap analysis process is______ Select the best answer.

A. a responsible, accountable, consulted, and informed (RACI) chart and communication plan

B. supporting data for the project business case

C. the implementation\\'s requirements

D. a report on impacted identity and access management (IAM) infrastructure

Correct Answer: C

A critical product of the gap analysis process is the implementation\\'s requirements, which are the specifications and criteria that define the desired outcomes, capabilities, and functionalities of the ZTA. The implementation\\'s requirements are

derived from the gap analysis, which identifies the current state, the target state, and the gaps between them. The implementation\\'s requirements help to guide the design, development, testing, and deployment of the ZTA, as well as the

evaluation of its effectiveness and alignment with the business objectives and needs.

References:

Zero Trust Planning - Cloud Security Alliance, section "Scope, Priority, and Business Case"

The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section "Second Phase: Assess"

Planning for a Zero Trust Architecture: A Planning Guide for Federal ..., section "Gap Analysis"

QUESTION 7

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

Correct Answer: B

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 8

What is the function of the rule-based security policies configured on the policy decision point (PDP)?

A. Define rules that specify how information can flow

B. Define rules that specify multi-factor authentication (MFA) requirements

C. Define rules that map roles to users

D. Define rules that control the entitlements to assets

Correct Answer: D

Rule-based security policies are a type of attribute-based access control (ABAC) policies that define rules that control the entitlements to assets, such as data, applications, or devices, based on the attributes of the subjects, objects, and

environment. The policy decision point (PDP) is the component in a zero trust architecture (ZTA) that evaluates the rule-based security policies and generates an access decision for each request.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2 A Zero Trust Policy Model | SpringerLink, section "Rule-Based Policies" Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section "Security policy

and control framework"

QUESTION 9

ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is______ Select the best answer.

A. prioritization based on risks

B. prioritization based on budget

C. prioritization based on management support

D. prioritization based on milestones

Correct Answer: A

ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is prioritization based on risks, which means that the organization should identify and assess the potential threats,

vulnerabilities, and impacts that could affect its assets, operations, and reputation, and prioritize the ZT initiatives that address the most critical and urgent risks. Prioritization based on risks helps to align the ZT project with the business

objectives and needs, and optimize the use of resources and time.

References:

Zero Trust Planning - Cloud Security Alliance, section "Scope, Priority, and Business Case"

The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section "Second Phase: Assess"

Planning for a Zero Trust Architecture: A Planning Guide for Federal ..., section "Gap Analysis"

QUESTION 10

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 11

In SaaS and PaaS, which access control method will ZT help define for access to the features within a service?

A. Data-based access control (DBAC)

B. Attribute-based access control (ABAC)

C. Role-based access control (RBAC)

D. Privilege-based access control (PBAC)

Correct Answer: B

ABAC is an access control method that uses attributes of the requester, the resource, the environment, and the action to evaluate and enforce policies. ABAC allows for fine-grained and dynamic access control based on the context of the request, rather than predefinedroles or privileges. ABAC is suitable for SaaS and PaaS, where the features within a service may vary depending on the customer\\'s needs, preferences, and subscription level. ABAC can help implement ZT by enforcing the principle of least privilege and verifying every request based on multiple factors. References: Attribute-Based Access Control (ABAC) Definition General Access Control Guidance for Cloud Systems A Guide to

Secure SaaS Access Control Within an Organization

QUESTION 12

What steps should organizations take to strengthen access requirements and protect their resources from unauthorized access by potential cyber threats?

A. Understand and identify the data and assets that need to be protected

B. Identify the relevant architecture capabilities and components that could impact ZT

C. Implement user-based certificates for authentication

D. Update controls for assets impacted by ZT

Correct Answer: A

The first step that organizations should take to strengthen access requirements and protect their resources from unauthorized access by potential cyber threats is to understand and identify the data and assets that need to be protected. This step involves conducting a data and asset inventory and classification, which helps to determine the value, sensitivity, ownership, and location of the data and assets. By understanding and identifying the dataand assets that need to be protected, organizations can define the appropriate access policies and controls based on the Zero Trust principles of never trust, always verify, and assume breach. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 2: Data and Asset Classification