CCZT$^{Q\&As}$

Certificate of Competence in Zero Trust (CCZT)

Pass Cloud Security Alliance CCZT Exam with 100% Guarantee

QUESTION 1

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 2

To successfully implement ZT security, two crucial processes must be planned and aligned with existing access procedures that the ZT implementation might impact. What are these two processes?

A. Incident and response management

B. Training and awareness programs

C. Vulnerability disclosure and patching management

D. Business continuity planning (BCP) and disaster recovery (DR)

Correct Answer: B

QUESTION 3

What is one of the key purposes of leveraging visibility and analytics capabilities in a ZTA?

A. Automatically granting access to all requested applications and data.

B. Ensuring device compatibility with legacy applications.

C. Enhancing network performance for faster data access.

D. Continually evaluating user behavior against a baseline to identify unusual actions.

Correct Answer: D

One of the key purposes of leveraging visibility and analytics capabilities in a ZTA is to continually evaluate user behavior against a baseline to identify unusual actions. This helps to detect and respond to potential threats, anomalies, and

deviations from the normal patterns of user activity. Visibility and analytics capabilities also enable the collection and analysis of telemetry data across all the core pillars of ZTA, such as user, device, network, application, and data, and provide

insights for policy enforcement and improvement.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3 Zero Trust for Government Networks: 4 Steps You Need to Know, section "Continuously verify trust with visibility and analytics" The role of visibility and analytics in

zero trust architectures, section "The basic NIST tenets of this approach include"

What is Zero Trust Architecture (ZTA)? | NextLabs, section "With real-time access control, users are reliably verified and authenticated before each session"

QUESTION 4

What is one benefit of the protect surface in a ZTA for an organization implementing controls?

A. Controls can be implemented at all ingress and egress points of the network and minimize risk.

B. Controls can be implemented at the perimeter of the network and minimize risk.

C. Controls can be moved away from the asset and minimize risk.

D. Controls can be moved closer to the asset and minimize risk.

Correct Answer: D

The protect surface in a ZTA is the collection of sensitive data, assets, applications, and services (DAAS) that require protection from threats1. One benefit of the protect surface in a ZTA for an organization implementing controls is that it allows the controls to be moved closer to the asset and minimize risk. This means that instead of relying on a single perimeter or boundary to protect the entire network, ZTA enables granular and dynamic controlsthat are applied at or near the DAAS components, based on the principle of least privilege2. This reduces the attack surface and the potential impact of a breach, as well as improves the visibility and agility of the security posture3. References: Zero Trust Architecture | NIST Zero Trust Architecture Explained: A Step-by-Step Approach - Comparitech What is Zero Trust Architecture (ZTA)? - CrowdStrike

QUESTION 5

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

CCZT PDF Dumps CCZT Practice Test CCZT Study Guide