CCZT Q&As

Certificate of Competence in Zero Trust (CCZT)

Pass Cloud Security Alliance CCZT Exam with 100% Guarantee

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

https://www.pass4itsure.com/cczt.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cloud Security Alliance Official Exam Center

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

QUESTION 1

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

QUESTION 2

The following list describes the SDP onboarding process/procedure.

What is the third step? 1. SDP controllers are brought online first. 2.

Accepting hosts are enlisted as SDP gateways that connect to and authenticate with the SDP controller. 3.

A. Initiating hosts are then onboarded and authenticated by the SDP gateway

B. Clients on the initiating hosts are then onboarded and authenticated by the SDP controller

C. SDP gateway is brought online

D. Finally, SDP controllers are then brought online

Correct Answer: A

The third step in the SDP onboarding process is to onboard and authenticate the initiating hosts, which are the clients that request access to the protected resources. The initiating hosts connect to and authenticate with the SDP gateway,

which acts as an accepting host and a proxy for the protected resources. The SDP gateway verifies the identity and posture of the initiating hosts and grants them access to the resources based on the policies defined by the SDP controller.

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

QUESTION 3

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 4

ZTA reduces management overhead by applying a consistent access model throughout the environment for all assets. What can be said about ZTA models in terms of access decisions?

A. The traffic of the access workflow must contain all the parameters for the policy decision points.

B. The traffic of the access workflow must contain all the parameters for the policy enforcement points.

C. Each access request is handled just-in-time by the policy decision points.

D. Access revocation data will be passed from the policy decision points to the policy enforcement points.

Correct Answer: C

ZTA models in terms of access decisions are based on the principle of "never trust, always verify", which means that each access request is handled just-in-time by the policy decision points. The policy decision points are the components in a ZTA that evaluate the policies and the contextual data collected from various sources, such as the user identity, the device posture, the network location, the resource attributes, and the environmental factors, and then generate an access decision. The access decision is communicated to the policy enforcement points, which enforce the decision on the resource. This way, ZTA models apply a consistent access model throughout the environment for all assets, regardless of their location, type, or ownership. References: Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2 What Is Zero Trust Architecture (ZTA)? - F5, section "Policy Engine" Zero trust security model - Wikipedia, section "What Is Zero Trust Architecture?" Zero Trust Maturity Model | CISA, section "Zero trust security model"

QUESTION 5

Which of the following is a common activity in the scope, priority, and business case steps of ZT planning?

A. Determine the organization\\'s current state

B. Prioritize protect surfaces O C. Develop a target architecture

C. Identify business and service owners

Correct Answer: A

A common activity in the scope, priority, and business case steps of ZT planning is to determine the organization\\'s current state. This involves assessing the existing security posture, architecture, policies, processes, and capabilities of the

organization, as well as identifying the key stakeholders, business drivers, and goals for the ZT initiative. Determining the current state helps to establish a baseline, identify gaps and risks, and define the scope and priority of the ZT

transformation.

References:

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

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