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.leads4pass.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

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 2

What does device validation help establish in a ZT deployment?

A. Connection based on user

B. High-speed network connectivity

C. Trusted connection based on certificate-based keys

D. Unrestricted public access

Correct Answer: C

Device validation helps establish a trusted connection based on certificate-based keys in a ZT deployment. Device validation is the process of verifying the identity and posture of the devices that request access to the protected resources.

Device validation relies on the use of certificates, which are digital credentials that bind the device identity to a public key. Certificates are issued by a trusted authority and can be used to authenticate the device and encrypt the

communication. Device validation helps to ensure that only healthy and compliant devices can access the resources, and that the connection is secure and confidential.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3 Zero Trust and Windows device health -

Windows Security, section "Device health attestation on Windows"

Devices and zero trust | Google Cloud Blog, section "In a zero trust environment, every device has to earn trust in order to be granted access."

QUESTION 3

When implementing ZTA, why is it important to collect logs from different log sources?

A. Collecting logs supports investigations, dashboard creation, and policy adjustments.

B. Collecting logs supports recording transaction flows, mapping transaction flows, and detecting changes in transaction flows.

C. Collecting logs supports change management, incident management, visibility and analytics.

D. Collecting logs supports micro-segmentation, device security, and governance.

Correct Answer: C

Log collection is an essential component of ZTA, as it provides the data needed to monitor, audit, and improve the security posture of the network. By collecting logs from different sources, such as devices, applications, firewalls, gateways,

and policies, ZTA can support various functions, such as:

Change management: Logs can help track and document any changes made to the network configuration, policies, or resources, and assess their impact on the security and performance of the network. Logs can also help identify and revert

any unauthorized or erroneous changes that may compromise the network integrity1.

Incident management: Logs can help detect and respond to any security incidents, such as breaches, attacks, or anomalies, that may occur in the network. Logs can provide the evidence and context needed to investigate the root cause,

scope, and impact of the incident, and to take appropriate remediation actions2. Visibility and analytics: Logs can help provide a comprehensive and granular view of the network activity, performance, and behavior. Logs can be used to

generate dashboards, reports, and alerts that can help measure and improve the network security and efficiency. Logs can also be used to apply advanced analytics techniques, such as machine learning, to identify patterns, trends, and

insights that can help optimize the network operations and security3.

References:

Zero Trust Architecture: Data Sources

Zero Trust Architecture: Incident Response

Zero Trust Architecture: Visibility and Analytics

QUESTION 4

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 5

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 6

To validate the implementation of ZT and ZTA, rigorous testing is essential. This ensures that access controls are functioning correctly and effectively safeguarded against potential threats, while the intended service levels are delivered. Testing of ZT is therefore

A. creating an agile culture for rapid deployment of ZT

B. integrated in the overall cybersecurity program

C. providing evidence of continuous improvement

D. allowing direct user feedback

Correct Answer: C

Testing of ZT is providing evidence of continuous improvement because it helps to measure the effectiveness and efficiency of the ZT and ZTA implementation. Testing of ZT also helps to identify and address any gaps, issues, or risks that may arise during the ZT and ZTA lifecycle. Testing of ZT enables the organization to monitor and evaluate the ZT and ZTA performance and maturity, and to apply feedback and lessons learned to improve the ZT and ZTA processes and outcomes. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 8: Testing and Validation

QUESTION 7

What measures are needed to detect and stop malicious access attempts in real-time and prevent damage when using ZTA\\'s centralized authentication and policy enforcement?

A. Audit logging and monitoring

B. Dynamic firewall policies

C. Network segregation

D. Dynamic access policies

Correct Answer: D

QUESTION 8

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 9

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 10

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

CCZT Practice Test CCZT Study Guide CCZT Braindumps