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

How can ZTA planning improve the developer experience?

A. Streamlining access provisioning to deployment environments.

B. Require deployments to be grouped into quarterly batches.

C. Use of a third-party tool for continuous integration/continuous deployment (CI/CD) and deployments.

D. Disallowing DevOps teams access to the pipeline or deployments.

Correct Answer: A

ZTA planning can improve the developer experience by streamlining access provisioning to deployment environments. This means that developers can access the resources and services they need to deploy their applications in a fast and secure manner, without having to go through complex and manual processes. ZTA planning can also help to automate and orchestrate the access provisioning using dynamic and granular policies based on the context and attributes of the developers, devices, and applications. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 10: ZTA Planning and Implementation

QUESTION 2

Which of the following is a required concept of single packet authorizations (SPAs)?

A. An SPA packet must be digitally signed and authenticated.

B. An SPA packet must self-contain all necessary information.

C. An SPA header is encrypted and thus trustworthy.

D. Upon receiving an SPA, a server must respond to establish secure connectivity.

Correct Answer: A

Single Packet Authorization (SPA) is a security protocol that allows a user to access a secure network without the need to enter a password or other credentials. Instead, it is an authentication protocol that uses a single packet ?an encrypted packet of data ?to convey a user\\'s identity and request access1. A key concept of SPA is that the SPA packet must be digitally signed and authenticated by the SPA server before granting access to the user. This ensures that only authorized users can send valid SPA packets and prevents replay attacks, spoofing attacks, or brute-force attacks23. References: Zero Trust: Single Packet Authorization | Passive authorization Single Packet Authorization | Linux Journal Single Packet Authorization Explained | Appgate Whitepaper

QUESTION 3

To ensure an acceptable user experience when implementing SDP, a security architect should collaborate with IT to do what?

A. Plan to release SDP as part of a single major change or a "big-bang" implementation.

B. Model and plan the user experience, client software distribution, and device onboarding processes.

C. Build the business case for SDP, based on cost modeling and business value.

D. Advise IT stakeholders that the security team will fully manage all aspects of the SDP rollout.

Correct Answer: B

To ensure an acceptable user experience when implementing SDP, a security architect should collaborate with IT to model and plan the user experience, client software distribution, and device onboarding processes. This is because SDP requires users to install and use client software to access the protected resources, and the user experience may vary depending on the device type, operating system, network conditions, and security policies. By modeling and planning the user experience, the security architect and IT can ensure that the SDP implementation is user-friendly, consistent, and secure. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT)

-Module 7: Network Infrastructure and SDP

QUESTION 4

Which of the following is a key principle of ZT and is required for its implementation?

A. Implementing strong anti-phishing email filters

B. Making no assumptions about an entity\\'s trustworthiness when it requests access to a resource

C. Encrypting all communications between any two endpoints

D. Requiring that authentication and explicit authorization must occur after network access has been granted

Correct Answer: B

Explanation: One of the core principles of Zero Trust (ZT) is to "never trust, always verify" every request for access to a resource, regardless of where it originates or what resource it accesses1. This means that ZT does not rely on implicit trust based on network perimeters, device types, or user roles, but rather on explicit verification based on multiple data points, such as user identity, device health, location, service, data classification, and anomalies1. References: Zero Trust Architecture | NIST Zero Trust Model - Modern Security Architecture | Microsoft Security How To Implement Zero Trust: 5-steps Approach and its challenges - Fortinet

QUESTION 5

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 6

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 7

In a ZTA, automation and orchestration can increase security by using the following means:

A. Kubernetes and docker

B. Static application security testing (SAST) and dynamic application security testing (DAST)

C. Data loss prevention (DLP) and cloud security access broker (CASB)

D. Infrastructure as code (IaC) and identity lifecycle management

Correct Answer: D

Explanation: In a ZTA, automation and orchestration can increase security by using the following means: Infrastructure as code (IaC): IaC is a practice of managing and provisioning IT infrastructure through code, rather than manual processes or configuration tools1. IaC can increase security by enabling consistent, repeatable, and scalable deployment of ZTA components, such as policies, gateways, firewalls, and micro- segments2. IaC can also facilitate compliance, auditability, and change management, as well as reduce human errors and configuration drifts3. Identity lifecycle management: Identity lifecycle management is a process of managing the creation, modification, and deletion of user identities and their access rights throughout their lifecycle4. Identity lifecycle management can increase security by ensuring that users have the appropriate level of access to resources at any given time, based on the principle of least privilege5. Identity lifecycle management can also automate the provisioning and deprovisioning of user accounts, enforce strong authentication and authorization policies, and monitor and audit user activity and behavior6. References: What is Infrastructure as Code? | Cloudflare Zero Trust Architecture: Infrastructure as Code Infrastructure as Code: Security Best Practices What is Identity Lifecycle Management? | One Identity Zero Trust Architecture: Identity and Access Management Identity Lifecycle Management: A Zero Trust Security Strategy

QUESTION 8

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 9

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

QUESTION 10

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