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

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 2

Scenario: An organization is conducting a gap analysis as a part of its ZT planning. During which of the following steps will risk appetite be defined?

A. Create a roadmap

B. Determine the target state

C. Determine the current state

D. Define requirements

Correct Answer: D

During the define requirements step of ZT planning, the organization will define its risk appetite, which is the amount and type of risk that it is willing to accept in pursuit of its objectives. Risk appetite reflects the organization\\'s risk culture,

tolerance, and strategy, and guides the development of the ZT policies and controls. Risk appetite should be aligned with the business priorities and needs, and communicated clearly to the stakeholders.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3 Risk Appetite Guidance Note - GOV.UK, section "Introduction" How to improve risk management using Zero Trust architecture | Microsoft Security Blog, section

"Risk management is an ongoing activity"

QUESTION 3

According to NIST, what are the key mechanisms for defining, managing, and enforcing policies in a ZTA?

A. Policy decision point (PDP), policy enforcement point (PEP), and policy information point (PIP)

B. Data access policy, public key infrastructure (PKI), and identity and access management (IAM)

C. Control plane, data plane, and application plane

D. Policy engine (PE), policy administrator (PA), and policy broker (PB)

Correct Answer: A

According to NIST, the key mechanisms for defining, managing, and enforcing policies in a ZTA are the policy decision point (PDP), the policy enforcement point (PEP), and the policy information point (PIP). The PDP is the component that

evaluates the policies and the contextual data collected from various sources and generates an access decision. The PEP isthe component that enforces the access decision on the resource. The PIP is the component that provides the

contextual data to the PDP, such as the user identity, the device posture, the network location, the resource attributes, and the environmental factors.

References:

Zero Trust Architecture Project - NIST Computer Security Resource Center, slide 9 What Is Zero Trust Architecture (ZTA)? - F5, section "Policy Engine" Zero Trust Frameworks Architecture Guide - Cisco, page 4, section "Policy Decision

Point"

QUESTION 4

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 5

Which security tools or capabilities can be utilized to automate the response to security events and incidents?

A. Single packet authorization (SPA)

B. Security orchestration, automation, and response (SOAR)

C. Multi-factor authentication (MFA)

D. Security information and event management (SIEM)

Correct Answer: B

SOAR is a collection of software programs developed to bolster an organization\\'s cybersecurity posture. SOAR tools can automate the response to security events and incidents by executing predefined workflows or playbooks, which can include tasks such as alert triage, threat detection, containment, mitigation, and remediation. SOAR tools can also orchestrate the integration of various security tools and data sources, and provide centralized dashboards and reporting for security operations. References: Certificate of Competence in Zero Trust (CCZT) prepkit, page 23, section 3.2.2 Security Orchestration, Automation and Response (SOAR) - Gartner Security Automation: Tools, Process and Best Practices - Cynet, section "What are the different types of security automation tools?" Introduction to automation in Microsoft Sentinel

Latest CCZT Dumps CCZT VCE Dumps CCZT Braindumps