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

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 3

To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of

A. learning and growth.

B. continuous risk evaluation and policy adjustment.

C. continuous process improvement.

D. project governance.

Correct Answer: B

To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of continuous risk evaluation and policy adjustment. This means that the organization should constantly monitor the threat

landscape, assess the security posture, and update the policies and controls accordingly to maintain a high level of protection and resilience. The organization should also embrace feedback, learning, and improvement as part of the ZT

journey.

References:

Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3 Cultivating a Zero Trust mindset - AWS Prescriptive Guidance, section "Continuous learning and improvement"

Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section "Continuous monitoring and improvement"

QUESTION 4

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 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