CCZT Q&As

Certificate of Competence in Zero Trust (CCZT)

Pass Cloud Security Alliance CCZT Exam with 100% Guarantee

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

QUESTION 1

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 2

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

QUESTION 3

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 4

Which activity of the ZT implementation preparation phase ensures the resiliency of the organization\\'s operations in the event of disruption?

A. Change management process

B. Business continuity and disaster recovery

C. Visibility and analytics

D. Compliance

Correct Answer: B

Business continuity and disaster recovery are the activities of the ZT implementation preparation phase that ensure the resiliency of the organization\\'s operations in the event of disruption. Business continuity refers to the process of

maintaining or restoring the essential functions of the organization during and after a crisis, such as a natural disaster, a cyberattack, or a pandemic. Disaster recovery refers to the process of recovering the IT systems, data, and infrastructure

that support the business continuity. ZT implementation requires planning and testing the business continuity and disaster recovery strategies and procedures, as well as aligning them with the ZT policies and controls.

References:

Zero Trust Planning - Cloud Security Alliance, section "Monitor and Measure" Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section "Continuous monitoring and improvement"

Zero Trust Implementation, section "Outline Zero Trust Architecture (ZTA) implementation steps"

QUESTION 5

To successfully implement ZT security, two crucial processes must be planned and aligned with existing access procedures that the ZT implementation might impact. What are these two processes?

A. Incident and response management

B. Training and awareness programs

C. Vulnerability disclosure and patching management

D. Business continuity planning (BCP) and disaster recovery (DR)

Correct Answer: B