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.certbus.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

QUESTION 1

What should be a key component of any ZT project, especially during implementation and adjustments?

A. Extensive task monitoring

B. Frequent technology changes

C. Proper risk management

D. Frequent policy audits

Correct Answer: C

Proper risk management should be a key component of any ZT project, especially during implementation and adjustments, because it helps to identify, analyze, evaluate, and treat the potential risks that may affect the ZT and ZTA objectives and outcomes. Proper risk management also helps to prioritize the ZT and ZTA activities and resources based on the risk level and impact, and to monitor and review the risk mitigation strategies and actions. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 9: Risk Management

QUESTION 2

Of the following, which option is a prerequisite action to understand the organization\\'s protect surface clearly?

A. Data and asset classification

B. Threat intelligence capability and monitoring

C. Gap analysis of the organization\\'s threat landscape

D. To have the latest risk register for controls implementation

Correct Answer: A

Data and asset classification is a prerequisite action to understand the organization\\'s protect surface clearly because it helps to identify the most critical and sensitive data and assets that need to be protected by Zero Trust principles. Data and asset classification also helps to define the appropriate policies and controls for different levels of data and asset sensitivity. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 2: Data and Asset Classification

QUESTION 3

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 4

Which vital ZTA component enhances network security and simplifies management by creating boundaries between resources in the same network zone?

A. Micro-segmentation

B. Session establishment or termination

C. Decision transmission

D. Authentication request/validation request (AR/VR)

Correct Answer: A

Micro-segmentation is a vital ZTA component that enhances network security and simplifies management by creating boundaries between resources in the same network zone. Micro-segmentation divides the network into smaller segments or zones based on the attributes and context of the resources, such as data sensitivity, application functionality, user roles, etc. Micro-segmentation helps to isolate and protect the resources from unauthorized access and lateral movement of attackers within the same network zone. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 6: Micro-segmentation

QUESTION 5

Which ZT element provides information that providers can use to keep policies dynamically updated?

A. Communication

B. Data sources

C. Identities

D. Resources

Correct Answer: B

Data sources are the ZT element that provide information that providers can use to keep policies dynamically updated. Data sources are the inputs that feed the policy engine and the policy administrator with the relevant data and context about the entities, resources, transactions, and environment in the ZTA. Data sources help to inform the policy decisionsand actions based on the current state and conditions of the ZTA. Data sources can include identity providers, device management systems, threat intelligence feeds, network monitoring tools, etc. References: Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 3: ZTA Architecture and Components

QUESTION 6

Network architects should consider__________ before selecting an SDP model.

Select the best answer.

A. leadership buy-in

B. gateways

C. their use case

D. cost

Correct Answer: C

Different SDP deployment models have different advantages and disadvantages depending on the organization\\'s use case, such as the type of resources to be protected, the location of the clients and servers, the network topology, the

scalability, the performance, and the security requirements. Network architects should consider their use case before selecting an SDP model that best suits their needs and goals.

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 Why SDP Matters in Zero Trust | SonicWall, section "SDP Deployment Models"

QUESTION 7

ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is______ Select the best answer.

A. prioritization based on risks

B. prioritization based on budget

C. prioritization based on management support

D. prioritization based on milestones

Correct Answer: A

ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is prioritization based on risks, which means that the organization should identify and assess the potential threats, vulnerabilities, and impacts that could affect its assets, operations, and reputation, and prioritize the ZT initiatives that address the most critical and urgent risks. Prioritization based on risks helps to align the ZT project with the business

objectives and needs, and optimize the use of resources and time.

References:

Zero Trust Planning - Cloud Security Alliance, section "Scope, Priority, and Business Case"

The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section "Second Phase: Assess"

Planning for a Zero Trust Architecture: A Planning Guide for Federal ..., section "Gap Analysis"

QUESTION 8

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 9

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 10

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"