Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

NEW QUESTION 1
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

Answer: C

Explanation:
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

NEW QUESTION 2
Which architectural consideration needs to be taken into account while deploying SDP? Select the best answer.

A. How SDP deployment fits into existing network topologies and technologies.
B. How SDP deployment fits into external vendor assessment.
C. How SDP deployment fits into existing human resource management systems.
D. How SDP deployment fits into application validation.

Answer: A

Explanation:
A key architectural consideration that needs to be taken into account while deploying SDP is how SDP deployment fits into existing network topologies and technologies. This is because SDP deployment may require changes or adaptations to the existing network infrastructure, such as routers, switches, firewalls, VPNs, etc. SDP deployment may also affect the network performance, availability, scalability, and resilience. Therefore, it is important to assess the impact and compatibility of SDP deployment with the existing network topologies and technologies, and to plan and design the SDP deployment accordingly.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 7: Network Infrastructure and SDP

NEW QUESTION 3
Which element of ZT focuses on the governance rules that define the "who, what, when, how, and why" aspects of accessing target resources?

A. Policy
B. Data sources
C. Scrutinize explicitly
D. Never trust, always verify

Answer: A

Explanation:
Policy is the element of ZT that focuses on the governance rules that define the ??who, what, when, how, and why?? aspects of accessing target resources. Policy is the core component of a ZTA that determines the access decisions and controls for each request based on various attributes and factors, such as user identity, device posture, network location, resource sensitivity, and environmental context. Policy is also the element that enables the ZT principles of ??never trust, always verify?? and ??scrutinize explicitly?? by enforcing granular, dynamic, and data-driven rules for each access request. 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 Architecture Project - NIST Computer Security Resource Center, slide 9
? [Zero Trust Frameworks Architecture Guide - Cisco], page 4, section ??Policy Decision Point??

NEW QUESTION 4
Which ZT tenet is based on the notion that malicious actors reside inside and outside the network?

A. Assume breach
B. Assume a hostile environment
C. Scrutinize explicitly
D. Requiring continuous monitoring

Answer: A

Explanation:
The ZT tenet of assume breach is based on the notion that malicious actors reside inside and outside the network, and that any user, device, or service can be compromised at any time. Therefore, ZT requires continuous verification and validation of all entities and transactions, and does not rely on implicit trust or perimeter-based defenses

NEW QUESTION 5
At which layer of the open systems interconnection (OSI) model does network access control (NAC) typically operate? Select the best answer.

A. Layer 6, the presentation layer
B. Layer 2, the data link layer

C. Layer 3, the network layer
D. Layer 4, the transport layer

Answer: B

Explanation:
Network access control (NAC) typically operates at layer 2, the data link layer, of the open systems interconnection (OSI) model. The data link layer is responsible for transferring data between adjacent nodes on a network, such as switches and endpoints. NAC operates at this layer by inspecting and controlling the access of devices to the network based on their MAC addresses, device profiles, security posture, and compliance status. References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 6: Micro-segmentation

NEW QUESTION 6
In a continual improvement model, who maintains the ZT policies?

A. System administrators
B. ZT administrators
C. Server administrators
D. Policy administrators

Answer: D

Explanation:
In a continual improvement model, policy administrators are the ones who maintain the ZT policies. Policy administrators are ZTA policy entities that are responsible for crafting and maintaining the policies that govern the access to resources in a ZT environment1. Policy administrators define the rules and conditions that specify who, what, when, where, and how an entity can access a resource, based on the principle of least privilege2. Policy administrators also update and review the policies periodically to ensure they are aligned with the changing business and security requirements3.
References =
? Zero Trust Architecture | NIST
? Zero Trust Architecture: Policy Engine and Policy Administrator
? Zero Trust Architecture: Policy Administration

NEW QUESTION 7
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

Answer: A

Explanation:
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

NEW QUESTION 8
During the monitoring and analytics phase of ZT transaction flows, organizations should collect statistics and profile the behavior of transactions. What does this support in the ZTA?

A. Creating firewall policies to protect data in motion
B. A continuous assessment of all transactions
C. Feeding transaction logs into a log monitoring engine
D. The monitoring of relevant data in critical areas

Answer: B

Explanation:
During the monitoring and analytics phase of ZT transaction flows, organizations should collect statistics and profile the behavior of transactions to support a continuous assessment of all transactions. A continuous assessment of all transactions means that the organization constantly evaluates the security posture, performance, and compliance of each transaction, and detects and responds to any anomalies, deviations, or threats. Acontinuous assessment of all transactions helps to maintain a high level of protection and resilience in the ZTA, and enables the organization to adjust and improve the policies and controls accordingly.
References =
? Zero Trust Planning - Cloud Security Alliance, section ??Monitor & Measure??
? The role of visibility and analytics in zero trust architectures, section ??The basic NIST tenets of this approach include??
? Move to the Zero Trust Security Model - Trailhead, section ??Monitor and Maintain Your Environment??

NEW QUESTION 9
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

Answer: C

Explanation:
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

NEW QUESTION 10
What does device validation help establish in a ZT deployment?

A. Connection based on user
B. High-speed network connectivity
C. Trusted connection based on certificate-based keys
D. Unrestricted public access

Answer: C

Explanation:
Device validation helps establish a trusted connection based on certificate-based keys in a ZT deployment. Device validation is the process of verifying the identity and posture of the devices that request access to the protected resources. Device validation relies on the use of certificates, which are digital credentials that bind the device identity to a public key. Certificates are issued by a trusted authority and can be used to authenticate the device and encrypt the communication. Device validation helps to ensure that only healthy and compliant devices can access the resources, and that the connection is secure and confidential.
References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3
? Zero Trust and Windows device health - Windows Security, section ??Device health attestation on Windows??
? Devices and zero trust | Google Cloud Blog, section ??In a zero trust environment, every device has to earn trust in order to be granted access.??

NEW QUESTION 10
SDP incorporates single-packet authorization (SPA). After successful authentication and authorization, what does the client usually do next? Select the best answer.

A. Generates an SPA packet and sends it to the initiating host.
B. Generates an SPA packet and sends it to the controller.
C. Generates an SPA packet and sends it to the accepting host.
D. Generates an SPA packet and sends it to the gateway.

Answer: B

Explanation:
After successful authentication and authorization, the client typically sends an SPA packet to the controller, which acts as an intermediary in authenticating the client's request before access to the accepting host is granted. References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 9: Risk Management

NEW QUESTION 13
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)

Answer: A

Explanation:
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??

NEW QUESTION 16
What is the function of the rule-based security policies configured on the policy decision point (PDP)?

A. Define rules that specify how information can flow
B. Define rules that specify multi-factor authentication (MFA) requirements
C. Define rules that map roles to users
D. Define rules that control the entitlements to assets

Answer: D

Explanation:
Rule-based security policies are a type of attribute-based access control (ABAC) policies that define rules that control the entitlements to assets, such as data, applications, or devices, based on the attributes of the subjects, objects, and environment. The policy decision point (PDP) is the component in a zero trust architecture (ZTA) that evaluates the rule-based security policies and generates an access decision for each request. References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
? A Zero Trust Policy Model | SpringerLink, section ??Rule-Based Policies??
? Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section ??Security policy and control framework??

NEW QUESTION 21
Scenario: As a ZTA security administrator, you aim to enforce the principle of least privilege for private cloud network access. Which ZTA policy entity is mainly responsible for crafting and maintaining these policies?

A. Gateway enforcing access policies
B. Policy enforcement point (PEP)
C. Policy administrator (PA)
D. Policy decision point (PDP)

Answer: C

Explanation:
A policy administrator (PA) is a ZTA policy entity that is responsible for crafting and maintaining the policies that govern the access to resources in a ZT environment1. A PA defines the rules and conditions that specify who, what, when, where, and how an entity can access a resource, based on the principle of least privilege2. A PA also updates and reviews the policies periodically to ensure they are aligned with the changing business and security requirements3.
References =
? Zero Trust Architecture | NIST
? Zero Trust Architecture: Policy Engine and Policy Administrator
? Zero Trust Architecture: Policy Administration

NEW QUESTION 24
How can device impersonation attacks be effectively prevented in a ZTA?

A. Strict access control
B. Micro-segmentation
C. Organizational asset management
D. Single packet authorization (SPA)

Answer: D

Explanation:
SPA is a security protocol that prevents device impersonation attacks in a ZTA by hiding the network infrastructure from unauthorized and unauthenticated users. SPA uses a single encrypted packet to convey the user??s identity and request access to a resource. The SPA packet must be digitally signed and authenticated by the SPA server before granting access. This ensures that only authorized devices can send valid SPA packets and prevents spoofing, replay, or brute-force attacks12.
References =
? Zero Trust: Single Packet Authorization | Passive authorization
? Single Packet Authorization | Linux Journal

NEW QUESTION 28
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

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 & its challenges - Fortinet

NEW QUESTION 30
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)

Answer: B

Explanation:
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

NEW QUESTION 33

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CCZT Practice Exam Features:

* CCZT Questions and Answers Updated Frequently

* CCZT Practice Questions Verified by Expert Senior Certified Staff

* CCZT Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCZT Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CCZT Practice Test Here