Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

NEW QUESTION 1
What is one benefit of the protect surface in a ZTA for an organization implementing controls?

A. Controls can be implemented at all ingress and egress points of the network and minimize risk.
B. Controls can be implemented at the perimeter of the network and minimize risk.
C. Controls can be moved away from the asset and minimize risk.
D. Controls can be moved closer to the asset and minimize risk.

Answer: D

Explanation:
The protect surface in a ZTA is the collection of sensitive data, assets, applications, and services (DAAS) that require protection from threats1. One benefit of the protect surface in a ZTA for an organization implementing controls is that it allows the controls to be moved closer to the asset and minimize risk. This means that instead of relying on a single perimeter or boundary to protect the entire network, ZTA enables granular and dynamic controlsthat are applied at or near the DAAS components, based on the principle of least privilege2. This reduces the attack surface and the potential impact of a breach, as well as improves the visibility and agility of the security posture3.
References =
? Zero Trust Architecture | NIST
? Zero Trust Architecture Explained: A Step-by-Step Approach - Comparitech
? What is Zero Trust Architecture (ZTA)? - CrowdStrike

NEW QUESTION 2
The following list describes the SDP onboarding process/procedure. What is the third step? 1. SDP controllers are brought online first. 2. Accepting hosts are enlisted as SDP gateways that connect to and authenticate with the SDP controller. 3.

A. Initiating hosts are then onboarded and authenticated by the SDP gateway
B. Clients on the initiating hosts are then onboarded and authenticated by the SDP controller
C. SDP gateway is brought online
D. Finally, SDP controllers are then brought online

Answer: A

Explanation:
The third step in the SDP onboarding process is to onboard and authenticate the initiating hosts, which are the clients that request access to the protected resources. The initiating hosts connect to and authenticate with the SDP gateway, which acts as an accepting host and a proxy for the protected resources. The SDP gateway verifies the identity and posture of the initiating hosts and grants them access to the resources based on the policies defined by the SDP controller.
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

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
Of the following options, which risk/threat does SDP mitigate by mandating micro-segmentation and implementing least privilege?

A. Identification and authentication failures
B. Injection
C. Security logging and monitoring failures
D. Broken access control

Answer: D

Explanation:
SDP mitigates the risk of broken access control by mandating micro-segmentation and implementing least privilege. Micro-segmentation divides the network into smaller, isolated segments that can prevent unauthorized access and contain lateral movement. Least privilege grants the minimum necessary access to users and devices for specific resources, while hiding all other assets from their view. This reduces the attack surface and prevents attackers from exploiting weak or misconfigured access controls

NEW QUESTION 5
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 6
In a ZTA, where should policies be created?

A. Data plane
B. Network
C. Control plane
D. Endpoint

Answer: C

Explanation:
In a ZTA, policies should be created in the control plane, which is the logical component that defines and manages the policies for accessing resources. The control plane consists of policy entities, such as policy administrators, policy engines, and policy decision points, that are responsible for crafting, maintaining, evaluating, and enforcing the policies1. Thecontrol plane interacts with the data plane, which is the logical component that handles the data transmission and processing, and the network, which is the physical or virtual component that provides the connectivity and transport for the data plane1. The endpoint is the device or system that requests or provides access to a resource1. References =
? Zero Trust Architecture | NIST

NEW QUESTION 7
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.

Answer: C

Explanation:
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??

NEW QUESTION 8
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

Answer: B

Explanation:
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 & 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??

NEW QUESTION 9

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 10
Which approach to ZTA strongly emphasizes proper governance of access privileges and entitlements for specific assets?

A. ZTA using device application sandboxing
B. ZTA using enhanced identity governance
C. ZTA using micro-segmentation
D. ZTA using network infrastructure and SDPs

Answer: B

Explanation:
ZTA using enhanced identity governance is an approach to ZTA that strongly emphasizes proper governance of access privileges and entitlements for specific assets. This approach focuses on managing the identity lifecycle, enforcing granular and dynamic policies, and auditing and monitoring access activities. ZTA using enhanced identity governance helps to ensure that only authorized and verified entities can access the protected assets based on the principle of least privilege and the context of the request.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 5: Enhanced Identity Governance

NEW QUESTION 10
When preparing to implement ZTA, some changes may be required. Which of the following components should the organization consider as part of their checklist to ensure a successful implementation?

A. Vulnerability scanning, patch management, change management, and problem management
B. Organization's governance, compliance, risk management, and operations
C. Incident management, business continuity planning (BCP), disaster recovery (DR), and training and awareness programs
D. Visibility and analytics integration and services accessed using mobile devices

Answer: B

Explanation:
When preparing to implement ZTA, some changes may be required in the organization??s governance, compliance, risk management, and operations. These components are essential for ensuring a successful implementation of ZTA, as they involve the following aspects12:
? Governance: This refers to the establishment of a clear vision, strategy, and roadmap for ZTA, as well as the definition of roles, responsibilities, and authorities for ZTA stakeholders. Governance also involves the alignment of ZTA with the organization??s mission, goals, and objectives, and the communication and collaboration among ZTA teams and other business units.
? Compliance: This refers to the adherence to the relevant laws, regulations, standards, and policies that apply to the organization??s ZTA. Compliance also involves the identification and mitigation of any legal or contractual risks or issues that may arise from ZTA implementation, such as data privacy, security, and sovereignty.
? Risk management: This refers to the assessment and management of the risks associated with ZTA implementation, such as technical, operational, financial, or reputational risks. Risk management also involves the development and implementation of risk mitigation strategies, controls, and metrics, as well as the monitoring and reporting of risk status and performance.
? Operations: This refers to the execution and maintenance of the ZTA processes, technologies, and services, as well as the integration and interoperability of ZTA with the existing IT infrastructure and systems. Operations also involve the optimization and improvement of ZTA efficiency and effectiveness, as well as the resolution of any operational issues or incidents.
References =
? Zero Trust Architecture: Governance
? Zero Trust Architecture: Acquisition and Adoption

NEW QUESTION 13
When kicking off ZT planning, what is the first step for an organization in defining priorities?

A. Determine current state
B. Define the scope
C. Define a business case
D. Identifying the data and assets

Answer: A

Explanation:
The first step for an organization in defining priorities for ZT planning is to determine the current state of its network, security, and business environment. This involves conducting a comprehensive assessment of the existing IT infrastructure, systems, applications, data, and assets, as well as the threats, risks, and vulnerabilities that affect them. The current state analysis also involves identifying the gaps, challenges, and opportunities for improvement in the current security posture, as well as the business goals, objectives, and requirements for ZT implementation12. By determining the current state, the organization can establish a baseline for measuring the progress and impact of ZT, as well as prioritize the most critical and urgent areas for ZT adoption.
References =

? Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators | CSRC Publications NIST
? Zero Trust Architecture Explained: A Step-by-Step Approach - Comparitech

NEW QUESTION 16
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 18
.....

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