Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

NEW QUESTION 1
In a ZTA, the logical combination of both the policy engine (PE) and policy administrator (PA) is called

A. policy decision point (PDP)
B. role-based accessO
C. policy enforcement point (PEP)
D. data access policy

Answer: A

Explanation:
In a ZTA, the logical combination of both the policy engine (PE) and policy administrator (PA) is called the policy decision point (PDP). The PE is the component that evaluates the policies and the contextual data collected from various sources and generates an access decision. The PA is the component that establishes or terminates the communication between a subject and a resource based on the access decision. The PDP communicates with the policy enforcement point (PEP), which enforces the access decision on the resource.
References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
? Zero Trust Architecture Project - NIST Computer Security Resource Center, slide 9
? What Is a Zero Trust Security Framework? | Votiro, section ??The Policy Engine and Policy Administrator??
? Zero Trust Frameworks Architecture Guide - Cisco, page 4, section ??Policy
Decision Point??

NEW QUESTION 2
What is a server exploitation threat that SDP features (server isolation, single packet authorization [SPA], and dynamic drop-all firewalls) protect against?

A. Certificate forgery attacks
B. Denial of service (DoS)/distributed denial of service (DDoS) attacks
C. Phishing attacks
D. Domain name system (DNS) poisoning attacks

Answer: A

Explanation:
SDP features protect against certificate forgery attacks by using identity verification mechanisms that prevent attackers from impersonating servers or users.References = Zero Trust Training (ZTT) - Module 8: Testing and Validation

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 component in a ZTA is responsible for deciding whether to grant access to a resource?

A. The policy enforcement point (PEP)
B. The policy administrator (PA)
C. The policy engine (PE)
D. The policy component

Answer: C

Explanation:
The policy engine (PE) is the component in a ZTA that is responsible for deciding whether to grant access to a resource. The PE evaluates 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 generates an access decision. The PE communicates the access decision to the policy enforcement point (PEP), which enforces the decision on the resource.
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??
? What is Zero Trust Architecture (ZTA)? | NextLabs, section ??Core Components??
? [SP 800-207, Zero Trust Architecture], page 11, section 3.3.1

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
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

Answer: C

Explanation:
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

NEW QUESTION 8
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

Answer: D

Explanation:
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??

NEW QUESTION 9
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)

Answer: A

Explanation:
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

NEW QUESTION 10
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 10
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 13
Optimal compliance posture is mainly achieved through two key ZT features: _____ and _____

A. (1) Principle of least privilege (2) Verifying remote access connections
B. (1) Discovery (2) Mapping access controls and network assets
C. (1) Authentication (2) Authorization of all networked assets
D. (1) Never trusting (2) Reducing the attack surface

Answer: D

Explanation:
Optimal compliance posture is mainly achieved through two key ZT features: never trusting and reducing the attack surface. Never trusting means that no entity or resource is assumed to be trustworthy or secure by default, and that every request for access or transaction is verified and validated before granting access or allowing the transaction. Reducing the attack surface means that the exposure and vulnerability of the assets and resources are minimized by implementing granular and dynamic policies, controls, and segmentation. These two features help to ensure that the organization complies with the security standards and regulations, and that the risks of breaches and incidents are reduced.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 1: Strategy and Governance

NEW QUESTION 15
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 18
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 21
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 26
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 27
What is one of the key purposes of leveraging visibility & 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.

Answer: D

Explanation:
One of the key purposes of leveraging visibility & 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 & 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 & 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??

NEW QUESTION 30
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 35
When planning for ZT implementation, who will determine valid users, roles, and privileges for accessing data as part of data governance?

A. IT teams
B. Application owners
C. Asset owners
D. Compliance officers

Answer: C

Explanation:
Asset owners are the ones who will determine valid users, roles, and privileges for accessing data as part of data governance. Asset owners are responsible for defining the data classification, sensitivity, and ownership of the data assets they own. They also have the authority to grant or revoke access to the data assets based on the business needs and the Zero Trust policies.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 2: Data and Asset Classification

NEW QUESTION 36
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.

Answer: C

Explanation:
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.

NEW QUESTION 39
To ensure a successful ZT effort, it is important to

A. engage finance regularly so they understand the effort and do not cancel the project
B. keep the effort focused within IT to avoid any distractions
C. engage stakeholders across the organization and at all levels, including functional areas
D. minimize communication with the business units to avoid "scope creep"

Answer: C

Explanation:
To ensure a successful ZT effort, it is important to engage stakeholders across the organization and at all levels, including functional areas. This helps to align the ZT vision and goals with the business priorities and needs, gain buy-in and support from the leadership and the users, and foster a culture of collaboration and trust. Engaging stakeholders also enables the identification and mapping of the critical assets, workflows, and dependencies, as well as the communication and feedback mechanisms for the ZT transformation.

References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3
? Zero Trust Planning - Cloud Security Alliance, section ??Scope, Priority, & Business Case??
? The ??Zero Trust?? Model in Cybersecurity: Towards understanding and ??, section ??3.1 Ensuring buy-in across the organization with tangible impact??

NEW QUESTION 44
.....

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