Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

NEW QUESTION 1
How can we use ZT to ensure that only legitimate users can access a SaaS or PaaS? Select the best answer.

A. Implementing micro-segmentation and mutual Transport Layer Security (mTLS)
B. Configuring the security assertion markup language (SAML) service provider only to accept requests from the designated ZT gateway
C. Integrating behavior analysis and geofencing as part of ZT controls
D. Enforcing multi-factor authentication (MFA) and single-sign on (SSO)

Answer: B

Explanation:
Configuring SAML to accept requests only from the designated ZT gateway ensures that all access requests are authenticated and authorized appropriately.
References = Zero Trust Architecture related sources including NIST

NEW QUESTION 2
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 3
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 4
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 5
To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of

A. learning and growth.
B. continuous risk evaluation and policy adjustment.
C. continuous process improvement.
D. project governance.

Answer: B

Explanation:
To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of continuous risk evaluation and policy adjustment. This means that the organization should constantly monitor the threat landscape, assess the security posture, and update the policies and controls accordingly to maintain a high level of protection and resilience. The organization should also embrace feedback, learning, and improvement as part of the ZT journey.
References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3
? Cultivating a Zero Trust mindset - AWS Prescriptive Guidance, section ??Continuous learning and improvement??
? Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section ??Continuous monitoring and improvement??

NEW QUESTION 6
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

Answer: A

Explanation:
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, & 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??

NEW QUESTION 7
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 8
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 9
In a ZTA, what is a key difference between a policy decision point (PDP) and a policy enforcement point (PEP)?

A. A PDP measures incoming signals against a set of access determination criteri
B. A PEP uses incoming signals to open or close a connection.
C. A PDP measures incoming signals and makes dynamic risk determination
D. A PEP uses incoming signals to make static risk determinations.
E. A PDP measures incoming control plane authentication signal
F. A PEP measures incoming data plane authorization signals.

G. A PDP measures incoming signals in an untrusted zon
H. A PEP measures incoming signals in an implicit trust zone.

Answer: A

Explanation:
In a ZTA, a policy decision point (PDP) is a logical component that evaluates the incoming signals from an entity requesting access to a resource against a set of access determination criteria, such as identity, context, device, location, and behavior1. A PDP then makes a decision to grant or deny access, or to request additional information or verification, based on the policies defined by the policy administrator1. A policy enforcement point (PEP) is a logical component that uses the incoming signals from the PDP to open or close a connection between the entity and the resource1. A PEP acts as a gateway or intermediary that enforces the decision made by the PDP and prevents unauthorized or risky access2.
References =
? Zero Trust Architecture | NIST
? Policy Enforcement Point (PEP) - Pomerium

NEW QUESTION 10
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

Answer: A

Explanation:
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

NEW QUESTION 10
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 12
When planning for a ZTA, a critical product of the gap analysis process is _____
Select the best answer.

A. a responsible, accountable, consulted, and informed (RACI) chart and communication plan
B. supporting data for the project business case
C. the implementation's requirements
D. a report on impacted identity and access management (IAM) infrastructure

Answer: C

Explanation:
A critical product of the gap analysis process is the implementation??s requirements, which are the specifications and criteria that define the desired outcomes, capabilities, and functionalities of the ZTA. The implementation??s requirements are derived from the gap analysis, which identifies the current state, the target state, and the gaps between them. The implementation??s requirements help to guide the design, development, testing, and deployment of the ZTA, as well as the evaluation of its effectiveness and alignment with the business objectives and needs.
References =
? Zero Trust Planning - Cloud Security Alliance, section ??Scope, Priority, & 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??

NEW QUESTION 14
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 17
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

Answer: B

Explanation:
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.

NEW QUESTION 19
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 22
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 24
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 25
In a ZTA, automation and orchestration can increase security by using the following means:

A. Kubernetes and docker
B. Static application security testing (SAST) and dynamic application security testing (DAST)
C. Data loss prevention (DLP) and cloud security access broker (CASB)
D. Infrastructure as code (laC) and identity lifecycle management

Answer: D

Explanation:
In a ZTA, automation and orchestration can increase security by using the following means:
? Infrastructure as code (laC): laC is a practice of managing and provisioning IT
infrastructure through code, rather than manual processes or configuration
tools1. laC can increase security by enabling consistent, repeatable, and scalable deployment of ZTA components, such as policies, gateways, firewalls, and micro- segments2. laC can also facilitate compliance, auditability, and change management, as well as reduce human errors and configuration drifts3.
? Identity lifecycle management: Identity lifecycle management is a process of managing the creation, modification, and deletion of user identities and their access rights throughout their lifecycle4. Identity lifecycle management can increase security by ensuring that users have the appropriate level of access to resources at any given time, based on the principle of least privilege5. Identity lifecycle management can also automate the provisioning and deprovisioning of user accounts, enforce strong authentication and authorization policies, and monitor and audit user activity and behavior6.
References =
? What is Infrastructure as Code? | Cloudflare
? Zero Trust Architecture: Infrastructure as Code
? Infrastructure as Code: Security Best Practices
? What is Identity Lifecycle Management? | One Identity
? Zero Trust Architecture: Identity and Access Management
? Identity Lifecycle Management: A Zero Trust Security Strategy

NEW QUESTION 28
When implementing ZTA, why is it important to collect logs from different log sources?

A. Collecting logs supports investigations, dashboard creation, and policy adjustments.
B. Collecting logs supports recording transaction flows, mapping transaction flows, and detecting changes in transaction flows.
C. Collecting logs supports change management, incident management, visibility and analytics.
D. Collecting logs supports micro-segmentation, device security, and governance.

Answer: C

Explanation:
Log collection is an essential component of ZTA, as it provides the data needed to monitor, audit, and improve the security posture of the network. By collecting logs from different sources, such as devices, applications, firewalls, gateways, and policies, ZTA can support various functions, such as:
? Change management: Logs can help track and document any changes made to the network configuration, policies, or resources, and assess their impact on the security and performance of the network. Logs can also help identify and revert any unauthorized or erroneous changes that may compromise the network integrity1.
? Incident management: Logs can help detect and respond to any security incidents, such as breaches, attacks, or anomalies, that may occur in the network. Logs can provide the evidence and context needed to investigate the root cause, scope, and impact of the incident, and to take appropriate remediation actions2.
? Visibility and analytics: Logs can help provide a comprehensive and granular view of the network activity, performance, and behavior. Logs can be used to generate dashboards, reports, and alerts that can help measure and improve the network security and efficiency. Logs can also be used to apply advanced analytics techniques, such as machine learning, to identify patterns, trends, and insights that can help optimize the network operations and security3.
References =
? Zero Trust Architecture: Data Sources
? Zero Trust Architecture: Incident Response
? Zero Trust Architecture: Visibility and Analytics

NEW QUESTION 30
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 31
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 35
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 40
Which of the following is a required concept of single packet authorizations (SPAs)?

A. An SPA packet must be digitally signed and authenticated.
B. An SPA packet must self-contain all necessary information.
C. An SPA header is encrypted and thus trustworthy.
D. Upon receiving an SPA, a server must respond to establish secure connectivity.

Answer: A

Explanation:
Single Packet Authorization (SPA) is a security protocol that allows a user to access a secure network without the need to enter a password or other credentials. Instead, it is an authentication protocol that uses a single packet – an encrypted packet of data – to convey a user??s identity and request access1. A key concept of SPA is that the SPA packet must be digitally signed and authenticated by the SPA server before granting access to the user. This ensures that only authorized users can send valid SPA packets and prevents replay attacks, spoofing attacks, or brute-force attacks23.
References =
? Zero Trust: Single Packet Authorization | Passive authorization
? Single Packet Authorization | Linux Journal
? Single Packet Authorization Explained | Appgate Whitepaper

NEW QUESTION 42
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 46
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 51
Which of the following is a potential outcome of an effective ZT implementation?

A. Regular vulnerability scanning
B. A comprehensive catalogue of all transactions, dependencies, and services with associated IDs
C. Deployment of traditional firewall solutions
D. Adoption of biometric authentication

Answer: B

Explanation:
A comprehensive catalogue of all transactions, dependencies, and services with associated IDs is a potential outcome of an effective ZT implementation because it helps to map the data flows and interactions among the assets and entities in the ZTA. This catalogue enables the ZTA to enforce granular and dynamic policies based on the context and attributes of the transactions, dependencies, and services. It also facilitates the monitoring and auditing of the ZTA activities and performance.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 3: ZTA Architecture and Components

NEW QUESTION 55
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 57
.....

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