Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
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 3
Which ZT element provides information that providers can use to keep policies dynamically updated?

A. Communication
B. Data sources
C. Identities
D. Resources

Answer: B

Explanation:
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

NEW QUESTION 4
How can ZTA planning improve the developer experience?

A. Streamlining access provisioning to deployment environments.
B. Require deployments to be grouped into quarterly batches.
C. Use of a third-party tool for continuous integration/continuous deployment (CI/CD) and deployments.
D. Disallowing DevOps teams access to the pipeline or deployments.

Answer: A

Explanation:
ZTA planning can improve the developer experience by streamlining access provisioning to deployment environments. This means that developers can access the resources and services they need to deploy their applications in a fast and secure manner, without having to go through complex and manual processes. ZTA planning can also help to automate and orchestrate the access provisioning using dynamic and granular policies based on the context and attributes of the developers, devices, and applications.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 10: ZTA Planning and Implementation

NEW QUESTION 5
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 6
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 7
To successfully implement ZT security, two crucial processes must be planned and aligned with existing access procedures that the ZT implementation might impact. What are these two processes?

A. Incident and response management
B. Training and awareness programs
C. Vulnerability disclosure and patching management
D. Business continuity planning (BCP) and disaster recovery (DR)

Answer: B

NEW QUESTION 8
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 9
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 10
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
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 13
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 14
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 18
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 20
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 25
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 27
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 31

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 32
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 (IaC) and identity lifecycle management

Answer: D

Explanation:
In a ZTA, automation and orchestration can increase security by using the following means:
? Infrastructure as code (IaC): IaC is a practice of managing and provisioning IT
infrastructure through code, rather than manual processes or configuration
tools1. IaC can increase security by enabling consistent, repeatable, and scalable deployment of ZTA components, such as policies, gateways, firewalls, and micro- segments2. IaC 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 34
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 35
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 40
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 43
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 48
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 49
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 51
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 53
What measures are needed to detect and stop malicious access attempts in real-time and prevent damage when using ZTA's centralized authentication and policy enforcement?

A. Audit logging and monitoring
B. Dynamic firewall policies
C. Network segregation
D. Dynamic access policies

Answer: D

NEW QUESTION 58
.....

Relate Links

100% Pass Your CCZT Exam with Exambible Prep Materials

https://www.exambible.com/CCZT-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/