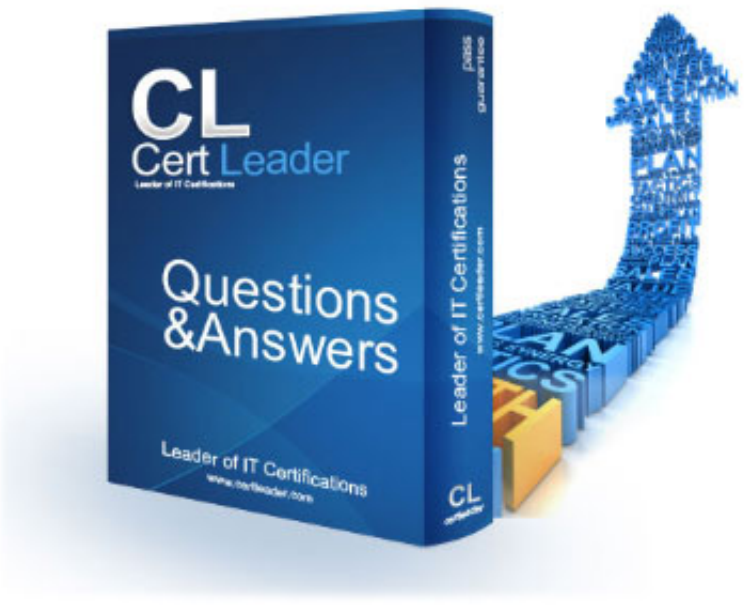
CCZT Dumps

Certificate of Competence in Zero Trust (CCZT)

https://www.certleader.com/CCZT-dumps.html



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
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 3
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 4
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 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
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
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 10
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 11
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 15
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 18
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 21
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 24
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 26
How can device impersonation attacks be effectively prevented in a ZTA?

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

Answer: D

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

NEW QUESTION 28
Which of the following is a key principle of ZT and is required for its implementation?

A. Implementing strong anti-phishing email filters
B. Making no assumptions about an entity's trustworthiness when it requests access to a resource
C. Encrypting all communications between any two endpoints
D. Requiring that authentication and explicit authorization must occur after network access has been granted

Answer: B

Explanation:
One of the core principles of Zero Trust (ZT) is to ??never trust, always verify?? every request for access to a resource, regardless of where it originates or what resource it accesses1. This means that ZT does not rely on implicit trust based on network perimeters, device types, or user roles, but rather on explicit verification based on multiple data points, such as user identity, device health, location, service, data classification, and anomalies1. References =
? Zero Trust Architecture | NIST
? Zero Trust Model - Modern Security Architecture | Microsoft Security
? How To Implement Zero Trust: 5-steps Approach & its challenges - Fortinet

NEW QUESTION 33
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 38
Which security tools or capabilities can be utilized to automate the response to security events and incidents?

A. Single packet authorization (SPA)
B. Security orchestration, automation, and response (SOAR)
C. Multi-factor authentication (MFA)
D. Security information and event management (SIEM)

Answer: B

Explanation:
SOAR is a collection of software programs developed to bolster an organization??s cybersecurity posture. SOAR tools can automate the response to security events and incidents by executing predefined workflows or playbooks, which can include tasks such as alert triage, threat detection, containment, mitigation, and remediation. SOAR tools can also orchestrate the integration of various security tools and data sources, and provide centralized dashboards and reporting for security operations.
References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 23, section 3.2.2
? Security Orchestration, Automation and Response (SOAR) - Gartner
? Security Automation: Tools, Process and Best Practices - Cynet, section ??What are the different types of security automation tools???
? Introduction to automation in Microsoft Sentinel

NEW QUESTION 41
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CCZT Exam with Our Prep Materials Via below:

https://www.certleader.com/CCZT-dumps.html