Cloud-Security-Alliance

Exam Questions CCZT

Certificate of Competence in Zero Trust (CCZT)

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 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
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 8
In SaaS and PaaS, which access control method will ZT help define for access to the features within a service?

A. Data-based access control (DBAC)
B. Attribute-based access control (ABAC)
C. Role-based access control (RBAC)
D. Privilege-based access control (PBAC)

Answer: B

Explanation:
ABAC is an access control method that uses attributes of the requester, the resource, the environment, and the action to evaluate and enforce policies. ABAC allows for fine-grained and dynamic access control based on the context of the request, rather than predefinedroles or privileges. ABAC is suitable for SaaS and PaaS, where the features within a service may vary depending on the customer??s needs, preferences, and subscription level. ABAC can help implement ZT by enforcing the principle of least privilege and verifying every request based on multiple factors.
References =
? Attribute-Based Access Control (ABAC) Definition
? General Access Control Guidance for Cloud Systems
? A Guide to Secure SaaS Access Control Within an Organization

NEW QUESTION 9
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 10
At which layer of the open systems interconnection (OSI) model does network access control (NAC) typically operate? Select the best answer.

A. Layer 6, the presentation layer
B. Layer 2, the data link layer
C. Layer 3, the network layer
D. Layer 4, the transport layer

Answer: B

Explanation:
Network access control (NAC) typically operates at layer 2, the data link layer, of the open systems interconnection (OSI) model. The data link layer is responsible for transferring data between adjacent nodes on a network, such as switches and endpoints. NAC operates at this layer by inspecting and controlling the access of devices to the network based on their MAC addresses, device profiles, security posture, and compliance status. References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 6: Micro-segmentation

NEW QUESTION 10
SDP features, like multi-factor authentication (MFA), mutual transport layer security (mTLS), and device fingerprinting, protect against

A. phishing
B. certificate forgery
C. domain name system (DNS) poisoning
D. code injections

Answer: A

Explanation:
SDP features, like multi-factor authentication (MFA), mutual transport layer security (mTLS), and device fingerprinting, protect against phishing attacks by verifying the identity and authenticity of both the user and the device before granting access to a resource. Phishing attacks are attempts to trick users into revealing their credentials or other sensitive information by impersonating a legitimate entity or service1. SDP features can prevent phishing attacks by:
? MFA: MFA is a security mechanism that requires a user to provide more than one piece of evidence to prove their identity, such as a password, a one-time code, a biometric factor, or a physical token2. MFA can protect against phishing attacks by making it harder for attackers to access a resource even if they manage to obtain the user??s password or other credentials2.
? mTLS: mTLS is a security protocol that enables mutual authentication and encryption between two parties, such as a client and a server3. mTLS can protect against phishing attacks by ensuring that both the client and the server have valid and trusted certificates, and by preventing attackers from intercepting or modifying the communication between them3.
? Device fingerprinting: Device fingerprinting is a technique that identifies and verifies a device based on its unique characteristics, such as its operating system, browser, IP address, or hardware configuration4. Device fingerprinting can protect against phishing attacks by allowing only authorized devices to access a resource, and by detecting any anomalies or changes in the device??s attributes that may indicate a compromise4.
References =
? What is Phishing? | How to Identify & Prevent Phishing Attacks | Cloudflare
? What is Multi-Factor Authentication (MFA)? | Cloudflare
? What is Mutual TLS (mTLS)? | Cloudflare
? What is Device Fingerprinting? | Cloudflare

NEW QUESTION 11
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 13
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 15
To ensure an acceptable user experience when implementing SDP, a security architect should collaborate with IT to do what?

A. Plan to release SDP as part of a single major change or a "big-bang" implementation.
B. Model and plan the user experience, client software distribution, and device onboarding processes.
C. Build the business case for SDP, based on cost modeling and business value.
D. Advise IT stakeholders that the security team will fully manage all aspects of the SDP rollout.

Answer: B

Explanation:
To ensure an acceptable user experience when implementing SDP, a security architect should collaborate with IT to model and plan the user experience, client software distribution, and device onboarding processes. This is because SDP requires users to install and use client software to access the protected resources, and the user experience may vary depending on the device type, operating system, network conditions, and security policies. By modeling and planning the user experience, the security architect and IT can ensure that the SDP implementation is user-friendly, consistent, and secure.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 7: Network Infrastructure and SDP

NEW QUESTION 18
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 20
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 21

.....

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