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
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 3
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 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
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 6
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 7
Which of the following is a common activity in the scope, priority, and business case steps of ZT planning?

A. Determine the organization's current state
B. Prioritize protect surfacesO
C. Develop a target architecture
D. Identify business and service owners

Answer: A

Explanation:
A common activity in the scope, priority, and business case steps of ZT planning is to determine the organization??s current state. This involves assessing the existing security posture, architecture, policies, processes, and capabilities of the organization, as well as identifying the key stakeholders, business drivers, and goals for the ZT initiative. Determining the current state helps to establish a baseline, identify gaps and risks, and define the scope and priority of the ZT transformation.
References =
? Zero Trust Planning - Cloud Security Alliance, section ??Scope, Priority, & Business Case??
? The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section ??First Phase: Prepare??

NEW QUESTION 8
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 9
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 10
What does device validation help establish in a ZT deployment?

A. Connection based on user
B. High-speed network connectivity
C. Trusted connection based on certificate-based keys
D. Unrestricted public access

Answer: C

Explanation:
Device validation helps establish a trusted connection based on certificate-based keys in a ZT deployment. Device validation is the process of verifying the identity and posture of the devices that request access to the protected resources. Device validation relies on the use of certificates, which are digital credentials that bind the device identity to a public key. Certificates are issued by a trusted authority and can be used to authenticate the device and encrypt the communication. Device validation helps to ensure that only healthy and compliant devices can access the resources, and that the connection is secure and confidential.
References =
? Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3
? Zero Trust and Windows device health - Windows Security, section ??Device health attestation on Windows??
? Devices and zero trust | Google Cloud Blog, section ??In a zero trust environment, every device has to earn trust in order to be granted access.??

NEW QUESTION 10
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 14
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 17
Scenario: A multinational org uses ZTA to enhance security. They collaborate with third-party service providers for remote access to specific resources. How can ZTA policies authenticate third-party users and devices for accessing resources?

A. ZTA policies can implement robust encryption and secure access controls to prevent access to services from stolen devices, ensuring that only legitimate users can access mobile services.
B. ZTA policies should prioritize securing remote users through technologies like virtual desktop infrastructure (VDI) and corporate cloud workstation resources to reduce the risk of lateral movement via compromised access controls.
C. ZTA policies can be configured to authenticate third-party users and their devices, determining the necessary access privileges for resources while concealing all other assets to minimize the attack surface.
D. ZTA policies should primarily educate users about secure practices and promote strong authentication for services accessed via mobile devices to prevent data compromise.

Answer: C

Explanation:
ZTA is based on the principle of never trusting any user or device by default, regardless of their location or ownership. ZTA policies can use various methods to verify the identity and context of third-party users and devices, such as tokens, certificates, multifactor authentication, device posture assessment, etc. ZTA policies can also enforce granular and dynamic access policies that grant the minimum necessary privileges to third-party users and devices for accessing specific resources, while hiding all other assets from their view. This reduces the attack surface and prevents unauthorized access and lateral movement within the network.

NEW QUESTION 20
For ZTA, what should be used to validate the identity of an entity?

A. Password management system
B. Multifactor authentication
C. Single sign-on
D. Bio-metric authentication

Answer: B

Explanation:
Multifactor authentication is a method of validating the identity of an entity by requiring two or more factors, such as something the entity knows (e.g., password, PIN), something the entity has (e.g., token, smart card), or something the entity is (e.g., biometric, behavioral). Multifactor authentication enhances the security of Zero Trust Architecture (ZTA) by reducing the risk of identity compromise and unauthorized access.
References = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 4: Identity and Access Management

NEW QUESTION 21
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 26
.....

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