Free Questions for CCZT by certsinside

Shared by Rasmussen on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a common activity in the scope, priority,

and business case steps of ZT planning?

Options:

A- Determine the organization's current state

B- Prioritize protect surfaces

O 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.

Reference=

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"

Question 2

Question Type: **MultipleChoice**

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.

Options:

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.

Reference=

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

Question 3

Question Type: MultipleChoice

What is one of the key purposes of leveraging visibility & analytics

capabilities in a ZTA?

Options:

A- Automatically granting access to all requested applications and data.

B- Ensuring device compatibility with legacy applications.

C- Enhancing network performance for faster data access.

D- Continually evaluating user behavior against a baseline to identify unusual actions.

Answer:

D

Explanation:

One of the key purposes of leveraging visibility & analytics capabilities in a ZTA is to continually evaluate user behavior against a baseline to identify unusual actions. This helps to detect and respond to potential threats, anomalies, and deviations from the normal patterns of user activity. Visibility & analytics capabilities also enable the collection and analysis of telemetry data across all the core pillars of ZTA, such as user, device, network, application, and data, and provide insights for policy enforcement and improvement.

Reference=

Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3

Zero Trust for Government Networks: 4 Steps You Need to Know, section "Continuously verify trust with visibility & analytics"

The role of visibility and analytics in zero trust architectures, section "The basic NIST tenets of this approach include"

What is Zero Trust Architecture (ZTA)? | NextLabs, section "With real-time access control, users are reliably verified and authenticated before each session"

Question 4

Question Type: MultipleChoice

To respond quickly to changes while implementing ZT Strategy, an

organization requires a mindset and culture of

Options:

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.

Reference=

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"

Question 5

Question Type: MultipleChoice

What is the function of the rule-based security policies configured

on the policy decision point (PDP)?

Options:

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.

Reference=

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"

Question 6

Question Type: MultipleChoice

Which component in a ZTA is responsible for deciding whether to

grant access to a resource?

Options:

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.

Reference=

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

Question 7

Question Type: **MultipleChoice**

Network architects should consider_____ before selecting an SDP model.

Select the best answer.

Options:

A- leadership buy-in

B- gateways

C- their use case

D- cost

Answer:

C

Explanation:

Different SDP deployment models have different advantages and disadvantages depending on the organization's use case, such as the type of resources to be protected, the location of the clients and servers, the network topology, the scalability, the performance, and the security requirements. Network architects should consider their use case before selecting an SDP model that best suits their needs and goals.

Reference=

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

Why SDP Matters in Zero Trust | SonicWall, section "SDP Deployment Models"