ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Zscaler

Code: ZDTA

Exam: Zscaler Digital Transformation Administrator

https://www.examsnest.com/exam/zdta/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 5.0

Question: 1

Which is an example of Inline Data Protection?

A. Preventing the copying of a sensitive document to a USB drive.
B. Preventing the sharing of a sensitive document in OneDrive.
C. Analyzing a customer's M365 tenant for security best practices.
D. Blocking the attachment of a sensitive document in webmail.

Answer: D

Explanation:

Inline Data Protection is the process of inspecting data as it transits the network in real time, enforcing policies that prevent sensitive data from being leaked or transmitted improperly. Blocking the attachment of a sensitive document in webmail represents inline data protection because it intercepts and controls data transmission at the network level, stopping sensitive content before it leaves the organization.
Preventing copying to a USB drive is endpoint control and does not happen inline in network traffic. Preventing sharing in OneDrive is cloud access security broker (CASB) activity, often done through API integrations, not inline network control. Analyzing M365 tenant security is an audit or advisory activity, not real-time inline protection.
Therefore, the correct example of inline data protection in Zscaler's cloud security services is blocking the attachment of a sensitive document in webmail.

Question: 2

Which attack type is characterized by a commonly used website or service that has malicious content like malicious JavaScript running on it?

A. Watering Hole Attack
B. Pre-existing Compromise
C. Phishing Attack
D. Exploit Kits

Answer: A

Explanation:

A Watering Hole Attack targets users by compromising a website or service that is commonly visited by the intended victims. The attacker injects malicious content such as malicious JavaScript or malware into the website, so when the user visits the site, their system gets infected. This attack relies on the trust users have in popular or legitimate websites and exploits it by turning those sites into infection vectors. Pre-existing Compromise refers to attacks where the target environment is already compromised before the attack is recognized, but it does not specifically describe malicious content injected into popular websites. Phishing Attack involves deceiving users to click malicious links or reveal credentials, not compromising websites directly. Exploit Kits are automated tools that scan for vulnerabilities and deliver exploits but are not characterized by the use of commonly used websites hosting malicious scripts.
The study guide clearly explains Watering Hole Attacks as a method where attackers infect trusted websites frequented by target users to deliver malicious payloads.

Question: 3

What is the name of the feature that allows the platform to apply URL filtering even when a Cloud APP control policy explicitly permits a transaction?

A. Allow Cascading
B. Allow and Quarantine
C. Allow URL Filtering
D. Allow and Scan

Answer: A

Explanation:

The feature that allows Zscaler to apply URL filtering even when a Cloud App control policy explicitly permits a transaction is called Allow Cascading. This feature ensures that even if a cloud application is permitted by the Cloud App control policy, the URL filtering policy can still be enforced. This is useful in cases where granular URL control is needed on top of cloud app permissions, providing layered security controls.
The study guide clearly explains that Allow Cascading enables URL filtering policies to cascade or take precedence and thus still inspect and potentially block URLs even if the cloud app is allowed by policy. This allows administrators to fine-tune access and ensure additional inspection layers on web traffic .

Question: 4

Which proprietary technology does Zscaler use to calculate risk attributes dynamically for websites?

A. Third-Party Sandbox
B. Zscaler PageRisk
C. Browser Isolation Feedback Form
D. Deception Controller

Answer: B

Explanation:

Zscaler uses a proprietary technology called Zscaler PageRisk to calculate risk attributes dynamically for websites. PageRisk assesses the risk level of a website based on a variety of dynamic factors, including the site's content, reputation, and behavior, helping to identify potentially harmful or suspicious sites in real time.
This dynamic risk scoring allows Zscaler to enforce security policies more effectively, blocking or allowing access based on calculated risk rather than static lists alone. The study guide specifies that PageRisk is integral to the platform's adaptive security posture and URL filtering capabilities .

Question: 5

Which list of protocols is supported by Zscaler for Privileged Remote Access?

A. RDP, VNC and SSH
B. RDP, SSH and DHCP
C. SSH, DNS and DHCP
D. RDP, DNS and VNC

Answer: A

Explanation:

Zscaler supports RDP, VNC, and SSH protocols for Privileged Remote Access. These are commonly used protocols for remote management and privileged user sessions, allowing secure access to internal applications or systems without exposing the network or requiring VPN connections.
The study guide clearly states that Privileged Remote Access capabilities focus on these protocols to ensure secure, monitored, and controlled remote sessions for administrators and privileged users, supporting remote desktop and shell access securely .

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Zscaler

Code: ZDTA

Exam: Zscaler Digital Transformation Administrator

https://www.examsnest.com/exam/zdta/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation