Free Questions for NSK100

Shared by Roach on 11-10-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

There is a DLP violation on a file in your sanctioned Google Drive instance. The file is in a deleted state. You need to locate information pertaining to this DLP violation using Netskope. In this scenario, which statement is correct?

Options:

A- You can find DLP violations under Forensic profiles.
B- DLP incidents for a file are not visible when the file is deleted.
C- You can find DLP violations under the Incidents dashboard.
D- You must create a forensic profile so that an incident is created.

Answer:

C

Explanation:

To locate information pertaining to a DLP violation on a file in your sanctioned Google Drive instance, you can use the Incidents dashboard in Netskope. The Incidents dashboard provides a comprehensive view of all the incidents that have occurred in your cloud environment, such as DLP violations, malware infections, anomalous activities, etc. You can filter the incidents by various criteria, such as app name, incident type, severity, user name, etc. You can also drill down into each incident to see more details, such as file name, file path, file owner, file size, file type, etc. The Incidents dashboard can show DLP violations for files that are in a deleted state, as long as they are still recoverable from the trash bin of the app. If the file is permanently deleted from the app, then the incident will not be visible in the dashboard.Reference:Netskope Incidents Dashboard

Question 2

Question Type: MultipleChoice

Which two use cases would be considered examples of Shadow IT within an organization? (Choose two.)

Options:

A- a sanctioned Salesforce account used by a contractor to upload non-sensitive data

B- a sanctioned Wetransfer being used by a corporate user to share sensitive data

C- an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data

D- an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data

Answer:

C, D

Explanation:

Shadow IT is the term for the unauthorized use of IT resources and functions by employees within an organization. It can include cloud services, software, and hardware that are not approved or managed by the IT department. Two use cases that would be considered examples of shadow IT within an organization are: an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data and an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data. In both cases, the corporate user is using a personal cloud storage service that is not sanctioned by the organization to store work-related data. This can introduce security risks, such as data leakage, data loss, compliance violations, malware infections, etc. The IT department may not have visibility or control over these cloud services or the data stored in them.Reference:What is shadow IT? | CloudflareWhat is Shadow IT? | IBM

Question 3

Question Type: MultipleChoice

You want to deploy Netskope's zero trust network access (ZTNA) solution, NP

Options:

A- In this scenario, which action would you perform to accomplish this task?

A- Create an OAuth identity access control between your users and your applications.

B- Set up a reverse proxy using SAML and an identity provider.

C- Enable Steer all Private Apps in your existing steering configuration(s) from the admin console.

D- Configure SCIM to exchange identity information and attributes with your applications.

Answer:

C

Explanation:

To deploy Netskope's zero trust network access (ZTNA) solution, NPA, you need to enable Steer all Private Apps in your existing steering configuration(s) from the admin console. This will allow you to create private app profiles and assign them to your applications. NPA will then provide secure and granular access to your applications without exposing them to the internet or requiring VPNs.Reference:[Netskope Private Access (NPA) Deployment Guide]

Question 4

Question Type: MultipleChoice

You want to prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application. In this scenario, which method would you use?

Options:

A- Use a stronger encryption algorithm.
B- Use certificate pinning.
C- Use a proxy for the connection.
D- Use a weaker encryption algorithm.

Answer:

B

Explanation:

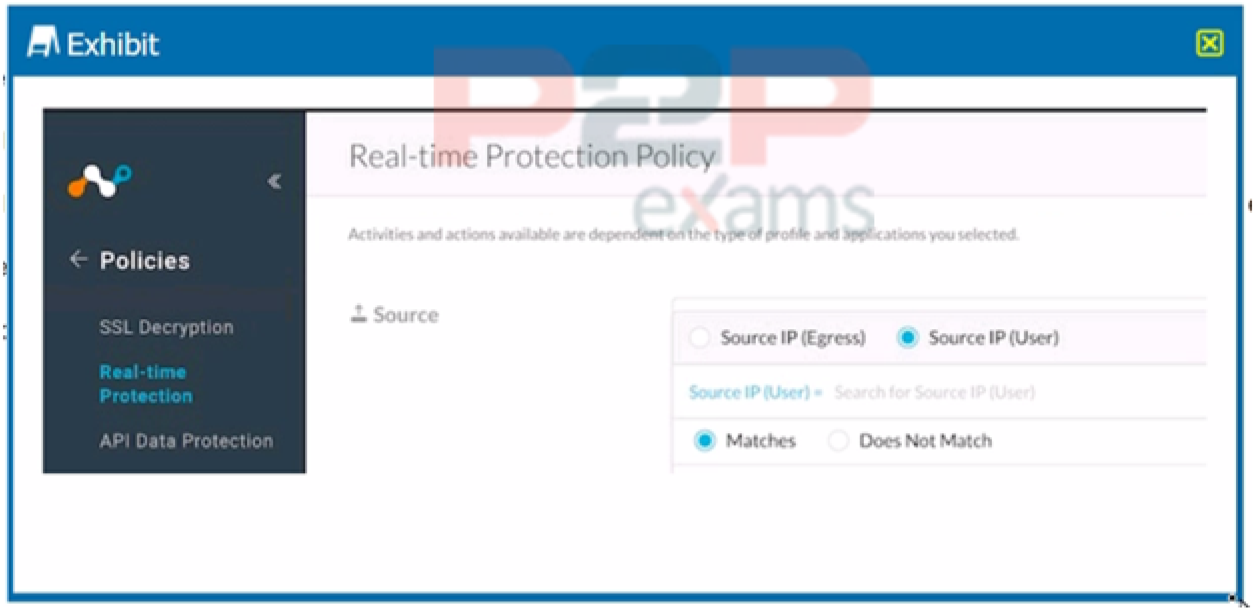
To prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application, one method that you can use is certificate pinning. Certificate pinning is a technique that restricts which certificates are considered valid for a particular website or application, limiting risk. Instead of allowing any trusted certificate to be used, operators 'pin' the certificate authority (CA) issuer(s), public keys or even end-entity certificates of their choice. Certificate pinning helps to prevent MITM attacks by validating the server certificates against a hardcoded list of certificates in the website or application. If an attacker tries to intercept or modify the traffic using a fraudulent or compromised certificate, it will be rejected by the website or application as invalid, even if it is signed by a trusted CA.Reference:Certificate pinning - IBMCertificate and Public Key Pinning |

OWASP Foundation

Question 5

Question Type: MultipleChoice

Refer to Exhibit.



Real-time Protection Policy

Activities and actions available are dependent on the type of profile and applications you selected.

Source

○ Source IP (Egress) ● Source IP (User)

Source IP (User) = Search for Source IP (User)

● Matches ○ Does Not Match

Click the Exhibit button.

Referring to the exhibit, which statement accurately describes the difference between Source IP (Egress) and Source IP (User) address?

Options:

A- Source IP (Egress) is the IP address of the destination Web server while Source IP (User) is the IP address assigned to your network.

B- Source IP (Egress) is the IP address assigned to the endpoint host IP address while Source IP (User) is the public IP address of your Internet edge router.

C- You must always leave the source IP fields blank and configure the user identity as a source criteria.

D- Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint.

Answer:

D

Explanation:

The statement that accurately describes the difference between Source IP (Egress) and Source IP (User) address is: Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint. Source IP (Egress) is the IP address that is visible to external networks when you send traffic from your network to the Internet. It is usually the IP address of your Internet edge router or gateway that performs NAT (Network Address Translation). Source IP (User) is the IP address that is assigned to your endpoint device, such as a laptop or a smartphone, within your network. It is usually a private IP address that is not routable on the Internet. You can use these two criteria to filter traffic based on where it originates from within your network or outside your network.Reference:Source Address / Source Port vs Destination Address / Destination PortHow to explain Source IP Address, Destination IP Address & Service in easy way

Question 6

Question Type: MultipleChoice

You want to set up a Netskope API connection to Box.

What two actions must be completed to enable this connection? (Choose two.)

Options:

A- Install the Box desktop sync client.

B- Authorize the Netskope application in Box.

C- Integrate Box with the corporate IdP.

D- Configure Box in SaaS API Data protection.

Answer:

B, D

Explanation:

To set up a Netskope API connection to Box, two actions that must be completed are: authorize the Netskope application in Box and configure Box in SaaS API Data protection. Authorizing the Netskope application in Box allows Netskope to access the Box API and perform out-of-band inspection and enforcement of policies on the data that is already stored in Box. Configuring Box in SaaS API Data protection allows you to specify the Box instance details, such as domain name, admin email, etc., and enable features such as retroactive scan, event stream, etc.Reference:Authorize Netskope Introspection App on Box Enterprise - Netskope Knowledge PortalConfigure Box Instance in Netskope UI - Netskope Knowledge Portal

Question 7

Question Type: MultipleChoice

According to Netskope. what are two preferred methods to report a URL miscategorization? (Choose two.)

Options:

A- Use www.netskope.com/url-lookup.

B- Use the URL Lookup page in the dashboard.

C- Email support@netskope.com.

D- Tag Netskope on Twitter.

Answer:

A, B

Explanation:

According to Netskope, two preferred methods to report a URL miscategorization are: use www.netskope.com/url-lookup and use the URL Lookup page in the dashboard. The first method allows you to visit www.netskope.com/url-lookup in your browser and enter any URL that you want to check or report for miscategorization. You will see the current category assigned by Netskope for that URL and you can submit a request to change it if you think it is incorrect. The second method allows you to use the URL Lookup page in the dashboard of your Netskope platform tenant and enter any URL that you want to check or report for miscategorization. You will see the current category assigned by Netskope for that URL and you can submit a request to change it if you think it is incorrect. Emailing support@netskope.com or tagging Netskope on Twitter are not preferred methods to report a URL miscategorization, as they are not designed for this purpose and may not be as efficient or effective as using the dedicated tools provided by Netskope.Reference:[Netskope URL Lookup],Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Course, Module 8: Skope IT, Lesson 2: Page Events.

Question 8

Question Type: MultipleChoice

A customer wants to detect misconfigurations in their AWS cloud instances.

In this scenario, which Netskope feature would you recommend to the customer?

Options:

A- Netskope Secure Web Gateway (SWG)

B- Netskope Cloud Security Posture Management (CSPM)

C- Netskope Advanced DLP and Threat Protection

D- Netskope SaaS Security Posture Management (SSPM)

Answer:

B

Explanation:

If a customer wants to detect misconfigurations in their AWS cloud instances, the Netskope feature that I would recommend to them is Netskope Cloud Security Posture Management (CSPM). Netskope CSPM is a service that provides continuous assessment and remediation of public cloud deployments for risks, threats, and compliance issues. Netskope CSPM leverages the APIs available from AWS and other cloud service providers to scan the cloud infrastructure for misconfigurations, such as insecure permissions, open ports, unencrypted data, etc. Netskope CSPM also provides security posture policies, profiles, and rules that can be customized to match the customer's security standards and best practices. Netskope CSPM can also alert, report, or remediate the misconfigurations automatically or manually.Reference:Netskope CSPMCloud Security Posture Management

Question 9

Question Type: MultipleChoice

What are two reasons why legacy solutions, such as on-premises firewalls and proxies, fail to secure the data and data access compared to Netskope Secure Web Gateway? (Choose two.)

Options:

A- Legacy solutions are unable to see the user who is trying to access the application.
B- The applications where the data resides are no longer in one central location.
C- Legacy solutions do not meet compliance standards.
D- The users accessing this data are not in one central place.

Answer:

B, D

Explanation:

Legacy solutions, such as on-premises firewalls and proxies, fail to secure the data and data access compared to Netskope Secure Web Gateway because they are designed for a perimeter-based security model, where the applications and the users are both within the corporate network. However, with the rise of cloud computing and remote work, this model is no longer valid. The applications where the data resides are no longer in one central location, but distributed across multiple cloud services and regions. The users accessing this data are not in one central place, but working from anywhere, on any device. Legacy solutions cannot provide adequate visibility and control over this dynamic and complex environment, resulting in security gaps and performance issues. Netskope Secure Web Gateway, on the other hand, leverages a cloud-native architecture that provides high-performance and scalable inspection of traffic from any location and device, as well as granular policies and advanced threat and data protection for web and cloud applications.Reference:Netskope Architecture OverviewNetskope Next Gen SWG

Question 10

Question Type: MultipleChoice

Which two traffic steering configurations are supported by Netskope? (Choose two.)

Options:

A- browser isolation traffic only
B- cloud applications only
C- all Web traffic including cloud applications
D- Web traffic only

Answer:

B, C

Explanation:

The two traffic steering configurations that are supported by Netskope are cloud applications only and all Web traffic including cloud applications. These configurations allow you to control what kind of traffic gets steered to Netskope for real-time deep analysis and what kind of traffic gets bypassed. You can choose one of these options for both on-premises and off-premises scenarios, depending on your network environment and security needs. You can also create exceptions for specific domains, IP addresses, or certificate-pinned applications that you want to bypass or steer regardless of the configuration option.Reference:Steering ConfigurationCreating a Steering Configuration