Free Questions for NSK101

Shared by Hickman on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A user has performed a bulk delete activity. In this scenario, which Netskope feature monitors potential risky users for a malicious activity that would cause data loss?

Options:

A- Netskope's Threat Protection inline policies

B- Netskope's Behavior Analytics rule-based policies

C- Netskope's API Data Protection policies

D- Netskope's Cloud Threat Exchange integration

Answer:

B

Explanation:

Netskope's Behavior Analytics rule-based policies are designed to monitor user behavior for patterns that may indicate risky or malicious activities, such as bulk deletions. These policies can identify anomalies in user behavior that deviate from the norm, flagging potential threats and taking appropriate actions to prevent data loss.

Netskope's Behavior Analytics rule-based policies: This feature analyzes user actions and behaviors to detect anomalies and potentially malicious activities. It helps in identifying and mitigating risks associated with compromised accounts, insider threats, and other suspicious activities.

Netskope documentation on Behavior Analytics and its capabilities.

Security best practices for detecting and responding to insider threats and anomalous user behavior.

Question 2

Question Type: MultipleChoice

Which Netskope component would an administrator use to see an overview of private application usage and performance?

Options:

A- Digital Experience Management

B- Publishers page

C- Incident Management

D- Cloud Exchange

Answer:

A

Explanation:

An administrator would use the Digital Experience Management (DEM) component to see an overview of private application usage and performance. DEM provides comprehensive insights into the performance and user experience of private applications, including metrics on latency, bandwidth, and application health.

Digital Experience Management (DEM): This component focuses on monitoring and optimizing the user experience for private and public applications by collecting detailed performance data and providing actionable insights.

The other options do not provide the same level of detailed performance and usage overview for private applications:

Publishers page: Typically used for managing and configuring Netskope Publishers.

Incident Management: Focuses on tracking and resolving security incidents.

Cloud Exchange: Deals with integrations and data sharing between Netskope and other security solutions.

Netskope documentation on Digital Experience Management and its capabilities.

Best practices for using DEM to monitor application performance and enhance user experience.

Question 3

Question Type: MultipleChoice

Digital Experience Management (DEM) allows an administrator to monitor which two areas? (Choose two.)

Options:

A- User activities

B- Bandwidth consumption

C- Information on triggered policies

D- Client steering data

Answer:

B, D

Explanation:

Digital Experience Management (DEM) in Netskope allows administrators to monitor the following areas:

Bandwidth consumption: DEM provides insights into how much bandwidth is being used by different applications and services, helping administrators to optimize network performance and ensure efficient use of resources.

Client steering data: DEM collects data on how traffic is being steered through the Netskope infrastructure, including details about routing decisions, performance metrics, and user experiences. This helps administrators understand the impact of their steering policies and make adjustments to improve performance.

User activities (option A) and information on triggered policies (option C) are more directly related to other features such as activity logs and policy enforcement dashboards rather than DEM.

Netskope documentation on Digital Experience Management.

Guides on monitoring and optimizing network performance using DEM.

Question 4

Question Type: MultipleChoice

As an administrator, you are investigating an increase in the number of incidents related to compromised credentials. You are using the Netskope Compromised Credentials feature on your tenant to assess the situation. Which insights would you find when using this

feature? (Choose two)

Options:

A- Compromised usernames

B- Breach information source

C- Compromised passwords

D- Affected managed applications

Answer:

A, B

Explanation:

When using the Netskope Compromised Credentials feature, administrators can gain valuable insights into security incidents related to compromised credentials. The insights provided by this feature include:

Compromised usernames: This information helps identify which user accounts have been compromised, allowing administrators to take necessary actions such as resetting passwords and notifying affected users.

Breach information source: Netskope provides details on the source of the breach, such as which third-party service or data breach resulted in the compromise of credentials. This helps in understanding the context of the breach and implementing measures to prevent

future incidents.

While compromised passwords (option C) are indirectly involved, they are not explicitly listed as an insight provided by this feature. Similarly, affected managed applications (option D) are related but not directly part of the primary insights.

Netskope documentation on Compromised Credentials feature and incident response.

Security best practices for managing and mitigating compromised credential incidents.

Question 5

Question Type: MultipleChoice

Your customer asks you to secure all Web traffic as part of the initial configuration. In the Netskope platform, which statement is correct in this scenario?

Options:

A- Add the all Web traffic option to the steering configuration.

B- Netskope automatically steers all Web traffic.

C- Netskope cannot steer Web traffic.

D- Select all Web traffic in the SSL decryption section.

Answer:

A

Explanation:

To secure all web traffic as part of the initial configuration in the Netskope platform, you need to:

Add the all Web traffic option to the steering configuration: This ensures that all web traffic is routed through Netskope for inspection and policy enforcement. By steering all web traffic, you enable Netskope to apply security measures, such as SSL decryption, threat protection, and DLP, to all HTTP and HTTPS traffic.

Netskope does not automatically steer all web traffic by default; it requires configuration in the steering policies. Selecting all web traffic in the SSL decryption section only pertains to decrypting traffic, not the actual steering of the traffic.

Netskope documentation on configuring steering settings and policies.

Guidelines for setting up web traffic steering and SSL decryption in the Netskope platform.

Question 6

Question Type: MultipleChoice

You are asked to review files affected by malware in your organization. In this scenario, which two actions are possible and would be accessible from the Netskope UI -> Incidents --> Malware? (Choose two)

Options:

A- Download the original malware file generating the alert to be analyzed by the SOC team

B- Identify the exposure of the file identified as malware.

C- Remediate the compromised devices.

D- Determine the Detection Engine used to identify the malware.

Answer:

B, D

Explanation:

When reviewing files affected by malware in the Netskope UI under Incidents -> Malware, you have the following options:

Identify the exposure of the file identified as malware: This allows you to see where the malware has spread within the organization, which users or systems are affected, and any potential data exposure resulting from the malware.

Determine the Detection Engine used to identify the malware: Netskope provides details on which detection engine (such as AV, sandboxing, or other heuristic engines) identified the malware. This helps in understanding the threat vector and the reliability of the detection.

Downloading the original malware file (option A) is generally not recommended for security reasons and may not be supported directly from the Netskope UI. Remediation of compromised devices (option C) would typically be handled through endpoint security solutions rather than directly from the Netskope UI.

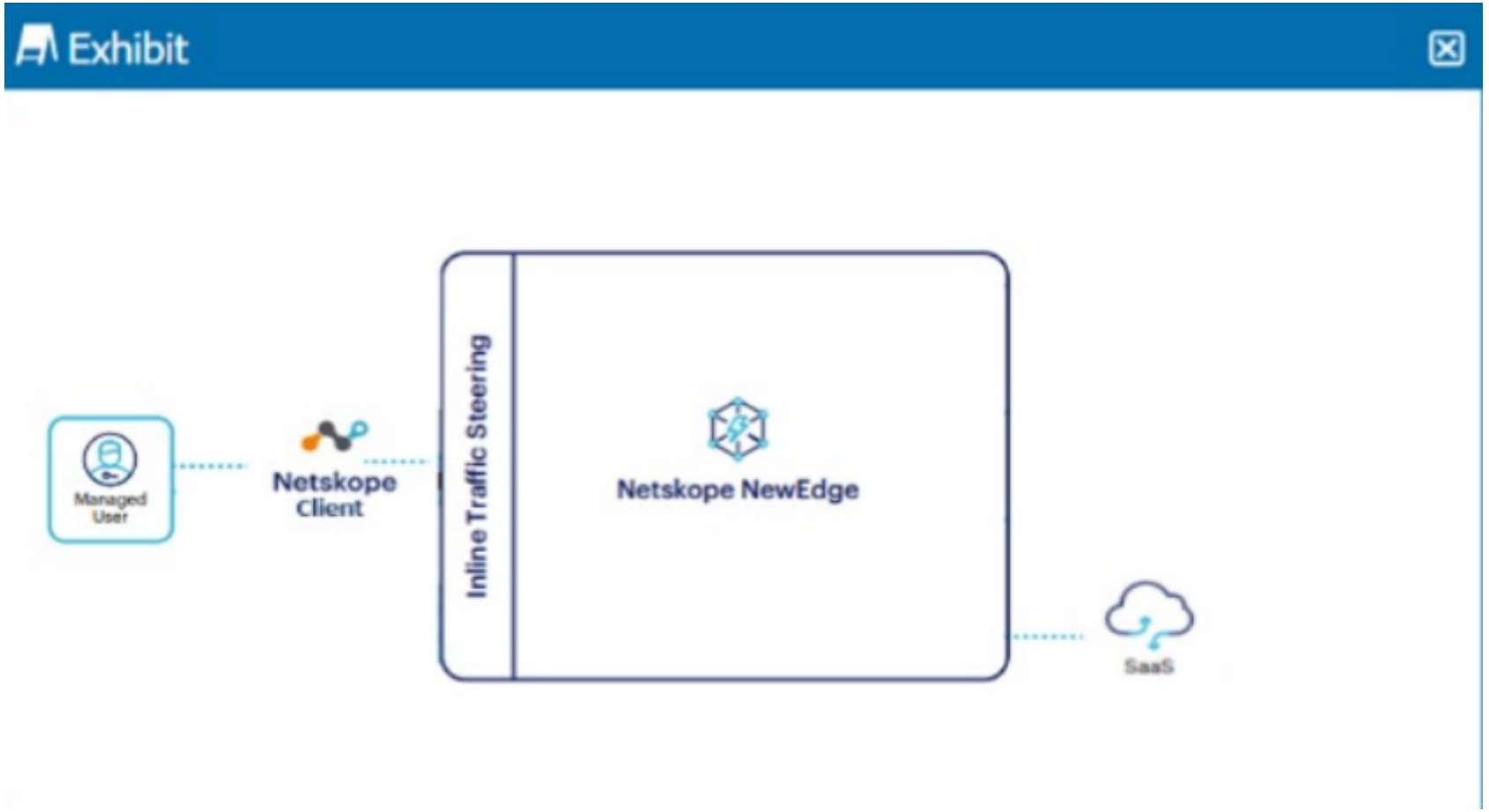
Netskope documentation on malware detection and incident response.

Best practices for handling malware incidents and using the Netskope UI for threat analysis.

Question 7

Question Type: **MultipleChoice**

Click the Exhibit button.



A user is connected to a SaaS application through Netskope's Next Gen SWG with SSL inspection enabled. In this scenario, what information is available in SkopeIT? (Choose three.)

Options:

A- User activity, CCL

B- Destination IP, OS patch version

C- Account instance, category

D- Username, source location

E- File version, shared folder

Answer:

A, C, D

Explanation:

In the scenario where a user is connected to a SaaS application through Netskope's Next Gen Secure Web Gateway (SWG) with SSL inspection enabled, the following information is available in SkopeIT:

User activity, CCL: SkopeIT provides detailed logs of user activities, including actions taken within SaaS applications, and uses the Cloud Confidence Level (CCL) to rate the trustworthiness of cloud applications.

Account instance, category: It logs information about the specific instance of the account being accessed and categorizes the type of service or application in use, which helps in identifying the context of the user's activities.

Username, source location: The username of the user accessing the SaaS application and their source location (such as IP address or geographic location) are logged for audit and compliance purposes.

Netskope documentation on SSL inspection and SkopeIT logging.

Detailed configuration guides on using Next Gen SWG and the types of data collected by SkopeIT.

Question 8

Question Type: MultipleChoice

Your customer has cloud storage repositories containing sensitive files of their partners, including bank statements, consulting, and disclosure agreements. In this scenario, which feature would help them control the flow of these types of documents?

Options:

A- ZTNA

B- Netskope Advanced Analytics

C- DLP document classifiers

D- Sandboxing

Answer:

C

Explanation:

Data Loss Prevention (DLP) document classifiers are designed to identify and control the flow of sensitive information based on predefined patterns and criteria. In this scenario, where the customer has cloud storage repositories containing sensitive files such as bank statements, consulting agreements, and disclosure agreements, DLP document classifiers can help:

Identify sensitive documents: By scanning and classifying documents based on their content, DLP document classifiers ensure that sensitive files are recognized and handled appropriately.

Control data flow: Policies can be applied to prevent unauthorized access, sharing, or movement of sensitive files, thereby protecting the data from leakage or exposure.

Netskope DLP documentation, detailing how document classifiers work and how they can be configured to protect sensitive information.

Best practices for implementing DLP solutions to safeguard sensitive data in cloud storage environments.