Free Questions for NSK200 by ebraindumps

Shared by Potter on 24-05-2024

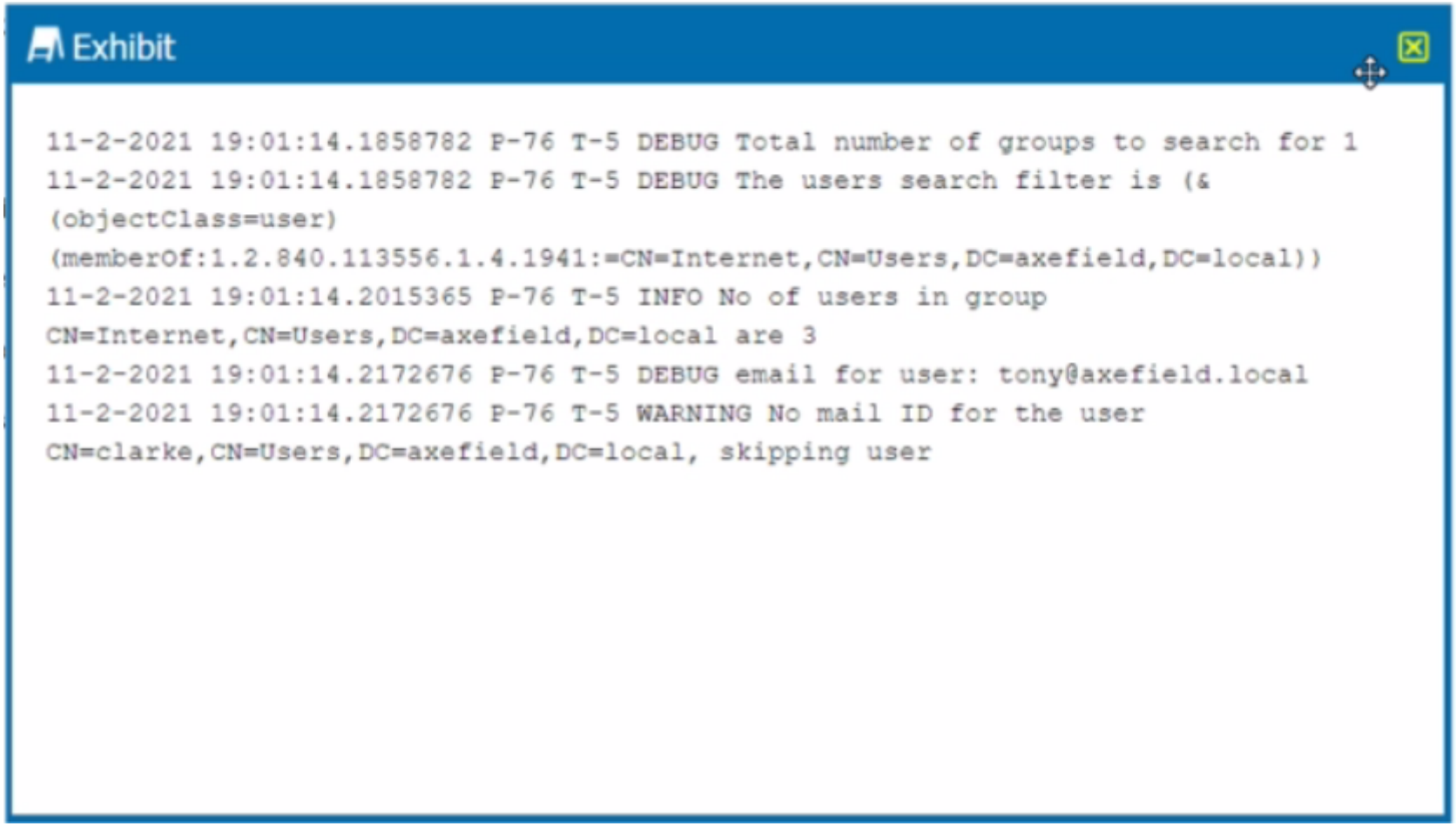
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the exhibit.



You are troubleshooting a Netskope client for user Clarke which remains in a disabled state after being installed. After looking at various logs, you notice something which might explain the problem. The exhibit is an excerpt from the nsADImporterLog.log.

Referring to the exhibit, what is the problem?

Options:

A- The client was not Installed with administrative privileges.

B- The Active Directory user is not synchronized to the Netskope tenant.

C- This is normal; it might take up to an hour to be enabled.

D- The client traffic is decrypted by a network security device.

Answer:

B

Explanation:

The problem is B. The Active Directory user is not synchronized to the Netskope tenant. This is evident from the log message "WARNING No mail ID for the user: Clarke, Daxmeifield, DC=local, skipping use". This means that the user Clarke does not have a valid email address in the Active Directory, which is required for the Netskope client to work. The Netskope client uses the email address of the user to authenticate and enable the client. Therefore, option B is correct and the other options are incorrect.

Question 2

Question Type: MultipleChoice

Your company needs to keep quarantined files that have been triggered by a DLP policy. In this scenario, which statement Is true?

Options:

A- The files are stofed remotely In your data center assigned In the Quarantine profile.

B- The files are stored In the Netskope data center assigned in the Quarantine profile.

C- The files are stored In the Cloud provider assigned In the Quarantine profile.

D- The files are stored on the administrator console PC assigned In the Quarantine profile.

Answer:

B

Explanation:

When a policy flags a file to be quarantined, that file is placed in a quarantine folder and a tombstone file is put in the original location in its place. The quarantine folder is located in the Netskope data center assigned in the Quarantine profile. The Quarantine profile is configured in Settings > Threat Protection > API-enabled Protection. The quarantined file is zipped and protected with a password to prevent users from inadvertently downloading the file.Netskope then notifies the admin specified in the profile1. Therefore, option B is correct and the other options are incorrect.Reference:Quarantine - Netskope Knowledge Portal,Threat Protection - Netskope Knowledge Portal

Question 3

Question Type: MultipleChoice

You want to secure Microsoft Exchange and Gmail SMTP traffic for DLP using Netskope. Which statement is true about this scenario when using the Netskope client?

Options:

A- Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail.

B- Enable Cloud Firewall to Inspect Inbound SMTP traffic for Microsoft Exchange and Gmail.

C- Netskope can inspect inbound and outbound SMTP traffic for Microsoft Exchange and Gmail.

D- Enable REST API v2 to Inspect inbound SMTP traffic for Microsoft Exchange and Gmail.

Answer:

A

Explanation:

Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail using the Netskope client. The Netskope client intercepts the SMTP traffic from the user's device and forwards it to the Netskope cloud for DLP scanning. The Netskope client does not inspect inbound SMTP traffic, as this is handled by the cloud email service or the MTA. Therefore, option A is correct and the other options are incorrect.Reference:Configure Netskope SMTP Proxy with Microsoft O365 Exchange,Configure Netskope SMTP Proxy with Gmail,SMTP DLP,Best Practices for Email Security with SMTP proxy

Question 4

Question Type: MultipleChoice

Your learn is asked to Investigate which of the Netskope DLP policies are creating the most incidents. In this scenario, which two statements are true? (Choose two.)

Options:

A- The Skope IT Applications tab will list the top five DLP policies.

B- You can see the top Ave DLP policies triggered using the Analyze feature

C- You can create a report using Reporting or Advanced Analytics.

D- The Skope IT Alerts tab will list the top five DLP policies.

Answer:

B, C

Explanation:

To investigate which of the Netskope DLP policies are creating the most incidents, the following two statements are true:

You can see the top five DLP policies triggered using the Analyze feature. The Analyze feature allows you to create custom dashboards and widgets to visualize and explore your data.You can use the DLP Policy widget to see the top five DLP policies that generated the most incidents in a given time period3.

You can create a report using Reporting or Advanced Analytics. The Reporting feature allows you to create scheduled or ad-hoc reports based on predefined templates or custom queries.You can use the DLP Incidents by Policy template to generate a report that shows the number of incidents per DLP policy4. The Advanced Analytics feature allows you to run SQL queries on your data and export the results as CSV or JSON files.You can use the DLP_INCIDENTS table to query the data by policy name and incident count5.

The other two statements are not true because:

The Skope IT Applications tab will not list the top five DLP policies. The Skope IT Applications tab shows the cloud app usage and risk summary for your organization.It does not show any information about DLP policies or incidents6.

The Skope IT Alerts tab will not list the top five DLP policies. The Skope IT Alerts tab shows the alerts generated by various policies and profiles, such as DLP, threat protection, IPS, etc.It does not show the number of incidents per policy, only the number of alerts per incident7.

Question 5

Question Type: MultipleChoice

Which object would be selected when creating a Malware Detection profile?

Options:

A- DLP profile

B- File profile

C- Domain profile

D- User profile

Answer:

B

Explanation:

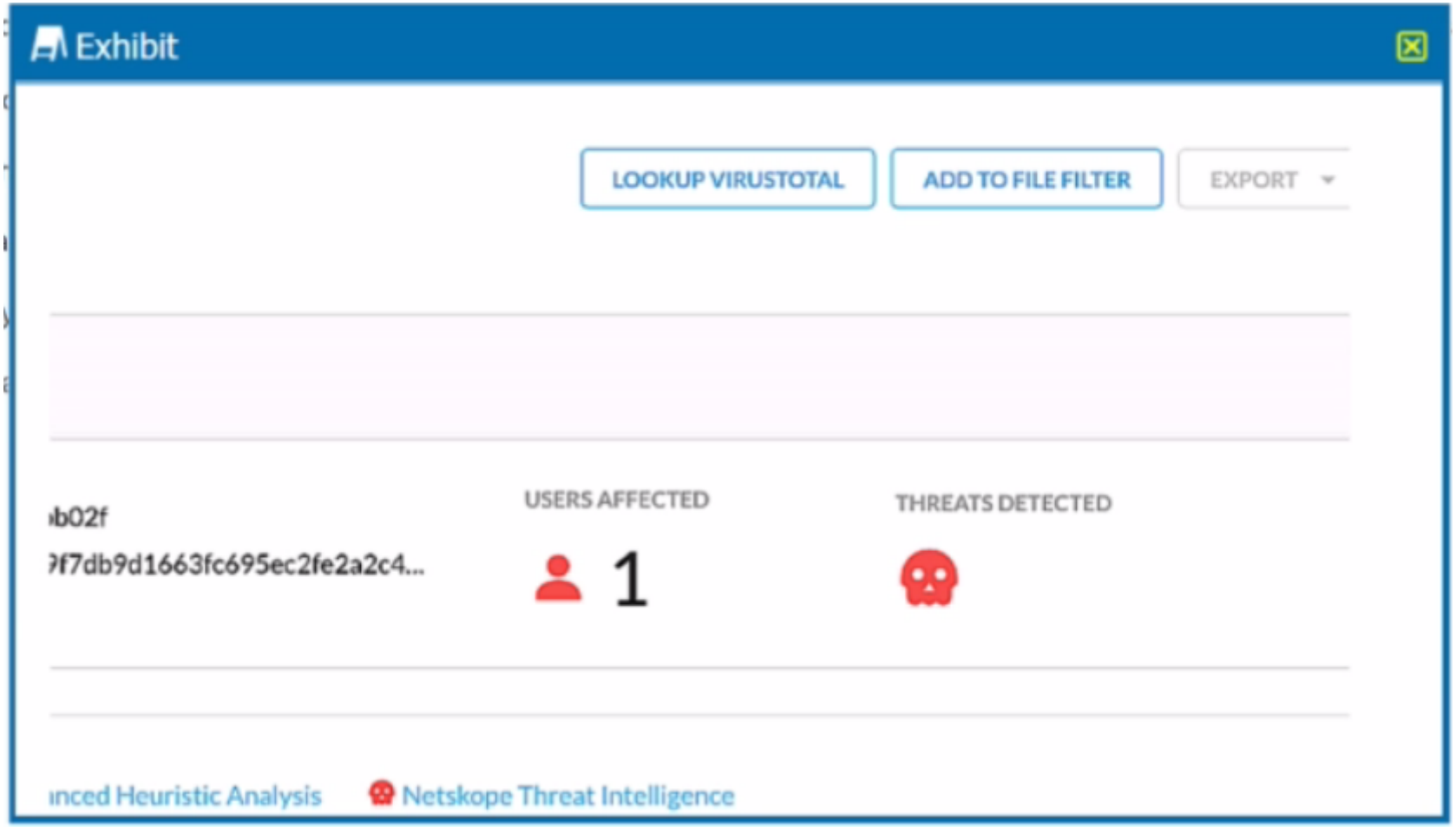
A file profile is an object that contains a list of file hashes that can be used to create a malware detection profile. A file profile can be configured as an allowlist or a blocklist, depending on whether the files are known to be benign or malicious.A file profile can be created in the Settings > File Profile page1. A malware detection profile is a set of rules that define how Netskope handles malware incidents.A

malware detection profile can be created in the Policies > Threat Protection > Malware Detection Profiles page2. To create a malware detection profile, one needs to select a file profile as an allowlist or a blocklist, along with the Netskope malware scan option. The other options are not objects that can be selected when creating a malware detection profile.

Question 6

Question Type: MultipleChoice

Review the exhibit.



You are at the Malware Incident page. A virus was detected by the Netskope Heuristics Engine. Your security team has confirmed that the virus was a test data file You want to allow the security team to use this file

Referring to the exhibit, which two statements are correct? (Choose two.)

Options:

A- Click the 'Add To File Filter button to add the IOC to a file list.

B- Contact the CrowdStrike administrator to have the file marked as safe.

C- Click the "Lookup VirusTotal' button to verify if this IOC is a false positive.

D- Create a malware detection profile and update the file hash list with the IOC.

Answer:

A, C

Explanation:

To allow the security team to use the test data file that was detected as a virus by the Netskope Heuristics Engine, the following two steps are correct:

Click the "Add To File Filter" button to add the IOC to a file list. This will exclude the file from future malware scans and prevent false positive alerts.The file list can be managed in the Settings > File Filter page1.

Click the "Lookup VirusTotal" button to verify if this IOC is a false positive. This will open a new tab with the VirusTotal report for the file hash. VirusTotal is a service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content.The report will show how many antivirus engines detected the file as malicious and provide additional information about the file2.

https://docs.netskope.com/en/netskope-help/admin-console/incidents/

Question 7

Question Type: MultipleChoice

An engineering firm is using Netskope DLP to identify and block sensitive documents, including schematics and drawings. Lately, they have identified that when these documents are blocked, certain employees may be taking screenshots and uploading them. They want to block any screenshots from being uploaded.

Which feature would you use to satisfy this requirement?

Options:

A- exact data match (EDM)

B- document fingerprinting

C- ML image classifier

D- optical character recognition (OCR)

Answer:

C

Explanation:

To block any screenshots from being uploaded, the engineering firm should use the ML image classifier feature of Netskope DLP. This feature uses machine learning to detect sensitive information within images, such as screenshots, whiteboards, passports, driver's licenses, etc. The firm can create a DLP policy that blocks any image upload that matches the screenshot classifier. This will prevent employees from circumventing the DLP controls by taking screenshots of sensitive documents.Reference:Improved DLP Image Classifiers,Netskope Data Loss Prevention,The Importance of a Machine Learning-Based Source Code Classifier

Question 8

Question Type: MultipleChoice

Your customer currently only allows users to access the corporate instance of OneDrive using SSO with the Netskope client. The users are not permitted to take their laptops when vacationing, but sometimes they must have access to documents on OneDrive when there is an urgent request. The customer wants to allow employees to remotely access OneDrive from unmanaged devices while enforcing DLP controls to prohibit downloading sensitive files to unmanaged devices.

Which steering method would satisfy the requirements for this scenario?

Options:

A- Use a reverse proxy integrated with their SSO.

B- Use proxy chaining with their cloud service providers integrated with their SSO.

C- Use a forward proxy integrated with their SSO.

D- Use a secure forwarder integrated with an on-premises proxy.

Answer:

A

Explanation:

A reverse proxy integrated with their SSO would satisfy the requirements for this scenario. A reverse proxy intercepts requests from users to cloud apps and applies policies based on user identity, device posture, app, and data context. It can enforce DLP controls to prohibit downloading sensitive files to unmanaged devices. It can also integrate with the customer's SSO provider to authenticate users and allow access only to the corporate instance of OneDrive. The other steering methods are not suitable for this scenario because they either require the Netskope client or do not provide granular control over cloud app activities.

Question 9

Question Type: MultipleChoice

You have deployed a development Web server on a public hosting service using self-signed SSL certificates. After some troubleshooting, you determined that when the Netskope client is enabled, you are unable to access the Web server over SSL. The default Netskope tenant steering configuration is in place.

In this scenario, which two settings are causing this behavior? (Choose two.)

Options:

A- SSL pinned certificates are blocked.

B- Untrusted root certificates are blocked.

C- Incomplete certificate trust chains are blocked.

D- Self-signed server certificates are blocked.

Answer:

B, D

Explanation:

The default Netskope tenant steering configuration blocks untrusted root certificates and self-signed server certificates. These settings are intended to prevent man-in-the-middle attacks and ensure the validity of the SSL connection. However, they also prevent the access to the development Web server that uses self-signed SSL certificates. To allow access to the Web server, the settings need to be changed or an exception needs to be added for the Web server domain.