Netskope

Exam Questions NSK300

Netskope Certified Cloud Security Architect Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

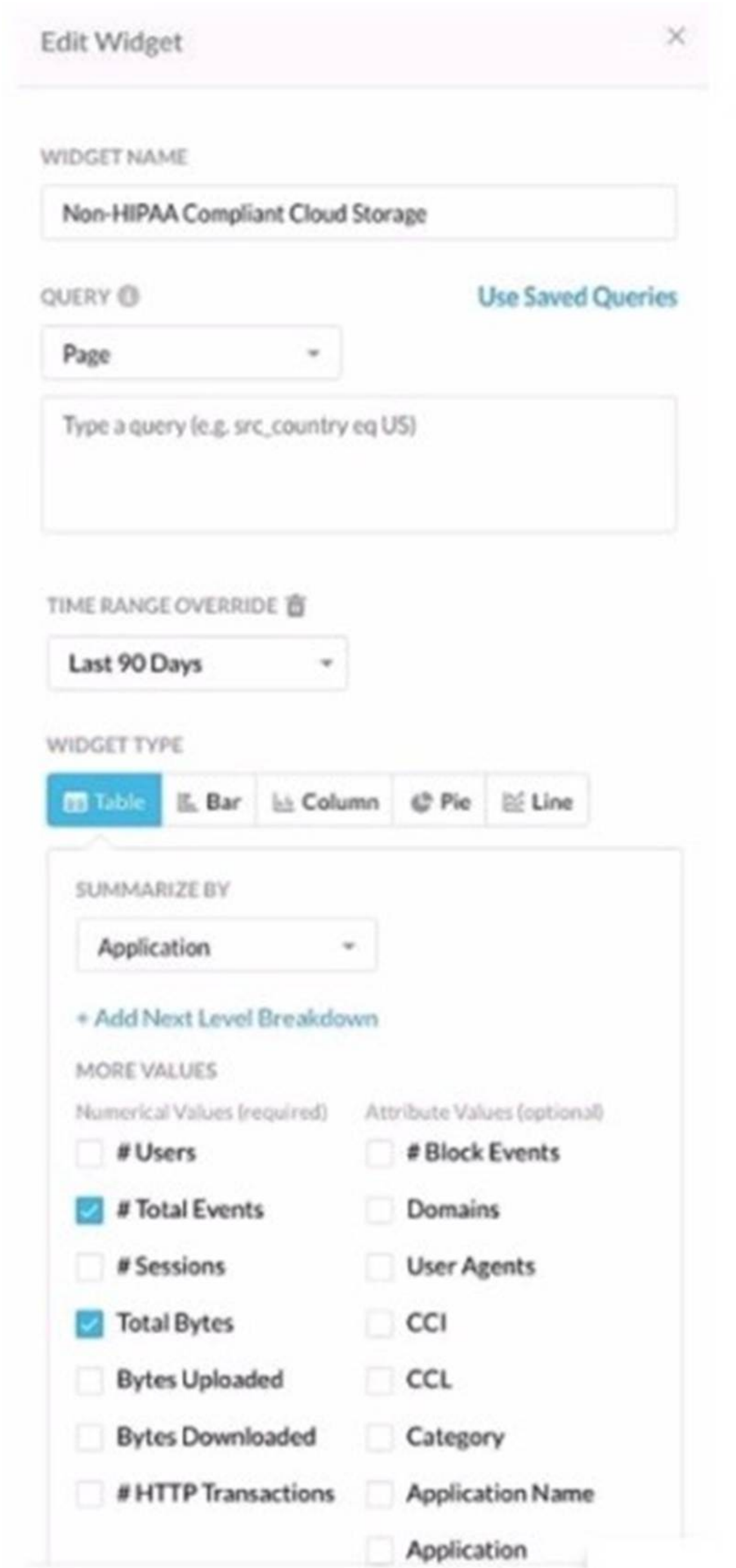
If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Users at your company's branch office in San Francisco report that their clients are connecting, but websites and SaaS applications are slow When troubleshooting, you notice that the users are connected to a Netskope data plane in New York where your company's headquarters is located.
What is a valid reason for this behavior?

A. The Netskope Client's on-premises detection check failed.
B. The Netskope Client's default DNS over HTTPS call is failing.
C. The closest Netskope data plane to San Francisco is unavailable.
D. The Netskope Client's DNS call to Secure Forwarder is failing

Answer: C

NEW QUESTION 2
Review the exhibit.


Edit Widget
WIDGET NAME
Non-HIPAA Compliant Cloud Storage
QUERY
Use Saved Queries
Page
Type a query (e.g. src_country eq US)
TIME RANGE OVERRIDE
Last 90 Days
WIDGET TYPE
Table
Bar
Column
Pie
Line
SUMMARIZE BY
Application
+ Add Next Level Breakdown
MORE VALUES
Numerical Values (required)
Attribute Values (optional)
Users
Total Events
Sessions
Total Bytes
Bytes Uploaded
Bytes Downloaded
HTTP Transactions
Block Events
Domains
User Agents
CCI
CCL
Category
Application Name
Application

You work for a medical insurance provider. You have Netskope Next Gen Secure Web Gateway deployed to all managed user devices with limited block policies. Your manager asks that you begin blocking Cloud Storage applications that are not HIPAA compliant Prior to implementing this policy, you want to verity that no business or departmental applications would be blocked by this policy.
Referring to the exhibit, which query would you use in the Edit Widget window to narrow down the results?

A. app-ccl-compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'
B. Cloud Confidence Compliance neq HIPAA and Cloud Confidence Category is Cloud Storage
C. SELECT application WHERE 'HIPAA' NOT IN app-cci-compliance AND WHERE 'Cloud Storage' IN category
D. app-compliance does not contain HIPAA and category must equal Cloud Storage

Answer: A

NEW QUESTION 3
You jus! deployed and registered an NPA publisher for your first private application and need to provide access to this application for the Human Resources (HR) users group only. How would you accomplish this task?

A. 1. Enable private app steering in the Steering Configuration assigned to the HR group.* 2. Create a new Private App.* 3. Create a new Real-time Protection policy as follows;Source = HR user group Destination = Private App Action = Allow
B. 1. Create a new private app and assign it to the HR user group.* 2. Create a new Real-time Protection policy as follows:Source = HR user group Destination = Private App Action = Allow.
C. 1. Enable private app steering in Tenant Steering Configuration.* 2. Create a new private app and assign it to the HR user group.
D. 1. Enable private app steering in the Steering Configuration assigned to the HR group.* 2. Create a new private app and assign it to the HR user group* 3. Create a new Real-time Protection policy as follows:Source = HR user group Destination = Private App Action = Allow

Answer: A

NEW QUESTION 4
You are using Netskope CSPM for security and compliance audits across your multi-cloud environments. To decrease the load on the security operations team, you are researching how to auto-re mediate some of the security violations found in low-risk environments.
Which statement is correct in this scenario?

A. Netskope does not support automatic remediation of security violation results due to the high risk associated with it.
B. You can use Netskope API-enabled Protection for auto-remediation of security violation results.
C. You can use Netskope Auto-remediation frameworks from the public Netskope GitHub Open Source repository for auto-re mediation of security violation results.
D. You can use Netskope Cloud Exchange for auto-remediation of security violation results.

Answer: C

Explanation:
Netskope supports automatic remediation of security violations through its Auto-Remediation frameworks, which are available in the public Netskope GitHub Open Source repository. These frameworks allow for the automatic mitigation of risks associated with security misconfigurations in your cloud environment. The Netskope Auto-Remediation framework for AWS, for example, deploys a set of AWS Lambda functions that query the Netskope API at scheduled intervals and automatically mitigates supported violations 1. Similarly, there are frameworks for GCP and other cloud environments that follow the same principle 2 . This capability is particularly useful for low-risk environments where the security operations team??s workload can be reduced by automating the remediation process.
[: The answer is based on the information provided by Netskope??s community resources and documentation, which detail the use of their Auto-Remediation frameworks for various cloud platforms,]

NEW QUESTION 5
Review the exhibit.

You are the proxy administrator for a medical devices company. You recently changed a pilot group of users from cloud app steering to all Web traffic. Pilot group users have started to report that they receive the error shown in the exhibit when attempting to access the company intranet site that is publicly available. During troubleshooting, you realize that this site uses your company's internal certificate authority for SSL certificates.
Which three statements describe ways to solve this issue? (Choose three.)

A. Import the root certificate for your internal certificate authority into Netskope.
B. Bypass SSL inspection for the affected site(s).
C. Create a Real-time Protection policy to allow access.
D. Change the SSL Error Settings from Block to Bypass in the Netskope tenant.
E. Instruct the user to proceed past the error message

Answer: ABD

NEW QUESTION 6
You are attempting to merge two Advanced Analytics reports with DLP incidents: Report A with 3000 rows and Report B with 6000 rows. Once merged, you notice that the merged report is missing a significant number of rows.
What is causing this behavior?

A. Netskope automatically deduplicates data in merged reports.
B. Missing data is due to viewing limits.
C. Filters are applied differently to dimensions and measures
D. Visualizations have a system limit of 5000 rows.

Answer: B

Explanation:
When merging two Advanced Analytics reports in Netskope, if the merged report is missing rows, it is likely due to viewing limits within the system. Netskope??s Advanced Analytics platform has limitations on the number of rows that can be viewed at once, which can result in missing data when dealing with large reports. This viewing limit ensures performance and manageability of the data within the system.
[: The behavior of data viewing limits in Netskope Advanced Analytics is discussed in the Netskope Knowledge Portal, which provides insights into how data is explored and managed within the platform1,]

NEW QUESTION 7
Your Netskope Client tunnel has connected to Netskope; however, the user is not receiving any steering or client configuration updates What would cause this issue?

A. The client is unable to establish communication to add-on-[tenantl.goskope.com.
B. The client is unable to establish communication to gateway-(tenant|.goskope.com.
C. The Netskope Client service is not running.
D. An invalid steering exception was created in the tenant

Answer: C

Explanation:
When the Netskope Client service is not running, it cannot execute the necessary processes to receive steering or client configuration updates. The service must be active to establish communication with the Netskope cloud and apply the configurations and policies defined by the administrator.
[: This information aligns with the Netskope Cloud Security Architect learning objectives and documents, which emphasize the importance of running client services for proper communication and functionality,]

NEW QUESTION 8
You want to verify that Google Drive is being tunneled to Netskope by looking in the nsdebuglog file. You are using Chrome and the Netskope Client to steer traffic. In this scenario, what would you expect to see in the log file?
A)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:64000, process: google drive to host: play.googleapis.com, addr: 172.217.4.46:443 to nsProxy
```

B)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:63720, process: google chrome helper to host: drive.google.com, addr: 172.217.4.46:443 to nsProxy
```

C)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info bypassAppMgr.cpp:538 BypassAppMgr Bypassing UDP flow to process
google chrome helper ip: 172.217.4.46, Port: 443, host: drive.google.com
```

D)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info AppProxyProvider.mm:303 main New UDP flow: Process = google chrome
helper, IP:Port = [8.8.8.8:53]
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 9
Your organization's software deployment team did the initial install of the Netskope Client with SCCM. As the Netskope administrator, you will be responsible for all up-to-date upgrades of the client.
Which two actions would be required to accomplish this task9 (Choose two.)

A. In the Client Configuration, set Upgrade Client Automatically to Latest Release.
B. Set the installmode-IDP flag during the original Install.
C. Set the autoupdate-on flag during the original Install.
D. In the Client Configuration, set Upgrade Client Automatically to Specific Golden Release.

Answer: AC

NEW QUESTION 10
You are building an architecture plan to roll out Netskope for on-premises devices. You determine that tunnels are the best way to achieve this task due to a lack of support for explicit proxy in some instances and IPsec is the right type of tunnel to achieve the desired security and steering.
What are three valid elements that you must consider when using IPsec tunnels in this scenario? (Choose three.)

A. cipher support on tunnel-initiating devices
B. bandwidth considerations

C. the categories to be blocked
D. the impact of threat scanning performance
E. Netskope Client behavior when on-premises

Answer: ABD

NEW QUESTION 10
A company needs to block access to their instance of Microsoft 365 from unmanaged devices. They have configured Reverse Proxy and have also created a policy that blocks login activity for the AD group "marketing-users" for the Reverse Proxy access method. During UAT testing, they notice that access from unmanaged devices to Microsoft 365 is not blocked for marketing users. What is causing this issue?

A. There is a missing group name in the SAML response.
B. The username in the name ID field is not in the format of the e-mail address.
C. There is an invalid certificate in the SAML response.
D. The username in the name ID field does not have the "marketing-users" group name.

Answer: A

NEW QUESTION 15
You recently began deploying Netskope at your company. You are steering all traffic, but you discover that the Real-time Protection policies you created to protect Microsoft OneDrive are not being enforced.
Which default setting in the Ul would you change to solve this problem?

A. Disable the default Microsoft appsuite SSL rule.
B. Disable the default certificate-pinned application
C. Remove the default steering exception for domains.
D. Remove the default steering exception for Cloud Storage.

Answer: C

NEW QUESTION 20
What are three valid Instance Types for supported SaaS applications when using Netskope's API-enabled Protection? (Choose three.)

A. Forensic
B. API Data Protection
C. Behavior Analytics
D. DLP Scan
E. Quarantine

Answer: ABE

NEW QUESTION 21
You want to see all instances of malware that were detected by the Netskope Cloud Sandbox.
Which process would you use to achieve this task in the Netskope tenant UI?

A. Go to Incidents > Malicious Sites, and perform the detection_engine eq ??Advanced Detection?? query.
B. Go to Incidents > Malware and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.
C. Go to Skope IT > Alerts, switch to Query Mode and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.
D. Go to Skope IT > Page Events, switch to Query Mode and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.

Answer: B

NEW QUESTION 22
You configured a pair of IPsec funnels from the enterprise edge firewall to a Netskope data plane. These tunnels have been implemented to steer traffic for a set of defined HTTPS SaaS applications accessed from end-user devices that do not support the Netskope Client installation. You discover that all applications steered through this tunnel are non- functional.
According to Netskope. how would you solve this problem?

A. Restart the tunnel to stop the tunnel from flapping.
B. Downgrade from IKE v2 to IKE v1.
C. Install the Netskope root and intermediate certificates on the end-user devices.
D. Disable Perfect Forward Secrecy on the tunnel configuration.

Answer: C

NEW QUESTION 24
You have deployed Netskope to all users of the organization and you are now ready to begin ingesting all events, alerts, and Web transactions into your SIEM as a part of your requirements.
What are three ways in which you would accomplish this task? (Choose three.)

A. Use custom API calls to ingest to a data lake and then into your SIEM.
B. Use the Netskope Publisher to a stream syslog to your SIEM.
C. Use syslog directly to Splunk.
D. Use Cloud Log Shipper to an IaaS storage repository and then into your SIEM.

Answer: ACD

NEW QUESTION 25
You successfully configured Advanced Analytics to identify policy violation trends Upon further investigation, you notice that the activity is NULL. Why is this happening in this scenario?

A. The SSPM policy was not configured during setup.
B. The REST API v1 token has expired.
C. A policy violation was identified using API Protection.
D. A user accessed a static Web page.

Answer: D

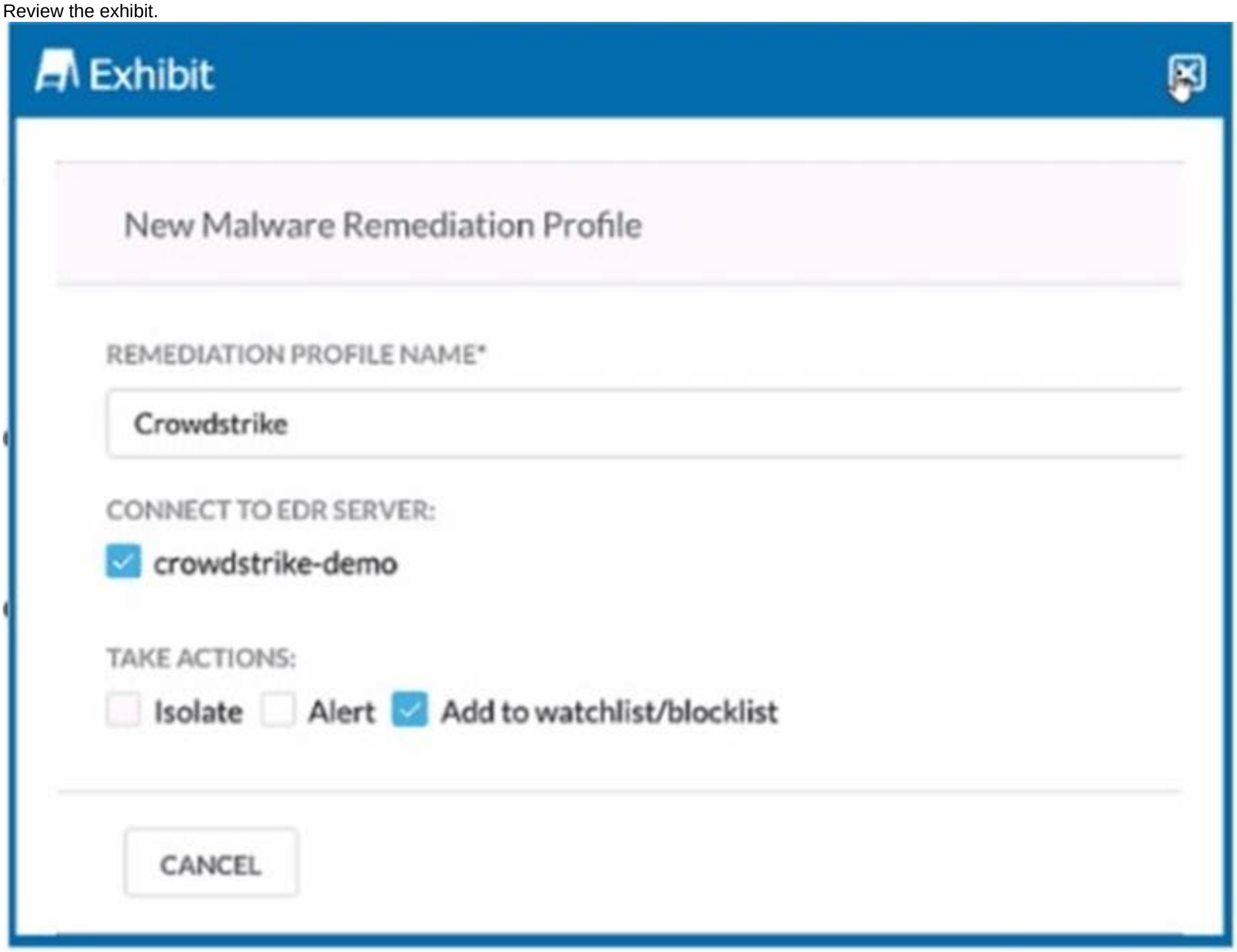
Explanation:
The reason for the activity being NULL in this scenario is likely because a user accessed a static Web page . In Netskope??s Advanced Analytics, when the activity is reported as NULL, it often indicates that there was no dynamic interaction or transaction to record, which is typical when a static web page is accessed 1 . Static web pages do not generate the kind of events or activities that are tracked by policies, hence they appear as NULL in the activity field.
[: This explanation is supported by the Netskope Knowledge Portal, which mentions that applications fields with null values indicate incidents generated from web traffic, such as accessing static web pages2. Further information on interpreting NULL values in Advanced Analytics reports can be found in the Netskope documentation1., , In Advanced Analytics, the Activity field is populated only when Netskope can identify a specific app activity (e.g., upload, download, edit, share, delete)., When the traffic is simply generic web browsing — especially static web pages (HTML, images, CSS, JS) — Netskope cannot map the request to an application-level activity, so the Activity field becomes:, ?? NULL, This is expected behavior for traffic that is:, Not associated with a sanctioned/unsanctioned cloud app, Does not contain a user action like upload/download, Classified only as generic web content (static website), Why other options are incorrect, A. The SSPM policy was not configured during setupSSPM configuration does not impact the Activity field in Analytics for inline events., B. The REST API v1 token has expiredAPI token expiration would impact API logs collection, not inline event Activity values., C. A policy violation was identified using API ProtectionAPI Protection events always include an activity type (e.g., ??Download via API??), so they wouldn??t show NULL., ,]

NEW QUESTION 27
Your CISO asks that you to provide a report with a visual representation of the top 10 applications (by number of objects) and their risk score. As the administrator, you decide to use a Sankey visualization in Advanced Analytics to represent the data in an efficient manner.
In this scenario, which two field types are required to produce a Sankey Tile in your report? (Choose two.)

A. Dimension
B. Measure
C. Pivot Ranks
D. Period of Type

Answer: AB

NEW QUESTION 28
Review the exhibit.



You are asked to integrate Netskope with Crowdstrike EDR. You added the Remediation profile shown in the exhibit.

Which action will this remediation profile take?

A. The endpoint will be isolated.
B. The malware hash will be added as an IOC in Crowdstrike.
C. The malware will be quarantined.
D. The malware hash will be added as an IOC in Netskope.

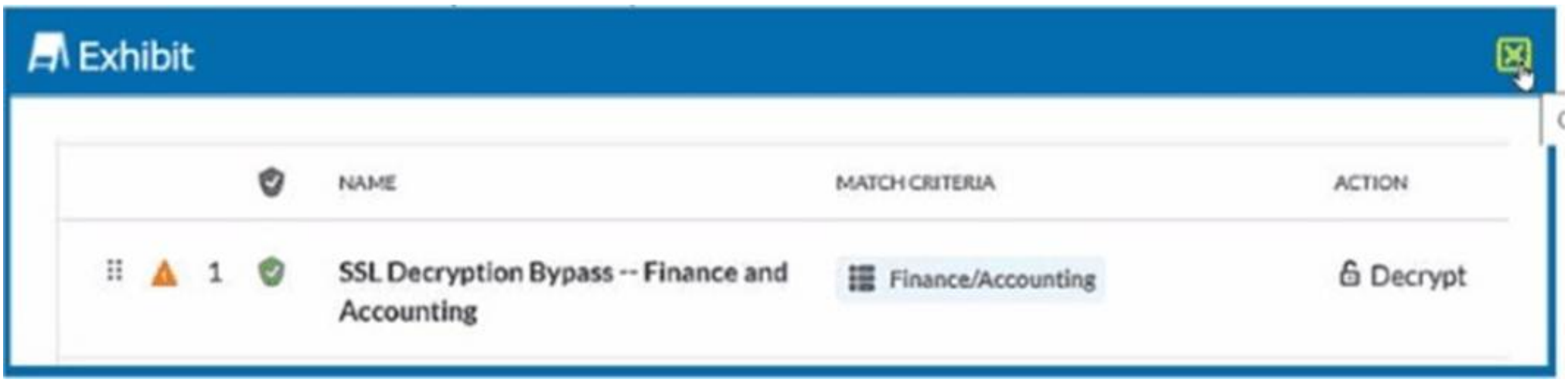
Answer: B

NEW QUESTION 30
You do not want a scheduled Advanced Analytics dashboard to be automatically updated when Netskope makes improvements to that dashboard. In this scenario, what would you do to retain the original dashboard?

A. Create a new dashboard from scratch that mimics the Netskope dashboard you want to use.
B. Copy the dashboard into your Group or Personal folders and schedule from these folders.
C. Ask Netskope Support to provide the dashboard and import into your Personal folder.
D. Download the dashboard you want and Import from File into your Group or Personal folder.

Answer: B

NEW QUESTION 31
Review the exhibit.



You created an SSL decryption policy to bypass the inspection of financial and accounting Web categories. However, you still see banking websites being inspected.
Referring to the exhibit, what are two possible causes of this behavior? (Choose two.)

A. The policy is in a "disabled" state.
B. An incorrect category has been selected
C. The policy is in a "pending changes" state.
D. An incorrect action has been specified.

Answer: BD

NEW QUESTION 34
Your client is an NG-SWG customer. They are going to use the Explicit Proxy over Tunnel (EPoT) steering method. They have a specific list of domains that they do not want to steer to the Netskope Cloud.
What would accomplish this task"

A. Define exception domains in the PAC file.
B. Define exceptions in the Netskope steering configuration
C. Create a real-time policy with a bypass action.
D. Use an SSL decryption policy.

Answer: A

NEW QUESTION 37
You created a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, but determine that the policy is too restrictive. Specifically, users are complaining that normal websites have stopped rendering properly.
How would you solve this problem?

A. Create a Real-time Protection policy to allow the Browse activity to the Amazon S3 application.
B. Create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category
C. Create a Real-time Protection policy to allow the Download activity to the Cloud Storage category
D. Create a Real-time Protection policy to allow the Download activity to the Amazon S3 application

Answer: B

NEW QUESTION 41
You want to integrate with a third-party DLP engine that requires ICAP. In this scenario, which Netskope platform component must be configured?

A. On-Premises Log Parser (OPLP)
B. Secure Forwarder
C. Netskope Cloud Exchange
D. Netskope Adapter

Answer: B

NEW QUESTION 45
You are consuming Audit Reports as part of a Salesforce API integration. Someone has made a change to a Salesforce account record field that should not have been made and you are asked to venfy the previous value of the structured data field. You have the approximate date and time of the change, user information, and the new field value.
How would you accomplish this task?

A. Create a classic report and apply a query that filters on the changed field value.
B. Use the Application Events Data Collection within Advanced Analytics and filter on the changed field value.
C. Query Skope IT Page Events and look for the specific Page URL that was called under the Application section.
D. Query Skope IT for an Access Method of API Connector and search Application Event Details for the Old Value field using the User details and Edit Activity.

Answer: D

Explanation:
To verify the previous value of a structured data field in Salesforce after an unauthorized change, you would use Skope IT with an Access Method of API Connector. This method allows you to search the Application Event Details for the ??Old Value?? field. By filtering with the user details and the edit activity, you can pinpoint the exact change and retrieve the original value of the field.
[: The approach is consistent with the Netskope Cloud Security Architect??s guidelines for using API Data Protection with Salesforce.The documentation provides a detailed procedure for configuring Salesforce for API Data Protection, which includes the use of Netskope Audit Reports and the ability to track changes through the ??Old Value?? field,]

NEW QUESTION 47
You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?

A. Alert, Quarantin
B. Block, User Notification
C. Alert, User Notification
D. Alert only
E. Alert, Quarantine

Answer: D

Explanation:
When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine . These actions allow you to be notified when a policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately 1 .
[: The information about policy actions for AWS S3 bucket scans is available in the Netskope documentation, which provides guidance on creating API Data Protection policies for scanning S3 buckets and the actions that can be taken when a policy is triggered1.,]

NEW QUESTION 52
You want to enable the Netskope Client to automatically determine whether it is on- premises or off-premises. Which two options in the Netskope Ul would you use to accomplish this task? (Choose two.)

A. the All Traffic option in the Steering Configuration section of the Ul
B. the New Exception option in the Traffic Steering options of the Ul
C. the Enable Dynamic Steering option in the Steering Configuration section of the Ul
D. the On Premises Detection option under the Client Configuration section of the Ul

Answer: CD

Explanation:
To enable the Netskope Client to automatically determine whether it is on-premises or off-premises, you can use the following options in the Netskope UI:
Enable Dynamic Steering:
This option is available in theSteering Configurationsection of the UI.
By enabling dynamic steering, the Netskope Client can intelligently determine the appropriate data plane (on-premises or cloud) based on the user??s location and network conditions.
It ensures that traffic is directed to the optimal data plane for improved performance and security.
[Reference: Netskope Documentation on Dynamic Steering, On Premises Detection:, This option is available under theClient Configurationsection of the UI., By configuring on-premises detection, the Netskope Client can identify whether it is connected to the local network (on-premises) or accessing resources from outside (off-premises)., It helps in applying relevant policies and steering traffic accordingly., Reference: Netskope Documentation on Client Configuration,]

NEW QUESTION 54
Your company just had a new Netskope tenant provisioned and you are asked to create a secure tenant configuration. In this scenario, which two default settings should you change? {Choose two.)

A. Change Safe Search to Disabled
B. Change Untrusted Root Certificate to Block.
C. Change the No SNI setting to Block.
D. Change "Disallow concurrent logins by an Admin" to Enabled.

Answer: BD

NEW QUESTION 58
You are asked to ensure that a Web application your company uses is both reachable and decrypted by Netskope. This application is served using HTTPS on port 6443. Netskope is configured with a default Cloud Firewall configuration and the steering configuration is set for All Traffic.

Which statement is correct in this scenario?

A. Create a Firewall App in Netskope along with the corresponding Real-time Protection policy to allow the traffic.
B. Nothing is required since Netskope is steering all traffic.
C. Enable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port
D. Enable "Steer non-standard ports" in the steering configuration and create a corresponding Real-time Protection policy to allow the traffic

Answer: C

NEW QUESTION 60
You are architecting a Netskope steering configuration for devices that are not owned by the organization The users could be either on-premises or off-premises and the architecture requires that traffic destined to the company's instance of Microsoft 365 be steered to Netskope for inspection.
How would you achieve this scenario from a steering perspective?

A. Use IPsec and GRE tunnels.
B. Use reverse proxy.
C. Use explicit proxy and the Netskope Client
D. Use DPoP and Secure Forwarder

Answer: B

NEW QUESTION 62
You are assisting your network administrator to troubleshoot an issue with client-based NPA.
In the Netskope UI, what information do you need from the administrator to run the NPA troubleshooter for this user? (Choose two.)

A. Publisher Name
B. User & Device
C. Private App ID
D. Private App Name

Answer: BD

NEW QUESTION 65
You are asked to create a Real-time Protection policy to inspect outbound e-mail for DLP violations. You must prevent sensitive e-mail from leaving the corporate mail relay.
In this scenario, which Real-time Protection policy action must be specified?

A. Alert
B. Block
C. Forward to Proxy
D. Add SMTP Header

Answer: D

NEW QUESTION 67
.....

Relate Links

100% Pass Your NSK300 Exam with Exambible Prep Materials

https://www.exambible.com/NSK300-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/