Best Netskope NSK100 2024 Training With 62 QA's [Q24-Q40

Best Netskope NSK100 2024 Training With 62 QA's
Netskope NSK100 Certification Exam Questions

Netskope NSK100 Exam Syllabus Topics:

TopicDetailsTopic 1- Identifying cloud risk using the Cloud Confidence Index (CCI)- Common industry compliance standards Topic 2- Common cloud service model concepts- Collect log files used for service requestsTopic 3- Traffic steering concepts- Basic configuration elementsTopic 4- Real-time inline or API policy configuration concepts- Data-in-motion protection compared to data-at-rest conceptsTopic 5- Policy-related misconfigurations- Features and architectural benefitsTopic 6- Netskope Platform Management- Cloud security risk management- reduction

NEW QUESTION 24

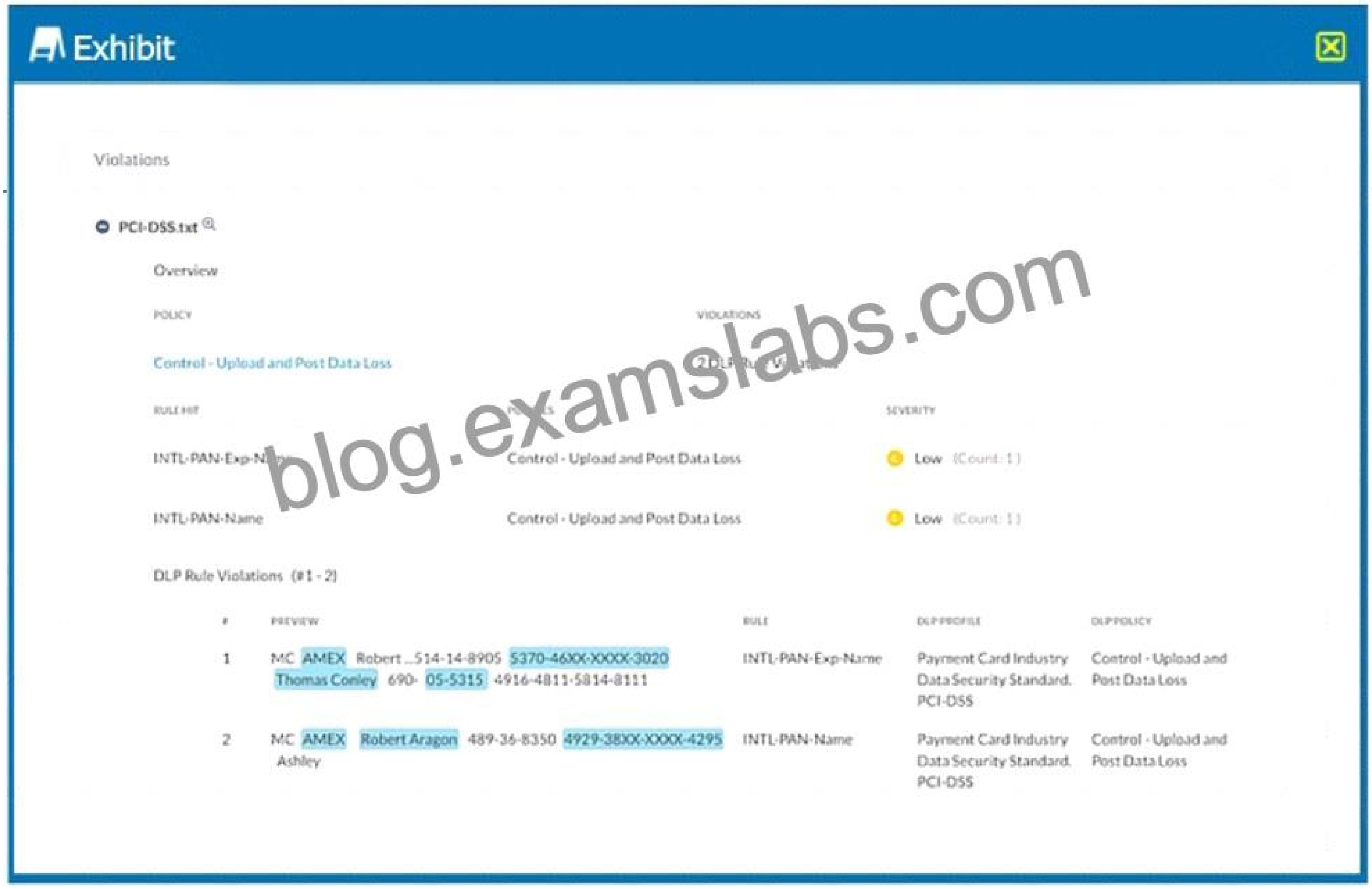
Which two controls are covered by Netskope&#8217;s security platform? (Choose two.)
* ZTNA
* VPN
* CASB

* EDR
Explanation

Netskope&#8217;s security platform covers two controls: ZTNA and CASB. ZTNA stands for Zero Trust Network Access, which is a solution that provides secure and granular access to private applications without exposing them to the internet or requiring VPNs. CASB stands for Cloud Access Security Broker, which is a solution that provides visibility and control over cloud services and web traffic, as well as data and threat protection for cloud users and devices. References: Netskope PlatformNetskope ZTNANetskope CASB

NEW QUESTION 25

Exhibit



Violations

PCI-DSS.txt

Overview

POLICY	VIOLATIONS
Control - Upload and Post Data Loss	2 DLP Rule Violations

RULE HIT	POLICIES	SEVERITY
INTL-PAN-Exp-Name	Control - Upload and Post Data Loss	Low (Count: 1)
INTL-PAN-Name	Control - Upload and Post Data Loss	Low (Count: 1)

DLP Rule Violations (#1 - 2)

#	PREVIEW	RULE	DLP PROFILE	DLP POLICY
1	MC AMEX Robert ...514-14-8905 5370-46XX-XXXX-3020 Thomas Conley 690- 05-5315 4916-4811-5814-8111	INTL-PAN-Exp-Name	Payment Card Industry Data Security Standard. PCI-DSS	Control - Upload and Post Data Loss
2	MC AMEX Robert Aragon 489-36-8350 4929-38XX-XXXX-4295 Ashley	INTL-PAN-Name	Payment Card Industry Data Security Standard. PCI-DSS	Control - Upload and Post Data Loss

Which portion of the interface shown in the exhibit allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content?
* Skope IT-> Alerts
* Incidents -> DLP
* API-enabled Protection -> Inventory
* Reports -> New Report
Explanation

The portion of the interface shown in the exhibit that allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content is Incidents -> DLP. 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. You can also assign an owner to an incident, change its status and severity, add notes or comments, and view the excerpts of the violating content that triggered the DLP policy. References: Netskope Incidents Dashboard

NEW QUESTION 26

Your company asks you to obtain a detailed list of all events from the last 24 hours for a specific user. In this scenario, what are two methods to accomplish this task? (Choose two.)
* Export the data from Skope IT Alerts.
* Use the Netskope REST API.
* Export the data from Skope IT Application Events.
* Use the Netskope reporting engine.
Explanation

In this scenario, there are two methods to obtain a detailed list of all events from the last 24 hours for a specific user. One method is to export the data from Skope IT Application Events, which is a feature in the Netskope platform that allows you to view and analyze all the activities performed by users on cloud applications. You can use filters to narrow down your search by user name, time range, application, activity, and other criteria. You can then export the data to a CSV or JSON file for further analysis or reporting.

Another method is to use the Netskope REST API, which is a programmatic interface that allows you to access and manipulate data from the Netskope platform using HTTP requests. You can use the API to query for events by user name, time range, application, activity, and other parameters. You can then retrieve the data in JSON format for further analysis or integration with other tools. Using the Netskope reporting engine or exporting the data from Skope IT Alerts are not methods to obtain a detailed list of all events from the last 24 hours for a specific user, as they are more suited for generating summary reports or alerts based on predefined criteria or thresholds, rather than granular event data. References: [Netskope Skope IT Application Events],

[Netskope REST API].

NEW QUESTION 27

Your department is asked to report on GDPR data publicly exposed in Microsoft 365, Salesforce. and Slack-sanctioned cloud applications. Which deployment model would you use to discover this data?
* reverse proxy
* on-premises appliance
* API-enabled protection
* inline protection
Explanation

To discover GDPR data publicly exposed in Microsoft 365, Salesforce, and Slack-sanctioned cloud applications, you need to use a deployment model that allows Netskope to access and scan the data stored in these applications using out-of-band API connections. The deployment model that would match this requirement is API-enabled protection, which is a feature in the Netskope platform that allows you to connect your sanctioned cloud applications to Netskope using API connectors. This enables you to discover sensitive data, enforce near real-time policy controls, and quarantine malware in your cloud applications without affecting user experience or performance. You can use Netskope&#8217;s data loss prevention (DLP) engine to scan for GDPR data in your cloud applications and identify any public exposure or sharing settings that may violate the regulation. A reverse proxy, an on-premises appliance, or an inline protection are not deployment models that would help you discover GDPR data publicly exposed in your sanctioned cloud applications, as they are more suitable for inline modes that rely on intercepting traffic to and from these applications in real time, rather than accessing data stored in these applications using APIs. References: [Netskope SaaS API-enabled Protection], [Netskope Data Loss Prevention].

NEW QUESTION 28

Which two traffic steering configurations are supported by Netskope? (Choose two.)
* browser isolation traffic only
* cloud applications only
* all Web traffic including cloud applications
* Web traffic only
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. References: Steering ConfigurationCreating a Steering Configuration

NEW QUESTION 29

You want to prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application. In this scenario, which method would you use?
* Use a stronger encryption algorithm.
* Use certificate pinning.
* Use a proxy for the connection.
* Use a weaker encryption algorithm.
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 &#8220;pin&#8221; 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. References: Certificate pinning &#8211; IBMCertificate and Public Key Pinning | OWASP Foundation

NEW QUESTION 30

You want to take into account some recent adjustments to CCI scoring that were made in your Netskope tenant.

In this scenario, which two CCI aspects in the Ul would be used in a real-time protection policy? (Choose two.)
* App Tag
* CCL
* App Score
* GDPR Readiness
Explanation

To take into account some recent adjustments to CCI scoring that were made in your Netskope tenant, you can use the App Tag and

App Score aspects in the UI to create a real-time protection policy. The App Tag is a label that indicates the level of enterprise readiness of a cloud app based on its CCI score. The App Score is a numerical value that represents the CCI score of a cloud app based on various criteria such as security, auditability, and business continuity. You can use these aspects to filter cloud apps by their CCI ratings and apply policies accordingly. For example, you can create a policy that blocks access to cloud apps with an App Tag of Poor or an App Score below 50. References: Netskope Cloud Confidence IndexCreating Real-Time Policies for Cloud Applications

NEW QUESTION 31

Which three technologies describe the primary cloud service models as defined by the National Institute of Standards and Technology (NIST)? (Choose three.)
* Cloud Service Provider (CSP)
* Identity as a Service (IDaaS)
* Platform as a Service (PaaS)
* Software as a Service (SaaS)
* Infrastructure as a Service (laaS)
Explanation

The three technologies that describe the primary cloud service models as defined by the National Institute of Standards and Technology (NIST) are Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). These service models are based on the type of computing capability that is provided by the cloud provider to the cloud consumer over a network. According to NIST, these service models have the following definitions:

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider&#8217;s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

References: The NIST Definition of Cloud ComputingNIST Cloud Computing Program

NEW QUESTION 32

What are two uses for deploying a Netskope Virtual Appliance? (Choose two.)
* as an endpoint for Netskope Private Access (NPA)
* as a local reverse-proxy to secure a SaaS application
* as a log parser to discover in-use cloud applications
* as a Secure Forwarder to steer traffic
Explanation

A Netskope Virtual Appliance is a software-based appliance that can be deployed on-premises or in the cloud to provide various functions and features for the Netskope Security Cloud platform. One use for deploying a Netskope Virtual Appliance is as an endpoint for Netskope Private Access (NPA), which is a service that allows users to securely access private applications without exposing them to the internet or using VPNs.

Another use for deploying a Netskope Virtual Appliance is as a Secure Forwarder to steer traffic from on-premises devices or networks to the Netskope platform for inspection and policy enforcement. Using a Netskope Virtual Appliance as a local reverse-proxy to secure a SaaS application or as a log parser to discover in-use cloud applications are not valid uses, as these functions are performed by other components of the Netskope Security Cloud platform, such as the Cloud Access Security Broker (CASB) or the Cloud XD engine. References: Netskope Security Cloud Operation & Administration (NSCO&A) &#8211; Classroom Course, Module 2: Architecture Overview; [Netskope Private Access]; [Netskope Secure Forwarder].

NEW QUESTION 33

Which two functions are available for both inline and API protection? (Choose two.)
* multi-factor authentication
* threat protection
* DLP
* Cloud Security Posture Management (CSPM)
Explanation

Netskope provides both inline and API protection for cloud applications and web traffic. Inline protection refers to the real-time inspection and enforcement of policies on the traffic between users and cloud applications, using Netskope&#8217;s inline proxy mode. API protection refers to the retrospective inspection and enforcement of policies on the data that is already stored in cloud applications, using Netskope&#8217;s API connectors. Two functions that are available for both inline and API protection are threat protection and DLP.

Threat protection is the capability to detect and block malware, ransomware, phishing, and other cyber threats that may compromise cloud data or users. DLP is the capability to detect and protect sensitive data, such as personal information, intellectual property, or regulated data, that may be exposed or leaked through cloud applications. References: Netskope Inline Proxy ModeNetskope API ProtectionNetskope Threat ProtectionNetskope DLP Engine

NEW QUESTION 34

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

In this scenario, which Netskope feature would you recommend to the customer?
* Netskope Secure Web Gateway (SWG)
* Netskope Cloud Security Posture Management (CSPM)
* Netskope Advanced DLP and Threat Protection
* Netskope SaaS Security Posture Management (SSPM)
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&#8217;s security standards and best practices. Netskope CSPM can also alert, report, or remediate the misconfigurations automatically or manually. References: Netskope CSPMCloud Security Posture Management

NEW QUESTION 35

You need to create a service request ticket for a client-related issue using the Netskope client Ul. In this scenario, you generate the client logs by right-clicking on the system tray icon and choosing
* Save logs
* Configuration
* Troubleshoot
* Help
Explanation

To create a service request ticket for a client-related issue using the Netskope client UI, you need to generate the client logs by right-clicking on the system tray icon and choosing Troubleshoot. This will open a window where you can select the option to Save Logs, which will create a zip file containing the client logs. You can then attach this file to your service request ticket and provide any relevant details about the issue. Choosing Save logs, Configuration, or Help will not generate the client logs, as they perform different functions, such as saving the current configuration, opening the settings menu, or opening the help page. References: [Netskope Client Troubleshooting].

NEW QUESTION 36

Why would you want to define an App Instance?
* to create an API Data Protection Policy for a personal Box instance
* to differentiate between an enterprise Google Drive instance vs. a personal Google Drive instance
* to enable the instance_id attribute in the advanced search field when using query mode
* to differentiate between an enterprise Google Drive instance vs. an enterprise Box instance
Explanation

An App Instance is a feature in the Netskope platform that allows you to define and identify different instances of the same cloud application based on the domain name or URL. For example, you can define an App Instance for your enterprise Google Drive instance (such as drive.google.com/a/yourcompany.com) and another App Instance for your personal Google Drive instance (such as drive.google.com). This way, you can differentiate between them and apply different policies and actions based on the App Instance. You would want to define an App Instance to achieve this level of granularity and control over your cloud application activities. Creating an API Data Protection Policy for a personal Box instance, enabling the instance_id attribute in the advanced search field, or differentiating between an enterprise Google Drive instance vs. an enterprise Box instance are not valid reasons to define an AppInstance, as they are either unrelated or irrelevant to the App Instance feature. References: Netskope Security Cloud Operation & Administration (NSCO&A) &#8211; Classroom Course, Module 5: Real-Time Policies, Lesson 4: App Instances.

NEW QUESTION 37

When using an out-of-band API connection with your sanctioned cloud service, what are two capabilities available to the administrator? (Choose two.)
* to quarantine malware
* to find sensitive content
* to block uploads
* to allow real-time access
Explanation

When using an out-of-band API connection with your sanctioned cloud service, two capabilities available to the administrator are: to quarantine malware and to find sensitive content. An out-of-band API connection is a method of integrating Netskope with your cloud service provider using the APIs exposed by the cloud service.

This allows Netskope to access the data that is already stored in the cloud service and perform retrospective inspection and enforcement ofpolicies. One capability that the administrator can use with an out-of-band API connection is to quarantine malware. This means that Netskope can scan the files in the cloud service for malware, ransomware, phishing, and other threats, and move them to a quarantine folder or delete them if they are found to be malicious. Another capability that the administrator can use with an out-of-band API connection is to find sensitive content. This means that Netskope can scan the files in the cloud service for sensitive data, such as personal information, intellectual property, or regulated data, and apply data loss prevention (DLP) policies to protect them. For example, Netskope can encrypt, redact, or watermark the files that contain sensitive content, or notify the administrator or the file owner about the exposure. References: Netskope API ProtectionReal-time Control and Data Protection via Out-of-Band API

NEW QUESTION 38

You are working with a large retail chain and have concerns about their customer data. You want to protect customer credit card data so that it is never exposed in transit or at rest. In this scenario, which regulatory compliance standard should be used to govern this data?
* SOC 3
* PCI-DSS
* AES-256
* ISO 27001
Explanation

PCI-DSS stands for Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that handle credit card data. It aims to protect cardholder data from unauthorized access, disclosure, or theft, both in transit and at rest. PCI-DSS covers various aspects of security, such as encryption, authentication, firewall, logging, monitoring, andincident response. If you are working with a large retail chain and have concerns about their customer data, you should use PCI-DSS as the regulatory compliance standard to govern this data. SOC 3, AES-256, and ISO 27001 are not specific to credit card data protection, although they may have some relevance to general security practices. References: [PCI-DSS], [SOC 3], [AES-256],

[ISO 27001].

NEW QUESTION 39

Your company asks you to obtain a detailed list of all events from the last 24 hours for a specific user. In this scenario, what are two methods to accomplish this task? (Choose two.)
* Use the Netskope reporting engine.
* Export the data from Skope IT Application Events.
* Use the Netskope REST API.
* Export the data from Skope IT Alerts.
Explanation

In this scenario, there are two methods to obtain a detailed list of all events from the last 24 hours for a specific user. One method is to export the data from Skope IT Application Events, which is a feature in the Netskope platform that allows you to view and analyze all the activities performed by users on cloud applications. You can use filters to narrow down your search by user name, time range, application, activity, and other criteria. You can then export the data to a CSV or JSON file for further analysis or reporting.

Another method is to use the Netskope REST API, which is a programmatic interface that allows you to access and manipulate data from the Netskope platform using HTTP requests. You can use the API to query for events by user name, time range, application, activity, and other parameters. You can then retrieve the data in JSON format for further analysis or integration with other tools.

Using the Netskope reporting engine or exporting the data from Skope IT Alerts are not methods to obtain a detailed list of all events from the last 24 hours for a specific user, as they are more suited for generating summary reports or alerts based on predefined criteria or thresholds, rather than granular event data. References: [Netskope Skope IT Application Events],

[Netskope REST API].

NEW QUESTION 40

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?
* You can find DLP violations under Forensic profiles.
* DLP incidents for a file are not visible when the file is deleted.
* You can find DLP violations under the Incidents dashboard.
* You must create a forensic profile so that an incident is created.
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. References: Netskope Incidents Dashboard