Free Questions for NSK101 by go4braindumps

Shared by Edwards on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements describe a website categorized as a domain generated algorithm (DGA)? (Choose two.)

Options:

A- The website is used for domain registration.

B- The domain contains malicious algorithms.

C- The website is used to hide a command-and-control server.

D- The domain was created by a program.

Answer:

C, D

Explanation:

Two statements that describe a website categorized as a domain generated algorithm (DGA) are: The website is used to hide a command-and-control server and the domain was created by a program. A domain generated algorithm (DGA) is a technique used by cyber attackers to generate new domain names and IP addresses for malware's command and control servers. Executed in a manner

that seems random, it makes it nearly impossible for threat hunters to detect and contain the attack. A command-and-control server is a server that communicates with malware installed on infected machines and sends commands or updates to them. A program is a piece of software that performs a specific task or function. A domain generated algorithm is implemented by a program that runs on the attacker's machine or the malware itself, and produces a large number of domain names based on some logic, such as date, time, seed, dictionary, etc.Reference:Domain generation algorithmAmong cyber-attack techniques, what is a DGA?

Question 2

Question Type: MultipleChoice

Which two statements are correct about DLP Incidents in the Netskope platform? (Choose two.)

Options:

A- An incident can be associated to one or more DLP policies.

B- An incident can have one or more DLP violations.

C- An incident can be assigned to one or more administrators.

D- An incident can be associated to one or more DLP rules.

Answer:

B, D

Explanation:

Two statements that are correct about DLP Incidents in the Netskope platform are: An incident can have one or more DLP violations and an incident can be associated to one or more DLP rules. A DLP violation occurs when a file or object matches a DLP rule used in a DLP profile. A DLP rule defines the criteria for detecting sensitive data, such as keywords, regular expressions, fingerprints, machine learning classifiers, etc. A DLP profile is a collection of DLP rules that can be applied to a policy. An incident is a record of a file or object that triggered a DLP policy violation. An incident can have multiple violations if the file or object matches multiple DLP rules from different profiles. An incident can also be associated to multiple DLP rules if the file or object matches more than one rule from the same profile.Reference:About DLPDLP Profiles

Question 3

Question Type: MultipleChoice

Which two controls are covered by Netskope's security platform? (Choose two.)

Options:

A- ZTNA

B- VPN

C- CASB

D- EDR

Answer:

A, C

Explanation:

Netskope'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.Reference:Netskope PlatformNetskope ZTNANetskope CASB

Question 4

Question Type: MultipleChoice

Which three technologies describe the primary cloud service models as defined by the National Institute of Standards and Technology (NIST)? (Choose three.)

Options:

A- Cloud Service Provider (CSP)

B- Identity as a Service (IDaaS)

C- Platform as a Service (PaaS)

D- Software as a Service (SaaS)

E- Infrastructure as a Service (IaaS)

Answer:

C, D, E

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'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).

Question 5

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

Question 6

Question Type: MultipleChoice

You are working with traffic from applications with pinned certificates. In this scenario, which statement is correct?

Options:

A- An exception should be added to the steering configuration.

B- The domains used by certificate-pinned applications should be added to the authentication bypass list.

C- Traffic with pinned certificates should be blocked.

D- The domains used by applications with pinned certificates should be allowed in an inline policy.

Answer:

A

Explanation:

When working with traffic from applications with pinned certificates, you should add an exception to the steering configuration to bypass them. Pinned certificates are a security technique that prevents man-in-the-middle attacks by validating the server certificates against a hardcoded list of certificates in the application. If you try to intercept or inspect the traffic from such applications, they will reject the connection or display an error message. Therefore, you should add the domains used by certificate-pinned applications as exceptions in your steering configuration, so that they are not steered to Netskope for analysis and enforcement.Reference:Certificate Pinned ApplicationsCreating a Steering Configuration

Question 7

Question Type: MultipleChoice

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.)

Options:

A- App Tag

B- CCL

C- App Score

D- GDPR Readiness

Answer:

A, C

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.Reference:Netskope Cloud Confidence IndexCreating Real-Time Policies for Cloud Applications

Question 8

Question Type: MultipleChoice

What are two CASB inline interception use cases? (Choose two.)

Options:

A- blocking file uploads to a personal Box account

B- running a retroactive scan for data at rest in Google Drive

C- using the Netskope steering client to provide user alerts when sensitive information is posted in Slack

D- scanning Dropbox for credit card information

Answer:

A, C

Explanation:

CASB inline interception use cases are scenarios where you need to apply real-time policies and actions on the traffic between users and cloud applications. For example, you may want to block file uploads to a personal Box account to prevent data leakage or exfiltration. You can use Netskope's inline proxy mode to intercept and inspect the traffic between users and Box, and apply granular policies based on user identity, device type, app instance, file metadata, etc. You can also use Netskope's inline proxy mode to provide user alerts when sensitive information is posted in Slack. For example, you may want to warn users when they share credit card numbers or social security numbers in Slack channels or messages. You can use Netskope's steering client to redirect the traffic between users and Slack to Netskope's inline proxy for inspection and enforcement. You can also use Netskope's DLP engine to detect sensitive data patterns and apply actions such as alerting or blocking.Reference:Netskope Inline Proxy ModeNetskope Steering Client[Netskope DLP Engine]

Question 9

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 10

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 11

Question Type: MultipleChoice

You are creating a real-time policy for cloud applications.

In addition to users, groups, and organizational units, which two source criteria would support this scenario? (Choose two.)

Options:

A- protocol version

B- access method

C- browser version

D- device classification

Answer:

B, D

Explanation:

When creating a real-time policy for cloud applications, you can use access method and device classification as source criteria, in addition to users, groups, and organizational units. Access method refers to how the user accesses the cloud application, such as browser, sync client, mobile app, etc. Device classification refers to the type of device used by the user, such as managed or unmanaged, Windows or Mac, etc. These criteria can help you define granular policies based on different scenarios and risks.Reference:[Creating Real-Time Policies for Cloud Applications]

Question 12

Question Type: MultipleChoice

What is the limitation of using a legacy proxy compared to Netskope's solution?

Options:

A- Netskope architecture requires on-premises components.

B- Legacy solutions offer higher performance and scalability for corporate and remote users.

C- Legacy on-premises solutions fail to provide protection for traffic from on-premises users.

D- To enforce policies, traffic needs to traverse back through a customer's on-premises security stack.

Answer:

D

Explanation:

A limitation of using a legacy proxy compared to Netskope's solution is that to enforce policies, traffic needs to traverse back through a customer's on-premises security stack. This creates latency, bandwidth, and scalability issues for remote users and cloud applications. Netskope's solution, on the other hand, leverages a cloud-native architecture that provides high-performance and scalable inspection of traffic from any location and device.Reference:[Netskope Architecture Overview]