IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **NSK101**

Title : Netskope Certified Cloud Security Administrator (NCCSA)

Version : DEMO

1.You investigate a suspected malware incident and confirm that it was a false alarm.
A. In this scenario, how would you prevent the same file from triggering another incident?
B. Quarantine the file. Look up the hash at the VirusTotal website.
C. Export the packet capture to a pcap file.
D. Add the hash to the file filter.
Answer: D
Explanation:
A file filter is a list of file hashes that you can use to exclude files from inspection by Netskope. By adding the hash of the file that triggered a false alarm to the file filter, you can prevent it from being scanned again by Netskope and avoid generating another incident. Quarantining the file, exporting the packet capture, or looking up the hash at VirusTotal are not effective ways to prevent the same file from triggering another incident, as they do not affect how Netskope handles the file.
Reference: Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Course, Module 6: Data Loss Prevention, Lesson 2: File Filters.

2.Which two common security frameworks are used today to assess and validate a vendor's security practices? (Choose two.)
A. Data Science Council of America
B. Building Security in Maturity Model
C. ISO 27001
D. NIST Cybersecurity Framework
Answer: B, C
Explanation:
The Building Security in Maturity Model (BSIMM) is a framework that measures and compares the security activities of different organizations. It helps organizations to assess their current security practices and identify areas for improvement. ISO 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining, and improving an information security management system. It helps organizations to manage their information security risks and demonstrate their compliance with best practices. Data Science Council of America (DASCA) is not a security framework, but a credentialing body for data science professionals. NIST Cybersecurity Framework (NIST CSF) is a security framework, but it is not commonly used to assess and validate a vendor’s security practices, as it is more focused on improving the cybersecurity of critical infrastructure sectors in the United States.
Reference: [BSIMM], [ISO 27001], [DASCA], [NIST CSF].

3.You have applied a DLP Profile to block all Personally Identifiable Information data uploads to Microsoft 365 OneDrive. DLP Alerts are not displayed and no OneDrive-related activities are displayed in the Skope IT App Events table.
In this scenario, what are two possible reasons for this issue? (Choose two.)
A. The Cloud Storage category is in the Steering Configuration as an exception.
B. The destination domain is excluded from decryption in the decryption policy.
C. A Netskope POP is not in your local country and therefore DLP policies cannot be applied.
D. DLP policies do not apply when using IPsec as a steering option.
Answer: AB

Explanation:
If the Cloud Storage category is in the Steering Configuration as an exception, then Netskope will not steer any traffic to or from cloud storage applications, such as Microsoft 365 OneDrive, to its platform. This means that Netskope will not be able to inspect or apply any policies to this traffic, including DLP policies. Similarly, if the destination domain is excluded from decryption in the decryption policy, then Netskope will not decrypt any traffic to or from that domain, such as onedrive.com. This means that Netskope will not be able to inspect or apply any policies to this traffic, including DLP policies. The location of the Netskope POP or the use of IPsec as a steering option do not affect the application of DLP policies, as long as Netskope can steer and decrypt the relevant traffic.
Reference: Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Course, Module 3: Steering Configuration, Lesson 1: Steering Options and Lesson 2: Exceptions; Module 4: Decryption Policy, Lesson 1: Decryption Policy Overview and Lesson 2: Decryption Policy Configuration.
: https://www.bsimm.com/: https://www.iso.org/isoiec-27001-information-security.html: https://www.dasca.org/: https://www.nist.gov/cyberframework

4.A customer changes CCI scoring from the default objective score to another score.
In this scenario, what would be a valid reason for making this change?
A. The customer has discovered a new SaaS application that is not yet rated in the CCI database.
B. The customer's organization places a higher business risk weight on vendors that claim ownership of their data.
C. The customer wants to punish an application vendor for providing poor customer service.
D. The customer's organization uses a SaaS application that is currently listed as "under research".
Answer: B
Explanation:
The CCI scoring is a way to measure the security posture of cloud applications based on a set of criteria and weights. The default objective score is calculated by Netskope using industry best practices and standards. However, customers can change the CCI scoring to suit their own business needs and risk appetite. For example, a customer may want to place a higher business risk weight on vendors that claim ownership of their data, as this may affect their data sovereignty and privacy rights. Changing the CCI scoring for this reason would be valid, as it reflects the customer’s own security requirements and preferences. Changing the CCI scoring for other reasons, such as discovering a new SaaS application, punishing an application vendor, or using an application under research, would not be valid, as they do not align with the purpose and methodology of the CCI scoring.
Reference: Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Course, Module 7: Cloud Confidence Index (CCI), Lesson 1: CCI Overview and Lesson 2: CCI Scoring.

5.What are two use cases for Netskope's DLP solution? (Choose two.)
A. to stop unintentional data movement
B. to detect malware in files before they are uploaded to a cloud application
C. to detect sensitive data in password protected files
D. to ensure regulatory compliance
Answer: A, D
Explanation:
Netskope’s DLP solution is a powerful tool that can help customers protect their sensitive data from

unauthorized access, exposure, or loss. One use case for Netskope’s DLP solution is to stop unintentional data movement, such as accidental uploads, downloads, or sharing of confidential files or information to or from cloud applications. Another use case for Netskope’s DLP solution is to ensure regulatory compliance, such as GDPR, HIPAA, PCI-DSS, or other industry-specific standards that require data protection and privacy measures. Netskope’s DLP solution can help customers comply with these regulations by detecting and preventing data breaches, enforcing encryption policies, applying data retention rules, and generating audit reports. Detecting malware in files before they are uploaded to a cloud application or detecting sensitive data in password protected files are not use cases for Netskope’s DLP solution, as they are more related to threat protection or file inspection capabilities. Reference: Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Course, Module 6: Data Loss Prevention, Lesson 1: DLP Overview.