Providing You Trustable 350-701 Pdf Files with 100% Passing Guarantee

350-701
Implementing and Operating Cisco Security
Certification Questions & Exams Dumps
www.edurely.com

DOWNLOAD the newest Dumpkiller 350-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1-HFo6ehD6puLmGFSi8gskjhSXb_mMrK3

In order to meet the different demands of the different customers, these experts from our company have designed three different versions of the 350-701 study materials. All customers have the right to choose the most suitable version according to their need after buying our study materials. The PDF version of the 350-701 Study Materials has many special functions, including download the demo for free, support the printable format and so on.

Upon passing the Cisco 350-701 Certification Exam, candidates earn the Cisco Certified Specialist - Security Core certification. Implementing and Operating Cisco Security Core Technologies certification demonstrates to employers that the candidate has a solid understanding of network security concepts and skills in implementing and operating Cisco Security Core Technologies.

Cisco 350-701 Certification Exam covers a broad range of topics, including network security, cloud security, content security, endpoint protection and detection, secure network access, visibility and enforcement, and security automation. These topics are essential for security professionals to ensure the security of their networks and devices and mitigate the risk of cyber-attacks.

>> 350-701 Pdf Files <<

Easy Access to Cisco 350-701 Exam Questions in PDF Format

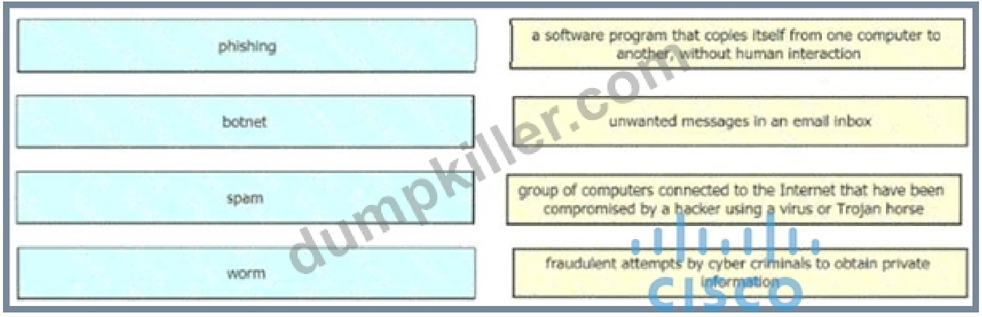
There is no denying that no exam is easy because it means a lot of consumption of time and effort. Especially for the upcoming 350-701 exam, although a large number of people to take the exam every year, only a part of them can pass. If you are also worried about the exam at this moment, please take a look at our 350-701 Study Materials, whose content is carefully designed for the 350-701 exam, rich question bank and answer to enable you to master all the test knowledge in a short period of time.

Cisco 350-701 Certification Exam is an ideal choice for IT professionals who want to advance their careers in the field of network security. Implementing and Operating Cisco Security Core Technologies certification is particularly valuable for those who work in security operations centers, network administration, or security consulting. By earning this certification, candidates can demonstrate their ability to design, implement, and manage secure networks and protect them against cyber threats.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q439-Q444):

NEW QUESTION # 439

Drag and drop the common security threats from the left onto the definitions on the right.



phishing

botnet

spam

worm

a software program that copies itself from one computer to another, without human interaction

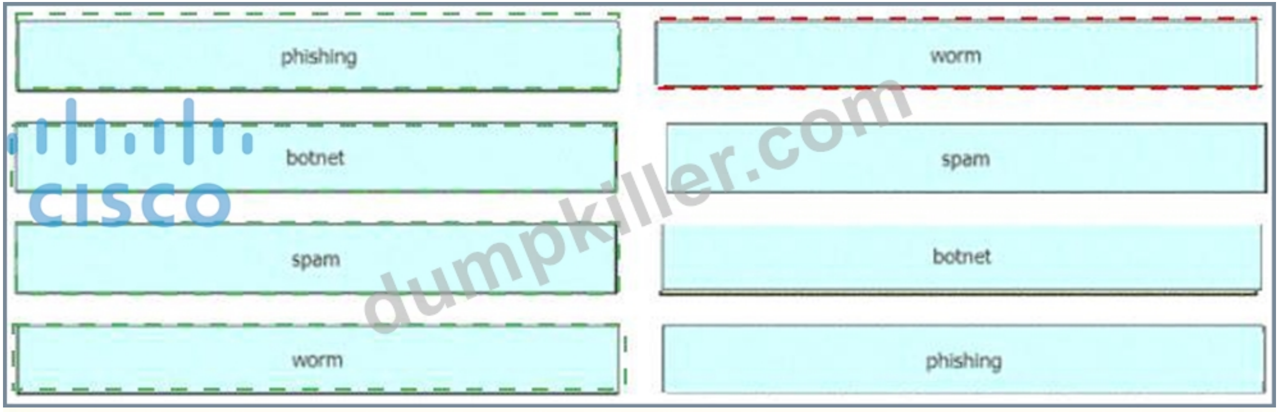
unwanted messages in an email inbox

group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse

fraudulent attempts by cyber criminals to obtain private information

Answer:

Explanation:



phishing

botnet

spam

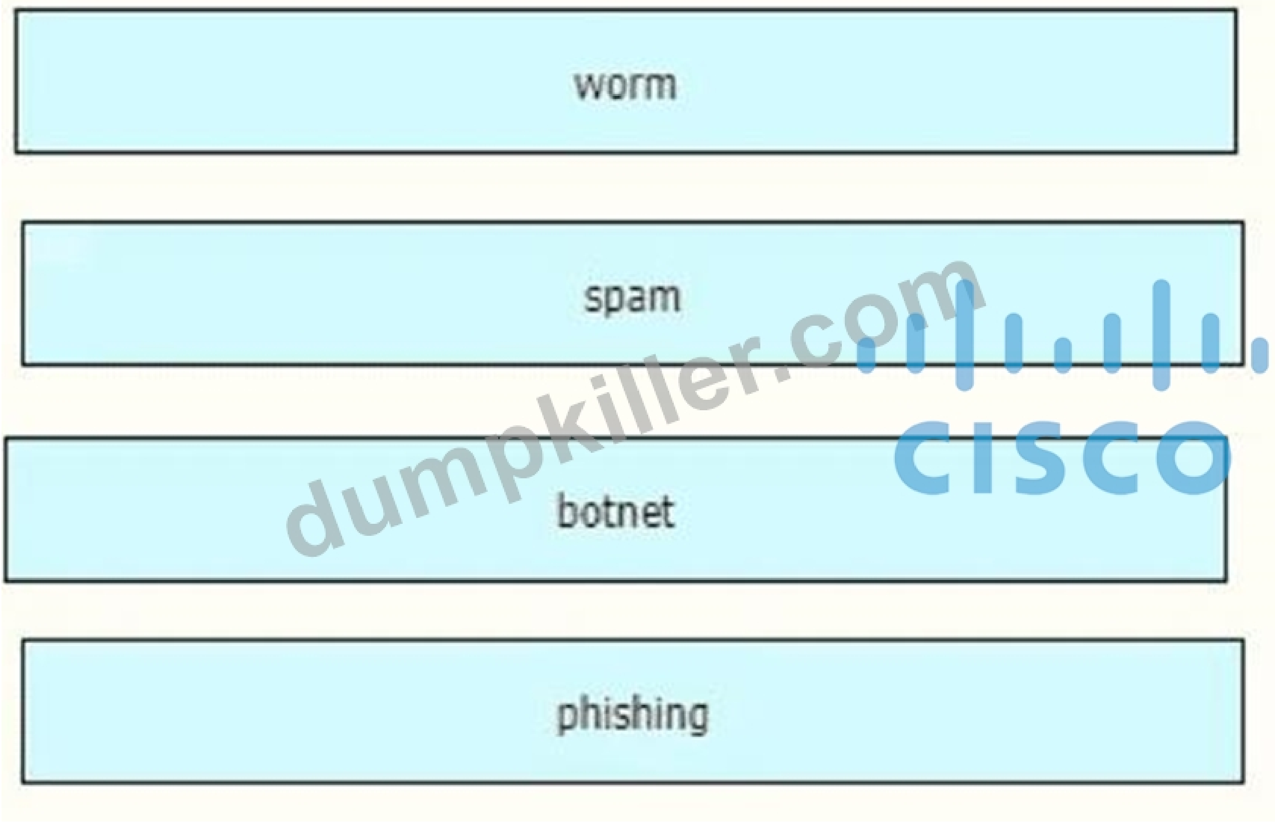
worm

worm

spam

botnet

phishing



worm

spam

botnet

phishing

NEW QUESTION # 440

A network engineer has configured a NTP server on a Cisco ASA. The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

- A. An access list entry for UDP port 123 on the inside interface is missing.
- B. An access list entry for UDP port 123 on the outside interface is missing.
- C. NTP is not configured to use a working server.
- D. Resynchronization of NTP is not forced

Answer: C

Explanation:
NTP uses UDP port 123 to communicate with its servers and peers. If the Cisco ASA has IP reachability to the NTP server and is not filtering any traffic, then the most likely cause of the unsynchronized state and the stratum of 16 is that the NTP server is not working properly or is not configured to provide NTP service. A stratum of 16 means that the NTP server is unreachable or is not considered a viable candidate1. The value.
INIT. in the refid column indicates that NTP is initializing, and the server has not yet been reached1. To resolve this issue, the network engineer should verify the status and configuration of the NTP server, and use a different server if needed. Alternatively, the network engineer can use the ntp server command with the prefer keyword to specify a preferred NTP server, or use the ntp update-calendar command to force a resynchronization of NTP2. References:
* 1: NTP server is unsynchronized or unreachable, a Wireshark perspective.
* 2: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Network Security, Lesson 1.3: Configuring Network Time Protocol.

NEW QUESTION # 441
An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

- A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
- B. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
- C. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
- D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.

Answer: A

Explanation:
The correct answer is to enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI.
Two-factor authentication is a security feature that requires users to provide two forms of identification before accessing the SEG, such as a username and password, and a one-time code or token. This adds an extra layer of protection against unauthorized access and phishing attacks. The SEG supports two-factor authentication through external RADIUS servers, which can be configured on the System Administration > Users page in the web interface, or the userconfig command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Two-Factor Authentication) for more details.
To join a cluster, the SEG must communicate with other cluster members using either SSH or CCS (Cluster Communication Service). The cluster communication port and method can be configured on the Network > Cluster Communication page in the web interface, or the clusterconfig command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Cluster Communication) for more details.
If two-factor authentication is enabled on the SEG, it cannot join a cluster using the web interface, because the web interface does not support two-factor authentication for cluster operations. Therefore, the SEG must join the cluster using the CLI, and provide a pre-shared key that matches the cluster's admin passphrase. The pre-shared key can be configured using the clusterconfig > prepjoin command in the CLI. See User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) (Section: Creating and Joining a Cluster) for more details.
The other options are incorrect because they either use the wrong authentication server (TACACS+ instead of RADIUS), or the wrong communication method (GUI instead of CLI). References:
* User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment)
* Configure an Email Security Appliance (ESA) Cluster - Cisco
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_

NEW QUESTION # 442

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

- A. inter-EPG isolation
- B. intra-EPG isolation
- C. placement in separate EPGs
- D. inter-VLAN security

Answer: B

Explanation:

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another.

NEW QUESTION # 443

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

- A. intelligent proxy
- B. snort
- C. URL categorization
- D. command and control communication
- E. data exfiltration

Answer: D,E

Explanation:

Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before. Detection and analytics features provided in Cognitive Threat Analytics are shown below: + Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content + Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats ... Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-736555.pdf Detection and analytics features provided in Cognitive Threat Analytics are shown below:

+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content

+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats

...

Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before. Detection and analytics features provided in Cognitive Threat Analytics are shown below: + Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content + Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores.

Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats ... Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-736555.pdf

NEW QUESTION # 444

......

Dumps 350-701 Vce: https://www.dumpkiller.com/350-701_braindumps.html

- 350-701 Reliable Exam Cram □ Study 350-701 Reference □ 350-701 Test Topics Pdf □ Enter □ www.vce4dumps.com □ and search for 【 350-701 】 to download for free □350-701 Latest Practice Materials
- Latest 350-701 Exam Vce □ Exam Topics 350-701 Pdf □ Pass 350-701 Guarantee ❤ Search for 「 350-701 」 and easily obtain a free download on □ www.pdfvce.com □ □New 350-701 Test Vce
- Latest Implementing and Operating Cisco Security Core Technologies exam pdf, 350-701 practice exam □ Search for ➥ 350-701 □ on 「 www.testkingpass.com 」 immediately to obtain a free download ✈350-701 Latest Learning Materials
- Latest Implementing and Operating Cisco Security Core Technologies exam pdf, 350-701 practice exam □ Open □ www.pdfvce.com □ enter "350-701" and obtain a free download □Questions 350-701 Exam
- 350-701 Reliable Exam Cram □ 350-701 Valid Exam Vce □ 350-701 Latest Learning Materials □ Open ➠ www.pass4test.com □ and search for ✔ 350-701 □✔□ to download exam materials for free □Exam Topics 350-701 Pdf
- TOP 350-701 Pdf Files - Cisco Implementing and Operating Cisco Security Core Technologies - High-quality Dumps 350-701 Vce □ Simply search for ➠ 350-701 □ for free download on { www.pdfvce.com } □Latest 350-701 Exam Vce
- Get Latest 350-701 Pdf Files and High Hit Rate Dumps 350-701 Vce □ Easily obtain ➥ 350-701 □ for free download through 【 www.exam4labs.com 】 □Reliable 350-701 Exam Guide
- Get Latest 350-701 Pdf Files and High Hit Rate Dumps 350-701 Vce □ The page for free download of ➤ 350-701 □ on □ www.pdfvce.com □ will open immediately □New 350-701 Test Vce
- Pass Guaranteed Quiz 2026 Cisco Fantastic 350-701: Implementing and Operating Cisco Security Core Technologies Pdf Files □ Enter ⇛ www.prepawayete.com ⇚ and search for 「 350-701 」 to download for free □Reliable 350-701 Exam Guide
- Pass 350-701 Guarantee □ 350-701 Test Topics Pdf □ 350-701 Test Topics Pdf □ Search for 【 350-701 】 and download exam materials for free through ➥ www.pdfvce.com □ ♥350-701 Latest Learning Materials
- Get Valid 350-701 Pdf Files and Excellent Dumps 350-701 Vce □ Download 《 350-701 》 for free by simply searching on ➽ www.pdfdumps.com □ ☀350-701 Valid Exam Vce
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, ezzatedros.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, infofitsoftware.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

DOWNLOAD the newest Dumpkiller 350-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1-HFo6ehD6puLmGFSi8gskjhSXb_mMrK3