

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

<https://www.2passeasy.com/dumps/350-701/>



NEW QUESTION 1

Which two preventive measures are used to control cross-site scripting? (Choose two.)

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. SameSite cookie attribute should not be used.

Answer: AB

NEW QUESTION 2

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

Answer: D

NEW QUESTION 3

Which two capabilities does TAXII support? (Choose two.)

- A. exchange
- B. pull messaging
- C. binding
- D. correlation
- E. mitigating

Answer: BC

NEW QUESTION 4

An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10. What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

- A. Cisco Identity Services Engine and AnyConnect Posture module
- B. Cisco Stealthwatch and Cisco Identity Services Engine integration
- C. Cisco ASA firewall with Dynamic Access Policies configured
- D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/administration/guide/b_AnyConnect_Administrator_Guide_4-6/configure-posture.html

NEW QUESTION 5

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

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

Answer: AB

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf>

NEW QUESTION 6

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two.)

- A. TACACS+
- B. central web auth
- C. single sign-on
- D. multiple factor auth
- E. local web auth

Answer: BE

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01110.html

NEW QUESTION 7

Which deployment model is the most secure when considering risks to cloud adoption?

- A. public cloud
- B. hybrid cloud
- C. community cloud
- D. private cloud

Answer: D

NEW QUESTION 8

Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

- A. DNS tunneling
- B. DNSCrypt
- C. DNS security
- D. DNSSEC

Answer: A

Explanation:

Reference: <https://learn-umbrella.cisco.com/cloud-security/dns-tunneling>

NEW QUESTION 9

Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

- A. SNMP
- B. SMTP
- C. syslog
- D. model-driven telemetry

Answer: D

Explanation:

Reference: <https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide>

NEW QUESTION 10

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

- A. Nexus
- B. Stealthwatch
- C. Firepower
- D. Tetration

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products>

NEW QUESTION 10

DRAG DROP

Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis,
and remediation to protect against
targeted persistent malware attacks

superior threat prevention and mitigation
for known and unknown threats

application-layer control and ability to
enforce usage and tailor detection policies
based on custom applications and URLs

combined integrated solution of strong
defense and web protection, visibility, and
controlling solutions

Next Generation
Intrusion Prevention System

Advanced Malware
Protection

application
control and URL filtering

Cisco
Web Security Appliance

A. Mastered

B. Not Mastered

Answer: A

Explanation:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

superior threat prevention and mitigation for known and unknown threats

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

NEW QUESTION 11

In which cloud services model is the tenant responsible for virtual machine OS patching?

- A. IaaS
- B. UCaaS
- C. PaaS
- D. SaaS

Answer: A

Explanation:

Reference: <https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php>

NEW QUESTION 15

Which two descriptions of AES encryption are true? (Choose two.)

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

Answer: BD

Explanation:

Reference: https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

NEW QUESTION 20

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. FireSIGHT
- D. ASA

Answer: A

NEW QUESTION 25

Which benefit does endpoint security provide the overall security posture of an organization?

- A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
- B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
- C. It allows the organization to detect and respond to threats at the edge of the network.
- D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer: D

NEW QUESTION 28

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

- A. STIX

- B. XMPP
- C. pxGrid
- D. SMTP

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.pdf

NEW QUESTION 29

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html>

NEW QUESTION 32

Which two mechanisms are used to control phishing attacks? (Choose two.)

- A. Enable browser alerts for fraudulent websites.
- B. Define security group memberships.
- C. Revoke expired CRL of the websites.
- D. Use antispyware software.
- E. Implement email filtering techniques.

Answer: AE

NEW QUESTION 36

Which VPN technology can support a multivendor environment and secure traffic between sites?

- A. SSL VPN
- B. GET VPN
- C. FlexVPN
- D. DMVPN

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

NEW QUESTION 39

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

NEW QUESTION 43

Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

- A. IP Blacklist Center
- B. File Reputation Center
- C. AMP Reputation Center
- D. IP and Domain Reputation Center

Answer: D

NEW QUESTION 46

Under which two circumstances is a CoA issued? (Choose two.)

- A. A new authentication rule was added to the policy on the Policy Service node.
- B. An endpoint is deleted on the Identity Service Engine server.
- C. A new Identity Source Sequence is created and referenced in the authentication policy.

- D. An endpoint is profiled for the first time.
- E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Answer: BD

Explanation:

Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

NEW QUESTION 50

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

- A. Patch for cross-site scripting.
- B. Perform backups to the private cloud.
- C. Protect against input validation and character escapes in the endpoint.
- D. Install a spam and virus email filter.
- E. Protect systems with an up-to-date antimalware program.

Answer: DE

NEW QUESTION 51

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

- A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
- B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
- C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
- D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
- E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: AC

NEW QUESTION 55

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP

Answer: AD

NEW QUESTION 58

How is Cisco Umbrella configured to log only security events?

- A. per policy
- B. in the Reporting settings
- C. in the Security Settings section
- D. per network in the Deployments section

Answer: A

Explanation:

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/log-management>

NEW QUESTION 59

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

- A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
- B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
- C. EPP focuses on network security, and EDR focuses on device security.
- D. EDR focuses on network security, and EPP focuses on device security.

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html>

NEW QUESTION 64

On which part of the IT environment does DevSecOps focus?

- A. application development
- B. wireless network
- C. data center
- D. perimeter network

Answer: A

NEW QUESTION 69

What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html>

NEW QUESTION 70

Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)

- A. put
- B. options
- C. get
- D. push
- E. connect

Answer: AC

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

NEW QUESTION 71

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

- A. hypervisor
- B. virtual machine
- C. network
- D. application

Answer: D

Explanation:

Reference: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>

NEW QUESTION 73

An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

- A. device flow correlation
- B. simple detections
- C. application blocking list
- D. advanced custom detections

Answer: C

NEW QUESTION 74

Which ASA deployment mode can provide separation of management on a shared appliance?

- A. DMZ multiple zone mode
- B. transparent firewall mode
- C. multiple context mode
- D. routed mode

Answer: C

NEW QUESTION 77

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

- A. Cisco Umbrella
- B. External Threat Feeds
- C. Cisco Threat Grid
- D. Cisco Stealthwatch

Answer: C

NEW QUESTION 79

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI
- C. Prime Infrastructure
- D. Telemetry

Answer: C

NEW QUESTION 84

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Answer: D

Explanation:

Reference: https://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION 85

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

- A. Port Bounce
- B. CoA Terminate
- C. CoA Reauth
- D. CoA Session Query

Answer: C

NEW QUESTION 86

Refer to the exhibit.

```
Sysauthcontrol          Enabled
Dot1x Protocol Version    3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 30
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
```

Which command was used to display this output?

- A. show dot1x all
- B. show dot1x
- C. show dot1x all summary
- D. show dot1x interface gi1/0/12

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xr-3se/3850/sec-user-8021x-xr-3se-3850-book/config-ieee-802x-pba.html

NEW QUESTION 87

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

- A. quality of service
- B. time synchronization
- C. network address translations
- D. intrusion policy

Answer: B

NEW QUESTION 89

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

- A. SDN controller and the cloud
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the management solution

Answer: D

NEW QUESTION 93

Which information is required when adding a device to Firepower Management Center?

- A. username and password
- B. encryption method
- C. device serial number
- D. registration key

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d

NEW QUESTION 96

Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

- A. DDoS
- B. antispam
- C. antivirus
- D. encryption
- E. DLP

Answer: DE

Explanation:

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

NEW QUESTION 99

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

- A. File Analysis
- B. SafeSearch
- C. SSL Decryption
- D. Destination Lists

Answer: C

NEW QUESTION 102

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-701 Product From:

<https://www.2passeasy.com/dumps/350-701/>

Money Back Guarantee

350-701 Practice Exam Features:

- * 350-701 Questions and Answers Updated Frequently
- * 350-701 Practice Questions Verified by Expert Senior Certified Staff
- * 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year