Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. correlation
B. intrusion
C. access control
D. network discovery

Answer: D

NEW QUESTION 3
Refer to the exhibit.

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations
B. show authentication method
C. show dot1x all
D. show authentication sessions

Answer: B

NEW QUESTION 4
Which two capabilities does TAXII support? (Choose two.)

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

Answer: BC

NEW QUESTION 5
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

NEW QUESTION 6
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Answer: B

Explanation:
Reference: https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories

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
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features

NEW QUESTION 9
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 10
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
What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000

NEW QUESTION 11
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

A. RADIUS
B. TACACS+
C. DHCP
D. sFlow
E. SMTP

Answer: AC

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

NEW QUESTION 15
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	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	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 18
How does Cisco Umbrella archive logs to an enterprise- owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

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

NEW QUESTION 21
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 24
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 29
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 34
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)

A. computer identity
B. Windows service
C. user identity
D. Windows firewall
E. default browser

Answer: BC

NEW QUESTION 38
DRAG DROP
Drag and drop the descriptions from the left onto the correct protocol versions on the right.
[MISSING]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
[MISSING]

NEW QUESTION 40
Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settings
D. destination lists

Answer: D

NEW QUESTION 43
Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.

C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

NEW QUESTION 44
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A. RSA SecureID
B. Internal Database
C. Active Directory
D. LDAP

Answer: C

NEW QUESTION 46
How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets
B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

NEW QUESTION 50
When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure

Answer: AC

Explanation:
Reference: https://www.lookingpoint.com/blog/ise-series-802.1x

NEW QUESTION 55
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 59
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 62
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center

Answer: B

NEW QUESTION 63
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 64
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

NEW QUESTION 69
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

NEW QUESTION 72
What is the primary role of the Cisco Email Security Appliance?

A. Mail Submission Agent
B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent

Answer: B

NEW QUESTION 74
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

NEW QUESTION 78
Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS
B. XaaS
C. IaaS
D. SaaS

Answer: A

NEW QUESTION 79
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 83
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 84
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 86
Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Answer: A

NEW QUESTION 91
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 93
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 98
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

NEW QUESTION 100
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 102
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 106
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 111
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: AB

Explanation:
Reference: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 112
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 116
Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*     0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C          1.1.1.0 255.255.255.0 is directly connect, outside
S          172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C          192.168.100.0 255.255.255.0 is directly connected, inside
C          172.16.10.0 255.255.255.0 is directly connected, dmz
S           10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz
_____

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

What is a result of the configuration?

A. Traffic from the DMZ network is redirected.
B. Traffic from the inside network is redirected.
C. All TCP traffic is redirected.
D. Traffic from the inside and DMZ networks is redirected.

Answer: D

NEW QUESTION 120
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 123
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html

NEW QUESTION 126
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The 350-701 Practice Test Here