Cisco.350-701.v2020-10-14.q49

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	49
Version:	v2020-10-14
# of views:	1242
# of Questions views:	28838
https://www.freecram.net/torrent/Cisco.350-701.v2020-10-14.q49.html	

NEW QUESTION: 1
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It alerts users when the WSA decrypts their traffic.
B. It decrypts HTTPS application traffic for unauthenticated users
C. It provides enhanced HTTPS application detection for AsyncOS.
D. It decrypts HTTPS application traffic for authenticated users.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?
A. forward
B. proxy gateway
C. redirection
D. transparent
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which functions of an SDN architecture require southbound APIs to enable communication?
A. SDN controller and the cloud
B. SDN controller and the network elements
C. management console and the cloud
D. management console and the SDN controller
Answer: (SHOW ANSWER)

NEW QUESTION: 4

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

NEW QUESTION: 5
On which part of the IT environment does DevSecOps focus?
A. perimeter network
B. wireless network
C. application development
D. data center
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which command enables 802.1X globally on a Cisco switch?
A. dot1x system-auth-control
B. aaa new-model
C. authentication port-control auto
D. dot1x pae authenticator
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. Destination Lists
B. SSL Decryption
C. SafeSearch
D. File Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 8

Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

A. NGIPS

B. Cisco Umbrella

C. Cisco Stealthwatch

D. Cisco Firepower

Answer: (SHOW ANSWER)

NEW QUESTION: 9

How many interfaces per bridge group does an ASA bridge group deployment support?

A. up to 2

B. up to 16

C. up to 8

D. up to 4

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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. CoA Reauth

B. CoA Session Query

C. Port Bounce

D. CoA Terminate

Answer: (SHOW ANSWER)

NEW QUESTION: 11

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

A. intelligent proxy

B. snort

C. URL categorization

D. data exfiltration

E. command and control communication

Answer: (SHOW ANSWER)

NEW QUESTION: 12

Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

A. Cisco FTDv with two management interfaces and one traffic interface configured

B. Cisco FTDv with one management interface and two traffic interfaces configured

C. Cisco FTDv configured in routed mode and IPv6 configured

D. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS

E. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises

Answer: (SHOW ANSWER)

NEW QUESTION: 13

How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

B. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.

C. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.

D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 14

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

A. ip flow-export destination 1.1.1.1 2055

B. flow-export destination inside 1.1.1.1 2055

C. ip flow monitor<name> input

D. flow exporter <name>

Answer: (SHOW ANSWER)

NEW QUESTION: 15

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

A. Cisco Firepower

B. Cisco Cloudlock

C. Cisco SDA

D. Cisco HyperFlex

Answer: (SHOW ANSWER)

NEW QUESTION: 16

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

A. LDAP

B. Active Directory

C. Internal Database

D. RSA SecureID

Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?
A. flow insight variation
B. software package variation
C. interpacket variation
D. process details variation
Answer: (SHOW ANSWER)

NEW QUESTION: 18
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?
A. It sends the application information to an administrator to act on
B. It discovers and controls cloud apps that are connected to a company's corporate environment
C. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously
D. It deletes any application that does not belong in the network
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?
A. Activate the Advanced Malware Protection license
B. Activate SSL decryption
C. Enable IP Layer enforcement
D. Enable Intelligent Proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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. simple detections

B. advanced custom detections
C. application blocking list
D. device flow correlation
Answer: (SHOW ANSWER)

NEW QUESTION: 21
An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group.
Which probe must be enabled for this type of profiling to work?
A. NetFlow
B. SNMP
C. DHCP
D. NMAP
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)
A. assurance
B. authentication
C. accounting
D. automation
E. encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 23
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1.
Which command achieves this goal?
A. snmp-server host inside 10.255.254.1 snmpv3 myv3
B. snmp-server host inside 10.255.254.1 version 3 andy
C. snmp-server host inside 10.255.254.1 version 3 myv3
D. snmp-server host inside 10.255.254.1 snmpv3 andy
Answer: (SHOW ANSWER)

NEW QUESTION: 24
How does Cisco Stealthwatch Cloud provide security for cloud environments?
A. It delivers visibility and threat detection.
B. It assigns Internet-based DNS protection for clients and servers.
C. It prevents exfiltration of sensitive datA.
D. It facilitates secure connectivity between public and private networks.

Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?
A. aaa new-model
B. aaa server radius dynamic-author
C. ip device-tracking
D. auth-type all
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?
A. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.
B. DHCP snooping has not been enabled on all VLANs.
C. The no ip arp inspection trust command is applied on all user host interfaces
D. Dynamic ARP Inspection has not been enabled on all VLANs
Answer: (SHOW ANSWER)

NEW QUESTION: 27
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)
A. default browser
B. Windows firewall
C. Windows service
D. user identity
E. computer identity
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Where are individual sites specified to be blacklisted in Cisco Umbrella?
A. content categories
B. destination lists
C. application settings
D. security settings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Which algorithm provides encryption and authentication for data plane communication?
A. SHA-96
B. SHA-384
C. AES-GCM
D. AES-256
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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 with PxGrid services enabled
B. Cisco Identity Services Engine and AnyConnect Posture module
C. Cisco ASA firewall with Dynamic Access Policies configured
D. Cisco Stealthwatch and Cisco Identity Services Engine integration
Answer: (SHOW ANSWER)

NEW QUESTION: 31
In which cloud services model is the tenant responsible for virtual machine OS patching?
A. SaaS
B. PaaS
C. IaaS
D. UCaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?
A. profile

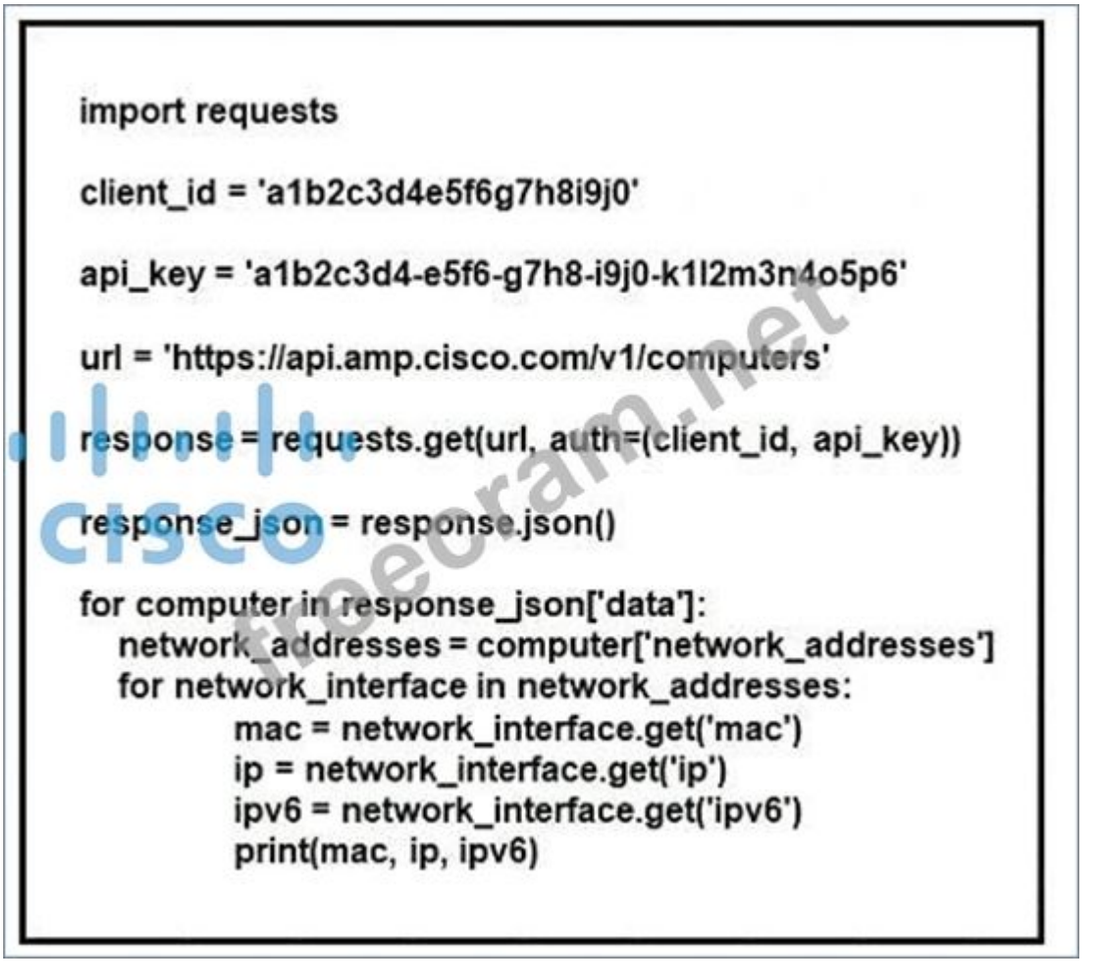
B. terminal
C. selfsigned
D. url
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)
A. phishing
B. man-in-the-middle
C. brute force
D. DDOS
E. tear drop
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 34
Which two activities can be done using Cisco DNA Center? (Choose two.)
A. accounting
B. DNS
C. design
D. DHCP
E. provision
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent?
(Choose two.)
A. Malware infects the messenger application on the user endpoint to send company data.
B. An exposed API for the messaging platform is used to send large amounts of data.
C. Outgoing traffic is allowed so users can communicate with outside organizations.
D. Messenger applications cannot be segmented with standard network controls.
E. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Refer to the exhibit.



```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

A. gather the network interface information about the computers AMP sees

B. get the process and PID information from the computers in the network

C. create an SNMP pull mechanism for managing AMP

D. gather network telemetry information from AMP for endpoints

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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

A. DDoS

B. buffer overflow

C. water holing

D. cross-site scripting

Answer: (SHOW ANSWER)

NEW QUESTION: 38

Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
       'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
       "     'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```


What is the result of this Python script of the Cisco DNA Center API?

A. receives information about a switch

B. adds a switch to Cisco DNA Center

C. adds authentication to a switch

Answer: (SHOW ANSWER)

NEW QUESTION: 39

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. Protect against input validation and character escapes in the endpoint.

C. Protect systems with an up-to-date antimalware program

D. Perform backups to the private cloud.

E. Install a spam and virus email filter

Answer: (SHOW ANSWER)

NEW QUESTION: 40

Why would a user choose an on-premises ESA versus the CES solution?

A. The server team wants to outsource this service.

B. Demand is unpredictable

C. ESA is deployed inline

D. Sensitive data must remain onsite

Answer: (SHOW ANSWER)

NEW QUESTION: 41

What is the function of the Context Directory Agent?

A. accepts user authentication requests on behalf of Web Security Appliance for user identification

B. relays user authentication requests from Web Security Appliance to Active Directory

C. maintains users' group memberships

D. reads the Active Directory logs to map IP addresses to usernames

Answer: D (LEAVE A REPLY)

NEW QUESTION: 42

What is the function of Cisco Cloudlock for data security?

A. controls malicious cloud apps

B. detects anomalies

C. data loss prevention

D. user and entity behavior analytics

Answer: (SHOW ANSWER)

NEW QUESTION: 43

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

A. XMPP

B. SMTP

C. STIX

D. pxGrid

Answer: (SHOW ANSWER)

NEW QUESTION: 44
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: (SHOW ANSWER)

NEW QUESTION: 45
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?
A. Talos
B. DynDNS
C. AMP
D. AnyConnect
Answer: (SHOW ANSWER)

NEW QUESTION: 46
What are two rootkit types? (Choose two)
A. buffer mode
B. bootloader
C. virtual
D. user mode
E. registry
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which deployment model is the most secure when considering risks to cloud adoption?
A. hybrid cloud

B. community cloud
C. private cloud
D. public cloud
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two.)
A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes. and push notifications
B. identification and correction of application vulnerabilities before allowing access to resources
C. secure access to on-premises and cloud applications
D. integration with 802.1x security using native Microsoft Windows supplicant
E. single sign-on access to on-premises and cloud applications
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which two services must remain as on-premises equipment when a hybrid email solution is deployed?
(Choose two.)
A. DDoS
B. encryption
C. antispam
D. antivirus
E. DLP
Answer: (SHOW ANSWER)