

350-701 Dumps

Implementing and Operating Cisco Security Core Technologies

<https://www.certleader.com/350-701-dumps.html>



NEW QUESTION 1

- (Exam Topic 2)

An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.

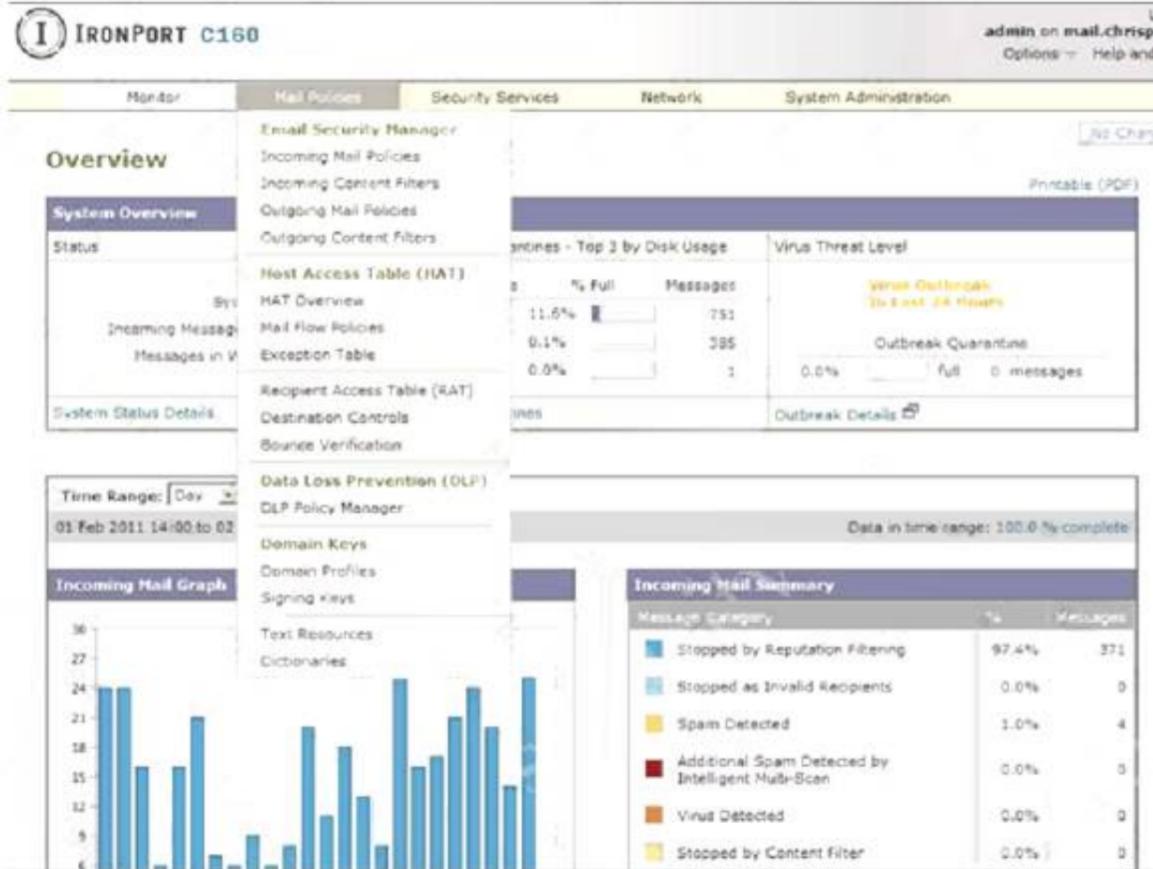
What must be configured to accomplish this?

- A. Configure the Cisco WSA to modify policies based on the traffic seen
- B. Configure the Cisco ESA to receive real-time updates from Talos
- C. Configure the Cisco WSA to receive real-time updates from Talos
- D. Configure the Cisco ESA to modify policies based on the traffic seen

Answer: D

Explanation:

The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



NEW QUESTION 2

- (Exam Topic 2)

What is a function of 3DES in reference to cryptography?

- A. It hashes files.
- B. It creates one-time use passwords.
- C. It encrypts traffic.
- D. It generates private keys.

Answer: C

NEW QUESTION 3

- (Exam Topic 2)

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

Answer: A

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION 4

- (Exam Topic 2)

An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

- A. deliver and send copies to other recipients

- B. quarantine and send a DLP violation notification
- C. quarantine and alter the subject header with a DLP violation
- D. deliver and add disclaimer text

Answer: D

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A

NEW QUESTION 5

- (Exam Topic 2)

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

- A. to prevent theft of the endpoints
- B. because defense-in-depth stops at the network
- C. to expose the endpoint to more threats
- D. because human error or insider threats will still exist

Answer: D

NEW QUESTION 6

- (Exam Topic 2)

What is managed by Cisco Security Manager?

- A. access point
- B. WSA
- C. ASA
- D. ESA

Answer: C

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/security-manager/index.html>

NEW QUESTION 7

- (Exam Topic 2)

What are two DDoS attack categories? (Choose two)

- A. sequential
- B. protocol
- C. database
- D. volume-based
- E. screen-based

Answer: BD

Explanation:

There are three basic categories of attack:+ volume-based attacks, which use high traffic to inundate the network bandwidth+ protocol attacks, which focus on exploiting server resources+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks

Reference: <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

NEW QUESTION 8

- (Exam Topic 2)

What is an attribute of the DevSecOps process?

- A. mandated security controls and check lists
- B. security scanning and theoretical vulnerabilities
- C. development security
- D. isolated security team

Answer: C

Explanation:

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives. Three key things make a real DevSecOps environment:+ Security testing is done by the development team.+ Issues found during that testing is managed by the development team.+ Fixing those issues stays within the development team.

NEW QUESTION 9

- (Exam Topic 2)

Refer to the exhibit.



An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

- A. configure manager add DONTRESOLVE kregistration key>
- B. configure manager add <FMC IP address> <registration key> 16
- C. configure manager add DONTRESOLVE <registration key> FTD123
- D. configure manager add <FMC IP address> <registration key>

Answer: D

Explanation:

Reference: <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/>

NEW QUESTION 10

- (Exam Topic 2)

What is a benefit of using Cisco FMC over Cisco ASDM?

- A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
- B. Cisco FMC provides centralized management while Cisco ASDM does not.
- C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
- D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

Answer: B

Explanation:

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.ht>

NEW QUESTION 10

- (Exam Topic 2)

An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

- A. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud
- B. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud
- C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
- D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

Answer: D

Explanation:

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 13

- (Exam Topic 1)

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/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html>

NEW QUESTION 17

- (Exam Topic 1)

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

NEW QUESTION 21

- (Exam Topic 1)

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

- A. Group Policy
- B. Access Control Policy
- C. Device Management Policy
- D. Platform Service Policy

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platfo> the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

NEW QUESTION 25

- (Exam Topic 1)

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 27

- (Exam Topic 1)

What is the primary benefit of deploying an ESA in hybrid mode?

- A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment
- B. It provides the lowest total cost of ownership by reducing the need for physical appliances
- C. It provides maximum protection and control of outbound messages
- D. It provides email security while supporting the transition to the cloud

Answer: D

Explanation:

Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email security infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud users at any time throughout the term of your contract, assuming the total number of users does not change. This allows for deployment flexibility as your organization's needs change.

NEW QUESTION 32

- (Exam Topic 1)

Refer to the exhibit.

```
snmp-server group SNMP v3 auth access  
15
```

What does the number 15 represent in this configuration?

- A. privilege level for an authorized user to this router
- B. access list that identifies the SNMP devices that can access the router
- C. interval in seconds between SNMPv3 authentication attempts
- D. number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

Explanation:

The syntax of this command is shown below: `snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]] [read read-view] [write write-view] [notify notify-view] [access access-list]` The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP

access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION 35

- (Exam Topic 1)

Refer to the exhibit.

```
aaa new-model
radius-server host 10.0.0.12 key
secret12
```

Which statement about the authentication protocol used in the configuration is true?

- A. The authentication request contains only a password
- B. The authentication request contains only a username
- C. The authentication and authorization requests are grouped in a single packet
- D. There are separate authentication and authorization request packets

Answer: C

Explanation:

This command uses RADIUS which combines authentication and authorization in one function (packet).

NEW QUESTION 37

- (Exam Topic 1)

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

NEW QUESTION 40

- (Exam Topic 1)

After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations. Which task can you perform to determine where each message was lost?

- A. Configure the trackingconfig command to enable message tracking.
- B. Generate a system report.
- C. Review the log files.
- D. Perform a trace.

Answer: A

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A

NEW QUESTION 43

- (Exam Topic 1)

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

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

Answer: C

NEW QUESTION 45

- (Exam Topic 1)

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 48

- (Exam Topic 1)

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. DHCP snooping has not been enabled on all VLANs.
- B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.
- C. Dynamic ARP Inspection has not been enabled on all VLANs
- D. The no ip arp inspection trust command is applied on all user host interfaces

Answer: D

Explanation:

Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

NEW QUESTION 50

- (Exam Topic 1)

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

- A. DMVPN
- B. FlexVPN
- C. IPsec DVTI
- D. GET VPN

Answer: D

Explanation:

Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_

NEW QUESTION 53

- (Exam Topic 1)

An MDM provides which two advantages to an organization with regards to device management? (Choose two)

- A. asset inventory management
- B. allowed application management
- C. Active Directory group policy management
- D. network device management
- E. critical device management

Answer: AB

NEW QUESTION 55

- (Exam Topic 1)

Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

- A. exploits
- B. ARP spoofing
- C. denial-of-service attacks
- D. malware
- E. eavesdropping

Answer: AD

Explanation:

Malware means "malicious software", is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden. An exploit is a code that takes advantage of a software vulnerability or security flaw. Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

NEW QUESTION 59

- (Exam Topic 1)

What is a feature of the open platform capabilities of Cisco DNA Center?

- A. intent-based APIs
- B. automation adapters
- C. domain integration
- D. application adapters

Answer: A

NEW QUESTION 61

- (Exam Topic 1)

Which two fields are defined in the NetFlow flow? (Choose two)

- A. type of service byte
- B. class of service bits
- C. Layer 4 protocol type
- D. destination port
- E. output logical interface

Answer: AD

Explanation:

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow: Ingress interface (SNMP ifIndex)+ Source IP address+ Destination IP address+ IP protocol+ Source port for UDP or TCP, 0 for other protocols+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols+ IP Type of Service Note: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION 65

- (Exam Topic 1)

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

- A. It allows the endpoint to authenticate with 802.1x or MAB.
- B. It verifies that the endpoint has the latest Microsoft security patches installed.
- C. It adds endpoints to identity groups dynamically.
- D. It allows CoA to be applied if the endpoint status is compliant.

Answer: A

NEW QUESTION 70

- (Exam Topic 1)

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. NMAP
- C. SNMP
- D. DHCP

Answer: B

Explanation:

Reference:

<http://www.network-node.com/blog/2016/1/2/ise-20-profiling>

NEW QUESTION 75

- (Exam Topic 1)

Which function is the primary function of Cisco AMP threat Grid?

- A. automated email encryption
- B. applying a real-time URI blacklist
- C. automated malware analysis
- D. monitoring network traffic

Answer: C

NEW QUESTION 77

- (Exam Topic 1)

Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

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: D

Explanation:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c> Displaying the Summary of All Auth Manager Sessions on the Switch

Enter the following:

Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success

0A3462B10000000D24F80B58

Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

NEW QUESTION 79

- (Exam Topic 1)

Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

- A. Time-based one-time passwords
- B. Data loss prevention
- C. Heuristic-based filtering
- D. Geolocation-based filtering
- E. NetFlow

Answer: BD

Explanation:

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 81

- (Exam Topic 1)

Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

- A. It allows traffic if it does not meet the profile.
- B. It defines a traffic baseline for traffic anomaly deduction.
- C. It inspects hosts that meet the profile with more intrusion rules.
- D. It blocks traffic if it does not meet the profile.

Answer: B

NEW QUESTION 83

- (Exam Topic 1)

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. url
- B. terminal
- C. profile
- D. selfsigned

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/vpn/public-key-infrastructure-pki/211333-IOSPKI-Deploy>

NEW QUESTION 84

- (Exam Topic 1)

Which SNMPv3 configuration must be used to support the strongest security possible?

- A. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- B. asa-host(config)#snmp-server group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- C. asa-host(config)#snmpserver group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- D. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D

NEW QUESTION 86

- (Exam Topic 1)

Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

- A. RADIUS Change of Authorization
- B. device tracking
- C. DHCP snooping
- D. VLAN hopping

Answer: A

NEW QUESTION 88

- (Exam Topic 1)

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:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 93

- (Exam Topic 1)

Which compliance status is shown when a configured posture policy requirement is not met?

- A. compliant
- B. unknown
- C. authorized
- D. noncompliant

Answer: D

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide

NEW QUESTION 95

- (Exam Topic 1)

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:

The profiling service issues the change of authorization in the following cases:– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network. An exception action is configured—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy. The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

NEW QUESTION 99

- (Exam Topic 1)

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. adds authentication to a switch
- B. adds a switch to Cisco DNA Center
- C. receives information about a switch
- D. deletes a switch from Cisco DNA Center

Answer: B

NEW QUESTION 100

- (Exam Topic 1)

Which two activities can be done using Cisco DNA Center? (Choose two)

- A. DHCP
- B. Design
- C. Accounting
- D. DNS
- E. Provision

Answer: BE

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html>

NEW QUESTION 101

- (Exam Topic 1)

Which command enables 802.1X globally on a Cisco switch?

- A. dot1x system-auth-control
- B. dot1x pae authenticator
- C. authentication port-control aut
- D. aaa new-model

Answer: A

NEW QUESTION 103

- (Exam Topic 1)

Which threat involves software being used to gain unauthorized access to a computer system?

- A. virus
- B. NTP amplification
- C. ping of death
- D. HTTP flood

Answer: A

NEW QUESTION 106

- (Exam Topic 1)

Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

- A. Port
- B. Rule
- C. Source
- D. Application
- E. Protocol

Answer: BC

NEW QUESTION 110

- (Exam Topic 1)

Which two behavioral patterns characterize a ping of death attack? (Choose two)

- A. The attack is fragmented into groups of 16 octets before transmission.
- B. The attack is fragmented into groups of 8 octets before transmission.
- C. Short synchronized bursts of traffic are used to disrupt TCP connections.
- D. Malformed packets are used to crash systems.
- E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: BD

Explanation:

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command. A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

NEW QUESTION 111

- (Exam Topic 1)

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

NEW QUESTION 115

- (Exam Topic 1)

Which API is used for Content Security?

- A. NX-OS API
- B. IOS XR API
- C. OpenVuln API
- D. AsyncOS API

Answer: D

NEW QUESTION 120

- (Exam Topic 1)

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html>

NEW QUESTION 121

- (Exam Topic 1)

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
- B. A spear phishing campaign is aimed at a specific person versus a group of people.
- C. Spear phishing is when the attack is aimed at the C-level executives of an organization.

D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information – and craft a fake email tailored for that person.

NEW QUESTION 125

- (Exam Topic 1)

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

Explanation:

Reference: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 127

- (Exam Topic 1)

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

- A. up to 2
- B. up to 4
- C. up to 8
- D. up to 16

Answer: B

Explanation:

Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router. As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces. Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION 131

- (Exam Topic 1)

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 134

- (Exam Topic 1)

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

NEW QUESTION 137

- (Exam Topic 3)

Which command is used to log all events to a destination collector 209.165.201.107?

- A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
- B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
- C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
- D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

Answer: C

NEW QUESTION 141

- (Exam Topic 3)

Which solution stops unauthorized access to the system if a user's password is compromised?

- A. VPN
- B. MFA
- C. AMP
- D. SSL

Answer: B

NEW QUESTION 144

- (Exam Topic 3)

What are two functionalities of SDN Northbound APIs? (Choose two.)

- A. Northbound APIs provide a programmable interface for applications to dynamically configure the network.
- B. Northbound APIs form the interface between the SDN controller and business applications.
- C. OpenFlow is a standardized northbound API protocol.
- D. Northbound APIs use the NETCONF protocol to communicate with applications.
- E. Northbound APIs form the interface between the SDN controller and the network switches or routers.

Answer: AB

NEW QUESTION 146

- (Exam Topic 3)

Which two Cisco ISE components must be configured for BYOD? (Choose two.)

- A. local WebAuth
- B. central WebAuth
- C. null WebAuth
- D. guest
- E. dual

Answer: BD

NEW QUESTION 148

- (Exam Topic 3)

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

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

Answer: B

NEW QUESTION 149

- (Exam Topic 3)

An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?

- A. It is included in the license cost for the multi-org console of Cisco Umbrella
- B. It can grant third-party SIEM integrations write access to the S3 bucket
- C. No other applications except Cisco Umbrella can write to the S3 bucket
- D. Data can be stored offline for 30 days.

Answer: D

NEW QUESTION 150

- (Exam Topic 3)

What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?

- A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
- B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
- C. Cisco AMP for Endpoints automatically researches indicators of compromise ..
- D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.

Answer: D

Explanation:

<https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3?> [https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Power Cisco Advanced Malware Protection \(AMP\) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform \(EPP\), and advanced endpoint detection and response \(EDR\). Providing Protection – Detection Response](https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Power Cisco Advanced Malware Protection (AMP) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform (EPP), and advanced endpoint detection and response (EDR). Providing Protection – Detection Response)

While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC). Any malicious domains requested and IPs resolved are indicators of compromise IO(C)

NEW QUESTION 153

- (Exam Topic 3)

Drag and drop the cloud security assessment components from the left onto the definitions on the right.

user entity behavior assessment	develop a cloud security strategy and roadmap aligned to business priorities
cloud data protection assessment	identify strengths and areas for improvement in the current security architecture during onboarding
cloud security strategy workshop	understand the security posture of the data or activity taking place in public cloud deployments
cloud security architecture assessment	detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service application

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

user entity behavior assessment	cloud security strategy workshop
cloud data protection assessment	cloud security architecture assessment
cloud security strategy workshop	cloud data protection assessment
cloud security architecture assessment	user entity behavior assessment

NEW QUESTION 156

- (Exam Topic 3)

Which solution should be leveraged for secure access of a CI/CD pipeline?

- A. Duo Network Gateway
- B. remote access client
- C. SSL WebVPN
- D. Cisco FTD network gateway

Answer: A

NEW QUESTION 160

- (Exam Topic 3)

Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

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

Answer: A

NEW QUESTION 164

- (Exam Topic 3)

A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

- A. RADIUS communication must be permitted between the ISE server and the domain controller.
- B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.

- C. Active Directory only supports user authentication by using MSCHAPv2.
- D. LDAP communication must be permitted between the ISE server and the domain controller.
- E. Active Directory supports user and machine authentication by using MSCHAPv2.

Answer: BC

NEW QUESTION 168

- (Exam Topic 3)

Refer to the exhibit.

```
crypto ikev2 name-mangler MANGLER
dn organization-unit
```

An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

- A. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
- B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
- C. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
- D. The OU of the IKEv2 peer certificate is set to MANGLER

Answer: A

NEW QUESTION 170

- (Exam Topic 3)

Which statement describes a serverless application?

- A. The application delivery controller in front of the server farm designates on which server the application runs each time.
- B. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
- C. The application is installed on network equipment and not on physical servers.
- D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

Answer: B

NEW QUESTION 173

- (Exam Topic 3)

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

Explanation:

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 175

- (Exam Topic 3)

Which baseline form of telemetry is recommended for network infrastructure devices?

- A. SDNS
- B. NetFlow
- C. passive taps
- D. SNMP

Answer: D

NEW QUESTION 177

- (Exam Topic 3)

What is a benefit of using Cisco Umbrella?

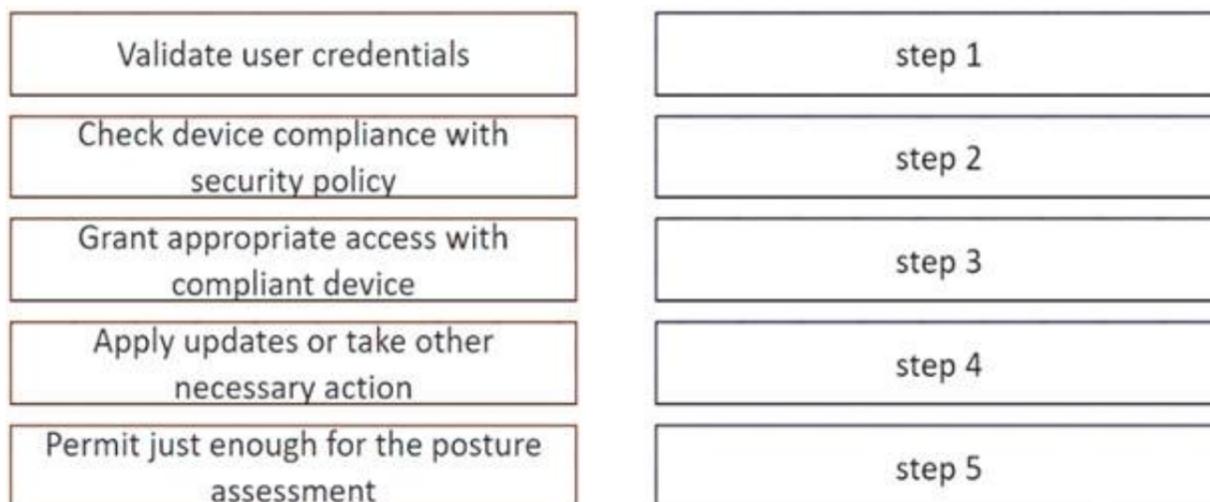
- A. DNS queries are resolved faster.
- B. Attacks can be mitigated before the application connection occurs.
- C. Files are scanned for viruses before they are allowed to run.
- D. It prevents malicious inbound traffic.

Answer: B

NEW QUESTION 179

- (Exam Topic 3)

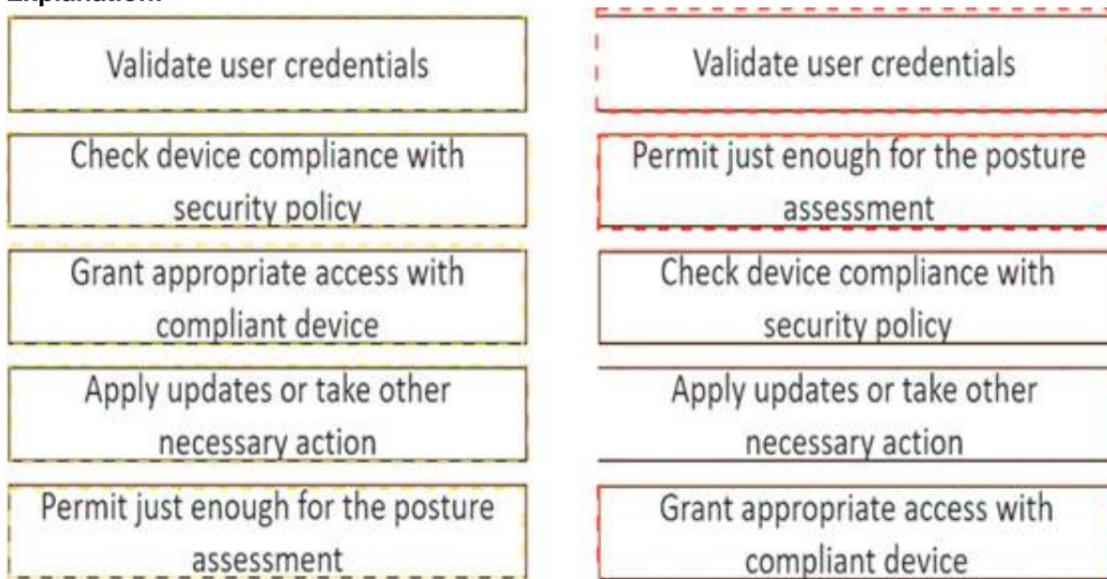
Drag and drop the posture assessment flow actions from the left into a sequence on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 180

- (Exam Topic 3)

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

- A. The hosts must run Cisco AsyncOS 10.0 or greater.
- B. The hosts must run different versions of Cisco AsyncOS.
- C. The hosts must have access to the same defined network.
- D. The hosts must use a different datastore than the virtual appliance.

Answer: C

NEW QUESTION 182

- (Exam Topic 3)

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

- A. Create an LDAP authentication realm and disable transparent user identification.
- B. Create NTLM or Kerberos authentication realm and enable transparent user identification.
- C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
- D. The eDirectory client must be installed on each client workstation.
- E. Deploy a separate eDirectory server; the default IP address is recorded in this server.

Answer: AC

NEW QUESTION 187

- (Exam Topic 3)

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal?

- A. single-SSID BYOD
- B. multichannel GUI
- C. dual-SSID BYOD
- D. streamlined access

Answer: C

NEW QUESTION 191

- (Exam Topic 3)

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

- A. third-party
- B. self-signed
- C. organization owned root
- D. SubCA

Answer: C**NEW QUESTION 192**

- (Exam Topic 3)

An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

- A. Configure Dynamic ARP inspection and add entries in the DHCP snooping database.
- B. Configure DHCP snooping and set trusted interfaces for all client connections.
- C. Configure Dynamic ARP inspection and antispoofing ACLs in the DHCP snooping database.
- D. Configure DHCP snooping and set a trusted interface for the DHCP server.

Answer: B**Explanation:**Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuratio**NEW QUESTION 193**

- (Exam Topic 3)

What is a benefit of using Cisco Tetration?

- A. It collects telemetry data from servers and then uses software sensors to analyze flow information.
- B. It collects policy compliance data and process details.
- C. It collects enforcement data from servers and collects interpacket variation.
- D. It collects near-real time data from servers and inventories the software packages that exist on servers.

Answer: C**NEW QUESTION 195**

- (Exam Topic 3)

Which Cisco security solution provides patch management in the cloud?

- A. Cisco Umbrella
- B. Cisco ISE
- C. Cisco CloudLock
- D. Cisco Tetration

Answer: C**NEW QUESTION 196**

- (Exam Topic 3)

```
aaa new-model
radius-server host 10.0.0.12 key secret12
```

Refer to the exhibit. What is the result of using this authentication protocol in the configuration?

- A. The authentication request contains only a username.
- B. The authentication request contains only a password.
- C. There are separate authentication and authorization request packets.
- D. The authentication and authorization requests are grouped in a single packet.

Answer: D**NEW QUESTION 197**

- (Exam Topic 3)

An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.

The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

- A. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not
- B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.
- C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not
- D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

Answer: C

NEW QUESTION 201

- (Exam Topic 3)

An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

- A. Blocked Application
- B. Simple Custom Detection
- C. Advanced Custom Detection
- D. Android Custom Detection

Answer: C

NEW QUESTION 205

- (Exam Topic 3)

Drag and drop the concepts from the left onto the correct descriptions on the right

guest services	requires probes to collect attributes of connected endpoints
profiling	sponsor portal that is used to gain access to network resources
posture assessment	My Devices portal that allows users to register their device
BYOD	Results can have a status of compliant or noncompliant.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

guest services	profiling
profiling	guest services
posture assessment	BYOD
BYOD	posture assessment

NEW QUESTION 206

- (Exam Topic 3)

What is the target in a phishing attack?

- A. perimeter firewall
- B. IPS
- C. web server
- D. endpoint

Answer: D

NEW QUESTION 208

- (Exam Topic 3)

What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

- A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
- B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
- C. The WSA hosts PAC files on port 9001 by default.

- D. The WSA hosts PAC files on port 6001 by default.
- E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Answer: AD

NEW QUESTION 211

- (Exam Topic 3)

Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

- A. Configure an advanced custom detection list.
- B. Configure an IP Block & Allow custom detection list
- C. Configure an application custom detection list
- D. Configure a simple custom detection list

Answer: A

NEW QUESTION 214

- (Exam Topic 3)

What is a feature of container orchestration?

- A. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane
- B. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane
- C. ability to deploy Kubernetes clusters in air-gapped sites
- D. automated daily updates

Answer: C

NEW QUESTION 216

- (Exam Topic 3)

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

- A. api/v1/fie/config
- B. api/v1/onboarding/pnp-device/import
- C. api/v1/onboarding/pnp-device
- D. api/v1/onboarding/workflow

Answer: B

NEW QUESTION 217

- (Exam Topic 3)

An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined. Which action meets this configuration requirement?

- A. Identify the network IPs and place them in a blocked list.
- B. Modify the advanced custom detection list to include these files.
- C. Create an application control blocked applications list.
- D. Add a list for simple custom detection.

Answer: C

NEW QUESTION 218

- (Exam Topic 3)

What is a difference between a DoS attack and a DDoS attack?

- A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
- B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
- C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
- D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

Answer: A

NEW QUESTION 219

- (Exam Topic 3)

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

- A. RADIUS-based REAP
- B. fingerprinting
- C. Dynamic ARP Inspection
- D. multifactor authentication

Answer: D

NEW QUESTION 223

- (Exam Topic 3)

In which scenario is endpoint-based security the solution?

- A. inspecting encrypted traffic
- B. device profiling and authorization
- C. performing signature-based application control
- D. inspecting a password-protected archive

Answer: C

NEW QUESTION 226

- (Exam Topic 3)

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

- A. Cisco Umbrella
- B. Cisco ISE
- C. Cisco DNA Center
- D. Cisco TrustSec
- E. Cisco Duo Security

Answer: AE

NEW QUESTION 231

- (Exam Topic 3)

Which solution is made from a collection of secure development practices and guidelines that developers must follow to build secure applications?

- A. AFL
- B. Fuzzing Framework
- C. Radamsa
- D. OWASP

Answer: D

NEW QUESTION 234

- (Exam Topic 3)

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

- A. OpenC2
- B. OpenIOC
- C. CybOX
- D. STIX

Answer: D

NEW QUESTION 237

- (Exam Topic 3)

What are two workloaded security models? (Choose two)

- A. SaaS
- B. IaaS
- C. on-premises
- D. off-premises
- E. PaaS

Answer: CD

NEW QUESTION 239

- (Exam Topic 3)

Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

- A. AAA attributes
- B. CoA request
- C. AV pair
- D. carrier-grade NAT

Answer: C

NEW QUESTION 244

- (Exam Topic 3)

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

- A. Cisco FMC
- B. CSM
- C. Cisco FDM

D. CDO

Answer: B

NEW QUESTION 248

- (Exam Topic 3)

What are two functions of TAXII in threat intelligence sharing? (Choose two.)

- A. determines the "what" of threat intelligence
- B. Supports STIX information
- C. allows users to describe threat motivations and abilities
- D. exchanges trusted anomaly intelligence information
- E. determines how threat intelligence information is relayed

Answer: BE

NEW QUESTION 249

- (Exam Topic 3)

What is the most commonly used protocol for network telemetry?

- A. SMTP
- B. SNMP
- C. TFTP
- D. NctFlow

Answer: D

NEW QUESTION 253

- (Exam Topic 3)

Which security solution protects users leveraging DNS-layer security?

- A. Cisco ISE
- B. Cisco FTD
- C. Cisco Umbrella
- D. Cisco ASA

Answer: C

NEW QUESTION 256

- (Exam Topic 3)

Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

- A. Audit
- B. Mandatory
- C. Optional
- D. Visibility

Answer: B

Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_Mandatory_Requirements_During_policy_evaluation,](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_Mandatory_Requirements_During_policy_evaluation.html) the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

NEW QUESTION 258

- (Exam Topic 3)

A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to ensure that bandwidth is available for VPN users needing access to corporate resources on the 10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the network?

- A. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.
- B. Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,
- C. Configure VPN load balancing to send non-corporate traffic straight to the internet.
- D. Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

Answer: A

NEW QUESTION 261

- (Exam Topic 3)

A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow for additional protocols to terminate network devices with. They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?

- A. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy
- B. Make the priority for the new policy 5 and the primary policy 1
- C. Change the encryption to AES* to support all AES algorithms in the primary policy

D. Make the priority for the primary policy 10 and the new policy 1

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html>

NEW QUESTION 262

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC feature?

- A. It is an incident response tool.
- B. It provides stealth threat prevention.
- C. It is a signature-based engine.
- D. It provides precompromise detection.

Answer: A

Explanation:

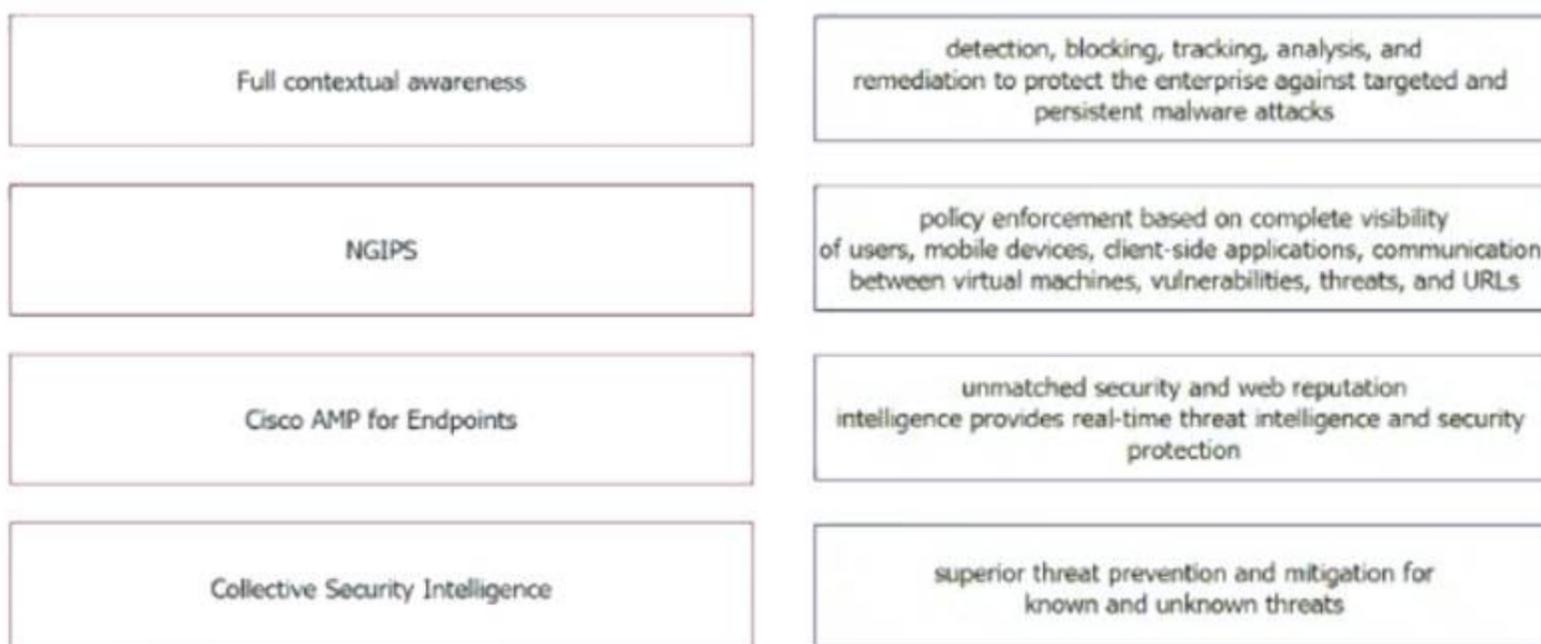
Reference: <https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf>

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION 267

- (Exam Topic 3)

Drag and drop the security solutions from the left onto the benefits they provide on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Diagram Description automatically generated

NEW QUESTION 271

- (Exam Topic 3)

Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

- A. inbound
- B. north-south
- C. east-west
- D. outbound

Answer: D

NEW QUESTION 274

- (Exam Topic 3)

Why should organizations migrate to a multifactor authentication strategy?

- A. Multifactor authentication methods of authentication are never compromised
- B. Biometrics authentication leads to the need for multifactor authentication due to its ability to be hacked easily
- C. Multifactor authentication does not require any piece of evidence for an authentication mechanism
- D. Single methods of authentication can be compromised more easily than multifactor authentication

Answer: D

NEW QUESTION 278

- (Exam Topic 3)

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

- A. SDLC
- B. Docker
- C. Lambda
- D. Contiv

Answer: B

NEW QUESTION 283

- (Exam Topic 3)

A company identified a phishing vulnerability during a pentest. What are two ways the company can protect employees from the attack? (Choose two.)

- A. using Cisco Umbrella
- B. using Cisco ESA
- C. using Cisco FTD
- D. using an inline IPS/IDS in the network
- E. using Cisco ISE

Answer: AB

NEW QUESTION 286

- (Exam Topic 3)

What are two functions of IKEv1 but not IKEv2? (Choose two)

- A. NAT-T is supported in IKEv1 but not in IKEv2.
- B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
- C. With IKEv1, mode negotiates faster than main mode
- D. IKEv1 uses EAP authentication
- E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Answer: CE

NEW QUESTION 288

- (Exam Topic 3)

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

- A. Cisco Umbrella
- B. Cisco AMP for Endpoints
- C. Cisco ISE
- D. Cisco Stealthwatch

Answer: C

NEW QUESTION 289

- (Exam Topic 3)

Which VPN provides scalability for organizations with many remote sites?

- A. DMVPN
- B. site-to-site IPsec
- C. SSL VPN
- D. GRE over IPsec

Answer: A

NEW QUESTION 290

- (Exam Topic 3)

What are two workload security models? (Choose two.)

- A. SaaS
- B. PaaS
- C. off-premises
- D. on-premises
- E. IaaS

Answer: CD

NEW QUESTION 293

- (Exam Topic 3)

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

- A. The latest antivirus updates are applied before access is allowed.
- B. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
- C. Patch management remediation is performed.
- D. A centralized management solution is deployed.

E. Endpoint supplicant configuration is deployed.

Answer: AD

NEW QUESTION 298

- (Exam Topic 3)

A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment. They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

- A. DMVPN because it supports IKEv2 and FlexVPN does not
- B. FlexVPN because it supports IKEv2 and DMVPN does not
- C. FlexVPN because it uses multiple SAs and DMVPN does not
- D. DMVPN because it uses multiple SAs and FlexVPN does not

Answer: C

Explanation:

FlexVPN supports IKEv2 -> Answer A is not correct. DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct. FlexVPN support multiple SAs -> Answer D is not correct.

NEW QUESTION 299

- (Exam Topic 3)

How does Cisco AMP for Endpoints provide next-generation protection?

- A. It encrypts data on user endpoints to protect against ransomware.
- B. It leverages an endpoint protection platform and endpoint detection and response.
- C. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.
- D. It integrates with Cisco FTD devices.

Answer: B

NEW QUESTION 304

- (Exam Topic 3)

Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?

- A. pxGrid
- B. NetFlow
- C. SNMP
- D. Cisco Talos

Answer: A

NEW QUESTION 305

- (Exam Topic 3)

Which two parameters are used for device compliance checks? (Choose two.)

- A. endpoint protection software version
- B. Windows registry values
- C. DHCP snooping checks
- D. DNS integrity checks
- E. device operating system version

Answer: CE

NEW QUESTION 308

- (Exam Topic 3)

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

- A. server farm
- B. perimeter
- C. core
- D. East-West gateways

Answer: B

NEW QUESTION 313

- (Exam Topic 3)

What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

- A. mobile device management
- B. mobile content management
- C. mobile application management
- D. mobile access management

- A. Spectre Worm
- B. Eternal Blue Windows
- C. Heartbleed SSL Bug
- D. W32/AutoRun worm

Answer: D

NEW QUESTION 325

- (Exam Topic 3)

Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

- A. cluster
- B. transparent
- C. routed
- D. multiple context

Answer: B

NEW QUESTION 326

- (Exam Topic 3)

What is a description of microsegmentation?

- A. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate
- B. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery
- C. Environments implement private VLAN segmentation to group servers with similar applications.
- D. Environments deploy centrally managed host-based firewall rules on each server or container

Answer: A

NEW QUESTION 329

- (Exam Topic 2)

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

phishing	a software program that copies itself from one computer to another, without human interaction
botnet	unwanted messages in an email inbox
spam	group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse
worm	fraudulent attempts by cyber criminals to obtain private information

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing application Description automatically generated

NEW QUESTION 334

- (Exam Topic 2)

What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

- A. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces
- B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot
- C. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added
- D. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot

Answer: A

NEW QUESTION 339

- (Exam Topic 2)

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

- A. 1
- B. 3

- C. 5
- D. 10

Answer: D

Explanation:

We choose "Chat and Instant Messaging" category in "URL Category":

To block certain URLs we need to choose URL Reputation from 6 to 10.

NEW QUESTION 341

- (Exam Topic 2)

Which attack type attempts to shut down a machine or network so that users are not able to access it?

- A. smurf
- B. bluesnarfing
- C. MAC spoofing
- D. IP spoofing

Answer: A

Explanation:

Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to itsintended users.The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP)packets with the intended victim's spoofed source IP are broadcast to a computer network using an IPbroadcast address.

NEW QUESTION 344

- (Exam Topic 2)

Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

- A. westbound AP

- B. southbound API
- C. northbound API
- D. eastbound API

Answer: C

NEW QUESTION 347

- (Exam Topic 2)

What is a capability of Cisco ASA Netflow?

- A. It filters NSEL events based on traffic
- B. It generates NSEL events even if the MPF is not configured
- C. It logs all event types only to the same collector
- D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui_Policy_Order.html The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

NEW QUESTION 350

- (Exam Topic 2)

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command `ntp authentication-key 1 md5 Cisc392368270`. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

- A. `ntp peer 1.1.1.1 key 1`
- B. `ntp server 1.1.1.1 key 1`
- C. `ntp server 1.1.1.2 key 1`
- D. `ntp peer 1.1.1.2 key 1`

Answer: B

Explanation:

To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
`NTP_Server(config)#ntp authentication-key 2 md5 securitytut`
`NTP_Server(config)#ntp authenticate`
`NTP_Server(config)#ntp trusted-key 2`
 Then you must configure the same authentication-key on the client router:
`NTP_Client(config)#ntp authentication-key 2 md5 securitytut`
`NTP_Client(config)#ntp authenticate`
`NTP_Client(config)#ntp trusted-key 2`
`NTP_Client(config)#ntp server 10.10.10.1 key 2`
 Note: To configure a Cisco device as a NTP client, use the command `ntp server <IP address>`. For example:
`Router(config)#ntp server 10.10.10.1`. This command will instruct the router to query 10.10.10.1 for the time.

NEW QUESTION 354

- (Exam Topic 2)

Drag and drop the threats from the left onto examples of that threat on the right

DoS/DDoS	A stolen customer database that contained social security numbers and was published online.
Insecure APIs	A phishing site appearing to be a legitimate login page captures user login information.
data breach	An application attack using botnets from multiple remote locations that flood a web application causing a degraded performance or a complete outage.
compromised credentials	A malicious user gained access to an organization's database from a cloud-based application programming interface that lacked strong authentication controls.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password.

NEW QUESTION 357

- (Exam Topic 2)

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

- A. Encrypted Traffic Analytics
- B. Threat Intelligence Director
- C. Cognitive Threat Analytics
- D. Cisco Talos Intelligence

Answer: B

NEW QUESTION 360

- (Exam Topic 2)

What are two benefits of Flexible NetFlow records? (Choose two)

- A. They allow the user to configure flow information to perform customized traffic identification
- B. They provide attack prevention by dropping the traffic
- C. They provide accounting and billing enhancements
- D. They converge multiple accounting technologies into one accounting mechanism
- E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Answer: AD

Explanation:

Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0_d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these layers.

NEW QUESTION 365

- (Exam Topic 2)

What is the difference between Cross-site Scripting and SQL Injection, attacks?

- A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
- B. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
- C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.
- D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

Answer: A

Explanation:

Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack. Answer C is not correct because the statement "Cross-site Scripting is when executives in a corporation are attacked" is not true. XSS is a client-side vulnerability that targets other application users. Answer D is not correct because the statement "Cross-site Scripting is an attack where code is executed from the server side". In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client's side. Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters. Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

NEW QUESTION 368

- (Exam Topic 2)

An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

- A. TCP 6514
- B. UDP 1700
- C. TCP 49
- D. UDP 1812

Answer: B

Explanation:

CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION 372

- (Exam Topic 2)

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

- A. Cisco Defense Orchestrator
- B. Cisco Secureworks
- C. Cisco DNA Center
- D. Cisco Configuration Professional

Answer: A

Explanation:

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html>

NEW QUESTION 377

- (Exam Topic 2)

What are the two types of managed Intercloud Fabric deployment models? (Choose two.)

- A. Public managed
- B. Service Provider managed
- C. Enterprise managed
- D. User managed
- E. Hybrid managed

Answer: BC

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_

NEW QUESTION 380

- (Exam Topic 2)

Refer to the exhibit.

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept' : application/json
    'content-type' : application/json
    'authorization' : Basic API Credentials
    'cache-control' : "no cache"
}
response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

What will happen when this Python script is run?

- A. The compromised computers and malware trajectories will be received from Cisco AMP
- B. The list of computers and their current vulnerabilities will be received from Cisco AMP
- C. The compromised computers and what compromised them will be received from Cisco AMP
- D. The list of computers, policies, and connector statuses will be received from Cisco AMP

Answer: D

Explanation:

Reference:

https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.

NEW QUESTION 384

- (Exam Topic 2)

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.

Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

- A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.
- B. Use EEM to have the ports return to service automatically in less than 300 seconds.
- C. Enter the shutdown and no shutdown commands on the interfaces.
- D. Enable the snmp-server enable traps command and wait 300 seconds
- E. Ensure that interfaces are configured with the error-disable detection and recovery feature

Answer: CE

Explanation:

You can also bring up the port by using these commands: + The “shutdown” interface configuration command followed by the “no shutdown” interface configuration command restarts the disabled port. + The “errdisable recovery cause ...” global configuration command enables the timer to automatically recover error-disabled state, and the “errdisable recovery interval interval” global configuration command specifies the time to recover error-disabled state.

NEW QUESTION 389

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 350-701 Exam with Our Prep Materials Via below:

<https://www.certleader.com/350-701-dumps.html>