Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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.
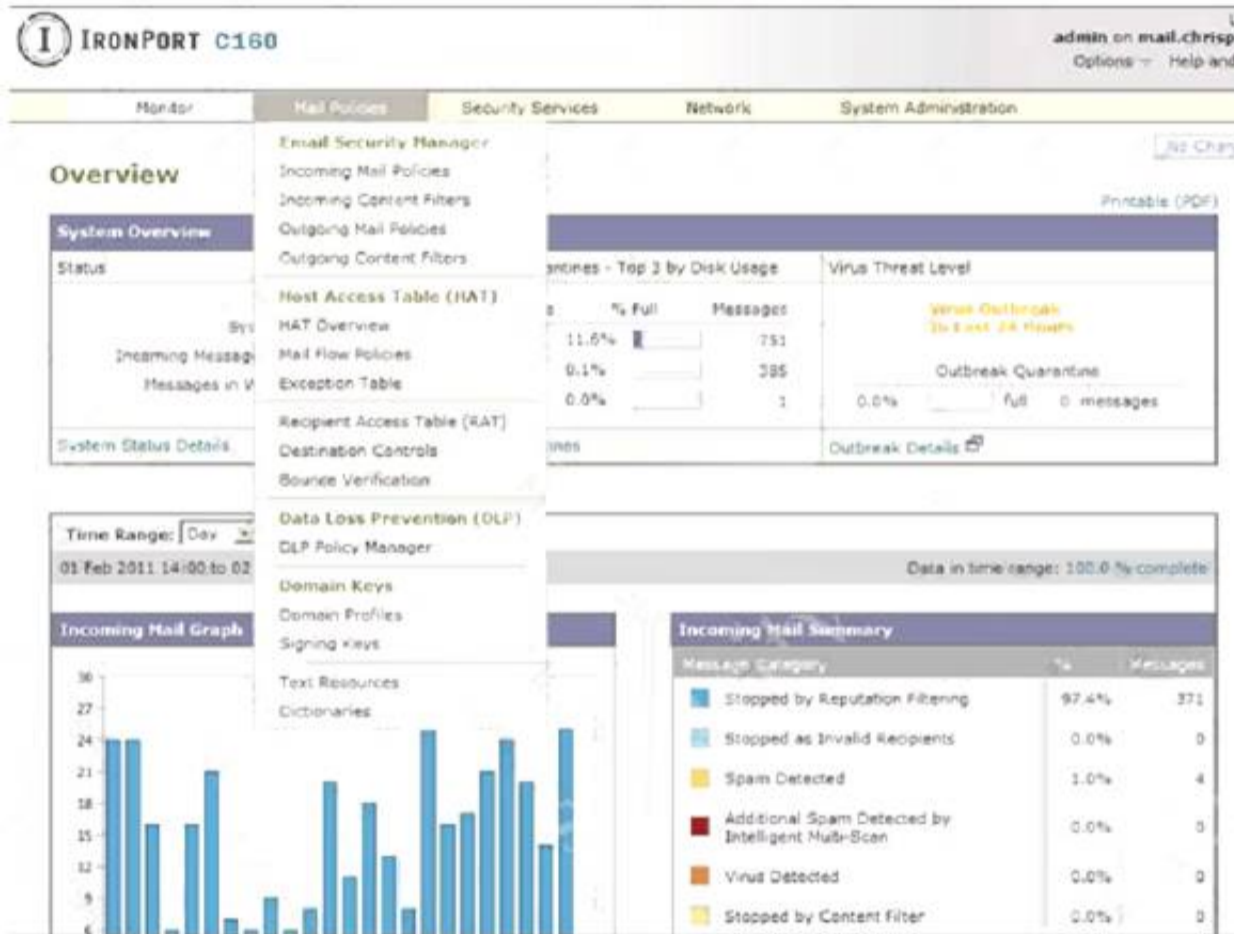
NEW QUESTION 2
- (Exam Topic 2)
An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which
vulnerability allows the attacker to see the passwords being transmitted in clear text?

A. weak passwords for authentication
B. unencrypted links for traffic
C. software bugs on applications
D. improper file security

Answer: B

NEW QUESTION 3
- (Exam Topic 2)
An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

A. NetFlow
B. Packet Tracer
C. Network Discovery
D. Access Control

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper

NEW QUESTION 4
- (Exam Topic 2)
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based? (Choose two)

A. URLs
B. protocol IDs
C. IP addresses
D. MAC addresses
E. port numbers

Answer: AC

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/secu

NEW QUESTION 5
- (Exam Topic 2)
In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

A. It allows multiple security products to share information and work together to enhance security posture in the network.
B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
D. It integrates with third-party products to provide better visibility throughout the network.
E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Answer: CE

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-c

NEW QUESTION 6
- (Exam Topic 1)
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. aaa server radius dynamic-author
B. aaa new-model
C. auth-type all
D. ip device-tracking

Answer: D

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

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

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

A. interpacket variation
B. software package variation
C. flow insight variation

D. process details variation

Answer: A

Explanation:
Reference: https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_

NEW QUESTION 10
- (Exam Topic 1)
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense

Answer: B

Explanation:
With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION 11
- (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 12
- (Exam Topic 1)
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

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

Answer: D

NEW QUESTION 13
- (Exam Topic 1)
What is the function of Cisco Cloudlock for data security?

A. data loss prevention
B. controls malicious cloud apps
C. detects anomalies
D. user and entity behavior analytics

Answer: A

NEW QUESTION 14
- (Exam Topic 1)
An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

A. Disable telnet using the no ip telnet command.
B. Enable the SSH server using the ip ssh server command.
C. Configure the port using the ip ssh port 22 command.
D. Generate the RSA key using the crypto key generate rsa command.

Answer: D

Explanation:
In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was missing the "crypto key generate rsa" command.

NEW QUESTION 15
- (Exam Topic 1)
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

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

Answer: AC

NEW QUESTION 16
- (Exam Topic 3)
An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

A. Summarized server-name information and MD5-hashed path information
B. complete URL,without obfuscating the path segments
C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
D. none because SensorBase Network Participation is disabled by default

Answer: B

NEW QUESTION 17
- (Exam Topic 3)
Which technology provides a combination of endpoint protection endpoint detection, and response?

A. Cisco AMP
B. Cisco Talos
C. Cisco Threat Grid
D. Cisco Umbrella

Answer: A

NEW QUESTION 18
- (Exam Topic 3)
Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface
B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
D. one listener on one logical IPv4 address on a single logical interface

Answer: D

NEW QUESTION 19
- (Exam Topic 3)
When choosing an algorithm to us, what should be considered about Diffie Hellman and RSA for key establishment?

A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys
B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys
C. DH is a symmetric key establishment algorithm intended to output asymmetric keys
D. DH is an asymmetric key establishment algorithm intended to output symmetric keys

Answer: D

Explanation:
Diffie Hellman (DH) uses a private-public key pair to establish a shared secret, typically a symmetric key. DH is not a symmetric algorithm – it is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm.

NEW QUESTION 20
- (Exam Topic 3)
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the service provider manages the operating system

Answer: C

NEW QUESTION 21
- (Exam Topic 3)
Refer to the exhibit.

```
ASA#   show   service-policy sfr

Global policy:
   Service-policy:  global_policy
      Class-map:  SFR
         SFR:  card status Up,  mode fail-open monitor-only
            Packet input 0, packet output           drop 0,  reset-drop 0
```

What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

A. The module is operating in IDS mode.
B. Traffic is blocked if the module fails.
C. The module fails to receive redirected traffic.
D. The module is operating in IPS mode.
E. Traffic continues to flow if the module fails.

Answer: AE

Explanation:
sfr {fail-open | fail-close [monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

NEW QUESTION 22
- (Exam Topic 3)
For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings
B. by specifying the websites in a custom blocked category
C. by adding the websites to a blocked type destination list
D. by adding the website IP addresses to the Cisco Umbrella blocklist

Answer: C

NEW QUESTION 23
- (Exam Topic 3)
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP

Answer: D

Explanation:
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.The traditional use of the pull

model, where the client requests data from the network does not scale when what you want is near real-time data.Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.
Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry

NEW QUESTION 24
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

A. routed mode
B. transparent mode
C. single context mode
D. multiple context mode

Answer: B

NEW QUESTION 25
- (Exam Topic 3)
An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

A. Specify the NTP version
B. Configure the NTP stratum
C. Set the authentication key
D. Choose the interface for syncing to the NTP server
E. Set the NTP DNS hostname

Answer: CD

NEW QUESTION 26
- (Exam Topic 3)
Which encryption algorithm provides highly secure VPN communications?

A. 3DES
B. AES 256
C. AES 128
D. DES

Answer: B

NEW QUESTION 27
- (Exam Topic 3)
What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 28
- (Exam Topic 3)
An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on but it sees only the requests from its public IP address instead of each internal IP address. What must be done to resolve this issue?

A. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address
B. Use the tenant control features to identify each subnet being used and track the connections within theCisco Umbrella dashboard
C. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard
D. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains

Answer: A

NEW QUESTION 29
- (Exam Topic 3)
What is the purpose of a NetFlow version 9 template record?

A. It specifies the data format of NetFlow processes.
B. It provides a standardized set of information about an IP flow.
C. It defines the format of data records.
D. It serves as a unique identification number to distinguish individual data records

Answer: C

NEW QUESTION 30
- (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 configurationcommand 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 31
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

350-701 Practice Exam Features:

* 350-701 Questions and Answers Updated Frequently

* 350-701 Practice Questions Verified by Expert Senior Certified Staff

* 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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