Free Questions for 350-701 by certscare

Shared by Holcomb on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a benefit of a Cisco Secure Email Gateway Virtual as compared to a physical Secure Email Gateway?

Options:

A- simplifies the distribution of software updates

B- provides faster performance

C- provides an automated setup process

D- enables the allocation of additional resources

Answer:

D

Explanation:

One of the benefits of a Cisco Secure Email Gateway Virtual appliance compared to a physical one is the ability to allocate additional resources as needed. Virtual appliances can be easily scaled up by allocating more CPU, memory, or storage resources, providing flexibility and scalability in response to changing demands or growth.

Question 2

Question Type: MultipleChoice

A network administrator is modifying a remote access VPN on an FTD managed by an FMC. The administrator wants to offload traffic to certain trusted domains. The administrator wants this traffic to go out of the client's local internet and send other internet-bound traffic over the VPN Which feature must the administrator configure?

Options:

A- dynamic split tunneling

B- local LAN access

C- dynamic access policies

D- reverse route injection

Answer:

A

Explanation:

In a remote access VPN configuration, dynamic split tunneling allows traffic to certain trusted domains to bypass the VPN tunnel and exit through the client's local internet gateway. This feature selectively directs only the necessary traffic over the VPN, while allowing direct internet access for specific domains or traffic deemed safe or trusted, optimizing bandwidth and performance for remote users.

Question 3

Question Type: MultipleChoice

A security test performed on one of the applications shows that user input is not validated. Which security vulnerability is the application more susceptible to because of this lack of validation?

Options:

A- denial -of-service

B- cross-site request forgery

C- man-in-the-middle

D- SQL injection

Answer:

D

Explanation:

An application that does not validate user input is particularly susceptible to SQL injection attacks. In an SQL injection attack, an attacker can insert or 'inject' a SQL query via the input data from the client to the application. Due to the lack of validation, the malicious SQL commands are executed by the database server, leading to unauthorized access or manipulation of the database.

Question 4

Question Type: MultipleChoice

Which Cisco solution provides a comprehensive view of Internet domains. IP addresses, and autonomous systems to help pinpoint attackers and malicious infrastructures?

Options:

A- Cisco Threat Indication Database

B- Cisco Advanced Malware Investigate

C- Cisco Umbrella Investigate

D- Cisco Secure Workload Cloud

Answer:

C

Explanation:

Cisco Umbrella Investigate provides a comprehensive view of Internet domains, IP addresses, and autonomous systems, offering a wealth of information about the infrastructure of the internet. It helps security analysts and threat investigators to pinpoint current and emerging threats by providing access to data from Cisco's global network, thereby enabling the identification of attackers and malicious infrastructures.

Question 5

Question Type: MultipleChoice

Which action configures the IEEE 802.1X Flexible Authentication feature lo support Layer 3 authentication mechanisms?

Options:

A- Identity the devices using this feature and create a policy that allows them to pass Layer 2 authentication.

B- Configure WebAuth so the hosts are redirected to a web page for authentication.

C- Modify the Dot1x configuration on the VPN server lo send Layer 3 authentications to an external authentication database

D- Add MAB into the switch to allow redirection to a Layer 3 device for authentication.

Answer:

D

Explanation:

Configuring the IEEE 802.1X Flexible Authentication feature to support Layer 3 authentication mechanisms involves adding MAC Authentication Bypass (MAB) into the switch configuration. This allows devices that do not support 802.1X to be authenticated using their MAC address. Once MAB identifies the device, it can then be redirected to a Layer 3 device for further authentication, thus providing a mechanism to support devices requiring Layer 3 authentication methods.

Question 6

Question Type: MultipleChoice

What is the purpose of the Trusted Automated exchange cyber threat intelligence industry standard?

Options:

A- public collection of threat intelligence feeds

B- threat intelligence sharing organization

C- language used to represent security information

D- service used to exchange security information

Answer:

D

Explanation:

Trusted Automated eXchange of Intelligence Information (TAXII) is a collection of services and message exchanges that enable the sharing of cyber threat intelligence across product, service, and organizational boundaries. It is designed to support the exchange of CTI represented in STIX, but is not limited to STIX. TAXII defines an API that aligns with common sharing models, such as hub-and-spoke, peer-to-peer, and subscribe/publish. TAXII is not a public collection of threat intelligence feeds, a threat intelligence sharing organization, or a language used to represent security information. Those are possible descriptions of STIX, which is a complementary standard to TAXII.Reference:STIX and TAXII Approved as OASIS Standards to Enable Automated Exchange of Cyber Threat Intelligence,STIX V2.1 and TAXII V2.1 OASIS Standards are published,What is STIX/TAXII? | Cloudflare,What is STIX / TAXII? Learn about the industry

Question 7

Question Type: MultipleChoice

A network administrator is setting up Cisco FMC to send logs to Cisco Security Analytics and Logging (SaaS). The network administrator is anticipating a high volume of logging events from the firewalls and wants lo limit the strain on firewall resources. Which method must the administrator use to send these logs to Cisco Security Analytics and Logging?

Options:

A- SFTP using the FMCCLI

B- syslog using the Secure Event Connector

C- direct connection using SNMP traps

D- HTTP POST using the Security Analytics FMC plugin

Answer:

B

Explanation:

The Secure Event Connector is a component of the Security Analytics and Logging (SaaS) solution that enables the FMC to send logs to the cloud-based service. The Secure Event Connector uses syslog to forward events from the FMC and the managed devices to the cloud. This method reduces the load on the firewall resources, as the events are sent in batches and compressed before transmission. The Secure Event Connector also provides encryption, authentication, and reliability for the log data.The other methods are not supported by the Security Analytics and Logging (SaaS) solution12Reference:=1: Cisco Security Analytics and Logging (On Premises)

Question 8

Question Type: MultipleChoice

What is the purpose of a denial-of-service attack?

Options:

A- to disrupt the normal operation of a targeted system by overwhelming It

B- to exploit a security vulnerability on a computer system to steal sensitive information

C- to prevent or limit access to data on a computer system by encrypting It

D- to spread throughout a computer system by self-replicating to additional hosts

Answer:

A

Explanation:

The purpose of a Denial-of-Service (DoS) attack is to disrupt the normal operation of a targeted system, server, or network by overwhelming it with a flood of internet traffic. This is achieved by utilizing multiple compromised computer systems as sources of attack traffic. The overwhelming amount of traffic can cause the targeted system to slow down significantly or even crash and become unavailable to legitimate users, thereby denying service to intended users.

Question 9

Question Type: MultipleChoice

What is a functional difference between Cisco Secure Endpoint and Cisco Umbrella Roaming Client?

Options:

A- Secure Endpoint authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.

B- Secure Endpoint stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

C- The Umbrella Roaming Client authenticates users and provides segmentation, and Secure Endpoint allows only for VPN connectivity.

D- The Umbrella Roaming client stops and tracks malicious activity on hosts, and Secure Endpoint tracks only URL-based threats.

Answer:

B

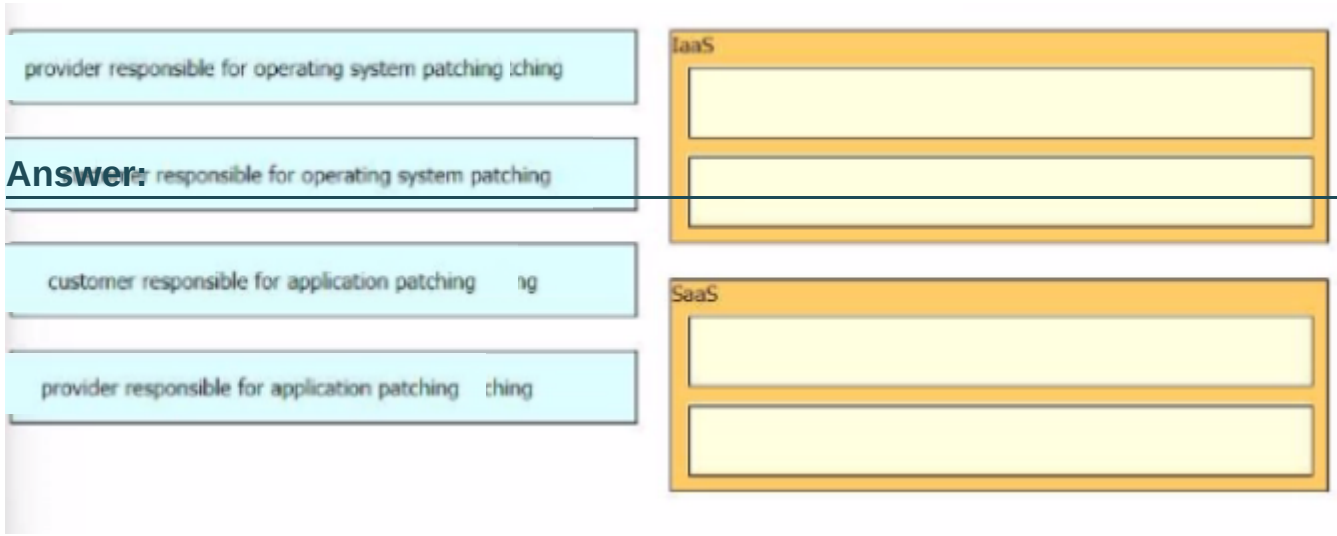
Explanation:

The functional difference between Cisco Secure Endpoint (formerly known as AMP for Endpoints) and Cisco Umbrella Roaming Client lies in their approach to security. Cisco Secure Endpoint is designed to prevent, detect, and respond to threats on the endpoint devices. It provides comprehensive protection by stopping and tracking malicious files and activities on hosts, utilizing continuous analysis and retrospective security to address threats at various stages of the attack continuum. On the other hand, Cisco Umbrella Roaming Client is focused on DNS and IP layer enforcement to prevent internet-based threats before a connection is established. It primarily tracks and blocks URL-based threats by enforcing security at the DNS layer, thus preventing access to malicious domains. Therefore, while Secure Endpoint provides broad endpoint protection against a variety of threats, the Umbrella Roaming Client specifically targets URL-based threats.

Question 10

Question Type: DragDrop

Drag and drop the security responsibilities from the left onto the corresponding cloud service models on the right.



Answer: