Leads4Pass

350-701^Q&As

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

A. inter-EPG isolation

B. inter-VLAN security

C. intra-EPG isolation

D. placement in separate EPGs

Correct Answer: C

C. Intra-EPG Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from on another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent

QUESTION 2

Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

A. retrospective detection

B. indication of compromise

C. file trajectory

D. elastic search

Correct Answer: B

QUESTION 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 an untrusted interface for all clients

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

Correct Answer: D

QUESTION 4

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

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight- management-center/datasheetc78-736775.html

QUESTION 5

An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration? (Choose two.)

A. Specify the SNMP manager and UDP port.

B. Specify an SNMP user group

C. Specify a community string.

D. Add an SNMP USM entry

E. Add an SNMP host access entry

Correct Answer: BD

QUESTION 6

DRAG DROP

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the righ.

Select and Place:

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to lock at sensitive files.
interesting file access	Tetration platform watches user access failures and methods
file access from a different user	Tetration platform watches for movement in the process lineage tree.

Correct Answer:

file access from a different user
interesting file access
user login suspicious behavior
privilege escalation

Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

User login suspicious behavior: Cisco Secure Workload platform watches user login failures and user login methods.

Interesting file access: Cisco Secure Workload platform can be armed to look at sensitive files.

File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user.

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html

QUESTION 7

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

Correct Answer: B

Cisco FMC\\'s Threat Intelligence Director allows security teams to integrate security intelligence observables from various sources, such as Cisco Talos, into their Cisco FMC environment. This allows the FMC to push updated security intelligence to its sensors, enabling them to better detect and respond to potential threats.

QUESTION 8

What must be used to share data between multiple security products?

A. Cisco Rapid Threat Containment

B. Cisco Platform Exchange Grid

C. Cisco Advanced Malware Protection

D. Cisco Stealthwatch Cloud

Correct Answer: B

QUESTION 9

A hacker initiated a social engineering attack and stole username and passwords of some users within a company. Which product should be used as a solution to this problem?

A. Cisco NGFW

B. Cisco AnyConnect

C. Cisco AMP for Endpoints

D. Cisco Duo

Correct Answer: D

QUESTION 10

What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices

B. to request a newly provisioned mobile device

C. to provision userless and agentless systems

D. to manage and deploy antivirus definitions and patches on systems owned by the end user

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2- 4/mydevices/b_mydevices_2x.html

---

QUESTION 11

How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.

B. It prevents exfiltration of sensitive data.

C. It assigns Internet-based DNS protection for clients and servers.

D. It facilitates secure connectivity between public and private networks.

Correct Answer: A

Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

QUESTION 12

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling

B. Use MAB with posture assessment.

C. Use 802.1X with posture assessment.

D. Use 802.1X with profiling.

Correct Answer: A

Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design- guide/ta-p/3739456

QUESTION 13

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

A. NetFlow

B. desktop client

C. ASDM

D. API

Correct Answer: D

QUESTION 14

Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

A. Cisco Identity Services Engine

B. Cisco Enterprise Security Appliance

C. Cisco Web Security Appliance

D. Cisco Advanced Stealthwatch Appliance

Correct Answer: C

QUESTION 15

An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

A. EAPOL

B. SSH

C. RADIUS

D. TACACS+

Correct Answer: D

350-701 PDF Dumps   350-701 Practice Test   350-701 Exam Questions