

➤ **Vendor: Cisco**

➤ **Exam Code: 350-701**

➤ **Exam Name: Implementing and Operating Cisco Security Core Technologies (SCOR)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [March/2021](#))**

### **Visit Braindump2go and Download Full Version 350-701 Exam Dumps**

#### **QUESTION 257**

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

- A. Use security services to configure the traffic monitor, .
- B. Use URL categorization to prevent the application traffic.
- C. Use an access policy group to configure application control settings.
- D. Use web security reporting to validate engine functionality

**Answer: C**

#### **Explanation:**

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

#### **QUESTION 258**

Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?

- A. BYOD on boarding
- B. Simple Certificate Enrollment Protocol
- C. Client provisioning
- D. MAC authentication bypass

**Answer: A**

#### **Explanation:**

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices.

Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.

Reference: [https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin\\_guide/b\\_ISE\\_admin\\_guide\\_24/m\\_ise\\_devices\\_byod.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html)

#### **QUESTION 259**

Refer to the exhibit. What will happen when this Python script is run?

**[350-701 Exam Dumps](#) [350-701 Exam Questions](#) [350-701 PDF Dumps](#) [350-701 VCE Dumps](#)**

**<https://www.braindump2go.com/350-701.html>**

```
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.text)
```

- 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:**

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees.

Reference:

[https://api-](https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1)

[docs.amp.cisco.com/api\\_actions/details?api\\_action=GET+%2Fv1%2Fcomputers&api\\_host=api.apjc.amp.cisco.com&api\\_resource=Computer&api\\_version=v1](https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1)

**QUESTION 260**

An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch
- D. Cisco Tetration

**Answer: D**

**Explanation:**

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.

Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies. To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change.

Reference: <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solution-overview-c22-739268.pdf>

**QUESTION 261**

Which factor must be considered when choosing the on-premise solution over the cloud-based one?

**[350-701 Exam Dumps](#) [350-701 Exam Questions](#) [350-701 PDF Dumps](#) [350-701 VCE Dumps](#)**

**<https://www.braindump2go.com/350-701.html>**

- A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it
- B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
- C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
- D. With an on-premise solution, the customer is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the provider is responsible for it.

**Answer:** D

**QUESTION 262**

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

- A. consumption
- B. sharing
- C. analysis
- D. authoring

**Answer:** A

**Explanation:**

<https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector>

**QUESTION 263**

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:**

You can also monitor on-premises networks in your organizations using Cisco Stealthwatch Cloud. In order to do so, you need to deploy at least one Cisco Stealthwatch Cloud Sensor appliance (virtual or physical appliance).

**QUESTION 264**

What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

- A. Ethos Engine to perform fuzzy fingerprinting
- B. Tetra Engine to detect malware when me endpoint is connected to the cloud
- C. Clam AV Engine to perform email scanning
- D. Spero Engine with machine learning to perform dynamic analysis

**Answer:** A

**Explanation:**

ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.

**QUESTION 265**

What are two characteristics of Cisco DNA Center APIs? (Choose two)

- A. Postman is required to utilize Cisco DNA Center API calls.

**[350-701 Exam Dumps](#) [350-701 Exam Questions](#) [350-701 PDF Dumps](#) [350-701 VCE Dumps](#)**

**<https://www.braindump2go.com/350-701.html>**

- B. They do not support Python scripts.
- C. They are Cisco proprietary.
- D. They quickly provision new devices.
- E. They view the overall health of the network

**Answer:** DE

**QUESTION 266**

What is a benefit of conducting device compliance checks?

- A. It indicates what type of operating system is connecting to the network.
- B. It validates if anti-virus software is installed.
- C. It scans endpoints to determine if malicious activity is taking place.
- D. It detects email phishing attacks.

**Answer:** B

**QUESTION 267**

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:**

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.

Reference: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsecwith-easy-connect-configuration-guide.pdf>

**QUESTION 268**

What is the benefit of installing Cisco AMP for Endpoints on a network?

- A. It provides operating system patches on the endpoints for security.
- B. It provides flow-based visibility for the endpoints network connections.
- C. It enables behavioral analysis to be used for the endpoints.
- D. It protects endpoint systems through application control and real-time scanning

**Answer:** D

**QUESTION 269**

An administrator is configuring a DHCP server to better secure their environment. They need to be able to rate-limit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

- A. Set a trusted interface for the DHCP server
- B. Set the DHCP snooping bit to 1
- C. Add entries in the DHCP snooping database
- D. Enable ARP inspection for the required VLAN

**Answer: A**

**QUESTION 270**

Refer to the exhibit. What will happen when the Python script is executed?

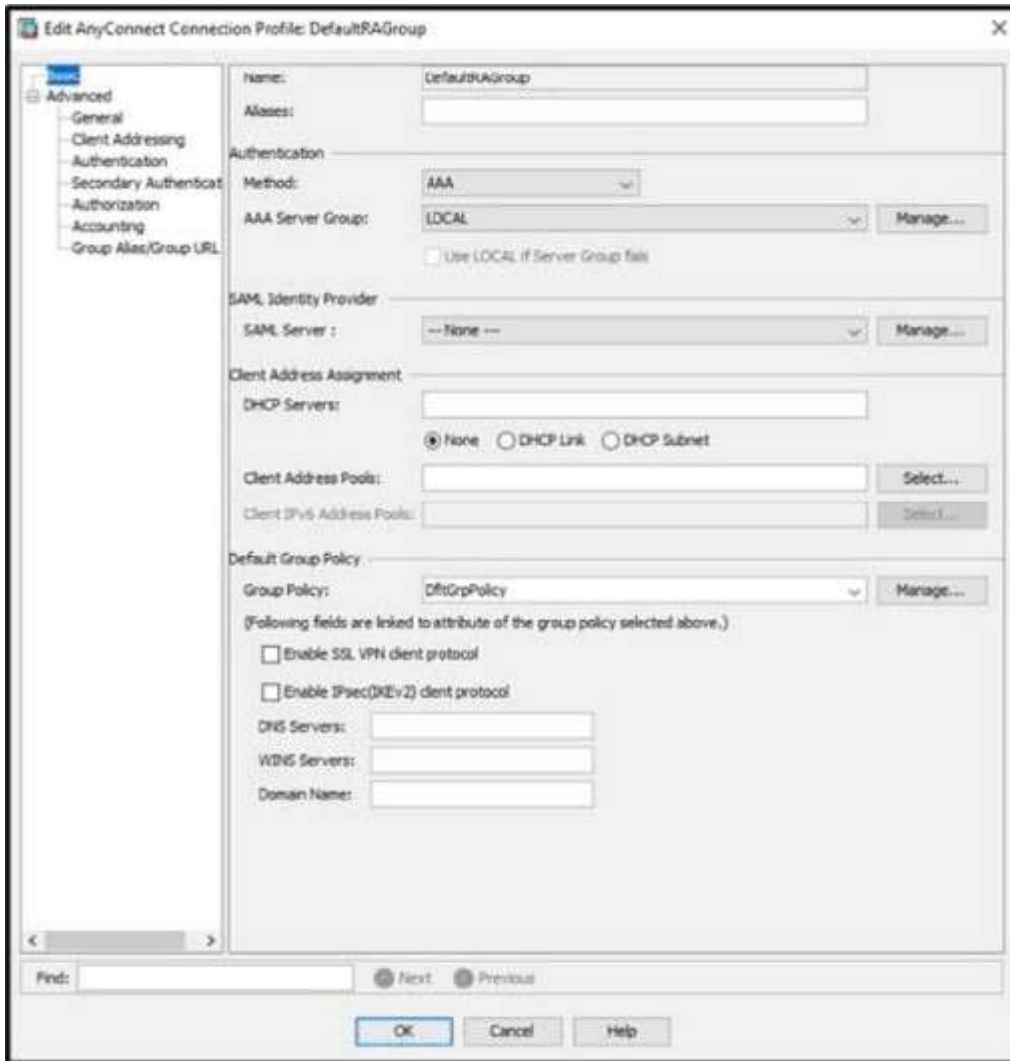
```
import requests
client_id = '<Client ID>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```

- A. The hostname will be translated to an IP address and printed.
- B. The hostname will be printed for the client in the client ID field.
- C. The script will pull all computer hostnames and print them.
- D. The script will translate the IP address to FQDN and print it

**Answer: C**

**QUESTION 271**

Refer to the exhibit. When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?



- A. Group Policy
- B. Method
- C. SAML Server
- D. DHCP Servers

**Answer: B**

**Explanation:**

In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

#### **QUESTION 272**

An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

- A. Cisco Umbrella
- B. Cisco Cloud Email Security
- C. Cisco NGFW
- D. Cisco Cloudlock

**Answer: D**

**Explanation:**

**[350-701 Exam Dumps](#) [350-701 Exam Questions](#) [350-701 PDF Dumps](#) [350-701 VCE Dumps](#)**

**<https://www.braindump2go.com/350-701.html>**



Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glancec45-738565.pdf>

**QUESTION 273**

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

- A. SIEM
- B. CASB
- C. Adaptive MFA
- D. Cisco Cloudlock

**Answer: D**

**Explanation:**

+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.

+ Cloudlock is API-based.

+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).

Reference: <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>

Note:

+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.

+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.

**QUESTION 274**

Why is it important to implement MFA inside of an organization?

- A. To prevent man-the-middle attacks from being successful.
- B. To prevent DoS attacks from being successful.
- C. To prevent brute force attacks from being successful.
- D. To prevent phishing attacks from being successful.

**Answer: C**

**QUESTION 275**

A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views.

What must the administrator do to accomplish this?

- A. map SNMPv3 users to SNMP views
- B. set the password to be used for SNMPv3 authentication
- C. define the encryption algorithm to be used by SNMPv3
- D. specify the UDP port used by SNMP

**Answer: B**

**QUESTION 276**

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: C**

**QUESTION 277**

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

**Answer: A**

**QUESTION 278**

Drag and Drop Question

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Version 1	appropriate only for legacy systems
Version 5	appropriate only for the main cache
Version 8	introduced extensibility
Version 9	introduced support for aggregation caches

**Answer:**

Version 1
Version 5
Version 9
Version 8

**Explanation:**

The Version 1 format was the initially released version.

Do not use the Version 1 format unless you are using a legacy collection system that requires it.

Use Version 9 or Version 5 export format. Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features.

Version 8 export format is available only for aggregation caches; it cannot be expanded to support new features.

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mtbook/cfg-nflow-data-expt.html>

**QUESTION 279**

Drag and Drop Question

Drag and drop the solutions from the left onto the solution's benefits on the right.



Cisco Stealthwatch	obtains contextual identity and profiles for all the users and devices connected on a network
Cisco ISE	software-defined segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network
Cisco TrustSec	rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic
Cisco Umbrella	secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

**Answer:**

Cisco ISE
Cisco TrustSec
Cisco Stealthwatch
Cisco Umbrella