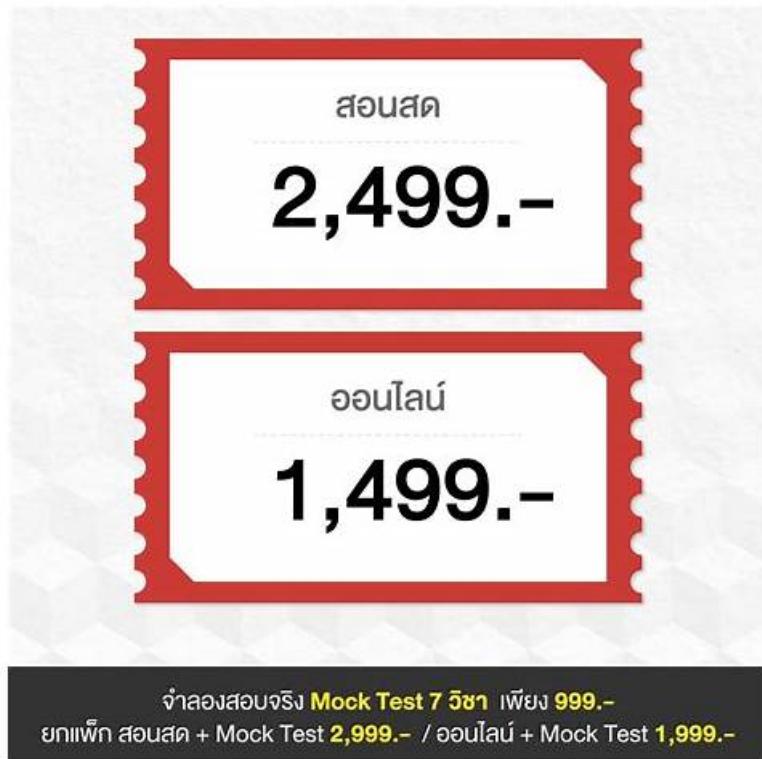


# Accurate 350-701 Practice Mock | 100% Free 350-701 Exam Tests



BTW, DOWNLOAD part of ITdumpsfree 350-701 dumps from Cloud Storage: <https://drive.google.com/open?id=1E5U08qHebPYInkZsF74jG38yBU7qqIDm>

Do not waste further time and money, get real Cisco 350-701 pdf questions and practice test software, and start Cisco 350-701 test preparation today. ITdumpsfree will also provide you with up to 365 days of free Implementing and Operating Cisco Security Core Technologies exam questions updates, It will just need to take one or two days to practice Cisco 350-701 Test Questions and remember answers. You will free access to our test engine for review after payment.

Cisco 350-701 Exam is an industry-standard certification that tests the knowledge and skills of IT professionals on the principles of implementing and operating Cisco Security Core Technologies. 350-701 exam is designed to assess the individual's ability to manage complex security solutions, identify network vulnerabilities, and implement security policies to mitigate security threats. 350-701 exam is a core requirement for the CCNP Security certification and is ideal for IT professionals who want to advance their careers in security.

## Who Should Take Cisco 350-701 Exam?

Test 350-701 is for those willing to discover more about how Cisco network security systems work and aiming to earn the Cisco Specialist – Security Core certification or any of the related higher-level certificates. Also, it covers network access and visibility and thus is ideal for network engineers and designers, as well as security engineers, system engineers, or network managers.

When it comes to prerequisites, the vendor doesn't have any mandatory conditions. However, it is important that the candidate has some prior experience using basic Cisco network security. Also, the understanding of networking fundamentals or consistent knowledge equivalent to Cisco CCNA is recommended.

>> 350-701 Practice Mock <<

## 350-701 Exam Tests, 350-701 Reliable Dumps Files

If you always feel that you can't get a good performance when you come to the exam room. There is Software version of our 350-

701 exam braindumps, it can simulate the real exam environment. If you take good advantage of this 350-701 practice materials character, you will not feel nervous when you deal with the Real 350-701 Exam. Furthermore, it can be downloaded to all electronic devices so that you can have a rather modern study experience conveniently. Why not have a try?

## **Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q423-Q428):**

### **NEW QUESTION # 423**

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. placement in separate EPGs
- B. inter-VLAN security
- C. inter-EPG isolation
- D. **intra-EPG isolation**

### **Answer: D**

Explanation:

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.

### **NEW QUESTION # 424**

What are two Trojan malware attacks? (Choose two)

- A. Smurf
- B. **Rootkit**
- C. Backdoor
- D. Frontdoor
- E. Sync

### **Answer: B,C**

Explanation:

A Trojan malware attack is a type of malicious code or software that disguises itself as a legitimate program or file to trick users into executing it. Once executed, the Trojan can perform various harmful actions on the infected system or network, such as stealing data, deleting files, or installing other malware. There are different types of Trojan malware attacks, depending on their purpose and behavior. Two common types are:

\* Rootkit: A rootkit is a type of Trojan that hides itself and other malware from detection and removal by antivirus software or system tools. A rootkit can modify the operating system or the firmware of the device to gain persistent and privileged access to the system. A rootkit can also intercept and manipulate system calls, network traffic, or user input to conceal its activities or redirect them to malicious servers.

\* Backdoor: A backdoor is a type of Trojan that creates a secret or unauthorized access point to the infected system or network. A backdoor can allow an attacker to remotely control the system, execute commands, upload or download files, or monitor the system activity. A backdoor can also be used to install other malware or launch further attacks on other systems or networks.

References:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 1: Malware Threats, Lesson 1: Identifying Malware Threats, Topic: Trojan Horse What is a Trojan? Is it a virus or is it malware? - Norton Trojan Horse Examples (2024): The 6 Worst Attacks Ever - SoftwareLab

### **NEW QUESTION # 425**

What is the function of SDN southbound API protocols?

- A. to enable the controller to use REST
- B. to allow for the dynamic configuration of control plane applications
- C. **to enable the controller to make changes**
- D. to allow for the static configuration of control plane applications

**Answer: C**

Explanation:

Explanation

**NEW QUESTION # 426**

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

- A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
- B. EPP focuses on network security, and EDR focuses on device security.
- C. EDR focuses on network security, and EPP focuses on device security.
- D. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.

**Answer: A**

Explanation:

Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) are both important components of an endpoint security strategy, but they have different goals and capabilities. EPP is designed to act as a preventive security measure, blocking known and unknown malware and malicious activity on endpoint devices using various techniques such as antivirus, data encryption, and data loss prevention. EPP solutions are mainly cloud-managed and assisted by cloud data, and use multiple detection engines such as signature-based, machine learning, and behavioral analysis. EPP solutions prevent breaches by leveraging threat intelligence and sandboxing capabilities to continuously protect endpoints from emerging threats<sup>12</sup>.

EDR, on the other hand, focuses on detecting and responding to advanced threats that have already evaded the front-line defenses and infiltrated the environment. EDR solutions provide continuous and comprehensive visibility into endpoint activity in real time, allowing security teams to quickly and effectively identify and remediate cyberattacks such as ransomware and fileless malware. EDR solutions offer advanced threat detection, investigation, and response capabilities, including incident data search and investigation, alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. EDR solutions serve as a safety net to capture threats that go undetected by traditional antivirus software and uncover incidents that would otherwise remain invisible<sup>34</sup>.

Therefore, the primary difference between an EPP and an EDR is that EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses. References: 1: Endpoint Protection Platform (EPP) Definition - Cisco 2: EPP vs. EDR: Why You Need Both - CrowdStrike 3: Endpoint Detection and Response (EDR) Definition - Cisco 4: EDR vs EPP: Why Should You Have to Choose? - Check Point Software

**NEW QUESTION # 427**

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

- A. to manage and deploy antivirus definitions and patches on systems owned by the end user
- B. to request a newly provisioned mobile device
- C. to provision userless and agentless systems
- D. to register new laptops and mobile devices

**Answer: D**

Explanation:

Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

**NEW QUESTION # 428**

.....

The contents of 350-701 study materials are all compiled by industry experts based on the examination outlines and industry development trends over the years. And our 350-701 exam guide has its own system and levels of hierarchy, which can make users improve effectively. Our 350-701 learning dumps can simulate the real test environment. After the exam is over, the system also gives the total score and correct answer rate.

**350-701 Exam Tests:** <https://www.itdumpsfree.com/350-701-exam-passed.html>

P.S. Free & New 350-701 dumps are available on Google Drive shared by ITdumpsfree: <https://drive.google.com/open?id=1E5U08qHebPYInkZsF74jG38yBU7qqIDm>