

642-513

Cisco

Securing Hosts Using Cisco Security Agent

Visit: <http://www.pass4sureofficial.com/exams.asp?examcode=642-513>

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 642-513 exam in first attempt, but also you can get a high score to acquire Cisco certification.

If you use pass4sureofficial 642-513 Certification questions and answers, you will experience actual 642-513 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 642-513 exam. Every point from pass4sure 642-513 PDF, 642-513 review will help you take Cisco 642-513 exam much easier and become Cisco certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Cisco 642-513 course:

- * Up-to-Date Cisco 642-513 questions taken from the real exam.
- * 100% correct Cisco 642-513 answers you simply can't find in other 642-513 courses.
- * All of our tests are easy to download. Your file will be saved as a 642-513 PDF.
- * Cisco 642-513 brain dump free content featuring the real 642-513 test questions.

Cisco 642-513 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 642-513 exam training are an absolute favorite in the industry. You will pass Cisco 642-513 certification test and career opportunities will be open for you.



Question: 1

Company chose the Cisco CSA product to protect the network against the newest attacks. Cisco Security Agent provides Day Zero attack prevention by using which of these methods?

- A. Using signatures to enforce security policies
- B. Using API control to enforce security policies
- C. Using stateful packet filtering to enforce security policies
- D. Using algorithms that compare application calls for system resources to the security policies
- E. None of the above

Answer: D

Explanation:

Because Cisco Security Agent analyzes behavior rather than relying on signature matching, it never needs updating to stop a new attack. This zero-update architecture provides protection with reduced operational costs and can identify so-called "Day Zero" threats." At a high level, Cisco? Security Agent is straightforward. It intercepts system calls between applications and the operating system, correlates them, compares the correlated system calls against a set of behavioral rules, and then makes an "allow" or "deny" decision based on the results of its comparison. This process is called INCORE, which stands for intercept, correlate, rules engine.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_white_paper0900aecd8020f448.shtml

Question: 2

Company has implemented the CSA product to provide security for all of their devices. For which layers of the OSI reference model does CSA enforce security?

- A. Layer 1
through Layer 4
- B. Layer 1 through Layer 7
- C. Layer 2 through Layer 4
- D. Layer 3 through Layer 7

Answer: D

Explanation:

Cisco Security Agent provides threat protection for server and desktop computing systems, also known as endpoints. It helps to reduce operational costs by identifying, preventing, and eliminating known and unknown security threats. The Cisco Security Agent consolidates endpoint security functions in a single agent, providing:

1. Host intrusion prevention
2. Spyware/adware protection
3. Protection against buffer overflow attacks
4. Distributed firewall capabilities
5. Malicious mobile code protection
6. Operating-system integrity assurance
7. Application inventory
8. Audit log-consolidation

This provides security for endpoints at the network layer (layer 3) through the application layer (layer 7).

Question: 3

The CSA architecture model is made up of three major components. Which three are they? (Choose three)

- A. Cisco Trust Agent
- B. Cisco Security Agent
- C. Cisco Security Agent Management Center
- D. Cisco Intrusion Prevention System
- E. An administrative workstation
- F. A syslog server

Answer: B, C, E

Explanation:

The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers. The agents themselves, and an administrative workstations, combined with the Management Center, comprise the three aspects of the CSA architecture. Agents register with CSA MC. CSA MC checks its configuration database for a record of the system. When the system is found and authenticated, CSA MC deploys a configured policy for that particular system or grouping of systems.

Question: 4

As a Company trainee you are required to match the Cisco Trust Agent posture state with its definition.

| | | |
|-------------|---|------------|
| do not care | Host credentials are up to date, and the risk to the network from this host is low. | Place here |
| healthy | This state is not provided by ACS. All received posture states can match or not match this selection, and the policy state is not affected. | Place here |
| checkup | Host credentials are out of date. The host is vulnerable to compromise and should be updated immediately. | Place here |
| quarantine | Host credentials are not quite up to date, but the risk to the network is low. | Place here |

Answer:

| | | |
|-------------|---|-------------|
| do not care | Host credentials are up to date, and the risk to the network from this host is low. | healthy |
| healthy | This state is not provided by ACS. All received posture states can match or not match this selection, and the policy state is not affected. | do not care |
| checkup | Host credentials are out of date. The host is vulnerable to compromise and should be updated immediately. | quarantine |
| quarantine | Host credentials are not quite up to date, but the risk to the network is low. | checkup |

Question: 5

As a Company student you are required to match the CSA MC view with the corresponding definition.

| | | |
|----------------------|--|-------------------|
| Groups | Use this option to create and manage installable CSA software that can be used for mass deployment and automatic registration. | <i>Place here</i> |
| Hosts | Use this option to control the set of systems running CSA software that are allowed to register with this system. | <i>Place here</i> |
| Software Updates | Use this option to view detailed status and configuration information of systems running CSA software. | <i>Place here</i> |
| Agent Kits | Use this option to define and manage groups of systems running CSA software. | <i>Place here</i> |
| Registration Control | Use these options to schedule automatic remote upgrades of older versions of CSA software. | <i>Place here</i> |

Answer:

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time \$99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads

<http://www.pass4sureofficial.com/allexams.asp>

View list of All Study Guides (SG) downloads

<http://www.pass4sureofficial.com/study-guides.asp>

View list of All Audio Exams (AE) downloads

<http://www.pass4sureofficial.com/audio-exams.asp>

Download All Exams Samples

<http://www.pass4sureofficial.com/samples.asp>

To purchase \$99 Lifetime Full Access Membership click here

<http://www.pass4sureofficial.com/purchase.asp>

| | | | | | | |
|------------|--------------------|------------------|---------|------------------|--------------|-----------|
| 3COM | CompTIA | Filemaker | IBM | LPI | OMG | Sun |
| ADOBE | ComputerAssociates | Fortinet | IISFA | McAfee | Oracle | Sybase |
| APC | CWNP | Foundry | Intel | McData | PMI | Symantec |
| Apple | DELL | Fujitsu | ISACA | Microsoft | Polycom | TeraData |
| BEA | ECCouncil | GuidanceSoftware | ISC2 | Mile2 | RedHat | TIA |
| BICSI | EMC | HDI | ISEB | NetworkAppliance | Sair | Tibco |
| CheckPoint | Enterasys | Hitachi | ISM | Network-General | SASInstitute | TruSecure |
| Cisco | ExamExpress | HP | Juniper | Nokia | SCP | Veritas |
| Citrix | Exin | Huawei | Legato | Nortel | See-Beyond | Vmware |
| CIW | ExtremeNetworks | Hyperion | Lotus | Novell | SNIA | |

