

642-545 braindumps

Cisco CCSP

642-545: Implementing Cisco Security Monitoring, Analysis and Response System

Practice Exam: 642-545 Exams

Exam Number/Code: 642-545

Exam Name: Implementing Cisco Security Monitoring, Analysis and Response System

Questions and Answers: 42 Q&As

([CCSP](#))



Exam : [642-545](#)

"Implementing Cisco Security Monitoring, Analysis and Response System", also known as 642-545 exam, is a Cisco certification. With the complete collection of exam questions, Just4Study has assembled to take you through 42 Q&As to your 642-545 exam preparation. In the 642-545 exam resources, you will cover every field and category in Cisco Certification helping to ready you for your successful Cisco Certification.

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Cisco CCSP 642-545 (Implementing Cisco Security Monitoring, Analysis and Response System) examination of original title complete coverage. 642-545 exam questions help you pass the exam.

Just4Study 642-545 Feature:

* High quality - High quality and valued for the 642-545 Exam: 100% Guarantee to Pass Your 642-545 exam and get your CCSP certification.

* Authoritative - Authoritative braindumps with complete details about 642-545 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed CCSP resources, you will minimize your **Cisco CCSP** cost and be ready to pass your 642-545 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free CCSP demo before you decide to buy it in <http://www.Just4Study.com>.

Just4Study Guarantee:

Just4Study provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the 642-545 exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

Free 642-545 Demo Download

Just4Study offers free demo for CCSP 642-545 exam (Implementing Cisco Security Monitoring, Analysis and Response System). You can check out the interface, question quality and usability of our practice exams before you decide to buy it. We are the only one site can offer demo for almost all products.

The Questions & Answers cover the latest real test and with all the correct answer.we promise the Q&A for **Cisco CCSP 642-545** examination of original title complete coverage.642-545 Questions & Answers help you pass the exam. Otherwise,we will give you a full refund.

VUE/Prometric Code: 642-545

Exam Name: Implementing Cisco Security Monitoring, Analysis and Response System(CCSP)

Questions and Answers: 42 Q&A

[Cisco 642-545](#) Test belongs to one of the CCSP certified test, if needs to obtain the CCSP certificate, you also need to participate in other related test, the details you may visit the [CCSP](#) certified topic, in there, you will see all related CCSP certified subject of examination.

Just4Study professional provide CCSP 642-545 the newest Q&A, completely covers 642-545 test original topic. With our complete CCSP resources, you will minimize your CCSP cost and be ready to pass your 642-545 tests on Your First Try, 100% Money Back Guarantee included!

Just4Study Help You Pass Any IT Exam

[Just4Study.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : Cisco 642-545

Title : Implementing Cisco Security Monitoring, Analysis and Response System

1. At what level of operation does the Cisco Security MARS appliance perform NAT and PAT resolution?

- A. Local (Level 0)
- B. Basic (Level 1)
- C. Intermediate (Level 2)
- D. Advanced (Level 3)
- E. Global (Level 4)

Answer: C

2. What are the two options for handling false-positive events reported by the Cisco Security MARS appliance?

(Choose two.)

- A. archive to NFS only
- B. save as a false-positive report
- C. drop
- D. mitigate at Layer 2
- E. log to the database only
- F. escalate to the Cisco Security MARS administrator

Answer: CE

3. Which attack can be detected by Cisco Security MARS using NetFlow data?

- A. man-in-the middle attack
- B. day-zero attack
- C. spoof attack
- D. Land attack
- E. buffer overflow attack

Answer: B

4. Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely, or by just logging them to the database?

- A. creating system inspection rules using the drop operation
- B. creating drop rules
- C. inactivating the rules
- D. inactivating the events
- E. deleting the false-positive events from the Incidents page
- F. deleting the false-positive events from the Event Management page

Answer: B

5. Which statement is true about the case management feature of Cisco Security MARS?

- A. Cases are created on a global controller, but they can be viewed and modified on a local controller.
- B. The global controller has a Case bar and all cases are selected from the Query/Reports > Cases page.
- C. Cases are created on a local controller, but they can be viewed and modified on a global controller.
- D. The Cases page on a local controller has an additional drop-down filter to display cases per a global controller.

Answer: C

6. Which three statements are true about Cisco Security MARS rules? (Choose three.)

- A. There are three types of rules.
- B. Rules can be saved as reports.
- C. Rules can be deleted.
- D. Rules trigger incidents.
- E. Rules can be defined using a seed file.
- F. Rules can be created using a query.

Answer: ADF

7. Which statement best describes the case management feature of Cisco Security MARS?

- A. It is used to automatically collect and save information on incidents, sessions, queries, and reports dynamically without user interventions.
- B. It is used to capture, combine, and preserve user-selected Cisco Security MARS data within a specialized report.
- C. It is used to very quickly evaluate the state of the network.
- D. It is used in conjunction with the Cisco Security MARS incident escalation feature for incident reporting.

Answer: B

8. What is a supported mitigation feature on the Cisco Security MARS appliance?

- A. generating and pushing configuration commands to Layer 3 devices
- B. generating and pushing configuration commands to Layer 2 devices
- C. automatically dropping all suspected traffic at the nearest IPS appliance
- D. storing and identifying NetFlow data for attack mitigation

Answer: B

9. What is used to publish events to Cisco Security MARS about Cisco IPS signatures that have fired?

- A. SNMP
- B. SSL
- C. HTTPS
- D. SDEE
- E. syslog
- F. Secure FTP

Answer: D

10. Which two configuration options enable the Cisco Security MARS appliance to perform mitigation? (Choose two.)

- A. SNMP RW community string
- B. Cisco Security MARS integration with Cisco Security Manager
- C. Telnet or SSH access type with SNMP RO community
- D. a NetFlow device added in the Cisco Security MARS database
- E. SSL communications with the network devices

Answer: AC

[642-545 Braindumps](#)

[642-515](#) *Securing Networks with ASA Advanced*

[642-545](#) *Implementing Cisco Security Monitoring, Analysis and Response System*

[642-542](#) *Cisco SAFE Implementation Exam*

[642-552](#) *Securing Cisco Network Devices Exam*

[642-513](#) *Securing Hosts Using Cisco Security Agent Exam (HIPS)*

[642-502](#) *Securing Networks with Cisco Routers and Switches Exam (SNRS)*

[642-503](#) *Securing Networks with Cisco Routers and Switches*

[642-523](#) *Securing Networks with PIX and ASA*

[642-522](#) *Securing Networks with PIX and ASA Exam (SNPA)*

[642-521](#) *Cisco Secure PIX Firewall Advanced*

[642-532](#) *Securing Networks Using Intrusion Prevention Systems Exam (IPS)*

[642-551](#) *Securing Cisco Network Devices Exam (SND)*

Other Cisco Exams

[642-072](#) [646-363](#) [642-067](#) [642-381](#) [642-523](#) [642-241](#) [642-432](#) [642-564](#)

[642-972](#) [350-040](#) [642-436](#) [640-553](#) [644-141](#) [646-563](#) [642-979](#) [642-531](#)

[640-802](#) [646-204](#) [646-229](#) [642-873](#)