

642-545 CCSP

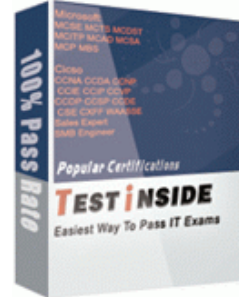
Cisco Implementing Cisco Security Monitoring, Analysis and Response System

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](#))



"Implementing Cisco Security Monitoring, Analysis and Response System", also known as 642-545 exam, is a Cisco certification. With the complete collection of questions and answers, TestInside 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.

Exam : [642-545](#)

Quality and Value for the 642-545 Exam TestInside Practice Exams for Cisco **CCSP** Certification 642-545 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

TestInside provide the professional Q&A.

1. We offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the 642-545 Exam.

642-545 simulation test questions, including the examination question and the answer, complete by our senior IT lecturers and the CCSP product experts, included the current newest 642-545 examination questions.

3. 100% Guarantee to Pass Your CCSP exam and get your CCSP Certification.

If you do not pass the Cisco Certification 642-545 exam (Implementing Cisco Security Monitoring, Analysis and Response System) on your first attempt using our TestInside testing engine and pdf file, we will give you a FULL REFUND of your purchasing fee.

use TestInside 642-545 Q&A ensure you pass the exam at your first try.

TestInside 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!

[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.

TestInside Testing Engine Features

Comprehensive questions and answers about 642-545 exam

642-545 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

642-545 exam questions updated on regular basis

Same type as the certification exams, 642-545 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 642-545 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Cisco 642-545

Title : Implementing Cisco Security Monitoring, Analysis and Response System

1. 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

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 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. 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

[More 642-545 Information](#)

Related 642-545 Exams

[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*

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

642-521 *Cisco Secure PIX Firewall Advanced*

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

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

Other Cisco Exams

<u>350-026</u>	<u>350-020</u>	<u>646-589</u>	<u>642-359</u>	<u>350-018-</u>	<u>642-681</u>	<u>642-353</u>	<u>642-871</u>
				<u>LAB</u>	<u>646-151</u>	<u>642-243</u>	<u>642-072</u>
<u>351-001</u>	<u>642-591</u>	<u>650-251</u>	<u>642-274</u>	<u>640-811</u>	<u>642-978</u>	<u>640-821</u>	<u>640-801</u>
<u>642-654</u>							