642-545

Cisco

Implementing Cisco Security Monitoring, Analysis and Response System

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 642-545 exam in first attempt and also get high scores to acquire Cisco certification.

If you use OfficialCerts 642-545 Certification questions and answers, you will experience actual 642-545 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 642-545 exam. Every point from pass4sure 642-545 PDF, 642-545 review will help you take Cisco 642-545 exam much easier and become Cisco certified.

Here's what you can expect from the OfficialCerts Cisco 642-545 course:

** Up-to-Date Cisco 642-545 questions as experienced in the real exam.*
** 100% correct Cisco 642-545 answers you simply can't find in other 642-545 courses.*
** All of our tests are easy to download. Your file will be saved as a 642-545 PDF.*
** Cisco 642-545 brain dump free content featuring the real 642-545 test questions.*

Cisco 642-545 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 642-545 exam training are an absolute favorite in the industry. You will pass Cisco 642-545 certification test and career opportunities will be open for you.

http://news.ift.org/?newsid=exams.asp?examcode=642-545

Question: 1
The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) is an appliance-based, all-inclusive solution that provides unmatched insight and control of your existing security deployment. Which three items are correct with regard to Cisco Security MARS rules? (Choose three.)

A. There are three types of rules.
B. Rules can be deleted.
C. Rules can be created using a query.
D. Rules trigger incidents.

Answer: A, C, D

Question: 2
Which three benefits are of deploying Cisco Security MARS appliances by use of the global and local controller architecture? (Choose three.)

A. A global controller can provide a summary of all local controllers information (network topologies, incidents, queries, and reports results).
B. A global controller can provide a central point for creating rules and queries, which are applied simultaneously to multiple local controllers.
C. A global controller can correlate events from multiple local controllers to perform global sessionizations.
D. Users can seamlessly navigate to any local controller from the global controller GUI.

Answer: A, B, D

Question: 3
Which item is the best practice to follow while restoring archived data to a Cisco Security MARS appliance?

A. Use Secure FTP to protect the data transfer.
B. Use "mode 5" restore from the Cisco Security MARS CLI to provide enhanced security during the data transfer.
C. Choose Admin > System Maintenance > Data Archiving on the Cisco Security MARS GUI to perform the restore operations on line.
D. To avoid problems, restore only to an identical or higher-end Cisco Security MARS appliance.

Answer: D

Question: 4
A Cisco Security MARS appliance can't access certain devices through the default gateway. Troubleshooting has determined that this is a Cisco Security MARS configuration issue. Which additional Cisco Security MARS configuration will be required to correct this issue?

A. Use the Cisco Security MARS GUI to configure multiple default gateways
B. Use the Cisco Security MARS GUI or CLI to configure multiple default gateways
C. Use the Cisco Security MARS GUI or CLI to enable a dynamic routing protocol
D. Use the Cisco Security MARS CLI to add a static route

Answer: D

Question: 5
Which two options are for handling false-positive events reported by the Cisco Security MARS appliance? (Choose two.)

A. mitigate at Layer 2
B. archive to NFS only
C. drop
D. log to the database only

Answer: C, D

Question: 6
What is the reporting IP address of the device while adding a device to the Cisco Security MARS appliance?

A. The source IP address that sends syslog information to the Cisco Security MARS appliance
B. The pre-NAT IP address of the device
C. The IP address that Cisco Security MARS uses to access the device via SNMP
D. The IP address that Cisco Security MARS uses to access the device via Telnet or SSH

Answer: A

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

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

Answer: B

Question: 8
Which two configuration tasks are needed on the Cisco Security MARS for it to receive syslog messages relayed from a syslog relay server? (Choose two.)

A. Define the syslog relay collector.
B. Add the syslog relay server application to Cisco Security MARS as Generic Syslog Relay Any.
C. Define the syslog relay source list.
D. Add the reporting devices monitored by the syslog relay server to Cisco Security MARS.

Answer: B, D

Question: 9
Here is a question that you need to answer. You can click on the Question button to the left to view the question and click on the MARS GUI Screen button to the left to capture the MARS GUI screen in order to answer the question. While viewing the GUI screen capture, you can view the complete screen by use of the left/right scroll bar on the bottom of the GUI screen. Choose the correct answer from among the options. What actions will you take to configure the MARS appliance to send out an alert when the system rule fires according to the MARS GUI screen shown?

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

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	Google