642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/642-627.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Anomaly detection may send an alert under which two circumstances? (Choose two.)

A. The attacker obfuscates a malicious HTTP request.

B. Inbound traffic arrives from a source with a low reputation score.

C. Outbound traffic is destined towards a known botnet system.

D. A single worm-infected source enters the network and starts scanning for other vulnerable hosts.

E. Benign traffic is misinterpreted as an attack.

F. The network starts becoming congested by worm traffic.

Correct Answer: DF

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/anomaly_detector/v5.0/configuration/guide/Intro.html#wp1046115

The Detector module analyzes the zone traffic, and sends out an alert when a DoS attack is detected. The Detector module can detect attacks and activate protection mechanisms. It is best suited to work alongside with the Cisco Anomaly Guard Module but it can also operate as a separate DDoS detection and alarm component.

QUESTION 2

Threat rating calculation is performed based on which factors?

A. risk rating and adjustment based on the prevention actions taken

B. threat rating and event action overrides

C. event action overrides and event action filters

D. risk rating and target value rating

E. alert severity and alert actions

Correct Answer: A

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

Threat rating is a quantitative measure of your network\\'s threat level after IPS mitigation. The formula for threat rating is:

Threat Rating = Risk Rating - Alert Rating The values of the alert ratings are listed below. ?45: deny-attacker-inline ?40: deny-attacker-victim-pair-inline ?40: deny-attacker-service-pair-inline ?35: deny-connection-inline ?35: deny-packet-inline ?35: modify-packet-inline ?20: request-block-host ?20: request-block-connection ?20: reset-tcp-connection ?20: request-rate-limit

For example, if an alert had a risk rating of 100 and the IPS mitigates the event with a deny- attacker-inlineaction, the

threat rating would be calculated as: Threat Rating = Risk Rating - Alert Rating, or 100 - 45 = 55.

Threat rating brings the value of risk rating to a new level. By taking the IPS mitigation action into account, threat rating helps you further focus on the most important threats that have not been mitigated.

QUESTION 3

You are working with Cisco TAC to troubleshoot a software problem on the Cisco IPS appliance. TAC suspects a fault with the NotificationApp software module in the Cisco IPS appliance. In this case, which Cisco IPS appliance operations may be most affected by the NotificationApp software module fault?

A. SNMP

B. IDM or IME

C. global correlation

D. remote blocking

E. anomaly detection

F. SDEE

Correct Answer: A

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_architecture.ht ml#wp1009053

NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in the Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

QUESTION 4

Which option is best to use to capture only a subset of traffic (capturing traffic per-IP-address, per- protocol, or per-application) off the switch backplane and copy it to the Cisco IPS appliance?

A. SPAN

B. PBR

C. VACL

D. MPF

E. STP

Correct Answer: C

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vacl.html#wp1037197

QUESTION 5

In Cisco IDM, the Configuration > Sensor Setup > SSH > Known Host Keys screen is used for what purpose?

A. to enable the Cisco IPS appliance as a master blocking sensor

B. to enable management hosts to access the Cisco IPS appliance

C. to regenerate the Cisco IPS appliance SSH host key

D. to regenerate the Cisco IPS appliance SSL RSA key pair

E. to enable communications with a blocking device

Correct Answer: E

http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliTasks.html#wp1067312

You must add hosts to the SSH known hosts list so that the sensor can recognize the hosts that it can communicate with through SSH. These hosts are SSH servers that the sensor needs to connect to for upgrades and file copying, and other hosts, such as Cisco routers, PIX Firewalls, and Catalyst switches that the sensor will connect to for blocking.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: