

Cisco.500-275.v2018-03-10.q137

Exam Code:	500-275
Exam Name:	Securing Cisco Networks with Sourcefire FireAMP Endpoints
Certification Provider:	Cisco
Free Question Number:	137
Version:	v2018-03-10
# of views:	778
# of Questions views:	37408
https://www.freecram.net/torrent/Cisco.500-275.v2018-03-10.q137.html	

NEW QUESTION: 1

When you are viewing information about a computer, what is displayed?

- A. the type of antivirus software that is installed
- B. the internal IP address
- C. when the operating system was installed
- D. the console settings

Answer: (SHOW ANSWER)

Explanation/Reference:

fit answer.

NEW QUESTION: 2

Which output method is the fastest for Snort?

- A. database
- B. unified2
- C. binary (tcpdump)
- D. CSV

Answer: (SHOW ANSWER)

NEW QUESTION: 3

When discussing the FireAMP product, which term does the acronym DFC represent?

- A. It is not an acronym that is associated with the FireAMP product.
- B. It means Detected Forensic Cause.
- C. It means Device Flow Correlation.
- D. It means Duplicate File Contents.

Answer: (SHOW ANSWER)

NEW QUESTION: 4

When you are editing an intrusion policy, how do you know that you have changes?

- A. A yellow, triangular icon displays next to the Policy Information option in the navigation panel.
- B. You are prompted to save your changes on every screen refresh.
- C. The Commit Changes button is enabled.
- D. A system message notifies you.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

Which interface type allows for VLAN tagging?

- A. passive
- B. inline
- C. switched
- D. high-availability link

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

Given the rule option byte_jump:4,4,relative, align:, how many bytes are being jumped?

- A. align
- B. relative
- C. 4
- D. cannot be determined

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

Which statement is true regarding malware blocking over HTTP?

- A. HTTP is not a supported protocol for malware blocking.
- B. It can be done in both the download and upload direction.
- C. It can be done only in the download direction.
- D. It can be done only in the upload direction.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 8

Custom whitelists are used for which purpose?

- A. to specify which files to sandbox
- B. to specify which files to alert on
- C. to specify which files to delete
- D. to specify which files to ignore

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 9

Access control policy rules can be configured to block based on the conditions that you specify in each rule. Which behavior block response do you use if you want to deny and reset the connection of HTTP traffic that meets the conditions of the access control rule?

- A. block with reset
- B. block
- C. interactive block
- D. interactive block with reset

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

Where is the File Fetch context menu option available?

- A. from the configuration in the Business Defaults page
- B. anywhere a filename or SHA-256 hash is displayed
- C. only from the Filter Event View page
- D. from the Audit Event page

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

Which statement is true when adding a network to an access control rule?

- A. You can select only source networks.
- B. You must have preconfigured the network as an object.
- C. You cannot include multiple networks or network groups as sources or destinations.
- D. You can select the source and destination networks or network groups.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

File information is sent to the Sourcefire Collective Security Intelligence Cloud using which format?

- A. MD5
- B. SHA-1
- C. filenames
- D. SHA-256

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

exact answer.

NEW QUESTION: 13

Which option is a valid whitelist evaluation value?

- A. violation
- B. not-evaluated
- C. semi-compliant

D. pending

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

Which interface type allows for bypass mode?

A. switched

B. inline

C. grouped

D. routed

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

What is a valid data source for DFC Windows connector policy configuration?

A. Emerging Threats

B. Custom and Sourcefire

C. NIST

D. SANS

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

Remote access to the Defense Center database has which characteristic?

A. Estreamer

B. Postgres

C. read/write

D. read-only

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (**50** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 17

Which feature of the preprocessor configuration pages lets you quickly jump to a list of the rules associated with the preprocessor that you are configuring?

A. the rule group accordion

B. a link below the preprocessor heading

- C. a button next to each preprocessor option that has a corresponding rule
- D. a filter bar

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

Which option is not a characteristic of dashboard widgets or Context Explorer?

- A. Widgets offer users an at-a-glance view of their environment.
- B. Context Explorer can be added as a widget to a dashboard.
- C. Widgets are offered to all users, whereas Context Explorer is limited to a few roles.
- D. Context Explorer is a tool used primarily by analysts looking for trends across varying periods of time.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

Which file is the primary configuration file for keeping rules up to date?

- A. porker.conf
- B. pulledpork.conf
- C. snort.conf
- D. pulled.config

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 20

What does packet sniffing do?

- A. rebuilds datagram streams
- B. transmits datagrams over a wireless network
- C. isolates datagrams into like groups
- D. reads datagrams directly off the wire

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 21

Which syntax correctly expresses a port variable?

- A. ipportvar /HTTP_PORTS: 80,1080,8080
- B. portvar HTTP_PORTS [80,1080,8080]
- C. ports: HTTP_PORTS (80,1080,8080)
- D. var: ports = 80,1080,8080

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

What is a GID?

- A. gradual interrupt detection
- B. general intrusion domain

- C. Gigabit interface definition
- D. Generator ID

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations?

- A. logging to database, SMTP, SNMP, and PCAP
- B. logging to database, SNMP, syslog, and email
- C. logging to database, PCAP, SMS, and SNMP
- D. logging to database, SMS, SMTP, and SNMP

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 24

Which information does the File Trajectory feature show?

- A. the time that the scan was run
- B. the name of the file
- C. the hosts on which the file was seen and points in time where events occurred
- D. the protocol

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

verified answer.

NEW QUESTION: 25

Which information does the rule body contain?

- A. port number
- B. protocol
- C. source IP
- D. specification of which portion of a packet payload to examine

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 26

Which statement about the FTPTelnet preprocessor is true?

- A. It can normalize FTP network traffic.
- B. It can check for correctness of Telnet commands.
- C. It can limit how much server-side traffic to process.
- D. It can reassemble FTP fragments.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

Which command-line argument can you use with Snort to produce a binary output file?

- A. -B
- B. -U
- C. -b
- D. -u

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

Which output is in a lightweight, binary form?

- A. PCAP
- B. SNMP
- C. CSV
- D. unified2

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

The Update Window allows you to perform which action?

- A. identify which hosts need to be updated
- B. email the user to download a new client
- C. update your cloud instance
- D. specify a timeframe when an upgrade can be started and stopped

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

Which option is derived from the discovery component of FireSIGHT technology?

- A. connection event table view
- B. host profile
- C. authentication objects
- D. network profile

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

Context Explorer can be accessed by a subset of user roles. Which predefined user role is not valid for FireSIGHT event access?

- A. Security Analyst
- B. Intrusion Administrator
- C. Security Analyst (Read-Only)
- D. Administrator

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (50 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 32

FireSIGHT recommendations appear in which layer of the Policy Layers page?

- A. FireSIGHT recommendations do not show up as a layer.
- B. Layer Summary
- C. Built-In Layers
- D. User Layers

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 33

When a user initiates a scan, which types of scan are available as options?

- A. none, because user-initiated scans are not allowed
- B. scheduled scan, thorough scan, quick scan, network scan
- C. jiffy scan, overnight scan, scan when available, vulnerability scan
- D. flash scan, custom scan, full scan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 34

When building a platform for a Snort installation, which set of components is a major security concern?

- A. default accounts and settings
- B. URL feed vendors
- C. IP address, mask, and gateway settings
- D. host naming conventions

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

When adding source and destination ports in the Ports tab of the access control policy rule editor, which restriction is in place?

- A. The protocol is restricted to TCP and UDP.
- B. The protocol is restricted to TCP only.
- C. The protocol is restricted to UDP only.
- D. The protocol is restricted to TCP or UDP.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 36

The collection of health modules and their settings is known as which option?

- A. correlation policy
- B. system policy
- C. health policy
- D. appliance policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 37

In a FireAMP Private Cloud installation, which server does an administrator use to manage connector policy and view events?

- A. opadmin.<your domain>.com
- B. cloud.<your domain>.com
- C. aws.<your domain>.com
- D. console.<your domain>.com

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 38

Which event source can have a default workflow configured?

- A. discovery events
- B. user events
- C. connection events
- D. server events

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

Which version of libpcap does DAQ require?

- A. none
- B. 0.9.8 or later
- C. any version
- D. 1.0.0 or later

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

Other than intrusion sensing, which other function set can Snort perform?

- A. packet sniffing and disassembly
- B. packet sniffing and logging
- C. packet logging and alerting
- D. intrusion sensing and packet sniffing

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 41

How do you configure URL filtering?

- A. Create an access control rule and, on the URLs tab, select the URLs or URL categories that are to be blocked or allowed.
- B. Create a variable.
- C. Create a Security Intelligence object that contains the blocked URLs and add the object to the access control policy.
- D. Add blocked URLs to the global blacklist.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 42

Context Explorer can be accessed by a subset of user roles. Which predefined user role is valid for FireSIGHT event access?

- A. Administrator
- B. Intrusion Administrator
- C. Maintenance User
- D. Database Administrator

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

What is the first system that is infected with a particular malware called?

- A. Infector
- B. Source
- C. Carrier
- D. Patient Zero

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Which preprocessor maintains connection state so that attacks that manifest over multiple packets in a session can be detected?

- A. flow tracking module
- B. detection engine
- C. frag3
- D. stream5

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 45

For connector-to-FireAMP Private Cloud communication, which port number is used for lower-overhead communication?

- A. 22

- B. 443
- C. 80
- D. 32137

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

In a FireAMP Private Cloud installation, an administrator uses which server to configure the FireAMP Private Cloud properties?

- A. opadmin.<your domain>.com
- B. console.<your domain>.com
- C. cloud.<your domain>.com
- D. aws.<your domain>.com

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

given answer is applicable.

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (**50** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 47

What is VRT?

- A. Very Reliable Technology
- B. Vulnerability Resolved Testing
- C. Vulnerability Resources and Testing
- D. Vulnerability Research Team

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 48

If a file's SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

- A. Clean
- B. Neutral
- C. Malware
- D. Unavailable

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
agreed with answer.

NEW QUESTION: 49

What does the log_dump output plug-in do?

- A. converts data to CVS format
- B. converts data into a format similar to Snort fast alert mode
- C. converts data into a format similar to Snort ASCII packet dump mode
- D. converts log data to PCAP-formatted output

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

From the Deployment screen, you can deploy agents via which mechanism?

- A. push to client
- B. zip install file
- C. user download from Sourcefire website or email
- D. precompiled RPM package

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
best answer.

NEW QUESTION: 51

Which type of activity is shown in the Device Trajectory page?

- A. file creation
- B. the IP addresses of hosts on which a file was seen
- C. the hosts that are in the same group as the selected host
- D. the activity of the FireAMP console users

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule?

- A. enforcing two-factor authentication for access to critical servers
- B. testing password strength when accessing an application
- C. limiting general user access to administrative file shares
- D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 53

What is the purpose of using a span or monitor port on a switch?

- A. to overcome problems that switches have in accurately reproducing desired traffic
- B. to limit the amount of traffic that passes through the switch
- C. to aggregate traffic from multiple switch ports
- D. to tap data off network media

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 54

The FireAMP connector monitors the system for which type of activity?

- A. vulnerabilities
- B. enforcement of usage policies
- C. file operations
- D. authentication activity

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
appropriate.

NEW QUESTION: 55

Which application can read Barnyard log_pcap output plug-in files?

- A. tcpdump
- B. Snorby
- C. SnortReport
- D. BASE or ACID

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

When Snort receives packets, in which order are they placed into the preprocessors?

- A. flow, frag3, stream5, application preprocessors, detection engine
- B. detection engine, frag3, stream5, flow, application preprocessors
- C. frag3, stream5, application preprocessors, detection engine
- D. flow, stream5, frag3, application preprocessors, detection engine

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 57

A context box opens when you click on an event icon in the Network File Trajectory map for a file. Which option is an element of the box?

- A. File Name
- B. Application Protocol
- C. Scan
- D. Threat Name

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 58

How is the basic construct of a port variable formatted in the Snort.conf file?

- A. portvar value
- B. var arguments
- C. port variable
- D. variable

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 59

Which preprocessor uses a global directive and an engine instance directive in the snort.conf file for configuration to provide target context during packet reassembly?

- A. frag3
- B. SMTP
- C. frag2
- D. sfPortscan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 60

Which action is valid for decoder/preprocessor stub rules?

- A. inspect
- B. file I/O
- C. reject
- D. recurse

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 61

Which of these can you use for two-step authentication?

- A. any RFC 1918 compatible application
- B. a SecurID token
- C. the Apple Authenticator app
- D. the Google Authenticator app

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

Special Discount Code: **freecram**)

NEW QUESTION: 62

Which option transmits policy-based alerts such as SNMP and syslog?

- A. FireSIGHT
- B. the host
- C. the Defense Center
- D. the managed device

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 63

Which option is true of the Packet Information portion of the Packet View screen?

- A. shows you the user that triggered the event
- B. allows you to download a PCAP formatted file of the session that triggered the event
- C. provides a table view of events
- D. displays packet data in a format based on TCP/IP layers

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 64

Where do you configure widget properties?

- A. dashboard properties
- B. the Local Configuration page
- C. the Widget Properties button in the title bar of each widget
- D. Context Explorer

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 65

When configuring an LDAP authentication object, which server type is available?

- A. Oracle
- B. SMTP
- C. Yahoo
- D. Microsoft Active Directory

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

Which hosts merit special consideration for crafting a policy?

- A. none, because all hosts should get equal consideration
- B. domain controllers
- C. end-user hosts
- D. Linux servers

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 67

Which disposition can be returned in response to a malware cloud lookup?

- A. Virus
- B. Dirty
- C. Malware
- D. Infected

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 68

Which protocol operates below the network layer?

- A. UDP
- B. DNS
- C. ICMP
- D. ARP

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

Which question should be in your predeployment checklist?

- A. How often are backup jobs run?
- B. Are any Linux servers being deployed?
- C. Who are the users of the hosts on which you will deploy?
- D. Which applications are installed on the hosts on which you will deploy?

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

exact.

NEW QUESTION: 70

Which IPS placement option is the noisiest?

- A. inside the firewall
- B. inside the DMZ
- C. outside the firewall
- D. inside general user segments

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 71

A default FireAMP Private Cloud installation can accommodate how many connectors over which period of time?

- A. 100 connectors over a 15-day period
- B. 1000 connectors over a 45-day period

- C. 5000 connectors over a 10-day period
- D. 500 connectors over a 30-day period

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
updated answer.

NEW QUESTION: 72

Given the rule option byte_test:1, ,64,2;, what is the offset?

- A. 2
- B. 1
- C. cannot be determined
- D. 64

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 73

What is the minimum action that you should take when configuring a new Snort installation?

- A. Provision more network bandwidth in case your installation causes latency.
- B. Turn on all the rules.
- C. Inform your users that you have deployed an IDS/IPS.
- D. Configure your HOME_NET to include the networks that you want the sensor to protect.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 74

Which option is true regarding the \$HOME_NET variable?

- A. is a policy-level variable
- B. is used by all rules to define the internal network
- C. defines the network the active policy protects
- D. has a default value of "all"

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 75

A user discovery agent can be installed on which platform?

- A. RADIUS
- B. Ubuntu
- C. OpenLDAP
- D. Windows

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 76

Which statement is true concerning static NAT?

- A. Static NAT supports only TCP traffic.

- B. Static NAT is normally deployed for outbound traffic only.
- C. Static NAT provides a many-to-one mapping between IP addresses.
- D. Static NAT provides a one-to-one mapping between IP addresses.

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (50 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 77

An IPS addresses evasion by implementing countermeasures. What is one such countermeasure?

- A. send packets to the origination host of a given communication session, to confirm or eliminate spoofing
- B. perform pattern and signature analysis against the entire packet, rather than against individual fragments
- C. automate scans of suspicious source IP addresses
- D. periodically reset statistical buckets to zero for memory utilization, maximization, and performance

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 78

Which tool can you use to query the history.db file?

- A. Curl
- B. SQLite
- C. FireAMP_Helper.vbs
- D. cscript

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 79

Which item examines packets for malformation, anomalies, and protocol compliance and gathers and presents packets in one consistent fashion?

- A. output and alerting module
- B. preprocessors
- C. detection engine
- D. Sniffer

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 80

What does protocol normalization do?

- A. removes any protocol-induced or protocol-allowable ambiguities
- B. compares evaluated packets to normal, daily network-traffic patterns
- C. removes application layer data, whether or not it carries protocol-induced anomalies, so that packet headers can be inspected more accurately for signs of abuse
- D. compares a packet to related traffic from the same session, to determine whether the packet is out of sequence

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 81

Which keyword can you use to check a packet IP header TTL value?

- A. ttl
- B. byte_test
- C. tos
- D. ipopts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 82

Which area is created between screening devices in an egress/ingress path for housing web, mail, or DNS servers?

- A. EMZ
- B. harbor
- C. DMZ
- D. inlet

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 83

Which statement is true about the Device Trajectory feature?

- A. It shows hosts that display Indications of Compromise.
- B. A "plus" sign on the File Trajectory map indicates that you can execute the file inside FireAMP.
- C. It shows where the endpoint devices have moved in your environment by displaying each IP address that a device has had over time.
- D. In the File Trajectory map, you can view the parent process for a file by selecting the infected system.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 84

The Accounts menu contains items that are related to FireAMP console accounts. Which menu allows you to set the default group policy?

- A. Users
- B. Applications
- C. Audit Log
- D. Business

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 85

In a FireAMP Private Cloud installation, deployed connectors communicate with which server?

- A. opadmin.<your domain>.com
- B. console.<your domain>.com
- C. cloud.<your domain>.com
- D. aws.<your domain>.com

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

right answer.

NEW QUESTION: 86

Which option represents a configuration step on first use?

- A. Verify, Contain, and Protect
- B. User Account Setup
- C. Event Filtering
- D. System Defaults Configuration

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 87

What do policies enable you to do?

- A. specify a custom whitelist
- B. specify group membership
- C. specify hosts to include in reports
- D. specify which events to view

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

given answer is fine.

NEW QUESTION: 88

Which character must a rule body end with?

- A. parenthesis
- B. period
- C. semicolon

D. exclamation mark

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 89

How many days' worth of data do the widgets on the dashboard page display?

- A. the previous 6 days of data
- B. the number of days you set in the dashboard configuration
- C. the previous 7 days of data
- D. the previous 5 days of data

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 90

Which option describes a requirement for using Remote File Fetch?

- A. It must be done from a private cloud console.
- B. The administrator must have two-step authentication enabled.
- C. It can be done only over port 32137.
- D. The feature is integrated into the product, so no specific requirements must be fulfilled.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 91

The gateway VPN feature supports which deployment types?

- A. PPTP and MPLS
- B. SSL and HTTPS
- C. client and route-based
- D. point-to-point, star, and mesh

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (50 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 92

Which statement describes an advantage of cloud-based detection?

- A. Limited customization allows for faster detection.
- B. Fewer resources are required on the endpoint.
- C. Sandboxing reduces the overall management overhead of the system.

D. High-speed analytical engines on the endpoint limit the amount of work the cloud must perform.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
fantastic answer.

NEW QUESTION: 93

Advanced custom signatures are written using which type of syntax?

- A. Snort signatures
- B. Firewall signatures
- C. ClamAV signatures
- D. bash shell

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
rightful.

NEW QUESTION: 94

Stacking allows a primary device to utilize which resources of secondary devices?

- A. interfaces, CPUs, memory, and storage
- B. interfaces and storage
- C. CPUs and memory
- D. interfaces, CPUs, and memory

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 95

Which statement describes the meaning of a red health status icon?

- A. A critical threshold has been exceeded.
- B. A health policy has been disabled on a monitored device.
- C. A warning threshold has been exceeded.
- D. At least one health module has failed.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

Controlling simultaneous connections is a feature of which type of preprocessor?

- A. TCP and network layer preprocessors
- B. detection enhancement
- C. rate-based attack prevention
- D. performance settings

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 97

The FireAMP connector supports which proxy type?

- A. SOCKS5_filename
- B. SOCKS6
- C. SOCKS7
- D. HTTP_proxy

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 98

What are the two categories of variables that you can configure in Object Management?

- A. Policy-Specific Variables and Procedural Variables
- B. System Default Variables and Procedural Variables
- C. System Default Variables and FireSIGHT-Specific Variables
- D. Default Variables and Custom Variables

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 99

Which option is true when configuring an access control rule?

- A. You can use geolocation criteria to specify source and destination IP addresses by country but not by continent.
- B. You can use geolocation criteria to specify source IP addresses by country and continent, as well as destination IP addresses by country and continent.
- C. You can use geolocation criteria to specify source and destination IP addresses by continent but not by country.
- D. You can use geolocation criteria to specify destination IP addresses by country but not source IP addresses.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 100

Which keyword can you use to try to close a session when an alert is triggered?

- A. resp
- B. react
- C. logto
- D. tag

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 101

Which preprocessor provides a means to measure Snort performance?

- A. stream5
- B. stats
- C. flow
- D. performance statistics

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 102

Where does an administrator go to get a copy of a fetched file?

- A. the Business Defaults page
- B. the File menu, followed by Downloads
- C. the File Repository
- D. the Search selection in the Analysis menu

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
exact.

NEW QUESTION: 103

Which option is used to implement suppression in the Rule Management user interface?

- A. Source
- B. Global
- C. Protocol
- D. Rule Category

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 104

What does the whitelist attribute value "not evaluated" indicate?

- A. The host is not a target of the whitelist.
- B. The host could not be evaluated because no profile exists for it.
- C. The whitelist status could not be updated because the correlation policy it belongs to is not enabled.
- D. The host is not on a monitored network segment.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 105

The IP address ::/0 is equivalent to which IPv4 address and netmask?

- A. The IP address ::/0 is not valid IPv6 syntax.
- B. 0.0.0.0/24
- C. 0.0.0.0/0
- D. 0.0.0.0

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 106

To execute a command in Linux while in the directory where it is located, and be sure you are only running that particular copy, what would you use in front of the executable name?

- A. ./

B. ../

C. .\

D. ..\

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (50 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 107

To accept input from Snort and produce various forms of output, the Barnyard architecture consists of which components?

- A. data processors and reassemblers
- B. data processors and output plug-ins
- C. preprocessors and reassemblers
- D. preprocessors and detection engine

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 108

What must you do to produce ASCII-formatted output from Snort?

- A. Use the -K ascii switch when you start Snort from the command line.
- B. Compile Snort with the -K ascii flag in the configure command.
- C. Do nothing because Snort produces ASCII output by default.
- D. Use a third-party application to convert native Snort output to ASCII.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 109

Alert priority is established in which way?

- A. event classification
- B. host criticality selection
- C. through Context Explorer
- D. priority.conf file

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 110

FireSIGHT uses three primary types of detection to understand the environment in which it is deployed. Which option is one of the detection types?

- A. devices
- B. objects
- C. protocol layer
- D. application

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 111

Which statement about two-step authentication is true?

- A. It is the ability to use two separate passwords.
- B. It is the ability to enable biometric authentication.
- C. It is the ability to have a passphrase sent to a mobile device.
- D. It is the ability to use a verification code in conjunction with the correct username and password.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:
authentic.

NEW QUESTION: 112

When you instruct Snort to place ASCII-formatted log data in a specific directory, what does Snort use to organize the alert data?

- A. port number
- B. IP address
- C. interface
- D. packet

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 113

Which FireAMP capability can tell you how malware has spread in a network?

- A. File Analysis
- B. Threat Root Cause
- C. File Trajectory
- D. Heat Map

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 114

Which action can you take from the Detections/Quarantine screen?

- A. Create a policy.
- B. Restore the detected file.
- C. Run a report.

D. Change computer group membership.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

corrected.

NEW QUESTION: 115

Which statement about the distribution of SO rules is true?

- A. SO rules ship with the regular Snort distribution.
- B. SO rules ship as a separate download.
- C. SO rules ship with the regular rules download.
- D. SO rules are not distributed because you need to build your own rules.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 116

Which management and analysis tool can you use to enhance a Snort installation?

- A. Nmap
- B. PulledPork
- C. tcpdump
- D. Wireshark

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 117

Which action should you perform to enable or disable entire classes of rules through the snort.conf file?

- A. Specify the -e or :-d command-line argument.
- B. Specify the enable or the disable argument.
- C. Build and reference a separate rules-configuration file.
- D. Comment or uncomment the rule class.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 118

Which statement about the detection engine configuration settings in snort.conf is true?

- A. All the decoder settings are off by default.
- B. The decoder is no longer in use.
- C. All the decoder alerts are on by default.
- D. Some decoder settings are on and others must be uncommented.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 119

Which set of actions would you take to create a simple custom detection?

- A. Add a SHA-256 value; upload a file to calculate a SHA-256 value; upload a text file that contains SHA-256 values.
- B. Upload a packet capture; use a Snort rule; use a ClamAV rule.
- C. Manually input the PE header data, the MD-5 hash, and a list of MD-5 hashes.
- D. Input the file and file name.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

100% fit answer.

NEW QUESTION: 120

Which statement regarding user exemptions is true?

- A. Exempt users have a browser session timeout restriction of 24 hours.
- B. By default, all users cannot be exempt from any browser session timeout value.
- C. Non-administrators can be made exempt on an individual basis.
- D. Administrators can be exempt from any browser session timeout value.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 121

Which option is a remediation module that comes with the Sourcefire System?

- A. Nmap Route Scan
- B. Syslog Route
- C. Response Group
- D. Cisco IOS Null Route

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (**50** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 122

The FireAMP Mobile endpoint connector currently supports which mobile OS device?

- A. Firefox
- B. HTML5
- C. Android
- D. iPhone

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 123

If Snort is installed and the sensor, database, and web server all reside on the same machine, to which ports should remote access of the sensor be restricted?

- A. 22 and 443
- B. 23 and 80
- C. 80 and 443
- D. 443 and 3306

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 124

How can customers feed new intelligence such as files and hashes to FireAMP?

- A. from the connector
- B. by uploading it to the FTP server
- C. by sending it via email
- D. through the management console

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 125

Which configuration is optimal for the frag3 engine?

- A. Keep the configuration as simple as possible, for better performance.
- B. Bind target IP addresses to policies that represent operating systems, so that the IPS engine can process traffic the same way that target hosts do.
- C. Deploy the engine only in passive mode, for better performance.
- D. Bind client IP addresses to policies that represent operating systems, so that clients can process traffic the same way that the IPS engine does.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 126

In the IP addressing scheme of your organization, each subnet consists of 4096 hosts, and the beginning of the addressing scheme is 172.16.0.0. Your remote office is allocated the range of addresses from the first subnet. What are the CIDR notation, network address, broadcast address, and valid IP address in your assigned range?

- A. 172.16.0.0/24, 172.16.0.0, 172.16.8.255, 172.16.0.51
- B. 172.16.0.0/12, 172.16.0.0, 172.16.64.255, 172.16.52.112
- C. 172.16.0.0/20, 172.16.0.0, 172.16.15.255, 172.16.8.252
- D. 172.16.0.0/16, 172.16.0.0, 172.16.32.255, 172.16.22.4

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 127

Which statement about implementing DAQ is true?

- A. You must obtain it from Sourceforge.
- B. It is a shell script that works on any Linux platform.
- C. It must be compiled separately.
- D. It is not open source.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 128

Which option describes the two basic components of Sourcefire Snort rules?

- A. a rule header to define source, destination, and protocol, and the output configuration to determine which form of output to produce if the rule triggers
- B. preprocessor configurations to define what to do with packets before the detection engine sees them, and detection engine configurations to define exactly how alerting is to take place
- C. a rule statement characterized by the message you configure to appear in the alert, and the rule body that contains all of the matching criteria such as source, destination, and protocol
- D. a rule body that contains packet-matching criteria or options to define where to look for content in a packet, and a rule header to define matching criteria based on where a packet originates, where it is going, and over which protocol

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 129

Which option is a detection technology that is used by FireAMP?

- A. fuzzy matching
- B. Norton AntiVirus
- C. network scans
- D. Exterminator

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

great answer.

NEW QUESTION: 130

Which pair represents equivalent processes whose names differ, depending on the connector version that you are running?

- A. TETRA and SPERO
- B. ETHOS and SPERO
- C. immunet_protect and iptray
- D. agent.exe and sfc.exe

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 131

Which component is one of the four primary components of Snort?

- A. postprocessor
- B. iptables
- C. ACL
- D. output and alerting

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 132

Which preprocessor can normalize the IIS %u encoding scheme?

- A. ftp_telnet
- B. SMTP
- C. http_inspect
- D. sfPortscan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 133

How does application blocking enhance security?

- A. It identifies and logs usage.
- B. It tracks application abuse.
- C. It deletes identified applications.
- D. It blocks vulnerable applications from running, until they are patched.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

good answer.

NEW QUESTION: 134

Which preprocessor plays a role in detecting the reconnaissance phase of an attack?

- A. sfPortscan
- B. frag3
- C. rpc_decode
- D. telnet_decode

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 135

Which file defines Snort IDs and associated alert labels that are not provided within the unified output format?

- A. snort-id.msg
- B. sid-msg.map
- C. snort-id.tab
- D. sid-id.conf

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 136

In addition to the discovery of new hosts, FireSIGHT can also perform which function?

- A. route traffic
- B. block traffic
- C. discover information about users
- D. determine which users are involved in monitored connections

Answer: ([SHOW ANSWER](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (**50** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 137

Which engine or module presents alert and log data in the format that you specify?

- A. tap
- B. detection
- C. sniffing
- D. output

Answer: D ([LEAVE A REPLY](#))

Valid 500-275 Dumps shared by EduDump.com for Helping Passing 500-275 Exam!
EduDump.com now offer the **newest 500-275 exam dumps**, the EduDump.com 500-275 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 500-275 dumps with Test Engine here:

<https://www.edudump.com/exams/Cisco/500-275/premium/> (**50** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)