

# 500-275<sup>Q&As</sup>

Securing Cisco Networks with Sourcefire FireAMP Endpoints (SSFAMP)

# Pass Cisco 500-275 Exam with 100% Guarantee

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

https://www.leads4pass.com/500-275.html

100% Passing Guarantee 100% Money Back Assurance

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

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers





# **QUESTION 1**

Which c	ption is	a dete	ection	technology	that is	s used	by	FireAMP <sup>4</sup>	?

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

Correct Answer: A

# **QUESTION 2**

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

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

Correct Answer: D

# **QUESTION 3**

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

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

Correct Answer: C

# **QUESTION 4**

Which statement describes an advantage of cloud-based detection?

- A. Limited customization allows for faster detection.
- B. Fewer resources are required on the endpoint.

Leads4Pass https://www.leads4pass.com/500-275.html
2024 Latest leads4pass 500-275 PDF and VCE dumps Download

- 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.

Correct Answer: B

# **QUESTION 5**

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

Correct Answer: C

# **QUESTION 6**

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

- A. Vulnerabilities
- B. Enforcement of usage policies
- C. File operations
- D. Authentication activity

Correct Answer: C

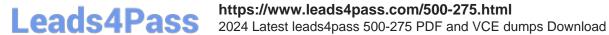
# **QUESTION 7**

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.

Correct Answer: D

# **QUESTION 8**



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

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

Correct Answer: B

# **QUESTION 9**

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

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

Correct Answer: C

# **QUESTION 10**

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

- A. SANS
- B. NIST
- C. Emerging Threats
- D. Custom and Sourcefire

Correct Answer: D

500-275 PDF Dumps

500-275 Study Guide

500-275 Exam Questions