250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

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

https://www.leads4pass.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

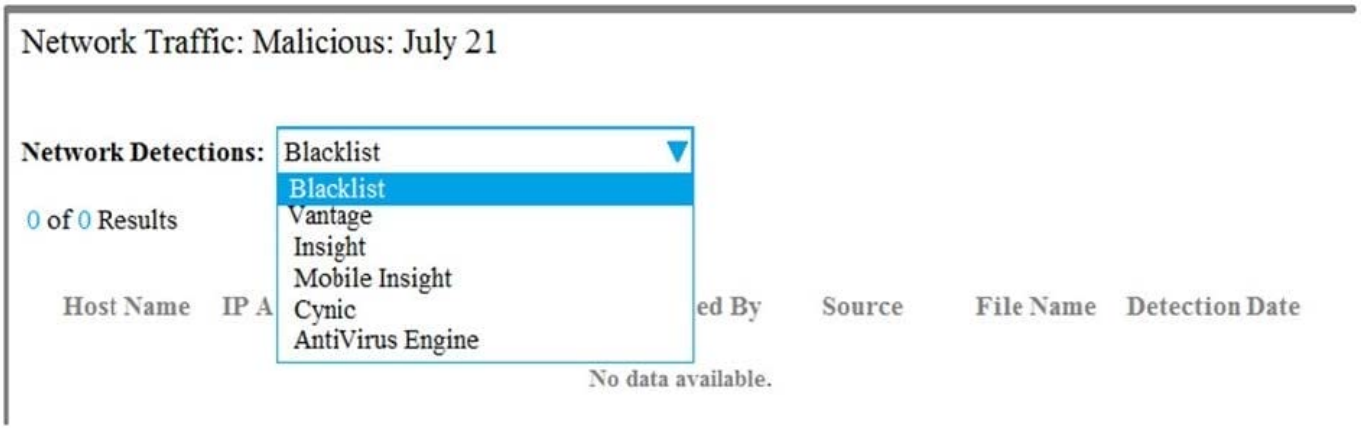
Following Questions and Answers are all new published by Symantec Official Exam Center

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

QUESTION 1

Refer to the exhibit. An Incident Responder wants to see what was detected on a specific day by the IPS engine.

Which item must the responder choose from the drop-down menu?



A. Insight

B. Cynic

C. Vantage

D. Blacklist

Correct Answer: A

QUESTION 2

An Incident Responder observes an incident with multiple malware downloads from a malicious domain. The domain in question belongs to one of the organization\\'s suppliers. The organization needs access to the site to continue placing orders. ATP: Network is configured in Inline Block mode.

How should the Incident Responder proceed?

A. Whitelist the domain and close the incident as a false positive

B. Identify the pieces of malware and blacklist them, then notify the supplier

C. Blacklist the domain and IP of the attacking site

D. Notify the supplier and block the site on the external firewall

Correct Answer: D

QUESTION 3

Which threat is an example of an Advanced Persistent Threat (APT)?

A. Koobface

B. Brain

C. Flamer

D. Creeper

Correct Answer: C

QUESTION 4

Which service is the minimum prerequisite needed if a customer wants to purchase ATP: Email?

A. Email Protect (antivirus and anti-spam)

B. Email Safeguard (antivirus, anti-spam, encryption, data protection and image control)

C. Symantec Messaging Gateway

D. Skeptic

Correct Answer: A

Reference: http://www.ingrammicrocloud.nl/wp-content/uploads/sites/44/2016/06/Email-Security.cloudPricing-Licensing-Guide.pdf

QUESTION 5

Which two non-Symantec methods for restricting traffic are available to the Incident Response team? (Choose two.)

A. Temporarily disconnect the local network from the internet.

B. Create an Access Control List at the router to deny traffic.

C. Analyze traffic using Wireshark protocol analyzer to identify the source of the infection.

D. Create a DNS sinkhole server to block malicious traffic.

E. Isolate computers so they are NOT compromised by infected computers.

Correct Answer: CD

QUESTION 6

Which threat is an example of an Advanced Persistent Threat (APT)?

A. ILOVEYOU

B. Conficker

C. MyDoom

D. GhostNet

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/white_papers/badvanced_persistent_threats_WP_21215957.en-us.pdf

QUESTION 7

What occurs when an endpoint fails its Host Integrity check and is unable to remediate?

A. The endpoint automatically switches to using a Compliance location, where a Compliance policy is applied to the computer.

B. The endpoint automatically switches to using a System Lockdown location, where a System Lockdown policy is applied to the computer.

C. The endpoint automatically switches to using a Host Integrity location, where a Host Integrity policy is applied to the computer.

D. The endpoint automatically switches to using a Quarantine location, where a Quarantine policy is applied to the computer.

Correct Answer: D

QUESTION 8

In which two locations should an Incident Responder gather data for an After Actions Report in ATP? (Choose two.)

A. Policies page

B. Action Manager

C. Syslog

D. Incident Manager

E. Indicators of compromise (IOC) search

Correct Answer: CD

QUESTION 9

What are two policy requirements for using the Isolate and Rejoin features in ATP? (Choose two.)

A. Add a Quarantine firewall policy for non-compliant and non-remediated computers.

B. Add a Quarantine LiveUpdate policy for non-compliant and non-remediated computers.

C. Add and assign an Application and Device Control policy in the Symantec Endpoint Protection Manager (SEPM).

D. Add and assign a Host Integrity policy in the Symantec Endpoint Protection Manager (SEPM).

E. Add a Quarantine Antivirus and Antispyware policy for non-compliant and non-remediated computers.

Correct Answer: AD

Reference: https://support.symantec.com/en_US/article.HOWTO128427.html

QUESTION 10

An organization is considering an ATP: Endpoint and Network deployment with multiple appliances. Which form factor will be the most effective in terms of performance and costs?

A. Virtual for management, physical for the network scanners and ATP: Endpoint

B. Physical for management and ATP: Endpoint, virtual for the network scanners

C. Virtual for management and ATP: Endpoint, physical for the network scanners

D. Virtual for management, ATP: Endpoint, and the network scanners

Correct Answer: B

QUESTION 11

Which two questions can an Incident Responder answer when analyzing an incident in ATP? (Choose two.)

A. Does the organization need to do a healthcheck in the environment?

B. Are certain endpoints being repeatedly attacked?

C. Is the organization being attacked by this external entity repeatedly?

D. Do ports need to be blocked or opened on the firewall?

E. Does a risk assessment need to happen in the environment?

Correct Answer: BE

QUESTION 12

How can an Incident Responder generate events for a site that was identified as malicious but has NOT triggered any events or incidents in ATP?

A. Assign a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

B. Run an indicators of compromise (IOC) search in ATP manager.

C. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that blocks traffic to the domain.

D. Add the site to a blacklist in ATP manager.

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO126023.html

QUESTION 13

A large company has 150,000 endpoints with 12 SEP sites across the globe. The company now wants to implement ATP: Endpoint to improve their security. However, a consultant recently explained that the company needs to implement more than one ATP manager.

Why does the company need more than one ATP manager?

A. An ATP manager can only connect to a SQL backend

B. An ATP manager can only support 30,000 SEP clients

C. An ATP manager can only support 10 SEP site connections.

D. An ATP manager needs to be installed at each location where a Symantec Endpoint Protection Manager (SEPM) is located.

Correct Answer: D

QUESTION 14

An Incident Responder has noticed that for the last month, the same endpoints have been involved with malicious traffic every few days. The network team also identified a large amount of bandwidth being used over P2P protocol.

Which two steps should the Incident Responder take to restrict the endpoints while maintaining normal use of the systems? (Choose two.)

A. Report the users to their manager for unauthorized usage of company resources

B. Blacklist the domains and IP associated with the malicious traffic

C. Isolate the endpoints

D. Blacklist the endpoints

E. Find and blacklist the P2P client application

Correct Answer: CE

QUESTION 15

Which section of the ATP console should an ATP Administrator use to evaluate prioritized threats within the

environment?

A. Search

B. Action Manager

C. Incident Manager

D. Events

Correct Answer: B