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

An ATP Administrator has deployed ATP: Network, Endpoint, and Email and now wants to ensure that all connections are properly secured.

Which connections should the administrator secure with signed SSL certificates?

A. ATP and the Symantec Endpoint Protection Manager (SEPM) ATP and SEP clients Web access to the GUI

B. ATP and the Symantec Endpoint Protection Manager (SEPM) ATP and SEP clients ATP and Email Security.cloud Web access to the GUI

C. ATP and the Symantec Endpoint Protection Manager (SEPM)

D. ATP and the Symantec Endpoint Protection Manager (SEPM) Web access to the GUI

Correct Answer: C

QUESTION 2

What is the role of Insight within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Detonation/sandbox

C. Network detection component

D. Event correlation

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/brochures/atp-brochure-en.pdf

QUESTION 3

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

A. Zeus

B. Melissa

C. Duqu

D. Code Red

Correct Answer: C

QUESTION 4

An organization has five (5) shops with a few endpoints and a large warehouse where 98% of all computers are located. The shops are connected to the warehouse using leased lines and access internet through the warehouse network.

How should the organization deploy the network scanners to observe all inbound and outbound traffic based on Symantec best practices for Inline mode?

A. Deploy a virtual network scanner at each shop

B. Deploy a virtual network scanner at the warehouse and a virtual network scanner at each shop

C. Deploy a physical network scanner at each shop

D. Deploy a physical network scanner at the warehouse gateway

Correct Answer: D

QUESTION 5

Which two ATP control points are able to report events that are detected using Vantage? Enter the two control point names:

A. ATP: network ATP: Endpoint

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO126027.html

QUESTION 6

Where can an Incident Responder view Cynic results in ATP?

A. Events

B. Dashboard

C. File Details

D. Incident Details

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO128417.html

QUESTION 7

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B

QUESTION 8

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 9

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 10

Which two tasks should an Incident Responder complete when recovering from an incident? (Choose two.)

A. Rejoin healthy endpoints back to the network

B. Blacklist any suspicious files found in the environment

C. Submit any suspicious files to Cynic

D. Isolate infected endpoints to a quarantine network

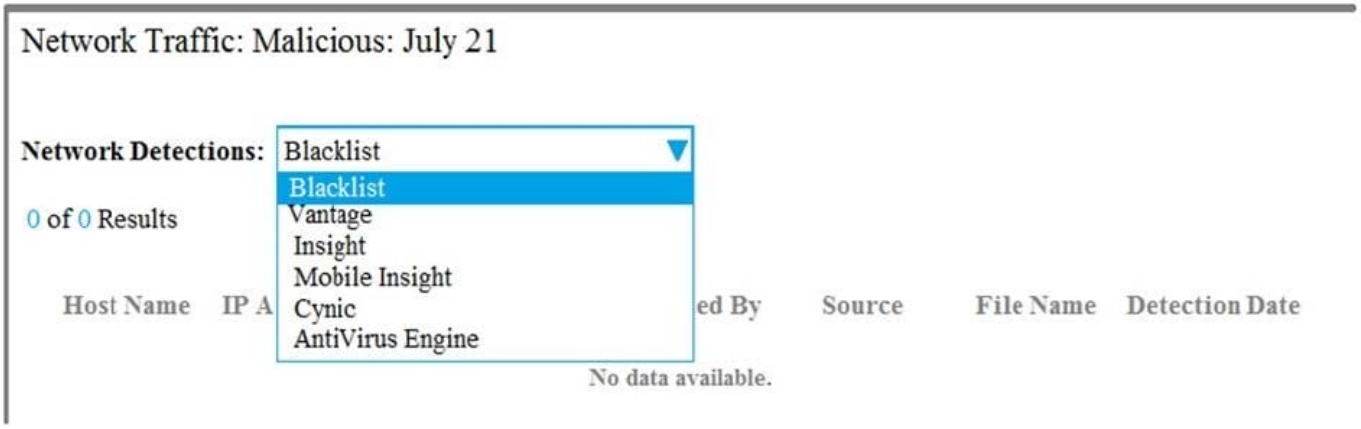
E. Delete threat artifacts from the environment

Correct Answer: BE

QUESTION 11

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 12

A medium-sized organization with 10,000 users at Site A and 20,000 users at Site B wants to use ATP: Network to scan internet traffic at both sites.

Which physical appliances should the organization use to act as a network scanner at each site while using the fewest appliances and assuming typical network usage?

A. Site A 8840 x4 ?Site B 8880 x2

B. Site A 8880 x2 ?Site B 8840 x1

C. Site A 8880 x1 ?Site B 8840 x6

D. Site A 8880 x1 ?Site B 8880 x2

Correct Answer: D

QUESTION 13

An ATP administrator is setting up correlation with Email Security.cloud.

What is the minimum Email Security.cloud account privilege required?

A. Standard User Role - Report

B. Standard User Role - Service

C. Standard User Role - Support

D. Standard User Role - Full Access

Correct Answer: B

QUESTION 14

Which Advanced Threat Protection (ATP) component best isolates an infected computer from the network?

A. ATP: Email

B. ATP: Endpoint

C. ATP: Network

D. ATP: Roaming

Correct Answer: B

Reference: https://www.symantec.com/products/advanced-threat-protection

QUESTION 15

Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security.cloud

B. Web security.cloud

C. Skeptic

D. Symantec Messaging Gateway

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-detection-andresponse-atp-endpoint-en.pdf

Latest 250-441 Dumps | 250-441 Practice Test | 250-441 Study Guide