Vendor: Symantec

Exam Code:250-441

Exam Name: Administration of Symantec Advanced Threat Protection 3.0

Version: Demo

QUESTION 1

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

A. Network detection component

B. Event correlation

C. Reputation-based security

D. Detonation/sandbox

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO119277.html

---

QUESTION 2

An Incident Responder wants to investigate whether msscrt.pdf resides on any systems. Which search query and type should the responder run?

A. Database search filename "msscrt.pdf"

B. Database search msscrt.pdf

C. Endpoint search filename like msscrt.pdf

D. Endpoint search filename ="msscrt.pdf"

Correct Answer: A

QUESTION 3

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 4

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 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

Which action should an Incident Responder take to remediate false positives, according to Symantec best practices?

A. Blacklist

B. Whitelist

C. Delete file

D. Submit file to Cynic

Correct Answer: B

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10899/en_US/satp_security_ops_guide_3.0.5.pdf?__gda__=1541987119_a3559016c9355c98c2ec53278a8df2a0 (119)

QUESTION 7

In which scenario should an Incident Responder manually submit a file to the Cynic portal?

A. There is a file on a USB that an Incident Responder wants to analyze in a sandbox.

B. An Incident Responder is unable to remember the password to the .zip archive.

C. The file has generated multiple incidents in the ATP manager and an Incident Responder wants to blacklist the file.

D. The file is a legitimate application and an Incident Responder wants to report it to Symantec as a false positive.

Correct Answer: D

Reference: https://support.symantec.com/content/unifiedweb/en_US/article.HOWTO124806.html

---

QUESTION 8

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

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B

QUESTION 9

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 10

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

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-advanced-threat-protectionemail-DS-21349610.pdf

---

QUESTION 11

Which default port does ATP use to communicate with the Symantec Endpoint Protection Manager (SEPM) web services?

A. 8446

B. 8081

C. 8014

D. 1433

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO81103.html

---

QUESTION 12

An Incident Responder wants to use a STIX file to run an indicators of compromise (IOC) search. Which format must the administrator use for the file?

A. .csv

B. .xml

C. .mht

D. .html

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.howto125534.html