250-441$^{\text{Q\&As}}$

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.pass2lead.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which two widgets can an Incident Responder use to isolate breached endpoints from the Incident details page? (Choose two.)

A. Affected Endpoints

B. Dashboard

C. Incident Graph

D. Events View

E. Actions Bar

Correct Answer: CE

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 (114)

QUESTION 2

Which National Institute of Standards and Technology (NIST) cybersecurity function includes Risk Assessment or Risk Management Strategy?

A. Recover

B. Protect

C. Respond

D. Identify

Correct Answer: D

Reference: https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION 3

How does an attacker use a zero-day vulnerability during the Incursion phase?

A. To perform a SQL injection on an internal server

B. To extract sensitive information from the target

C. To perform network discovery on the target

D. To deliver malicious code that breaches the target

Correct Answer: D

Reference: https://www.symantec.com/connect/blogs/guide-zero-day-exploits

QUESTION 4

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

A. Loyphish

B. Aurora

C. ZeroAccess

D. Michelangelo

Correct Answer: B

QUESTION 5

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

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.info5060.html

QUESTION 6

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 7

Which two database attributes are needed to create a Microsoft SQL SEP database connection? (Choose two.)

A. Database version

B. Database IP address

C. Database domain name

D. Database hostname

E. Database name

Correct Answer: BD

QUESTION 8

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 9

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 10

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 11

What is the minimum amount of RAM required for a virtual deployment of the ATP Manager in a production environment?

A. 48 GB

B. 64 GB

C. 16 GB

D. 32GB

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO126029.html

QUESTION 12

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 13

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 14

Which policies are required for the quarantine feature of ATP to work?

A. Firewall Policy and Host Integrity Policy

B. Quarantine Policy and Firewall Policy

C. Host Integrity Policy and Quarantine Policy

D. Quarantine and Intrusion Prevention Policy

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.tech248959.html

QUESTION 15

An Incident Responder wants to run a database search that will list all client named starting with SYM. Which syntax should the responder use?

A. hostname like "SYM"

B. hostname "SYM"

C. hostname "SYM*"

D. hostname like "SYM*"

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO124805.html

Latest 250-441 Dumps   250-441 VCE Dumps   250-441 Exam Questions