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

Administration of Symantec Advanced Threat Protection 3.0

QUESTION 1

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 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

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 4

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as "finding incursions"?

A. Protect

B. Identify

C. Respond

D. Detect

Correct Answer: B

QUESTION 5

What is the main constraint an ATP Administrator should consider when choosing a network scanner model?

A. Throughput

B. Bandwidth

C. Link speed

D. Number of users

Correct Answer: B