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

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

QUESTION 1

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Correct Answer: A

QUESTION 2

Which two actions an Incident Responder take when downloading files from the ATP file store? (Choose two.)

A. Analyze suspicious code with Cynic

B. Email the files to Symantec Technical Support

C. Double-click to open the files

D. Diagnose the files as a threat based on the file names

E. Submit the files to Security Response

Correct Answer: AC

QUESTION 3

An Incident Responder has reviewed a STIX report and now wants to ensure that their systems have NOT been compromised by any of the reported threats.

Which two objects in the STIX report will ATP search against? (Choose two.)

A. SHA-256 hash

B. MD5 hash

C. MAC address

D. SHA-1 hash

E. Registry entry

Correct Answer: AB

Reference: https://support.symantec.com/en_US/article.HOWTO124779.html

QUESTION 4

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 5

An Incident Responder is going to run an indicators of compromise (IOC) search on the endpoints and wants to use operators in the expression.

Which tokens accept one or more of the available operators when building an expression?

A. All tokens

B. Domainname, Filename, and Filehash

C. Filename, Filehash, and Registry

D. Domainname and Filename only

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.HOWTO125969.html#v115770112