250-561$^{Q\&As}$

Endpoint Security Complete - Administration R1

Pass Symantec 250-561 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/250-561.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which framework, open and available to any administrator, is utilized to categorize adversarial tactics and for each phase of a cyber attack?

A. MITRE RESPONSE

B. MITRE ATTandCK

C. MITRE ADVandNCE

D. MITRE ATTACK MATRIX

Correct Answer: C

QUESTION 2

The ICDm has generated a blacklist task due to malicious traffic detection. Which SES component was utilized to make that detection?

A. Antimalware

B. Reputation

C. Firewall

D. IPS

Correct Answer: A

QUESTION 3

Which term or expression is utilized when adversaries leverage existing tools in the environment?

A. opportunistic attack

B. script kiddies

C. living off the land

D. file-less attack

Correct Answer: B

QUESTION 4

In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?

A. Exfiltration

B. Discovery

C. Execution

D. Defense Evasion

Correct Answer: D

QUESTION 5

What is the frequency of feature updates with SES and the Integrated Cyber Defense Manager (ICDm)

A. Monthly

B. Weekly

C. Quarterly

D. Bi-monthly

Correct Answer: B