Cisco

Exam 700-270

NGFW Express for Account Managers (NGFWEAM)

Verson: Demo

[Total Questions: 10]

Question No : 1

Which two options are objectives that are defined as part of the "before" stage of the attack continuum? {Choose two.)

A. harden
B. retrospection
C. enforce
D. detect
E. shun

Answer: A,C

Question No : 2

Which method of discovery is used during impact assessment?

A. passive
B. statistical analysis
C. inline
D. heuristic analysis

Answer: C

Question No : 3

Detection of an exploit kit that is installed on a device is an example of which IoC event category?

A. firewall
B. malware
C. security intelligence
D. IPS

Answer: D

Question No : 4

Which two guidelines are important when showing proof of value using Cisco dCloud? (Choose two.)

A. Have demonstration screens open and prepopulated with data
B. Prepare primary customer takeaways
C. Ensure that the correct software versions are installed on demonstration equipment.
D. Ensure that the customer has Cisco SIO cloud access.
E. Install FireSIGHT Management Center on a demonstration workstation

Answer: A,B

Question No : 5

Which subscription license terms are available for FirePOWER services features?

A. 1 and 2 years
B. 1 and 3 years
C. 1 and 5 years
D. 1, 2, and 3 years

Answer: B

Question No : 6

Which three features are considered next-generation firewall capabilities? (Choose three)

A. external intelligence to enhance controls
B. application visibility and control
C. NAT
D. identity-based controls
E. VPN
F. RFC-based inspection

Answer: B,C,E

Question No : 7

Which option is an attribute of a day-zero attack?

A. It can be mitigated with content inspection that is based on static rulesets
B. It can be prevented through RFC application-level compliance checks.
C. It consists of a set of known threat vectors
D. It can be mitigated through the external intelligence and contextual awareness

Answer: D

Question No : 8

What are two challenges that are faced by traditional defense-in-depth security solutions? (Choose two.)

A. Applying security policy is generally by manual and static methods
B. They require that all components be provided by a single vendor
C. Large amounts of logged data lead to poor threat visibility.
D. They mandate network change control
E. Security services must be outsourced.

Answer: B,C

Question No : 9

Which AMP feature provides continuous analysis capabilities?

A. retrospection
B. file reputation
C. file analysis
D. sandboxing

Answer: A

Question No : 10

What are the two requirements for conducting a customer on-site evaluation? (Choose two.)

A. FirePOWER services module deployed in monitor-only mode
B. access to Cisco dCloud
C. FirePOWER services module deployed in inline mode
D. switch with a SPAN port
E. switch with SVI in the same subnet as the adaptive security appliance

Answer: A,B