

Palo Alto Networks

PCCSA Exam

Palo Alto Networks Certified Cybersecurity Associate Exam

**Questions & Answers
Demo**

Version: 9.0

Question: 1

Which type of adversary would commit cybercrimes with the authorization of their country's government?

- A. state-sponsored
- B. hacktivist
- C. gray hat
- D. white hat

Answer: A

Question: 2

When a company chooses to deploy a branch location with antivirus software, which risk model are they using to manage risk?

- A. limiting
- B. assuming
- C. transferring
- D. avoiding

Answer: A

Question: 3

Which option describes a characteristic of a distributed denial-of-service attack?

- A. uses multiple types of malware to corrupt system services
- B. uses a single remote host to delete data from multiple target servers
- C. uses a single remote host to flood a target network with traffic
- D. uses a botnet to flood traffic to a target network

Answer: D

Question: 4

DRAG DROP

Match the Palo Alto Networks Wild Fire analysis verdict with its definition.

Benign	Drag answer here	malicious in the intent and can pose a security threat
Grayware	Drag answer here	does not pose a direct security threat
Malware	Drag answer here	does not exhibit a malicious behavior

Answer:

Benign – does not exhibit a malicious behavior

Grayware – does not pose a direct security threat

Malware – malicious in the intent and can pose a security threat

Reference:

<https://docs.paloaltonetworks.com/wildfire/8-0/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts>

Question: 5

From which resource can a Palo Alto Networks firewall get URL category information for URLs whose categories cannot be found on the firewall?

- A. App-ID database
- B. WildFire
- C. PDF file
- D. PAN-DB database

Answer: D
