# Free Questions for PCCET by go4braindumps

## Shared by Hines on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type:** **MultipleChoice**

Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

## Options:

**A-** Statistical-based

**B-** Knowledge-based

**C-** Behavior-based

**D-** Anomaly-based

## Answer:

B

## Explanation:

A knowledge-based system uses a database of known vulnerabilities and attack profiles

to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.

A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.

These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

## Question 2

**Question Type:** **MultipleChoice**

Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

### Options:

**A-** endpoint antivirus software

**B-** strong endpoint passwords

**C-** endpoint disk encryption

**D-** endpoint NIC ACLs

## Answer:

A

## Explanation:

Endpoint antivirus software is a type of software designed to help detect, prevent, and eliminate malware on devices, such as laptops, desktops, smartphones, and tablets. Endpoint antivirus software can block viruses that are not seen and blocked by the perimeter firewall, which is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. Perimeter firewall can block some known viruses, but it may not be able to detect and stop new or unknown viruses that use advanced techniques to evade detection.Endpoint antivirus software can provide an additional layer of protection by scanning the files and processes on the devices and using various methods, such as signatures, heuristics, behavior analysis, and cloud-based analysis, to identify and remove malicious code123.Reference:

What Is Endpoint Antivirus? Key Features & Solutions Explained - Trellix

Microsoft Defender for Endpoint | Microsoft Security

Download ESET Endpoint Antivirus | ESET

# Question 3

**Question Type:** **MultipleChoice**

What are three benefits of SD-WAN infrastructure? (Choose three.)

## Options:

**A-** Improving performance of SaaS applications by requiring all traffic to be back-hauled through the corporate headquarters network

**B-** Promoting simplicity through the utilization of a centralized management structure

**C-** Utilizing zero-touch provisioning for automated deployments

**D-** Leveraging remote site routing technical support by relying on MPLS

**E-** Improving performance by allowing efficient access to cloud-based resources without requiring back-haul traffic to a centralized location

## Answer:

B, C, E

### Explanation:

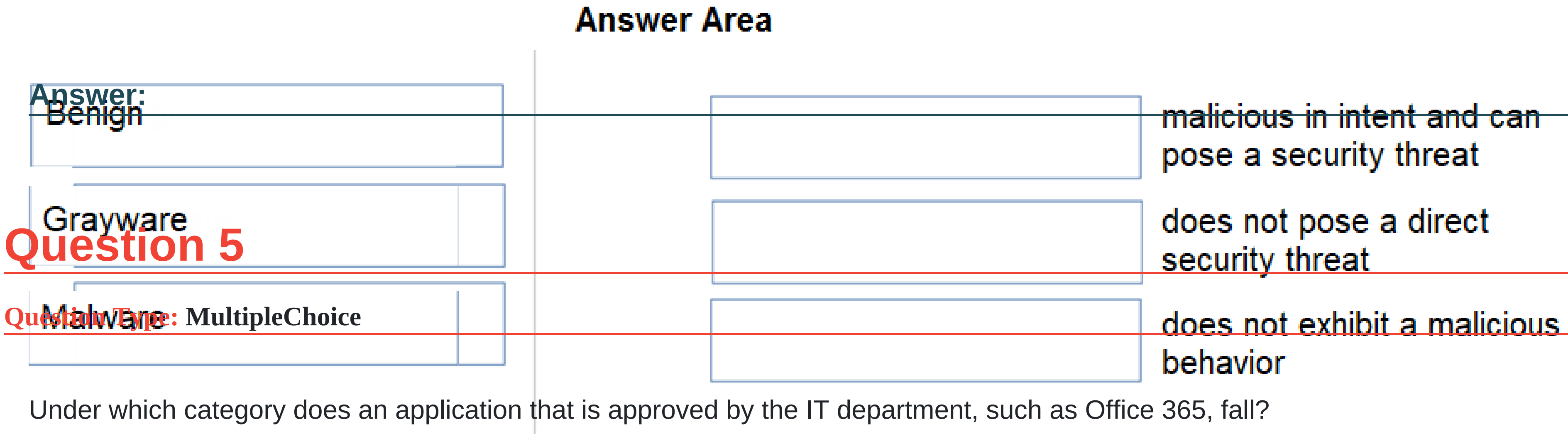
Simplicity: Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites. Improved performance: By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.

## Question 4

**Question Type: DragDrop**

Match the Palo Alto Networks WildFire analysis verdict with its definition.

## Answer:



Answer Area

Benign

Grayware

Malware

malicious in intent and can pose a security threat

does not pose a direct security threat

does not exhibit a malicious behavior

## Question 5

**Question Type:** MultipleChoice

Under which category does an application that is approved by the IT department, such as Office 365, fall?

## Options:

**A-** unsanctioned

**B-** prohibited

**C-** tolerated

**D-** sanctioned

## Answer:

D

### Explanation:

A sanctioned application is an application that is approved by the IT department and meets the security and compliance requirements of the organization. Sanctioned applications are allowed to access the organization's network and data and are monitored and protected by the IT department. Examples of sanctioned applications are Office 365, Salesforce, and Zoom. Sanctioned applications are different from unsanctioned, prohibited, and tolerated applications, which are not approved by the IT department and may pose security risks to the organization. Unsanctioned applications are applications that are used by the employees without the IT department's knowledge or consent, such as Dropbox, Gmail, or Facebook. Prohibited applications are applications that are explicitly forbidden by the IT department, such as BitTorrent, Tor, or malware. Tolerated applications are applications that are not approved by the IT department, but are not blocked or restricted, such as Skype, Spotify, or YouTube.Reference:Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET),Cloud Security Fundamentals - Module 4: Cloud Security Best Practices,Application Visibility and Control

## Question 6

**Question Type:** **MultipleChoice**

What is used to orchestrate, coordinate, and control clusters of containers?

### Options:

**A-** Kubernetes

**B-** Prisma Saas

**C-** Docker

**D-** CN-Series

## Answer:

A

## Explanation:

As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale.

https://www.dynatrace.com/news/blog/kubernetes-vs-docker/

20%
DISCOUNT