PCCET$^{Q\&As}$

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Pass Palo Alto Networks PCCET Exam with 100% Guarantee

QUESTION 1

Which type of IDS/IPS uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt?

A. Knowledge-based

B. Signature-based

C. Behavior-based

D. Database-based

Correct Answer: C

IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems: 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

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

A. Threat Prevention

B. DNS Security

C. WildFire

D. URL Filtering

Correct Answer: D

The URL Filtering service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

QUESTION 3

What is the key to "taking down" a botnet?

A. prevent bots from communicating with the C2

B. install openvas software on endpoints

C. use LDAP as a directory service

D. block Docker engine software on endpoints

Correct Answer: A

QUESTION 4

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

A. People

B. Accessibility

C. Processes

D. Understanding

E. Business

Correct Answer: ACE

The six pillars include:

1.

Business (goals and outcomes)

2.

People (who will perform the work)

3.

Interfaces (external functions to help achieve goals)

4.

Visibility (information needed to accomplish goals)

5.

Technology (capabilities needed to provide visibility and enable people)

6.

Processes (tactical steps required to execute on goals) All elements must tie back to the business itself and the goals of the security operations

QUESTION 5

Which endpoint product from Palo Alto Networks can help with SOC visibility?

A. STIX

B. Cortex XDR

C. WildFire

D. AutoFocus

Correct Answer: B

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today\\'s increasingly sophisticated threats. With XDR, cybersecurity teams can: Identify hidden, stealthy, and sophisticated threats proactively and quickly Track threats across any source or location within the organization Increase the productivity of the people operating the technology Get more out of their security investments Conclude investigations more efficiently