KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **SecOps Generalist**

Title : Palo Alto Networks Network Security Generalist

Version : DEMO

1.Which of the following are the primary roles available in Cortex XDR? (Choose two)
A. Administrator
B. Incident Responder
C. Threat Hunter
D. Data Analyst
Answer: A, B
Explanation:
Cortex XDR includes role-based access control, where Administrators manage configurations and Incident Responders handle threat detection and response. Threat Hunters and Data Analysts are functionalities rather than predefined roles.

2.What is the primary function of log ingestion in Cortex XDR?
A. To store endpoint backup files
B. To enable real-time and historical threat analysis
C. To automate firewall rule creation
D. To encrypt user traffic
Answer: B
Explanation:
Cortex XDR ingests logs from multiple sources, allowing analysts to correlate, analyze, and detect threats across endpoints, network, and cloud environments. This enables real-time and historical investigations for security teams.

3.Which log type in Cortex XDR provides insights into endpoint process execution?
A. Firewall logs
B. Agent logs
C. Authentication logs
D. Network traffic logs
Answer: B
Explanation:
Agent logs track system processes, application behavior, and user activity on endpoints. These logs help identify suspicious activities like malware execution, privilege escalation, or anomalous behaviors.

4.Which feature of Cortex XDR ensures compliance with data protection regulations?
A. Data Retention Policies
B. Automated Firewall Updates
C. DNS Sinkholing
D. Virtual Private Network (VPN) Integration
Answer: A
Explanation:
Data Retention Policies define how long logs and alerts are stored before deletion, ensuring compliance with GDPR, HIPAA, and SOC 2 by managing data lifecycle and protecting sensitive information.

5.Which of the following methods improve log management efficiency in Cortex XDR? (Choose two)
A. Filtering logs based on event severity

B. Deleting logs older than 24 hours
C. Using Cortex Data Lake for long-term storage
D. Preventing log correlation to reduce noise
Answer: A, C
Explanation:
Filtering logs ensures that analysts focus on critical threats, while Cortex Data Lake enables long-term storage and analysis. Deleting logs too soon or avoiding correlation reduces detection capabilities.