ExamsIndex
Practice Materials & Tests

DEMO VERSION

Palo Alto Networks

XDR-Analyst Exam

Palo Alto Networks XDR Analyst

Exam Latest Version: 6.0

Question 1. (Single Select)

Which syntax snippet will correctly extract the user_name field from the alerts dataset?

A: dataset = alerts | select user_name
B: xdr_data.alerts | filter user_name == "*"
C: dataset = xdr_data.alerts | fields user_name
D: select xdr_data.alerts where user_name=*

Correct Answer: C

Question 2. (Multi Select)

When designing a prevention profile, which options can be enforced? (Choose three)

A: Blocking credential theft
B: Monitoring ransomware activity
C: Alert-only for fileless attacks
D: Bypassing proxy logs

Correct Answer: A, B, C

Question 3. (Single Select)

What is included in an incident overview tab?

A: XQL schema
B: Alert stitching visualization

C: Agent uninstallation options
D: Endpoint BIOS info

Correct Answer: B

Question 4. (Single Select)

Match the incident component to its function:

Component

A) Causality Chain

B) Alert Summary

C) Timeline

D) Related Endpoints

Function

1. Shows how related processes are connected

2. Overview of incident-contributing alerts

3. Chronological view of alert activity

4. Hosts involved in the incident

A: A–1, B–2, C–3, D–4
B: A–4, B–2, C–3, D–1
C: A–1, B–3, C–2, D–4
D: A–2, B–1, C–3, D–4

Correct Answer: A

Question 5. (Single Select)

Match each query option to its function:

each query

A) Pre-defined Query Builder

B) Query Library

C) Scheduled Query

D) Manual Query

function

1. Guided query creation

2. Saved and reusable query bank

3. Periodic automatic query execution

4. Direct ad-hoc query without assistance

A: A-1, B-2, C-3, D-4
B: A-4, B-2, C-3, D-1
C: A-1, B-3, C-2, D-4
D: A-1, B-4, C-3, D-2

Correct Answer: A

ExamsIndex

Demo PDF Complete

Your XDR-Analyst Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 50% off, use Coupon Code: OCT50

https://examsindex.com/exam/xdr-analyst