

Palo Alto Networks SecOps-Architect

Palo Alto Networks Security Operations Architect

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/secops-architect>

Latest Version: 6.0

Question: 1

Which TWO risks should be considered before enabling automated containment?
(Choose 2)

- A. Dashboard background preferences for analysts
- B. Browser compatibility across regional SOC teams
- C. Potential disruption to legitimate business services
- D. Accuracy and confidence level of triggering detection
- E. Number of executive report templates available

Answer: C,D

Question: 2

A cloud identity source provides valuable authentication events but requires custom field mapping. Which onboarding approach is MOST appropriate?

- A. Use ingestion methods that support mapping and normalization
- B. Exclude the source because field mapping is required
- C. Store events without parsing to reduce configuration effort
- D. Route events only to dashboards without normalization

Answer: A

Question: 3

An organization wants to provide external auditors with limited access to Cortex XSIAM reporting data while preventing access to investigative content. Which approach BEST satisfies this requirement?

- A. Assign administrator privileges and monitor activity regularly
- B. Create role-based access controls with restricted permissions
- C. Provide shared analyst accounts with reporting access enabled
- D. Disable audit reports and export data through email requests

Answer: B

Question: 4

Which factor is MOST important when selecting between direct ingestion and pipeline-mediated ingestion?

- A. Need for filtering, routing, transformation, or enrichment
- B. Analyst preference for report layout and dashboard themes
- C. Number of executive users viewing monthly SOC metrics
- D. Browser configuration settings used by regional SOC teams

Answer: A

Question: 5

Which TWO business considerations commonly influence access-control design?
(Choose 2)

- A. Regulatory and compliance obligations
- B. Separation of duties requirements
- C. Desktop operating system preferences
- D. Dashboard theme customization needs
- E. Browser bookmark organization standards

Answer: A,B

Question: 6

A company needs separate development and production Cortex environments for testing detection content before release. Which design approach BEST supports this requirement?

- A. Test all detection content directly in production tenants
- B. Use separate development and production tenant structures
- C. Share one unrestricted tenant for all development work
- D. Disable production detections during development testing

Answer: B

Question: 7

What is the PRIMARY benefit of using a development tenant for detection engineering?

- A. Replace production telemetry with synthetic reports
- B. Remove all change-control requirements from production
- C. Increase dashboard quantity across analyst workspaces
- D. Test detection logic safely before production deployment

Answer: D

Question: 8

Which TWO objectives are commonly achieved through data pipeline filtering?
(Choose 2)

- A. Reduction of unnecessary telemetry volume
- B. Increased dashboard customization options
- C. Improved efficiency of downstream processing
- D. Elimination of retention policy requirements
- E. Removal of access-control governance obligations

Answer: A,C

Question: 9

An organization wants automation to adapt investigation steps based on incident context rather than follow a fixed sequence every time. Which capability BEST supports this requirement?

- A. Dashboard filters configured for executive reporting
- B. Static playbooks with no conditional decision branches
- C. Agentic automation guided by contextual incident information
- D. Manual analyst notes stored outside Cortex XSIAM

Answer: C

Question: 10

What is the PRIMARY purpose of detection use-case prioritization?

- A. Focus engineering effort on highest-risk and highest-value threats
- B. Increase dashboard quantity across all analyst workspaces
- C. Eliminate the need for telemetry quality validation
- D. Replace SOC reporting requirements with automation

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>