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 : **XSIAM Engineer**

Title : Palo Alto Networks XSIAM Engineer

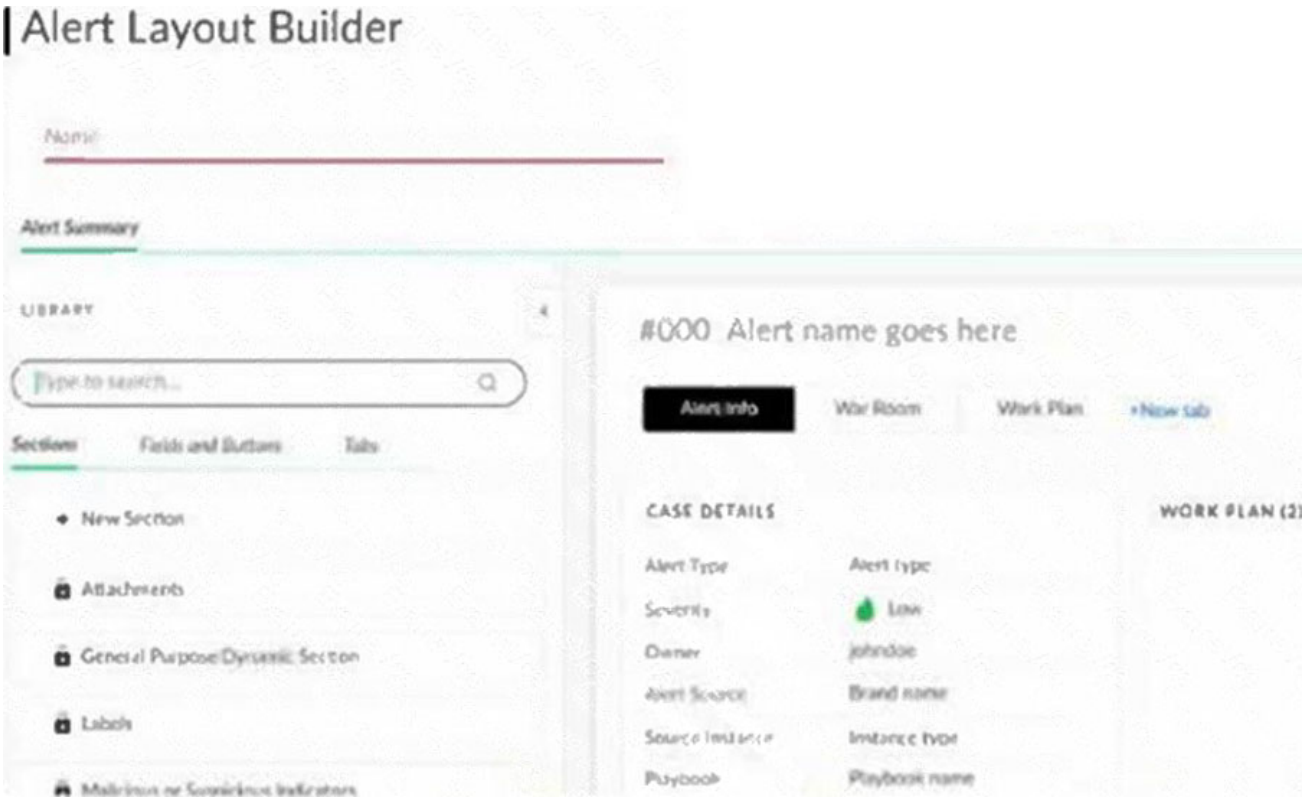
Version : DEMO

1.Which types of content may be included in a Marketplace content pack?
A. Integrations, playbooks, parsers, and server configuration keys
B. Predefined dashboards, indicators, and reports
C. Scripts, playbooks, integrations, and correlation rules
D. Behavioral indicator of compromise (BIOC) rules, layouts, and custom dashboards
Answer: C
Explanation:
A Marketplace content pack in Cortex XSIAM can include scripts, playbooks, integrations, and correlation rules. These packaged content items extend platform functionality, automate workflows, and enhance detection and response capabilities.

2.When a Cortex XSIAM playbook execution reaches a breakpoint on a non-manual task, which two actions will allow the playbook to continue? (Choose two.)
A. Disable the breakpoint and rerun the playbook from the start.
B. Skip the task with the breakpoint to let the playbook proceed automatically.
C. Wait for all parallel tasks to be completed before the breakpoint task resumes automatically.
D. Click Run Script Now or Complete Manually.
Answer: B D
Explanation:
When a playbook execution reaches a breakpoint on a non-manual task, you can skip the task with the breakpoint to allow the playbook to continue, or manually trigger continuation using "Run Script Now" or "Complete Manually". These actions resume execution without restarting the entire playbook.

3.During a new Cortex XSIAM deployment, a user consistently experiences timeout sessions while trying to connect to the agent through Live Terminal, even though the firewall engineer has confirmed that all source IP addresses, port 443, and destinations are allowed.
What could be causing these persistent timeout issues?
A. User does not have administrative privileges on the managed endpoint.
B. SSL Decryption is currently being used to inspect the underlying traffic.
C. NTP is not synchronized with the server time.
D. Live Terminal feature is not supported on the current OS.
Answer: B
Explanation:
Persistent timeout issues with Cortex XSIAM Live Terminal, despite firewall rules being open, are often caused by SSL Decryption inspecting the traffic. Live Terminal relies on secure, end-to-end TLS communication, and decryption breaks this channel, leading to session failures.

4.Based on the image below, which statement applies to the ability to remove tabs when creating a new alert layout?



A. Only "Alert Info" tab can be removed.
B. Only "Alert Info" and "War Room" tabs can be removed.
C. Only "War Room" and "Work Plan" tabs can be removed.
D. Only "Work Plan" tab can be removed.
Answer: C
Explanation:
In Cortex XSIAM's Alert Layout Builder, the "War Room" and "Work Plan" tabs are optional and can be removed, while the "Alert Info" tab is mandatory and cannot be deleted. This ensures that essential alert details are always retained, while collaboration and workflow tabs can be customized.

5.What is the function of the "MODEL" section when creating a data model rule?
A. To make a list of all the relevant fields to be mapped from the logs to XDM
B. To define the mapping between a single dataset and XDM
C. To finalize rule definition with all XQL statements
D. To map log fields to corresponding Cortex XSIAM Data Model (XDM) fields
Answer: D
Explanation:
The MODEL section in a data model rule is used to map log fields to the corresponding Cortex XSIAM Data Model (XDM) fields. This ensures that ingested data aligns with XDM, enabling consistent analytics, detections, and queries across different data sources.