Visual XSIAM-Analyst Cert Exam, Valid Braindumps XSIAM-Analyst Sheet

P.S. Free & New XSIAM-Analyst dumps are available on Google Drive shared by PDFBraindumps: https://drive.google.com/open?id=1s8WmK8R5iQDaBOav3iQcw8ZLX70D9ukl

This certification gives us more opportunities. Compared with your colleagues around you, with the help of our XSIAM-Analyst preparation questions, you will also be able to have more efficient work performance. Our XSIAM-Analyst study materials can bring you so many benefits because they have the following features. I hope you can use a cup of coffee to learn about our XSIAM-Analyst training engine. Perhaps this is the beginning of your change.

Palo Alto Networks XSIAM-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Incident Handling and Response: This section of the exam measures the skills of Incident Response Analysts and covers managing the complete lifecycle of incidents. It involves explaining the incident creation process, reviewing and investigating evidence through forensics and identity threat detection, analyzing and responding to security events, and applying automated responses. The section also focuses on interpreting incident context data, differentiating between alert grouping and data stitching, and hunting for potential IOCs.
Topic 2	• Threat Intelligence Management and ASM: This section of the exam measures the skills of Threat Intelligence Analysts and focuses on handling and analyzing threat indicators and attack surface management (ASM). It includes importing and managing indicators, validating reputations and verdicts, creating prevention and detection rules, and monitoring asset inventories. Candidates are expected to use the Attack Surface Threat Response Center to identify and remediate threats effectively.
Topic 3	• Automation and Playbooks: This section of the exam measures the skills of SOAR Engineers and focuses on leveraging automation within XSIAM. It includes using playbooks for automated incident response, identifying playbook components like tasks, sub-playbooks, and error handling, and understanding the purpose of the playground environment for testing and debugging automated workflows.

>> Visual XSIAM-Analyst Cert Exam <<

Latest Visual XSIAM-Analyst Cert Exam & Latest updated Valid Braindumps XSIAM-Analyst Sheet & Trustable XSIAM-Analyst Exam Dumps

Do you want to get the XSIAM-Analyst learning materials as fast as possible? If you do, we can do this for you. We will give you XSIAM-Analyst exam dumps downloading link and password within ten minutes after buying. If you don't receive the XSIAM-Analyst learning materials, please contact us, and we will solve it for you. Besides, the XSIAM-Analyst Learning Materials is updated according to the exam centre, if we have the updated version, our system will send the latest one to you for one year for free. If you have any other question, just contact us.

Palo Alto Networks XSIAM Analyst Sample Questions (Q138-Q143):

NEW QUESTION # 138
What is the purpose of data stitching in Cortex XSIAM?
Response:

- A. Backing up datasets
- B. Disabling correlation
- C. Encrypting alert payloads
- D. Combining alert metadata across sources

Answer: D

NEW QUESTION # 139
Two security analysts are collaborating on complex but similar incidents. The first analyst merges the two incidents into one for easier management. The other analyst immediately discovers that the custom incident field values relevant to the investigation are missing. How can the team retrieve the missing details?

- A. Examine the incident context of the source incident
- B. Unmerge the incidents to capture the missing details.
- C. Check the timeline view of the incident
- D. Check the War Room of the destination incident

Answer: B

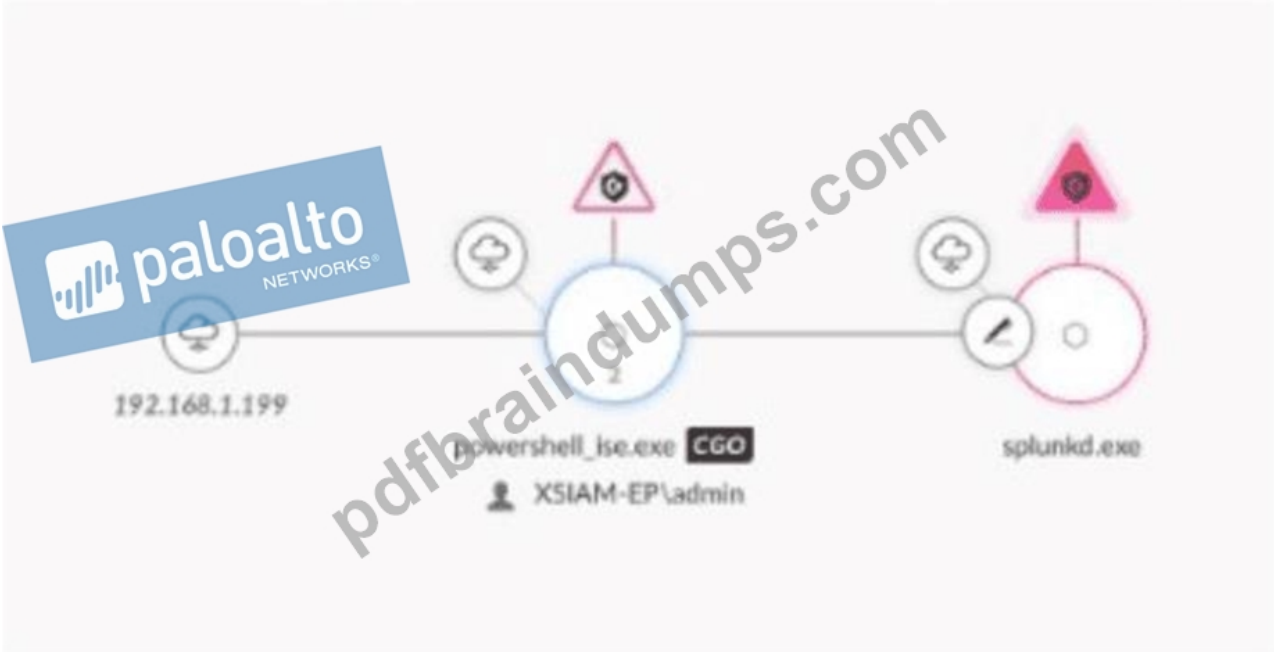
Explanation:
The correct answer isB - Unmerge the incidents to capture the missing details.
When incidents are merged in Cortex XSIAM, custom field values from the source (secondary) incident are not always automatically transferred to the destination (primary) incident. The recommended way to retrieve the missing custom incident field values is tounmergethe incidents. This action restores the original incidents, including all their individual fields and context, allowing analysts to access and capture the missing details.
"If incident field values are missing after a merge, unmerging incidents will restore the original context and custom field data from each incident." Document Reference:XSIAM Analyst ILT Lab Guide.pdf Page:Page 45 (Incident Handling section)

NEW QUESTION # 140
You notice certain threat types are under-prioritized. What two customizations can address this?
Response:

- A. Adjust scoring weights by alert name
- B. Reconfigure BIOC severity
- C. Tag alerts as "Suppressed"
- D. Add alert field conditions in scoring policy

Answer: A,D

NEW QUESTION # 141
Based on the image below, which two additional steps should a SOC analyst take to secure the endpoint?
(Choose two.)



- A. Isolate the affected workstation.
- B. Reboot the machine.
- C. Live Terminal into the workstation to verify.
- D. Block 192.168.1.199.

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct answers areC - Block 192.168.1.199andD - Isolate the affected workstation.
* Block 192.168.1.199:The image shows that the suspicious or malicious activity originated from this source IP address, making it a potential threat actor or compromised system on the network. Blocking this IP helps prevent further communication or lateral movement from the suspected attacker.
* Isolate the affected workstation:Since suspicious activities (like powershell_ise.exe running as an admin and launching splunkd.exe) are detected, isolating the workstation is a critical containment measure. This action disconnects the endpoint from the network, stopping any ongoing attack, lateral movement, or command-and-control activity, while allowing for forensic investigation.
"Isolating an endpoint and blocking the source IP address are best practices for immediate containment in the event of detected compromise or suspicious activity." Document Reference:XSIAM Analyst ILT Lab Guide.pdf Page:Page 40 (Incident Handling section)

NEW QUESTION # 142
Which configuration will ensure any alert involving a specific critical asset will always receive a score of 100?

- A. A user scoring rule for the critical asset
- B. An asset as critical in Asset Inventory
- C. SmartScore to apply the specific score to the critical asset
- D. A risk scoring policy for the critical asset

Answer: D

Explanation:
The correct answer isD, a risk scoring policy for the critical asset.
In Cortex XSIAM, to consistently apply a high score (e.g., 100) to any alert involving a particular asset, analysts should define and apply a risk scoring policy. Such policies allow organizations to specifically customize and enforce a scoring framework to reflect the

critical nature of certain assets, ensuring they are always prioritized during incident response activities.
* Asset criticality alone (option A) doesn't automatically assign a static high score to every alert.
* SmartScore (option B) is AI-driven and dynamic; it cannot guarantee a fixed, always-maximized score.
* User scoring rules (option C) target user entities, not specifically the assets themselves.
"Risk scoring policies are explicitly defined to consistently assign specific scores to incidents or alerts involving critical assets, ensuring prioritized visibility in the incident queue."

NEW QUESTION # 143
.....

In the face of fierce competition, you should understand the importance of time. You must walk in front of the competitors. If you have more strength, you will get more opportunities. Your dream life can really become a reality! XSIAM-Analyst learning materials are here, right to choose! And you will find that you will get benefited from XSIAM-Analyst Exam Braindumps far beyond you can image. Not only you can get more professional knowledge but also you can get the XSIAM-Analyst certification to find a better career.