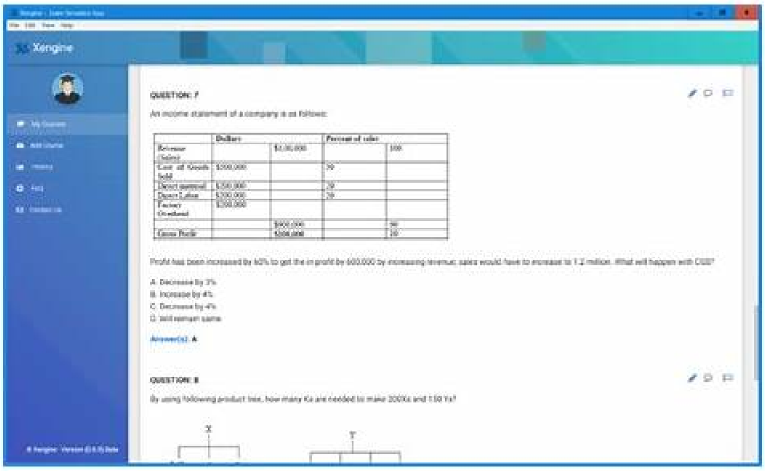
Exam XSIAM-Engineer Questions, Dumps XSIAM-Engineer Reviews



QUESTION: 7

An income statement of a company is as follows:

	Dollars		Percent of sales	
Revenue (Sales)		$2,00,000		100
Cost of Goods Sold	$500,000		50	
Direct material	$250,000		25	
Direct Labor	$200,000		20	
Factory Overhead	$500,000			
		$900,000		90
Gross Profit		$200,000		10

Profit has been increased by 60% to get the in profit by 600,000 by increasing revenue; sales would have to increase to 1.2 million. What will happen with CGS?

A. Decrease by 3%
B. Increase by 4%
C. Decrease by 4%
D. Will remain same

Answer(s): A

QUESTION: 8

By using following product tree, how many Xs are needed to make 200Xs and 150 Ys?

BONUS!!! Download part of Real4Prep XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1SOmE2jCLSvlZXMbMjFGxHk2aNztbw3vE

If you don't pass the Selling Palo Alto Networks XSIAM Engineer (XSIAM-Engineer) exam, Real4Prep will refund the money. Some terms and conditions related to the refund are given on the guarantee page. You will not find such excellent offers anywhere else. Therefore, don't miss this golden opportunity and Palo Alto Networks XSIAM Engineer (XSIAM-Engineer) practice test material today!

These formats are Palo Alto Networks XSIAM-Engineer PDF dumps, web-based practice test software, and desktop practice test software. All these three Palo Alto Networks XSIAM Engineer (XSIAM-Engineer) exam questions contain the real, valid, and updated Palo Alto Networks Exams that will provide you with everything that you need to learn, prepare and pass the challenging but career advancement XSIAM-Engineer Certification Exam with good scores.

>> Exam XSIAM-Engineer Questions <<

Exam XSIAM-Engineer Questions | Pass-Sure XSIAM-Engineer: Palo Alto Networks XSIAM Engineer 100% Pass

Although our XSIAM-Engineer exam braindumps have been recognised as a famous and popular brand in this field, but we still can be better by our efforts. In the future, our XSIAM-Engineer study materials will become the top selling products. Although we come across some technical questions of our XSIAM-Engineer learning guide during development process, we still never give up to developing our XSIAM-Engineer practice engine to be the best in every detail.

Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Maintenance and Troubleshooting: This section of the exam measures skills of Security Operations Engineers and covers post-deployment maintenance and troubleshooting of XSIAM components. It includes managing exception configurations, updating software components such as XDR agents and Broker VMs, and diagnosing data ingestion, normalization, and parsing issues. Candidates must also troubleshoot integrations, automation playbooks, and system performance to ensure operational reliability.

Topic 2	• Planning and Installation: This section of the exam measures skills of XSIAM Engineers and covers the planning, evaluation, and installation of Palo Alto Networks Cortex XSIAM components. It focuses on assessing existing IT infrastructure, defining deployment requirements for hardware, software, and integrations, and establishing communication needs for XSIAM architecture. Candidates must also configure agents, Broker VMs, and engines, along with managing user roles, permissions, and access controls.
Topic 3	• Content Optimization: This section of the exam measures skills of Detection Engineers and focuses on refining XSIAM content and detection logic. It includes deploying parsing and data modeling rules for normalization, managing detection rules based on correlation, IOCs, BIOCs, and attack surface management, and optimizing incident and alert layouts. Candidates must also demonstrate proficiency in creating custom dashboards and reporting templates to support operational visibility.
Topic 4	• Integration and Automation: This section of the exam measures skills of SIEM Engineers and focuses on data onboarding and automation setup in XSIAM. It covers integrating diverse data sources such as endpoint, network, cloud, and identity, configuring automation feeds like messaging, authentication, and threat intelligence, and implementing Marketplace content packs. It also evaluates the ability to plan, create, customize, and debug playbooks for efficient workflow automation.

Palo Alto Networks XSIAM Engineer Sample Questions (Q244-Q249):

NEW QUESTION # 244
An XSIAM engineer is investigating a persistent alert from an indicator rule that flags 'attempts to modify critical system files.' The rule's current XQL is:
□
After analysis, it's determined that legitimate patching and antivirus updates are triggering these alerts. How should the engineer refine this rule to eliminate these false positives while preserving detection of malicious activity?

- A. Filter by and exclude 'SYSTEM' user, as legitimate updates often run as SYSTEM.
- B. Remove the rule, as critical system file modification is too noisy to reliably detect with indicator rules.
- C. Modify the XQL to include a check for the 'digital_signature' of the process performing the write, ensuring it's not signed by Microsoft or the organization's trusted vendors, specifically for update/patch processes.
- D. Add 'and not (process_name in ('msiexec.exe', 'wusa.exe') and parent_process_name = ' TrustedInstaller.exe')' to the XQL query.
- E. Change the 'file_path' to only look for executable files with a .exe' extension, ignoring DLLs.

Answer: C

Explanation:
Option C is the most effective and robust solution for handling legitimate updates. Digital Signatures: Legitimate patching and antivirus updates are almost always performed by digitally signed executables from trusted vendors (like Microsoft for OS updates, or a reputable AV vendor). By filtering based on the absence of a valid, trusted digital signature, you can effectively distinguish legitimate updates from malicious attempts to modify system files. This is a high-fidelity filter. Option A is a surrender. Option B is a partial solution, as patchers and installers can use various processes and parent processes, and 'TrustedInstaller.exe' might not always be the direct parent, also it's often more reliable to use signatures. Option D would eliminate many legitimate updates, as SYSTEM often performs these, and also miss malicious activity by SYSTEM. Option E would completely miss malicious modifications to critical DLLS, which is a common technique.

NEW QUESTION # 245
A large enterprise uses XSIAM for comprehensive security. They have a strict policy against the use of insecure authentication protocols like NTLMv1 , even for internal services. They want to create an ASM rule to detect any internal server or application attempting to authenticate using NTLMv1. Given that XSIAM collects authentication logs from various sources (Active Directory, Linux authentication, network authentications), which of the following XQL approaches would be most effective for detecting NTLMv1 usage across their distributed environment?

- A. □
- B. □
- C. □

- D. Combine insights from 'xdr_authentication_logs' (for protocol details) and 'xdr_network_sessions' (for application protocol and potential deep packet inspection insights if available) to precisely identify NTLMv1. An example would be:
- E.

Answer: D

Explanation:
Option E is the most comprehensive and effective approach for detecting NTLMv1 across a distributed environment in XSIAM. It leverages the 'union' operator to combine data from different relevant datasets. is ideal for explicit authentication protocol details, while can provide insights from network-level detections (like deep packet inspection signatures if available for NTLMv1 or related SMBv1 traffic, which often implies NTLMv1 usage). This multi-source correlation provides a more robust and complete picture. Option A is too broad and inefficient. Option B assumes a specific 'authentication_version' field, which might not be uniformly present across all authentication logs. Option C relies solely on a specific network signature, which might not always fire or be available for all NTLMv1 scenarios. Option D focuses only on failures and might miss successful NTLMv1 authentications.

NEW QUESTION # 246
A global enterprise uses XSIAM and has different SOC teams responsible for different geographical regions. When an incident occurs, the default incident layout shows all available fields, leading to information overload for regional teams who only care about region- specific attributes (e.g., 'Region', 'Local Compliance Regulations'). How can XSIAM's content optimization capabilities be leveraged to provide a tailored incident layout based on the user's role or assigned region, without creating multiple duplicate incident types?

- A. Develop custom scripts to filter incident data before it's displayed in the XSIAM UI.
- B. Manually train each SOC analyst to ignore irrelevant fields.
- C. Create separate XSIAM instances for each geographical region.
- D. Implement an external workflow automation tool to pre-process incidents.
- E. Utilize XSIAM's 'Layout Context' feature, defining different incident layouts that dynamically apply based on criteria like incident 'tags' (e.g., 'region:APAC', 'region:EMEA') or user group membership, allowing different views for different teams.

Answer: E

Explanation:
To provide tailored incident layouts based on user roles or region without duplicating incident types, XSIAM's 'Layout Context' feature is the most suitable content optimization capability. This allows defining multiple layouts for a single incident type, which are then dynamically applied based on conditions like incident tags (e.g., 'region:APAC') or the user's group membership, ensuring that regional teams see only the most relevant information. Options A, C, D, and E are either impractical, inefficient, or do not directly address dynamic layout customization within XSIAM.

NEW QUESTION # 247
Which section of a parsing rule defines the newly created dataset?

- A. COLLECT
- B. INGEST
- C. CONST
- D. RULE

Answer: A

Explanation:
In a Cortex XSIAM parsing rule, the COLLECT section defines the newly created dataset. This section specifies how the parsed fields and data should be structured and stored for further use in analytics and queries.

NEW QUESTION # 248
A large enterprise is planning to deploy Cortex XSIAM and expects to ingest data from 50,000 endpoints, 100 network devices, and 20 cloud accounts daily, generating an estimated 5 TB of raw log data per day. The security team requires a 90-day hot storage retention and a I-year cold storage retention for compliance. Given these requirements, which of the following considerations are paramount when planning the XSIAM Engine deployment architecture to ensure optimal performance, scalability, and cost-

efficiency?

- A. Implementing a distributed Engine architecture with multiple Engine instances across different geographical regions to minimize latency for data ingestion.
- B. Prioritizing the deployment of a single, monolithic XSIAM Engine instance with maximum available resources to simplify management.
- C. Ignoring the daily data ingestion volume, as XSIAM's cloud infrastructure automatically scales to accommodate any data load without prior planning.
- D. Carefully sizing the Engine's local storage for temporary processing and event buffering, and verifying sufficient bandwidth to XSIAM's cloud storage for long- term retention.
- E. Focusing solely on the CPU and RAM allocation for the Engine, as storage is managed independently by XSIAM's backend.

Answer: D

Explanation:
While options C might seem appealing for certain scenarios, the core issue with 5TB/day ingestion and specific retention policies lies in storage and network planning. Option D directly addresses the critical aspects of local storage sizing for temporary processing and the crucial bandwidth requirements for efficient data offload to XSIAM's cloud storage for long-term retention, which is essential for performance, scalability, and cost-efficiency in such a high-volume environment. Option A is incorrect as a single monolithic instance would be a single point of failure and likely unable to handle the load. Option B is incorrect because local storage on the Engine is vital for processing and buffering. Option E is fundamentally flawed as proper planning for data volume is always necessary for any cloud-based solution.

NEW QUESTION # 249
......

For candidates who buy XSIAM-Engineer exam bootcamp online, they may have the concern about the money safety. We apply the international recognition third party for the payment, and it will protect the interests of you. Therefore you put your mind at rest if you buy XSIAM-Engineer exam bootcamp from us. In addition, we have free demo for you to have a try, so that you can have a deeper understanding the complete version of the XSIAM-Engineer Exam Dumps. If you have any other questions, just contact us, and we will do what we can do to help you.

Dumps XSIAM-Engineer Reviews: https://www.real4prep.com/XSIAM-Engineer-exam.html

- The Best XSIAM-Engineer - Exam Palo Alto Networks XSIAM Engineer Questions □ Search for （ XSIAM-Engineer ） and download it for free on 「 www.troytecdumps.com 」 website □Reliable XSIAM-Engineer Test Pattern
- Latest updated Exam XSIAM-Engineer Questions - Guaranteed Palo Alto Networks XSIAM-Engineer Exam Success with Pass-Sure Dumps XSIAM-Engineer Reviews □ Simply search for ✔ XSIAM-Engineer □✔□ for free download on { www.pdfvce.com } □Related XSIAM-Engineer Exams
- XSIAM-Engineer Exam Sample Online □ Reliable XSIAM-Engineer Test Pattern □ XSIAM-Engineer Latest Exam Answers □ Easily obtain free download of （ XSIAM-Engineer ） by searching on ➡ www.validtorrent.com □□□ □ □XSIAM-Engineer Test Dates
- Pdfvce Palo Alto Networks XSIAM-Engineer Dumps PDF Format □ Open " www.pdfvce.com " and search for （ XSIAM-Engineer ） to download exam materials for free □XSIAM-Engineer Exam Sample Online
- Exam XSIAM-Engineer Questions | Newest Palo Alto Networks XSIAM Engineer 100% Free Dumps Reviews □ Easily obtain free download of 【 XSIAM-Engineer 】 by searching on ➥ www.troytecdumps.com □ □Reliable XSIAM-Engineer Exam Guide
- Free PDF Palo Alto Networks - Fantastic XSIAM-Engineer - Exam Palo Alto Networks XSIAM Engineer Questions □ Open □ www.pdfvce.com □ and search for （ XSIAM-Engineer ） to download exam materials for free ☣VCE XSIAM-Engineer Dumps
- 100% Pass Quiz Palo Alto Networks - XSIAM-Engineer –Professional Exam Questions □ Open ⇛ www.practicevce.com ⇚ enter ➥ XSIAM-Engineer □ and obtain a free download □Reliable XSIAM-Engineer Exam Guide
- VCE XSIAM-Engineer Dumps □ New XSIAM-Engineer Dumps Ppt □ XSIAM-Engineer Exam Sample Online □ Immediately open □ www.pdfvce.com □ and search for □ XSIAM-Engineer □ to obtain a free download □XSIAM-Engineer Test Dates
- Newest XSIAM-Engineer Exam Collection - XSIAM-Engineer Practice Torrent - XSIAM-Engineer Actual Pdf □ Search for ➠ XSIAM-Engineer □ and download it for free immediately on □ www.vce4dumps.com □ □XSIAM-Engineer Free Exam

- XSIAM-Engineer Test Dates □ XSIAM-Engineer Exam Dumps Pdf □ VCE XSIAM-Engineer Dumps □ Download ⇛ XSIAM-Engineer ⇚ for free by simply searching on ☀ www.pdfvce.com □☀□ □XSIAM-Engineer Exam Sample Online
- The Best XSIAM-Engineer - Exam Palo Alto Networks XSIAM Engineer Questions □ Go to website □ www.exam4labs.com □ open and search for □ XSIAM-Engineer □ to download for free □XSIAM-Engineer Valid Exam Cram
- www.stes.tyc.edu.tw, learn.csisafety.com.au, dopementor.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.dibiz.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Real4Prep XSIAM-Engineer dumps now are free: https://drive.google.com/open?id=1SOmE2jCLSvlZXMbMjFGxHk2aNztbw3vE