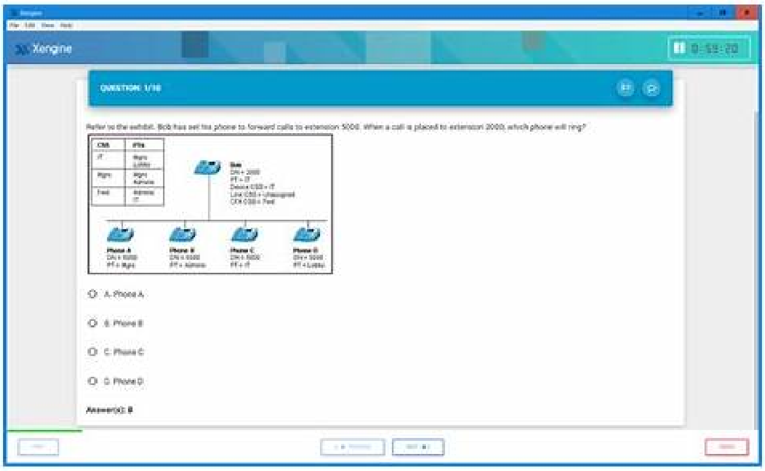
Palo Alto Networks XDR-Analyst Reliable Dumps, Valid XDR-Analyst Exam Simulator



QUESTION: 1/10

Refer to the exhibit. Bob has set his phone to forward calls to extension 5000. When a call is placed to extension 2000, which phone will ring?

○ A. Phone A

○ B. Phone B

○ C. Phone C

○ D. Phone D

Answer(s): B

Dumpkiller Palo Alto Networks Certification Exam comes in three different formats so that the users can choose their desired design and prepare Palo Alto Networks XDR-Analyst exam according to their needs. The first we will discuss here is the PDF file of real Palo Alto Networks XDR-Analyst Exam Questions. It can be taken to any place via laptops, tablets, and smartphones.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights.
Topic 2	• Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
Topic 3	• Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions.
Topic 4	• Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques.

>> Palo Alto Networks XDR-Analyst Reliable Dumps <<

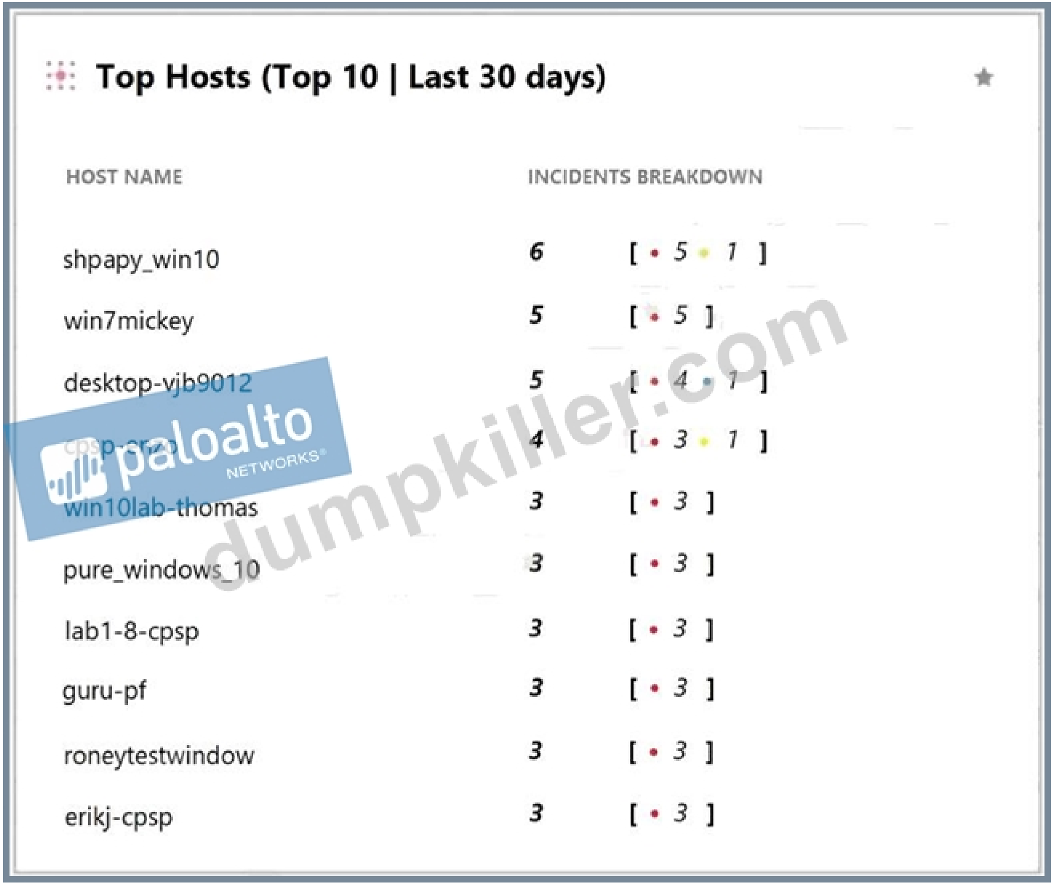
Valid XDR-Analyst Exam Simulator - XDR-Analyst Exam Questions Fee

If you are busy with your work and study and have little time to prepare for your exam, then choose us, we can do the rest for you. XDR-Analyst exam torrent is high-quality, and you just need to spend about 48 to 72 hours on study, you can pass you exam just one time. In addition, we are pass guarantee and money back guarantee for XDR-Analyst Exam Braindumps, and therefore you don't need to worry about that you will waste your money. We offer you free update for one year, and the update version for XDR-Analyst exam materials will be sent to your email automatically.

Palo Alto Networks XDR Analyst Sample Questions (Q65-Q70):

NEW QUESTION # 65

What does the following output tell us?



Top Hosts (Top 10 | Last 30 days)

HOST NAME	INCIDENTS BREAKDOWN
shpapy_win10	6 [● 5 ● 1]
win7mickey	5 [● 5]
desktop-vjb9012	5 [● 4 ● 1]
cpsp-cr20	4 [● 3 ● 1]
win10lab-thomas	3 [● 3]
pure_windows_10	3 [● 3]
lab1-8-cpsp	3 [● 3]
guru-pf	3 [● 3]
roneytestwindow	3 [● 3]
erikj-cpsp	3 [● 3]

- A. Host shpapy_win10 had the most vulnerabilities.
- B. This is an actual output of the Top 10 hosts with the most malware.
- C. There is one informational severity alert.
- D. There is one low severity incident.

Answer: B

Explanation:
The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more .
Reference:
Use the ACC to Analyze Network Activity
Top 10 Hosts with the Most Malware

NEW QUESTION # 66
Which profiles can the user use to configure malware protection in the Cortex XDR console?

- A. Anti-Malware profile
- B. Malware Protection profile
- C. Malware profile
- D. Malware Detection profile

Answer: B

Explanation:
The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different

actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. Reference:
Malware Protection Profile
Endpoint Security Policy

NEW QUESTION # 67
If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

- A. Local Agent Installer and Content Caching
- B. Broker VM Pathfinder
- C. Broker VM Syslog Collector
- D. Local Agent Proxy

Answer: D

Explanation:
If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it here1 and here2. Reference:
Local Agent Proxy
Configure the Local Agent Proxy Setup

NEW QUESTION # 68
When creating a BIOC rule, which XQL query can be used?

- A. dataset = xdr_data
  | filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
  | fields action_process_image
- B. dataset = xdr_data
  | filter event_behavior = true
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- C. dataset = xdr_data
  | filter event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- D. dataset = xdr_data
  | filter event_type = PROCESS and
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Answer: D

Explanation:
A BIOC rule is a custom detection rule that uses the Cortex Query Language (XQL) to define the behavior or actions that indicate a potential threat. A BIOC rule can use the xdr_data and cloud_audit_log datasets and presets for these datasets. A BIOC rule can also use the filter stage, alter stage, and functions without any aggregations in the XQL query. The query must return a single field named action_process_image, which is the process image name of the suspicious process. The query must also include the event_type and event_sub_type fields in the filter stage to specify the type and sub-type of the event that triggers the rule.
Option B is the correct answer because it meets all the requirements for a valid BIOC rule query. It uses the xdr_data dataset, the

filter stage, the event_type and event_sub_type fields, and the action_process_image_name field with a regular expression to match any process image name that ends with .pdf.exe or .docx.exe, which are common indicators of malicious files.
Option A is incorrect because it does not include the event_type field in the filter stage, which is mandatory for a BIOC rule query.
Option C is incorrect because it does not include the event_type and event_sub_type fields in the filter stage, and it uses the fields stage, which is not supported for a BIOC rule query. It also returns the action_process_image field instead of the action_process_image_name field, which is the expected output for a BIOC rule query.
Option D is incorrect because it uses the event_behavior field, which is not supported for a BIOC rule query. It also does not include the event_type field in the filter stage, and it uses the event_sub_type field incorrectly. The event_sub_type field should be equal to PROCESS_START, not true.
Reference:
Working with BIOCs
Cortex Query Language (XQL) Reference

NEW QUESTION # 69
What is an example of an attack vector for ransomware?

- A. A URL filtering feature enabled on a firewall
- B. Performing SSL Decryption on an endpoint
- C. Performing DNS queries for suspicious domains
- D. Phishing emails containing malicious attachments

Answer: D

Explanation:
An example of an attack vector for ransomware is phishing emails containing malicious attachments. Phishing is a technique that involves sending fraudulent emails that appear to come from a legitimate source, such as a bank, a company, or a government agency. The emails typically contain a malicious attachment, such as a PDF document, a ZIP archive, or a Microsoft Office document, that contains ransomware or a ransomware downloader. When the recipient opens or downloads the attachment, the ransomware is executed and encrypts the files or data on the victim's system. The attacker then demands a ransom for the decryption key, usually in cryptocurrency.
Phishing emails are one of the most common and effective ways of delivering ransomware, as they can bypass security measures such as firewalls, antivirus software, or URL filtering. Phishing emails can also exploit the human factor, as they can trick the recipient into opening the attachment by using social engineering techniques, such as impersonating a trusted sender, creating a sense of urgency, or appealing to curiosity or greed. Phishing emails can also target specific individuals or organizations, such as executives, employees, or customers, in a technique called spear phishing, which increases the chances of success.
According to various sources, phishing emails are the main vector of ransomware attacks, accounting for more than 90% of all ransomware infections12. Some of the most notorious ransomware campaigns, such as CryptoLocker, Locky, and WannaCry, have used phishing emails as their primary delivery method3 . Therefore, it is essential to educate users on how to recognize and avoid phishing emails, as well as to implement security solutions that can detect and block malicious attachments. Reference:
Top 7 Ransomware Attack Vectors & How to Avoid Becoming a Victim - Bitsight What Is the Main Vector of Ransomware Attacks? A Definitive Guide CryptoLocker Ransomware Information Guide and FAQ
[Locky Ransomware Information, Help Guide, and FAQ]
[WannaCry ransomware attack]

NEW QUESTION # 70
......

Preparation of professional Palo Alto Networks XDR Analyst (XDR-Analyst) exam is no more difficult because experts have introduced the preparatory products. With Dumpkiller products, you can pass the Palo Alto Networks XDR Analyst (XDR-Analyst) exam on the first attempt. If you want a promotion or leave your current job, you should consider achieving a professional certification like Palo Alto Networks XDR Analyst (XDR-Analyst) exam. You will need to pass the Palo Alto Networks XDR-Analyst exam to achieve the Palo Alto Networks XDR Analyst (XDR-Analyst) certification.

Valid XDR-Analyst Exam Simulator: https://www.dumpkiller.com/XDR-Analyst_braindumps.html

- Reliable Palo Alto Networks XDR-Analyst PDF Questions Pass Exam With Confidence □ Search on ➥ www.exam4labs.com □ for □ XDR-Analyst □ to obtain exam materials for free download □XDR-Analyst Valid Dumps
- Exam XDR-Analyst Simulations □ XDR-Analyst Certification □ XDR-Analyst Reliable Exam Prep □ ▷ www.pdfvce.com ◁ is best website to obtain 《 XDR-Analyst 》 for free download □XDR-Analyst Certification Dumps
- XDR-Analyst Reliable Exam Prep □ Latest XDR-Analyst Exam Format □ Certification XDR-Analyst Exam Infor □ Open website ✔ www.easy4engine.com □✔□ and search for （ XDR-Analyst ） for free download □XDR-Analyst Exam Actual Questions
- XDR-Analyst Flexible Testing Engine □ XDR-Analyst Certification Dumps □ XDR-Analyst Valid Dumps □ Download ⇛ XDR-Analyst ⇚ for free by simply searching on 「 www.pdfvce.com 」 □Free XDR-Analyst Download
- XDR-Analyst Certification □ Certification XDR-Analyst Exam Infor □ Free XDR-Analyst Download □ Search for ▷ XDR-Analyst ◁ and download it for free immediately on 【 www.examcollectionpass.com 】 □Valid Braindumps XDR-Analyst Files
- XDR-Analyst Exam Actual Questions □ Latest XDR-Analyst Exam Format □ Latest Test XDR-Analyst Discount □ Download 《 XDR-Analyst 》 for free by simply entering ➤ www.pdfvce.com □ website □Real XDR-Analyst Exam Answers
- Reliable Palo Alto Networks XDR-Analyst PDF Questions Pass Exam With Confidence □ Search on ➥ www.exam4labs.com □ for 【 XDR-Analyst 】 to obtain exam materials for free download □Latest XDR-Analyst Exam Format
- Trusted XDR-Analyst Reliable Dumps - Useful Palo Alto Networks Certification Training - Trustworthy Palo Alto Networks Palo Alto Networks XDR Analyst □ Search for ☀ XDR-Analyst □☀□ and download exam materials for free through 「 www.pdfvce.com 」 □XDR-Analyst Labs
- www.prep4away.com Offers Three Formats of Updated Palo Alto Networks XDR-Analyst Exam Questions □ Go to website ⇛ www.prep4away.com ⇚ open and search for { XDR-Analyst } to download for free □XDR-Analyst Flexible Testing Engine
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, eishkul.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, carolai.com, www.stes.tyc.edu.tw, giphy.com, Disposable vapes