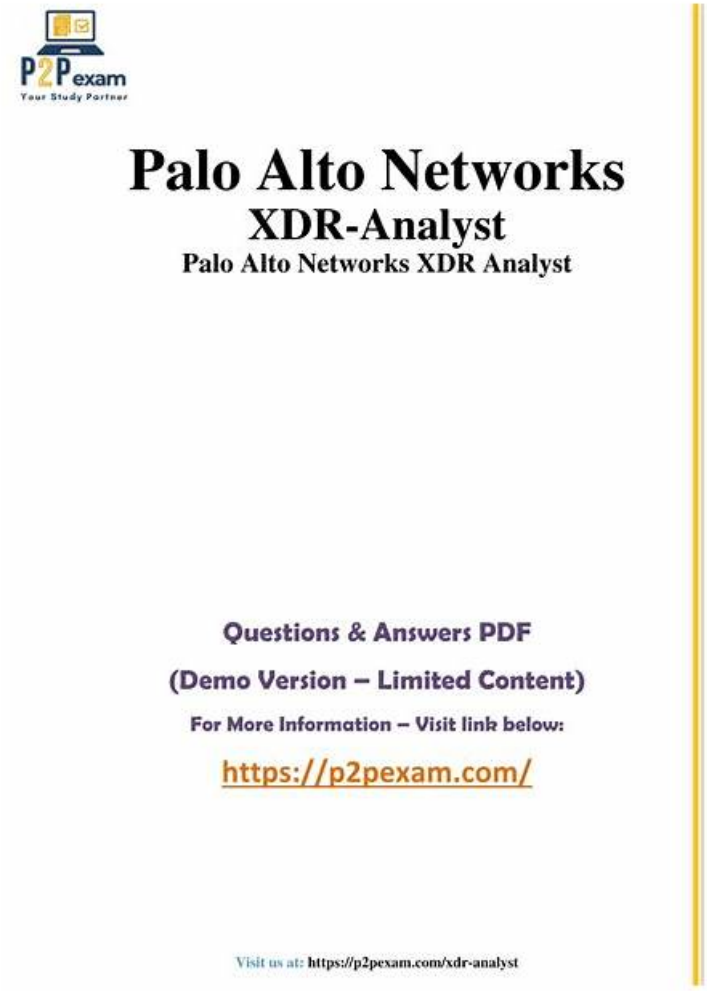
Free Palo Alto Networks XDR-Analyst Braindumps & Reliable XDR-Analyst Test Question



The Real4exams offers three formats for applicants to practice and prepare for the XDR-Analyst exam as per their needs. The pdf format of Real4exams is portable and can be used on laptops, tablets, and smartphones. Print real Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions in our PDF file. The pdf is user-friendly and accessible on any smart device, allowing applicants to study from anywhere at any time.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.

Topic 4	• 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.

Reliable XDR-Analyst Test Question - New XDR-Analyst Mock Test

Our desktop software also tracks your progress, and identifies your strengths and weaknesses, to ensure you're getting the best possible experience for the XDR-Analyst Exam. All features of the web-based version are available in the desktop software. But the desktop software works offline and only on Windows computers.

Palo Alto Networks XDR Analyst Sample Questions (Q50-Q55):

NEW QUESTION # 50
Which of the following is an example of a successful exploit?

- A. executing a process executable for well-known and signed software.
- B. identifying vulnerable services on a server.
- C. connecting unknown media to an endpoint that copied malware due to Autorun.
- D. a user executing code which takes advantage of a vulnerability on a local service.

Answer: D

Explanation:
A successful exploit is a piece of software or code that takes advantage of a vulnerability and executes malicious actions on the target system. A vulnerability is a weakness or flaw in a software or hardware component that can be exploited by an attacker. A successful exploit is one that achieves its intended goal, such as gaining unauthorized access, executing arbitrary code, escalating privileges, or compromising data.
In the given options, only B is an example of a successful exploit, because it involves a user executing code that exploits a vulnerability on a local service, such as a web server, a database, or a network protocol. This could allow the attacker to gain control over the service, access sensitive information, or perform other malicious actions.
Option A is not a successful exploit, because it involves connecting unknown media to an endpoint that copied malware due to Autorun. Autorun is a feature that automatically runs a program or script when a removable media, such as a USB drive, is inserted into a computer. This feature can be abused by malware authors to spread their malicious code, but it is not an exploit in itself. The malware still needs to exploit a vulnerability on the endpoint to execute its payload and cause damage.
Option C is not a successful exploit, because it involves identifying vulnerable services on a server. This is a step in the reconnaissance phase of an attack, where the attacker scans the target system for potential vulnerabilities that can be exploited. However, this does not mean that the attacker has successfully exploited any of the vulnerabilities, or that the vulnerabilities are even exploitable.
Option D is not a successful exploit, because it involves executing a process executable for well-known and signed software. This is a legitimate action that does not exploit any vulnerability or cause any harm. Well-known and signed software are programs that are widely used and trusted, and have a digital signature that verifies their authenticity and integrity. Executing such software does not pose a security risk, unless the software itself is malicious or compromised.
Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 What Is an Exploit? Definition, Types, and Prevention Measures(https://heimdalsecurity.com/blog/what-is-an-exploit/) Exploit Definition & Meaning - Merriam-Webster(https://www.merriam-webster.com/dictionary/exploit)

NEW QUESTION # 51
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_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

- C. dataset = xdr_data
| filter event_behavior = true
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 # 52
What kind of the threat typically encrypts user files?

- A. ransomware
- B. Zero-day exploits
- C. SQL injection attacks
- D. supply-chain attacks

Answer: A

Explanation:
Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack123456 Reference:
What is Ransomware? | How to Protect Against Ransomware in 2023
Ransomware - Wikipedia
What is ransomware? | Ransomware meaning | Cloudflare
What Is Ransomware? | Ransomware.org
Ransomware - FBI

NEW QUESTION # 53
Which Type of IOC can you define in Cortex XDR?

- A. e-mail address
- B. destination port
- C. App-ID
- D. full path

Answer: D

Explanation:
Cortex XDR allows you to define IOCs based on various criteria, such as file hashes, registry keys, IP addresses, domain names, and full paths. A full path IOC is a specific location of a file or folder on an endpoint, such as C:\Windows\System32\calc.exe. You can use full path IOCs to detect and respond to malicious files or folders that are located in known locations on your endpoints12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . destination port: This is not the correct answer. Destination port is not a type of IOC that you can define in Cortex XDR. Destination port is a network attribute that indicates the port number to which a packet is sent. Cortex XDR does not support defining IOCs based on destination ports, but you can use XQL queries to filter network events by destination ports3.
B . e-mail address: This is not the correct answer. E-mail address is not a type of IOC that you can define in Cortex XDR. E-mail address is an identifier that is used to send and receive e-mails. Cortex XDR does not support defining IOCs based on e-mail addresses, but you can use the Cortex XDR - IOC integration with Cortex XSOAR to ingest IOCs from various sources, including e-mail addresses4.
D . App-ID: This is not the correct answer. App-ID is not a type of IOC that you can define in Cortex XDR. App-ID is a feature of Palo Alto Networks firewalls that identifies and controls applications on the network. Cortex XDR does not support defining IOCs based on App-IDs, but you can use the Cortex XDR Analytics app to create custom rules that use App-IDs as part of the rule logic5.
In conclusion, full path is the type of IOC that you can define in Cortex XDR. By using full path IOCs, you can enhance your detection and response capabilities and protect your endpoints from malicious files or folders.
Reference:
Create an IOC Rule
XQL Reference Guide: Network Events Schema
Cortex XDR - IOC
Cortex XDR Analytics App
PCDRA: Which Type of IOC can define in Cortex XDR?

NEW QUESTION # 54
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

- A. Create IOCs of the malicious files you have found to prevent their execution.
- B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- C. Enable DLL Protection on all servers but there might be some false positives.
- D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Answer: B

Explanation:
To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a

Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted3.
C . Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection4.
D . Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not have an option to enable or configure BTP rules.
In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply chain attack.
Reference:
Behavioral Threat Protection
Create a BTP Rule
DLL Protection
Create an IOC Rule
[Cytool]

NEW QUESTION # 55
.....

Exam Online

- XDR-Analyst Exam Reference □ Latest XDR-Analyst Test Materials □ XDR-Analyst Valid Braindumps □ Enter 《 www.pdfvce.com 》 and search for ▶ XDR-Analyst ◀ to download for free □Pass4sure XDR-Analyst Dumps Pdf
- High-quality Free XDR-Analyst Braindumps - Easy and Guaranteed XDR-Analyst Exam Success □ Search for 《 XDR-Analyst 》 on 「 www.prepawaypdf.com 」 immediately to obtain a free download □Valid XDR-Analyst Test Sample
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.notebook.ai, Disposable vapes