XDR-Analyst Frequent Updates, Valid Real XDR-Analyst Exam

Our XDR-Analyst training dumps are highly salable not for profit in our perspective solely, they are helpful tools helping more than 98 percent of exam candidates get the desirable outcomes successfully. Our XDR-Analyst guide prep is priced reasonably with additional benefits valuable for your reference. High quality and accuracy XDR-Analyst Exam Materials with reasonable prices can totally suffice your needs about the exam. All those merits prefigure good needs you may encounter in the near future.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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.

>> XDR-Analyst Frequent Updates <<

Valid Real XDR-Analyst Exam | XDR-Analyst Exam Actual Questions

Our company is a multinational company which is famous for the XDR-Analyst training materials in the international market. After nearly ten years' efforts, now our company have become the topnotch one in the field, therefore, if you want to pass the XDR-Analyst Exam as well as getting the related certification at a great ease, I strongly believe that the XDR-Analyst study materials compiled by our company is your solid choice.

Palo Alto Networks XDR Analyst Sample Questions (Q43-Q48):

NEW QUESTION # 43
How can you pivot within a row to Causality view and Timeline views for further investigate?

- A. Using the Open Card and Open Timeline actions respectively
- B. Using the Open Card Only
- C. Using Open Timeline Actions Only
- D. You can't pivot within a row to Causality view and Timeline views

Answer: A

Explanation:
To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident. Reference:
Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

NEW QUESTION # 44
What is the purpose of the Unit 42 team?

- A. Unit 42 is responsible for threat research, malware analysis and threat hunting
- B. Unit 42 is responsible for the rapid deployment of Cortex XDR agents
- C. Unit 42 is responsible for the configuration optimization of the Cortex XDR server
- D. Unit 42 is responsible for automation and orchestration of products

Answer: A

Explanation:
Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents3.
B . Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server4.
C . Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints5.
In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture and protect against the latest cyberthreats.
Reference:
About Unit 42: Our Mission and Team

Unit 42: Threat Intelligence & Response
Cortex XSOAR
Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies
Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

NEW QUESTION # 45
When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

- A. A list of all the current exceptions applied to the agent.
- B. The unique agent id.
- C. The distribution id of the agent.
- D. The agent technical support file.
- E. The prevention archive from the alert.

Answer: D,E

Explanation:
When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:
The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.
The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.
The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:
The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.
A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.
The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.
Reference:
Generate and Download the Agent Technical Support File
Generate and Download the Prevention Archive
Cortex XDR Agent Administrator Guide: Agent Distribution ID
Cortex XDR Agent Administrator Guide: Exception Security Profiles
[Cortex XDR Agent Administrator Guide: Unique Agent ID]

NEW QUESTION # 46
When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. Pending
- B. New
- C. It is blank
- D. Unassigned

Answer: D

Explanation:
The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the

default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
B . It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group12.
D . New: This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.
Reference:
Cortex XDR Pro Admin Guide: Manage Incidents
Cortex XDR Pro Admin Guide: Assign Incidents
Cortex XDR Pro Admin Guide: Update Incident Status

NEW QUESTION # 47
Which of the following is an example of a successful exploit?

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

Answer: A

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 # 48
.....

We guarantee that after purchasing our XDR-Analyst exam torrent, we will deliver the product to you as soon as possible within ten minutes. So you don't need to wait for a long time and worry about the delivery time or any delay. We will transfer our XDR-

Analyst prep torrent to you online immediately, and this service is also the reason why our XDR-Analyst Test Braindumps can win people's heart and mind. And what is more, if you study with our XDR-Analyst training guide for only 20 to 30 hours, then you will be ready to take the XDR-Analyst exam with confidence to pass it.

Valid Real XDR-Analyst Exam: https://www.vce4dumps.com/XDR-Analyst-valid-torrent.html