# PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

## Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.passapply.com/pcdra.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

**QUESTION 1**

Which profiles can the user use to configure malware protection in the Cortex XDR console?

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

Correct Answer: A

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. References: Malware Protection Profile Endpoint Security Policy

**QUESTION 2**

What is the Wildfire analysis file size limit for Windows PE files?

A. No Limit

B. 500MB

C. 100MB

D. 1GB

Correct Answer: C

Explanation: The Wildfire analysis file size limit for Windows PE files is 100MB. Windows PE files are executable files that run on the Windows operating system, such as .exe, .dll, .sys, or .scr files. Wildfire is a cloud-based service that analyzes files and URLs for malicious behavior and generates signatures and protections for them. Wildfire can analyze various file types, such as PE, APK, PDF, MS Office, and others, but each file type has a different file size limit. The file size limit determines the maximum size of the file that can be uploaded or forwarded to Wildfire for analysis. If the file size exceeds the limit, Wildfire will not analyze the file and will return an error message. According to the Wildfire documentation1, the file size limit for Windows PE files is 100MB. This means that any PE file that is larger than 100MB will not be analyzed by Wildfire. However, the firewall can still apply other security features, such as antivirus, antispyware, vulnerability protection, and file blocking, to the PE file based on the security policy settings. The firewall can also perform local analysis on the PE file using the Cortex XDR agent, which uses machine learning models to assess the file and assign it a verdict2. References: WildFire File Size Limits: This document provides the file size limits for different file types that can be analyzed by Wildfire. Local Analysis: This document explains how the Cortex XDR agent performs local analysis on files that cannot be sent to Wildfire for analysis.

**QUESTION 3**

Phishing belongstowhich of the following MITRE ATTandCK tactics?

A. Initial Access, Persistence

B. Persistence, Command and Control

C. Reconnaissance, Persistence

D. Reconnaissance, Initial Access

Correct Answer: D

Explanation: Phishing is a technique that belongs to two MITRE ATTandCK tactics: Reconnaissance and Initial Access. Reconnaissance is the process of gathering information about a target before launching an attack. Phishing for information is a sub- technique of Reconnaissance that involves sending phishing messages to elicit sensitive information that can be used during targeting. Initial Access is the process of gaining a foothold in a network or system. Phishing is a sub-technique of Initial Access that involves sending phishing messages to execute malicious code on victim systems. Phishing can be used for both Reconnaissance and Initial Access depending on the objective and content of the phishing message. References: Phishing, Technique T1566 - Enterprise | MITRE ATTandCK?1 Phishing for Information, Technique T1598 - Enterprise | MITRE ATTandCK?2 Phishing for information, Part 2: Tactics and techniques 3 PHISHING AND THE MITREATTandCK FRAMEWORK - EnterpriseTalk 4 Initial Access, Tactic TA0001 - Enterprise | MITRE ATTandCK?5

**QUESTION 4**

What is an example of an attack vector for ransomware?

A. Performing DNS queries for suspicious domains

B. Performing SSL Decryption on an endpoint

C. Phishing emails containing malicious attachments

D. A URL filtering feature enabled on a firewall

Correct Answer: C

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 alegitimate 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. References: Top 7 Ransomware Attack Vectors and 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]

**QUESTION 5**

Which of the following is an example of a successful exploit?

A. connecting unknown media to an endpoint that copied malware due to Autorun.

B. a user executing code which takes advantage of a vulnerability on a local service.

C. identifying vulnerable services on a server.

D. executing a process executable for well-known and signed software.

Correct Answer: B

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. References: 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 and Meaning - Merriam-Webster(https://www.merriam- webster.com/dictionary/exploit)