



# PCDRA<sup>Q&As</sup>

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.pass4itsure.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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

When creating a scheduled report which is not an option?

- A. Run weekly on a certain day and time.
- B. Run quarterly on a certain day and time.
- C. Run monthly on a certain day and time.
- D. Run daily at a certain time (selectable hours and minutes).

Correct Answer: B

Explanation: When creating a scheduled report in Cortex XDR, the option to run quarterly on a certain day and time is not available. You can only schedule reports to run daily, weekly, or monthly. You can also specify the start and end dates, the time zone, and the recipients of the report. Scheduled reports are useful for generating regular reports on the security events, incidents, alerts, or endpoints in your network. You can create scheduled reports from the Reports page in the Cortex XDR console, or from the Query Center by saving a query as a report. References: Run or Schedule Reports Create a Scheduled Report

---

### QUESTION 2

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. It is blank
- C. Unassigned
- D. New

Correct Answer: C

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 rule<sup>12</sup>. 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"<sup>3</sup>.
- 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 group<sup>12</sup>.
- 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"<sup>3</sup>.

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.

References:

Cortex XDR Pro Admin Guide: Manage Incidents

Cortex XDR Pro Admin Guide: Assign Incidents

Cortex XDR Pro Admin Guide: Update Incident Status

---

### QUESTION 3

Which statement regarding scripts in Cortex XDR is true?

- A. Any version of Python script can be run.
- B. The level of risk is assigned to the script upon import.
- C. Any script can be imported including Visual Basic (VB) scripts.
- D. The script is run on the machine uploading the script to ensure that it is operational.

Correct Answer: B

Explanation: The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk

determines the permissions and restrictions for running the script on endpoints. The levels of risk are:

Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.

The other options are incorrect for the following reasons:

A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts

must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.

C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR



documentation.

VB scripts are not supported by Cortex XDR, and will not run on the endpoints. D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and

size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.

References:

Agent Script Library

Import a Script

Run Scripts on an Endpoint

---

#### QUESTION 4

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>)

---

**QUESTION 5**

What types of actions you can execute with live terminal session?

- A. Manage Network configurations, Quarantine Files, Run PowerShell scripts
- B. Manage Processes, Manage Files, Run Operating System Commands, Run Ruby Commands and Scripts
- C. Apply patches, Reboot System, send notification for end user, Run Python Commands and Scripts
- D. Manage Processes, Manage Files, Run Operating System Commands, Run Python Commands and Scripts

Correct Answer: D

Explanation: Live terminal session is a feature of Cortex XDR that allows you to remotely access and control endpoints from the Cortex XDR console. With live terminal session, you can execute various actions on the endpoints, such as:

Manage Processes: You can view, start, or kill processes on the endpoint, and monitor their CPU and memory usage.

Manage Files: You can view, create, delete, or move files and folders on the endpoint, and upload or download files to or from the endpoint.

Run Operating System Commands: You can run commands on the endpoint using the native command-line interface of the operating system, such as cmd.exe for Windows, bash for Linux, or zsh for macOS.

Run Python Commands and Scripts: You can run Python commands and scripts on the endpoint using the Python interpreter embedded in the Cortex XDR agent. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint.

References: Initiate a Live Terminal Session Manage Processes Manage Files Run Operating System Commands Run Python Commands and Scripts

[Latest PCDRA Dumps](#)

[PCDRA Study Guide](#)

[PCDRA Exam Questions](#)