Vendor: Palo Alto Networks

Exam Code:PSE-CORTEX

Exam Name: Palo Alto Networks System Engineer - Cortex Professional

Version: Demo

QUESTION 1

When analyzing logs for indicators, which are used for only BIOC identification\\'?

A. observed activity

B. artifacts

C. techniques

D. error messages

Correct Answer: A

QUESTION 2

An administrator has a critical group of systems running Windows XP SP3 that cannot be upgraded The administrator wants to evaluate the ability of Traps to protect these systems and the word processing applications running on them

How should an administrator perform this evaluation?

A. Gather information about the word processing applications and run them on a Windows XP SP3 VM Determine if any of the applications are vulnerable and run the exploit with an exploitation tool

B. Run word processing exploits in a latest version of Windows VM in a controlled and isolated environment. Document indicators of compromise and compare to Traps protection capabilities

C. Run a known 2015 flash exploit on a Windows XP SP3 VM. and run an exploitation tool that acts as a listener Use the results to demonstrate Traps capabilities

D. Prepare the latest version of Windows VM Gather information about the word processing applications, determine if some of them are vulnerable and prepare a working exploit for at least one of them Execute with an exploitation tool

Correct Answer: C

QUESTION 3

What is the difference between an exception and an exclusion?

A. An exception is based on rules and exclusions are on alerts

B. An exclusion is based on rules and exceptions are based on alerts.

C. An exception does not exist

D. An exclusion does not exist

Correct Answer: A

QUESTION 4

In an Air-Gapped environment where the Docker package was manually installed after the Cortex XSOAR installation which action allows Cortex XSOAR to access Docker?

A. create a "docker" group and add the "Cortex XSOAR" or "demisto" user to this group

B. create a "Cortex XSOAR\\' or "demisto" group and add the "docker" user to this group

C. disable the Cortex XSOAR service

D. enable the docker service

Correct Answer: B

QUESTION 5

How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context

B. When set to private, task outputs automatically get written to the root context

C. When set to global, allows parallel task execution.

D. When set to global, sub-playbook tasks do not have access to the root context

Correct Answer: D

QUESTION 6

A General Purpose Dynamic Section can be added to which two layouts for incident types? (Choose two)

A. "Close" Incident Form

B. Incident Summary

C. Incident Quick View

D. "New"/Edit" Incident Form

Correct Answer: BC

QUESTION 7

In the DBotScore context field, which context key would differentiate between multiple entries for the same indicator in a multi-TIP environment?

A. Vendor

B. Type

C. Using

D. Brand

Correct Answer: A

QUESTION 8

Given the exception thrown in the accompanying image by the Demisto REST API integration, which action would most likely solve the problem?

Desmisto REST API

Name: Demisto REST API_instance_1

Demisto Server URL: https://127.0.0.1

Demisto Server API Key: *******

User system proxy settings

Use sigle engine: No engine

! Script failed to run: Demisto REST APIs-

Request Failed.

Status code:1

Body:{"StatusCode":-1,"Status":"Get https://127.0.0.1/user:x509;cannot validate certificate for 127.0.0.1 because it doesn\\'t contain any IP SANs","Cookies":

[],"Body":"","Bytes":[],"Headers":{},"Path":"}, at sendRequest(script:59:23(79)):(2603)

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

A. Generic Polling Automation Playbook

B. Playbook Tasks

C. Sub-Play books

D. Playbook Functions

Correct Answer: CD

QUESTION 9

Whichfour types of Traps logs are stored within Cortex Data Lake?

A. Threat, Config, System,Data

B. Threat, Config, System, Analytic

C. Threat, Monitor. System, Analytic

D. Threat, Config, Authentication, Analytic

Correct Answer: A

QUESTION 10

In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three.)

A. Domain/workgroup membership

B. quarantine status

C. hostname

D. OS

E. attack threat intelligence tag

Correct Answer: ACD

QUESTION 11

Given the integration configuration and error in the screenshot what is the cause of the problem? [missing the exhibits]

A. incorrect instance name

B. incorrect Username and Password

C. incorrect appliance port

D. incorrect server URL

Correct Answer: A

QUESTION 12

How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen

B. Linked Indicators column in Incident Screen

C. Related Indicators column in Incident Screen D. Related Incidents column in Indicator Screen

Correct Answer: B