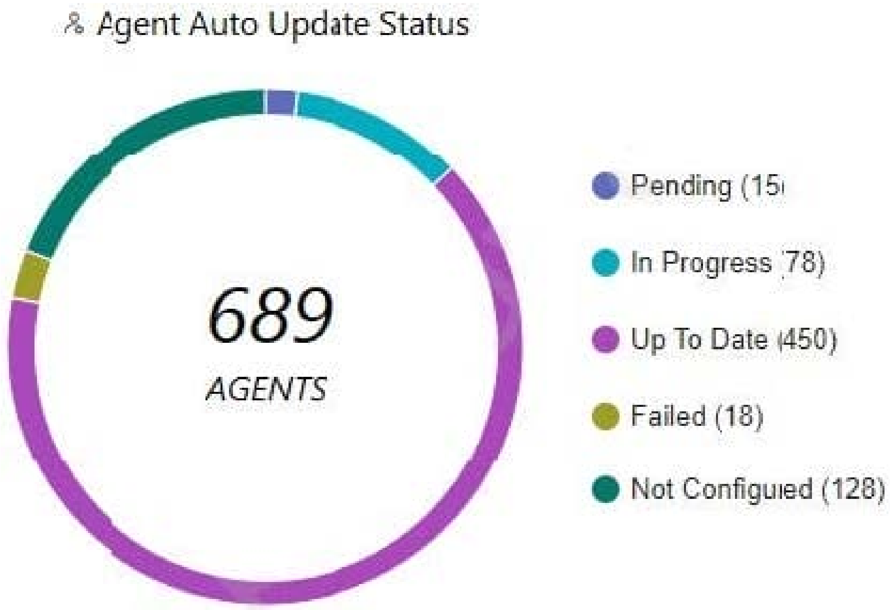
PCDRA$^{\text{Q\&As}}$

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

QUESTION 1

Which statement is true based on the following Agent Auto Upgrade widget?



A. There are a total of 689 Up To Date agents.

B. Agent Auto Upgrade was enabled but not on all endpoints.

C. Agent Auto Upgrade has not been enabled.

D. There are more agents in Pending status than In Progress status.

Correct Answer: B

QUESTION 2

What kind of the threat typically encrypts user files?

A. ransomware

B. SQL injection attacks

C. Zero-day exploits

D. supply-chain attacks

Correct Answer: A

QUESTION 3

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile?

(Choose two.)

A. Automatically close the connections involved in malicious traffic.

B. Automatically kill the processes involved in malicious activity.

C. Automatically terminate the threads involved in malicious activity.

D. Automatically block the IP addresses involved in malicious traffic.

Correct Answer: AD

QUESTION 4

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

QUESTION 5

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

A. Security Manager Dashboard

B. Data Ingestion Dashboard

C. Security Admin Dashboard

D. Incident Management Dashboard

Correct Answer: A

QUESTION 6

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

Correct Answer: D

QUESTION 7

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: D

QUESTION 8

Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP

B. WebSocket

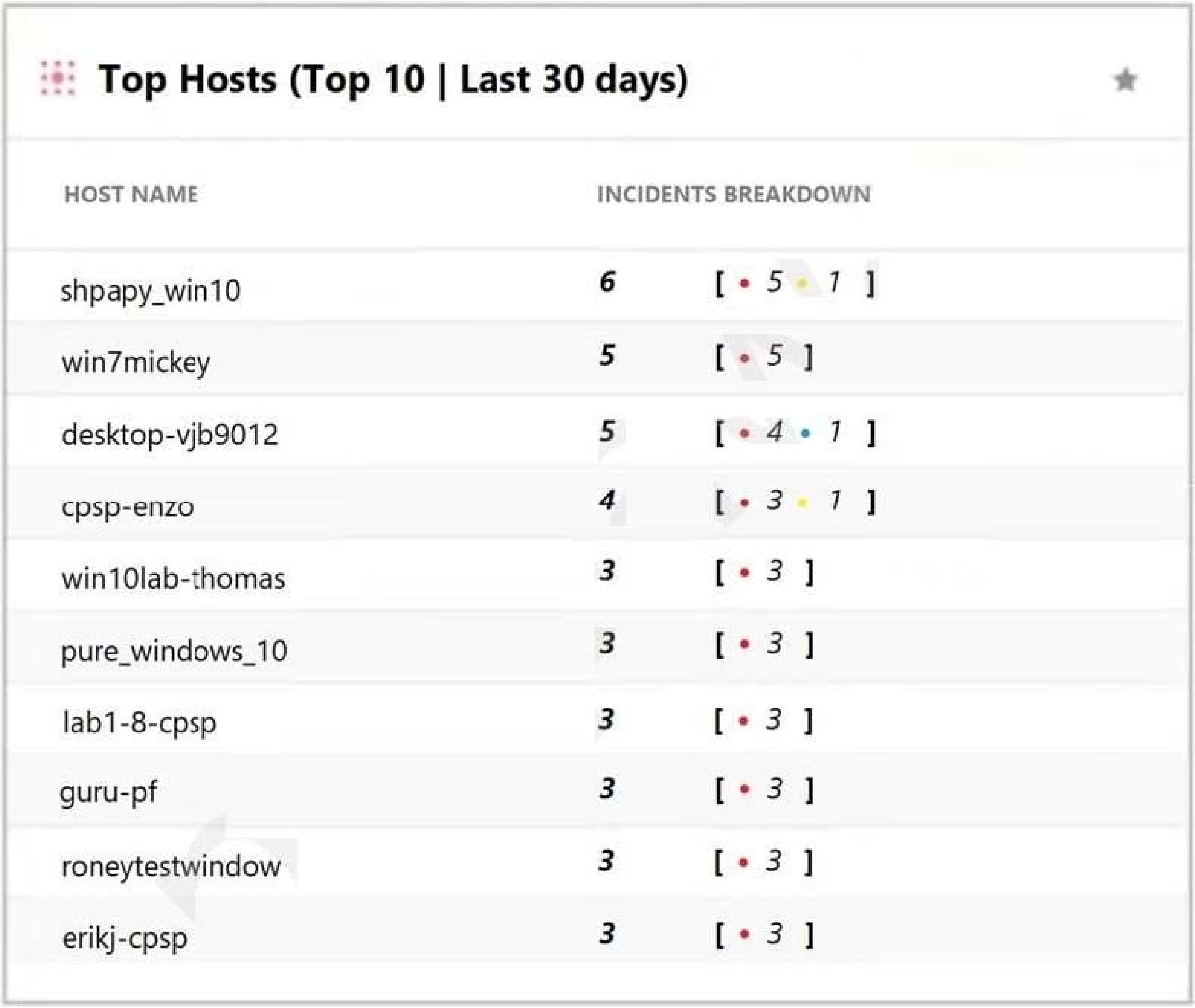
C. UDP and a random port

D. TCP, over port 80

Correct Answer: B

QUESTION 9

What does the following output tell us?



Top Hosts (Top 10 | Last 30 days) ★

HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	6	[● 5 ● 1]
win7mickey	5	[● 5]
desktop-vjb9012	5	[● 4 ● 1]
cpsp-enzo	4	[● 3 ● 1]
win10lab-thomas	3	[● 3]
pure_windows_10	3	[● 3]
lab1-8-cpsp	3	[● 3]
guru-pf	3	[● 3]
roneytestwindow	3	[● 3]
erikj-cpsp	3	[● 3]

A. There is one low severity incident.

B. Host shpapy_win10 had the most vulnerabilities.

C. There is one informational severity alert.

D. This is an actual output of the Top 10 hosts with the most malware.

Correct Answer: D

QUESTION 10

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within a three hour time frame are grouped together into one Incident.

]

C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D. Every alert creates a new Incident.

Correct Answer: A