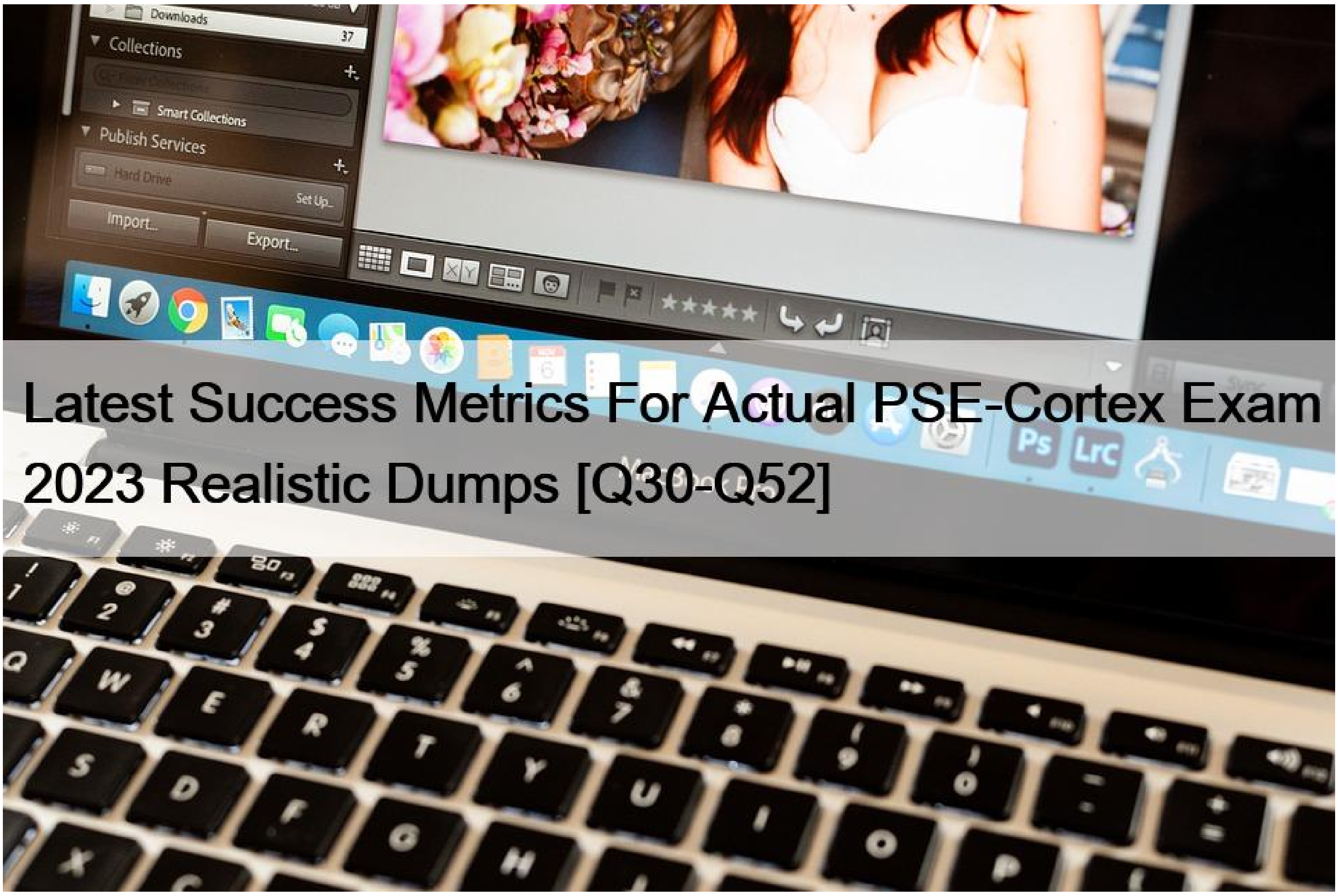
Latest Success Metrics For Actual PSE-Cortex Exam 2023 Realistic Dumps [Q30-Q52



Latest Success Metrics For Actual PSE-Cortex Exam 2023 Realistic Dumps Updated PSE-Cortex Dumps Questions For Palo Alto Networks Exam

The PSE-Cortex certification is a valuable credential for IT professionals who work with Palo Alto Networks Cortex products. It demonstrates that the holder has the knowledge and skills needed to effectively use Cortex technology to detect and respond to cyber threats. Additionally, the certification can help IT professionals advance their careers by showing potential employers that they have the skills needed to secure their organization's infrastructure.

NEW QUESTION 30

Which Cortex XDR Agent capability prevents loading malicious files from USB-connected removable equipment?
* Agent Configuration
* Device Control
* Device Customization
* Agent Management

https://live.paloaltonetworks.com/t5/blogs/cortex-xdr-features-introduced-in-december-2019/ba-p/302231

NEW QUESTION 31

Whichfour types of Traps logs are stored within Cortex Data Lake?
* Threat, Config, System,Data
* Threat, Config, System, Analytic
* Threat, Monitor. System, Analytic
* Threat, Config, Authentication, Analytic

NEW QUESTION 32

If you have a playbook task that errors out. where could you see the output of the task?
* /var/log/messages
* War Room of the incident
* Demisto Audit log
* Playbook Editor

NEW QUESTION 33

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

NEW QUESTION 34

If a customer activates a TMS tenant and has not purchased a Cortex Data Lake instance.

Palo Alto Networks will provide the customer with a free instance

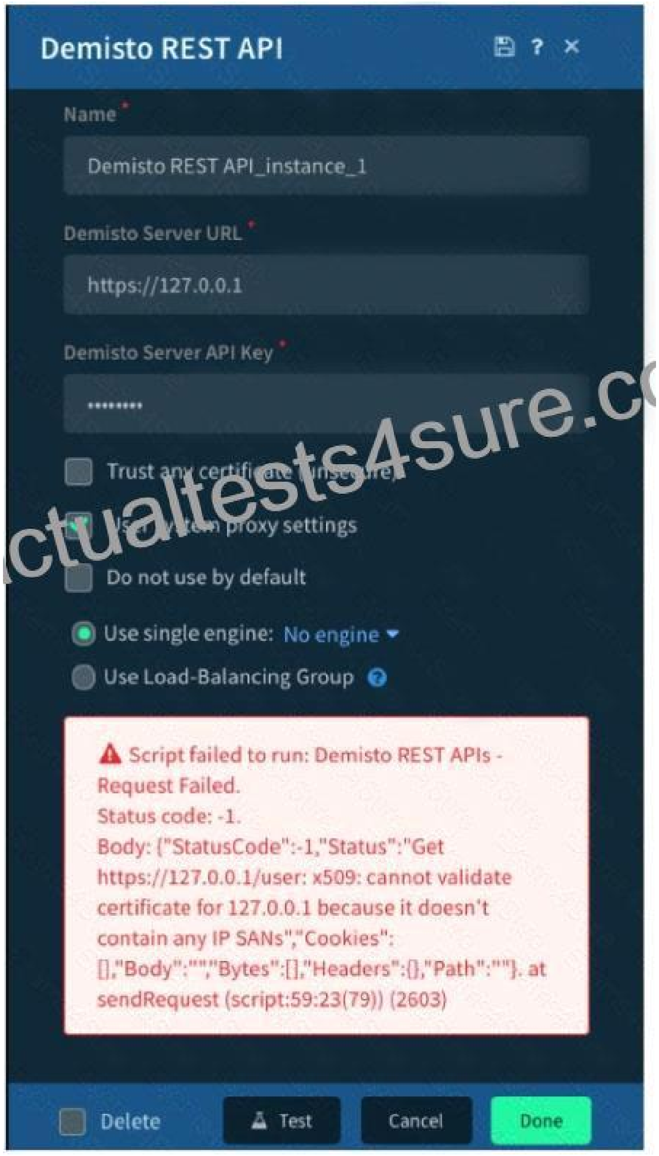
What size is this free Cortex Data Lake instance?
* 1 TB
* 10 GB
* 100 GB
* 10 TB

NEW QUESTION 35

The prospect is deciding whether to go with a phishing or a ServiceNow use case as part of their POC We have integrations for both but a playbook for phishing only Which use case should be used for the POC?
* phishing
* either
* ServiceNow
* neither

NEW QUESTION 36

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



Name *
Demisto REST API_instance_1

Demisto Server URL *
https://127.0.0.1

Demisto Server API Key *
•••••••••

☐ Trust any certificate (insecure)

☑ Use system proxy settings

☐ Do not use by default

● Use single engine: No engine

○ Use Load-Balancing Group

```
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.)

* Generic Polling Automation Playbook
* Playbook Tasks
* Sub-Play books
* Playbook Functions

NEW QUESTION 37

How do sub-playbooks affect the Incident Context Data?

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

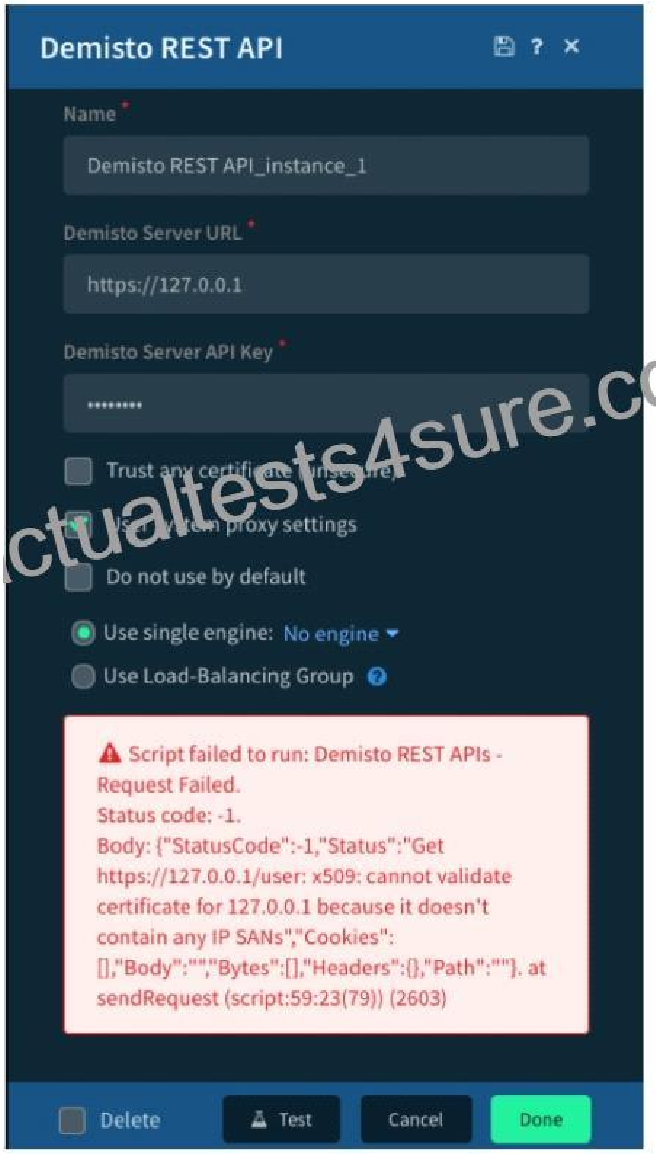
* When set to global, allows parallel task execution.
* When set to global, sub-playbook tasks do not have access to the root context

NEW QUESTION 38

Which task allows the playbook to follow different paths based on specific conditions?
* Conditional
* Automation
* Manual
* Parallel

NEW QUESTION 39

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



Demisto REST API

Name *
Demisto REST API_instance_1

Demisto Server URL *
https://127.0.0.1

Demisto Server API Key *
****

□ Trust any certificate (insecure)
☑ Use system proxy settings
□ Do not use by default

● Use single engine: No engine
○ Use Load-Balancing Group

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.)
* Generic Polling Automation Playbook
* Playbook Tasks
* Sub-Play books
* Playbook Functions

NEW QUESTION 40

&#8220;Bob&#8221; is a Demisto user. Which command is used to add &#8216;Bob&#8221; to an investigation from the War Room CLI?
* #Bob
* /invite Bob
* @Bob
* !invite Bob

NEW QUESTION 41

In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three.)
* Domain/workgroup membership
* quarantine status
* hostname
* OS
* attack threat intelligence tag

NEW QUESTION 42

How does an &#8220;inline&#8221; auto-extract task affect playbook execution?
* Doesn&#8217;t wait until the indicators are enriched and continues executing the next step
* Doesn&#8217;t wait until the indicators are enriched but populate context data before executing the next
* step. Wait until the indicators are enriched but doesn&#8217;t populate context data before executing the next step.
* Wait until the indicators are enriched and populate context data before executing the next step.

NEW QUESTION 43

Which two entities can be created as a BIOC? (Choose two.)
* file
* registry
* event log
* alert log
Explanation

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xd

NEW QUESTION 44

Which two log types should be configuredfor firewall forwarding to the Cortex Data Lake for use by Cortex XDR?(Choose two)
* Security Event
* HIP
* Correlation
* Analytics

NEW QUESTION 45

Which step is required to prepare the VDI Golden Image?
* Review any PE files that WildFire determined to be malicious
* Ensure the latest content updates are installed
* Run the VDI conversion tool
* Set the memory dumps to manual setting

NEW QUESTION 46

An antivirus refresh project was initiated by the IT operations executive. Who is the best source for discussion about the project&#8217;s operational considerations&#8217;?
* endpoint manager
* SOC manager
* SOC analyst
* desktop engineer

NEW QUESTION 47

&#8220;Bob&#8221; is a Demisto user. Which command is used to add &#8216;Bob&#8221; to an investigation from the War Room CLI?
* #Bob
* /invite Bob
* @Bob
* !invite Bob

NEW QUESTION 48

Which Cortex XDR capability extends investigations to an endpoint?
* Log Stitching
* Causality Chain
* Sensors
* Live Terminal
Explanation

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-conc

NEW QUESTION 49

If a customer activates a TMS tenant and has not purchased a Cortex Data Lake instance.

Palo Alto Networks will provide the customer with a free instance

What size is this free Cortex Data Lake instance?
* 1 TB
* 10 GB
* 100 GB
* 10 TB

NEW QUESTION 50

When a Demisto Engine is part of a Load-Balancing group it?

* Must be in a Load-Balancing group with at least another 3 members
* It must have port 443 open to allow the Demisto Server to establish a connection
* Can be used separately as an engine, only if connected to the Demisto Server directly
* Cannot be used separately and does not appear in the in the engines drop-down menu when configuring an integration instance

NEW QUESTION 51

What are two manual actions allowed on War Room entries? (Choose two.)

* Mark as artifact
* Mark as scheduled entry
* Mark as note
* Mark as evidence

NEW QUESTION 52

Which process in the causality chain does the Cortex XDR agent identify as triggering an event sequence?

* the relevant shell
* The causality group owner
* the adversary&#8217;s remote process
* the chain&#8217;s alert initiator

The PSE-Cortex exam is designed to validate an individual's knowledge and skills in deploying, configuring, and troubleshooting Cortex XDR, Cortex Data Lake, and Cortex XSOAR. This certification is highly regarded in the cybersecurity industry and is recognized by major organizations and employers worldwide.

Full PSE-Cortex Practice Test and 60 Unique Questions, Get it Now!:
https://www.actualtests4sure.com/PSE-Cortex-test-questions.html]