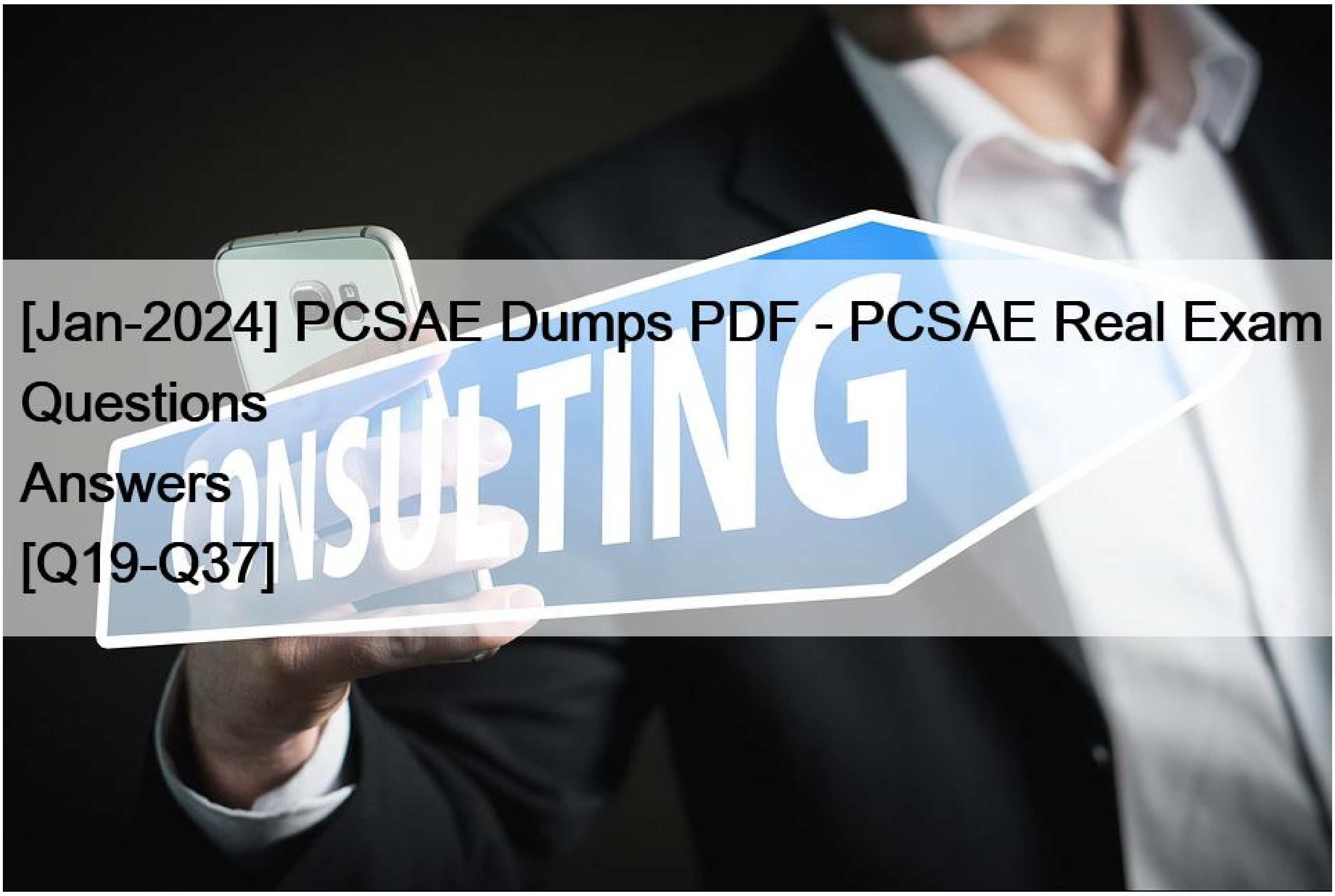
# [Jan-2024 PCSAE Dumps PDF - PCSAE Real Exam Questions Answers [Q19-Q37



[Jan-2024] PCSAE Dumps PDF - PCSAE Real Exam Questions Answers
PCSAE Dumps 100% Pass Guarantee With Latest Demo

**Q19.** What can you use to assign a layout, field, and playbook to an incoming incident?
* Playbook
* Classification and mapping
* Incident type
* Pre-processing

**Q20.** What are two primary uses of standard tasks? (Choose two.)
* To highlight different paths in a playbook
* To generate new widgets for a dashboard
* To create an incident or escalate an existing incident
* To automate tasks such as parsing a file or enriching indicators

**Q21.** On the System Diagnostics page, what is the default minimum size for a Work Plan to be considered big?
* 2MB

* 3MB
* 1MB
* 5MB

**Q22.** A playbook task generates a report as HTML in the context data.

An engineer creates a custom indicator field of type &#8220;HTML&#8221; and adds the field to a section in a custom indicator layout. How can the engineer populate the HTML field in the indicator layout?
* Populate the custom indicator field with the built-in !SetIndicator command.
* Add HTML to a list using !setList and use it as an HTML template to populate the custom indicator field.
* Create a custom Indicator Mapper and populate the custom indicator field.
* Use the Mapping option in the playbook task that generates the HTML report to populate the custom indicator field.

**Q23.** An engineer would like to add a custom field to the New Job form for a job triggered from a threat intel feed.

How would the engineer implement this?
* The new job form changes based on the threat intel feed integration configuration
* The new job form can be edited from the Indicator Feed incident type editor
* The new job form for a threat intel feed job cannot be edited
* The new job form can be edited from the threat intel feeds integration settings

**Q24.** Which two causes may be occurring if an integration test is working, but the integration is not fetching incidents? (Choose two.)
* The &#8216;Fetches Incidents&#8217; option may not have been enabled
* There are no new events from the external service
* The first fetch should be manually triggered to start the fetching process
* It can take up to 1-hour before incidents are initially fetched

**Q25.** A SOC manager built a dashboard and would like to share the dashboard with other team members. How would the SOC manager create a dashboard that meets this requirement?
* Manually share the dashboard through user emails
* Dashboard is shared to all XSOAR users
* Propagate the dashboard based on SAML authentication
* Dashboard is shared to all XSOAR users in a selected role

**Q26.** Where would you look to find a personalized view of your own incidents and tasks?
* Incident Summary View
* My Incidents
* My Threat Landscape
* My Dashboard

**Q27.** Which of the following are valid methods to contribute custom content? (Choose three.)
* Submit content directly through feature requests
* Private GitHub repository submission for premium content
* A Github pull request on the public XSOAR Content Repository
* Using the marketplace interface to upload the content
* Using the content submission tool on live.paloaltonetworks.com

**Q28.** What is a primary use case of data collection tasks?
* To allow multi-question surveys without authentication restrictions

* To automate tasks such as parsing a file or enriching indicators
* To generate new widgets for a dashboard
* To determine different paths in a playbook

**Q29.** In which two scenarios would it be appropriate to implement a loop for a sub-playbook? (Choose two.)
* In repetitive process flows to iterate for each playbook input
* When continuously ingesting incidents from third-party systems
* In repetitive process flows with no more than 10 loops
* In repetitive processes that requires sub-playbook re-execution

**Q30.** What will happen if a playbook debugger is left running for more than 24 hours?
* By default, every 24 hours, the system closes any debugger sessions that have been open for more than 180 minutes.
* The session must be stopped during 180 minutes manually by administrator, user will receive notification automatically.
* The session will be running till stopped manually by administrator.
* By default, the system closes automatically any debugger session that have been open 180 minutes.

**Q31.** A large number of incidents were deleted by mistake.

Which two architecture components can be used to recover the lost data? (Choose two.)
* Live backup
* Engine
* Distributed database
* Local backup
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-6/cortex-xsoar-admin/disaster-recovery-and-live-backup/backup-the-database.html

**Q32.** Management would like to get an incident report automatically following an incident&#8217;s closure. How would this be accomplished?
* Define a task in a playbook to generate an incident report before the closure occurs
* Manually create an &#8216;Incident Report&#8217;
* Configure post-processing using a script
* Create an &#8216;Incident Report&#8217; from the Reports page

**Q33.** Multiple company assets were reported by vulnerability scanners as being vulnerable to CVE-2017-11882. This vulnerability affects applications installed on workstations. The SOC team needs to take action and apply the new vulnerability patch that was just released. The team must first create a cause for each of the identified assets in ServiceNow IT Service Management (ITSM), in order to notify the IT department. Next, the team creates a task in the main playbook, which extracts the list of assets from the scanner report.

After the list of assets are created, what are the two solutions that the SOC team could take so that a case could be created and a patch installed? (Choose two.)
* Create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Condition: AreValuesEqual &#8211; Exit on yes &#8211; left:1, right 1) and perform the following tasks:

&#8211; Active Directory User Enrichment based on the computerName

&#8211; Create the ServiceNow Record by adding the enrichment information

&#8211; Mark the ticket severity as Urgent
* Create a sub-playbook with a single input containing the computer names that will loop &#8216;For Each Input&#8217; and

perform the following tasks:

&#8211; Active Directory User Enrichment based on the computerName

&#8211; Create the ServiceNow Record by adding the enrichment information

&#8211; Mark the ticket severity as Urgent
* Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator contains the count of the number of items in the list) and perform the following tasks:

&#8211; Active Directory User Enrichment based on the computerName

&#8211; Create the ServiceNow Record by adding the enrichment information

&#8211; Mark the ticket severity as Urgent
* Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator equal to count of the number of item in the list) and perform the following tasks:

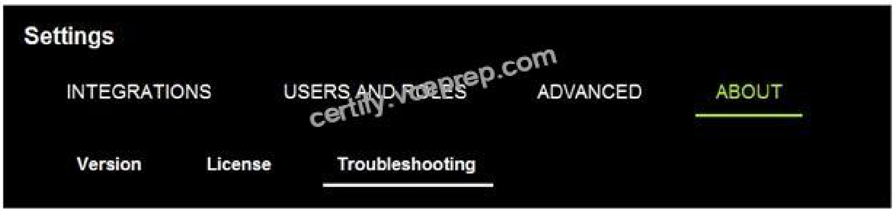
&#8211; Increase the iterator value by one each time

&#8211; Active Directory User Enrichment based on the computerName

&#8211; Create the ServiceNow Record by adding the enrichment information
&#8211; Mark the ticket severity as Urgent

**Q34.** An engineer would like to change an incident&#8217;s SLA according to the severity field changes. How can the engineer achieve this task?
* Use a field trigger script
* Use a field display script
* Create a job that queries for incident severity changes
* Change the SLA manually every time the severity changes

**Q35.** Which three actions can an engineer take on the troubleshooting page? (Choose three.)



* Download the debug log bundle
* Put the XSOAR server in maintenance mode
* View and modify server configuration settings
* Export and import custom content
* View a list of server administrators

**Q36.** How can Cortex XSOAR administrators prevent junior analysts from viewing a senior analyst dashboard?
* Share the dashboard in Read and Edit mode for senior analysts.
* Share the dashboard in Read & Edit mode for senior analysts and Read Only for juniors analysts.
* Share the dashboard in Read and Write mode for senior analysts.
* Share the dashboard in Read Only mode for junior analysts and senior analysts.

**Q37.** An engineer is developing a playbook that will be run multiple times for testing purposes. What is the recommended first task to be used in the playbook?
* DeleteContext
* GenerateTest
* PrintContext
* SetContext

**Dumps Real Palo Alto Networks PCSAE Exam Questions [Updated 2024:** https://www.vceprep.com/PCSAE-latest-vce-prep.html]