check

1.

It is possible to import or export a Dashboard

check

True

False

This answer is correct.

close

2.

Where can you check all Active System Modules?

Permissions

License Management

close

Ontology

Integrations

This answer is not correct. Go back and review the module.

close

3.

A playbook will only run if its priority is defined within the logic

close

True

False

This answer is not correct. Go back and review the module.

check

4.

Analysts can communicate with any internal Chronicle SOAR user as part of the platform

check

True

False

This answer is correct.

check

5.

Playbook actions can be configured to be executed automatically or manually.

check

True

False

This answer is correct.

check

6.

Which Flow step requires an analyst to manually answer a question?

check

MultiChoiceQuestion

Previous Actions Conditions

Condition

This is the correct answer.

check

7.

You can uninstall an integration that has a dependable playbook

False

check

True

This answer is correct.

check

8.

A "Trigger" is the very first step in each playbook

False

check

True

This answer is correct.

check

9.

You need to configure an integrations before using it with the downloaded use cases

check

True

False

This answer is correct.

check

10.

When selecting an active incident within Command Center, what filters can be applied under Workstation tab?

Time

Department

Collaborator

check

All of the above

This is the correct answer.

close

11.

Where can you find an execution log of an Alert?

Case

Chronicle SOAR blog

Problem

close

Action

This answer is not correct. Go back and review the module.

check

12.

\_\_\_\_\_\_ allows you to ingest raw source data into the platform?

check

Connector

Ontology Mapping

Jobs

IDE

This is the correct answer.

check

13.

Which widget includes a visual graph of the Case Entities?

Alert Graph

check

Entities Graph Widget

MITRE Graph Widget

Case Graph Widget

This is the correct answer

check

14.

In playbook designer when you toggle the "Simulator" button what is the expected behavior?

check

The playbook can now be tested with simulated alerts.

To enable the simulator option the playbook requires Admin privileges.

It can only be enabled in a test environment.

The playbook will simulate an attack on target device.

This is the correct answer.

check

15.

Do you require multiple dashboards in order to configure data widgets that show results from multiple Environments?

True

check

False

This answer is correct.

check

16.

Conditions are built based on case data such as the following

Cases

Events

check

All of the above

Alerts

Environment

Entities

This answer is correct.

check

17.

White text within Chronicle SOAR Mapping represents

Field not mapped

Field mapped and Event has data

check

Field mapped and no data in event

This is the correct answer.

check

18.

Which hierarchy is correct for Ontology?

Event->Product->Source

check

Source->Product->Event

Source->Event-> Product

Event->Source->Product

This is the correct answer.

close

19.

All playbook triggers except "All" can be scoped with the following parameters: (select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

check

"() Contains"

This is a correct answer.

"=> More than or Equal to"

check

"\*\_Starts With"

This is a correct answer.

"= Equal"

check

20.

Blocks can be used for

Condition features

Insight features

check

Repeatable actions

This is the correct answer.

close

21.

Can a user have restrictions to view certain environments within platform?

close

False

True

This answer is not correct. Go back and review the module.

check

22.

When a playbook is activated, the toggle next to a playbook name appears green

check

True

False

This answer is correct.

check

23.

Can report templates be downloaded form the Chronicle SOAR Marketplace?

check

True

False

This answer is correct.

check

24.

Who typically has sufficient rights to turn off the "simulator" mode? (select all that apply)

check

Admin

This is a correct answer.

SOC Analyst

check

SOC Manager

This is a correct answer.

None of these roles

check

25.

You are limited to inviting internal users to the Command Center when collaborating on incidents

check

False

True

This answer is correct.

close

26.

Which of the following fields are displayed under "Entities Highlights" section? (select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

Email Subject

File Name

check

User Name

This is a correct answer.

check

IP Address

This is a correct answer.

check

27.

Can PowerUp integration help you enhance your playbook capabilities?

check

True

False

This answer is correct.

check

28.

A "Playbook" can only be attached to a specific Environment

check

False

True

This answer is correct.

check

29.

In Command Center, when creating a new status assessment, can you add a severity above 100?

True

check

False

This answer is correct.

close

30.

What tabs are available within Homepage? (select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

My Cases

check

My Tasks

This is a correct answer.

Completed Actions

Announcements

check

Pending Actions

This is a correct answer.

close

Your Cases

This answer is not correct. Go back and review the module.

check

Workspace

This is a correct answer.

close

31.

When installing an integration (select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

Simply click the download button for your selected integration.

check

Check if you require subscription for the integration to work optimally within Chronicle SOAR.

This is a correct answer.

close

Ensure the integration is compatible for your Chronicle SOAR version before downloading.

This answer is not correct. Go back and review the module.

To download community edition you need permission from the creator.

close

32.

\_\_\_\_\_\_ alloWhen a playbook is activated, the toggle

close

Actions

Blocks

Events

Playbooks

This answer is not correct. Go back and review the module.

close

33.

What can you find within the Chronicle SOAR Marketplace? (select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

Phishing Alert Tips

check

Integrations

This is a correct answer.

check

Power Ups

This is a correct answer.

Analytics

close

Vendors

This answer is not correct. Go back and review the module.

close

34.

What are the mandatory checks required for installing a Use Case? (Select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

Ensuring a test environment exists before downloading the use case.

check

Configuration of integrations

This is a correct answer.

close

Enabling simulations before downloading the integration.

This answer is not correct. Go back and review the module.

check

Selection of integrations

This is a correct answer.

check

35.

When creating a playbook if you select "All Environments" button, what does such scope mean?

The function will run all the time regardless of the playbook selection.

The function will run on all current Environments.

check

This function created within playbook will run on all current environments as well as on all future environments.

The function will run on all future Environments.

This is the correct answer.

check

36.

In case of multiple matches for an Alert, which Playbook priority determines precedence?

None of the above

Second

Third

check

First

This is the correct answer.

check

37.

A playbook can be attached to all Environments within the platform

False

check

True

This answer is correct.

close

38.

What type of activities can be added by collaborators to the Command Center workstation?

Assessment

Fact

close

Task

Fact

Key Items

All of the above

This is not the correct answer.

close

39.

A manual action within a playbook can be identified by

"MAN" letters

close

Hand symbol

"M" letter

The purple color

This answer is not correct. Go back and review the module.

close

40.

What is available under Configuration tab? (Select all that apply)

info

Note: To get credit for a multiple-select question, you must select all of the correct options and none of the incorrect ones.

check

Jobs

This is the correct answer.

close

Playbooks

This answer is not correct. Go back and review the module.

check

Connectors

This is the correct answer.

Settings

close

41.

Red text within Chronicle SOAR Mapping represents

close

Field mapped and no data in event

Field mapped and Event has data

Field not mapped

This answer is not correct. Go back and review the module.

check

42.

By specifying a particular \_\_\_\_\_\_ field or general output of an action, you can create condition within a playbook.

check

JSON

HTTP

Visualization

Actions

This is the correct answer.

check

43.

A case tag can be added to high priority alerts only?

True

check

False

This answer is correct.

check

44.

Green text within Chronicle SOAR Mapping represents

Field not mapped

check

Field mapped and Event has data

Field mapped and no data in event

This is the correct answer.

close

45.

What module should be used within Chronicle SOAR to monitor health checks and synchronization tasks?

Jobs

Integrations

close

Insights

Connectors

This answer is not correct. Go back and review the module.

check

46.

Multiple incidents can be transferred into the Command Center from a single or multiple Environments

False

check

True

This answer is correct.