IBM Cloud Pak for Security V1.x Administrator Specialty (S1000-001)

Issued by IBM Professional Certification

This IBM Cloud Pak for Security v1.x Administrator Specialty has knowledge and experience with Cloud Pak for Security. This administrator is capable of performing basic tasks related to the daily management and operation, configuration, security and/or problem determination. They have an understanding of the security structure of their organization. This entry level administrator is working in a production environment of IBM Cloud Pak for Security.

A candidate for IBM Cloud Pak for Security v1.x Administrator Specialty has knowledge and experience with Cloud Pak for Security. This administrator is capable of performing basic tasks related to the daily management and operation, configuration, security and/or problem determination. They have an understanding of the security structure of their organization. This entry administrator is working in a production environment of Cloud Pak for Security.

Assumptions:

- The Cloud Pak for Security infrastructure has been deployed and configured.
- This individual is not the lead administrator
- This individual is not expected to code.
- This is not a sales exam.
- Basic knowledge of Red Hat OpenShift
    - Kubernetes and OpenShift: What's the Difference (https://youtu.be/cTPFwXsM2po)
    - OpenShift for Beginners (https://youtu.be/Ut2IA4bA-g8)
    - OpenShift Container Platform by RedHat (https://youtu.be/XD8Xnjpdrgs)

Register for the Certification Exam: https://home.pearsonvue.com/ibm Please ensure that you Person/VUE IBM candidate ID is "connected" to your IBM Business Partner Profile. This is the ONLY way that IBM will accept this credential for enhanced program incentives (margin opportunities). ALSO – you MUST accept your "badge" issued by Acclaim or the credentials won't flow properly.

Section 1 - Cloud Pak for Security Overview

Task 1.1 Describe the Cloud Pak for Security component stack

Subtask:

1.1.1 Red Hat OpenShift version 4.3

- 1.1.1.1 Container Platform

1.1.2 Cloud Pack Common services

- 1.1.2.1 Logging
- 1.1.2.2 Identity and Access
- 1.1.2.3 Monitor
- 1.1.2.4 Metering
- 1.1.2.5 Persistent Storage
- 1.1.2.6 Docker Registry/Helm
- 1.1.2.7 Security

1.1.3 Cloud Pack for Security Core Services

- 1.1.3.1 UDI (Universal Data Insights)
- 1.1.3.2 Connected Assets and Risk (CAR)
- 1.1.3.3 Analytics Tool Kit (ATK)

1.1.4 Cloud Pack for Security Apps

- 1.1.4.1 Data Explorer
- 1.1.4.2 Threat Intelligence Insights
- 1.1.4.3 Cases with Orchestration and Automation

1.1.5 Unified Workflow (UX)

1.1.6 Cloud Pack for Security (Cloud Pak for Security v1.3)

References: https://www.securitylearningacademy.com/course/view.php?id=5129

https://www.ibm.com/support/knowledgecenter/SSHKN6/kc_welcome_cs.html

Task 1.2. Summarize the basic terms for Cloud Pak for Security

Subtask:

1.2.1 STIX2 and STIX-shifter

1.2.2 Data Source

1.2.3 Playbooks (dynamic playbooks)

1.2.4 Threat Score

1.2.5 cloudctl

1.2.6 oc (openshift command line)

1.2.7 kubectl

1.2.8 pod

References:

https://github.com/opencybersecurityalliance/stix-shifter/blob/master/OVERVIEW.md

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/resilient/playbook/resilient_playbook_intro_playbooks.html

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/data-sources.html

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/threat-intelligence-insights/threat-scores.html

Task 1.3. Describe IBM Cloud Pak for Security core services and the applications

Subtask:

1..3.1 Universal Data Insights (UDI)

1.3.2 Connected Assets and Risk (CAR)

1.3.3 Analytics Tool Kit (ATK)

1.3.4 Data Explorer

    1.3.4.1 Query builder

1.3.5 Threat Intelligence Insights

1.3.6 Cases with Orchestration and Automation

References:

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/resilient/Resilient_SOAR.html

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/data-explorer/overview.html

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/threat-intelligence-insights/overview.html

https://www.securitylearningacademy.com/course/view.php?id=5129

https://www.ibm.com/support/knowledgecenter/SSHKN6/kc_welcome_cs.html

Task 1.4. Summarize the dependencies on Red Hat OpenShift and ICP common services

Subtasks:

1.4.1 Red Hat OpenShift

- 1.4.1.1 Persistent Storage
- 1.4.1.2 Monitoring

1.4.2 ICP Common Services

- 1.4.2.1 Logging
- 1.4.2.2 Identity and Access
- 1.4.2.3 Metering
- 1.4.2.4 Docker Registry/Helm
- 1.4.2.5 Security

References:

https://www.securitylearningacademy.com/enrol/index.php?id=5129

https://www.securitylearningacademy.com/course/view.php?id=5262

Task 1.5. Describe the basic characteristics of case management to include dynamic playbooks, roles, and automation.

Subtasks:

1.5.1 Rules

1.5.2 Conditions and Activities

1.5.3 Business Logic

1.5.4 Workflows

1.5.5 Tasks

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/resilient/playbook/resilient_playbook_intro_playbooks.html

Task 1.6. Describe the functionality of threat intelligence insights

Subtasks:

1.6.1 IBM-Derived TI across:

1.6.1.1 Threat Activity

1.6.1.2 Threat Groups

1.6.1.3 Malware

1.6.1.4 Industries

1.6.2 Am I Infected

1.6.3 Threat Scoring/Prioritization

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/threat-intelligence-insights/overview.html

Task 1.7. Describe the different Threat Intelligence Insight plans

Subtasks:

1.7.1 Standard (part of initial installation)

1.7.2 Advanced (additional functionality and feeds)

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/package-selection.html

Task 1.8. Describe a data connector

Subtasks:

1.8.1 Define purpose of a Data Connector

1.8 .1.1 Types of Data Sources a Data Connector can interface with (database, XML file, application (IBM and third-party) STIX bundle)

1.8.2 Types of Data Connectors

1.8 .2.1 Predefined applications (IBM QRadar, IBM Guardium, QRoC, Splunk, Elasticsearch, Carbon Black, BigFix, MS ATP, etc)

1.9.2.2 STIX Bundle

1.8 .2.2.1 Types of information that can be shared using STIX Objects

1.8.2.3 Proxy data source

1.8.2.3.1 New connector (development and testing) using the STIX-shifter project.

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/data-sources.html

Section 2 Cloud Pak for Security Administration

Task 2.1. Describe how to validate and install the various Cloud Pak for Security license modules, upgrade options and the additional apikeys

Subtasks:

2.1.1 Entitlements

2.1.1.1 SOAR Capabilities

2.1.2 Threat Intelligence Insights

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/resilient/admin/API_accounts.html

https://www.securitylearningacademy.com/course/view.php?id=5262

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/package-advanced.html

Task 2.2. Create a new user

Subtasks:

2.2.1 Describe Steps to validate and verify LDAP authentication to Cloud Platform Common Services cluster

2.2.2 Define three levels of user administration

2.2.2.1 LDAP, ICP Common Services, Cloud Pak for Security Platform

2.2.3 Describe procedure to grant a user access to Cloud Pak for Security

References:

https://www.securitylearningacademy.com/course/view.php?id=5171
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/security-pak/ldap-connect.html
https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/users.html
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/security-pak/users_scp.html

Task 2.3. Define a user role

Subtasks:

2.3.1 Describe capabilities of Cloud Pak for Security supported Platform services roles

2.3.1.1 User (Cloud Platform Common Services Viewer role) Admin (CPCS Administrator role)

2.3.2 Describe capabilities of Cloud Pak for Security supported Application roles

2.3.2.1 (Case Management, Data Explorer, Data Sources, Data Sources, Orchestration & Automation, Threat Intelligence Insights)

2.3.3 Describe procedure for creating an application roles

2.3.4 Describe procedure for creating an platform services role

To be included in 2.3 .Summarize the entitlements for the Cloud Pak for Security modules.

Subtasks:

1.5.1 Data Explorer

1.5.2 Threat Intelligence Insights

1.5.2.1 Basic versus advanced

1.5.3 Orchestration & Automation

1.5.3.1 Cases

1.5.3.2 SOAR

References:

https://www.securitylearningacademy.com/course/view.php?id=5262

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/cp4s_v1r3/docs/security-pak/license_UI.html

https://www.securitylearningacademy.com/enrol/index.php?id=5215

References:

https://www.securitylearningacademy.com/course/view.php?id=5171
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/users.html
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/access-permissions.html

Task 2.4. Add a user to a defined groups

Subtasks:

2.4.1 Describe purpose of Groups in SOAR

2.4.1.1 Describe where groups are not available

2.4.2 Describe steps to change case groups or roles

References:

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/resilient/admin/resilient_m_admin_settings_groups.html
https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.3.0/resilient/admin/resilient_m_admin_settings_users_change.html

Task 2.5. Use a data connector

Subtasks:
2.5.1 Describe the steps to configure a application data source
2.5.1.1 Configure the connection.
2.5.1.2 Set the query parameters.
2.5.1.3 Configure identity and access.
2.5.1.4 Add a connection certificate.
2.5.1.5 Import asset data.
2.5.2 Describe the steps to configure a STIX Bundle data source
2.5.3 Describe the steps to configure a Proxy data source

References:

https://www.ibm.com/support/knowledgecenter/en/search/data%20connector?scope=SSTDPP_1.3.0
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/data-sources.html
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/data-sources-stix.html
https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/data-sources-proxy.html

Task 2.6. Manage the Resilient app host integration with Cloud Pak for Security

Subtasks:

References:

Task 2.7. Manage the QRadar Proxy App

Subtasks:

References:

Section 3 Cloud Pak for Security Operation

Task 3. 1. Define basic protocols and topology used by data sources

Subtasks:

3.1.1 Define the topology of Cloud Pak for Security Connectors

3.1.2 Define a use of Data Connector to connect Data Sources

References:

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.1.0/docs/scp-core/data-sources-qradar.html?view=kc

Task 3. 2. Identify dependencies to configure Data Connector

Subtasks:

3.2.1 How to obtain API Keys

3.2.2 How to obtain Authentication Tokens

3.2.3 Understand Permissions required to configure Connector

3.2.4 Understand Access credentials required on Data Source

References:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.1.0/docs/scp-core/users.html

Task 3. 3. Describe how to use a Cloud Pak for Security applications

Subtasks:

3.3.1 Describe the functions of the Data Explorer session

- 3.3.1.1 Describe the function of a data query

3.3.2 Describe the functions an incident response process

- 3.3.2.1 Fundamentals of Workflow
- 3.3.2.2 Functions of Dynamic Playbook
- 3.3.2.3 Define Use Case

3.3.3 Describe the functions of the TII session

- 3.3.3.1 Fundamentals of the Threat Investigation using

References:

https://www.securitylearningacademy.com/course/view.php?id=4696

Task 3. 4. Manage the backup and restore process for Cloud Pak for Security

Subtasks:

3.4.1 List the data stores that are backed up using the native Cloud Pak for Security backup function

- 3.4.1.1 CouchDB (main datastore)
- 3.4.1.2 ArangoDB (graph for CAR)
- 3.4.1.3 PostgreSQL (case management)

3.4.2 Differentiate between which data available for backup and restore

- 3.4.2.1 Included
  - 3.4.2.1.1 Users and their entitlements/permissions
  - 3.4.2.1.2 Data source connections and configurations
  - 3.4.2.1.3 Case management data
- 3.4.2.2 NOT Included
  - 3.4.2.2.1 LDAP configuration (this is at the ICP level)

3.4.2.2.2 Data Explorer query results, even if they are stored with Cases

3.4.3 Describe the role of the toolbox pod in the backup and restore process

3.4.3.1 Pre-built pod that contains all the utilities needed for backup and restore

3.4.3.2 Location for the PVC where backup objects are stored

3.4.3.3 Executor of the backup and restore scripts (CouchDB, ArangoDB, and Case Management)

References:

https://www.ibm.com/support/knowledgecenter/SSTDPP_1.3.0/cp4s_v1r3/docs/scp-core/backup-intro.html

3.5 Manage widgits and dashboards in Cloud Pak for Security

Subtasks:

3.5.1 Widgets

3.5.1.1 Add widgets

3.5.1.2 Edit widgets

3.5.2 Dashboards

3.5.2.1 Manage Dashboards

Reference:

https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.4.0/platform/docs/p-dashboard/dashboard_intro.html

Section 4 Cloud Pak for Security Problem Determination

Task 4.1. Troubleshoot user permission issues

Subtasks: (examples below – please add and verify)

4.1.1 User roles

4.1.2 User groups

References:

Task 4.2.Troubleshoot connection and data gathering from the data source

Subtasks:

4.2.1

References: