IBM Professional Certification Program

Exam S1000 – 001 IBM Cloud Pak for Security V1.X Administrator Specialty

1. On which container platform can IBM Cloud Pak for Security be installed?

A. LXC
B. Docker
C. Solaris Zones
D. Red Hat OpenShift

2. What best describes a dynamic playbook in IBM Cloud Pak for Security?

A. A script used to perform daily backup and log gathering routines.
B. A set of rules, conditions, business logic, workflows and tasks used to respond to a case.
C. The Threat Intelligence Insights automated scanning process to scan a set of data sources.
D. A SOC analyst tool to assist in connecting to data sources for retrieval of search results.

3. Which Cloud Pak for Security service is used to share and provide asset and risk information to enable a better understanding of the clients' environment and risk posture?

A. Analytics Toolkit
B. Connected Assets and Risk
C. Threat Intelligence Insights
D. Consolidated Assets and Risk management

4. How many worker nodes are required to run IBM Cloud Pak for Security V1.4 on IBM Cloud?

A. 2
B. 4
C. 6

D. 3

5. Which feature helps test dynamic playbooks in the Cases application of IBM Cloud Pak for Security?

A. Workflow
B. Simulation
C. Automated rule
D. Connected Asset & Risk

6. What are two main contributors to the prioritization of threats within Threat Intelligence Insights (TII)?

A. asset profile
B. security control gaps
C. organizational profile
D. environmental telemetry
E. TII advanced subscription

7. What changes when a SOAR license is installed on IBM Cloud Pak for Security?

A. Script modules in the playbooks can be used.
B. A new Incident Type for a playbook can be defined.
C. The Automation and Orchestration App Host can be installed.
D. The access to the Automation and Orchestration > Permissions and Access page is enabled.

8. What happens when a user is removed from IBM Cloud Pak for Security using the User Management page?

A. The user profile is removed and they cannot log back in to IBM Cloud Pak for Security.
B. The user is removed from the LDAP repository and they cannot log back in to IBM Cloud Pak for Security.
C. The user cannot log back in to IBM Cloud Pak for Security and their access to the platform cannot be restored.
D. The user is removed from IBM Cloud Common Platform Services, but they are kept in the LDAP. The user cannot log back in to IBM Cloud Pak for Security.

9. What the minimum privilege role required to run an *Am I Affected* scan?

A. Platform Admin role
B. Standard Package role
C. Threat Intelligence Insights User role
D. Threat Intelligence Insights Admin role

10. When creating a group, what functionality is enabled when the *Allow Incident Ownership* box is selected?

A. It allows this group to own incidents.
B. It allows an incident to have an owner.
C. It allows a specific user to own incidents.
D. It allows only this group to have ownership of incidents.

11. What is a data connector in IBM Cloud Pak for Security?

A. A user interface to visualize threat intelligence insights.
B. An API to search and store threat intelligence data in IBM Cloud Pak for Security.
C. A definition that bridges repositories of cybersecurity data to IBM Cloud Pak for Security.
D. A plugin that connects and stores security data in cloud to power the dashboards in IBM Cloud Pak for Security.

12. Which two communication protocols are used between an App Host and an IBM Cloud Pak for Security the Orchestration & Automation app?

A. SSH
B. SMTP
C. AMQP
D. STOMP
E. Rest API

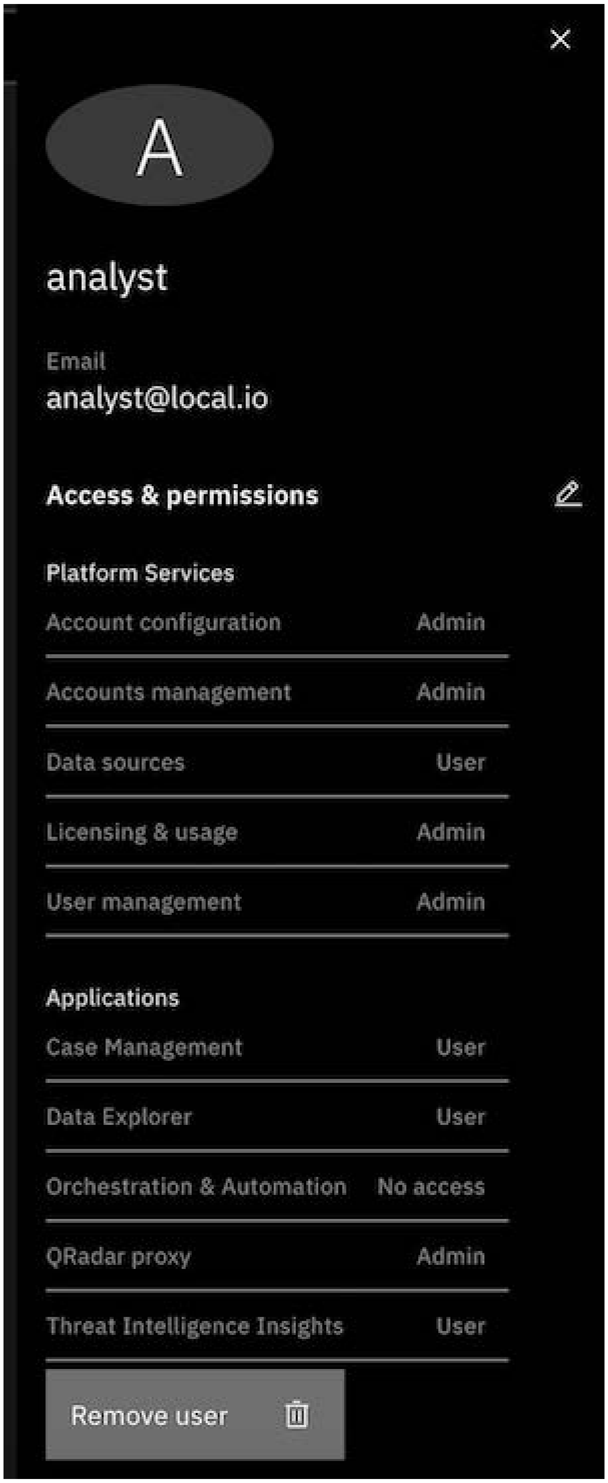
13. Which application within IBM Cloud Pak for Security is focused on incident investigation?

A. Data Explorer
B. Analyst Toolkit
C. Connected Asset & Risk
D. Threat Intelligence Insights

14. When performing backup, which statement is true for user entitlements?

A. Only user entitlements are part of the backup and restore process.
B. Only LDAP configurations are part of the backup and restore process.
C. LDAP configurations and user entitlements are not part of the backup process.
D. LDAP configurations and user entitlements are part of the backup and restore process.

15. Based on the image, to which section does the user have limited access?



analyst

Email
analyst@local.io

Access & permissions

Platform Services

Account configuration	Admin
Accounts management	Admin
Data sources	User
Licensing & usage	Admin
User management	Admin

Applications

Case Management	User
Data Explorer	User
Orchestration & Automation	No access
QRadar proxy	Admin
Threat Intelligence Insights	User

A. Data sources
B. User management
C. Accounts management

D. Account configuration

Answer Key:

1.	D
2.	B
3.	B
4.	D
5.	B
6.	CD
7.	A
8.	A
9.	C
10.	A
11.	C
12.	DE
13.	A
14.	A
15.	A