TD SYNNEX

IBM Cloud Pak for Security Specialty Exam Enablement S1000-001

Marshall Hall
Field Solutions Architect

Focus Areas Highlighted with Stars

Practice Questions

1. What capabilities does Cloud Pak for Security bring together?
   a. EDR
   b. Datalake and UBA
   c. SIEM and Identity
   d. All of the above

2. Which OpenShift configuration would be used when logging is required?
   a. 3 Masters (8 Cores,32 GB Mem) and 4 Workers (8 Cores, 32 GB Mem)
   b. 4 Workers (8 Cores, 32 GB Mem) only
   c. 3 Masters (8 Cores,16 GB Mem) only
   d. 3 Masters (8 Cores,16 GB Mem) and 4 Workers (8 Cores, 32 GB Mem)

3. Which CP4S component consolidates asset and risk data to identify security gaps?
   a. Connect Asset & Risk (CAR) Database
   b. Connect Asset & Risk (CAR) Dataset
   c. Consolidated Asset & Risk (CAR) Database
   d. Asset Risk & Threat (ART) Database

4. Which 3 fields are needed to collect the mustgather? (select 3)
   a. cpctl tool
   b. Namespace
   c. Modules
   d. Token

5. Which of the following are data query parameters?
   a. Connection name, connection description, hostname, port
   b. Concurrent search limit, SEC Token, result size limit, Secret Key
   c. Tenant ID, connection description, Secret, port
   d. Concurrent search limit, query search timeout, result size limit, query time range

6. What are the required general fields for a QRadar data connection?
   a. Concurrent search limit, query search timeout, result size limit, query time range
   b. Connection name, connection description, hostname, port
   c. Tenant ID, connection description, Secret, port
   d. Concurrent search limit, SEC Token, result size limit, Secret Key

7. What application role can assign access to Threat Intelligence Insights (TII)?
   a. TII Administrator and Data Explorer Administrator
   b. TII User
   c. Data Explorer User
   d. Platform Role Administrator

8. Asset Data must be configured separately for each connector?
   a. True
   b. False

9. What type of certificate is required for a CP4S installation not on IBM Cloud?
   a. Hypertext Transfer Protocol Secure (HTTPS) Certificate
   b. Public Key infrastructure (PKI) Certificate
   c. Transport Layer Security (TLS) Certificate
   d. Secure Sockets Layer (SSL) Certificate

10. Compete the following statement. 'IBM Cloud Pak for Security provides a platform ___ _?
   a. to manage all platforms from anywhere.
   b. to undertake costly migration projects, complex integrations, and continuously switch between different screens and products.
   c. to help more quickly integrate your existing security tools to generate deeper insights into threats across hybrid, multicloud environments, using an infrastructure-independent common operating environment that runs anywhere.
   d. to move client operations to the cloud piece by piece, with applications and data spread across multiple clouds and on-premise resources.

11. What is included with Threat Intelligence Insight's standard package?
   a. Access X-Force threat intelligence content with manually and automated threat scanning
   b. Access X-Force threat intelligence premium content and automated threat scanning
   c. Access X-Force threat intelligence premium content, the ability to manually to scan for threats, and automated threat scanning
   d. Access X-Force threat intelligence content and the ability to manually to scan for threats

12. Which dashboards have widgets that are read-only?
    a. Threat Intelligence Insight, QRadar, Case Management
    b. Connect Asset Risk, Risk Manager
    c. QRadar Proxy, Case Management

13. When a user is granted access to a data source, which roles can be assigned?
    a. Admin, user, no access
    b. Operator, admin, user
    c. Owner, viewer, no access

14. Which statement about a Fred's entitlement to multiple apps in Cloud Pak for Security is true??
    a. Fred cannot be assigned as Admin in more than one app.
    b. Fred can be assigned Admin id App A and User in App B.
    c. Fred must be assigned a user in app a if he is already a user in App B.

15. What must you obtain from QRadar to access QRadar data in Cloud Pak for Security dashboard widgets?
    a. Qradar username and password
    b. Server name indicator
    c. Qradar authorized service token

16. What is the time range for overnight automated Am I Affected scans when the Threat Intelligence Insights Advanced plan is active?
    a. 12 hours
    b. 72 hours
    c. 24 hours

17. What is excluded from a backup of Data Explorer?
    a. query results
    b. queries
    c. connections
    d. configuration

18. Which two third-party threat intelligence feeds can be enabled in Cloud Pak for Security?
    a. Virustotal
    b. Trustwave Spider Labs
    c. Mandiant Threat Intelligence
    d. Swimlane TI
    e. Crowdstrike

19. How can you determine if the Orchestration and Automation license is not applied?
    a. Go to **Application settings > Orchestration & Automation > SOAR Playbooks**, clicking **Customization Settings > Scripts**, and see a message **The Action Module** is not enabled.
    b. Case management is not available.
    c. SOAR is not installed.

20. How is the Orchestration and Automation license installed?
    a. Enter license when installing the SOAR app.
    b. Create a secret named isc-cases-customer-license with the license key in OpenShift.
    c. The license is installed automatically

21. How is the Threat Intelligence Insights app disabled when it is no longer needed?
    a. Delete the app pods
    b. Disable the app in **Settings > Application Settings**
    c. Uninstall Treat Intelligence Insights

- Answers:
  - 1: D
  - 2: A
  - 3: A
  - 4: B,C,D
  - 5: D
  - 6: B
  - 7: A
  - 8: B
  - 9: C
  - 10: C
  - 11: D
  - 12: A
  - 13: C
  - 14: B
  - 15: C
  - 16: C
  - 17: A
  - 18: A, C
  - 19: A
  - 20: B
  - 21: B