UiPath Security Quiz

1. Multitenancy feature in Orchestrator offers possibility to isolate between tenants the following entities:
   1. All entities
      1. Logs
      2. Users
      3. Audit trail
      4. Settings
      5. In addition to Robots, assets, queues, etc.
2. CyberArk can be integrated with Orchestrator in order to retrieve Robot credentials from CyberArk instead of SQL Server DB
   1. True
3. What are the most common security threats a code reviewer can cover?
   1. Not sending email to private accounts from workflow
   2. Not storing sensitive data in local files
   3. Not using hard-coded URLs, accounts, or email addresses
4. Access to local package executed by robot is granted to:
   1. Robot service and local admin
5. A valid SSL certificate is required to install Orchestrator
   1. True
6. Authenticating users on Orchestrator platform can be done with:
   1. Active Directory username using Windows Authentication
   2. Local username and password
   3. Azure Active Directory authentication
   4. Google accounts with OpenAuthentication 2.0
7. What are the main differences between guidelines and security features?
   1. Guidelines are recommended general best practices
   2. Security features are already implemented in product
8. Account Lockout security feature provided by Orchestrator platform ensures:
   1. Protection against Brute Force attacks
9. What TLS protocol is recommended by Orchestrator platform?
   1. TLS 1.2
10. Account Lockout settings are configurable per:
    1. Tenant
11. What is the purpose of code review?
    1. To ensure proper usage of credentials
    2. To ensure a malicious developer cannot utilize his own details to receive money or information overriding configurable settings
    3. Prevent sending sensitive data outside trusted scope
12. Passwords in Orchestrator:
    1. Can be set to expire after a certain number of days
    2. Cannot be changed without a direct request to your platform administrator
    3. Must be changed on the first login
13. Audit page on Orchestrator platform allows filtering by:
    1. Action
    2. Component
14. Messages logged by Robots are sent to Orchestrator and can be stored in:
    1. SQL Server and Elasticsearch by default, but also in other targets standard or custom
15. What are basic security measures already implemented, concerning Robot-Orchestrator connection?
    1. Robot must be provisioned in Orchestrator before it can connect to Orchestrator
    2. User must have local admin rights on Robot machine to connect to Orchestrator