Independent Assessor for MHBE IT Security Review
RFP # BPM026357
Additional Questions
11/9/2021

Questions from Tyler Cybersecurity

1. Is the MHBE willing to allow a non-invasive external port scan to be conducted in advance of proposal submission as a qualification exercise in order to validate public-facing IP ranges and the # of active hosts (i.e., open/listening ports)?
   Response: No

2. Are any systems or devices in scope hosted by a third party?
   Response: Yes, MDThink Shared Services

3. Can you please confirm the URL(s) of any public-facing web application(s) in scope?
   Response: The URLs in scope are not public facing.

4. Is the HBX application a custom application developed in-house or a vendor provided platform?
   Response: Developed in house

5. In order to qualify size/complexity of the site from an authenticated perspective (# of dynamic pages, forms/inputs, functional characteristics, etc.) is MHBE willing to support one of the two options below?
   Response: Yes
   A. Conduct virtual demo / walkthrough of application
   Response: Yes
   B. Provide temporary test user credentials with the desired privileges (i.e., end user, manager, admin, etc.)
   Response: Yes, we will provide temporary credentials

6. If not, what are the total # of dynamic pages and total number of forms/inputs of the website post-authentication? Please describe the overall functional attributes available to the user perspective that will be tested (links, radio buttons, drop-downs, report generation, etc.)
   Response: N/A based on response in question 5

7. Is web application testing to be conducted against the live production server environment or a test server environment?
   Response: It will be done in the test environment

8. If testing is performed on the live production server, are there portions of the site that should not be tested in order to avoid a potential interruption of service?
   Response: based on response in question 7

9. Is an internal penetration test expected as part of the "Penetration Test" requirement?
   Response: Yes

10. Is social engineering in scope as part of the "Penetration Test" requirement?
    Response: No

11. Is the MHBE willing to disable specific security controls once their effectiveness has been substantiated during testing in order to increase the substance of the testing effort and maximize cost efficiencies?
    Response: Yes

12. What are the desired configuration settings to be assessed against? If MHBE-specific, can you share a list of the settings in order to determine the required amount of production time? Are assessors expected to assess against manufacturer/vendor recommendations and/or industry best practice from independent third parties such as CIS, NSA, NIST, etc.?
    Response: CMS Assessor Workbook and MARS-e 2.2 workbook will be provided.

13. Are all the configuration "controls" to be assessed part of a standard baseline (i.e., CIS Benchmarks) that a tool like Nessus would be able to be used to collect the results? If not, will administrative access be provided to the devices so a manual review can be conducted?
    Response: CMS Assessor Workbook and MARS-e 2.2 workbook will be provided.

14. What operating systems and/or applications are in scope for the configuration assessments?
    Response: RHEL and Windows

15. How many departments are in scope for the Personnel Interviews requirement? Can you estimate the number of interviews that are required from the various business stakeholders involved?
    Response: IT Management

16. Does MHBE expect the selected Assessor to be onsite to satisfy the Observations requirement against physical controls and personnel behavior or can those objectives be satisfied with a remote fulfillment model?
    Response: Yes

17. Can you share expectations on the format of the required report deliverables as they relate to the Security Assessment Report (SAR)? Is one document required or are multiple reports acceptable that are specific to the related assessment/testing activities?
    Response: Template and Workbook will be provided

Questions Anvaya Solutions

18. How many web applications are included?
    Response: 4
- The consumer portal includes a WordPress content site and secure JAVA web application
- The worker portal includes a secure Java web application and a integrated live chat application

19. Are there any internal only applications that need to be tested?
    Response: Yes, the worker portal and components of the live chat are internal.

20. How many mobile applications?
    Response: 2 (iOS and Android)

21. What operating systems?
    Response: Duplicate (see #14) - RHEL and Windows

22. For each application:

    WordPress:

    How many dynamic pages?
    Response: 1000+ (WordPress site is very dynamic)

    Number of roles?
    Response: 3

Number of IPs.
Response: All applications are behind a load balancer and the number of IP's will not be given

Consumer Portal- Secure:

How many dynamic pages?
Response: 50

Number of roles?
Response: 2

Number of IPs
Response: All applications are behind a load balancer and the number of IP's will not be given

Worker Portal- Secure:

How many dynamic pages?
Response: 40

Number of roles?
Response: 36

Number of IPs
Response: All applications are behind a load balancer and the number of IP's will not be given

Live Chat Portal- Secure:

How many dynamic pages?
Response: 20

Number of roles?
Response: 4

Number of IPs
Response: All applications are behind a load balancer and the number of IP's will not be given