Cybersecurity Assessment – Questions and Answers

The Superior Court of California, County of Contra Costa (the Court) received all the following questions concerning the comprehensive Cybersecurity vulnerability Assessment of the Court's network from qualified vendors prior to the June 19, 2023, submission deadline.

Please see all questions and responses below provided by the Court's IT Infrastructure Manager:

1. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?
   a. *I am not aware of any qualified vendors who have recently completed a Cybersecurity Assessment for the Court.*

2. Specify the VLAN details how many are included in the Scope?
   a. *The Court has one domain (www.cc-courts.org) in scope for this project. It has 64 VLAN's at 9 locations: 5 in Martinez (Taylor, Bray, Spinetta, Annex, and Juvenile Hall), Walnut Creek, Richmond, Pittsburg, and Concord. There are 375 users with 700 endpoints including 195 servers.*

3. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?
   a. *The Court has 25 physical and 170 Virtual Servers with approximately 50 network devices.*

4. How much (%) of the infrastructure is in the cloud?
   a. *The Court has about 2% of its infrastructure in the cloud.*

5. In the IT department/environment, how many employees work?
   a. *The Court's IT team consists of 16 employees.*

6. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
   a. *The Court's IT team manages our data centers and does not use any co-location sites.*

7. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?
   a. *The Court had allocated up to $27,000 for this project.*

8. Has your organization had any previous 3rd party Security & Risk assessments in the past?
   a. *I am not aware of any 3rd party security & risk assessments completed in the past.*

9. Has your organization had any previous 3rd party penetration tests in the past? (internal and/or external)
   a. *I am not aware of any 3rd party penetration tests done for the courts.*

10. How many external facing IP addresses does your organization have that we would need to test?
    a. *The Court has 2 external facing IP addresses.*

11. How many networks/VLANS?
    a. *The Court has 64 VLAN's.*

Cybersecurity Assessment – Questions and Answers

12. How many are critical for segmentation testing?
    a. *All 64 VLAN's are critical for segmentation testing.*

13. What are the five (5) applications that need to be tested?
    a. *Tyler Odyssey*
    b. *Tyler Odyssey public portal*
    c. *Thomson Reuters C-Track*
    d. *Thomson Reuters C-Track*
    e. *Jury Duty System*

14. How many unique internal domains are in scope?
    a. *One domain (www.cc-courts.org) is in scope for this project.*

15. Please confirm if Active Directory is utilized.
    a. *Microsoft's proprietary directory service, Active Directory, is utilized in this organization.*

16. Does your organization use server virtualization? And what type? (VMware, Hyper-V etc)
    a. *The Court has a VMWare server virtualization environment.*

17. Is there a server or VM environment we can deploy scanning tools on to?
    a. *The Court has a VMWare environment that the prospective vendor may deploy network scanning tools.*

18. Number of sites/locations
    a. *There are 9 sites: 5 in Martinez (Taylor, Bray, Spinetta, Annex, and Juvenile Hall), Walnut Creek, Richmond, Pittsburg, and Concord.*

19. High level description on how the sites are connected to each other (network connectivity)
    a. *The locations are connected to each other using AT&T Switched Ethernet connections with redundant data centers.*

20. Can you provide an approximate number of:
    a. Staff members: *375*
    b. Endpoints: *700*
        i. Servers: *169*
        ii. Workstations and laptops: *600*
    c. Internal Subnets:

21. For C. B. vii - Is the court willing to provide a user account with standard permissions in order to perform "assumed compromise" testing?
    a. *The Court can provide a Microsoft Active Directory user account for testing to the prospective vendor.*

22. For C. B. V. – Is the court looking for an actual Security and Risk Assessment based on standards like NIST 800-53v5, or are you looking for an application-based pen test (i.e., Web pen test)?
    a. *The Court is seeking a cybersecurity assessment based on commonly accepted cyber*

Cybersecurity Assessment – Questions and Answers

security industry standards.

23. Are external cloud-based services in-scope (i.e., Azure, AWS, etc)?
    a. *No, no external cloud-based services will be in-scope for the current project.*

24. Does the court require on-site presence during this engagement, or do they allow/approve testing activities to be performed remotely?
    a. *The Court prefers on-premises engagements with the prospective vendor. Limited remote testing activities could be performed at the discretion of the Court IT team.*

25. Does the court have an IT team, or external vendor, to assist with necessary prerequisites for these engagements?
    a. *The Court has an IT team that may be able to assist prospective vendors with additional information.*

26. Are there any hour restrictions for testing?
    a. *On-premises testing is limited to 8am to 5pm, PT. Remote testing is restricted to the discretion of the Court due to operational constraints.*

27. As a Canadian company that is legally able to operate within California, are there any unique clearances/credentials needed for this proposal?
    a. *As of today, Court is not aware of any unique clearances/credentials needed for this proposal. We may visit this question if the Court gets interested in your proposal.*

28. Does the Assessment require a physical testing on-site (aka boots on the ground) portion, or can it be completed completely virtual?
    a. *The Court prefers a physical on-site testing segment of the project. An 100% virtual testing does not conform with current industry standards.*