THE UNIVERSITY OF SOUTHERN MISSISSIPPI

May 18th, 2022

Addendum 2 to RFP 22-45 Managed Security Services/Managed Detection Response.

This addendum provides answers to questions submitted by prospective bidders. The answers to the questions below are in red.

John Leggett, Buyer

1. **COV-0110: Do you have an existing network capture device, or will provider need to supply one?**
   We will not have one. If the solution requires a network capture device, then it will need to be provided in the proposal

2. **COV-0110: Can you provide a breakdown of operating system and numbers for the 5000 endpoints?**
   About 80% Windows and 20% MacOS - we don't have an exact count.

3. **COV-0114: Please describe what kind of IoT devices and what kind of operating systems you are running?**
   IoT systems are mostly VoIP handsets, PLC controllers, environmental controllers, IP cameras, etc.

4. **GEN-1015: (a) What specific information are you trying to obtain from ingesting Nmap scans? (b) Do you have a vulnerability scanner?**
   a. Information on open ports of hosts.
   b. We do have a vulnerability scanner.

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

5. **RIT-400: What kind of multiple retention disposable policies are you looking for the provider to report?**
   This is an optional requirement and what we are looking for is a service that can support different retention for different data. maybe certain devices we want to keep event information for 6 months, but others maybe 1 month are enough.

6. **SUP-0200: Does online knowledge base needed to be ran by provider, or would OEM vendor knowledge base be acceptable?**
   Provider should be responsible for Online support of its own product. Online knowledge base would be a source for us to go to if we had a simple support question. For instance, maybe we need to know how to craft a custom report. We could access the online knowledge base to find an article about how to do that.

7. **Can a one-week extension of the bid response date be accommodated?**

   The bid opening response deadline will not be extended at this time.

8. **Number 35.) of the Proposal Coversheet states that we can submit our bid electronically, while figure E. states that the proposal MUST be printed and bound. Please clarify how the proposal can be submitted.**
   You are welcome to use either of our secure options we offer to submit your response for this RFP. Figure E applies if you are not using the electronic submission option and submitting it as a physical sealed bid.

9. **COV-0107 – What's the operating system version of these domain controllers?**
   Windows Server 2016 or 2019

10. **COV-0107 – How many user accounts are required to be monitored? Please specify faculty and student accounts and any other accounts. "M. Scope of Work" specifies 3'000 employees and 14'100 students. Are these the numbers that should be considered to be included in the MDR Service?**
    ~3000. We would prefer to exclude student accounts (especially if the cost is significant).

11. **COV-0108 – What's the operating system version of these servers?**
    Windows server 2016 or 2019

12. **COV-0109 – What's the operating system version of these servers?**
    Oracle Enterprise Linux 7

13. **COV-0111 – What's the operating system version of these managed endpoints?**
    About 80% Windows and 20% MacOS - we don't have an exact count. – Not all are managed

14. **COV-0112 – How many M365 licenses are in place? Please specify if these are A3 or A5 licenses.**
    A3 for students: about 28K / A3 for faculty ~2100 / A1 faculty ~1600

15. **COV-0113 – What's the operating system version of these servers?**
    Various mostly Windows Server 2016, Windows 2019, Oracle Enterprise Linux (OEL) 7, OEL8, VMWare ESX 5.5|6.7|7.0

16. **COV-0114 – Can you elaborate on the different type of devices that would be in scope her? No exact list required but an idea of different types. Is this line related to request VIS-1300?**
    IoT systems are mostly VoIP handsets, PLC controllers, environmental controllers, IP cameras, etc. This is not related to VIS-1300.

17. **GEN-0400 – What device management is in place to manage the 5000 endpoints and 355 servers (InTune, SCCM, …)? This is relevant to understand rollout capabilities for Microsoft Defender for Endpoint on all endpoints and servers.**
    Most Windows machines are managed by SCCM (though we are looking at inTune). Some machines that are owned by USM aren't "managed".

18. **GEN-1000 – Are all these sources ingested into the current SIEM platform? Could you please share daily ingestion volumes. This is relevant to estimate costs around Sentinel ingestion.**
    No, not all the sources are being ingested by our current SIEM. Our current SIEM is seeing ~10000 events per second.

19. **What is your networks Events per Second (EPS)/ amount of daily log data?**
    Currently we are ingesting about 10,000 events per second

20. **Is there a current EDR solution in place on the university owned/managed endpoint computing devices? If so what EDR solution is it?**
    No, we do not have any EDR products.

21. **Microsoft defender is referenced in section GEN-0410. Is that running anti-virus or EDR mode?**
    anti-virus mode – I don't believe we are licensed for EDR in Defender

22. **GEN-1001 references comprehensive coverage of a syslog source. Is the intention to have an existing syslog server log forward to a the new solution? If so how many data sources are currently sending data to the Syslog server that will forward logs?**
    No, we were just indicating that the solution must be able to receive log info via syslog/syslog-ng. Systems would be individually sending logs.

23. **COV-0300 references Microsoft 365 and Azure activity monitoring. How many users exist inside the Office 365 environment?**
    We have about 35000 – but most of those are students, which wouldn't be in scope for UBA

24. **IRM-0700 - Does USM require the ticketing system to integrate with an existing ITSM solution?**
    It does not, it would be useful to work with a services management software (we use Cherwell), but it could use its own internal ticketing/workflow process.

25. **Does USM have geographic requirements? i.e., should the support team be U.S. based or does it matter?**
    a. Only what's specified in the Appendix C and RFP documents.

26. **Approximately, how many public facing web servers does USM have?**
    a. ~41

27. **Does USM have any specific compliance requirement that should be considered in the configuration that is offered. For example, PCI, HIPAA, ISO, FedRAMP?**
    a. Only what's listed in the Appendix C and RFP documents.

28. **AWS Environment:**
    a. We do not use AWS.

29. **For Native AWS Logs should your vendor consider:**
    a. We do not use AWS.

30. **For your Azure environment what would be the approximate number of:**
    a. We have 6 servers in Azure.

31. **Logs to collect: (estimates are acceptable)**
    a. -Please see Appendix C and RFP documents.

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

32. On Premise Locations:

a. -Please see Appendix C and RFP documents.

33. Quantities of Location Types with direct internet access?

a. -Please see Appendix C and RFP documents.

34. For USM On-Prem Network data sources

-Please see Appendix C and RFP documents.

35. On-Prem: Approximate Server/Endpoint Data Sources:

a. -Please see Appendix C and RFP documents.

36. Could you outline the timeline post May 24th? Evaluation, possible oral presentation, award, …

We do not have an exact timeline defined after the opening, but we plan to review all responses to the RFP in a timely manner depending on the volume of responses received. We will notify all respondents when an award is made.