Vendors are expected to provide preliminary pricing based on the general scope and assumptions outlined in this RFP. Sauk County understands that final pricing may be subject to adjustment following a more detailed review of the County's infrastructure, which will be made available only after NDA execution and preliminary vendor vetting.

TBD – "To Be Determined"
The County intends to take the broadest possible view in selecting the most appropriate MDR solution. As such, certain specifics have been intentionally left open for proposers to define and elaborate on based on their solution's capabilities. In these instances, the abbreviation "TBD" has been used in the responses below.

11/12/2025

1. What is the basic speed and configuration of the County's internet egress for each location?

   Answer – All county buildings are connected to the internet via a pair of interconnected firewalls configured as a high-availability (HA) pair, with each firewall located at a separate physical site. Each firewall has a dedicated 1 Gbps internet connection provided by the County's primary ISP. One of them is also connected to a 600 Mbps backup internet connection through an alternate ISP.

2. How many users are at each of the three main locations?

   Answer –

   - Main buildings in Baraboo = approximately 200
   - Law Enforcement = approximately 150
   - Highway Dept = approximately 75

11/13/2025

3. The RFP specifies 600 users; the above only identifies 425. What is the function of the balance of 175 Users?

   Answer – The remaining approximately 175 users are distributed across several locations, including the Health Care Center (nursing home), Reedsburg Human Services, and other county facilities. All sites are provisioned through the same centralized private network, which provides access to IT resources throughout the organization.

11/18/2025

4. Are there any specific integrations required with existing tools beyond Microsoft 365?

   Answer – Yes, the ability to integrate with most of the County's existing tools is desired.

5. Can you confirm that the requirement is for 24x7x365 monitoring with no service gap?

   Answer – Yes, the requirement is 24x7x365.

6. Are there any specific SLAs for response times that we should align with?

   Answer – There are not

7. For major incidents, do you expect on-site support, or will remote assistance suffice?

   Answer – On-site support is preferred.

8. Is vulnerability scanning and penetration testing to be part of the core MDR service or treated as an optional add-on?

   Answer – This is dependent on the service providers' offering and may be either included or treated as an optional add-on.

9. What is the current tier of M365 licensing?

   Answer – G3

10. Are there any plans to upgrade or change Microsoft licensing tiers in the foreseeable future?

    Answer – Not currently.

11/20/2025

11. Do you currently use automated scanners or perform manual penetration testing?

    Answer – Yes

12. If yes, how often are these performed?
    Answer – Monthly

13. Do you wish to include a SIEM solution as part of this project?

Answer – Proposers are welcome to propose a SIEM solution as an optional addon.

14. Regarding the 900 total endpoints (600 workstations, 80 servers), what makes up the remaining 220 endpoints?

    Answer – Switches, Wireless Access Points, Firewalls, Printers

15. Should the MDR solution being requested cover endpoints only, the data center (including network devices), or both?

    Answer - both

16. What is the total number of external IP addresses?

    Answer - 56

17. Total number of internal servers?

    Answer - 80

18. When is the expected purchase date?

    Answer – Q1 of 2026

19. Is the County open to an uplift to Microsoft G5 for Security licensing?

    Answer – If required by a particular solution, yes. However, this would be considered as part of the cost of the proposed solution for evaluation purposes.

20. How many IPs are in range for internal and external scanning?

    Answer - TBD

21. Does the county require an Incident Response Retainer as part of the solution?

    Answer - No

22. If down-selected in this RFP process, will providers/ vendors be called up to present their solution?

    Answer – TBD

23. Will there be a Q&A session?

    Answer - TBD

24. At what point does the county plan to finalize the evaluation and make a decision?

Answer – Early 2026

25. Should a copy of the Excel questionnaire be printed out and included within the hard copies that are submitted as well, or does the flash drive suffice?

    Answer – You need only provide it in electronic form.

11/25/25

26. Can Sauk County please clarify your scope of interest in penetration testing - continuous vs one-off? Internal vs external?

    Answer – It is up to the proposer to make a recommendation to support their approach.

27. Is there interest in a dedicated support resource with regularly scheduled support meetings?

    Answer - yes

28. What level of threat intelligence depth and granularity are you looking to achieve with your chosen vendor?

    Answer – this is dependent upon the capabilities of the vendor and their proposed solution.

29. Will the County provide an estimated budget or a Not-to-Exceed (NTE) amount for this contract?

    Answer – not at this time

30. Could the County please provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?

    Answer – TBD, however, an implementation by mid-summer 2026 is anticipated.

31. Could the County please clarify whether it intends to award this RFP to a single vendor or multiple vendors?

    Answer – TBD

32. Please confirm the exact device counts included in the scope:

a. Total endpoints (Windows/Mac/Linux)

   Answer - 600

b. Total servers (Windows/Linux)

   Answer 80

c. Firewalls

   Answer - 2

d. Network devices (switches, routers, wireless controllers)

   Answer - 218

e. Cloud workloads

   Answer – the County utilizes a number of cloud-based applications and the degree to which these are monitored would be dependent on upon the solution or solutions selected.

33. Please confirm the number of data/log sources expected to be integrated into the MDR platform.

    Answer – TBD

34. Are there any OT/IoT devices (CCTV, HVAC, printers, badge systems) that are expected to be in scope for logging or monitoring?

    Answer – TBD

35. Are you expecting the vendor to provide SIEM/XDR, or should the vendor manage your existing tools (e.g., Sentinel, Defender suite)?

    Answer – as stated in the specifications, the County would prefer that the selected vendor integrate existing tools into their proposed solution.

36. What is your expected log retention requirement?

    Answer – TBD

37. Do you require raw log storage, or only security-relevant events?

    Answer – TBD

38. Should the MDR vendor create custom incident response runbooks for the County?

    Answer – this would be preferred.

39. Under "Preferred Functionality," which items are mandatory and which are optional add-on services?

    Answer – "Preferred Functionality" refers to the features and capabilities that the County considers ideal in a proposed solution. These preferences outline desired functions, but the final evaluation will depend on the specific capabilities of each proposed solution and, most importantly, the level of security it can deliver.

40. What is your expectation regarding event triage SLAs?

    Answer – TBD

41. Is the vendor required to provide monitoring services as well? 24*7? If yes, what is the desired level of remediation?

    Answer – Yes, the level of remediation is up to the proposer to recommend.

42. What is the number of IT staff needing training?

    Answer - 10

43. Is on-site or virtual training required?

    Answer - Virtual training is acceptable

44. Do you require ongoing training, or only initial onboarding training?

    Answer – TBD – but likely only onboarding training.

45. Under the RFP pricing model, do you expect:
    a. One-time setup fee?

       Answer – yes, if proposed

    b. Annual recurring costs?

       Answer - yes

    c. Optional service pricing?

       Answer - yes, if proposed

46. What is your estimated log volume in GB per day (log/GB per day) across all systems, including servers, endpoints, firewalls, cloud platforms, and identity sources?

    Answer - TBD

47. Please confirm whether Sauk County expects the MDR provider to deliver SOC monitoring and tool onboarding services onsite, offsite/remote, or a hybrid of both
48. How many total Microsoft licenses are utilized?

    Answer – 600

49. Will a SOAR integration be required?

    Answer – Yes, this is anticipated, depending upon the proposed solution.

50. What is the preferred delivery model for the solution?

    Answer – TBD

51. Should the solution be fully managed by the service provider, or do you prefer a co-managed approach with your internal IT team?

    Answer – a co-managed approach would be preferred.

52. Do you wish to have the service provider manage your SIEM solution, or should the service provider utilize their own SIEM platform?

    Answer – If possible, the proposer should provide pricing information for either option.

53. Should the SIEM solution include advanced analytics, such as machine learning-based threat detection?

    Answer – TBD based on the solution proposed.

54. Are there specific security frameworks or standards (e.g., NIST, ISO 27001) that the SOC operations must adhere to?

    Answer – alignment with the NIST framework is preferable.

55. Do you require integration with existing IT service management (ITSM) tools for ticketing and incident management? If it is not present currently?

Answer – TBD

56. Are there existing endpoint protection tools in place that need to be integrated with the XDR solution?

    Answer – Yes

57. Do you have specific preferences for AI-based endpoint protection features or vendors?

    Answer – TBD

58. What types of endpoints (e.g., Windows, macOS, Linux) need to be protected by the XDR solution?

    Answer – Windows

59. What is the expected growth in data volume or endpoints over the next 3 years, and should the solution be scalable to accommodate this growth?

    Answer – It is anticipated that growth will be modest (less than 10 new endpoints annually), and the proposed solution must be able to accommodate such growth.

60. should the proposal include multiple pricing tiers for flexibility?

    Answer – This is up to the proposer, but it seems like a reasonable approach.

61. Are there additional services or features you foresee needing in the future (e.g., advanced threat intelligence feeds)?

    Answer – TBD

62. Can the County provide any information on the budget required to support these services? (E.g., budget details)

    Answer – not at this time.

11/26/25

63. Approximately how many log sources (servers, network devices, applications, cloud services) should vendors assume for SIEM/XDR onboarding?

    Answer – TBD

64. How many endpoints are in scope? (Desktops, Laptops, Servers)

    Answer – 680

65. Are there any tools not procured yet by the County that the Vendor should procure?

    Answer – TBD

66. Will the County be paying for the costs of log ingestion directly? Or will the MDR service team bear the costs for all log ingestion?

    Answer – TBD – vendors should anticipate some cost.

67. How many employees will we be potentially supporting?

    Answer – 600

68. Besides Microsoft 365, does the County use other cloud platforms (AWS, Azure, Google Cloud, SaaS applications) that should be included in MDR monitoring?

    Answer – There are a number of SaaS applications, and limited use of all of the aforementioned cloud services.

69. Will the County allow for any or all off-shoring for this project? Data, personnel, talent, etc.

    Answer – TBD; however, US-based will likely be given preference.

70. Is Dark web analysis of potential interest to the County?

    Answer – potentially, yes – as an optional service.

71. Is there a required log retention duration (e.g., 30 days, 90 days, 1 year) for SIEM/XDR data? Is this hot, warm, and/or cold retention?

    Answer – TBD

72. If vulnerability scanning is included, does the County have a preferred scanning cadence (weekly, monthly, quarterly)?

    Answer – TBD

73. Should vendors assume equal monitoring sensitivity across all subnets and departments, or are there priority zones?

Answer – there are priority zones

74. Can the County provide the list of external IP addresses, domains, or public-facing assets that should be included in the external vulnerability scan? If not, could one provide a CIDR notation range? Eg: /24, /25, /26, etc..

    Answer – there are three public connections CIDR = /27, /28, & /29

75. Could the County share how it defines co-management of incident responses and what its expectations are?

    Answer – Per the RFP*: The selected vendor will collaborate closely with the IT Department to proactively manage and respond to cybersecurity threats and incidents. The selected vendor will become an integral part of our security team, acting as an expert with regard to security incidents, vulnerability management, configuration, and identification of true positive security alerts*.

76. Given the highly dynamic nature and volatility of incident response, is it acceptable to propose incident response hourly rates separate from and outside of standard MDR services?

    Answer – yes

77. How do you define tier 1 and 2 analysts in a SOC?

    Answer:
    Tier 1 Analyst – Frontline / Alert Triage - Primary Role: First responder and alert triage specialist.

    Tier 2 Analyst – Incident Responder / Investigator - Primary Role: In-depth investigation and incident response.