DATE: September 13, 2024

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 2
PROJECT NAME:	Managed Detection & Response Services
JJC PROJECT NO.:	R25001

This Addendum forms a part of the Bidding and Contract Documents and modifies the original bidding document as posted on the JJC website. Acknowledge receipt of this addendum in the space provided on the Bid Form. FAILURE TO DO SO MAY SUBJECT BIDDER TO DISQUALIFICATION.

<u>**Questions Received:**</u>

1. Is College open to exploring non-USA/offshore based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity professionals in a cost-efficient manner. ***JJC prefers that services and solutions remain in the US. If the proposal is transparent about how data is used outside of the US, considerations will be made during evaluation.***

2. Can College provide any information on the budget required to support these services? (E.g., budget details) ***Joliet Junior College does not share budget information during the solicitation process.***

3. Is the College currently using any service providers that are assisting the College in performing the requested services? If so, who are these providers? **This information is not relevant to the RFP***.*

4. Please share the list of data source types and the count of data sources broken down by platform? ***Proposal should illustrate pricing for an array of data sources.***

5. Does Deschutes County have SOAR solutions and can you provide the name of solution? ***Joliet Junior College will not be providing this information as part of the RFP process.***

6. What are your desired data retention policies for log data?
   90 to 365 depending on the log type.

7. Does experience in Higher Education institutions is mandatory or other industry experience can be provided? ***Higher Education Preferred, other industries may be considered.***

8. Is the requirement for all personnel having access to JJC systems to be US based firm? ***Preferred***
   a. Is the requirement for all data related to the services to be US based firm? ***Yes***
   b. Is the requirement for all personnel having access to JJC systems to be US based firm? ***Preferred, Yes.***
   c. Is the requirement for all data related to the services to be US based firm? ***Preferred, Yes.***
   d. Is the requirement for all personnel having access to JJC systems to be US based firm? ***Preferred, Yes.***
   e. Is the requirement for all data related to the services to be US based firm? ***Preferred, Yes.***
   f. Is the requirement of all personnel having access to JJC systems to be based in the US firm? ***Preferred, Yes.***

9. Is the requirement for all data related to the services to be US based firm? ***Preferred, Yes.***

10. Complete list of assists and # of assets to be monitored ie Firewalls-make and model, Web apps firewalls, DNS Server(MS,BIND, etc) any NetFlow capabilities, number of infrastructure devices (routers, switches, etc) make and models, number of servers make and model, number of active directories or Ldap servers. ***This information will not be provided as part of the solicitation process, vendors should submit pricing for any array of assets.***

11. Complete list of all cloud instances ***This information will not be provided as part of the solicitation process, vendors should submit pricing for any array of assets.***

12. current list of security tools being used ie SIEM, Endpoint security/management, Vulnerability Identification, Intrusion Detection, CMBD solution etc. ***This information will not be provided as part of the solicitation process, vendors should submit pricing for any array of assets.***

13. Number of full-time employees ***~2150***

14. Does the solution need to be on premise solution or can it be a fully cloud solution / acceptable ***It can be a fully cloud solution***

15. For a cloud based SIEM/MDR solution, does the solution need to be FedRAMP certified. Or, GovCLOUD ? Is CJIS compliance required ? ***No this was not a current requirement listed in the RFP.***

16. Who is the project sponsor? ***This is a JJC project; there are no additional sponsors.***

17. Is there a budget allocated for this project
Joliet Junior College does not share budget information during the solicitation process.

18. If so for budget, what is it ?
Joliet Junior College does not share budget information during the solicitation process.

19. What is the expected timeline for delivery of services as outlined in RFP. ***Vendors should provide their availability and average timeline for a project within an organization comparable to the size of JJC. We would like to implement as soon as possible once a contract is executed.***

20. Will you contract with only one vendor ***Preferably, yes.***

21. Was this RFP created internally or was a 3rd party resource used to help create the RFP ? If so, will the 3rd party be allowed to participate in the bidding process
JJC Created the RFP Document internally

22. Please confirm the current RFP scope is for Managed, Detection and Response (MDR) services at a 24x7x365 pace ***CORRECT***

23. What is the current log collection and storage requirements for size and intervals to support analysis and response
This information will not be provided as part of the solicitation process.

24. Are there specific compliance reporting requirements
GLBA, FERPA, PIPA, HIPAA

25. What current storage solution is being utilized ***This information will not be provided as part of the solicitation process.***

26. What is the current backup solution being utilized ***This information will not be provided as part of the solicitation process.***

27. What phone system is being utilized ***Ring Central***

28. Do you have a SOAR solution and would like to implement as part of new solution
This information will not be provided as part of the solicitation process

29. Do you know your current EPS-Events Per Second for in-scope networks ***No***

30. What is the number of staff and total number of students ***2150 staff, ~20,000 students***

31. Can college provide the editable/fillable Appendix C and D in excel/word file? ***Please see the fillable appendices in Excel format on the college's website and in ESM.***

32. What technologies and tools does the incumbent MDR provider use for threat detection, response, and overall security management (e.g., SIEM, EDR, firewalls, etc.)? How many cloud endpoints are currently being monitored? What cloud platforms are in use (e.g., Azure, AWS, Google Cloud)? ***We will not be providing this information as part of the solicitation process.***

33. How many third-party SaaS applications are integrated with your environment? Are there any specific integrations we need to be aware of (e.g., Office 365, Salesforce)? How many internal applications are critical to your operations? Are these internal applications web-based, hosted on-premises, or cloud-native? ***This information will not be provided as part of the solicitation process. Vendor should submit pricing for an array of applications and services.***

34. How many total endpoints, including physical and virtual machines, are currently managed? How many of these endpoints are cloud-based or virtual machines? ***This information will not be provided as part of the solicitation process. JJC is ~2150 employees, information should be able to be drawn from that.***

35. How many laptops are currently in use by students, faculty, and staff? Can you provide details on the types of laptops and operating systems being used? Do you have any Operational Technology (OT) or Internet of Things (IoT) devices connected to the network? If so, how many and what types? Are there specific security protocols in place for OT or IoT devices? ***This information will not be provided as part of the solicitation process. JJC is ~2150 employees, information should be able to be drawn from that.***

36. What is the size of your internal security team? Do you have a dedicated incident response team in-house, or is this entirely managed by the outsourced MDR provider? How many security analysts and threat hunters are currently working under your MDR contract? What is the cadence and methodology? ***This information will not be provided as part of the solicitation process.***

37. What is the current shift structure for security monitoring (e.g., 24/7 monitoring, on-call support)? Is your Security Operations Center (SOC) fully in-house, outsourced, or a hybrid of both? How many analysts are assigned to MDR services? ***This information will not be provided as part of the solicitation process.***

38. How frequently do you experience security incidents that require full response (on average per month)? What is your current log ingest (in GB) daily? What is your current process for incident escalation and resolution? Do you expect the outsourced

MDR provider to manage the entire process or collaborate with your internal teams? ***This information will not be provided as part of the solicitation process.***

39. How do you currently track and manage security incidents? Do you have an existing ticketing system that you expect the MDR provider to integrate with, or will they be required to bring their own? Are there any specific automations or integrations with other systems within your ticketing process that need to be preserved or enhanced? ***This information will not be provided as part of the solicitation process.***

40. What are your data storage and retention policies for security logs and incident data? Are there specific requirements for long-term storage, especially for sensitive or classified data? ***See the response to question #6.***

41. Are there any federal research-driven mandates that Joliet Junior College must comply with (e.g., CMMC, NIST SP 800-171, FERPA)? What compliance standards and frameworks does your organization follow, and what is your timeline for adherence? ***See the response to question #24.***

42. Do you have interconnections with third-party networks or systems (e.g., other educational institutions, vendors) that require monitoring? What security protocols are in place for managing and monitoring external connections with third-party vendors or institutions?
This information will not be provided as part of the solicitation process.

43. Can you provide an overview of your network topology, including segmentation between critical infrastructure, student networks, and staff/administrative networks? How is network traffic currently being monitored? Are there specific tools in place, and do you have a preference for keeping or replacing these tools? How many virtual networks are in place, and what is the current cloud architecture? ***This information will not be provided as part of the solicitation process.***

44. Are there specific cloud security measures or policies we need to be aware of (e.g., hybrid cloud, multi-cloud environments)? What are your current bandwidth requirements, and do you have failover or redundancy measures in place for network availability?
This information will not be provided as part of the solicitation process.

45. Do you expect the MDR provider to manage network monitoring tools to ensure uptime and availability? ***No.***

46. Are there any third-party vendors, partners, or service providers that require monitoring as part of the MDR scope? How do you currently monitor interconnections and shared resources with these third parties? ***This information will not be provided. Vendors can provide pricing and make infereneces from the information already provided withing the RFP.***

47. What level of collaboration do you expect between the MDR provider and your internal security staff? What type of cyber insurance coverage do you have in place,

and are there any specific security practices required to meet the insurance conditions? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided withing the RFP.***

48. Do you expect the MDR provider to help with compliance reporting and audits related to cybersecurity standards? ***No*** Do you have any internal processes or guidelines for responding to large-scale incidents or breaches that we need to align with? ***We have an IR plan and process.***

49. Do you have any specific administrative requirements for onboarding and offboarding users, particularly with regard to network and security tool access? ***This information is not relevant to the proposal.***

50. What kind of reporting cadence do you expect from the MDR provider (e.g., daily, weekly, monthly)? Do you require specific types of reports such as compliance reports, incident summaries, or performance metrics? ***Weekly or monthly are both acceptable.***

51. Are there any administrative policies in place that govern how changes to security configurations, access controls, or monitoring rules are managed and approved? Who will be the primary point of contact for day-to-day management and coordination between your internal teams and the MDR provider?
This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.

52. What is your current process for requesting and approving changes to your security environment, and will the MDR provider be expected to follow this process? ***We have an internal Change Control process and team.***

53. How do you currently handle invoicing and billing with service providers? Is there a specific system or format you require for invoices from the MDR provider? Do you require fixed-cost pricing for services, or would you prefer a more flexible, usage-based pricing model? ***There is* **n*****o specific system/format required for invoicing. Please provide your most competitive pricing model available within your proposal.***

54. Are there any service level agreements (SLAs) in place for other service providers that the MDR provider will need to align with?
This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.

55. What are your expectations for response times and resolution times for different levels of incidents? Do you have specific SLAs or escalation procedures for critical incidents? How are you currently reporting and tracking SLAs and KPIs?

This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.

56. Do you require any assistance from the MDR provider in managing procurement processes for security tools, licenses, or other technology components? ***No***
    a. What percentage of the yearly operating budget is dedicated to MDR activities in support of threat detection, response, and overall security management? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

57. What is JJC's estimated monthly volume of alerts generated in SIEM and true positive rate? An MDR vendor should be able to ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

58. Does JJC have any specific requirements for the location or geographic presence of the vendor's SOC/MDR operations? ***Within the U.S.***

59. What percentage of the whole environment is integrated with SIEM today? (This info is required to plan for growth projections) ***Vendor should be able to make assumptions in regard to the size of the organization.***

60. What is the current average and peak EPS (events per second)? ***This information will not be provided as part of the solicitation process.***

61. Please provide the individual counts for the following assets across your environment: Servers: (Windows, Linux) Workstations: (Windows, Linux, macOS) Network Devices: (e.g., Firewalls, Routers, Switches) Security Solutions: (e.g., WAF, VPN, Proxy, DLP, etc.) ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

62. Could you please provide details on the types of licenses currently assigned to users in the O365 tenant? Examples may include Office 365 A3, A5, etc. ***A5; We have no licensing concerns.***

63. Could you please provide information on the configured daily data capping and data retention policies? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

    Are there any specific security standards that you require compliance with, such as HIPAA, PCI, ISO 27001, or others? ***We use the NIST Cybersecurity Framework. Some regulatory requirements we report to are GLBA, FERPA, PIPA, HIPAA***

64. Could you please confirm if JJC is also seeking Threat Intelligence and Threat Hunting services in addition to the requested SOC services? ***This is referenced in the RFP. Vendors can make inferences from the information already provided.***

65. How are incidents currently handled at JJC? Is JJC currently utilizing any automated response or SOAR tools? If so, could you please provide details on the tools being used? ***This should not be relevant to provide a proposal. Vendor should be able to build a proposal without this information.***

66. Is scope for staff only or are students also included? • How many total employees/workers in scope? o Count considered information workers? o Count considered frontline workers (grounds keeper, maintenance, custodial, food service, etc.) • Is JJC utilizing Microsoft E5/F5 or equivalent licensing? • If so how many licensed users for staff/college? How many for students? • Are Microsoft Defender XDR components (Defender for Identity, Office 365, Cloud Apps and Entra ID Identity Protection deployed? • How many Microsoft Defender for Endpoints are licensed (workstations/laptops/servers)? o Is this license for Plan 1 or Plan 2 for MDE? • Is JJC utilizing Defender for Cloud - Defender for Servers for their servers? o If so, how many servers? o If so, Is this license for Plan 1 or Plan 2 of DFS? • For Microsoft Sentinel, how many current or in scope individual security data source types for scope (Palo Alto NGFW is an example of one)? • RFP mentions existing analytics rules for MS Sentinel, are these custom or out of the box? o How many custom analytics rules, if applicable? • For vulnerability management, does JJC currently have a tool in place? o If so, which product? o How many assets/IPs are currently being scanned? • Any other compliance certifications or controls frameworks that JJC adhere to, besides those outlined in the RFP? • To protect the privacy of our customers, are references able to be introduced at a later date after down selection? ***2150 staff, ~20,000 students. This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

67. How are alerts/events currently triaged at JJC? Is there an ITSM or ticketing tool being used for this process? If yes, could you please provide details on the tool? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

68. If answer for above question is no, does JJC expect to implement a new ITSM solution as part of the proposed services, or would you prefer to integrate with Inspira's MSSP ITSM solution? ***This information will not be provided.***

69. Is JJC looking for the management of Microsoft Defender as part of the scope of services? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

70. Is scope for staff only or are students also included? ***Employees***

71. How many total employees/workers in scope? Count considered information workers? Count considered frontline workers (grounds keeper, maintenance, custodial, food service, etc.) This is answered already. ***~2150.***

72. Does it mandatory to have experience with higher education/government clients? ***This is preferable.***
    a. Can we show our similar experience in other industry? ***Experience in other industries may be considered.***

73. Is JJC utilizing Microsoft E5/F5 or equivalent licensing? ***A5***

74. If so how many licensed users for staff/college? ***~2150*** How many for students? ***NA***

75. Are Microsoft Defender XDR components (Defender for Identity, Office 365, Cloud Apps and Entra ID Identity Protection deployed? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC***

76. Any additional Services to be Provisioned? • Incident Response Retainer services • Threat Intelligence Platform • Digital risk protection • Attack surface management • Advanced Threat Hunting • SOAR Platform Implementation • Playbook As a Service • Breach and attack Simulation • Digital Forensics and Incident Response ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

77. How many Microsoft Defender for Endpoints are licensed (workstations/laptops/servers)? Is this license for Plan 1 or Plan 2 for MDE? ***We have enough licensing to cover our devices, proposers do not need to be concerned about MS licensing.***

78. Is JJC utilizing Defender for Cloud - Defender for Servers for their servers? If so, how many servers? If so, Is this license for Plan 1 or Plan 2 of DFS? ***We have enough licensing to cover our devices, proposers do not need to be concerned about out MS licensing.***

79. For Microsoft Sentinel, how many current or in scope individual security data source types for scope (Palo Alto NGFW is an example of one)? ***This information will not be provided. Vendors can provide pricing and make inferences from the information already provided within the RFP and organizations the size of JJC.***

80. RFP mentions existing analytics rules for MS Sentinel, are these custom or out of the box? How many custom analytics rules, if applicable? ***Out of the box. There may be a very small amount that are custom.***

81. For vulnerability management, does JJC currently have a tool in place? If so, which product? How many assets/IPs are currently being scanned? ***Vendor should be able to make assumptions from what has been provided.***

82. Any other compliance certifications or controls frameworks that JJC adhere to, besides those outlined in the RFP? ***We use the NIST Cybersecurity Framework. Some regulatory requirements we report to are GLBA, FERPA, PIPA, HIPAA***

83. To protect the privacy of our customers, are references able to be introduced at a later date after down selection? ***References need to be provided with the proposal. Do not share any sensitive data of your other customers.***

84. Can JJC provide the number of SOFTWARE AND LICENSES required. Full Licenses (Indicate if there are different Tiers in Licenses) Limited Licenses Unassigned DIDs Agent Licenses. ***Vendor should provide pricing tiers. And any thresholds where pricing would change.***

85. How many employees need the training? ***3-10***

86. Does it mandatory to meet the 30% goal for BEP utilization?
No, it is not mandatory to meet the 30% goal; however, please keep in mind that your commitment to diversity is weighted at 20% for the RFP evaluation. Please see page 7 of the RFP document to learn what commitment to diversity entails.

87. Clarification on Scope of MDR Services: “Do you expect the MDR vendor to provide full threat mitigation services, or will the vendor’s role be limited to threat escalation and notification to your internal team?” ***Vendors can provide pricing for full threat mitigation and pricing for simple escalation and notification.***

88. Security Architecture Integration: “You mention integration with Microsoft Azure Sentinel, Microsoft Defender for Endpoint, and Palo Alto NGFW. Are there other security tools or products in your environment that will require integration, or are these the only ones?” ***We cannot provide further details.***

89. Compliance and Reporting: “Could you clarify the specific compliance standards the MDR solution needs to address? Are there particular certifications (e.g., SOC2, ISO27001) that are critical to your compliance requirements? ***NIST Cybersecurity Framework***

90. Data Handling and Storage: “You require that data be stored within U.S. data centers. Are there any specific retention policies or data sovereignty rules that we should be aware of for this project?” ***GLBA, FERPA, PIPA, HIPAA. It is a priority for JJC policy to keep data handling and storage within the US.***

91. Incident Response Responsibilities: “In the event of a critical security incident, what level of involvement do you expect from the MDR provider in terms of hands-on incident response, versus simply alerting your internal team?” ***Some level of remediation should take place before handing off.***

92. Endpoint Coverage: “For coverage under the MDR solution, do you require protection across all endpoints (servers, workstations, mobile devices), or are certain device types prioritized for monitoring?” ***There would likely be tiered monitoring.***

93. Vulnerability Management: “Does JJC currently have a vulnerability management program in place, or would you expect the MDR provider to establish and manage that as part of this engagement?” ***Vulnerability management is not in scope for this MDR RFP.***

94. Onboarding and Implementation: “Could you provide more details on your expected timeline for the onboarding process, and do you have any preferred milestones or deliverables during the implementation phase?” ***We would like to onboard as soon as possible, vendors should provide their timelines and average turnaround.***

95. Third-Party Access: “Will the MDR provider need administrative access to JJC’s systems, and if so, are there specific protocols or third-party agreements we should adhere to?” ***There is a 3rd party agreement provided that details this.***

96. Success Metrics and Reporting: “Could you clarify your preferred reporting frequency and the specific metrics you would like to see in MDR performance reports (e.g., number of threats detected, mean time to respond)?” ***Weekly or Monthly is fine, this is flexible***

97. Can you confirm the number of FTE users in your environment that excludes adjuncts, students, interns, and service accounts? This information will help us align our proposal accurately to your staffing profile.. ***2150 staff, ~20,000 students***

98. I'm aware that JJC requires a minimum payment term of Net 45. Would JJC consider upfront annual payment? We offer discounts for upfront annual payments. ***The college will not pay more than one year at a time.***

99. Is the BEP required even if the solution offered does not call for the need of a partner?
Please see the response to question #87.

100. We price based on source counts. A source is defined as workstations, firewalls, servers and any SaaS applications. Can you please provide a breakdown of these? We don't need specifics, just number of sources. ***Rather than JJC providing numbers, please provide your pricing structure and if there are thresholds with specific pricing changes.***

101. Does JJC utilize any cloud environments? (AWS, Azure, GCP) ***Yes AWS and Azure are used.***

102. Is JJC keeping Microsoft Azure Sentinel in place, or is JJC seeking to replace Microsoft Azure Sentinel with another SIEM? ***AZ Sentinel is***

preferred.

103. Does JJC expect the MDR to manage Microsoft Azure Sentinel? ***Managing some alerts from Azure, especially after business hours would be considered in scope to this RFP.***

104. Is JJC open to a vendor providing their own SIEM and MDR Service as a direct replacement for MS Sentinel, assuming vendor is able to provide equal value, if not more, than Sentinel? ***This would be considered.***

105. Could you please provide the total number of workstations, including servers, desktops, and laptops, in your environment? ***We have ~2150 employees, please make an inference from that.***

106. Could you also share any preferred partners or resellers that the College typically engages for purchases? ***This information is not needed for this RFP.***

107. Additionally, could you please provide the College's Tax Exemption Certificate? ***The college's tax exemption certificate can be shared with the awarded vendor.***

108. Rapid7 offers various MDR solutions tailored to the College's requirements. One option combines MDR/SOC as a service and Vulnerability Management. Is Vulnerability Management outside the scope of this RFP, or would the College prefer to see both options (MDR Standalone and MDR with Vulnerability Management)? ***Vulnerability Management is out of scope, but vulnerability notifications per se are not.***

End of Addendum #2

Addendum #2

DATE: September 13, 2024

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO: Prospective Respondents
SUBJECT: Addendum No. 2
PROJECT NAME: Managed Detection & Response Services
JJC PROJECT NO.: R25001

Please acknowledge receipt of these addenda by including this page with your proposal. Include your company name, printed name, title, and signature in your acknowledgement below. Failure to do so could result in disqualification of your bid.

Issued by:

Matt Stephenson
Senior Director of Business & Auxiliary Services
Joliet Junior College
815.280.6643

I acknowledge receipt of Addendum #2.

____
Company Name

____
Printed Name

____
Title

____
Signature