Clear Form

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA
SCHOOL BOARD ADMINISTRATION BUILDING
Procurement Management Services
1450 N.E. 2nd Avenue, Room 650
Miami, FL 33132

Direct All Inquiries To
Procurement Management Services
Buyer's Name: Charisma Montfort
PHONE: (305) 995- 2364
Email: cmontfort@dadeschools.net
TDD PHONE: (305) 995-2400

BID/RFP ADDENDUM

Date: 5/20/2021

Addendum No. 2

BID/RFP No. RFP-20-046-CM BID/RFP TITLE: Security Information & Event Management (SIEM)

This addendum modifies the conditions of the above-referenced BID/RFP as follows:

Please see attached responses to submitted questions. All other terms and conditions apply.

All information, specifications terms, and conditions for the above-referenced BID/RFP, are included on the document posted on the Procurement Management website at http://procurement.dadeschools.net

The attached pages containing clarifications, additional information and requirements constitute an integral part of the referenced bid. If your bid/proposal has not been submitted, substitute the pages marked REVISED and mail your entire bid/proposal package.

I acknowledge receipt of Addendum Number _____

PLEASE NOTE: If your firm has forwarded a copy of this bid/proposal to another vendor, it is your responsibility to forward him/her a copy of this addendum.

(PLEASE TYPE OR PRINT BELOW)

LEGAL NAME OF BIDDER: _____

MAILING ADDRESS: _____

CITY, STATE ZIP CODE: _____

TELEPHONE NUMBER: _____ E-MAIL _____ FAX # _____

BY: SIGNATURE (Manual): _____
OF AUTHORIZED REPRESENTATIVE

NAME (Typed): _____ TITLE: _____
OF AUTHORIZED REPRESENTATIVE

RFP-20-046-CM

Security Information & Event Management (SIEM)

1. On page 25 for the minimum requirements, section c, it states the five year requirement. Are we not eligible to bid if we do not meet the five years, or will it just be scored according based on experience.
   The Selection Committee will score you according to your submitted years of experience.

2. In trying to put together a scope, we are trying to narrow down the total number to go off of for licensing. It is usually per employee instead of per endpoint, which makes it more affordable for the organization. Should we assume the total number to be an estimated 41,000, which is what is shown on the school boards website?
   Log sources will include devices not only used by staff, but also those used by students as well as infrastructure equipment, etc. Ingestion volume or eps may be a better model for licensing. On the management side, there will be less than 20 end users of the solution.

3. Regarding the RFP for the SIEM Project, we are curious if the Miami-Dade SD Mainframe (zSeries) environment is within the scope?
   While we are not an enterprise SIEM provider, we offer best-in-class solutions for zSeries Security, including automated detection and response, plus our mainframe-specific SIEM solution, Command Center. This is not currently in scope, but please feel free to include a proposal that includes this option in the event the project scope changes.

4. Who would we submit the final proposal to for the SIEM RFP?
   Please submit your proposal per the requirements specified in Section 6 of this RFP.

5. Can you please provide quantities for the following log source types from the RFP?
   (Ranges provided for scoping considerations)
   a. Cisco ASA/Firepower 0-5
   b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
   c. Active Directory. 0-750 servers
   d. Radius 0-400 servers
   e. Support current industry-standard antivirus solutions
   f. Fortigate 0-100
   g. Windows/IIS 0-1250 servers
   h. Linux 0-20
   i. Office 365 Yes
   j. Tenable Nessus Professional 0-10
   k. SAP 0-200 Windows Servers
   l. Intrusion Prevention Systems 0-500
   m. Intrusion Detection Systems 0-500
   n. VMWare Virtual Center. 0-750 Hosts
   o. In-scope servers. 0-4000
   p. In-scope endpoint/workstations 0-500,000

6. If possible, can you please provide estimated events per second or Gigabytes for the scoped environment?
   If this is not known, we will use the information above to estimate size/architecture. Events per second 45,000 @ ~ 10kb per message

7. Can you please provide a total number of Active Directory accounts (users and service accounts)?
   0-1,000,000 Both active and retired

8. Is there a minimum requirement for both searchable data retention (hot/warm) vs cold data retention?
   There is no minimum requirement, per se; however, a preference would be a minimum of 3 months hot/warm. Please provide pricing for cold data retention and retention ranges if applicable.

9. Is there a preference between a virtualized environment, a HW solution, or a cloud based SaaS solution?
   No preference.

10. Will you accept DocuSign in lieu of notary due to COVID restrictions?
    Please submit notarized signatures. Electronic notary is acceptable.

11. What is the current AV and EDR solution being run on your in-scope servers and endpoints/workstations?
    Blackberry Cylance and Microsoft Defender for Endpoint

12. How many resources have been designated to manage the SIEM?
    3 resources will have shared responsibility for managing the SIEM (among other functions)

13. How will Security Incident responses be handled?
    Incident responses will be evaluated internally and escalated as necessary.

14. Would MDCPS consider a hosted “SIEM-as a Service” model of delivery?
    Yes

15. Would MDCPS consider a fully managed SIEM/SOC solution that includes managed SIEM and Security Event alerting/investigation?
    This solicitation is for a system that will be monitored/managed by internal staff; we are not currently looking for a managed solution.

16. Does MDCPS currently have an on-premises SIEM solution?
    Yes

17. What are the deployment expectations?
    Easily deployed with central management of agent versions, etc.

18. Does Miami-Dade have multiple SIEMs?
    No.

19. How many logs is Miami-Dade estimated to currently ingest daily? (in gigabytes, Gb)
    45,000 @ ~ 10kb per message

20. Does Miami-Dade currently work with an MSSP or MSP for security operations?
    No.

21. Approximately how many employees are on the Miami-Dade security operations team?
    3
22. Approximately how many employees are on the Miami-Dade infrastructure and SIEM management team?
    3

23. Does Miami-Dade currently have SOAR capabilities for automated response to security incidents?
    No.

24. Does Miami-Dade currently have a multi-cloud SaaS/IaaS environment? Will multiple instances of specific SaaS apps need to monitored - e.g. Salesforce? Will multiple instances of infrastructure cloud environments need to be monitored - e.g. AWS?
    O365,AWS,Azure.

25. What is the current Miami-Dade annual estimated SIEM vendor costs, including storage, log ingestion, and licensing?
    We currently host our own solution in our own datacenter.

26. Does Miami-Dade currently have threat hunters that perform proactive discovery for indicators of compromise?
    No; currently limited capabilities.

27. What is Miami-Dade's annual estimated hardware and storage costs for on-premises infrastructure related to your current SIEM?
    We currently host our own solution in our own datacenter

28. Does Miami-Dade currently manage multiple Active Directory forests?
    Yes; 2

29. Does Miami-Dade currently manage multiple O365/Azure AD tenants?
    Yes, 2

30. Does Miami-Dade have a centralized security operations team or a decentralized security operations team that will leverage the SIEM solution?
    Yes.

31. Does Miami-Dade have any compliance requirements to store SIEM log data beyond 365 days for compliance? If so, what timeframe?
    No compliance requirements, per se; however, if your solution allows for archiving or longer-term storage, please include this as an option.

32. Does Miami-Dade use specific Linux Distro's in the current IT environment? If so, which distros?
    No.

33. Does Miami-Dade use a centralized IT service management solution for ticketing? If so, which one? If not, can the list of decentralized systems be provided?
    Ivanti ISM

34. Does Miami-Dade currently monitor security event logs across all schools in the county or is each school responsible for security monitoring?
    All schools are monitored centrally.

35. Does Miami-Dade require the SIEM solution to maintain additional compliance certifications beyond PCI-DSS?
    PCI-DSS is not required…ISO 27001 and/or SOC 1, 2 are required for hosted solutions.

36. What is the estimated minimum/maximum for log data ingestion (GB per day)?
    - e.g. Min = 200GB/day, Max = 1TB day 45,000 @ ~ 10kb per message

37. What is the estimated EPS (events per second) for the critical / important log sources required for baseline security monitoring?
    45,000 @ ~ 10kb per message

38. Is there a current provider we are competing against?
    This is a first-time solicitation.

39. Where is the data currently reside/where is it stored?
    On-Prem

40. What is the count of logs looking to be supported, broken out by log source type? 45,000 @ ~ 10kb per message

41. What is the scope of the monitoring (is it only the internal devices or also the external devices)?
    Internal Devices and Cloud tenants.

42. Do you want monitoring for all laptops or is monitoring the endpoint solution's logs on all the laptops sufficient?
    No/ We would monitor the endpoint solution

43. What SAP products are you looking to be supported?
    SAP ECC, PY and other SAP Core Services

44. Is the anticipated contract start date (7/16/21) the start of the one-month test period?
    No, the one-month test period will start at the time there is a fully executed contract.

45. ***Is your environment currently tuned to a specific level?
    More clarity is needed

46. Does M-DCPS have an existing staff of security analysts that will monitor/review/triage alerts and content from the SIEM or do you desire the vendor to provide these services?
    M-DCPS currently has an existing staff, but please include any options your company has for escalation.

47. If M-DCPS does have an existing staff of security analysts how many are there?
    3

48. For Maintenance or Updating of the SIEM, does M-DCPS desire the vendor to perform these tasks in support of the M-DCPS staff?
    No we would like to maintain and update our systems if services on-prem.

49. ***In Solution Criteria section on 42 please clarify if all supported advices. Is a through p all the support devices.

(Ranges provided for scoping considerations)

a. Cisco ASA/Firepower 0-5
b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
c. Active Directory. 0-750 servers
d. Radius 0-400 servers
e. Support current industry-standard antivirus solutions
f. Fortigate 0-100
g. Windows/IIS 0-1250 servers
h. Linux 0-20
i. Office 365 Yes
j. Tenable Nessus Professional 0-10
k. SAP 0-200 Windows Servers
l. Intrusion Prevention Systems 0-500
m. Intrusion Detection Systems 0-500
n. VMWare Virtual Center. 0-750 Hosts
o. In-scope servers. 0-4000
p. In-scope endpoint/workstations 0-500,000

50. Do we have to maintain PCI compliance?
    PCI-DSS is not required…ISO 27001 and/or SOC 1, 2 are required for hosted solutions.

51. Confirm that the proposal due date is May 20, not May 11th
    The deadline for proposals is May 25, 2021.

52. May we be provided with the "District's Cybersecurity Plan" as referenced in section 4.2 – Purpose of Request for Proposals in the RFP?
    In order to protect the integrity of the District network, no details regarding plan elements will be shared at this time.

53. If our business offices are located outside of Miami-Dade County how should we submit Exhibit 4, Local Business Affidavit of Eligibility, i.e. – should we mark it as "not-applicable"?
    Please mark Not Applicable.

54. Will the logs be retained only for the purpose of the SIEM provider or will they be for other purposes?
    Logs may be retained for SIEM, Data Integrity and Possible Law enforcement Investigations.

55. Will the logs be subject to retention compliance purposes?
    Yes

56. Do you have an estimate of the number of events per second being logged across your environment today?
    45,000 @ ~ 10kb per message

57. As a follow up to question 19 will this represent the entire environment subject to SIEM services?
    Yes

58. Reference RFP page 27, subpoint 6 on that page: "Provide a response to all of the items listed in Section 4 and 7 of this RFP." I am unsure exactly what in Section 7 of the RFP should be addressed within our Section 6 response; please provide complete clarity in this regard.
    Section 7 is for informational purposes only. There is no submission attached to Section 7.

59. Reference RFP pages 34-35: "Bidders shall be required to provide, at the time of submittal of their bid, evidence of insurance coverages and limits meeting, at a minimum, the following requirements"… In which of the prescribed sections should be include our evidence of insurance or should we include it in an appendix?
    The certificate can be included as an appendix.

60. What is the total number of logs per second to be monitored?
    45,000 @ ~ 10kb per message

61. How many endpoints?
    0-500,000 managed endpoints

62. Which of the following solutions is M-DCPS looking for?
    a. Managed Service with the solution to be managed and maintained by a third party?
    b. Product with professional services for implementation and training?
    c. Product only

    M-DCPS is looking for a product that can be implemented with professional services and possibly training.

63. Does M-DCPS deploy any assets or services in the cloud?
    a. If so, which clouds do they use?
       AZURE and AWS should be supported

64. Can you list any SaaS, IaaS, PaaS services they might integrate in your environment?
    LMS or any cloud services.

65. Can you list out any security tools/services that you may want to integrate with the SIEM platform?
    AV,IDS/IPS, Firewall

66. Can you tell us how you are protecting your endpoints (EDR/Anti-Virus/Anti-Malware solutions)?
    Cylance, Microsoft Defender, Trend Micro

67. Do you have any thoughts on how many EPS (events per second) you are currently creating in your environment for the existing monitoring solution?
    45,000 @ ~ 10kb per message

68. Does M-DCPS currently use a log-management system?
    a. If yes, could you please identify the current solution to enable an enhance response on any potential data conversions.

       We cannot currently disclose what our solution is; please make sure your solution can ingest syslog and raw json events.

69. Does M-DCPS have an estimate of the volume of log data to be ingested by the SIEM? If not, is it acceptable to respond with a pricing table that offers pricing?
    45,000 @ ~ 10kb per message

70. Is a high-level network diagram available?
    No

71. Could M-DCPS
    a. Numerate the number of internet gateways
    b. Quantity and brand of firewalls
    c. List any additional security devices for log analysis
    d. List the quantity and types of other (non-security) devices for log analysis

(Ranges provided for scoping considerations)

    e. Cisco ASA/Firepower 0-5
    f. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
    g. Active Directory. 0-750 servers
    h. Radius 0-400 servers
    i. Support current industry-standard antivirus solutions
    j. Fortigate 0-100
    k. Windows/IIS 0-1250 servers
    l. Linux 0-20
    m. Office 365 Yes
    n. Tenable Nessus Professional 0-10
    o. SAP 0-200 Windows Servers
    p. Intrusion Prevention Systems 0-500
    q. Intrusion Detection Systems 0-500
    r. VMWare Virtual Center. 0-750 Hosts
    s. In-scope servers. 0-4000

t. In-scope endpoint/workstations 0-500,000

72. ** What is the expected data volume to be sent to the solution? Either in EPS or GBs per day.
45,000 @ ~ 10kb per message

73. Is this data volume expected to change or remain relatively constant? (for example, are students included in this or are they expected to be added later?)
This would reflect a consistent Data volume, and students are included in this calculation.

74. ** Data retention requirements (hot / cold) – how long do the logs need to be retained?
At least 3 months hot. However, Archiving or cold storage is needed for records purposes and can be up to a year.

75. Use cases for the solution (data exfiltration, compromised credentials, compliance reporting, ransomeware, etc.) – any specific business outcome that the organization is trying to accomplish.
Yes, please include all use cases mentioned above ideally all SIEMS should have the capability to detect anomalous behavior at scale. As well as give us more visibility into our network.

76. What Data sources (logs, etc.) are available or are expected to be collected.
All major systems, please make sure that the syslog standard is supported if unsure.

77. Do you prefer a cloud-based solution, on-premise, or hybrid?
No preference.

78. Do you currently have another SIEM solution?
Please see response to Question 38.

79. Can you please provide quantities for the following log source types from the RFP?
    a. (Ranges provided for scoping considerations)
    b. Cisco ASA/Firepower 0-5
    c. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
    d. Active Directory. 0-750 servers
    e. Radius 0-400 servers
    f. Support current industry-standard antivirus solutions
    g. Fortigate 0-100
    h. Windows/IIS 0-1250 servers
    i. Linux 0-20
    j. Office 365 Yes
    k. Tenable Nessus Professional 0-10
    l. SAP 0-200 Windows Servers
    m. Intrusion Prevention Systems 0-500
    n. Intrusion Detection Systems 0-500
    o. VMWare Virtual Center. 0-750 Hosts
    p. In-scope servers. 0-4000
    q. In-scope endpoint/workstations 0-500,000

80. If possible, can you please provide estimated events per second or Gigabytes for the scoped environment? If this is not known, we will use the information above to estimate size/architecture.
    45,000 @ ~ 10kb per message

81. Can you please provide a total number of Active Directory accounts (users and service accounts)?
    805,000 Both active and retired

82. Is there a minimum requirement for both searchable data retention (hot/warm) vs cold data retention?
    3 months hot. However, Archiving or cold storage is needed for records purposes and can be up to a year.

83. Is there a preference between a virtualized environment, a HW solution, or a cloud based SaaS solution?
    No preference

84. Will you accept DocuSign in lieu of notary due to COVID restrictions?
    Please see response to Question 10.

85. What is the current AV and EDR solution being run on your in-scope servers and endpoints/workstations?
    Cylance, Trend Micro, Windows Defender

86. Page 21, #54 "Does the solution currently provide the ability to detect lateral movement on a network through the use of honeypot sensors?" Regarding the request for the use of honeypot sensors, does M-DCPS already have access to honeypot sensors from another vendor or would these be provided by the selected Service Provider?
    This RFP is only for SIEM we will not request anything additional.

87. Page 19, #42 Log Sources If possible, Service Providers may benefit from the obtaining the following information to help understand the scope of the services. What system are you using for RADIUS authentication? Is it tied to Active Directory or another IdP service? Approximately how many users are in Active Directory and Office 365?
    - Please provide the following to help with quoting:
    - # of Firewalls (include model number)
    - # of Domain Controllers
    - # or users in O365 and any other SaaS applications
    - # of endpoints

(Ranges provided for scoping considerations)

b. Cisco ASA/Firepower 0-5
c. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
d. Active Directory. 0-750 servers
e. Radius 0-400 servers
f. Support current industry-standard antivirus solutions

g. Fortigate 0-100
h. Windows/IIS 0-1250 servers
i. Linux 0-20
j. Office 365 Yes
k. Tenable Nessus Professional 0-10
l. SAP 0-200 Windows Servers
m. Intrusion Prevention Systems 0-500
n. Intrusion Detection Systems 0-500
o. VMWare Virtual Center. 0-750 Hosts
p. In-scope servers. 0-4000
q. In-scope endpoint/workstations 0-500,000

88. Page 20, #43.cc "Provide incident resolution on an as-needed basis" Regarding this request, is this a request for the Service Provider to include a formal Incident Response retainer as part of the RFP response?
No this RFP is for SIEM, we welcome the inclusion of such a service but it is not a request.

89. Are there any bandwidth constraints for each district?
Yes bandwidth is a consideration when we select a solution.

90. What is the bandwidth size available for each District?
Please list each site. 100 MBPS at least at every site.

91. What are the quantities of cloud data sources to be monitored (number of O365 users, number of virtual workloads, etc.)?
We currently utilize O365 and have approximately 300,000 users. Plus on prem workloads.

92. What are your current ingestion rates (EPS and/or data volume per day)?
45,000 @ ~ 10kb per message

93. Can virtual or physical infrastructure be placed at each District if the design calls for it?
Yes

    a. What are the quantities of each data source or device within each district?
    MDCPS is one district; In-scope endpoint/workstations 0-500,000

94. RFP 6.2 Response Format 27 6) Proposed Approach and Methodology Provide a response to all the items listed in Section 4 and 7 of this RFP. Section 7 of the RFP contains information regarding the evaluation and selection process and does not have defined questions like Section 4 of the RFP. There are also sections in the Proposal Response Format dedicated to the Evaluation Criteria found in Section 7 of the RFP (Proposal Response Sections 6, 7, 8, and 9).
Please see response to Question 58.

    To avoid being redundant, please clarify which portions of RFP Section 7 we need to respond to in Proposal Response Section 6 to be compliant?
    Please see response to Question 58.

95. RFP Exhibit 4 40 Local Business Affidavit How significant is the preference given to local businesses? Is there a numerical value associated with the local preference status?
    Please refer to Section 1 – XX of the Instructions to Bidders of the solicitations.

96. Multiple exhibits included in the RFP require signature by a notary. Will you accept virtual notary signatures?
    Yes.

97. 4.3 Scope of Services 15 3) Provide details demonstrating level of alignment to:
    - District environment of Microsoft IIS
    - SQL Server
    - .NET framework
    - Windows Active Directory
    - Microsoft Windows Server
    - Request clarification. Does level of alignment refer to configuration, metrics, effort, or something else?

      Please elaborate.

(Ranges provided for scoping considerations)

a. Cisco ASA/Firepower 0-5
b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
c. Active Directory. 0-750 servers
d. Radius 0-400 servers
e. Support current industry-standard antivirus solutions
f. Fortigate 0-100
g. Windows/IIS 0-1250 servers
h. Linux 0-20
i. Office 365 Yes
j. Tenable Nessus Professional 0-10
k. SAP 0-200 Windows Servers
l. Intrusion Prevention Systems 0-500
m. Intrusion Detection Systems 0-500
n. VMWare Virtual Center. 0-750 Hosts
o. In-scope servers. 0-4000
p. In-scope endpoint/workstations 0-500,000

98. 4.3 Scope of Services 18 41) Does your product allow for seamless integration with existing District SQL server databases to allow automatic data import and export, such as Clever, Inc.? If yes, describe how.
    a. Is this question about whether there is an authentication component that would be used to log forwarding? How is Clever, Inc. used in the context of forwarding security logs to a SIEM solution? Please provide an example.

    The reference to Clever was an unintended artifact;
    The intent of the question was to determine whether it is possible to dump data into SQL for storage, and does your solution allow for import from existing log aggregation tool or a SQL database?

99. 4.3 Scope of Services 23 93) Does the solution provide a manager dashboard for visibility by the manager? Please provide details pertaining to this functionality. Is this question about a technical manager (or administrator), a project manager from the MSSP, or a manager from SBMDC? Please define "manager."
The manager would be an M-DCPS employee.

100. Do you prefer a cloud-based solution, on-premise, or hybrid?
No preference

101. Do you currently have another SIEM solution? If so, are you looking to replace?
Yes/Yes

102. First deployment is going to be faculty and teachers? And later students?
All critical systems would be deployed first, regardless of whether the application impacts student or staff.

103. How you anticipate phasing out the project?
Critical functions first then additional systems will be added as the need arises.

General RFP

104. Who is the project's sponsor?
The owner department is Information Technology.

105. How is this project being funded?
The project is being funded by various sources.

106. What is the budget allocated for this project?
The budget is to be determined.

107. Is there an expected completion date? If so, what is it?
The project timeline will be negotiated with the awarded vendor.

108. Will M-DCPS select just one vendor to provide these services?
Yes

109. Did M-DCPS have an outside firm help in preparing the RFP? If yes, will that firm be allowed to bid on this project?
No outside firm was used in preparation of the RFP

SIEM Monitoring Service(s)

110. Does M-DCPS currently have a SIEM they are replacing? If so, what SIEM is currently being used and why is M-DCPS considering replacing the current SIEM?
Yes, more functionality and more visibility.

111. Is M-DCPS looking for a vendor to provide 24x7x365 Managed, Detect, and Respond (MDR) services?
No we prefer to manage our own services and systems.

112. Is M-DCPS looking for a vendor to supplement existing 24x7x365 Managed, Detect, and Respond (MDR) services?
No we prefer to manage our own services and systems.

113. Is M-DCPS looking for a product vendor to implement a SIEM solution without 24x7x365 Managed, Detect, and Respond services?
No we prefer to manage our own services and systems. We will escalate issues internally as needed.

114. Monitor, Detect & Respond
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

115. 24 x 7 | off-hours | hybrid | custom monitoring coverage
No we prefer to manage our own services and systems. We will escalate issues internally as needed.

116. What is M-DCPS's Log Collection & Storage requirements (some level of collection/storage will be required to support Analysis and Response)
3 months hot.
Warm storage 6 months,
Archiving or cold storage is needed for records purposes and can be up to a year.

117. Does M-DCPS's wish to include Vulnerability Identification (Scanning) as part of the services? If so, how many External/Internal IP addresses will be in scope and what would the frequency (monthly, quarterly, annually) of the scans be.
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

118. Does M-DCPS's wish to include Penetration Analysis (Pen Testing) as part of the services? If so, how many External/Internal IP addresses will be in scope and what would the frequency (monthly, quarterly, annually) of the scans be.
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

119. What security solutions is M-DCPS currently using?
    a. Anti-Virus
    b. Endpoint Detection & Response
    c. Intrusion Detect/Intrusion Prevention
    d. Content Filters
    e. Etc…

Blackberry Cylance and Microsoft Defender for Endpoint
(Ranges provided for scoping considerations)

    a. Cisco ASA/Firepower 0-5
    b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
    c. Active Directory. 0-750 servers

d. Radius 0-400 servers
e. Support current industry-standard antivirus solutions
f. Fortigate 0-100
g. Windows/IIS 0-1250 servers
h. Linux 0-20
i. Office 365 Yes
j. Tenable Nessus Professional 0-10
k. SAP 0-200 Windows Servers
l. Intrusion Prevention Systems 0-500
m. Intrusion Detection Systems 0-500
n. VMWare Virtual Center. 0-750 Hosts
o. In-scope servers. 0-4000
p. In-scope endpoint/workstations 0-500,000

120. Will M-DCPS need the SIEM to address any Compliance Reporting requirements? If so, what compliance requirements need to be addressed?
Possibly HIPPA and COPPA

121. Does M-DCPS need the SIEM to provide Cloud Services Monitoring? If so, what Cloud environments/services will be in scope?
AWS, Azure.

122. How many isolated network segments exist across the M-DCPS network?
2

123. Is M-DCPS expectation to deploy to all schools (600+) under one tenant or to a multi-tenant instance maintains it's own identity will be part of the collective whole?
A multi-tenant deployment would be easier to manage. One tenant

124. Will schools have security admins who want access to the data? If so, it makes sense for a separate multi-tenant instance with Miami as the parent and the schools as children.
Initially only Security staff will manage the data.

125. Do you know what the total Events Per Seconds (EPS) are currently being generated by all in scope schools.
45,000 @ ~ 10kb per message

126. What is M-DCPS's data retention requirements?
a. Our standard is 7 days of HOT Storage, 90 days of WARM storage and 365 days of COLD storage. Data retention levels can be adjusted to meet your requirements.
b. HOT storage data - Ability to Search data (spotter functionality) with indexed data- Millisecond response to search queries.
c. WARM storage data - data retrieval time 1-8 min for avg queries, complex ones may take longer time.
d. COLD storage data - searchable cold storage.

3 months hot. Warm storage 6 months, Archiving or cold storage is needed for records purposes and can be up to a year.

127. Are there specific threat scenarios (Use cases) that concern M-DCPS the most?
   a. Based on the data sources provided in the RFP the use cases would allow for cyber (malware), and light DLP.
   This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

128. What is the scope of the one-month evaluation period?
   a. Number of Schools
   b. Number of Employees
   c. Number of Students

The evaluation period is not a trial but a return policy assuming the implementation fails, and we cannot get it to work.

129. What will be the acceptance criteria for the one-month evaluation period? Successful implementation.

130. Number of Hosts to be Monitored

Number of Firewalls and each make/model?
(Ranges provided for scoping considerations)

   a. Cisco ASA/Firepower 0-5
   b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
   c. Active Directory. 0-750 servers
   d. Radius 0-400 servers
   e. Support current industry-standard antivirus solutions
   f. Fortigate 0-100
   g. Windows/IIS 0-1250 servers
   h. Linux 0-20
   i. Office 365 Yes
   j. Tenable Nessus Professional 0-10
   k. SAP 0-200 Windows Servers
   l. Intrusion Prevention Systems 0-500
   m. Intrusion Detection Systems 0-500
   n. VMWare Virtual Center. 0-750 Hosts
   o. In-scope servers. 0-4000
   p. In-scope endpoint/workstations 0-500,000

131. Any Web Application Firewalls?
See ranges provided for monitored hosts.

132. DNS Server (Microsoft, BIND, etc.)?
See ranges provided for monitored hosts.

133. Any Netflow capabilities?
We are in the initial stages of implementation.

134. Number of Infrastructure devices (routers, switches, etc…) and each make/model?
See ranges provided for monitored hosts.

135. Number of Servers and each make/model/OS?
See ranges provided for monitored hosts.

136. Number of Active Directory or Ldap Servers?
See ranges provided for monitored hosts.

137. Number of and any specific files, if file integrity monitoring is an objective
We welcome any additional services provided by the vendor but at this time, this RFP is for a SIEM

138. Number of endpoints (workstations) and each make/model/OS In-scope endpoint/workstations 0-500,000; Major brands should be considered.
OS support from 2012 server to Windows 10 and some Macs.

139. Does the Client have a virtual environment that can host the SIEM sensor virtual image?
Yes

140. ***Number of Virtual Services and make and model?
VMware ESX and Cisco UCS

141. What, if any, cloud environment would be in-scope (AWS, Azure, O365, etc.)?
Azure AWS, O365

142. Can you share your network diagrams?
No

143. Can you share an asset inventory for in-scope devices by asset type?
No

144. How many locations are in-scope for collection and monitoring? Are these locations reachable from a single site; are these sites independent / segmented?
Over 400 locations in distinct metropolitan areas.

145. How many isolated network segments exist across the network?
2

146. How many employees/contractors/vendors/interns have access to the network that will be monitored?
60,000

147. Do you know your current Events Per Second (EPS) for in-scope networks?
45,000 @ ~ 10kb per message

148. Do you know your current number of logs to be monitored for in-scope networks?
More clarification needed.

149. What other security controls do you have in place (IDS, EndPoint / EDR, Proxies, etc.)?
This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

150. For user data enrichment, we typically connect to either Active Directory or an HR system to add employee name, org, supervisor, etc. to data analysis. Does your AD have additional information, Full Name, Title, Department, Supervisor, Location, etc? Alternatively, is there an HR or other system you would like us to connect with to add that information?
Yes/Yes

Internet

151. Number and location of Internet ingress/egress points
400+/- current locations

152. Internet Pipe size at each ingress/egress
100 mbps synchronous

153. List of remote/branch sites if applicable
This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

154. At the very end of the Pre Proposal call, a number of 194 Million Events Per Second was mentioned. That seems extremely high. Can you confirm the correct Events Per Second number?
45,000 EPS @ ~ 10kb per message

155. For accurate sizing we need a count by system type. So, number of generic servers, number of Domain controllers, number of Database servers, IIS servers, etc. Number and type of firewalls, basically the number of each of the item types listed in question 42.

(Ranges provided for scoping considerations)

a. Cisco ASA/Firepower 0-5
b. Cisco switches/routers/firewalls/Wireless controllers and access points 0-1500 total devices
c. Active Directory. 0-750 servers
d. Radius 0-400 servers
e. Support current industry-standard antivirus solutions
f. Fortigate 0-100
g. Windows/IIS 0-1250 servers
h. Linux 0-20
i. Office 365 Yes
j. Tenable Nessus Professional 0-10
k. SAP 0-200 Windows Servers
l. Intrusion Prevention Systems 0-500
m. Intrusion Detection Systems 0-500
n. VMWare Virtual Center. 0-750 Hosts
o. In-scope servers. 0-4000
p. In-scope endpoint/workstations 0-500,000

156. You indicted some very high EPS rates on the call. Can you give us the size of those logs on disc? So how much space in GB or TB does 7 days or 30 day (whatever you can best measure) of that log data take up on disc?
45,000 EPS @ ~ 10kb per message

157. You have mentioned wanting to take actions to contain or remediate a breach or attack or run a Playbook in a few places in the RFP. This is what a SOAR addon to the SIEM can do. Do you want a price to add this capability quoted?
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

158. How Many Servers do you have in scope of security monitoring (Separate by Windows, Linux etc.)?
See ranges provided for monitored hosts.

159. Do the student devices exist in the same AD instance as the district devices?
Yes.

160. Does the district want to monitor student devices?
Yes; however, this does not necessarily mean logging directly from student devices, but possibly activities originating on student devices such as RADIUS or AD authentication, etc.

161. How Many Laptops/Desktops do you have in scope of security monitoring?
See ranges provided for monitored hosts.

162. How many total locations do you have and how are they connected today?
About 400 locations @ 100 mbps

163. What is your requirement for log retention?
3 months hot. Warm storage 6 months, Archiving or cold storage is needed for records purposes and can be up to a year.

164. How many devices do you want to license SIEM for?
Log sources will include a total scope of up to 1 million devices; log information will not necessarily come directly from each host.

165. What is the EPS (Events per second)?
45,000 @ ~ 10kb per message

166. On the call you mentioned 194,452,000 EPS. Can you translate this to GB/Day?
45,000 @ ~ 10kb per message

167. What is the Events per Second (EPS) on the existing log aggregation product?
45,000 @ ~ 10kb per message

168. Log volume in Gigabytes per day would also be a useful answer. The number given in the call of 194,000 EPS would create ~ 7,805 GB/day which is more data per day then we were told

the existing log aggregation product has.
45,000 @ ~ 10kb per message

169. What is the Endpoint Detection & Response (EDR) product?
This can affect the data ingestion volume and may be important in correctly estimating the cost. Blackberry Cylance and Microsoft Defender for Endpoint

170. Request a 5 day extension for final proposals based on time to consolidate all submitted questions, answer and republishing of answers in order to allow appropriate time for adjustments necessary.
The deadline for this solicitation is Tuesday, May 25, 2021.

171. 2. Can the district please clarify Evaluation Criteria questions 1-3? Is the expectation that the SIEM vendor provide technical scope without access to the current network or network diagrams? To what extent are we expected to respond? Page 15.
Yes, Please provide reference specs.

172. 3. Can the district please clarify Evaluation Criteria question 5? Is the expectation that the SIEM will be operated and maintained by the District and not the contractor? What FTE roles in relation to the SIEM is the contractor expected to provide? Page 15
The expectation is that the District will manage the SIEM

173. 4. Can the district please clarify Evaluation Criteria question 6? Is a general network diagram required or will we be provided the district's network diagram with which to demonstrate how our solution will integrate? Page 15
Please provide diagrams for typical implementations

174. 5. Can the district please clarify Evaluation Criteria questions 27 & 28? Is the expectation that the SIEM will be operated and maintained by the District and not the contractor? What FTE roles in relation to the SIEM is the contractor expected to provide? Page 17
Please provide a description of training models/resources that vendor is capable of providing.
The expectation is that the District will manage the SIEM.

175. 6. Can the district please clarify their definition of ASB and non-ASP as they apply to the evaluation criteria for this proposal? Pages 17-8
Application Service Provider questions apply to vendor-hosted applications

176. 7. Can the district please clarify Evaluation Criteria question 43? Is the contractor required to also provide cyber intelligence analysts to read and act on the SIEM reports? Or does the contract only cover procurement, deployment and maintenance of the SIEM?
At this time, we are looking only for a SIEM solution and implementation services, maintenance will be taken over by district staff. Page 19

177. 8. Can the district please clarify Evaluation Criteria question 47? Is the expectation that the SIEM will be operated and maintained by the District and not the contractor? What FTE roles in relation to the SIEM is the contractor expected to provide? Page 20
Please provide a description of training models/resources that vendor is capable of providing.
The expectation is that the District will manage the SIEM.

178. 9. Under Section G (Type of Business Organization and Authority of Signatory) on page 3, the RFP states: "As to other types of business organizations, please provide any and all documentation relating thereto..." What specific types of documentation should be provided? Page 3
Please submit documentation requested under the minimum requirements section of the solicitation.

179. 10. Under Section I.A (Proposer Qualification Form) on page 3, the RFP states: "Proposer Qualification Form qualifies the Proposer and the proposal and must be completed and submitted as page 1 of the proposal." However, page 27 states that Exhibit 1 found in Section 10 "is to be used as the cover page for the Proposal." Can the School Board please clarify which form is to be the first page of the proposal? Page 3
The first page of the proposal should be Exhibit 1 – Cover Page.

180. 11. Section 6.2 (Response Format) on page 27 lists the required proposal tabs/sections. Should each tab/section be submitted as a separate file or can offerors combine tabs/sections into one file? Page 27
The way in which you submit is up to you. One file is preferable.

181. 12. For ease of completion, can the School Board please provide Microsoft Word versions of all Exhibits?
Unfortunately, we are only able to provide the PDF version of documents.

182. How many end-user computing instance (e.g., notebook, laptop, workstation, VDI instance) are within the monitored environment? In-scope endpoint/workstations 0-

500,000

183. What type of operating systems are the end-user computing instance running?
Mostly Windows 10 and major server operating systems

184. How many servers (physical/virtual) are within the monitored environment?
3000

185. What type of operating systems are the servers (physical/virtual) running?
2008,2012,2016,2019

186. Will Microsoft Defender for Endpoint installed on all servers and all end-user computing instances?
Yes

187. What type of Office 365 license do you have?
A3

188. What ticketing systems does the IT Support/Security team use?
Ivanti

189. What is the count and composition (role/responsibility) of the security team who will be needing access to the SIEM?
3 members with multiple responsibilities not SIEM exclusive.

190. What Cloud Platform will be monitored (Azure, AWS, Google, Other)?
Azure, AWS

191. What Cloud Applications will be monitored?
At this time none that we are aware of.

192. What endpoint protection and prevention (EPP or NGAV) will you be using?
Blackberry Cylance and Microsoft Defender for Endpoint

193. What product is being used for Radius?
Windows server and NPS

194. What model of Cisco ASA/Firepower is being monitored? How many? Standalone or High Availability?
This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

195. What model of Fortigate is being monitored? How many? Standalone or High Availability? This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

196. What product is being used for Intrusion Prevention Systems? How many? Standalone or High Availability? This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

197. What product is being used for Intrusion Detection Systems? How many? Standalone or High Availability?
This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

198. How many systems are scanned by Tenable Nessus Professional?
0-500,000

199. To monitor Microsoft IIS, a log forwarding agent on the host is needed. What log forward agent will you be using?
We were hoping SIEM solution would provide an agent. In a case where this is not available we would utilize Sysmon.

200. To monitor Microsoft SQL Server, a log forwarding agent on the host is needed. What log forward agent will you be using?
We were hoping SIEM solution would provide an agent. In a case where this is not available we would utilize Sysmon.

201. To monitor .NET framework, a log forwarding agent on the host is needed. What log forward agent will you be using?
We were hoping SIEM solution would provide an agent. In a case where this is not available we would utilize Sysmon.

202. To what extend do you need an Assessment? Could you provide additional context for what expectations you have for this service?
We were hoping SIEM solution would provide an agent. In a case where this is not available we would utilize Sysmon. This RFP is for SIEM; we welcome any other services the provider will include but this is not a requirement or request at this time.

203. To what extend do you need Threat Monitoring and Communication Strategy? Could you provide additional context for what expectations you have for this service?
This RFP is for SIEM; we welcome any other services the provider will include but this is not a requirement or request at this time.

204. To what extend do you need incident resolution on an as-needed basis? Could you provide additional context for what expectations you have for this service?
This RFP is for SIEM; we welcome any other services the provider will include but this is not a requirement or request at this time.

205. Do you need the SIEM vendor to provide a 24/7 Tier1/Tier2 Security Analysis team to investigate and respond to SIEM alerts?
This RFP is for SIEM; we welcome any other services the provider will include but this is not a requirement or request at this time.

206. Log Management for Cisco Umbrella is accomplished by you configuring Cisco Umbrella to upload logs to what is called a 'bucket' (essentially a folder within AWS's S3 environment). A bucket for your Umbrella logs can be hosted by Cisco in one of two ways: Which do you intend to use with Cisco?
    a. Administered, managed and paid for by you, the company administrator.
    b. Administered, managed and paid for by Cisco Umbrella. We would prefer the provider handle all aspects of SIEM functionality if the service is SaaS or hosted on a public cloud.

207. Could the team please clarify the estimated data ingest rate for scoping purposes of the SIEM? During the Q&A call, the figure of roughly **4.6 Billion Events Per Month** was given; later the figure of **194 Million Events Per Second** was referenced. Understanding that specific data sources--and logs ingested from those sources--may change, what is the baseline data ingest rate that M-DCPS would like to use to scope the solution for the RFP?
45,000 @ ~ 10kb per message

208. Could you please share the recording link for the pre-bid conference for the SIEM RFP which occurred on May 11, 2021?
Please see attached.

209. Reference to MFA and May 11th are in the document… please correct

This solicitation is solely for Security Information and Event Management (SIEM).

210. Please provide all the questions Posted in Chat and their responses. Or a link so we can review.
   a. In the past, questions and answers were not considered official response(s) unless submitted and answered via Addendum.
   b. In case you need… here are the questions from Chat…. So, we can have an official answer.

211. What is the deadline to submit "Proposal Acknowledgment"?
The deadline for this solicitation is May 25, 2021.

212. How many Staff Members need to be trained on the SIEM solution?
3

213. Are you planning to send an addendum? In the 1st page-"Proposer Acknowledgment" indicates May 11th as well as in the page 65 (Opening bid) it says May 11th and it refers to MFA.
This addendum addresses the deadline as well as the topic of the solicitation.

214. Ms. Montfort ... how long after the Q&A are published will the due date be set? and if an extension is required, can you give us enough lead time.

We will try to give as much lead time as possible.

215. Are you planning to send written response to all the questions sent it via email?

Answers to all submitted questions are posted via the online Addendum.

216. Do we still have to get our responses notarized if we are submitting electronically?
Please see response to Question 10.

217. The RFP references the district's overall Cyber Security Plan. Is there a document for that which will be made available or which is available now?
In order to protect the integrity of the District network, no details regarding plan elements will be shared at this time.

218. Will M-DCPS operate the SOC that uses the SIEM or should this be part of the solution?
This solution will be operated by M-DCPS staff. The expectation is that the District will manage the SIEM.

219. Will all these questions posted in the CHAT be officially respond with the Addendum.
Chat questions are included in this addendum.

220. I did not see anything relating to total daily log volume. Can you share the log volume data with us?
45,000 @ ~ 10kb per message

221. Name of solution do you currently have?
Due to policy issues, we cannot name the current solution.

222. What is the expected data volume to be sent to the solution?
Either in EPS or GBs per day. 45,000 @ ~ 10kb per message

223. Please clarify the ongoing support and management requirements for the RFP. I thought the RFP included ongoing device/platform management and I just heard you say the county will take over ongoing management.
If the solution is cloud hosted support and management will be required from the provider. If the solution is hosted on prem we can run maintenance.

224. Any Cloud resources to be used as data sources to be monitored by the system?
O 365, AWS, Azure

225. If you submit hard copy do you still have to submit electronically?
Yes, for more information, please refer to Section 6.

226. Is this data volume expected to change or remain relatively constant? (for example, are students included in this or are they expected to be added later?
45,000 @ ~ 10kb per message

227. Are you able to share the name of the log management solution you currently have and are looking to augment?
No

228. How many devices such as: Network Devices, Severs, Laptop/Desktop, Cloud Solutions (AWS, Azure, Google, etc.)?
0-500,000; AWS,Azure, O365

229. how long do the logs need to be retained?
3 months hot. Warm storage 6 months, Archiving or cold storage is needed for records purposes and can be up to a year.

230. Did U hear 1 billion events months?
45,000 @ ~ 10kb per message

231. Does M-DCPS deploy any assets or services in the cloud?
a. If so, which clouds do they use?
O 365, AWS, Azure

232. What Data sources (logs, etc.) are available or are expected to be collected.
Please make sure proposed solution can utilize syslog or other industry standard for logging.

233. For support - do you require an onsite resident?
No

234. What type of ticketing system will the solution need to integrate with?
Ivanti

235. 4b plus events in what time frame?
45,000 EPS @ ~ 10kb per message

236. What is the SAP Software solution you have in place as listed in the RFP?
SAP ECC, PY and other SAP Core Services

237. Please calcify the data volume. He referenced 4.6B events. Is that per month?
45,000 EPS @ ~ 10kb per message

238. Do you have a current reference architecture that can be shared?
No

239. Does Miami-Dade currently monitor security event logs across all schools in the county or is each school responsible for security monitoring?
All Schools are monitored centrally.

240. What is your current log storage capacity?
45,000 @ ~ 10kb per message

241. Does Miami-Dade currently manage multiple Active Directory forests and or manage multiple O365/Azure AD tenants?
Yes; potentially 2 AD forests and 2 O365/Azure AD tenants

242. What is the endpoint protection system Miami-Dade currently utilizing?
Cylance, Trend Micro, Windows Defender

243. Does Miami-Dade currently have threat hunters that perform proactive discovery for indicators of compromise?
No

244. In the RFP question 8 - one-month test period. Could you speak to this question? Is the purpose of this to be a POC prior to purchase?
Please see response to Question 44.

245. Can you tell us how you are protecting your endpoints (EDR/Anti-Virus/Anti-Malware solutions)?
Cylance, Trend Micro, Windows Defender

246. Can you list out any security tools/services that you may want to integrate with the SIEM platform?
This information will not be disclosed publicly; applicable information will be provided to the entity providing the successful bid.

247. Is it safe to say that you are looking for a SIEM, EPP+EDR License solution and support?
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

248. if we present same solution as you currently have what will be your course of action? migrate to the new platform? will you need history logs for how long?
Yes, 3 months hot. Warm storage 6 months, Archiving or cold storage is needed for records purposes and can be up to a year.

249. Does Miami-Dade require the SIEM solution to maintain additional compliance certifications beyond PCI-DSS?
We require ISO-27001, SOC1 or SOC 2 compliance for hosted solutions.

250. Will implementation of the SIEM be part of RFP response or are you looking for a pure tech play via resell?
We would welcome managed services to implement system and provide training. The district is looking to manage the SIEM solution.

251. Do you require FedRAMP for SaaS Solutions?
Not at this time

252. is CASB or XDR integration an expected requirement after SIEM deployment?
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

253. can the endpoint data be collected from a console or cloud?
Cloud or console are fine.

254. Given the concerns regarding divulging log sources, can we assume that Miami Dade would be responsible for aggregating all logs (local or cloud log host(s) to be consumed by the SIEM?
Yes, if the solution provided scales.

255. Does Miami-Dade use a centralized IT service management solution for ticketing? If so, which one? If not, can the list of decentralized systems be provided?
Ivanti

256. And will you restart the RFP process if the solution selected not scale?
The Selection Committee will decide on the solution that is in the best interest of the District.

257. is the expectation 24x7 vendor IR support?
The District is not looking into SaaS, rather a self-managed SIEM. The District will evaluate incidents in-house, but an option to escalate to IR services (potentially at an increased cost) would be welcomed if available.

258. Any Database logging required - what type, how many?
0-300 SQL servers.

259. Is StateRamp compliance a requirement?
Not at this time.

260. Do you require encryption at rest if hosted
Yes NIST SOC 1 or SOC 2 Compliance would require it.

261. Are you looking for ANY support from a managed detection and response provider? 24/7 monitoring support?
This RFP is for SIEM we welcome any other services the provider will include but this is not a requirement or request at this time.

a. Cylance / Microsoft / Sysmon total endpoints - what's the count of endpoints and will you ingest logs from all of them?
Yes, we would ingest from all sources. In-scope endpoint/workstations 0-500,000

262. How many logs per second are projected?
45,000 EPS @ ~ 10kb per message

263. FedRAMP is a comprehensive cybersecurity assessment that is required by Cloud Service Providers to service Federal government. State and Local government has been adopting this requirement across the country. It is more comprehensive security assessment then ISO 27001 and SOC2. https://www.fedramp.gov/

264. Clever – are you using this for authentication and SSO, or is that Active Directory based? Furthermore, would you like to use Clever or AD for User Analytics?
The reference to Clever was an unintended artifact; The intent of the question was to determine whether it is possible to dump data into SQL for storage, and does your solution allow for import from existing log aggregation tool or a SQL database?

265. How soon after the contract is awarded do you require implementation to start? When do you need to have it completed?
As soon as the procurement process is complete, we would like to begin implementation as soon as possible.

266. Does Miami-Dade currently have SOAR capabilities for automated response to security incidents?
No

267. Are proposers able to submit multiple options for deployment methods - on-prem and cloud?
Yes

268. If there is no requirement for FedRAMP compliance nor StateRAMP compliance, does the vendor have to be ISO27001 or SOC 1, SOC2 compliant? If so, will Teaming Agreements or JVs be accepted in response?
Yes ISO 27001 or SOC 1 or SOC 2 compliance is required.

269. are you looking to ingest log data only or do you have requirement to ingest raw packets into SIEM through a Network TAP at the Data center
Log data only at this time.

270. Would you be open to an XDR/MDR solution response or just a SIEM only?
Please provide details about any proposed solutions; the current RFP is for a SIEM, but additional functionality may be considered if the cost/value is appropriate.

271. Was that 194 million EPS?
45,000 EPS @ ~ 10kb per message

272. Is all US hosting and all us soil support required?
Yes

273. Was the EPS provided for all data sources?
45,000 EPS @ ~ 10kb per message

274. To confirm did you state that US hosting only was a requirement?
Yes

275. In the last page 65 – Opening Instructions. The Information refers to Multi-Factor Authentication and also refers as May 11th as opening date, Is this a mistake? Are you planning to send an addendum?

276. What is the deadline to send a "Proposer Acknowledge" In the RFP documents (1st page) indicates that the due date for proposal is today May 11th, however the Deadline to receipt proposal according to the schedule is May 20th, could you please clarify?
The deadline for receipt has been extended through May 25, 2021.

277. Question number 8: one-month test period post implementation sign off.
What would the testing process look like exactly? Is this considered to be the POC (Proof of concept)? Will this be required to all vendors, or only to the selected vendor? Is this before or after a purchase is made?
Please see response to Question 256.

278. Questions number 29 and above: ASP.
Would this mean SaaS (Software as a Service) with MSP (managed service provider)?. Or does this refer to a SaaS offering without MSP?
SaaS without MSP

279. Question number 40: transition plan that will allow the District's team to successfully manage year two and beyond What is the plan for year one (1)? Under this RFP's requirements, who would be responsible for managing the solution on year one? Provider+MDCPS
Is this referring to MSP? Does the first year need to be managed by the MSP vendor and then transition to Miami-Dade Schools on year two ? Who should be responsible for managing the solution after Professional Services completes their part and does the hand off until year two?
MDCPS

280. Question number 42: Third party required devices/software that will need to be monitored - What IPS/IDS system does M-DCPS have? What AntiVirus solution does M-DCPS use? Please list all or indicate which are your solutions that need to be monitored that are Cloud

Blackberry Cylance, Windows Defender; additional information regarding District solutions will be disclosed to successful bidder.

281. Question number 43:
Are all of these requirements itemized from q. To jj. Applicable only to vendors who can provide a Managed Service Solution through an MSP?
Please respond to items that are applicable to what your organization can provide.

282. Question number 59: Are you asking if a GPO is required for our product or solution to work with Windows logs, or, is the question if our product or solution can make use of a GPO when working with Windows logs if desired by M-DCPS?
Can implementation be installed/configured using GPO also can the solution parse active directory logs and extract useful information.

283. Question number 82: What is it meant by sensor? Is this term referring to a data collector, or to an entity capable of analyzing data, or something else?
Yes, this would refer to an agent to push data to server.

284. Question number 85: Does the solution provide global search functionality with pre-built reporting for common use cases? Would need more clarity about what is expected from a global search functionality. Global in terms of how many different data sources can be searched at a time?
A global search function would allow the enterprise to perform a search across all systems in a preselected period for specific actions. Alternatively, AI could raise critical issues observed after analyzing data.

285. Would you please provide one or two examples of common use cases that would require pre-built reporting capabilities?
What is it meant by 'pre built' reporting capabilities? These are report templates (ie. Reports for management vs technical

286. Question number 100: This question needs more clarification please. What is EPS: Events Per Second, or something else? What is it meant by 'the billing/licensing needs to be reduced in proportion to the costing provided'? Can you please provide an example describing the situation depicted?
45,000 EPS @ ~ 10kb per message

287. Is the goal for the School District to manage the SIEM internally, or are you looking specifically for a managed SIEM offering?
The goal is to manage the SIEM internally.

288. How many FTE's will be managing the SIEM? Are there dedicated FTE's for this product?
3

289. Is there a preference for on premise, or BYOL cloud, or SaaS deployment for this solution?
No preference.