COLUMBUS METROPOLITAN LIBRARY

MEMORANDUM

To: All Interested Vendors

From: Procurement Department, Columbus Metropolitan Library

Date: June 24, 2025

Subject: Addendum No. 1
RFP 25-015 – Security Incident and Event Management (SIEM) Purchase and Implementation – E-Rate Schools and Libraries Cybersecurity Pilot Program

Summary of Pre-Proposal Meeting
Questions and Answers

Part I. Summary of Pre-Proposal Meeting: On Wednesday, June 18, 2025 at 11:00 a.m., the Columbus Metropolitan Library ("the library") conducted a Pre-proposal meeting for RFP 25-015 **Security Incident and Event Management (SIEM) Purchase and Implementation – E-Rate Schools and Libraries Cybersecurity Pilot Program.**

The meeting was held online via Microsoft Teams. The library sent the following representatives:

- Mona Mawalkar, Procurement Manager
- Brad Kamlet, Procurement Compliance Specialist
- Karl Jedretzky, IT Manager of Infrastructure Services
- Keith Levell, IT Manager of Information Security

The following companies sent representatives:

- Arctic Wolf
- C1
- CBTS
- Coro Cybersecurity
- Crown Castle
- Custom Computer Specialists
- Cyberleaf
- DataServ
- EasyIT
- Fortinet
- Jean Kongolo ETI-LTD
- Laketec
- MNJ
- Palo Alto Networks
- Shearer Intelligence
- Softchoice
- VEIT
- XTEK Partners
- Xtel
- Xtel Communications

Part II. Questions and Answers

Q1) Is the expectation for the vendor whose awarded this contract to also manage the SIEM platform moving forward? Or is this just to help stand up the platform then the internal IT team would manage moving forward?
A1) The vendor awarded the contract will provide assistance with the implementation and data integration of the SaaS SIEM platform, after which CML will handle management and ongoing operations.

Q2) Are you looking for only a SIEM tool or also the management of the SIEM and MDR services for all devices?
A2) The vendor awarded the contract will provide assistance with the implementation and data integration of the SaaS SIEM platform, after which CML will handle management and ongoing operations.

Q3) If looking for a managed solution, is it required to be internal W-2 employees or are 3rd party resources sufficient assuming valid documentation is included?
A3) We are not considering a managed solution for this initiative.

Q4) Do you intend to remain with Microsoft Defender P2 for endpoint protection or are you open to other options?
A4) We are not considering new endpoint protection services for this initiative.

Q5) Is this a managed service to support the SIEM or with CML be managed the SIEM? Post implementation, does CML wish to have this solution managed as a service?
A5) The vendor awarded the contract will provide assistance with the implementation and data integration of the SaaS SIEM platform, after which CML will handle management and ongoing operations.

Q6) What type of Microsoft cloud licensing does CML have or will be purchasing in the next quarter?
A6) Microsoft A5/E5 licensing.

Q7) Is there a priority order for integration into the technology and items outlined in 1.4 Scope E?
A7) There is no preferred CML sequencing order for data integrations, unless the tool has data prerequisites.

Q8) Can you elaborate on the technical staff that would assist on this project? Would a CML network engineer be available to assist and elaborate on CML's network security requirements.
A8) Internal technical resources, including CML's Infrastructure Services team, will be available. The team brings network engineering expertise to support system architecture and integration

Q9) What does CML's Microsoft Defender deployment look like currently?
A9) Defender A5/E5 stack: Defender for Endpoint, Defender for Office P2, Defender for Cloud Apps, Defender XDR, Entra ID Protection, Defender Vulnerability Management.

Q10) What is the current management platform for the 750 Windows Workstations? Who manages this?
A10) CML uses Microsoft Intune to manage these Windows 10/11 workstations.

Q11) Part F clarification. Can part F be clarified with exactly what the customer is seeking. For example, does this mean run books and if so, how many?
A11) CML anticipates that the SIEM will offer predesigned out-of-the-box runbooks/playbooks based on security best practices, that can be slightly modified if needed and match CML's technology stack in 1.4E. This includes automated SOAR workflows as listed in 1.4I.

Q12) Part G clarification Do you know what Feeds you want already? What ones do you have today? Are you interested in any vendor recommendations?
A12) Today we have feeds from servers, firewalls, sniffing appliances, and Entra. We would like to start ingesting from workstations, Meraki, Umbrella, and Defender. CML is open to considering vendor data feed recommendations.

Q13) Part H clarification Is building and configuring analytics part of this section? Can you elaborate on "pre-made" dashboard expectations please?
A13) Pre-made dashboard is used in this instance to refer to dashboards that come preconfigured within the SIEM tool, and those that may have already been developed by a vendor or user community.

Q14) Note of validation - For non-Microsoft integrations, a syslog server is required (or 2 for redundancy purposes). Are we to assuming CML will provided appropriate vm's for this role?
A14) CML does not currently maintain a traditional standalone syslog server. Instead, we utilize a centralized syslog aggregation point paired with a SIEM agent as part of our current logging and security infrastructure. A similar architecture can be implemented to support non-Microsoft integrations, and CML can provision the necessary virtual machines to support this role, including redundancy if required.

Q15) If a vendor has the capability to provide all desired additional integrations now and in the future, would you all consider a managed or co-managed solution?
A15) We may consider a co-managed solution.

Q16) Could you please clarify the audit and reporting expectations for vendors under the FCC Cybersecurity Pilot Program, including the expected frequency, format, retention period, audit types, and any preferred tools or platforms for compliance documentation?
A16) Even though vendors are not direct recipients of the FCC Cybersecurity Pilot Program, the selected vendor will play a critical role in helping CML meet its reporting and audit obligations under the terms of the program. *FCC Public Notice DA-25-53, issued on January 16, 2025*, is the authoritative source for all service provider audit, reporting and compliance requirements.

Q17) Are there specific performance benchmarks or SLAs for log ingestion and alert response times?
A17) We would expect log ingestion to be within 1 minute of real time

Q18) Which compliance frameworks (e.g., PCI DSS, HIPAA) are prioritized, and are there any reporting templates required for audit readiness?
A18) We do not believe CML has any audit readiness requirements on this project.

Q19) Post implementation, does CML wish to have this solution managed as a service?
A19) The vendor awarded the contract will assist with the implementation and data integration of the SaaS SIEM platform, after which CML will handle management and ongoing operations.

Q20) Does the solution include pre-built content or templates that align with specific compliance frameworks such as NIST CSF, NIST 800-171, or CIS Benchmarks?
A20) The solution should include pre-built visualizations and dashboards for the mass market products that we deploy

Q21) Does the proposed SIEM solution allow the customer full administrative access to configure, customize, and directly manage log ingestion, retention policies, correlation rules, dashboards, and compliance reporting without relying on a managed service provider?
A21) Yes

Q22) Would it be possible to obtain a copy of the transcript or recording from the June 18, 2025, pre-proposal meeting for RFP CML #25-015?
A22) The transcript was created to help record questions during the meeting. All questions asked during the meeting are included in this addendum, along with their corresponding responses.

Q23) Does the 80GB daily ingest include all of the data from the CML data sources (CISCO and Meraki Firewall Logs, Defender Endpoint)?
A23) This is an estimate of total ingestion.

Q24) How many playbooks are actively being used in Defender XDR E5 and what are they?
A24) Only built in AIR. We are currently not using a SOAR system.

Q25) Does the library use a threat feed(s) today, what are they?
A25) No additional third-party threat feeds are in use at this time.

Q26) Does the library have a Threat Intelligence Management (TIM) solution, if so what is it?
A26) No additional third-party threat feeds are in use at this time.

Q27) Does the library use an Attack Surface Management (ASM) solution today, if so what is it?
A27) The library does not currently use a formal dedicated Attack Surface Management (ASM) platform. However, we do maintain external attack surface monitoring through:

- Nessus vulnerability scanning, which is regularly used to scan internal and external assets.
- Federal external IP scans — we participate in external scanning provided by federal partner

Q28) Is the 90 day log retention requirement for hot searchable data, Cold storage or both? If both, what is the retention period for either?
A28) 90 days of hot searchable data, no retention required after that.

Q29) What's the current daily Elastic document ingestion rate?
A29) Our current ingestion is ~11mill documents/day.

Q30) Do we want to see SOAR licensing included?
A30) Though SOAR is not currently in use in our environment, our A5 licensed Defender deployment supports it. We would entertain a SOAR licensing line-item addon to the proposal as an optional cost.

Q31) Are you guys able to disclose the current product you're using?
A31) Our existing SIM is being hosted by Expedient, and it is an Elastic-based SIM tool

Q32) Are you looking to cover all your endpoints as part of the SIM or is it strategic with certain endpoints for your SIM?
A32) It is strategic, but the count provided In the RFP is correct. We are mainly looking at the workstations for staff.

Q33) Does your current SIM provide you with the event per second counts I see in the RFP? We have the GB per day, but do you guys have your EPS numbers?
A33) The 80 gig per day is an estimate, as adding all of those workstations which are not currently monitored.

Q34) I saw on the RFP that you wanted it to be a cloud hosted SIM. Is that going to live in your cloud environment or were you wanting it to live in in another cloud environment?
A34) We are anticipating a different cloud environment, a hosted solution with an ingestion rate of how much we can pump into it and us not having to manage or maintain it.

Q35) This RFP is not for a managed service, but would there be a component for hosting? The reason is that many people have set it up in their own Azure environment with their own subscription, so we didn't know which model you wanted to use as per the RFP.
A35) In general, a hosted cloud service with a portal would be nice if there were something very enticing that was an appliance that ran in our Azure cloud and provided a portal.

Q36) Will CML accept a combined XDR plus Siem solutions such as Centennial, One Vigilance Pro?
A36) The workstations are very, very likely to stay on defender. It's been working very well for us, and we have no desire to swap it out as it's also built into our Microsoft licensing.

Q37) As far as storage, I noticed in the RFP it mentions 90 days for analytics.
What about archival storage?
A37) We don't do that now, and do not anticipate doing that in the future. A 90-day standard is used for many backups, and this is treated more like transient data that's moving through the system than something we want to keep forever.

Q38) You have 25 Meraki firewalls. Are all those operating independently or do they take control from essentially the umbrella platform?

A38) The Meraki product is all controlled by the Meraki Cloud portal, and we would expect that data likely comes from the Meraki API, rather than assuming you're talking about a syslog connection or some syslog collector. We now have a syslog collector as part of our elastic solution, which we use for devices that only support syslog. However, Meraki's data is ingested differently. That is something we're looking to add, but have not yet.

Q39) The automated response you are wanting it to be for the endpoint detection?
At least you wanted to be able to connect into the Microsoft defender XDR platform.
A39) We would eventually like to see integration to Microsoft Defender. We are investigating whether automated remediations utilizing Defender require additional licensing.

Q40) Are you guys open to this being managed by SoC team?
A40) We are looking to buy hosted SIM tool service, including assistance with the setup and configuration, which we will handle operationally from then on.

Q41) Moving from Expedient's Elastic-based solution, are you open to Elastic Security for SIEM (Enterprise platform; not ELK-based third-party solution)?
A41) Elastic has been a good SIM, but we find that community support and pre-made templates don't seem to be available. The learning curve was very, very steep, and the goal would be to have a more featureful solution rather than a community-driven project. We would not say that it was a non-starter because at the end of the day we're ingesting log files and researching through things.

Q42) Is the Library team open to a hosted SIEM solution that offers AI to help simplify operations and queries with an LLM to use natural language to generate hunts and reports?
A42) We anticipate AI to be shoehorned into everything at this point.

Q43) Will the vendor have access to admin-level credentials for configuration tasks during deployment?
A43) Yes

Q44) Do you have any other projects in mind that you're hoping to cover under the Cyber Security pilot funding?
A44) We are approved for the current work, and any additional work will need approval through the FCC pilot program.

Q45) What's your current E rate discount percentage 85% or 90%?
A45) For this project the discount percentage will be 90%.

Q46) Would you as an IT team, want to be involved in the deployment process?
A46) We would have to be involved. We'd want to work closely so we can take those operations over smoothly

Q47) Are you planning to take full advantage of the available funding that you received from USAC?
A47) Yes, but we are always looking for value in a vendor's proposal.

Q48) Did you want the SOAR capabilities or not? I was not clear on the previous answer.

A47) Though SOAR is not currently in use in our environment, our A5 licensed Defender deployment supports it. We would entertain a SOAR licensing line-item in addition to the proposal as an optional cost.

All Proposals must be received no later than 12:00 Noon on July 1, 2025, EST.

PROPOSERS ARE REQUIRED TO ACKNOWLEDGE THE RECEIPT OF THIS MEMORANDUM (ADDENDUM NO. 1 ON THE ACKNOWLEDGEMENT OF THE ADDENDA FORM IN THE RFP DOCUMENTS).