



Request for Proposals
SIEM & SOC

Stillwater Area Public Schools / ISD#834

1875 South Greeley Street
Stillwater MN 55082

June 26, 2023

Table of Contents

I. Introduction	3
II. Timeline	4
III. Solution Specifications	5
IV. Confidential Criteria	6
V. Proposal Requirement and Format	6

I. Introduction

Invitation to Vendors

Stillwater Area Public Schools (“the District”) invites interested vendors to provide information to the District detailing their best solutions for a custom managed security operations center with a system information and event management solution (“SIEM & SOC”).

The best solution for the district will be based on all factors, including, but not limited to:

EVALUATION FACTORS

1. Total Cost
2. Proposal meets Solution Specifications
3. Demonstrated partnerships with other districts (on-site)
4. Demonstrated ability to proactively prevent security disruptions
5. Demonstrated ability to respond to security incidents
6. Demonstrated ability to meet NIST standards

SUBMISSION REQUIREMENTS

1. Responses will be accepted at the District until 4:00 p.m., July 19th, 2023.
NO LATE SUBMITTALS WILL BE ACCEPTED.
2. Proposals must be submitted via email to PERRYJ@STILLWATERSCHOOLS.ORG and GREENS@STILLWATERSCHOOLS.ORG
3. Proposal format must be PDF. Email subject must be “SIEM & SOC RFP Response”

All questions should be directed to John Perry, Director of Learning Technology (perryj@stillwaterschools.org) with the subject “RFP”. The District reserves the right to reject any or all submittals and/or portions of submittals, to waive any informality in any procurement process and to select the proposal that provides the best solution for the District.

The District reserves the right to amend any specifications and request additional responses from each vendor at any time throughout the RFP process.

All data, documents and other products used or developed during the project will remain the property of the District upon completion of the project.

Implementation is expected to occur August 2023 - October 2023.

II. Timeline

Event	Date
-------	------

RFP Posting	June 26, 2023
Deadline to Submit Questions	July 12, 2023 (4PM CST)
RFP Responses Due	July 19, 2023 (4PM CST)
RFP Selection And Award	TBD*
Implementation / Onboarding	August 2023 - October 2023

- *The RFP Selection and Award will occur after the district evaluates responses and negotiates a final contract based on those responses. The selection and award process does not have a defined time table but is expected to be completed by the end of July.*

III. Solution Specifications

Managed SOC & SIEM Solution

- Monitor Extended Threat Detection and Response (XDR) environment
- Monitor all district switch logs, performance metrics, and change logs (including backups)
- Monitor wireless controller logs, performance metrics, and change logs (including backups)
- Monitor firewall logs, performance metrics, and change logs (including backups)
- Monitor LDAP logs, Authentication logs, and permission changes
- Monitor Google Authentication logs, including both Google direct access and 3rd party access
- Monitor Google Authentication for access in context (e.g. location, time of day, etc)
- Monitor Backup Logs for success & failures
- Monitor Backup System Logs for access / attempted access
- Monitor SMTP logs for unauthorized access/usage
- Monitor Server logs (to be defined)
- Monitor Server SNMP performance metrics (to be defined)
- Monitor Power Systems, Generators, Air Conditioning, Environment (Server Rooms)
- Regularly review & report DNS entry status
- Regularly review & report 3rd party access changes for Google Authentication
- Regularly review & report SSL certificate status
- Perform Quarterly Vulnerability Scanning on server LAN
- Perform Annual review of Google Policies and work with ISD#834 to recommend security improvements
- Regularly review & report results of vulnerability scans
- Assist with network flow documentation; establish and change management
- Assist with network diagram documentation; establish and change management
- Review SOP documentation and recommend changes (NIST Compliant)
- Review Policy documentation and recommend change (NIST Compliant)
- Develop policy threshold for intervention and mitigation when serious threats arise
- Develop policy threshold for opening and assigning support tickets to ISD#834 staff for problem resolution
- Develop policy threshold for auto account disabling when suspicious activity is detected
- Develop an Incident Response Plan with and for ISD#834 (NIST Compliant)
- Develop a Disaster Recovery Plan with and for ISD#834 (NIST Compliant)
- Operate 24/7 staffed operation center to support immediate resolutions when issues arise
- Provide SNMP dashboard that is accessible by ISD#834 staff
- Provide contracted rates for ad hoc services in addition to predefined service solutions.

IV. Confidential Criteria

- 1) Qualified vendors must be willing and able to have regular (e.g. Monthly, Quarterly) **in-person** meetings at ISD#834 facilities. The purpose of these meetings is to deliver on Solution Specifications (above) to discuss confidential security information. The District believes that on-site support will be required at times and the vendor must have familiarity with the District's sites and staff in order to provide effective services.
- 2) Vendors wishing to participate in the RFP process that can meet Confidential Criteria #1 may reach out via email (perryj@stillwaterschools.org SUBJECT: RFP) and request additional information regarding specific district systems, vendors, brands, hardware, or software information. The District may set up an onsite meeting to discuss sensitive information if it is deemed necessary to the vendor's RFP response to the District. These meetings must occur on or before July 12, 2023 (deadline to submit questions).

V. Proposal Requirement and Format

No specific format is required. Please be careful to specifically address the Solution Specifications from Section III (above). Be sure to provide local (MN/WI) examples of how the vendor can meet the Evaluation Factors from Section I. Also provide references (MN/WI) that support the examples. Cost must be clearly defined and communicated. If necessary, define multiple cost configurations depending on how the package of services is delivered. The District understands that solutions may be presented as a combination of service offerings that include software subscriptions, managed services contracts, professional service agreements, etc.. The District reserves the right to negotiate the specifics of those service packages with each vendor during or after the RFP process concludes.

If you have any questions about the format of your submission, please contact us in advance of your submission (perryj@stillwaterschools.org SUBJECT: RFP).