CITY OF TUSCALOOSA, ALABAMA

REQUEST FOR PROPOSALS
Professional Services for
Security Event and Incident Management Solution

OCA File Number: A21-1689

Issued by:

City of Tuscaloosa
Information Technology Department
2201 University Boulevard
Tuscaloosa, Alabama 35401

Date Issued: January 27, 2022
Deadline for Proposals: February 17, 2022

LATE SUBMISSIONS WILL NOT BE ACCEPTED

CONTENTS

PART 1 – OVERVIEW

The City of Tuscaloosa is requesting proposals from firms for Professional Services for a Security Event and Incident Management Solution. Part 2 of this RFP provides a general description and abbreviated scope of work for the project.

This is a procurement of professional services, and will be conducted in a manner to provide full and open competition. A Selection Committee will review all proposals, and will rank firms based on criteria identified in Part 5.

The criteria may include, but is not limited to: Solution Requirements and Agreement Suitability, Implementation Methodology Plan, Price, References and professional expertise. Upon selection by the Selection Committee, the City will enter into negotiations with the successful Respondents. Pending successful negotiations, the successful Respondents will enter into a Contract for professional services with the City.

PART 2 – THE PROJECT AND SCOPE OF WORK

The City of Tuscaloosa seeks the services of a professional firm that has the knowledge, experience and expertise to perform the services as requested.

The firm must be able to perform the following types of services upon request from the City:
Professional Services for a Security Event and Incident Management Solution for the City of Tuscaloosa including, but not limited to: Overall implementation consultation and guidance. SIEM Solution Orientation/Overview, Online Help, and Training. Guides, formats and consultation for preparation for configuration or API. Collect all appropriate data from the City's technical infrastructure and setup and configure normalizing, analysis, alerting and dashboards. Responsible for readiness, transition, production launch and handover to support.

The firm must comply with all applicable state, local, and federal regulations related to the services provided to the City. The City reserves the right, subject to negotiation and agreement, in writing, with the selected firm, to either expand or limit the scope of services as needed.

The selected firm will be required to have sufficient personnel to complete the tasks required by this scope of services. The selected firm will complete the required tasks in a timely and efficient manner. The selected facility would be expected to enter into a contract for services based upon the negotiated fee structure.

PART 3 – CONTENT OF RESPONSE TO THIS REQUEST FOR PROPOSALS

In order to facilitate the Selection Committee's evaluation, each Respondent firm responding to this request for qualifications should include the following content, in the following order:

3.1 Numerically-Scored Criteria Please answer the questions as listed below in Section 3.1 that cover the following :

- SIEM Solution Requirements and Agreement Suitability
- Implementation Methodology
- Price
- References and professional expertise

3.2 Pass/Fail Criteria

- Compliance with RFP Instructions
- Licensing and Professional Standing
- Conflicts of Interest

Each of these items is discussed in more detail in the following sections.

3.1 SIEM Solution Requirements and Agreement Suitability; Implementation Methodology; Price; and References and Professional Expertise

Indicate the number of years your company has been in business.
Where is your company headquartered?
Indicate the licensing model(s) for your SIEM (i.e., perpetual, term/subscription, or other model).
are you proposing a single product solution or solution comprised of multiple products? If the latter, describe how the multiple products are integrated.
What is the core focus of the company? Where does SIEM fall in terms of organizational priority / focus for both the company and the parent company?
Describe how the SIEM architecture "scales" in larger deployments.
Does your SIEM have multitenant capability?
Describe how your SIEM functions are integrated with other solutions that you provide as well as with other third-party technologies.
Does your SIEM support integration with other log management solutions via standards like syslog? If Yes, please explain how.
Does your SIEM solution support north bound APIs? Examples are ability to connect, via API, to other solutions like cloud services, security technologies (firewalls, IDPS, etc.), ticketing systems, etc. If so, list them, or provide a detailed data sheet where they are specifically named.
The SIEM solution shall support inbound APIs than can be used to search and/or extract data from your solution. Can your solution perform such actions? Please provide an example. An example is a ticketing, or orchestration tool to pull data out of the SIEM.

Does your SIEM solution support inbound APIs for the ability to manage and/or configure the SIEM? An example is a way for other tools, like orchestration tools, to add administrators to the SIEM.
Describe support for centralized administration in a geographically dispersed deployment.
Describe support for role-based access and delegated administration.
Do you provide integration with Active Directory or other repositories for role and resource groupings?
Describe product support for asset grouping: (1) automatic asset grouping and classification by network segment, OS, application, etc.; (2) customer-defined groups; and (3) import from external asset repositories.
The solution shall provide centralized health monitoring of itself. Please explain how your SIEM performs these actions.
Describe features that simplify deployment and support for log management and compliance reporting (SOX, HIPAA, PCI, etc.).
Describe information capture capabilities, and include a general description of available methods (system log, agent, API and/or other).
Describe support for compression, data filtering and bandwidth management of the collected data.
Describe capabilities and user interfaces to collect and parse event and nonevent data from sources not formally supported.
Describe the data management and storage tier of your SIEM, including raw data, unstructured data, parsed/enriched data and event/incident data. Provide storage limit?
Is there a log management tier that can get, and store all of the log data? If not, describe specific support for the collection, storage and management of all log data from every source.
The SIEM shall forward a filtered subset of log data in native format from the log management tier. Please explain how your SIEM performs this action.
Describe support for data archiving and restoration of event and log data, archive policy options, and support for automation.
Does your SIEM provide support for encryption of stored data? If so, explain.
Describe any protection against loss of logs during collection (i.e., storing and forwarding onto collectors, etc.).
Describe capabilities or process for preserving the digital chain of custody.
The solution shall include alerting that can be easily configured if a source stops sending log data? Please explain how your SIEM does this.
How are logs stored and what storage mediums can be used for long term retention?
What processes are required for retrieving historical data / logs stored in long term storage? Does the process require the use of any separately purchased or licensed technologies?
Indicate support for real-time correlation. Describe capabilities in your response, including tiered deployment (across log manager or server instances).
Indicate support for an event taxonomy. Describe support for event normalization from multiple sources, and enrichment, such as IP address resolution, geolocation, etc.

Can your SIEM solution ingest/normalize custom logs? If so, how does the SIEM do it? Can it be done via a graphical user interface (GUI)? Also, can it be for different types of log sources (syslog/file/database/extensible markup language/multi-line)?
Indicate the number of predefined correlation rules.
Describe support for incorporating user context in event enrichment.
Describe any user session tracking capabilities (automatically mapping user - device relationships, who is using super user/admin accounts, etc.).
Indicate support for a correlation-rule-authoring system.
Indicate support for other real-time event analysis methods, such as profiling, anomaly detection or statistical correlation.
Can users add/edit correlation rules via a GUI/Wizard?
The SIEM shall keep "risk scores" for users and other entities. Explain how your SIEM does this.
Describe data enrichment capabilities, including the number and type of available fields.
Does the solution provide drill down, pivoting, and filtering capabilities to facilitate and accelerate investigations? If yes, please explain how.
Are large search results represented in a single view or does the product paginate large search results?
The solution shall perform geolocation to IP addresses. How does your SIEM do this?
Does the solution allow for the easy creation of custom dashboards? Can dashboard views be saved and shared among groups specific to a use case such as a Security Analyst or IT Operations?
Describe any native support for incident response (IR) management and what capabilities the SIEM provides to aid in the IR workflow.
Describe security orchestration capabilities, especially where automation is used. Describe how automation is used, e.g., context enrichment for an alert, initiating response capabilities with other security controls via integrations.
List Security Incident Response Platform (SIRP) and Security Orchestration solution integrations supported out of the box.
List integrations with service desk and problem management solutions, and describe how integration is achieved (e.g., single or bi-directional via email, API, etc.).
Does the SIEM provide role-based control within workflow to support segregation of incidents and cases?
Describe any SIEM capabilities to support proactive threat hunting and investigation.
Describe integration of SIEM with solutions for automated remediation and mitigation (e.g., security operations automation, patch or configuration management tools).
Describe additional capabilities to restrict visibility of specific fields in the workflow based on role to support regions with privacy considerations.
Does the solution provide out-of-the-box alarms designed to enforce continuous compliance and security best practices? If yes, please explain.
Do email alarm notifications include risk rating priority level? How granular are the ratings? Are alarm email subject lines configurable?
How many predefined reports do you provide? In addition, provide a general description of report types.
Can users create new reports or dashboards from ad hoc queries?

Indicate support for reporting with respect to specific regulations, and list each regulation that has a specific report.
Indicate reporting with respect to specific control standards and security best practices.
Describe any advanced prescriptive analytics and/or machine learning capabilities, such as statistical anomaly detection, peer group profiling or other sophisticated analytical approaches provided by the SIEM.
Describe included user and entity behavior analytics (UEBA) capabilities (e.g., profiling, anomaly detection, prebuilt analytics, prebuilt use cases, risk rating, etc.).
Does the SIEM have an integrated UEBA capability and/or does it have integrations with 3rd party UEBA solutions? If so, explain, and list the products if integrated via a 3rd party.
Does the SIEM support predictive or forecasting analytical capabilities? If so, describe the implemented use cases, algorithms and methods.
Does the SIEM provide a threat intelligence (TI) add-on? If so, does the cost include TI feeds, or are those TI feeds available as an additional subscription?
3rd party threat intelligence feeds shall be supported by the SIEM. Explain how your SIEM does this.
Describe any support and integrations for threat intelligence platforms (TIPs; e.g., STIX, TAXII, YARA, OpenIoC or any other TI formats).
What type of security is applied to internal communications between client and server machines? What method of encryption does the solution use to encrypt messages and transactions?
Does the solution provide a way to self-audit and record user activities within the solution itself? Please elaborate on this capability.
Does the solution maintain chain of custody for all collected log data with a secure hash to deter and identify log tampering?
Do you offer management or monitoring services provided directly by your company for your SIEM? If so, briefly describe.
For this proposal, the selected vendor must work with SHI on the procurement. Does your company partner with SHI?
How many FTE or Outsourced dedicated resources needed to manage the SIEM?
Describe integration with IAM products, enterprise directories or applications (such as Web Access Management applications) that enable identity-and-access-related policies to be established as a monitoring reference within the SIEM solution.
Describe specific support for IAM policy change monitoring — user or group permission changes, file or directory permission changes, etc.
What support options are available? Describe the SLA's for support.
Describe the available training courses specifically to the proposed deployment. List the available courses and options including online, classroom, onsite, etc. Is training delivered by the vendor or by a third party?
What happens to log data when license limits are exceeded for an extended period of time, such as in a sustained attack scenario? How are overage fees assessed when licenses are exceeded? What is the threshold? Are logs ever dropped as a result? Are there penalties or access issues if license is exceeded numerous times in any given period?

Are all add-on features such as modules, compliance packages, apps, dashboards, plug-ins, etc. included in the base price of the solution? If not, provide a complete list with prices and licensing information for all add-on features that cost extra.

3.2 Pass/Fail Criteria

a. Please provide brief narrative about the Respondent's experience, history, ownership and primary clients served by the firm. Include a statement as to whether the firm is a Minority/Disadvantaged/Women Owned Business Enterprise (MBE/DBE/WBE).

b. List of the Respondent's proposed project team and those team members' qualifications and experience.

c. Recently Completed Projects. Evidence of satisfactory performance of at least three (3) recently completed projects of the type indicated above. Relevant experience will be judged on the basis of the experience of those individuals named to the firm's project team for this project. Elements of recently completed projects are as follows:

1. Address.
2. Contact person for reference.
3. Project cost.

d. Conflicts of Interest. Please identify all actual or potential conflicts of interest that would prevent the Respondent from entering into a professional relationship with the City generally, or for this project specifically. If no such conflicts exist, please include a statement to that effect.

PART 4 – INSTRUCTIONS FOR PROPOSALS

Before submitting a response to this RFP, the Respondent should carefully review the entire RFP and be familiar with its contents. The Respondent firm's submission shall be considered evidence that the Respondent has fully studied the RFP and is familiar with the general conditions to be encountered in performing the services requested.

4.1 Format of Proposals

Proposals shall be submitted in electronic format only. General brochure type information is to be kept to a minimum and the font size must be 12-point or larger.

4.2 Inquiries

The City will accept inquiries on the contents and requirements of the RFP in electronic form only. Inquiries may only be submitted by email. Inquiries should be submitted to:

Keilum Griffin, Chief Information Security Officer
Information Technology Department
City of Tuscaloosa
kgriffin@tuscaloosa.com

Inquiries must be submitted at least seven (7) days before the deadline for submission of proposals. For this RFP, the deadline for inquiries is February 10, 2022, after which time no further inquiries will be addressed by the City.

If the City chooses to respond to an inquiry, the City will do so in writing, in the form of an addendum to this RFP. The addendum will be sent to all recipients of the RFP, and will be posted to the City's website at www.tuscaloosa.com/bids.

Each addendum issued by the City shall become part of this RFP and proposals shall include any work or requirements described in the addendum. No addendum will be issued or posted less than 72 hours before the deadline for submission of responses to this RFP.

4.3 Proposal Submissions

Respondent firm submissions must be received by the City by midnight CST on February 17, 2022. Late proposals will not be accepted or reviewed. It is the Respondent's responsibility to ensure that their submission is received within the time required by this RFP. Respondents must submit proposals electronically. Electronic submissions should be made in Portable Document Format (PDF) file format, and should be sent to via email to:

Keilum Griffin, Chief Information Security Officer
Information Technology Department
City of Tuscaloosa
kgriffin@tuscaloosa.com

The Respondent's email should reference "RFP Response for Professional Services for Security Event and Incident Management Solution". The Respondent is responsible for obtaining confirmation that the City received the Respondent's proposal.

4.4 Additional Items Related to submissions by Respondent Firms

a. Submission rejection/costs

By issuing this RFP, the City does not commit to entering into a contract, to paying any costs incurred in the preparation of a submission, proposal, or to procuring or contracting for services. The City reserves the right to cancel this RFP in whole or in part, to reject any and/or all submissions and proposals, to accept the submission and proposal it considers the most favorable to the City's interests in its sole discretion, and to waive irregularities or informalities in any submissions/proposals or in the submission procedures. The City reserves the right to reject all submissions or proposals and issue a new RFP, at its sole discretion. All submissions and proposals and other materials submitted in response to this RFP will become property of the City.

b. Contract and Insurance Requirements

The City has standard contract and insurance requirements for professional services contracts, and is unable to make substantial changes to the requirements for the contract to be used for this project. The laws of the State of Alabama shall govern the contract executed between the successful Consultant and the City, as well as any interpretations or constructions thereof. Further, the place of performance and transaction of business shall be deemed to be in the City of Tuscaloosa, Alabama, and in the event of litigation, the exclusive venue and place of jurisdiction shall be in the Tuscaloosa County, Alabama.

c. Requests for Additional Information

The City reserves the right to request additional information from Respondents to clarify the submissions.

4.5 Public Records

Each Respondent is hereby informed that, upon submission of its proposal to the City in response to this RFP, the proposal becomes the property of the City.

Unless otherwise compelled by a court order, the City will not disclose any submissions while the City conducts its deliberative process in accordance with the procedures identified in this RFP. However, after the City either awards an agreement to a firm, or after the City rejects all submissions, the City shall consider each submission from Respondents subject to the public disclosure requirements of the Alabama Open Records Act (Ala. Code § 36-12-40) and Tuscaloosa City Code § 2-4, unless there is a legal exception to public disclosure.

If a Respondent believes that any portion of its proposal is subject to a legal exception to public disclosure, the Respondent shall: (1) clearly mark the relevant portions of its proposal "Confidential"; (2) upon request from the City, identify the legal basis for exception from disclosure under the Open

Records Act; and (3) defend, indemnify, and hold harmless the City regarding any claim by any third party for the public disclosure of the “Confidential” portion of the qualifications submittal.

PART 5 – SELECTION PROCEDURE

The City will use a Selection Committee of qualified City employees for the evaluation of submissions. This is a qualifications-based procurement for professional services, in which the qualifications of the responding firms will be reviewed and evaluated, and the most qualified firm will be selected, subject to negotiation of fair and reasonable compensation.

The Selection Committee will review the submissions submitted in response to this RFP, and rate the submissions based on the following grading system, which includes both numerical and pass/fail criteria:

Numerically-Scored Criteria	**Max. Points**
• SIEM Solution Requirements and Agreement Suitability	30
• Implementation Methodology	25
• Price	25
• References and professional expertise	20
Pass/Fail Criteria	
• Compliance with RFP Instructions	P/F
• Licensing and Professional Standing	P/F
• Conflicts of Interest	P/F

The Selection Committee will eliminate from consideration any firm submission which receives a "Fail" grade on any one or more of the pass/fail criteria for evaluation.

After review and evaluation of the submissions, the Selection Committee may select one or more Respondents for interviews. However, the Selection Committee is not required to conduct interviews. The Selection Committee may determine that interviews are not necessary for the selection process, and such decision is within the sole discretion of the Selection Committee.

When the Selection Committee concludes its work, it will make a recommendation to the City Council's Public Projects Committee, and request authority to begin negotiating an agreement, including final scope of work and fees for services, with the successful Respondent firm.

Upon approval by the City Council's Public Projects Committee, City staff will begin contract negotiations with the successful Respondent. If the negotiations are unsuccessful, of if an agreement cannot be reached within a reasonable time, as determined by the City, then City staff will terminate negotiations the firm, and will request authority from the Public Projects Committee to begin negotiations with another Respondent firm. Any compensation discussed with one Respondent will not be disclosed or discussed with any other Respondent.

Upon the conclusion of negotiations, the successful Respondent firm will enter into an agreement with the City. The agreement shall not be in force until it is approved by the Tuscaloosa City Council, and it is signed by the Mayor. The City cannot pay for any work or services performed prior to the approval of the agreement by the City Council, and the issuance of a notice to proceed by the City.

Please note, this RFP does not guarantee that the City will make any contract award. The City reserves the right to modify, amend, or withdraw this RFP, in whole or in part, at any time and for any reason, in its sole discretion. The City also reserves the right to reject all submissions, in its sole discretion.

END OF RFP