CITY OF URBANA

Request for Information: Network Detection & Response Solutions (2223-23)

City of Urbana
400 S Vine St
Urbana, IL 61801

Issue Date: January 23rd, 2023
Response Due: February 14th, 2023 - 5 PM CT

RFI Contents:

Project Overview

The City of Urbana wants to improve our network security and implement a logging solution – ***and we are looking to do <u>both</u> through this effort.***

Terminology Note:

For this RFI, we are adopting "**Network** Detection and Response (NDR)" as a solution acronym. By this, we mean software that is running within our network to consume information and act automatically on detected threats. We are emphasizing the "N" (Network) part of the solution, as the City already has an Endpoint tool. We expect that the NDR will run locally on-premise, but includes access to a SOC to escalate issues and to download new threat signatures.

Goals for the City of Urbana:

The City seeks several goals with this effort, which are listed here in order of importance:

1) An always-on NDR tool that neutralizes threats based on events that vary from "normal" activity.
2) A logging solution to provide a history of activity in case an event requires research.
3) Configurable rules to improve notification and logging rules.
4) Access to a SOC to assist with incident research & response.
5) Ongoing penetration testing and vulnerability scanning of unpatched software.

Project Budget:

The City has a budget of $55,000 in the current fiscal year (ending June 30, 2023) to pay for the implementation and first year's licensing cost.

City IT Background:

More information will be provided to responders who submit answers and are asked to participate in discussions. However, some key points to understand us:

- The City has a full-time IT staff of 4, and supports approximately 375 users on ~300 endpoints.
- The City manages two network domains – one for the City and one for the Park District. In the future, this could increase to support other organizations. Any NDR purchased is expected to function on all domains the City supports.
- The City runs our network domains with core functions **on-premise** (email, file storage, Active Directory) on our own servers. The City does not use Office 365 or run network components in the cloud - so there is no AWS or Azure presence.
- The City deploys Crowdstrike Falcon on all endpoints. Any NDR purchased is expected to integrate with Crowdstrike Falcon.

About this RFI Process:

The City is issuing a Request for Information (RFI), because we don't know what purchasing vehicles exist for each vendor, nor do we know enough information about what we want to write a detailed Request for Proposals (RFP).

City of Urbana procurement rules allow that the RFI could be the only step before the City buys through a Procurement Cooperative. Or the City may complete this RFI and use the information to issue an RFP. The next step will depend on the RFI responses received, the pricing, and the procurement methods available.

The process we envision will be the following:

1) The City is issuing this RFI. It will remain open for three weeks.
2) Vendors will submit answers to the RFI questions. One of the most important questions is whether the City can purchase your solution from a Procurement Cooperative - see question #29 in **Pricing**.
3) The City will review the responses and schedule discussions with some or all of the vendors.
   a. At the meetings, the City will ask questions about your responses.
   b. At these meetings, the City will also share detailed information about our network and endpoints that will be needed for pricing.
   c. Vendors invited to these discussions will be asked to complete the application for an Urbana EEO Certificate of Compliance. (More information may be found here: https://www.urbanaillinois.us/government/mayors-office/human-relations/public-vendorscontractors) *Approval by the Urbana Human Relations Commission (HRC) will be required before the City signs a contract.*
4) Based on the results of the meetings and the information provided, vendors will be asked to offer final pricing through available Procurement Cooperative contracts.
5) If the City finds a satisfactory solution, we will purchase from a Procurement Cooperative contract. Otherwise, we will use what we have learned from the RFI to conduct an RFP.

Submittal Instructions / Terms and Conditions

Due Date:	Response are due on Tuesday, February 14th, 2023 at 5:00 p.m. CT
Contact:	Questions and RFI Responses should be submitted via email to Sanford Hess at sfhess@urbanaillinois.us
Submission Requirements:	There is no required format, but responses should include: • **Response to Questions**: Answer all questions. See instructions at the beginning of the **Questions** section below. • **Draft Contract/ Service Agreement:** Responses should include your standard agreement with a full and valid complement of standard warranties, ready for City review. • **References:** Provide at least 2 references who are similar to the City (see **City IT Background** in the **Project Overview**) and, in the ideal situation, who are local governments. • **Completed Vendor Representations and Additional Duties Form (VRAD):** This City form is accessible here: https://www.urbanaillinois.us/Purchasing-Forms • **Completed Addenda Acknowledgement Form**: City policy requires that all vendors submit this form, even if there are no addenda. This City form is accessible here: https://www.urbanaillinois.us/Purchasing-Forms
Communication:	Once the RFI is issued, communication must be sent to the Contact. Responses to non-routine questions or answers that deserve to be communicated to all will be issued via an addendum to the RFI. (This is why respondents must register for the RFI, so that the City can send them notification of any addenda.) The City may require a clarification of a response once submitted either via telephone, electronic meeting, or in writing. The City reserves the right to impose deadlines on clarifications.
Response Validity:	All responses to this request shall be irrevocable for a period of 90 days after the submission due date and many not be withdrawn by the respondent during this period.

Assumption of Risks:	The City is not responsible for any pre-contract costs incurred by a vendor participating in this process. Responses to this request become property of the City. Proprietary and confidential material should clearly be marked as such; however, the City shall only be able to comply to the extent allowed by law. The City reserves the right to terminate the selection process at any time, to reject any proposals, and to award contract in the best interest of the City.
Evaluation Criteria	The City will evaluate responses on the totality of factors: solution approach, implementation strategy, references, pricing, and the availability of Procurement Cooperatives for the purchase. Brevity and clarity in your responses is appreciated. The City reserves the right to waive technicalities or to accept or reject any responses based upon the City's determination of its best interest.

Questions – To Be Answered In Your Submission

Please provide information that addresses the following 30 items. If you are providing standard text through a separate document (e.g. an existing White Paper as an answer) *then your RFI response should cross-reference that document by page*. So an acceptable answer to a single question would be: "See our White Paper on XXXX, pages 12 – 14."

Core Functionality

1) Provide a brief overview of your NDR functionality. If modules can be purchased separately, describe each module.
2) What supporting technology does your solution require? List all hardware, software, networking, middleware, and database requirements. Include any associated costs as a separate line item in your pricing, including any necessary hardware and software to support them. (See question #28 in **Pricing**, below.)
3) Describe the capabilities for City IT staff to view dashboards, logs, and incidents – and to create, update, and close tickets related to the incidents.
4) Describe smartphone applications for IT staff to be notified of and manage incidents outside of office hours.
5) What experience and tools do you have to address Governance, Risk, and Compliance (GRC) for local government?
6) What differentiates your offering from your competitors?

SOC Escalation for an Incident

7) What options do you provide for a Security Operations Center (SOC) that will support us during an incident? If you charge retainers or extra fees for incident response capability, please elaborate on what you offer and how you charge for these services.
8) Is your SOC staffed 24/365?
9) What is your customer notification and escalation process?
10) Does your service provide full response reports on investigations? (If so, **please provide a sample report** with the appropriate information redacted.)
11) What does your Service Level Agreement specify for Mean Time to Detect, Mean Time to Remediate, and Mean Time to Respond? What is your Retention Rate for your clients? (Retention Rate = ratio who renew past the first term of the contract.)

Logging

12) Indicate the data sources supported for log collection, reporting, and retention. Describe the collection methods.

13) Is there a maximum duration for log retention?

14) Describe features for extracting log information for the forensic analysis of an incident and sharing it with other groups who are not on our network.

Solution Implementation

15) Describe your implementation and tuning process for a new customer.

16) What will the install process be for our on-premise network? (How many machines does your NDR need to be installed on? What other connectors or components must be installed on endpoints and other machines? Can your solution run in a virtualized Hyper-V environment?)

17) Describe your offerings for a proof of concept and/or "watch mode" installation – and if that implementation can be switched on for production use or if it must be re-installed.

18) What consulting support hours are included in your standard NDR contracts? (If this is an extra cost, please explain what is available and the pricing.)

19) What training hours or classes are included in your standard contracts? (If this is an extra cost, please explain what is available and the pricing.)

Ongoing improvement:

20) What are your capabilities to push updated threat intelligence to our installation, based on your corporate sources?

21) How does your solution improve NDR capabilities over time by monitoring our own network activity?

22) Describe offerings around penetration testing & threat hunting. (E.g. how frequently is threat hunting performed, and is it performed by scanning software releases or some other means?)

Security

23) What type of access will you need to our network, initially and on an ongoing basis? What access to our data will exist to users at your SOC?

24) How will we <u>securely</u> send our information to, and receive information from, the SOC?

25) What are all of the locations our data will reside? (On-premise, at your SOC, in your SOC's backups, and… other locations?)

26) How long will your company store data collected/created for or by us after contract termination?

27) If we terminate the contract, describe what data would be available for us to download and deploy to a replacement NDR.

Pricing

28) Provide detailed cost breakdowns of your proposal including licenses, startup/implementation, maintenance, SOC support, incident retainers, data egress, and other fees or required payments associated to your solution. If modules can be implemented separately, price each and identify which are required and which are optional. If third party software, hardware, or subscription services are required, include these with their costs.

29) What Procurement Cooperatives are available for this purchase?

a. State of Illinois contracts that are marked as a "Statewide Master Contract."
b. Sourcewell (including through a reseller)
c. TIPS-USA (including through a reseller)
d. Omnia (including through a reseller)
e. HGACBuy (including through a reseller)

30) Tell us about additional discount rates available for longer duration contracts.