



ST. LOUIS' ORIGINAL SEARCH ENGINE®

TO: All Proposers  
 FROM: Rita Kirkland  
 DATE: August 17, 2022  
 SUBJECT: Proposal Addendum No. 1  
 BID#: 22-990900  
 DATE ISSUED: August 17, 2022  
 THE PROJECT: MDR – Managed Detection and Response Solutions

---

1415 Olive Street  
 St. Louis, MO 63103  
 314.241.2288  
 slpl.org

**INTENT**

This addendum is issued to provide a modification/addition to proposal plans and/or specifications.

**MODIFICATION / ADDITIONS**

1. Additional information provided for lines 4 & 5 on Exhibit Q.

See attachment Exhibit - Q

2. (Exhibit Q – Questions 4) Does the service provider require installing of any additional agents for detections?

Yes, we would like to include the Cisco Firewall as a source.

3. (Exhibit Q – Questions 5) If the service provider can provide this service/solution, do they monitor events, and/or alerts in their solution?

See attachment Exhibit - Q

I have read and understand the preceding addendum and said changes are reflected in my proposal. The vendor signed addendum should be included with your response packet.

**Mission Statement**

The St. Louis Public Library will provide learning resources and information services that support and improve individual, family, and community life.

\_\_\_\_\_  
COMPANY:

\_\_\_\_\_  
VENDOR'S SIGNATURE

\_\_\_\_\_  
TITLE

\_\_\_\_\_  
(Date)

Exhibit - Q

| 1 Area                  | Need   |
|-------------------------|--|
| 2 General               | Does the service provider provide 24x7x365 SOC as a Service?   |
| 3 General               | Does the service provider provide us the access to a SOAR (Security Orchestration and Automated Response) platform?  |
| 4 General               | Does the service provider require installing of any additional agents for detections?  |
| 5 General               | Is it possible to customize the service offering to a tailored solution for each customer?   |
| 6 Detection             | Does the service provider leverage the Mitre ATT&CK framework for threat detections?   |
| 7 Detection             | Does the service provider provide full visibility on what detection contents deployed for my environment?  |
| 8 Detection             | Does the service provider has the ability to transform the data to fit the format that another system requires?  |
| 9 Detection             | Does the service provider has the ability to learn from decisions (ML/AI) that analysts have made in the past and use those to help analysts make those decisions better and faster? |
| 10 Detection            | Does the service provider has the ability to detect whether a behavior is normal or not, and use that in the triage process?   |
| 11 Response             | Does the service provider provides a case management portal so we can see all the Inprogress as well as escalated cases?   |
| 12 Response             | Does the service provider provides us access to ALL the systems that their SOC analysts use for the MDR service?   |
| 13 Response             | Does the service provider provides the the ability to enrich cases with additional data or take actions in an automated way?   |
| 14 Response             | Does the service offering include an automated response ability?   |
| 15 Response             | Does the service provider have the ability to find and link similar cases automatically?   |
| 16 Response             | Does the service provider have the ability to connect with our existing case management system, if we want to stick with that?   |
| 17 Integrations         | Does the service provider have the ability to integrate all the tools in my security stack - whether it is to fetch data or to take actions?   |
| 18 Playbook Automation  | Does the service provider include security orchestration, automation, and response (SOAR) functionality?   |
| 19 Playbook Automation  | Does the service provider's SOAR provide us the ability to build a playbook using an easy to use visual editor?  |
| 20 Playbook Automation  | Does the service provider provide us the ability to simply describe the playbook and get it automated in a timely fashion via service?   |
| 21 Playbook Automation  | Does the service provider's automation platform has the ability to automate a playbook without having to write any code?   |
| 22 Reporting/Dashboards | Does the service provider provide an MDR value dashboard that shows us how many alerts/cases handled by the MDR service?   |
| 23 Reporting/Dashboards | Does the service provider have the ability to create custom dashboard with KPI of our interest?  |
| 24 Reporting/Dashboards | Does the service provider have the ability to provide reports via email? eq: pdf   |
| 25 Reporting/Dashboards | Does the service provider's platform have the ability to visualize the data in multitude of ways - a table, a score, a pie chart, line chart or a bar chart?                         |
| 26 Reporting/Dashboards | Does the service provider have the ability to extract insights from data using powerful analytics and display that on a dashboard?   |