TOOELE
COUNTY

REQUEST FOR QUALIFICATIONS

PROJECT:

MANAGED DETECTION AND RESPONSE, SECURITY OPERATIONS

PREPARED FOR:

TOOELE COUNTY
ADMINISTRATION BUILDING

47 SOUTH MAIN
TOOELE, UTAH 84074

OCTOBER 2021

INTRODUCTION:

Tooele County ("County") is requesting qualifications from parties interested in providing the following cyber security's over a three (3) year, contracted service: Security Operations Center, Managed Detection and Response, and Incident Reporting. Upon completion of this Request for Qualifications (RFQ), qualified proposers will be given detailed descriptions of the services desired, and an opportunity to submit a bid in response to an offered Request for Proposal (RFP).

Each party responding to this RFQ is responsible to obtain all information, addenda, updates, etc., to meet the submittal dates and requirements.

MINIMUM QUALIFICATIONS:

Interested parties must submit a completed copy of the Service Questionnaire (Attachment A) by November 2, 2021 at 5:00 p.m. to be considered.

Vendors will be vetted solely on the responses provided in the Service Questionnaire.

Pricing options should not be provided at this time.

TIMELINE

Event / Action	**Date**
Advertise RFQ	October 18, 2021
RFQ Question Deadline	October 26, 2021 @ 5:00 p.m.
RFQ Submission Deadline	November 2, 2021 @ 5:00 p.m.
Private RFP Release	November 8, 2021
RFP Question Deadline	November 17, 2021 @ 5:00 p.m.
RFP Submission Deadline	November 18, 2021 @ 5:00 p.m.

QUALIFICATION SUBMISSION CONTENTS:

A. Cover Letter (1 page maximum)

The cover letter shall describe the vendor’s business entity (corporation, LLC, partnership, sole proprietorship, etc.), include a statement of the vendor’s general background, include a discussion of the vendor’s interest in the project, and acknowledge receipt of any addendums.

B. Service Questionnaire (Attachment A)

A fully completed copy of the Service Questionnaire will be required in order to provide the County with enough information to appropriately vet each vendor. Partially completed Questionnaires will not be considered.

C. Signature

The questionnaire shall be signed by a representative authorized to bind the team and shall expressly state the interest in being considered for an opportunity to bid. By signing the cover letter and submitting response to this RFQ, the vendor covenants that they are fully qualified to provide the required services, and that the submitted information is true and accurate and may be relied upon in evaluating their qualifications.

QUALIFICATION SUBMISSION:

Two (2), sealed, copies of the qualifications must be received by the due date for submittal: 5:00 p.m on Tuesday, November 2, 2021.

Questions must be submitted via email to Denise Lawrence at denise.lawrence@tooeleco.org no later than October 26, 2021 at 5:00 pm.

Completed submittals must be addressed and sent to:

Tooele County Administration Building
c/o Denise Lawrence
47 South Main Street
Tooele, UT 84074

Qualifications shall be submitted in a sealed envelope. The outside lower right-hand corner of the envelope shall be marked:

Sealed Proposal of (Firm Name)
Phase 1 – RFQ: Managed Detection and Response, Security Operations
Tooele County Administration Building

Submissions, modifications or corrections received after the closing time on November 2, 2021 will be considered late and will not be opened.

If only one submission is received, County will resolicit submissions for the purpose of obtaining additional submissions.

Tooele County shall not be obligated to respond to any qualification submitted, nor shall it be legally bound in any manner whatsoever by the receipt of a qualifications or future proposals.

Tooele County reserves the right to extend or cancel all scheduled qualification and proposal due dates. Notice of such extensions or cancellations shall be sent via addendum to this RFP.

QUALIFICATION REJECTION:

Tooele County reserves the right to reject all vendors deemed unqualified, unsatisfactory, or inappropriate, to waive defects or informalities, and to offer a contact with any firm in response to this RFQ. This RFQ does not constitute any form of offer to contract. Tooele County will not pay any costs incurred by the proposer in preparing or submitting the qualifications.

QUALIFICATION AWARD:

Vendors that pass though the County screen process and are deemed qualified and capable of providing the services desired, will receive a posting to a private RFP posting on November 8, 2021. There, further details regarding the scope of work will be provided.

Attachment A

Service Questionnaire

Category	MDR RFP Question	Response
Company Overview	How long as your company been in business?	
	How long have you offered MDR services to your clients?	
	Is MDR your primary business offering?	
	Approximately how many clients do you have fully implemented in your MDR offering?	
	Are you willing to demonstrate your services in a proof-of-concept implementation?	
	What is your client retention rate?	
	What is your NPS score?	
	Please provide at least two references we can contact, preferably from clients with similar size and scope of operations.	
	Please describe what you feel differentiates your offering from your competitors.	
Compliance	Please provide your latest SOC2 report.	
	Do you have experience with acting as a processor for GDPR controllers?	
	Do you use sub-processors to support your environment?	
	If yes, how do you ensure the sub-processors operate securely and effectively?	
	Indicate whether you've ever had a security or data breach.	
	If yes, has it happened in the preceding 36 months?	
	If yes, please describe and indicate what was learned from this incident?	
Architecture, Implementation, and Tuning	Describe your implementation and tuning process for a new customer.	
	Describe the overall level of effort and engagement of our internal team to assist in the POC and implementation of your MDR Services.	
	Describe the implementation process of your Company's MDR proposal including a description of any resources (along with their qualifications), methods, and tools to achieve on-going success.	
	What points of technical integration do you expect we will need to perform?	
	What is your typical time frame to implement your solution for a client with similar needs as us?	
	Describe your implementation methodology.	
	Does your solution require a SIEM solution be in place?	
	If yes, list SIEMs you integrate with and what SIEM you provide in-house.	
	Does your solution require an appliance to collect or forward log data to the SIEM?	
	Are there any third-party licensed products that we will need to purchase?	
	Please provide a list of necessary products and the associated costs?	
	What type of access will you need to our network?	
	Does this access need to be persistent (i.e., always-on)?	
	Are clients homed out of a specific monitoring center or is activity shared across your centers?	
	How do you address failover?	
	Define your SLA's associated with an outage and recovery?	
	Do you threat hunt 24x7x365?	
	Does your solution include 24x7x365 support for critical and high incidents/issues?	
	During off hours is it an on call staffing or are there live analysts in SOC 24/7?	
	Are there times you do not provide monitoring services?	
	Please specify the number and locations of the Data Centers you maintain?	
	How many analysts and engineers do you have on staff?	
	Are analysts and engineers allocated evenly over shifts?	
	Will you provide dedicated engineer or service delivery manager to Tooele County?	
	Do you require your staff to have industry recognized security certifications?	
	What security certifications are held by your staff?	
	How do you keep your staff current with technology?	
	Do you allocate time for your staff to attend training and/or obtain additional certifications?	
	What's your average response time?	
	What's your average time to resolution?	
	Can we call into the SOC?	
	Will we speak to an automated phone tree or scheduler?	

	Do you perform background checks on your employees with access to client information?	
	In addition, do you conduct education verification check against your employees?	
	Will anyone have access to client information or perform investigations outside of a secure environment (i.e., Home office, etc)	
Threat Intelligence	Does your SOC proposal include any threat intelligence or threat feeds?	
	If so, what is the distribution process and frequency? What distribution channels are available, and are they external or internal?	
	Do you have a dedicated internal Threat Intelligence team?	
	Do you apply threat intelligence to client security alerts as part of your process for vetting or determining if an alert should be escalated to security event status and action taken?	
	Does your threat intelligence feed account for client criticality to properly inform clients based on their threat surface?	
	Is security event data shared across your customer base?	
	How is this handled to ensure confidentiality?	
	Do you categorize threat intelligence by industry or sector?	
	Do you recommend/require your customers to subscribe to threat feeds?	
	How do you curate threat intelligence feeds for each client?	
MDR Approach	Do you offer different service level options for security monitoring/alerting?	
	If yes, what service level option are you quoting for Tooele County?	
	Does your service include a process for adding new rules/event correlations?	
	If yes, please explain your approach for communicating and gaining approval for these recommendations.	
	How often are signatures and threat intel updated?	
	Please describe the system maintenance process and schedule?	
	Describe the communication plan for system downtime notification.	
	Can you update your technologies during production hours, without a shutdown window?	
	How do you monitor client endpoints (e.g., agent)?	
	How do you monitor client networks (e.g., netflow)?	
	What (if any) access to Firewalls are necessary to adequately monitor?	
	Describe the Firewall access that is needed for monitoring?	
	What firewalls do you integrate with?	
	How do you classify/prioritize security events?	
	What is your process for detecting and responding to a threat?	
	How are events sorted between positive and false positive?	
	What service level agreements or service level objectives do your SOCs offer?	
	What is the turn-around time from detection, notify, respond on average?	
	Do you provide to your clients Security Education, Training, and Awareness to improve their security posture?	
	If yes, what are the ways you provide this to your clients?	
	How do you improve monitoring capabilities over time based on event history?	
	Please describe your approach and investment to AI and ML in assisting your threat hunting?	
	Do you require persistent access to client infrastructure and how is this access maintained?	
MDR Threat Hunting	Does your proposal include hunting for threats (including zero-day threats) within Tooele County's environment?	
	How do you perform this hunting?	
	How often do you perform hunting?	
	Is there any special software we need to deploy to support this hunting?	
	What part do humans play in the threat hunting lifecycle?	
	Incident Analysis and Response	
	Do you perform real-time inspection of every packet utilizing full packet capture?	
	If you do full packet capture please explain how long you do it for, when it starts, and how long you retain it for?	
	Does your solution detect unknown threats and attacks leveraging patterns and behavioral analytics?	
	Does your solution detect based on signatures and IOC's?	
	Do you do full forensic analysis to confirm threats and eliminate false positives?	

	Are you able to do near real-time communication disruption and isolation of threats on client’s behalf?	
	If so, are these placed autonomously or by human decision? If both please specify when and how the decision is derived.	
	Please describe the level of support provided until the incident is remediated and threat-actor is eliminated.	
	Do you charge retainers or extra fees on top of your base costs for this incident response capability?	
	If so, please elaborate on what this entails and how you charge for these services	
	What would constitute a variable bill?	
	At what point do you engage Tooele County to assist in mitigation?	
	What does your normal escalation and notification process look like?	
	Does your service provide full response reports on investigations?	
Metrics, Reporting and Dashboards	Do you provide operational reports to your customers?	
	What is the frequency for customer reporting?	
	Can you provide sample reports?	
	What is your preferred method for delivery of customer reports?	
	Are real time data and operational reports exportable?	
	If yes, what formats are supported (e.g., PDF, CSV)?	
	Does your solution allow reports to be scheduled and automatically distributed?	
Data Management	Where does client data reside (e.g., Public Cloud, vendor hosted data center, etc.)?	
	Data retention: How long will your company store data collected/created for or by Tooele County?	
	Data destruction: What is the process for purging or destroying historical data after use?	
	In the event we need comprehensive forensic data for an investigation, can you provide it and what can you provide?	
Client Satisfaction	How do you track your customer satisfaction?	
	Do you have SLA’s or SLO’s?	
	If so, please provide the matrix.	
	Do you conduct executive briefings?	
	If so, how often?	
	Do you ever participate in meetings with clients, regulators and due diligence questionnaires?	
	If so, please provide examples and outcomes	
Security - General	How does your solution authenticate users upon sign in?	
	How does your solution restrict access to sensitive client information?	
	Does your solution maintain a full audit trail for all changes to client data or access policy, including: • Account who made the change • Date/time of the change • Original value and the modified value • IP address of where the change was initiated	
	What level of logging is provided by the SOC? Does it contain all authentication events, administrative user activity, approval events, and modify/update/delete activity?	
	How long are logs retained for?	
	Can logs be exported by the client?	
	Does your solution require strong passwords, including the use of specific number of special characters, digits, mixed case letters, and minimum password lengths? (*please provide password policy specifics*)	
	Can the password policy be modified per client? For example, changing the maximum logon attempts or password reuse thresholds.	
Security - Access and Authentication	Can the product handle federated/SSO authentication from the client's Identity Provider (IdP)?	
	What methods (e.g., SCIM) does the product support for identity provisioning and deprovisioning?	
	If authentication cannot be federated/SSO, how does the application authenticate users? Can multi-factor be implemented? How are new users setup?	
	Do you require MFA for both client and internal account access?	

Authentication	Is access segregated into roles that allow for differentiation between users with different job functions? How does this work?	
	Does your solution allow for a role that is limited to case administration?	
	Does your solution allow for roles that limit access to individual clients?	
	Are all authentication events, both successful and failed, logged in the system, with alerts triggered when thresholds are exceeded?	
	Does the product come with any default administrative accounts?	
Security - Network & Vulnerability Mgt	Will the client data be stored and/or processed in a separate/dedicated tenant isolated from other customers?	
	If yes, how is client data be segregated from other clients?	
	Does the SOC utilize an IDS/IPS solution?	
	Does the MDR solution have DDoS protection?	
	Is the MDR solution penetration tested at least annually?	
	If yes, please provide the results of the last test?	
	How often is your environment scanned with a vulnerability scanning tool?	
	If yes, can you provide the results the last scan?	
	Is all traffic to/from the SOC encrypted in transit?	
Security - Backup and Disaster Recovery	How often do backups occur for our data?	
	How long are backups retained?	
	Are backups sent offsite from the production datacenter, or production 'Account' if the application is hosted in the Cloud?	
	Are backups transmitted offsite encrypted? What level of encryption is used?	
	Are backups and their copies stored at rest encrypted? What level of encryption is used?	
	Is the disaster recovery plan documented and do we have the ability to test the plan at least annually?	