|  |  |
| --- | --- |
| July 14, 2017 | Client Logo/Client Name |
| Request for xyz | |
| RFI Name/ Title | |

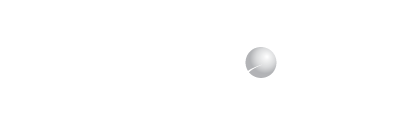


Table of Contents

[Table of Contents 2](#_Toc399751251)

[2 Introduction and Overview 3](#_Toc399751252)

[3 Company XYZ’s Current Business Environment 7](#_Toc399751253)

[4 Company XYZ’s Current Technical Environment 8](#_Toc399751254)

[5 Response Format 9](#_Toc399751255)

[6 Vendor Profile 10](#_Toc399751256)

[7 Business Attributes 11](#_Toc399751257)

[8 Service Attributes 14](#_Toc399751258)

[9 Value Attributes 21](#_Toc399751259)

[10 Pricing 22](#_Toc399751260)

2 Introduction and Overview

2.1 General

COMPANY XYZ issues this Request for Proposal (RFP) for a Managed Security Services Provider to deliver services consisting of but not limited to:

* Xxx
* Xxx
* Xxx
* xxx

All of the above will hereafter collectively be referred to as the “Solution.” “Proposal” shall mean the Vendor's bid to provide the services in response to this RFP. “Vendor” shall mean a recipient of this RFP who submits a proposal to COMPANY XYZ, and includes any subcontractors to be used by the Vendor to provide the solution. “Agreement” shall mean the agreement that COMPANY XYZ executes with the awarded Vendor for the services hereunder.

COMPANY XYZ issues this request for a Managed Security Services Provider with the intent of having a third party monitor the COMPANY XYZ network for attempted breaches or potential threats.

The approach to the response to this RFP Solution must be agreed to and approved by the parties prior to the start of the engagement.

2.2 Confidentiality of Company XYZ Information

This RFP, and all information provided to the Vendor in connection herewith, is COMPANY XYZ’s confidential and proprietary information (the “Information”). The Vendor may not disclose this RFP, or any Information that COMPANY XYZ may provide the Vendor to assist the Vendor in developing a Proposal, to any other person or entity without the prior written approval of COMPANY XYZ. The submitted Proposal, and all information provided by the Vendor in connection hereunder, is Vendor’s confidential and proprietary information (the “Information”). COMPANY XYZ may not disclose the Proposal, or any other Information that Vendor may provide to COMPANY XYZ regarding the Proposal, to any other person or entity without the prior written approval of Vendor. The parties may use the Information provided to it solely for the purpose of responding to and evaluating the response to this RFP. Neither party may disclose to any third party or person that it has received this RFP, the substance of this RFP, the response to the RFP or any COMPANY XYZ decision with respect to the Vendor's Proposal. Upon request, the parties shall return any Information provided by a party, and any copies thereof to such requesting party.

2.3 News Releases

Vendors who are submitting a Proposal are not at liberty to discuss this RFP outside the COMPANY XYZ community. Neither party shall release the details of this RFP or subsequent contract without written permission from COMPANY XYZ.

2.4 No Contractual Relationship

Nothing contained in this RFP creates, nor shall be construed to create, any contractual relationship between COMPANY XYZ and any Vendor. COMPANY XYZ makes no commitment in or by virtue of this RFP to purchase any services from any Vendor, nor does receipt of any Vendor's Proposal place COMPANY XYZ under obligation to award the Agreement to that or any other Vendor. Such commitments may be made only in and through a written Agreement signed by both parties.

2.5 Primary Contract Relationship

COMPANY XYZ will contract with the Vendor of the winning Proposal and Vendor will be known as the primary contractor. In the event of a subcontracting relationship, which has been approved by COMPANY XYZ and is being used by the primary contractor, the primary contractor assumes all responsibility for delivery, installation, maintenance, and support services that are supplied by the subcontractor.

2.6 Proposal Costs

Expenses incurred in preparing and presenting a Proposal is the sole responsibility of the Vendor and may not be charged to COMPANY XYZ in any way.

2.7 Evaluation of Proposals

The evaluation of all Proposals will be based on a single submission by each individual Vendor. This submission may include multiple alternative approaches for consideration by COMPANY XYZ provided that they meet the requirements of this RFP. No revisions or amendments to the proposal will be accepted after submission unless approved by COMPANY XYZ.

Once COMPANY XYZ has evaluated the submitted proposals, the finalists will be contacted and requested to do an onsite presentation of their solution at COMPANY XYZ headquarters in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

COMPANY XYZ will use some or all of the following criteria to evaluate Proposals (the order does not represent priority):

* The Vendor's ability to provide reliable services
* The Vendor’s ability and willingness to aid in configuring the Solution to meet COMPANY XYZ’s needs
* The services features and ability to support business and technical requirements
* The ability to integrate third-party software products and or services
* The level of complexity of the Solution
* The overall quality and presentation of the Proposal
* The price of the Solution
* The overall business case impact
* Any third-party evaluations of the vendor’s services
* Industry standing and expertise

2.8 Basis for Award of Agreement

COMPANY XYZ reserves the right in its sole discretion and for any reason whatsoever, to accept, reject or terminate consideration at any time of any or all Proposals. COMPANY XYZ specifically reserves the right to contract with a Vendor that does not offer the services at the lowest price or with one or more companies that did not submit a Proposal and to modify the terms of the projected transaction or the specifications of the services at any time prior to execution of the Agreement.

2.9 Amendments to RFP

COMPANY XYZ reserves the right to amend, modify, or withdraw this RFP at any time. If the RFP is amended or modified, it will be in writing from COMPANY XYZ. Vendors are required to acknowledge all amendments in writing.

2.10 RFP Schedule

The schedule for this RFP is as follows:

|  |  |
| --- | --- |
| **RFP Issued:** | XXX, 201\_ |
| **Vendor’s intention to respond by:** | XXX, 201\_ |
| **Last date to submit questions:** | XXX, 201\_ |
| **Answers provided by:** | XXX, 201\_ |
| **Proposal submission:** | XXX, 201\_ |
| **Target date for COMPANY XYZ decision:** | XXX, 201\_ |
| **Solution implementation:** | XXX, 201\_ |

2.11 Vendor Questions

Vendors should submit all questions about this RFP **in writing** by the date specified above to:

**Primary Contact:**

XXX

**Backup Contact:**

XXX

**or**

XXX

It is COMPANY XYZ’s intent to provide responses to questions to all Vendors where appropriate.

2.12 Acknowledgment of RFP Receipt

Within \_\_\_\_\_\_\_\_ business days of the receipt of this RFP Vendors must provide written or electronic acknowledgment of the receipt of this RFP and intention to respond. This communication should be addressed to the attention of the Primary Contact at the address noted above.

2.13 Election Not to Submit Proposal

In the event the Vendor elects not to proceed with submission of a Proposal to COMPANY XYZ, a letter denoting such intention should be sent to the Primary Contact at the above address. COMPANY XYZ would like to request that the Vendor provide rationale for the decision not to respond.

2.14 Proposal Submission

One (1) electronic copy of the Proposal must be delivered no later than 5 p.m., to the Primary Contact listed at the above address on the “Proposal Submission:” date in the RFP schedule above.

Proposals should be in Microsoft Word (compatible with Word 6.0 or higher) or PDF. The Vendor’s name should appear on the bottom of every page other than the cover page. Each page, other than the cover page, shall be numbered.

COMPANY XYZ reserves the right to reject Proposals received after the due date. Each Proposal shall constitute an offer, which remains valid for a minimum period of 90 days after the proposal submission date.

2.15 Form of Service Agreement

Vendor should submit a copy of their standard agreement form. When COMPANY XYZ completes its analysis and selects a Vendor, COMPANY XYZ will provide an agreement for execution by the successful Vendor. The Vendor must state its fee structure based on the contents of the RFP.

3 Company XYZ’s Current Business Environment

3.1 Company XYZ Overview

COMPANY XYZ delivers safe, reliable and affordable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. The purpose of this RFP is to help us identify technical solutions available to meet our business needs for protecting proprietary data and systems from unauthorized access. Subsequently, we are soliciting input from a select group of vendors to present their design for a comprehensive solution to ensure the confidentiality, integrity and availability of COMPANY XYZ data.

This document includes a profile of the current environment, from a business perspective as well as a technical point of view and includes detailed information. High-level business requirements have been defined, indicating the immediate focus for this initiative as well as the long-term strategy.

3.2 Business Requirements

As part of COMPANY XYZ security best practices, it has been deemed vital for COMPANY XYZ to implement, maintain and monitor appropriate security measures. This is to provide protection for our Internet-facing applications and client services, as well as preventing any internal damage to our network from the outside. This should encompass a 24x7 service that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the COMPANY XYZ security infrastructure and critical devices as well as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Additionally, COMPANY XYZ and/or Vendor must be able to declare an incident and the Vendor must provide incident response support to enable COMPANY XYZ to be able to conduct its business. These services will enhance our security posture and reduce our risk of a security breach.

4 Company XYZ’s Current Technical Environment

The following information is provided to give Vendor information concerning COMPANY XYZ’s technical environment, for the purposes of submitting a Proposal for the services requested:

xxxx

5 Response Format

COMPANY XYZ requires Vendor to organize its Proposal in the following order:

* **Executive Summary:** Provide an overview of the solution, including differentiators and value provided by the Solution. Vendors should limit the Executive Summary to a maximum of two pages.
* **Responses to Questions:** Provide concise responses to the Questions listed in the following sections, presented in the exact order as arranged in this document. Vendor must follow numbering sequence, use the same section titles and answer all questions in order for Vendor Proposal to be considered.
* **Pricing:** Provide detailed pricing for the proposed solution.
* **Supplemental Information:** Any information that Vendor deems relevant to the proposed solution can be included as an Appendix. Please note: Do not include information unless it directly relates to the solution proposed in Vendor Proposal.

Vendor Proposals must adhere to the above-stated format in order to be considered.

6 Vendor Profile

6.1 Primary Business Purpose

Please provide a brief statement of your organization’s primary business purpose.

6.2 Corporate History

Please provide a brief history of your company.

6.3 Management Team Bios

Please provide brief biographies of your management team.

6.4 Services Offered

Describe the services offered by your organization, including any optional services that might be of interest to COMPANY XYZ.

7 Business Attributes

Business attributes are one element of COMPANY XYZ’s requirements. They comprise characteristics, policies, processes and procedures that need to be described in a qualified RFP response and include:

* Financial Viability
* Managed Service Viability
* Security Vision and Investment
* Security Practices

7.1 Financial Viability

7.1.1 Provide information about your company’s financial stability. If your company is public, include an annual report and supporting financial statements. If your company is private, include supporting documentation to demonstrate a stable, profitable, sustainable business model.

7.1.2 Provide detail on any venture funding you have received, including the sources of the venture funding.

7.2 Managed Service Viability

7.2.1 What is your company’s core business strategy? What are your primary lines of business in terms of revenue? Where do security services fit into your business strategy?

7.2.2 Provide details that describe how your MSS business or business unit is profitable. If not profitable, please provide your expectations for reaching profitability.

7.2.3 Provide the annual revenue your company derives from the following services: Security Monitoring, SIEM, Log Management and Vulnerability Scanning (do not include any revenues from product bundling or resale).

7.2.4 Of the revenues provided above, what percentage does it comprise of your total corporate revenues?

7.2.5 Describe how any of the top research firms (i.e., Gartner, Forrester) have ranked your company in the MSSP market.

7.2.6 Describe any awards your company has won for MSS.

7.2.7 Provide the number of Managed Security Services clients at the end of last year, current, and projected at the end of this year. Only include clients for Device Management, Security Monitoring, SIEM, Log Management and Vulnerability Scanning services.

7.2.8 Provide details on how long you have offered each of your Managed Security Services.

7.2.9 Describe your most recent fiscal year’s Managed Security Services growth rate over the prior fiscal year.

7.3 Security Vision and Investment

7.3.1 Describe your company's vision and direction for developing new technologies in support of your Managed Security Services.

7.3.2 Describe, in detail, your company's investment approach to technology research and development as it relates to solving security challenges and improving client ROI.

7.3.3 Provide details on your level of investment in research and development.

7.4 Security Practices

7.4.1 Provide detail on your internal security policy and procedures, documenting any industry standards that you have adopted or follow.

7.4.2 Have you had an independent review of your MSSP infrastructure and service (SSAE 16 review)? Please provide detail on this review, including who executed it, when it was executed, scope of review, type of testing, frequency of testing and summary results. If possible, please provide the report.

7.4.3 If you haven't performed an independent review, are you planning to have a review performed in the future or are you in the process of having the review executed? If so, please provide detail on this review including who will be executing it, when it will be executed, scope of review, type of testing, and frequency of testing.

7.4.4 Do you perform internal reviews over your MSSP infrastructure and service? If so, please provide detail on this review including who executed it, when it was executed, scope of review, type of testing, frequency of testing and summary results.

7.4.5 If you haven't performed an independent review or the results cannot be distributed, would you grant us the right (or a third party on our behalf) to audit your operations and determine the appropriateness of implemented safeguards?

7.4.6 Describe your business continuity/disaster recovery policy.

7.5 MSS Infrastructure

7.5.1 Do you maintain full, dedicated Security Operation Centers (SOCs) to support your MSS?

7.5.2 Describe your SOCs, including details on the following points:

* Do you own and manage your SOCs?
* Where are your primary SOCs located?
* Where are your secondary SOCs located?
* Are all of your SOCs operational 24x7x365?
* Describe the level of SOC redundancy.

7.5.3 Describe how you limit service interruption if a SOC goes offline.

7.5.4 Describe security safeguards around the SOCs.

7.5.5 Describe the staffing for each of your SOCs.

7.5.6 Do you permit an onsite SOC visit? If so, what is the process for planning the visit?

7.5.7 What percentage of your staff is directly involved with delivering MSS and managing MSS client accounts? Describe your company’s annual staff retention rate for positions used to support the COMPANY XYZ account. Identify the number of employees versus contractors.

7.5.8 Describe your company’s staffing approach. What are your classifications for support (Example: Level 1, Level 2, etc.) Clearly define each level of support and the functions performed. (Example: Level 1 support monitors events, incident escalation, documentation, etc.)

7.5.9 What qualifications and certifications are required for each classification listed above? What types of career paths are available for employees (in the above classifications) within your company?

7.5.10 Describe your approach to background checks or screening you perform on employees, contractors, consultants and vendors associated with any aspect of your MSS offering.

8 Service Attributes

8.1 Threat Intelligence

8.1.1 Do you have a dedicated research team focused on threats and vulnerabilities?

8.1.2 What information sources do they source for intelligence?

8.1.3 How is intelligence analyzed and validated?

8.1.4 How is intelligence used in the management and monitoring of client devices?

8.1.5 What visibility do clients have into this intelligence?

8.1.6 What is the level of integration between the research team and SOC operations?

8.1.7 What services does your research team support? Is supporting research their only role?

8.1.8 How is this team modeled? What is their mission?

8.1.9 What access do MSS clients have to this team?

8.1.10 Provide examples of how threat research has been used to proactively protect clients.

8.1.11 Provide samples of research briefs or write-ups from research staff.

8.2 Vulnerability Scanning

8.2.1 Describe your vulnerability scanning architecture.

8.2.2 Where do you source your vulnerability checks?

8.2.3 What is the process to escalate and/or prioritize identified vulnerabilities?

8.2.4 Do you support web application scanning? Can you test for database vulnerabilities?

8.2.5 How are vulnerabilities confirmed? What is the process for reporting false positives?

8.2.6 Is vulnerability data used in the monitoring process? In what ways?

8.2.7 How are vulnerability scanning reports delivered?

8.2.8 How are scans scheduled?

8.2.9 Can you support internal and external scanning? What infrastructure does this involve?

8.2.10 Do you offer PCI ASV scanning to support quarterly compliance validation?

8.3 Endpoint Protection

8.3.1 Describe your managed service for endpoint security.

8.3.2 Does your solution require agents installed on every endpoint? If so, what are the bandwidth implications?

8.3.3 Is your endpoint managed service “always-on,” or does it rely on periodic scanning?

8.3.4 What visibility would we have into what is happening on our endpoints?

8.3.5 In the event of an alert, does your solution provide remediation recommendations?

8.3.6 What are our responsibilities in regards to managing the solution?

8.3.7 How long is the endpoint data retained for forensic purposes?

8.3.8 Do you have threat intelligence embedded in your solution?

8.3.9 Does your solution provide coverage for Windows, Linux and Mac OS endpoints?

8.3.10 Do you provide the ability for remote incident response and quickly isolating compromised endpoints from your network?

8.3.11 Do you solution use an onsite appliance and/or professional services to assist with implementation and training?

8.4 Malware Protection

8.4.1 Describe your managed service for advanced malware protection.

8.4.2 Does your solution utilize sandboxing technology? If so, what type?

8.4.3 Can your solution detect malware that is designed to evade traditional sandboxes?

8.4.4 Can your solution detect zero-day threats?

8.4.5 Do you have threat intelligence embedded into the solution?

8.4.6 Do you offer complimentary services to provide defense-in-depth?

8.4.7 In the event of a compromise, will you help us remediate?

8.5 Cloud Services

8.5.1 How do your cloud technology services assist in increasing our overall security posture?

8.5.2 Explain how your solution handles the ephemeral nature of the public cloud.

8.5.3 How do your monitored and managed cloud solutions enable correlation across Public Cloud and On Premises environments?

8.5.4 Describe the technical architecture for your Managed Security Services in the cloud, including whether an agent is installed.

8.5.5 Describe your cloud security solution’s activation process.

8.5.6 Describe your approach for implementing a monitored/monitored and managed IPS solution in the cloud for COMPANY XYZ.

8.5.7 Describe your approach to analyzing and correlating cloud log and event data and how you gain visibility into anomalous activity.

8.5.8 What log and event data sources from Cloud Service Providers (CSPs) are supported?

8.5.9 How long do you retain or make available cloud log and event data?

8.5.10 Can you monitor the performance of virtual Firewall and Web App Firewall applications in the cloud?

8.5.11 Do you have a security team that can assist us with security audits/certifications, if needed?

8.5.12 Do you have existing agreements with various Cloud Service Providers to perform intrusive and non-intrusive vulnerability management assessments?

8.5.13 Describe your analytic and correlation capabilities. How do you balance automated processing through human validation and assessment?

8.5.14 Do your clients have access to a cloud monitoring portal? What reports are available?

8.5.15 Do you have a dedicated team of security researchers? Describe their research and how it is incorporated into cloud threat intelligence.

8.5.16 Do you offer ancillary cloud security services such as Consulting, Technical Testing, Incident Response or Threat Remediation in the cloud?

8.6 Managed Security Services Reporting

8.6.1 Describe your standard reporting process? How frequently will we receive standard reports? Do you have web-based reporting capability? Provide samples reports and screen shots of web-based interface.

8.6.2 Do you have asset-based reporting allowing COMPANY XYZ to create and group assets, assign criticality and view event, scanning and all other information using asset views?

8.6.3 Do you support ad-hoc reporting requests? Describe the process for requesting ad-hoc reports. Provide the timeframe for turnaround of ad-hoc reporting.

8.6.4 Do you support the ability to create PDF reports? Can they be sent securely via email? Can they be digitally signed and tracked?

8.6.5 What is your approach to providing meaningful security metrics? Describe reports available in the portal that clients can use to demonstrate security effectiveness and ROI.

8.6.6 How is your reporting interface structured? Do we use multiple interfaces for different services? Is the information integrated across service line? What cross-service line metrics and reports do you offer?

8.6.7 Can we create custom reports? How is this accomplished?

8.6.8 What pre-built reports are available? Are there compliance reports? If so, which regulations are supported?

8.6.9 Describe help desk or ticketing functionality. What workflow management features are available?

8.6.10 Can you integrate with client ticketing systems?

8.611 How long is data available in the portal for reporting?

8.7 Client Support and Account Management

8.7.1 Describe your company’s process for client-initiated tickets, as it relates to incidents and support issues.

8.7.2 What is your approach to client support?

8.7.3 How is your client support structured? What is the escalation process for reported problems or issues?

8.7.4 What are the hours for client support? Does support change hands at any point? What locations is this support provided from? How do you maintain quality of support 24x7?

8.7.5 What kind of value-added support options are available? Can you provide a dedicated technical account manager? At what cost?

8.7.6 Describe how you measure and report client satisfaction, including frequency.

8.7.7 Describe your processes and mechanisms for handling client inquiries and reported problems.

8.7.8 Describe your client service responsiveness, hours of staff availability, and available communication mechanisms (e.g., written, verbal, electronic, face-to-face).

8.7.9 Describe how client satisfaction deficiencies are addressed and resolved.

8.8 Service Level Agreement

8.8.1 Describe your service level agreements for the proposed services. Provide detailed SLAs.

8.8.2 Explain your company’s methods for monitoring and measuring SLAs. What options are available to us upon failure to meet your stated SLAs?

8.9 Implementation

8.9.1 Describe your approach to implementing services.

8.9.2 What client resources are required to support implementation?

8.9.3 What is the typical implementation timeframe?

8.9.4 How do you ensure minimal impact or disruption to the client?

8.9.5 What steps do you take to ensure full and complete implementation?

8.9.6 Detail the handoff process once services are established.

8.9.7 What training is necessary to client staff to introduce them to the services?

8.9.8 How do you handle implementing services across widespread, geographically dispersed facilities?

9 Value Attributes

Value attributes are a third element of our requirements. They describe the overall value of your service offerings. Value attributes include:

* Industry Specific Experience
* References

9.1 Industry Specific Experience

9.1.1 How many clients do you provide monitoring or security device management services for in the [insert industry] industry?

9.1.2 Do you have experience monitoring [insert unique monitoring requirements for industry]?

9.1.3 What reports are available comparing clients to peers and others in their industry?

10 Pricing

10.1.1 Please provide pricing estimates for the proposed for a 12-month period. Please ensure all costs are reflected, including “implied” or non-explicit costs.