XYZ Company

|  |
| --- |
| Request for Proposal |
| TitleDUE DATE |

Instructions on How to Use This Document

Within this document, you will find:

* **Section 1:** Standard pre-populated administrative/instructional information (with yellow highlighting for your company to fill in specific details)
* **Section 2:** Starter information for your company to fill in specific details around objectives and solution requirements
* **Section 3:** Starter information for your company to fill in specific details around existing technical environment and scope requirements
* **Section 4**: Standard pre-populated instructional information regarding response requirements
* **Sections 5-8:** Pre-populated questions for potential vendors to answer when responding to your RFP
	+ It is important to note that, Section 7 specifically, ideally should be adapted to your service needs/requirements (for example, remove Section 7.3 if not interested in managed services; or mark each section as Required vs. Optional)

Table of Contents

1 Introduction and Overview 5

1.1 General 5

1.2 Confidentiality of XYZ Company Information 5

1.3 News Releases 5

1.4 No Contractual Relationship 5

1.5 Primary Contract Relationship 6

1.6 Proposal Costs 6

1.7 Evaluation of Proposals 6

1.8 Basis for Award of Agreement 6

1.9 Amendments to RFP 6

1.10 RFP Schedule 7

1.11 Vendor Questions 7

1.12 Acknowledgment of RFP Receipt 7

1.13 Election Not to Submit Proposal 7

1.14 Proposal Submission 7

1.15 Form of Service Agreement 8

2 XYZ Company’s Current Business Environment 9

2.1 XYZ Company Overview 9

2.2 Business Requirements 9

3 XYZ Company’s Current Technical Environment 10

3.1 Company Workforce 10

3.2 High Level Technical & Security Architecture 10

3.3 Offices and Regions 10

3.4 Computing Environment 10

3.5 Key Cloud Services and Applications 10

4 Response Format 12

5 Vendor Profile 13

5.1 Primary Business Purpose 13

5.2 Corporate History 13

5.3 Management Team 13

5.4 Services Offered 13

6 Business Attributes 14

6.1 Financial Viability 14

6.2 Managed Service Viability 14

6.3 Security Vision and Investment 14

6.4 Security Practices 15

6.5 Service Delivery Infrastructure 15

7 Service Attributes 16

7.1 Platform 16

7.2 Endpoint Technology 17

7.3 Managed Detection and Response 17

7.4 Incident Response 17

7.5 Implementation 17

8 Pricing 18

1. Introduction and Overview
	1. General

XYZ Company issues this Request for Proposal (RFP) for a Managed Detection and Response provider to deliver services consisting of but not limited to:

* 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 XYZ Company, and includes any subcontractors to be used by the Vendor to provide the solution. “Agreement” shall mean the agreement that XYZ Company executes with the awarded Vendor for the services hereunder.

XYZ Company issues this request for a Managed Detection and Response provider with the intent of having a third party monitor the XYZ Company 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.

* 1. Confidentiality of XYZ Company Information

This RFP, and all information provided to the Vendor in connection herewith, is XYZ Company’s confidential and proprietary information (the “Information”). The Vendor may not disclose this RFP, or any Information that XYZ Company may provide the Vendor to assist the Vendor in developing a Proposal, to any other person or entity without the prior written approval of XYZ Company. The submitted Proposal, and all information provided by the Vendor in connection hereunder, is Vendor’s confidential and proprietary information (the “Information”). XYZ Company may not disclose the Proposal, or any other Information that Vendor may provide to XYZ Company 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 XYZ Company 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.

* 1. News Releases

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

* 1. No Contractual Relationship

Nothing contained in this RFP creates, nor shall be construed to create, any contractual relationship between XYZ Company and any Vendor. XYZ Company 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 XYZ Company 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.

* 1. Primary Contract Relationship

XYZ Company 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 XYZ Company 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.

* 1. Proposal Costs

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

* 1. 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 XYZ Company provided that they meet the requirements of this RFP. No revisions or amendments to the proposal will be accepted after submission unless approved by XYZ Company.

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

XYZ Company 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 XYZ Company’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
	1. Basis for Award of Agreement

XYZ Company 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. XYZ Company 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.

* 1. Amendments to RFP

XYZ Company 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 XYZ Company. Vendors are required to acknowledge all amendments in writing.

* 1. RFP Schedule

The schedule for this RFP is as follows:

|  |  |
| --- | --- |
| **RFP Issued:** | XXX |
| **Vendor’s Intention to Bid by:** | XXX |
| **Last Date to submit questions:** | XXX |
| **Answers provided by:** | XXX |
| **Proposal Submission:** | XXX |
| **Target for XYZ Company** **Decision:** | XXX |
| **Solution Implementation:** | XXX |

* 1. 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 XYZ Company’s intent to provide responses to questions to all Vendors where appropriate.

* 1. Acknowledgment of RFP Receipt

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

* 1. Election Not to Submit Proposal

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

* 1. 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 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.

XYZ Company 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.

* 1. Form of Service Agreement

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

1. XYZ Company’s Current Business Environment
	1. XYZ Company Overview

XYZ Company delivers safe, reliable and affordable xxxxxxxxxxxxxxx. The purpose of this request for proposal 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 XYZ Company 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.

* 1. Business Requirements

As part of XYZ Company security best practices, it has been deemed vital for XYZ Company to implement, maintain and monitor appropriate security measures. This is to:

* Provide protection for our internet-facing applications and client services
* Prevent any internal damage to our network from the outside
* Provide sufficient security measures for XYZ Company assets on- and off-network

This should encompass a 24x7 service that:

* Differentiates based on detection use cases for credible threats
* Differentiates based on network, cloud, and endpoint data
* Differentiates based on a clear method for reducing false positive incidents
* Xxxxxxxxxxxx

Additionally, XYZ Company and/or Vendor must be able to declare an incident and the Vendor must provide incident response support to enable XYZ Company to be able to conduct its business. These services will enhance our security posture and reduce our risk of a security breach.

1. XYZ Company’s Current Technical Environment

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

(add and remove rows where needed)

* 1. Company Workforce

XYZ Company’s workforce is comprised of approximately ## persons. ##% of these workers are knowledge workers that use XYZ Company’s technical assets (##% are manufactory floor / retail / field workers that do not use technical assets).

* 1. High Level Technical & Security Architecture

[INSTRUCTION: Example information provided below, customize to your environment.]

XYZ Company operates ## facilities, each connected to a co-located datacenter and each other via a SDWAN. The datacenter is connected to AWS via a dedicated ExpressRoute link. Each office also maintains direct Internet connectivity.

E-mail services are provided by Microsoft Office365 E3 licensing. Infrastructure-as-a-Service are provided by Microsoft Azure and AWS.

* 1. Offices and Regions

|  |  |  |
| --- | --- | --- |
| Region | No of Offices | Special Regulations |
| US and Canada | # | # |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Computing Environment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Windows (Supported Versions) | Windows Legacy | Mac OSX | Linux |
| End-user Computing | # | # | # | # |
| On-Prem Servers(physical or virtual) | # | # | # | # |
| Cloud Instances | # | # | # | # |

* 1. Key Cloud Services and Applications

[INSTRUCTION: Example information provided below, customize to your environment.]

|  |  |  |
| --- | --- | --- |
| Name | Quantity | Comments |
| Microsoft Office 365 | 10,000 users E3 | primary messaging and productivity suite |
| Microsoft Azure | 50 | Internal applications servers |
| AWS | 200 | hosts externally facing marketing site |

1. Response Format

XYZ Company 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 three 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.

1. Vendor Profile
	1. Primary Business Purpose

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

* 1. Corporate History

Please provide a brief history of your company.

* 1. Management Team

Please provide brief biographies of your management team.

* 1. Services Offered

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

1. Business Attributes

**Business attributes are one element of XYZ Company’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**
	1. Financial Viability

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.

Describe your most recent fiscal year’s revenue growth rate over the prior fiscal year.

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

* 1. Managed Service Viability

What is your company’s core business strategy? What are your primary lines of business in terms of annual revenue, and in terms of customers? What is your growth driver? Where do security services fit into your business strategy?

Provide details on how long you have offered each of your services.

Describe any recent industry analysis (e.g., Gartner, Forrester) and awards your company has won.

* 1. Security Vision and Investment

Describe your company's vision and direction for developing new technologies in support of your solutions.

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

Describe how your security staff responsible for product and service delivery contribute to innovation and enhancements?

Describe how customer feedback influences your product and/or service enhancements.

Provide examples of innovation and enhancements to your product and/or service offerings.

Do you have a dedicated research team? If so, describe its function and focus areas.

What information sources does your research team source for intelligence?

Provide examples of your threat research.

* 1. Security Practices

Provide detail on your internal security policy and procedures, documenting any industry standards (ISO 17799, CobiT, etc) that you have adopted or follow.

Have you had an independent review of your MSSP infrastructure and service (ISO compliance review, SAS 70 review)? If so, please provide details. If not, describe your plans to have a review performed in the future.

Do you conduct internal security reviews of your infrastructure and service? If so, please provide details. If not, would you grant us the right (or a third party on our behalf) to audit your operations and determine the appropriateness of implemented safeguards?

Describe your business continuity/disaster recovery approach.

Describe how you handle data privacy, in relation to European customers.

* 1. Service Delivery Infrastructure

Do you operate and manage your own SOCs?

Where are your SOCs located?

Are all of your SOCs operational 24x7x365?

Describe security safeguards around the SOCs.

Do you permit an onsite SOC visit as part of the vendor evaluation process? If so, what is the process for planning the visit?

1. Service Attributes
	1. Platform

Describe your platform architecture

Does the platform rely on any third-party security technologies for event collection, correlation or analysis activities?

How are the key differentiators of your platform?

Describe any third-party testing your platform has undergone.

Provide a listing of technologies you can integrate with your platform. Please provide categories of devices as well as specific vendors technologies you support. Describe your preferred collection method used to gather security logs or events from devices. Describe other non-preferred collection methods that you support.

Describe how your platform analyzes EDR telemetry for threat detection.

Do you support analyzing telemetry from multiple EDR technologies simultaneously?

How scalable is your platform? Provide the current event load across your client base. How does your platform manage spikes in traffic growth?

What data do you analyze from collected logs?

Describe your ability to monitor technologies via their native APIs.

Describe your platform’s ability to extend functionality via APIs.

Describe how the confidentiality of the communications is protected across public networks.

Describe how your platform filters and normalizes incoming data.

Describe how your platform identifies suspicious activity.

Describe your data retention policy.

Describe the advanced analytics (machine learning, data science) capabilities of your platform.

Describe how threat intelligence is integrated in your platform.

Describe your approach to correlation of data across your customer base.

How do you gain visibility into anomalous activity and how is that activity analyzed?

Describe your approach to reducing false positives.

Describe the Service Level Agreements (SLAs) of the platform.

Describe your application interface functionality.

How do users connect to the application interface?

How many users can the application interface support?

Describe your customer support model. Can we access your security analysts without subscribing to your service?

Describe the qualifications and certifications of your security analysts.

* 1. Endpoint Technology

Describe the endpoint agent included in your solution.

Describe the endpoint agent’s detection and response capabilities.

Does the endpoint sensor allow for on-demand querying of endpoints?

What visibility does your endpoint agent provide?

What operating systems does your endpoint agent support?

* 1. Managed Detection and Response

What are the features of your MDR service?

What Endpoint Detection and Response (EDR) technologies are supported for your MDR service?

Describe the staff and qualifications involved in your MDR service delivery.

What types of data do your analysts consider in their investigations?

Describe your MDR investigation solution workflow, how conclusions are reached, and how customers are notified.

What kind of analysis and communication can we expect in the event of a security incident? Please provide a sample investigation.

Describe any Incident Response (IR) capabilities included in your MDR service.

Describe how your IR team interacts with the security analyst team.

Describe any threat hunting activities included in your MDR service.

Describe any security advisory functions included in your MDR service.

Describe any Service Level Agreement (SLAs) included in your MDR service.

Describe any service limitations or thresholds that we would be charged additional fees for exceeding. How many incidents can be escalated before additional fees are charged?

* 1. Incident Response

Do you offer an Incident Response retainer? Describe any emergency IR services covered by the retainer.

Describe any consulting services covered by the retainer.

Is there a minimum upfront financial commitment required for your retainer?

Describe the Service Level Agreements (SLAs) provided with your retainer.

Indicate the experience of your IR consultants.

Describe how you integrate and apply Threat Intelligence into your IR services.

* 1. Implementation

Describe your standard implementation approach.

Describe any options for on-site and additional support.

What client resources are required to support implementation?

What is the typical implementation timeframe?

1. Pricing

Describe your pricing model.

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