SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

RFP/RFI Questions for Managed Security Services

Sample MSSP RFP Template

Table of Contents

Request for Proposal Template Overview

Introduction

In order to request services from a Managed Security Services Provider (MSSP), many organizations create a Request for Proposal (RFP). This gives a number of MSSPs the opportunity to submit information on how they can assist the organization with their IT security needs as well as provide the pricing for their services.

This document is designed to assist with writing an RFP for MSSPs. The document outlines a sample RFP and various questions to use as a template for a RFP. The different sections are designed to convey information about an organization and the services the organization expects the MSSP to provide, as well as setting expectations about the partnership.

The first section, "Suggested RFP Outline" contains the RFP section headers. "RFP Sample Questions" outlines questions to potentially ask an MSSP. Keep in mind that the fewer questions asked, the shorter the response will be. So only use the questions that are the most relevant to the organization's individual needs.

Together, these two sections will develop a RFP template for Managed Security Services and also help the organization find the best MSSP for their needs.

How to Use this Document

For a copy of this document in Microsoft Word format, email solutionarynews@solutionary.com.

Use the document as needed to get the necessary information to make an informed decision. Make sure to delete any generic information and replace it with specific content, based on the organization's needs. Specific areas to modify and customize include:

- Headers that are specific to this document, such as "Request for Proposal Template Overview", "Suggested RFP Outline" and "RFP Sample Questions."
- Delete any questions not relevant to the organization in the "RFP Sample Questions" section. The MSSPs will be required to respond to those questions, so make sure they cover all the information necessary to make a decision.
- Read through and customize the five sections under "Suggested RFP Outline." This entire section will need to be specific to the organization and should include the information necessary for the MSSP to respond to the RFP.

The most important part of the RFP process is to be clear with expectations. The more information conveyed to the MSSPs, the better a response they can submit. A common mistake organizations make when writing an RFP for managed security services (MSS) is not listing all of the technologies in their environment that the MSSP will monitor or manage, including the quantity and type (model number) of each in-scope technology platform. Without this information, an MSSP won't be able to give the best response. They may have to make assumptions about the environment, which could impact the pricing and services they're submitting.

In addition, RFPs that are short and concise are typically the best options for the requesting organization and the MSSPs responding. Keep in mind what information is actually necessary for an RFP, and what can be done in an on-site presentation. Many organizations just use a template, without thinking about what type of response they will get back.

A 100 plus page response from an MSSP can be overwhelming, a strain on personnel resources and essentially useless because it just has too much information to go through, whereas a 30 page response with the exact information needed can expedite the process immensely.

Choosing the right MSSP partner is an important decision in an organization's overall security program. Writing an RFP is the first step in the process to finding the right fit for the organization. Using this document, an organization should be able to write a tailored RFP that will help make the best and most knowledgeable decision possible.

The companion documents Solutionary recommends for creating an RFP are listed below. **For your complimentary copy contact: solutionarynews@solutionary.com**

1. ***How to Choose an MSSP***
   This document lists items to consider when choosing between MSSPs and discusses details on criteria for successfully choosing an MSSP.

2. **Solutionary white paper - *How to Write an MSSP RFP***
   This white paper gives tips and suggestions for writing an RFP, poses several questions for the organization to address prior to the RFP process as well as provides a list of the top 25 RFP questions to ask an MSSP.

Suggested RFP Outline

Company Background

Describe the company - history, employee count, size of the environment, number of locations and any other relevant information pertaining to the requirements of the RFP. Particularly, describe how security and compliance information will be managed and consumed by the organization, whether the structure is centralized or decentralized and what groups or departments exist within the IT organization. This will give the MSSPs information about the organization, so they can tailor their proposed solution to match the any specific needs.

RFP Objective and Project Overview

In this section, state why the company is considering an MSSP service. Explain any specific requirements or needs. The RFP objective should be clear enough that any company receiving the RFP will know if they are a good fit for the request.

Also, include a list of all the technologies in the environment that the MSSP will monitor or manage. Make sure to include the quantity and type (model number) of each in-scope technology platform. This section should include as much information about the environment as possible to give the MSSP a solid understanding of what will be expected throughout the partnership.

Proposal Instructions and Timelines

The proposal instructions and timeline are needed to set clear expectations of the RFP and the format of the response. This section will include the date and time the RFP is due, who the RFP response will be sent to, and any font or formatting requirements. It should also include any additional information for the MSSP, such as the deadline for the intent to propose, a deadline for questions to be submitted, when the questions will be addressed, any vender onsite presentations and dates for the final decision.

List the point of contact for all RFP related questions and information on where to send the completed RFP. Any special requirements can be listed in this section as well, such as if the completed RFP must be mailed (provided in hard copy) or can be sent via e-mail (electronic copy). If hard copy is requested, make sure to include any requirements for the number of printed and/or electronic (flash drive) versions.

Point of Contact for RFP related Questions:

Name:
Title:
Email Address:
Phone Number:

Please submit the RFP by email to the following:

Name:
Title:
Email Address:
Phone Number:

Below is a suggested timeline:

Activity	Date and Time
RFP Distribution	Date/Time Distributed
Intent to Propose	Approximately 3 business days after distribution
Questions Due	Approximately 5 business days after distribution
Question Responses	Approximately 8 business days after distribution
Proposals Due	Approximately 14 business days after distribution
Vender Onsite Presentations	Approximately 10 days after proposals due
Decision	Approximately 30 days after proposals have been submitted

Proposal Response Outline

This section outlines the RFP response and describes what is expected in each section. Make sure to indicate any specific requirements that the RFP response needs to follow. An MSSP will follow this outline when responding to the RFP. Consider providing an outline of the type of response desired, as described below:

1. **Table of Contents**
2. **Executive Summary:** Brief introduction and overview of the Proposal. Explain how the MSSP will assist with the IT security posture of the company. Please limit the executive summary to 5 pages.
3. **Services Overview:** Brief overview of the services being proposed.
4. **RFP Requirements:** Respond to all questions in the requirements section. Give a detailed response to each of the questions or indicate that the proposed solution does not meet the requirements of the question.
5. **Pricing:** Provide a detailed list of the pricing for the MSSP services. Include any options that may be available and explain how the pricing was calculated. Make sure the explanation of pricing matches the services requested and that all vendors are providing a similar level of service.
6. **Appendix:** Any relevant information not addressed in the RFP Requirements, including any optional services.

Client Requirements

Please see the next section in this document labeled “RFP Sample Questions” for suggested questions/requirements.

RFP Sample Questions for Managed Security Services

These questions were written based on various requirements for Managed Security Services Providers (MSSPs) and will enable an organization to determine the best MSSP to partner with. Please remove any questions that are not relevant to the organization. The more questions in an RFP, the longer the response. A shorter, more concise response with less questions will be easier to review and compare MSSPs.

1. MSSP Overview

1.1. Please give a brief company description. Include how long the company has been providing MSS.
1.2. Please outline the proposed services.
1.3. Please describe any awards your company has won.
1.4. What industries do you provide services to?
1.5. Does your company have tiered service levels? If so, please list them here.
1.6. Has your company successfully completed an SSAE 16 SOC1 Type II Audit?
1.7. Explain you disaster recovery plan.

2. MSSP Services Overview

2.1. Describe the groups delivering the proposed services including the group name, whether they are in-house or partner staff, their qualification/certification process, their geographic location and the availability of personnel (24/7, 8/5, etc.).
2.2. Describe at a high level the general process flows for the proposed services. Explain any significant exceptions and differences that exist between service tiers.
2.3. Do you use your own technology, third party products or a combination for service delivery? Describe the technologies, products and tools used to deliver each of the proposed services. Describe any patents your technology has been awarded.
2.4. Will any hardware need to be installed to support the proposed services? If so, what specific hardware and who will install, maintain and manage the hardware?
2.5. Will any software need to be licensed and/or installed to support the proposed services? If so, what specific software and who will install, maintain and manage the software?
2.6. Describe your SOC and the level of support it provides. Please include your SOC qualifications and certifications.

3. Log Monitoring

3.1. Do you provide log monitoring services to your clients? If so, describe your log monitoring capabilities and service tiers.
3.2. Are you able to accept feeds from security devices, network devices, applications, endpoints and databases? Describe the devices your solution supports.
3.3. Describe your process for identifying the security relevant events from these feeds and explain, for example, the types of events you process from (both) a Windows host (and organizationally critical device) and how the event information can be used within your correlation and rules engine.
3.4. Do you enrich log data with contextual elements such as IP reputation, Geo IP or assets?
3.5. What are your analytic and correlation capabilities? Describe the continuum from automated processing through human validation and identify the hand-off between the two.
3.6. Can you analyze and correlate data to identify security events and classify events according to severity?
3.7. Can you correlate across multiple device types in a client environment? If so, how specifically is this accomplished?
3.8. How does device and environmental context factor into the identification, validation and escalation of security incidents?

3.9. Are you able to correlate events across clients?
3.10. Can you correlate events by identity (user)?
3.11. Do you have advanced threat detection capabilities?
3.12. Describe how you detect threats. Do you use signatures, behavioral analysis, anomaly detection, volume analysis or malicious host detection?
3.13. Do you have the ability to identify malicious hosts? If so, please explain the scope and mechanism(s) used to do so.
3.14. Can log data be stored for one year (at least 90 days online)?
3.15. How does your company incorporate unsupported devices? What is your process for adding new device support?
3.16. Do you have a customized escalation process for alerts? If so, please explain.

4. Device Management

4.1. Do you manage devices on behalf of your clients? If so, describe your device management capabilities and service tiers.
4.2. Describe the mechanism(s) available to request changes to a managed device.
4.3. Do you provide for the concept of “normal” changes vs. “emergency” changes? Describe how emergency changes are handled differently than normal changes.
4.4. Do you offer shared device management/co-management of devices? If so, describe the model used and any requirements or limitations.
4.5. Describe the on-boarding process for taking over management of new devices. What reviews, validations or rationalizations are performed on the device configuration and health?
4.6. Describe the support and assistance you can provide in moving from a traditional IP/network policy based firewall to a protocol/application policy (next-generation) based firewall?
4.7. How is troubleshooting handled as part of the device management service?
4.8. Describe your policy and process for validating changes requested to a managed device.
4.9. List the certifications/experience of the security engineers that will be managing the devices for the service proposed.
4.10. How are projects such as major version upgrades, vendor changes, and client infrastructure changes handled within the device management service?
4.11. Describe the relationships that you have with the device vendors included in the proposed services that ensure you are aware and understand device and software changes.

5. Vulnerability Management

5.1. Do you provide vulnerability management services to your clients? If so, describe your vulnerability management capabilities and service tiers.
5.2. Do you integrate with third-party vulnerability scanning services? If so, please describe which services and how.
5.3. Are you an approved PCI ASV? If so, describe the features of your vulnerability management services that help meet PCI compliance.
5.4. Do you provide managed application layer vulnerability scanning? If so, describe your application scanning capabilities and service tiers.
5.5. Describe your configuration, scoping and scheduling capabilities. Explain what is user configurable vs. what must be configured by you.
5.6. If we choose to use our own vulnerability scanning tool, does your system allow vulnerability scanning results to be uploaded? If so, which vulnerability scanners are supported?
5.7. Do you provide managed vulnerability result validation as part of your vulnerability management services? If so, describe how this validation is accomplished.
5.8. Do you provide a vulnerability lifecycle management capability? If so, describe the granularity with which vulnerabilities can be managed — how they can be assigned to appropriate groups, how they can be dispositioned and any auto-processing performed by the system to validate the disposition.
5.9. Can your system correlate vulnerability scanning results with event data to provide on-target/off-target status and an impact analysis rating?

6. Threat Intelligence

6.1. Do you have a dedicated team for security research? If so, describe the focus of the research.
6.2. How does the research performed by your team directly impact the services delivered?
6.3. What feedback mechanisms exist within your services to capture threat intelligence?
6.4. List the proprietary and third-party intelligence feeds that are integrated into the proposed services.
6.5. Does your security research team develop threat reports? If so, how often? Please attach any relevant reports.
6.6. Do you have partnerships with technology and service providers to keep updated with the latest alerts and notifications?

7. Incident Response

7.1. Do you have critical incident response services? If so, describe the different types / tiers of service available.
7.2. How is your incident response team integrated into the service delivery teams, particularly the log monitoring team?
7.3. Do your customers that subscribe both to log monitoring and incident response services receive an advantage as a result? If so, how do you achieve that advantage?
7.4. Describe your capabilities during an incident response engagement including incident management, evidence gathering, malware and forensic analysis capabilities, law enforcement interfaces and expert witness capability.

8. Reporting and Portal

8.1. Describe your reporting capabilities.
8.2. Can you support ad-hoc reports?
8.3. Can you create custom reports? If so, under what terms and conditions?
8.4. How do you support audit/compliance requirements?
8.5. Do you have a separate portal interface for clients, or is it the same interface that the SOC analysts use?
8.6. Provide example screenshots of the portal UI for the proposed services.
8.7. Does your portal provide the ability view raw log detail from a high level view?
8.8. Does your portal provide an executive dashboard view that is customizable?
8.9. Can your portal integrate security event data and vulnerability scanning results data in a “single pane of glass”?

9. Implementation and Customer Service

9.1. Describe your implementation services, including your normalization and tuning process.
9.2. Will we have the same dedicated point of contact for our contract, from the start of implementation to the end of the contract?
9.3. What are the hours of support? Will there be a difference in service during non-business hours?
9.4. Describe the typical interaction between your staff and our staff within each of the proposed services?
9.5. What resources will you need from us?
9.6. What training is offered to our staff?
9.7. Are there any additional costs associated with training?
9.8. What is your approach to customer service?
9.9. Explain your escalation process for customer-related problems, questions and concerns.

10. Optional Services

10.1. Please describe any optional services

About Solutionary

Solutionary is the next generation managed security services provider (MSSP), focused on delivering managed security services, professional services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

Solutionary Services include:

- Managed Security Services
  - Security Log Monitoring and Management
  - Security Device Management
  - Vulnerability Management
- Professional Security Services
  - Security Program Assessment
  - Compromise Assessment
  - CISO Advisory Services
  - Targeted Threat Intelligence
  - Incident Response
  - Penetration Testing
  - Social Engineering
  - Governance, Risk and Compliance

Contact Solutionary at info@solutionary.com or 866-333-2133

1286T 9/2015