NTT Security

How to Write an MSSP RFP

White Paper

Tables of Contents

Introduction

Request for Proposals (RFPs) are a necessary part of the sales and purchasing process. They help narrow down competition for a service and help organizations make informed decisions about which company to choose. As beneficial as an RFP is, however, they can hinder a process if not written correctly. Often, organizations write RFPs that do not ask specific questions, or ask too many questions, making the decision-making process harder than it should be.

The goal of this document is to overcome some of those issues and assist organizations with putting together a well-written RFP document that will not only ask the right questions, but will also get the correct responses needed to make an educated decision on which provider to choose.

Get the correct responses needed to make an educated decision on which provider to choose.

Why a Managed Security Services Provider?

With security threats becoming more prevalent, many organizations and businesses are looking for a Managed Security Services Provider (MSSP) to augment their internal security teams. MSSPs provide security log monitoring and management to help protect an organization's infrastructure from potential cybersecurity threats. MSSPs work as an extension of internal security teams to monitor systems in order to detect threats and malicious activity. By monitoring the environment, MSSPs are able to detect threats and alert their clients about threats. This enables the internal client team to respond and take steps to mitigate the threat. Since log monitoring and management are important parts of many security frameworks, regulations and best practices, MSSPs also support compliance requirements. Most MSSPs offer a range of services, including log monitoring, log management, security device management, vulnerability management and consulting services.

In most cases, MSSPs offer an alternative to on-premise security information and event management systems (SIEM). Using an MSSP allows organizations to avoid the costly and time-consuming installation and implementation process associated with on-premise solutions. Many internal security teams are not set up or properly staffed for 24/7 monitoring for SIEM systems. Tuning the SIEM solution and managing the alerts can also be burdensome for internal teams.

By outsourcing log monitoring and management services to an MSSP that is solely focused on securing and reducing risk to IT infrastructure, organizations have additional assurance that their environment is secure. MSSPs have visibility across their entire client base, giving them visibility to many more threats than a single organization has and allowing them to correlate threats across their client base. They also have established, proven processes for monitoring and

managing security events. Clients of MSSPs also benefit from experienced MSSP security staff who are solely focused on handling potential threats, saving time and money associated with establishing an in-house security solution.

Top benefits of partnering with an MSSP for log monitoring and management include:

- Access to security expertise, research and threat intelligence
- Highly efficient processes and workflow automation to significantly improve time to remediation for security issues
- Cost savings and scalability achieved by outsourcing time-consuming manual correlation and analysis
- Cross-device and cross-client correlation to improve security awareness and reduce risk
- Established 24/7 Security Operations Centers (SOCs) to validate and send alerts on potential security threats
- Broad visibility across the MSSP client base for improved threat intelligence

Major Items to Consider Before Writing an RFP

Many organizations struggle with writing an RFP. They often don't realize the specifics they should include about their organization. Depending on the information in an RFP, the organization could receive responses back from companies that weren't expected, not get responses back from the MSSPs from which responses are most wanted or even receive responses that answer the RFP but not necessarily fulfill the intent. The MSSP RFP process can be very tedious, stressful and overwhelming.

The most important part of the RFP process is for the expectations to be clear. The more information conveyed to the MSSPs, the better a response they can submit. A common mistake organizations make in MSSP RFPs is not listing out all 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 provide a quality response. They may have to make assumptions about the environment, which could impact the pricing and services they're submitting.

The most important part of the RFP process is for the expectations to be clear. The more information conveyed to the MSSPs, the better a response they can submit.

In addition, RFPs that are short and concise are typically the best options for the requesting organization and the MSSPs responding. Keep in mind the information that actually needs to be known in 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 receive.

A 100-page response from an MSSP can be overwhelming and a strain on resources because it is too much information to review. Whereas a 30-page response with the exact information needed can expedite the process immensely.

Current Organizational Expectations

Before even considering partnering with an MSSP, set out expectations of the relationship. Make sure to discuss what is needed from the relationship internally. Talk to the IT department about what they suggest and the best ways to be more secure and compliant. Most importantly, discuss a budget for the project (make sure it is a realistic budget). The more prepared the organization is before sending out an RFP, the more specific questions they can ask and the better information they will get back.

Some key questions to ask before working with an MSSP are listed below:

- What services are required?
- What are the time and personnel requirements? Can the organization support those requirements?
- What is the current security structure? What is currently in place? What does the IT team suggest?
- Is it required for the MSSP to implement the majority of the services they are offering?
- What level of tuning should the MSSP perform?
- How much effort can the IT security team commit to the MSSP?

Make sure to set realistic expectations. Don't start a partnership that takes time away from the current workload.

Potential questions to ask an MSSP before sending out an RFP:

- Is the MSSP able to align to the current organizational needs?
- How flexible are the MSSP services offered? Can they make a personalized solution based on the organizational needs?
- Can the MSSP monitor and manage a variety of device types?
- How will the MSSP make sure the implementation does not impact the organization?
- Is the MSSP able to work within the company budget?
- Can the MSSP provide suggestions for the security architect?

Future Partnership

Transferring between MSSPs can be costly, frustrating and strenuous on current operations. Think about the long term relationship with the MSSP as an investment that can last several years. Make sure to research and meet with the MSSP prior to the RFP. Below are several questions to address before considering a future partnership:

- How is the MSSPs customer service? Do they have a dedicated point of contact?
- Will their technology last in years to come? Are they continually updating?
- How are they planning to implement their services?
- Will implementation interrupt current operations?
- Is their reporting/portal easy to use?
- What are the training options?

These questions are essential when considering an MSSP. Always think back to how the MSSP services will benefit the organization.

MSSP Differentiators

Look at how each MSSP differentiates itself from each other. Do they have something that other MSSPs don't? Think about the below questions as you narrow down who to include in the RFP:

- Can they tailor their offering to fit the requested services?
- Are they active in threat intelligence?
- How will their technology assist with increasing the overall security posture?
- Can they meet SLA expectations?
- Do they continue to tune and improve even after implementation?

Don't be afraid to match up RFP responses to each other. Even ask a company how their services will be more beneficial than their competitors.

Don't be afraid to match up RFP responses to each other. Or even ask a company how their services will be more beneficial than their competitors.

Building an RFP

Organizations use many different sections and headers to build an RFP. Don't overcomplicate the process with content that isn't needed in the initial RFP stage. This is a fact-finding and first step in a long process to find what MSSP works best. Adding in contracts and legal is often not needed in this first stage. Should legal be sent contracts from each MSSP? Or wait until the MSSPs are narrowed down to the final two or three? Again, try to make the process as easy as possible. The RFP document is made to help make decisions easier and to obtain more information about organizations of interest.

Typically, there are only five major sections that should be included in an MSSP RFP: Company Background, RFP Objective and Project Overview, Proposal Instructions and Timelines, Proposal Response Outline and RFP Requirements. Use the below outline to build the MSSP document to send out to various MSSPs. The descriptions under each number will help to build the section in the RFP.

There are only five major sections that should be included in an MSSP RFP:

- **Company Background**
- **RFP Objective and Project Overview**
- **Proposal Instructions and Timelines**
- **Proposal Response Outline**
- **RFP Requirements**

1. **Company Background**
   Describe the company history, employee count, size of the environment, number of locations and any other relevant information the MSSP may need. 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.

2. **RFP Objective and Project Overview**
   State why an MSSP service is the right fit. Explain any specific requirements or needs, including audit, compliance and reporting needs. The RFP objective should be clear enough that the MSSP receiving the RFP will know if they are a good fit for the request.

   Include a list of all the technologies in the environment that the MSSP will be expected to monitor or manage along with the quantity and type (model number) of each in-scope technology platform. Provide as much information about the environment as possible to give the MSSP a solid understanding of what will be expected throughout the partnership.

3. **Proposal Instructions and Timelines**
   The proposal instructions and timelines are needed to set clear expectations of the RFP and the format of the response. This section should 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 vendor 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.

4. **Proposal Response Outline**

   Outline the RFP response and describe what is expected of the MSSP 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. Suggest giving an outline of the type of response desired, as outlined below:

   - Table of Contents
   - 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 five pages.
   - Services Overview: Brief overview of the services being proposed.
   - 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.
   - 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.
   - Appendix: Any relevant information not addressed in the RFP Requirements including any optional services.

5. **RFP Requirements**

   List any questions or requirements for the MSSP. See the section below for a list of sample questions. If using any of the questions, make sure to select the ones specific to what the organization needs.

   Keep in mind that the more questions sent to the MSSP, the longer a response. Keep it as short and concise as possible to get the necessary information. The simpler the format, the easier it will be to evaluate the responses.

Top 25 RFP Questions

This section includes some sample questions to use in an RFP for Managed Security Services. These questions were written based on various requirements for MSSPs and will enable a company to determine the best MSSP partner.

Please do not copy and paste all the questions listed below. Read through them and select the questions that are relevant to the organization. For the full RFP sample question document, please reach out to NTT Security.

Do not copy and paste all the questions listed below. Read through them and select the questions that are relevant to the organization.

Sample Questions

1. Please give a brief company description. Include how long the company has been providing MSS, an overview of your proposed services and explain your tiered service levels. Include information on any awards your company has won.
2. 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.
3. Are you able to accept feeds from security devices, network devices, applications, endpoints and databases? Describe the devices your solution supports.
4. 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.
5. Do you enrich log data with contextual elements such as IP reputation, Geo IP or assets?
6. What are your analytic and correlation capabilities? Describe the continuum from automated processing through human validation and identify the hand-off between the two.
7. Can you analyze and correlate data to identify security events and classify events according to severity?
8. Can you correlate across multiple device types in a client environment? If so, how specifically is this accomplished?
9. Are you able to correlate events across clients?
10. Can you correlate events by identity (user)?
11. Do you have advanced threat detection capabilities?
12. Describe how you detect threats. Do you use signatures, behavioral analysis, anomaly detection, volume analysis or malicious host detection?

13. How does your company incorporate unsupported devices? What is your process for adding new device support?
14. Do you have a customized escalation process for alerts? If so, please explain.
15. Do you manage devices on behalf of your clients? If so, describe your device management capabilities and service tiers.
16. Do you have a dedicated team for security research? If so, describe the focus of the research.
17. How does the research performed by your team directly impact the services delivered?
18. Does your security research team develop threat reports? If so, how often? Please attach any relevant reports.
19. Do you have critical incident response services? If so, describe the different types/tiers of service available.
20. How is your incident response team integrated into the service delivery teams, particularly the log monitoring team?
21. Describe your reporting capabilities. Be sure to provide example screen shots of the portal UI for the proposed services.
22. Do you have a separate portal interface for clients, or is it the same interface that the SOC analysts use?
23. Describe your implementation services, including your normalization and tuning process. Will we have the same dedicated point of contact for our contract, from the start of implementation to the end of the contract?
24. What resources will you need from us during implementation and throughout the contract?
25. Please describe any optional services.

Conclusion and Next Steps

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

The companion documents that NTT Security recommends for creating an RFP are listed below. For your complimentary copy visit: www.nttsecurity.com for regional contact information.

1. How to Choose an MSSP (datasheet): discusses details on criteria for successfully choosing an MSSP. This document will give more tips and items to consider.
2. RFP/RFI Questions for Managed Security Services (template): outlines how to write an RFP in more detail, and provides in-depth questions an organization can use to create an RFP document.

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security, and risk management programs with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com.**

1285WP 9/16