TechBeacon's 2019 Guide to Creating an RFP for Application Security Testing Tools and Services

Guide

www.microfocus.com

Guide
Security

MICRO FOCUS

Companies looking to query vendors about potential tools and services for application security can use this guide in creating a request for proposal.

While there are a lot of questions in this guide to an RFP, companies should choose no more than ten that are critical to their business. And, rather than waiting for the perfect product, companies should find the one that best matches their most important criteria.

Why should you narrow your RFP to ten or fewer questions? Because organizations that send out a long list of requirements run the risk of distorting their most critical needs. Vendors will likely describe how their product meets each of the needs you describe, and too many requirements can lead to confusion. Besides, you will be presented with too much to sort through, and comparing one proposal to another will become an arduous if not impossible task. Companies should instead focus on five to ten requirements that are most important for their app sec implementation and compare vendors on the basis of those issues.

Another good RFP example you might explore includes:

- OWASP's Application Security Verification (RFP-Criteria)

Statements About Your Current Status

Typically, an RFP includes a few up-front statements to clarify the security context for vendors. Consider writing a statement of goals and concerns and a statement of resources, as described below.

While there are a lot of questions in this model RFP, companies should choose no more than 10 that are critical to their business.

Statement of Goals and Concerns

Many effective RFPs start with a statement of a company's goals—in this case, application security goals. But often, when companies embark on an initiative to improve the security of their development process, the company's security effort is not mature enough to state firm goals. If that's the case, you can instead focus on describing your security problems.

State your goals for application security testing if you can, but most important is that you clearly state the greatest concerns your management team has regarding application security.

Goals may include:

- Services
- Manual code review
- Manual penetration testing
- Analysis of security design and architecture
- Threat modeling
- Products or services
- Automated code review (static analysis)
- Automated penetration tests and vulnerability assessments (dynamic analysis)
- Automated analysis of instrumented applications (interactive analysis)

Because vendors and service providers will often act in the role of a partner or provider, companies should also state their problems, which will aid vendors in determining if unasked-for services or products may be a better fit.

Often, the company's security effort is not mature enough to state firm goals. Instead, companies should focus on describing their security problems.

Here are examples of some potential problems:

- Our SIEM system detected significant vulnerabilities in our applications that we need to remediate
- A penetration test has found security problems in an Internet-facing application
- Our current app sec tools only partially cover our application portfolio
- Our developers continue to make the same coding mistakes that lead to vulnerabilities

Statement of Resources

In addition, you have to determine what resources and capabilities you currently have that you can use in targeting the problem:

- How much security expertise do you have and how many full-time employees (FTEs) can you dedicate to application security?
- How many websites or applications do you need to secure?
- How many developers will need to work with the tools?

Questions for Vendors

The remainder of your RFP should focus on the ten, or fewer, questions that get to the heart of your requirements. Use one or more queries from each of the following six categories to build out your RFP. Obviously, you should tailor the queries to fit your situation.

1. Vendor information

Purpose: To gather basic information about the vendor's company.

- Describe your company, its history, and its security focus.
- Who is the primary contact for sales? Who is the primary contact for technical questions?
- Do you have reference clients that we can contact?

Companies should also state their problems, which will aid vendors in determining if unasked-for services or products may be a better fit.

2. Products, services, and expertise

Purpose: Ask the vendor to describe products and services offered; the vendor's approach to application security testing; and what innovations the vendor offers. List your products and their coverage of languages and development environments. What is their primary category: SAST, DAST, IAST, or other areas?

- Is your product or service offered on-premises, or as a cloud service, or as a hybrid solution?
- What are the strengths of your product or service? What is its valid flaw (true positive) rate?
- What are the weaknesses of your product or service? For example, what is the false positive rate? And who provided those benchmarks?
- Which applications and programming languages can your products test? What development environments do you support?
- What are the core features or innovations that distinguish your product from your competitors?
- How often do you release new versions or update the software for new classes of vulnerabilities?

3. Deployment

Purpose: These questions are designed to gauge the level of investments—in money and human resources—needed to deploy and maintain a system. Flexible deployment models are in demand.

- Does the application security testing require an on-premises capital investment?
- How much time does it take to deploy the system? How long does it take to add an application to the security tests?
- Can geographically distributed development groups easily use the product or services? Please describe how.
- Does deployment require a consulting engagement? What other services do you offer before, during, or following deployment?
- What is the pricing model used? Please provide estimates for the following use case. (Describe a typical use case.)
- Does deployment require a support contract? What are the terms of your support contracts?

Ask your vendor: What are the strengths of your product or service? What is its false positive rate?

4. Operations

Purpose: This section characterizes the day-to-day operations, costs, and resource requirements of running the software or service.

- How long does the tool take to run? Will it slow down my development process?
- Is the tool appropriate for DevOps or agile development?
- Can the tool integrate with my continuous integration & continuous delivery pipeline? Is it typically run as part of the development process or as part of the QA process?
- How can learning (data output and analysis) from the system be incorporated into our development lifecycle?
- Can the tool be run by individual developers? Approximately how many full-time employees (FTEs) does it take to manage?

5. Reporting, interoperability, and integration

Purpose: The major deliverable from application security testing systems is vulnerability information. This section focuses on how that information is delivered.

- What types of reports do you offer and who are the consumers (developers, security, management) of each one?
- What information can be included in each report? Do vulnerability reports give detailed instructions on how to mitigate the vulnerability in a way that can be understood by a developer?

Contact us at:
www.microfocus.com

Like what you read? Share it.

- Do the reports provide historical trends and key benchmarks regarding the remediation of vulnerabilities?
- Does it provide such data in a format easily digestible by security information and event management (SIEM) systems and other security tools?
- Do vulnerability reports describe the specific steps needed for developers to remediate discovered vulnerabilities and steps to detect if the vulnerability has been closed?
- Does your product use or support APIs to directly communicate results with other security and IT management technology?

Can your product be integrated into a CI/CD pipeline? Approximately how many full-time employees (FTEs) does it take?

6. Privacy and data security

Purpose: Source code is a sensitive business asset. This section asks vendors how that information is protected.

- How is source code handled and secured?
- What types of encryption do you use and what data is encrypted?
- Do you offer a private key system where the encryption keys can be managed by our company?
- Do you keep data on our usage of the tools and other corporate sensitive data? What sort of security and privacy guarantees can you make?

Focus on Your Most Critical Needs

As you think through this information in creating your RFP, be sure to tailor it to your specific needs. Don't just send out all the questions provided in the six areas of enquiry! As noted earlier, pare your questions down to 10 critical requirements for your desired application security capabilities. Vendors will appreciate your laser focus, and the proposals you receive will be much easier to understand and compare as you narrow your candidates.

Good luck!

MICRO FOCUS®