Enterprise Vulnerability Management RFP

This document is designed to provide an outline for a standard Enterprise Vulnerability Management RFP. You should include any additional questions specific to your network environment and business.

Information to be included from RFP creator:

1. Goals and objectives of the RFP process

   Explain your expectations of the RFP process, including requirements, preferred format (hard copy, soft copy), due dates.

2. Description of the network environment

   Describe your network environment to allow vendors to tailor their response more closely to your actual environment. Include the number and location of separate offices and datacenters, types of applications, etc.

Information requested from vendors:

1. Vendor Information
2. Solution Architecture
3. Reporting & Alerts
4. Integration Capabilities
5. Solution and Data Security
6. Software and Vulnerability Updates
7. Discovery
8. Vulnerability Assessment
9. Remediation/Patch Management
10. Deployment and Administration
11. Training, Customer Support, Service Level Agreements, Documentation
12. Pricing

1. Vendor Information

- Primary Contact Information
- Company Description
- Business model description (software, appliance, service, consulting, MSP, etc.)
- Public or Privately held
- Number and location of offices
- Number of staff
- Number of customers
- Customer attrition rate
- Reference customers and deployment size metrics
- Patents and domain expertise
- Customer communication (advisory council, web forum, etc.)

2. Solution Architecture

- Describe your solution’s security architecture, describing how it drives efficiency within the IT security team and enhances existing security infrastructure.
- Describe how your solution’s operational requirements (hardware platform, operating system, database software, etc.) improve IT security team efficiency.
- Describe how your solution’s architecture minimizes impact and traffic on remote networks, regional offices, and campus backbones.
- Describe how your solution’s architecture minimizes impact on server performance.
- Describe how your solution’s architecture minimizes bandwidth impact.
- Describe your solution’s role-based access control (RBAC) and give examples of its use in large enterprise environments.
- Is your solution Common Criteria certified?
    - If yes, what level?

3. Reporting & Alerts

- Describe your solution’s user interface and how a user interacts with the system
    - What operating system platforms does the UI support
    - Describe any requirements (platform or otherwise) for the UI
- Describe your solution’s reporting capabilities.
- What types of standard reports does your solution provide?
- Provide samples of your solution’s standard reports.
- Does your solution support asset valuations and/or groupings?
    - If yes, describe in detail your solution’s capabilities.
- In what formats can your solution’s reports be downloaded and/or exported?
- Describe your solution’s vulnerability scoring system in detail and the methodology behind it.
- Describe the prioritization capabilities of your solution with respect to vulnerabilities and remediation tasks.
    - Describe the factors your solution utilizes to prioritize vulnerabilities (i.e. vulnerability risk, asset value, proximity of host to an insecure network, etc.)
- Explain how custom reports can be created that report on specific vulnerabilities, applications, hosts, etc.
- Describe any remediation information included in the reports.
- Does your solution provide the ability to consolidate scan data to produce a single report for the entire network?
- Does your solution provide regulatory-specific reports (Sarbanes-Oxley, FISMA, IAVA, etc.)?
- Can your product produce a report listing all hosts with a particular application?

- Does your product have any baselining/policy management capabilities (i.e. “show me all the hosts that do not match my corporate policy”)
- Can your product produce a report listing all applications on a host or network, regardless of whether the application is vulnerable?
- Can your product produce alerts:
    - Based on a specific vulnerability condition
    - When a new host is discovered
    - When a host exceeds its score threshold

4. Integration Capabilities

- Describe how your solution integrates with the typical enterprise network ecosystem (i.e. it provides vulnerability assessment, rogue device discovery, etc.)
- Describe in detail your solution’s integration capabilities with other security solutions (i.e. Security Information/Event Management, Patch Management, IDS, IPS, etc.)
    - Provide a list of all completed, functioning integrations
- Does your solution have an Application Programming Interface (API)?
    - If yes, describe the solution functionality available via the API.
    - If yes, describe how an external system or program accesses the API (i.e. protocol used, security, etc.)
- Does your solution integrate with any IDS system for the purpose of reducing false positives?
    - If yes, what is the rate of false positive reduction among your customers?
- Does your solution integrate with any asset management systems?

5. Solution and Data Security

- Explain the flow of data through your solution and the security measures in place to protect this data.
- If appliance based, what operating system is appliance based on?
- Where is the vulnerability data stored?
- What types of security are used to protect the data in transit?
- What access controls are in place on the user application?
- Describe the level of detail provided by your solution’s logging and audit-trail capabilities.

6. Software and Vulnerability Updates

- Explain your solution’s software and vulnerability update process.
- Is there any manual intervention required for software or vulnerability updates?
- Does your solution’s update capabilities support change control processes?
- What capabilities are present to accept or reject individual vulnerability updates?
- How often is your solution updated with vulnerability rules?
- Describe your vulnerability signature creation methodology and QA process.
- How often is your solution updated with new software?
- Does your solution have a service level agreement (SLA) for vulnerability updates?
- Provide a roadmap of upcoming features for your solution.

7. Discovery

- Describe in detail the method by which your solution performs network discovery, including types of information discovered by your solution (i.e. applications, network topology, etc.)
- How many ports does your solution probe by default?
- Can this list of default ports be modified (default ports excluded or additional ports included?)
    - If yes, is there any limitation to the number of ports that can be added or excluded?

- List the number and types of operating systems your solution can identify.
- List the number and types of services/protocols your solution can identify.
- List the number and types of applications identified by your solution.
- How many applications are identified as vulnerabilities? (i.e. “FTP Available”)
- How many unique vulnerabilities does your system profile?
- List devices (printers, routers, wireless access points, etc.) identified by your solution.
- Describe the ability of your solution to identify applications running on non-standard ports.
- How many hosts or services does your solution typically crash or cause to stop responding when discovering devices on the network?
- Does your solution track hosts over time in a dynamic IP environment (DHCP)? If so, describe its methodology.

8. Vulnerability Assessment

- Describe in detail the method by which your solution detects vulnerabilities.
  - Does your solution perform remote assessment, local checks with credentials, passive assessment, and/or agent-based assessment?
  - If your solution performs local checks with credentials, for what systems do you support credentials (i.e. Windows, SSH, SNMP, etc.)
  - If your solution performs local checks with credentials, describe the ability of your product to manage credentials for hosts in a large enterprise.
- What is the size of vulnerability signature database, including breakdown of types of signatures (i.e. CGI, RPC, etc.) and number of signatures that map directly to CVE IDs.
- What is the accuracy of your solution when performing vulnerability assessment (false positives, false negatives)?
- How often do your customers typically scan using your solution?
- Can your solution scan continuously?
- Scan windows/scheduled scans – explain how your solution can be configured to work around corporate “scan windows”, scan scheduling, and automatic/manual pausing/stopping/restarting of scans.
- Describe how to configure your solution to scan for a particular vulnerability or set of vulnerabilities.
- Does your solution allow users to modify existing rules or create their own rules?
  - If yes, describe the level of expertise necessary (i.e. scripting vs. wizard interface)

9. Remediation/Patch Management

- Describe your solution’s remediation workflow functionality.
- Describe in detail your solution’s integration capabilities with external ticketing systems (i.e. Remedy, iSupport, etc.)
- Describe a sample vulnerability lifecycle scenario including the steps an administrator would take to find, fix, and validate the remediation of a vulnerability.
- Does your solution’s workflow functionality include the ability to create policies enabling tickets to be created automatically based on set criteria?
- Do tickets generated by your solution include links to patches and remediation instructions?
- Does your solution support ticket validation (i.e. scan a specific host or group of hosts on demand to verify that vulnerabilities have been remediated.)
  - If yes, can this be automated in the internal workflow functionality?
  - If yes, can this be automated using an external ticketing system?
- Does your solution support individual and bulk ticket due dates?

10. Deployment and Administration

- Describe a typical deployment of your solution.

- Describe the capabilities of your solution to arrange IPs into groups.
  - Can you group non-contiguous IPs or ranges?
  - Can network groups be nested arbitrarily?
- Describe the capabilities of your solution to create users and user groups arbitrarily.
- Describe the capabilities of your solution to assign rights and privileges to users and user groups.
- What type of configuration is required prior to and during deployment?
- What are the staffing responsibilities prior to, during, and after deployment?

11. Training, Customer Support, Service Level Agreements, Documentation

- What training is available for your solution? How much is typically required and recommended?
- Does your company offer official training courses?
- What are the standard hours of your customer service and support organization?
- What are the standard support response times?
- Are any professional services required or recommended?
- What type of documentation is provided with your solution?
- Does your company provide a standard Service Level Agreement with service guarantees?
- Include a copy of your solution’s terms and conditions.

12. Pricing

Please provide a price quote based on the network topology described above. Include any maintenance fees, support fees, professional services fees, and any other fees required for deployment and ongoing support.