

Corresponde al expediente N° 22700-885/11

CONTRATACION DIRECTA 15/11

ANEXO I

ESPECIFICACIONES TECNICAS BASICAS

Herramienta de detección de vulnerabilidades e infracciones a las políticas de seguridad.

La presente solicitud tiene por objeto la adquisición de una solución de software para la detección de vulnerabilidades en la plataforma informática de Agencia de Recaudación de la provincia de Buenos Aires.

Deberá incluirse en la oferta el licenciamiento correspondiente para permitir el análisis de 100 servidores, con actualizaciones hasta el 31/12/2011.

El oferente deberá estar certificado por el fabricante de la solución. Deberá adjuntar documentación respaldatoria de la certificación solicitada, junto con la oferta.

La solución deberá tener las siguientes características. Cuya provisión deberá estar incluida en la oferta.

- Compatibilidad con plataformas Microsoft Windows, Unix, Linux y VMWare. En particular la solución se instalará en servidores con arquitectura Intel, y sistema operativo Windows Server o Linux, teniendo en cuenta la recomendación del proveedor, previa conformidad del personal técnico de Agencia de Recaudación de la provincia de Buenos Aires.
- Descubrimiento de dispositivos conectados a la red, mediante conexión a directorios (AD y LDAP), y mediante análisis de la red. Deberá incluir funciones de descubrimiento de múltiples dispositivos conectados a la red, incluyendo impresoras, routers, switches, Access points, teléfonos IP y otros dispositivos de uso habitual.

Agrupamiento automático por tipos, sistemas operativos, rangos de direcciones, nombres de host o reglas adicionales por el usuario.

- Identificación de sistemas operativos, y servicios activos.
- Descubrimiento de nivel de actualización, versiones y aplicación de parches en sistemas operativos y servicios.
- Escaneo de vulnerabilidades en sistemas operativos, servicios y aplicaciones de web (OWASP Top Ten, y CWE Top 25).
- Capacidad de análisis de plataformas Windows, Linux, AIX, Cisco, VMWare, Oracle, aplicaciones J2EE y .NET.
- Priorización de los resultados por nivel de riesgo, utilizando algoritmos avanzados que consideren la importancia de los activos, la calificación de riesgos para vulnerabilidades detectadas y tipos

Firma y aclaración

Corresponde al expediente N° 22700-885/11

de recursos, entre otros parámetros.

- Identificación de amenazas mediante correlación de eventos, vulnerabilidades y datos de los activos.
- Auditoria de directivas y evaluación de cumplimiento de normas. Compatibilidad con SCAP para la carga de directivas.
- Posibilidad de definir platillas de cumplimiento a través del escaneo de sistemas de referencia.
- Posibilidad de definir los nodos a analizar utilizando direcciones de red, tipos de sistemas, etiquetas asignadas por el usuario, entre otros múltiples criterios de clasificación.
- Generación de informes con flexibilidad para la definición de filtros y criterios de clasificación.
- Actualización permanente de las comprobaciones, firmas y técnicas de escaneo, con soporte de un laboratorio de reconocido prestigio en la materia.
- Posibilidad de realizar análisis autenticados, sin autenticar y pruebas de penetración.
- Deberá contar con un repositorio central para el almacenamiento seguro de credenciales.
- La performance de la herramienta, con un dimensionamiento adecuado del hardware donde ejecutara, deberá permitir un ciclo continuo de exploración del total de los nodos analizados en un tiempo menor a las 48 horas. El dimensionamiento mencionado deberá ser realizado por el proveedor, e informado como parte de la oferta.
- Inspección profunda, incluyendo técnicas como análisis de banners, configuraciones de directivas, claves de registro, permisos de archivos y unidades y servicios en ejecución.
- Inspecciones predefinidas de las vulnerabilidades más importantes. Posibilidad de definición de scripts personalizados para comprobaciones adicionales.
- Detección de contenido malicioso, incluyendo virus, troyanos y otro tipos de malware.
- Detección de amenazas en tiempo real, en base a información recolectada por el fabricante a nivel global, y actualizada en línea en los servidores de la solución.
- Gestión centralizada en una consola, que permita consolidar la operación de múltiples motores de análisis, con visión consolidada del estado total de la red.
- API documentada que permita la integración con sistemas propios para la gestión de incidentes y la administración de eventos.
- Almacenamiento no volátil de platillas, políticas y resultados de los escaneos.
- Monitoreo, configuración y aplicación de perches en forma centralizada para toda la solución.
- Notificación de eventos relevantes vía email.

INSTALACION

Firma y aclaración

Corresponde al expediente N° 22700-885/11

Se deberá incluir la instalación y puesta en marcha de toda la solución, sobre el hardware provisto por Agencia de Recaudación de la Provincia de Buenos Aires.

La configuración incluirá:

- Instalación en un servidor único.
- Configuración de un máximo de 3 roles de acceso a la consola.
- Configuración de un máximo de 5 escaneos personalizados.
- Configuración de un máximo de 5 reglas de asignación de tickets.
- Configuración de un máximo de 10 alertas automáticas,
- Se deberá instalar la última versión de del software disponible al momento de iniciar la implementación.
- Se deberá realizar la integración con 3 servidores Active Directory.

CAPACITACION

Se incluirá un servicio de capacitación de al menos veinte (20) horas para una cantidad de hasta ocho (8) participantes, dictado en las instalaciones de Agencia de Recaudación de la provincia de Buenos Aires. Esta capacitación incluirá aspectos teóricos y prácticos de la herramienta, incluyendo la operación y la interpretación de reportes.

SOPORTE TECNICO

Deberá presentarse un servicio de soporte técnico telefónico local (oficinas ubicadas en Argentina) durante horario laboral (5x8), que incluya la concurrencia al sitio de instalación ante problemas cuya severidad produzcan la detención del sistema, la pérdida de funcionalidades o degradación sensible de la performance de la solución.