MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

PROCURADURÍA GENERAL DE LA REPÚBLICA

PROCURADURÍA GENERAL DE LA REPÚBLICA

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN

FORMULARIO DE ESPECIFICACIONES TÉCNICAS DE EQUIPOS TECNOLÓGICOS

Formulario No.: DTIC-FORM-ESPEC-040 **Version 1.0**

ESPECIFICACIONES TÉCNICAS

INFORMACIONES DE ACUERDO AL RECURSO TECNOLÓGICO

COMPONENTES	***CARACTERÍSTICAS GENERALES***
RECURSO TECNOLÓGICO	**Scaneo de vulnerabilidades**
Tipo de Instalaciòn	Maquina Virtual / Appliance
Compatibilidad de virtualizador	VMWare
Plataforma de administración	WEB
Tipo administración	Centralizada
Tipo de escaners	Ilimitados
Implementacón	Capacidad de ser implementados remotamente sin costo
Funciones	Operaciones de exploración, administración de scaneo, administración de informes, administración de politicas
Scaneo con agentes	Debe soportarlo
Scaneo sin agentes	Debe soportarlo
Red	Debe soportar el scaneo de distintos segmentos de red y segmentos a traves de VPN
Nube	Si la solución usa componentes en la nube, debe garantizar que los datos no puedan ser manipulados por el fabricante de la tecnología. La base de datos de logs, reportes, políticas, y demás componentes, deben poder implementarse en sitio sin requerir envío de estos a la nube en caso de ser requerido por la entidad.
Informaciond e agentes	Los agentes utilizados deberán asegurarse que la orden recibida es del servidor legítimo de comando y control que hace parte de la implementación. Para comunicarse con la plataforma de nube que sea utilizada, se debe tener un intercambio tipo handshake con desafío y respuesta a través de una conexión HTTPS / TLS segura. Esta comunicación siempre debe ser iniciada por la consola local.
Integración de autenticación	Debe admitir la integración con Active Directory, Kerberos o cualquier directorio compatible con LDAP. La aplicación también deberá soportar dos almacenes de cuentas de usuario internos: Archivo XML con cuentas creadas por defecto. Un administrador global puede utilizar una cuenta incorporada para iniciar sesión en la aplicación en modo de mantenimiento para solucionar problemas y reiniciar el sistema cuando un error de base de datos u otros problemas impiden el acceso para otros usuarios. Datastore donde se enumeran las cuentas de usuario estándar, que son creadaspor un administrador global.
Integración con gestores de contraseñas	Debe tener integraciones fuera de la caja con tecnologías para protección de usuarios privilegiados como CyberArk, LastPass, Thycotic, Lieberman,
Alertas	Debe soportar la entrega de mensajes por medio de SNMP, SMTP y Syslog a las partes interesadas o soluciones integradas. La automatización personalizada se podrá realizar a través de la API basada en Web
Actualizaciones automaticas	Debe soportar actualizaciones automáticas de la cobertura de vulnerabilidades para permitir a los usuarios ejecutar exploraciones con la última cobertura inmediatamente sin interrupción del análisis.
Actualización sin conexión	Poder actualizar la solución de escaneo de vulnerabilidades en entornos en los que no haya acceso a la red ni a Internet ejecución del instalador más reciente que detecta una instalación existente y aplica cualquier actualización o reparación de archivos según sea necesario
Activos	La herramienta debe tener la capacidad de rastrear dispositivos que han sido virtualizados y pueden tener MAC y/o nombres de host comunes mediante el seguimiento de los activos a través de la dirección IP, hardware, nombre de alias, tipo de host, sistema operativo y CPE.
Programación de tareas	Las exploraciones programadas deben admitir exploraciones repetibles en ventanas de tiempo especificas e intervalos de tiempo. La duración, la fecha y la hora, así como el tiempo transcurrido entre las exploraciones, deben ser configurables.
API	La solución debe proporcionar una API bidireccional. El uso de la API no debe requerir cargos adicionales. La API debe ofrecer todas las funciones principales disponibles a través de la interfaz, con funciones adicionales extendidas para las integraciones.
Registro	Debe permitir la supervisión de escaneos y notificación automatizada cuando los escaneos están completos / incompletos.
Scaneo simplificado	La solución debe realizar el descubrimiento, el análisis de vulnerabilidades, el escaneo de aplicaciones web y la evaluación de la configuración en un
Integración con virtualizadores	Debe permitir la integración de la solución con la plataforma ESXi /vCenter de VMware permitirá la identificación de todas las máquinas independientemente del estado
Vulnerabilidades especificas	Debe admitir el escaneado automático de vulnerabilidades específicas. La solución podrá buscar vulnerabilidades específicas o cualquier combinación de vulnerabilidades
Exclusiones	Debe Permitir la exclusión de activos y vulnerabilidades de los scans
Scan Autenticados	Debe soportar realizar Scans con atenticaciòn de dispositivos de red, credenciales Microsoft, Linux, entre otros
Scaneo de hash	Debe admitir la capacidad de escanear usando "Pass The Hash" para identificar la reutilización de la contraseña.
Referencias	Debe proporcionar ID de referencia desde bases de datos de vulnerabilidades como NVD, CERT, SANS, Bugtraq, MSFT,Secunia entre otros.
Actualizacion de aplicaciones	La solución debe incluir opciones de actualizaciones automáticas y manuales
Descubrimiento automático	Debe soportar el descubrimiento automático de activos y el inventario
OWASP	Debe tener cobertura de las 10 categorías principales de OWASP
Scaneo WEB	Debe escanear las tecnologías web 2.0, incluyendo AJAX, ASP .NET 2.0 y sitios basados en Flash y utilizar Browser Emulation Scanning Technology (BEST) para recopilar datos tanto del servidor como del cliente y analizar la presencia de vulnerabilidades.
Scan en nube	La solución debe explorar las máquinas en AWS y Azure
Normativas	Debe determinar si sus sistemas cumplen con las políticas corporativas o normativas como PCI, HIPAA, NERC, SOX o FISMA.
Reportes pre-configurados	Debe incluir las plantillas de informes pre-configurados, incluyendo plantillas para generación de reportes basados en mejores practicas, que cubran riesgos, cumplimiento, remediación, y múltiples puntos de vista basados en la audiencia a quien se presenta el reporte.
Informes personalizados	Debe permitir la posibilidad de crear informes de forma personalizada
Informes automaticos	Debe permitir la posibilidad de generar informes de forma automatica y estos ser entregados via correo electronico
Gestion de riesgo	La calificación de riesgo entregada por la solución debe incluir la puntuación CVSS, posibilidad de explotación de los activos , la susceptibilidad a los kits de malware existentes, explotación y correlación de malware, la criticidad de los activos, y métricas temporales que indican por cuánto tiempo la vulnerabilidad ha existido desde su publicación.
Analisis de riesgo	la solución debe proporcionar Sistema de medición cuantitativos (Ejemplo 0-1000) así como cualitativos (es decir, alto, Medio, Bajo).
Priorización	La Puntuación de Riesgo debe permitir una priorización máxima de vulnerabilidades y proporcionar una mirada precisa a los problemas más apremiantes del sistema.
Criticidad de riesgo	La solución debe proporcionar capacidades para enfocar los esfuerzos de remediación de los activos críticos de negocio.
Exposición de Malware	Debe indicar las vulnerabilidades que son objetivo de Malware conocido o kits de explotación existentes.
Informes de remediación	Debe proporcionar informes de remediación incluyendo instrucciones de nivel ingeniero y vínculos hacia bases de datos externas para parches, descargas y referencias.
Priorización de remediación	Debe poder crear informes que identifiquen los 10 primeros pasos para reducir el riesgo de un grupo de dispositivos (definido por el usuario).
Integracion con plataformas de seguridad	Tener integración con tecnologías de seguridad de redes como IDS / IPS, GRC, NAC y SIEM.
Pruebas de penetración	Debe ser compatible con la integración con plataformas de pruebas de penetración del mismo fabricante de la solución ofertada, con el objetivo de confirmar que las vulnerabilidades pueden ser explotadas.
Contención	La solución de análisis de vulnerabilidades debe contar con un módulo de automatización y orquestación que pueda integrarse con Firewalls y Endpoints para aislar automáticamente aquellos dispositivos que represente un riesgo para la organización.
********** NO EXISTE MÁS INFORMACIÓN DEBAJO DE ESTA LÍNEA **********	