JUNTA DE RELACIONES LABORALES
DE LA AUTORIDAD DEL CANAL DE PANAMÁ
Tel (507) 321-0375 Fax (507) 321-0377
compras@juntalaboral-acp.com

COTIZACIÓN

De: Compras

Página (s): 2

Fecha: 24 de marzo de 2023

Agradecemos nos coticen lo siguiente:

Implementación (suministro - instalación y configuración) de consola Antimalware basado en la nube para 42 agentes (35 dispositvos y 7 servidores). Por un termino de 1 años

CARACTERISTICAS	DESCRIPCIÓN
Consola Centralizada de Administración	La solución debe contar con una consola de administración centralizada para administración de activos tecnológicos, políticas y reportaje.
Posicionamiento	La opción por evaluar debe estar posicionada como una solución de tipo "Next-Generation"
Agente Único	Todos los requerimientos de protección presentes en esta ficha técnica deben estar incorporados en un único módulo de despliegue que cuente con todas las funcionalidades requeridas y que no requiera diferentes ciclos de despliegue para la activación de cualesquiera de las funcionalidades necesarias.
Granularidad de Perfiles	La consola de administración debe proporcionar la capacidad de crear usuarios basados en nivel administrativo, administración por grupos y diferentes tipos de acceso basados en Roles.
Ciclos de Actualización	Es de vital importancia que la solución presentada no dependa de actualizaciones diarias de firmas y que reduzca en gran medida la dependencia de actualizaciones de cualquier índole para proporcionar un nivel de seguridad efectivo en las estaciones, de preferencia 1 o 2 actualizaciones por año.
Utilización de Recursos	La solución para evaluar debe garantizar un impacto bajo en el rendimiento de los sistemas, menos de un 10% de utilización de CPU preferiblemente.
Reportaje Avanzado	La consola de administración debe proveer información detallada sobre los incidentes de ataque, así como también del tipo de malware (programa maligno) que intenta afectar la infraestructura tecnológica presentando características tales como: capacidad anti-sandboxing, detección de ambientes virtuales y de auto-ejecución del malware (programa maligno) y capacidades de elevación de privilegios.
Sistemas Operativos Soportados	Debe soportar estaciones de trabajo de Windows XP SP3 hasta sus más recientes versiones, así como también servidores Windows Server 2003 en adelante. En adición, debe cubrir de igual forma plataformas Mac recientes y Linux (Redhat y Centos).
Motor de convicción No-Basado en Firmas (Signatures)	La solución debe poseer un motor de análisis y prevención que no dependa de actualizaciones diarias de firmas en las estaciones y servidores y que no depender del análisis tradicional de motores de antivirus (heurística y análisis de comportamiento)
Protección de Memoria Avanzada	Monitorear y controlar los incidentes en memoria a fin de proporcionar protección frente a violaciones de memoria tales como: Stack Pivot, Stack Protect, RAM Scraping, Malicious Payload, Process Injection (Incluyendo cualquier tipo de modificación o escritura en memoria) así como también intentos de elevacion de tipo LSASS Read ó Zero allocate
Control de Scripts	Monitoreo, control y bloqueo de scripts en sus diferentes variedades, teniendo la posibilidad inclusive de controlar el uso de Powershell en las estaciones basado en políticas cubriendo Active Scripts / PowerShell / Macros entre otros.
Control de Aplicaciones	De forma integrada en la solución de endpoint, no como módulo separado o adicional, la solución debe proporcionar la capacidad de implementar esquemas de control de aplicaciones de tipo "Listas blancas" con la intención de proteger equipos de trabajo de diversa índole y también permitiendo crear ventanas de cambios conforme se requiera por la administración.
Capacidades de Sandboxing	Capacidad de someter archivos detectados como sospechosos o potencialmente maliciosos para análisis adicional, detalles, acciones y especificaciones sobre como el malware(programa maligno) intenta afectar el sistema. Esta capacidad no debe estar limitada a cantidad de envíos y debe ser configurable acorde a las políticas de la institución.
Capacidad de Prevención	La solución debe poseer un alto nivel de prevención de ejecución de malware (programa maligno) y fundamentar su modelo de protección en detener las amenazas antes de que se ejecuten en el sistema y no depender de análisis de comportamiento post-ejecución.
Monitoreo de Nuevos Archivos en el sistema	Debe tener la capacidad de monitorear y analizar de forma silenciosa, todos los archivos nuevos que se crean en una estación o servidor a fin de identificar si son maliciosos o no.
Autoprotección de Servicios del Producto	Debe incorporar protección frente a los intentos de detención de servicios o procesos del AV por parte de usuarios.
Capacidad de Observar Inicio y Fin de los procesos ejecutados	La solución debe tener la característica de identificar la primera vez que identifica un nuevo proceso ejecutándose dentro de la estación y debe también informar la última vez que ha visto un proceso en ejecución
Obtención de Muestras	La solución debe permitir a los administradores, configurar la misma para que sea capaz de recolectar muestras de malware o de archivos sospechosos identificados en las estaciones a fin de poder someter los mismos a servicios de inteligencia de amenazas de terceros o realizar análisis forense exhaustivo mediante otros canales de investigación. Dichas muestras deben poder ser recogidas del sistema en cuestión o ser centralizadas en la consola de administración.
Control de Dispositivos	La solución debe contar con la funcionalidad integrada en un mismo agente, de control de dispositivos de almacenamiento removible, pudiendo identificar eventos de conexión de los mismos, su comportamiento y la capacidad de crear directivas basadas en ID del Fabricante, ID del producto, Serial del dispositivo, entre otros
Integración con Plataformas SIEM	Debe proporcionar integración transparente con los más importantes fabricantes de soluciones de Administración y Correlación de eventos de seguridad, para proporcionar eventos e información acerca de todos los componentes de la solución.
Capacidad de Análisis Forense	La consola de administración, así como el agente, deben estar en la capacidad de recolectar, analizar y presentar información relevante para los equipos de seguridad de la información, a fin de que puedan fácilmente recuperar información para análisis forense identificando detalles, vectores de ataque de forma intuitiva y fácil.
Investigar datos de alerta de ataques.	La solución debe contar que los usuarios puedan investigar las alertas de otros controles de seguridad, recuperando información del puto final.

CARACTERISTICAS	DESCRIPCIÓN
Búsqueda de amenazas	La solución debe buscar que los usuarios puedan buscar rápidamente archivos, ejecutables, valores hash y otros IOC en la totalidad de su red para descubrir amenazas ocultas.
Respuesta a incidentes rápida y automatizada basada en el libro de estrategias	La solución debe contar con los usuarios pueda recuperar información forense critica de los puntos finales que estén afectados automáticamente, así como se tomen medidas de respuesta automáticas que se descubra en un punto final dañino.
Garantía	1 año
Instalación	Consola para 42 agentes.
Capacitación	Al coordinador.

PERFIL PROFESIONAL DE LA EMPRESA CONTRATADA.

Se requiere la contratación de una empresa con especialistas en el área de instalación y configuración de servidores, equipos de telecomunicación, seguridad informática y almacenamiento.

Los especialistas deben contar, obligatoriamente, con:

Títulos profesionales en Ingeniería de Sistemas, en Computación, Ingeniería de Información, o áreas afines.

Experiencia comprobada en actividades de instalación y configuración de servidores, equipos de telecomunicación, seguridad informática y almacenamiento.

Experiencia en realización de análisis de vulnerabilidades.
Presentar constancia escrita mediante certificados que validen su experiencia. Los consultores encargados del proyecto deben contar con por lo menos siete (7) de las siguientes certificaciones aceptadas:

ECSA (EC-Council Certified Security Analyst),
OSCP (Offensive Security Certified Professional),
OSWP (Offensive Security Wireless Professional),
OSCE (Offensive Security Certified Expert),
OSWE (Offensive Security Web Expert),
GPEN (Giac Certified Pentester),
CPTS (Certified Penetration Testing Specialist)
GCIH (Giac Certified Incident Handler),
LPT (Licensed Penetration Tester)
CISSP (Certified Information Systems Security Professional)
Certificación del Producto Ofertado de la Marca del antivirus

REFERENCIAS

En forma obligatoria se debe presentar al menos dos (2) cartas de referencias de trabajos similares a los aquí solicitados. Debe incluirse el nombre de la compañía, nombre de contacto, cargo, dirección y teléfono.

REQUISITOS

Adjuntar Paz y Salvo nacional y de la Caja de Seguro Social vigentes.

Adjuntar certificación o nota que detalle el método de facturación.

La factura electrónica debe cumplir con las disposiciones de la Ley No.256 de 26 de noviembre de 2021, publicada en la gaceta oficial No.29424-B de la misma fecha, la que modifica artículos de la ley 76 de 1976, sobre medidas tributarias.

Tiempo de entrega: Inmediata

NOTA

Para consultas y aclaraciones contactar al ingeniero Rolando Rodríguez al correo rrodriguez@juntalaboral-acp.com

Esta compra se adjudica al precio más bajo, siempre y cuando cumpla con las características y requisitos mínimos establecidos

Atentamente,

La compra se adjudicará a la empresa que ofrezca el precio más bajo y cumpla con los requisitos solicitados.

La cancelación al proveedor seleccionado se hará a más tardar treinta (30) días posteriores a la presentación de la factura electrónica original y los certificados de Paz y Salvo Nacional y de la Caja de Seguro Social.

Enviar cotización por email a **compras@juntalaboral-acp.com** a más tardar el día 30 **de marzo de 2023 hasta las 3:15 p.m.** a nombre de "**JUNTA DE RELACIONES LABORALES**". Dicha cotización debe estar debidamente firmada, indicar el tiempo de entrega y garantía si fuese el caso.

En virtud del artículo 43 de la Ley Orgánica de la Autoridad del Canal de Panamá, la Junta de Relaciones Laborales de la ACP está exenta del pago de todo tributo, impuesto, derecho, tasa, cargo o contribución de carácter nacional o municipal.