Especificaciones Técnicas Suscripción Anual Herramienta de Seguridad TI

EDEESTE	
Item	**Especificaciones técnicas requeridas**
	Requisitos
1	**Generales**
1.1	El licenciamiento deberá estar basado en suscripción anual.
1.2	Se requiere al menos 1 años de suscripción para ciento ochenta y seis (206) Servidores
1.3	Se requiere al menos 1 años de suscripción para mil cuatrocientos diciesiete (1657) EndPoints
1.4	Análisis de vulnerabilidades Servidores/Endpoints: realizar análisis para detectar vulnerabilidades basadas en la red en el sistema operativo y las aplicaciones
1.5	Gestión y visibilidad de Servidores/EndPoints centralizadas para mejorar la protección y reducir la complejidad de la administración de la seguridad.
	Herramienta para Servidores
2	**Seguridad en la Red**
2.1	Intrusion Prevention: detectar y bloquear ataques con base en la red de vulnerabilidades conocidas en aplicaciones y sistemas operativos populares mediante el uso de reglas de prevención de intrusiones (IPS)
2.2	Firewall: firewall basado en el host que protega endpoints en la red mediante una inspección de estado.
3	**Seguridad de Sistemas**
3.1	Control de aplicaciones: bloquear la instalación y ejecución de cualquier ejecutable y secuencia de comandos que no se haya identificado como aplicación fiable conocida o DLL.
3.2	Inspección de registros: identificar y alertar sobre cambios imprevistos, intrusiones o ataques con malware avanzado, como el ransomware, conforme suceden en sus sistemas.
3.3	Supervisión de la integridad de archivos: supervisar archivos, bibliotecas, servicios, etc. para detectar cambios. Para ello, se crea una línea base que representa la configuración protegida. Cuando se detectan cambios respecto a este estado deseado, se registran los detalles y pueden emitirse alertas a las partes interesadas.
4	**Prevención de Malware**
4.1	File Reputation: bloquear archivos maliciosos conocidos usando firmas anti-malware.
4.2	Variant Protection: buscar malware oculto, polimórfico o variantes de malware usando fragmentos de malware visto anteriormente y algoritmos de detección.
4.3	Análisis conductual: examinar un elemento desconocido mientras se carga y analizar comportamientos sospechosos en el sistema operativo, aplicaciones, secuencias de comandos, etc. y cómo estos interactúan para su bloqueo.
4.4	Machine Learning: analizar archivos desconocidos y amenazas de día cero mediante algoritmos de machine learning para determinar si el archivo es malicioso.
4.5	Web Reputation: bloquear URL y sitios web maliciosos conocidos.
4.6	Escáner de SAP: habilitar el análisis anti-malware para NetWeaver a través de la interfaz de análisis de virus (VSI) de SAP.
5	**Sistema Operativo**
5.1	Soporte Windows Server
5.2	Soporte Linux
5.3	Soporte RedHat
5.4	Soporte CentOS
6	**Servicios**
6.1	Servicio de Sandbox integrado por cada endpoint. Entorno de prueba para aísla los cambios de código no probados y la experimentación absoluta del entorno de producción o repositorio, en el contexto del desarrollo de software, incluyendo el desarrollo web, la automatización y el control de revisión.
6.2	Generador de informes o reportes personalizables ya sea utilizando plantillas suministradas por el fabricante o totalmente custom.

SAMG

Especificaciones Técnicas Suscripción Anual Herramienta de Seguridad TI

EDEESTE	
Item	**Especificaciones técnicas requeridas**
	Herramienta para EndPoint
7	**Seguridad Usuario**
7.1	Barrido de servidor para identificar indicadores de amenaza.
7.2	Herramientas de búsqueda de amenazas que utilizan los indicadores de ataque
7.3	Detecta y analiza indicadores de amenazas avanzadas, como los ataques sin archivos.
7.4	Protección frente a vulnerabilidades
8	**Seguridad de Sistemas**
8.1	Control de Aplicaciones Bloquear la instalación/ejecución de cualquier ejecutable y secuencia de comandos que no se identifique como buenas aplicaciones conocidas o DLL
8.2	Prevención de pérdida de datos: Proporciona visibilidad y control de datos y evita la pérdida de datos.
8.3	Bloqueo de dispositivos de almacenamiento.
9	**Prevención de Malware**
9.1	Protección frente a malware y ransomware: defiende los endpoints de ataques de malware, ransomware, secuencias de comandos maliciosas y otras amenazas. Incorpora funciones de protección avanzadas que se adaptan para defender el sistema de amenazas nuevas, desconocidas y furtivas.
10	**Sistema Operativo**
10.1	Soporte Windows
10.2	Soporte Mac
11	**Servicios**
11.1	Funciones de detección y respuesta: Aportan capacidad de investigación en correo electrónico, endpoints y servidores.
11.2	Defensa contra amenazas conectadas: Integrarce con otros productos de seguridad a través de sistema de inteligencia mundial sobre amenazas en la nube para proporcionar actualizaciones de respuesta rápida en sandbox a los endpoints.
11.3	Servicio en la Nube: Modelo SaaS de consola en nube
11.4	Generador de informes o reportes personalizables ya sea utilizando plantillas suministradas por el fabricante o totalmente custom.
	Soporte y Mantenimiento
12	**Servicios de Implementación**
12.1	El servicio debe de incluir soporte y mantenimiento local 24/7 por 1 año.
12.2	El servicio debe de incluir actualizaciones, soporte y mantenimiento de fabrica 24/7 por 1 año.
13	**Condiciones Especificas del Suplidor**
13.1	El oferente deberá entregar una carta del fabricante con la certificación para implementar la solución.
13.2	Las Licencias nuevas para los sevidores y las estaciones de usuarios pueden instalarse y cuando se haga el corte de la renovación se generará el cobro de la misma.

Jose Manzueta
Gerente Seguridad TI