ANEXO 1

ESPECIFICACIONES TÉCNICAS

Categoría	Requisitos
Escaneo de objetos	La solución debe poder escanear archivos, flujos NTFS, registros maestros de arranque y sectores de arranque en discos duros y unidades extraíbles locales.
Detección de malware	Debe detectar malware en procesos ejecutados bajo el Subsistema de Windows para Linux.
Escaneo dinámico	Escanear unidades creadas dinámicamente por aplicaciones y servicios.
Conectividad con la nube	Integración con servicios en línea que consulten bases de conocimiento sobre reputación de archivos, recursos web y programas. Debe mostrar cantidad de objetos procesados con dicha base.
Análisis de tráfico de red	Analizar tráfico entrante por patrones de ataque. Bloquear actividad de red de computadoras atacantes. Configurar el tiempo de bloqueo.
Análisis bajo demanda	Ejecutar análisis en áreas específicas: archivos locales, objetos de ejecución automática, memoria del sistema y procesos, discos extraíbles, registros de arranque y carpetas compartidas.
Compatibilidad con Microsoft	Soporte para archivos bajo demanda de OneDrive y compatibilidad con AMSI (Antimalware Scan Interface).
Control de aplicaciones	Rastreo y control de inicio de aplicaciones basado en Default Deny. Permitir reglas de autorización y reputación consultada en la nube. Interceptar procesos iniciados en el Subsistema de Windows para Linux.
Modos de control de inicio	1) Activo (aplica reglas), 2) Solo estadísticas (registro sin bloqueo).
Creación de reglas de aplicaciones	Regla automatizada, basada en estadísticas y eventos de negación.
Control de dispositivos externos	Registro y uso de dispositivos USB (flash, CD/DVD, disquetes, adaptadores de red, móviles MTP). Control basado en denegación predeterminada.
Modos de control de dispositivos	1) Activo (aplica reglas), 2) Solo estadísticas (solo registra actividad).
Reglas para control de dispositivos	Reglas automatizadas, basadas en estadísticas, historial de conexiones y ampliación de reglas existentes.

Categoría	Requisitos
Administración del Firewall	Gestionar configuración del Firewall de Windows, bloquear configuraciones externas. Control del tráfico con reglas aplicadas al Firewall.
Monitoreo de integridad de archivos	Detección de cambios, rastreo en interrupciones, verificación con hash (MD5/SHA256), eventos del sistema.
Monitoreo del registro de Windows	Detectar acciones en claves y valores del registro, incluyendo accesos, cambios y seguridad. Supervisar acceso por usuarios confiables o no confiables.
Protección de procesos	Insertar agente externo para proteger memoria. Si se detecta explotación: terminar proceso o reportar compromiso.
Exclusiones	Permitir exclusiones en protección o análisis, aplicables a análisis bajo demanda y en tiempo real.
Rendimiento	Contadores para el Monitor del sistema (e.g. solicitudes denegadas, procesadas por segundo, cola de infectados, etc.).
Protocolos de integración	Soporte para SNMP, WMI y exportación SIEM por Syslog. Modos de SIEM: duplicar eventos o eliminar copias locales. Convertir eventos a formato estructurado y JSON.
Sistemas Operativos Soportados - Windows	- Windows XP Pro SP2/SP3 (32/64-bit)- Windows 7/8/8.1 Pro/Enterprise/Ultimate (32/64-bit)- Windows 10 (todas las ediciones y versiones desde 1507 hasta 22H2) (32/64-bit)- Windows 10 LTSC (2015, 2016, 2019, 2021) (32/64-bit)- Windows 11 (21H2, 22H2) Home/Pro/Education/Enterprise (64-bit)- Windows Embedded (XP, 7, 8, 8.1, 10, WEPOS, POSReady)
Sistemas Operativos Soportados - Linux	- Debian GNU/Linux 9.x/10.1+/11.0+ (32/64-bit)- Ubuntu Server 18.04/20.04/22.04 LTS (64-bit)- CentOS 7.2+/7.x, CentOS Stream 9- RHEL 7.2+/8.0+/9.0+- Oracle Linux 7.3+/8.0+/9.0+- Linux Mint 20.3+/21.1- openSUSE Leap 15.0+- Astra Linux (Common y Special Editions)- Rocky Linux 8.5+/9.1- RED OS, ROSA, ALT, GosLinux, EMIAS, Atlant, AlterOS
Consola de Administración On-Premise (Windows)	Compatible con:- Windows 7 SP1+, 8/8.1, 10, 11 (todas las ediciones y actualizaciones 32/64-bit)- Windows Server 2008 R2 SP1+, 2012/R2, 2016, 2019, 2022 (Standard, Datacenter, Core, Storage Server) 64-bit
Consola de Administración On-Premise (Linux)	Compatible con:- Debian GNU/Linux 9.x/10.x/11.x- Ubuntu Server 18.04/20.04 LTS- CentOS 7.x- RHEL 7.x/8.x- SUSE Linux Enterprise Server 12/15 (todos los SP)- Astra Linux Common y Special Editions- ALT Server 9.2/10, ALT 8 SP Server (varias versiones)- Oracle Linux 7/8- RED OS 7.3 Server/Certified Edition
Consola Cloud	La consola y el DBMS deben estar alojados en entorno en la nube, actualizados periódicamente y con copias de seguridad regulares del servidor y objetos (directivas, tareas, etc.)

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Calle 14 No. 2 - 49, Palacio Municipal
direcciontic@santamarta.gov.co
(605) 4209600 Ext. 1210

Categoría	Requisitos
Navegadores Compatibles para Consola Cloud	- Mozilla Firefox ESR 91.8.0 o superior- Google Chrome 100.0.4896.88 o superior- Microsoft Edge 100 o superior- Safari 15 en macOS
Bases de Datos Compatibles	- Microsoft SQL Server Express: 2012, 2014, 2016, 2017, 2019 (64-bit)- Microsoft SQL Server todas las ediciones: 2014, 2016, 2017, 2019 (Windows y Linux)- *Nota:* Para SQL Server 2019 en Linux se requieren acciones adicionales