LISTA DE CHEQUEO
CRITERIO DE EVALUACION
1. INTEGRACIÓN E INGESTA
El oferente demostrará la disponibilidad de un catálogo extenso de conectores nativos para fabricantes líderes del mercado, garantizando la interoperabilidad inmediata y fluida con la infraestructura que actualmente tiene la FAC. 5 pts: Demuestra un catálogo nativo exhaustivo (>300 conectores). 3 pts: Catálogo amplio (>150 conectores). 2 pts: Catálogo estándar. (>50 conectores).
El oferente debe demostrar que la plataforma permite gestionar, filtrar y transformar la telemetría en el punto de recolección (antes de su ingesta y almacenamiento), de modo que la institución pueda controlar el volumen y la calidad de los datos enviados, reducir ruido y costos, y redirigir flujos a distintos destinos, sin necesidad de reconfigurar manualmente cada equipo de origen. 5 pts : La plataforma ofrece una capa de recolección gestionada centralmente que permite, mediante una interfaz unificada: filtrar y descartar eventos irrelevantes en origen, transformar y reducir el tamaño de los datos antes de la ingesta, enrutar flujos hacia uno o varios destinos, y aplicar estos cambios a múltiples colectores de forma remota sin tocar cada equipo individualmente. Soporta protocolos estándar abiertos y es agnóstica al destino. 4 pts : Permite filtrado y enrutamiento de telemetría desde una consola central, pero las transformaciones avanzadas (reducción/reformateo) requieren configuración manual por colector o edición de archivos 3 pts : Ofrece recolección centralizada con capacidad básica de filtrado, pero el control del volumen y el enrutamiento a múltiples destinos es limitado o requiere componentes adicionales 2 pts : La recolección depende de agentes propietarios sin capacidad de filtrado o transformación en origen; todo el volumen se envía sin control previo y la optimización solo es posible tras la ingesta.

El oferente debe demostrar que su plataforma puede recibir información a través de múltiples métodos de comunicación estándares (como Syslog, API, Netflow o archivos planos), garantizando que cualquier equipo, por antiguo o moderno que sea, pueda integrarse.

5 pts: Demuestra soporte nativo para todos los estándares modernos (Syslog, API REST, Webhooks, NetFlow, SNMP y lectura de bases de datos) sin necesidad de instalar software adicional en los equipos de origen.

3 pts: El sistema es fuerte en métodos tradicionales (como Syslog), pero tiene opciones limitadas o complejas para tecnologías más nuevas como la recepción de datos desde la nube (Cloud).

2. USABILIDAD

El oferente debe demostrar la capacidad de la consola para filtrar y desglosar las capacidades de detección. Se evaluará qué tan profundo llega el sistema al identificar no solo la técnica general, sino las variantes específicas (sub-técnicas) de Movimiento Lateral.

5 pts : El sistema identifica y muestra en consola la Táctica, la Técnica y al menos 3 o más Sub-técnicas específicas (ej: bajo Remote Services, desglosa RDP, SSH y SMB). La visibilidad es total y detallada.

3 pts : El sistema identifica la Táctica y la Técnica, desglosando al menos 1 Sub-técnica específica de forma nativa en la visualización.

3. ORQUESTACIÓN Y RESPUESTA (SOAR)

El oferente debe demostrar madurez en automatización de respuesta y orquestación multicapas (SOAR)

5 pts : El sistema ejecuta de forma exitosa Playbooks tipo avanzado: dinámicos, contextuales y adaptativos, con capacidades de branching avanzado, ejecución de subprocesos paralelos, integración multicapas (mínimo 3 dominios: seguridad, IT, nube o IAM), consumo de inteligencia (Threat Intelligence u otras fuentes) y mecanismos de aprendizaje o ajuste automático.

4 pts : El sistema ejecuta de forma exitosa Playbooks tipo intermedio: flujos con lógica condicional (if/else), validaciones automáticas y toma de decisiones basada en reglas predefinidas, integración con al menos 2 sistemas o herramientas, y automatización parcial con intervención mínima del analista.

3 pts : El sistema ejecuta de forma exitosa Playbooks tipo básico: flujo lineal simple (alerta → acción), con integración limitada (mínimo 1 sistema), sin lógica condicional avanzada y con alta dependencia de intervención humana.

El oferente deberá demostrar que la plataforma incorpora capacidades avanzadas de Inteligencia Artificial (IA) para la generación automática de playbooks de respuesta, permitiendo asistir al analista en la toma de decisiones.

Métricas de Evaluación
5 pts: La IA genera automáticamente playbooks completos y contextualizados a partir del incidente, incorporando acciones multi-dominio (por ejemplo endpoint, red, identidad, etc), priorización basada en riesgo y posibilidad de ejecución directa, con aprendizaje continuo basado en eventos históricos.

3 pts: La IA sugiere playbooks genéricos basados en categorías de alertas, sin personalización avanzada ni aprendizaje contextual.

4. INTELIGENCIA ARTIFICIAL

El oferente debe demostrar la integración de un asistente de IA capaz de interpretar la telemetría compleja del incidente y traducirla a un lenguaje natural, proporcionando resúmenes ejecutivos y explicaciones técnicas detalladas de forma automática.

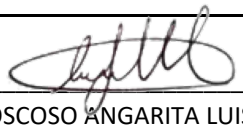
5 pts. La IA genera automáticamente un resumen que incluye: Vector de ataque, activos afectados, acciones realizadas por el malware y nivel de riesgo. El resumen es coherente, no omite datos técnicos críticos y se actualiza a medida que entra nueva evidencia.

3 pts La IA genera un resumen claro de los eventos principales, pero omite detalles sobre el vector inicial o requiere que el analista solicite el resumen manualmente mediante un comando.

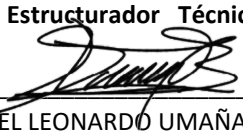
El oferente debe demostrar la capacidad de generar un informe consolidado en formato PDF que resuma la postura de seguridad del último mes y configurar una tarea programada para su envío automático por correo electrónico.

5 pts : El reporte PDF incluye Volumen de incidentes por severidad, MTTR (Tiempo de respuesta), activos más atacados, estado de cumplimiento de normativas y un resumen ejecutivo generado por IA. El diseño es profesional e incluye gráficas comparativas con el mes anterior.

3 pts : El reporte es una lista detallada de alertas y eventos ocurridos, sin una estructura de resumen ejecutivo o indicadores de alto nivel.



T1 MOSCOSO ANGARITA LUIS FELIPE
Estructurador Técnico



CT DANIEL LEONARDO UMAÑA BAUTISTA
GERENTE DEL PROYECTO