PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DEL SUMINISTRO, EN MODALIDAD DE SUSCRIPCIÓN CON SERVICIOS GESTIONADOS, DE UNA HERRAMIENTA BAS DENTRO DEL ENTORNO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA TI DE LA SOCIEDAD MERCANTIL CORPORACIÓ CATALANA DE MITJANS AUDIOVISUALS, SA

EXPEDIENTE N.º 2303OB02

1. SITUACIÓN ACTUAL DE LA CCMA, SA EN EL ENTORNO DE CIBERSEGURIDAD

Actualmente la CCMA, SA y sus empresas filiales están implantando de forma progresiva acciones, herramientas y servicios para reforzar todo el entorno relacionado con la ciberseguridad.

En el marco de tales acciones se quiere implantar una herramienta que ayude a identificar vulnerabilidades en la infraestructura TI de la CCMA, SA, en vectores tanto internos como externos, además de recibir información práctica para reforzar la seguridad.

Analizando estudios de Gartner se ha visto que ha creado un nuevo dominio dentro de la Seguridad denominado «Breach & Attack Simulation (BAS)» que justifica su adopción por las Organizaciones:

«La principal ventaja que proporcionan las plataformas BAS es su habilidad para el testeo continuo, la capacidad de identificar gaps de seguridad y la validación de las mitigaciones llevadas a cabo».

La CCMA, SA, como la mayoría de grandes organizaciones, necesita verificar su nivel de seguridad en sus infraestructuras TI, generando «simulaciones» de ataques, bajo demanda y contra sí misma, utilizando la tecnología de plataformas BAS, proporcionando de inmediato vulnerabilidades y procedimientos de mitigación para cerrar cada brecha. Este nuevo enfoque permitirá a la CCMA, SA conocer en cada momento y de forma inmediata el estado de su nivel de seguridad.

2. DESCRIPCIÓN DE LA OFERTA

Se requieren los **servicios gestionados de una herramienta BAS que permita la generación de ciberataques en tres vectores (endpoint, lateral movement y threat inmediate)** que permita simular vulnerabilidades y ataques cibernéticos actuales, que identifique las vulnerabilidades y facilite ayudas prácticas para corregir las vulnerabilidades detectadas en la infraestructura de la CCMA, SA.

La herramienta **debe basarse en una plataforma cloud con servicios gestionados**.

3. REQUISITOS TÉCNICOS OBLIGATORIOS

Características principales de la herramienta

- Debe ser una solución única que cubra la totalidad de los vectores de ataque siguientes:

- E-mail
- Web
- WAF
- Endpoint
- Phishing
- DLP
- Lateral Movement
- Reconocimiento
- Inteligencia
- Full Kill-Chain APT

Los ataques deben estar totalmente automatizados y diversificados para permitir que se efectúen pruebas de seguridad completas en cualquier momento, lo que proporcionará una mejor comprensión de su posición en seguridad y permitirá mejorar esta última continuamente, eliminando los falsos positivos que surjan.

- **Atomic Executions de Mitre att & ck + Execucions Multipath**, permitiendo la adecuación a un Red Team
- Plataforma 100 % segura, sin posibilidad de causar daño real a la infraestructura.
- **Las muestras reales de malware, actualizadas a diario e incluyendo gran cantidad de ataques.**
- **Ejecución de escenarios multivector.** Las pruebas de malware son simulaciones basadas en varios payloads y flujos de acción, como hacen los atacantes
- **Permitir la utilización de ataques «personalizados».**
- Equipo de inteligencia dedicado, actualizando la base de datos de ataques de forma casi diaria.

Características del despliegue y la puesta en marcha

La herramienta debe ofrecer sus servicios en formato completo SaaS. No se aceptarán propuestas que conlleven la instalación de appliances, consolas, servidores o grandes cambios en la configuración. El servicio no puede tener gran impacto en la infraestructura TI existente.

Servicio de despliegue rápido, con actualizaciones automáticas y transparentes. Asimismo, no se requiere instalación de agentes en todas las máquinas de la infraestructura TI objeto de análisis.

Soporte de Windows, MacOS y Linux.

Fácil uso de la Plataforma desde la Nube.

API completa disponible.

Características de las integraciones

- Única herramienta Breach and Attack Simulation (BAS) integrable con sistemas de EDR, SOAR, Siems, escáneres de vulnerabilidades y herramientas de ticketing.
- API completa disponible

Certificaciones de fabricante e integrador

- Disponer de certificaciones como las siguientes:
  - ISO27001
  - LEET SERVICIOS SEGURIDAD GESTIONADA MSSP
  - LEET CENTRO OPERACIONES DE SEGURIDAD (SOC)

  - LEET SEGURIDAD BASADA EN LA NUBE
  - ESQUEMA NACIONAL DE SEGURIDAD (ENS)

- El integrador debe disponer de otras referencias en las que tenga instalada o gestionada la herramienta.

Servicio gestionado

Se requieren los servicios siguientes:

- despliegue y configuración inicial de la herramienta
- configuración inicial del o de los agentes y configuraciones básicas de perfilado de los usuarios que accederán a la herramienta y la configuración deseada de los módulos
- monitorización de la operatividad del Servicio
- ejecución continua programada de los módulos contratados:
  - EndPoint, una vez al mes
  - Threat inmediate de forma «continua»
- elaboración de informes mensuales con lo detectado, indicando las correcciones que deban introducirse
- seguimiento de correcciones
- generación de informes mensuales de lo detectado, qué se ha corregido, con tendencias incluyendo métricas
- atención a incidencias 7x24, con respuesta dentro del horario laboral 8x5

Requisitos mínimos de la herramienta

Se considera requisito obligatorio de la herramienta cumplir un mínimo de 92 de las casuísticas expuestas en el **Anexo 3**.

Los licitadores que no cumplan esta condición quedarán excluidos del procedimiento.

4. ACUERDO DE NIVEL DE SERVICIO (ANS)

Atendiendo al nivel de criticidad:

Gravedad del incidente.	Condiciones para definir la gravedad
Muy grave	• Impacto importante en muchos sistemas/servicios. • Datos confidenciales y financieros en riesgo con responsabilidad legal para la CCMA. • Impacto en el sistema o servicio crítico de la empresa • Riesgo elevado de propagación
Grave	• Impacto importante en una cantidad moderada de sistemas/servicios. • Impactos en sistemas y servicios empresariales no críticos en riesgo. • Riesgo razonable de propagación.
Medio	• Amenaza de riesgo de nivel alto que no conlleva impacto para los activos en el momento de la detección. • Riesgo menor de propagación.
Bajo	• Recomendaciones de políticas de seguridad basadas en la experiencia del proveedor.

	• Errores menores en funciones que no afecten la producción.
Falso positivo	• Un acontecimiento o actividad sospechosa que, una vez investigado, no supone ninguna amenaza.

Se proponen los plazos siguientes para la notificación de las incidencias (siempre con un nivel de apoyo de 24x7). Se considera incumplimiento que se notifique en los plazos marcados como tales en la tabla,

Nivel de incidencia	Tiempo de respuesta	Nivel de incumplimiento
NIVEL 1 Crítico	< 1 hora	99 %
NIVEL 2 Alto	< 4 horas	99 %
NIVEL 3 Mediano/Bajo	< 8 horas	90%

Penalizaciones por incumplimiento del ANS

En caso de incumplimientos reiterados en el tiempo de respuesta ante incidencias por causas ajenas a la CCMA, SA, se podrá aplicar una penalización de rebaja con respecto al precio ofertado para la partida servicios gestionados. La rebaja corresponderá a un porcentaje por cada número de incumplimientos que se den según el criterio siguiente:

NÚMERO DE INCUMPLIMIENTOS	% DE PENALIZACIÓN
10 incumplimientos	0,1 % sobre el importe total ofrecido por precio servicio gestionado
20 incumplimientos	0,2 % sobre el importe total ofrecido por precio servicio gestionado

Sant Joan Despí, febrero de 2023