Servicio soporte externo de monitorización y gestión experta de alertas de ciberseguridad.

Unidad: Seguridad TIC
Área: Operació de Tecnologia de Sistemes
Fecha: 16 de Julio de 2021

CPV 50324100 Servicios de mantenimiento de sistemas

Expediente número: 15011226

Transports
Metropolitans
de Barcelona

Índice

1. Contratación de un Servicio soporte externo de monitorización y gestión experta de alertas de ciberseguridad

1.1 Introducción

La ciberseguridad se ha convertido en un elemento clave para garantizar la disponibilidad e integridad de los sistemas tecnológicos de TMB. Se requieren perfiles tecnológicos altamente especializados con un conocimiento muy específico en el ámbito de la ciberseguridad y constantemente actualizado.

El Área de Tecnología de TMB, concretamente Operaciones de Tecnología, tiene la responsabilidad de definir, implantar y controlar la seguridad lógica en todos los entornos IT y la física en cuanto a las dependencias de los CPD donde se encuentran los equipos IT.

Dentro de esta responsabilidad se incluye el seguimiento de los eventos de ciberseguridad para detectar posibles ataques, vulnerabilidades de los sistemas y actuar, tanto de manera proactiva como reactiva, de una manera eficaz y eficiente.

También se encuentra dentro de su responsabilidad la mejora de la Gestión de la Información y Eventos de Seguridad (SIEM), por lo que se realiza una mejora continua del sistema.

1.2 Objeto

El objeto de este documento es la solicitud de un Servicio soporte externo de monitorización y gestión experta de alertas de ciberseguridad en ámbito IT/OT que nos ayude en la vigilancia de la Ciberseguridad de TMB, actuando de manera diligente en caso de detectar cualquier ataque y a mejorar el SIEM de TMB para conseguir agilizar la detección de ataques y funcionamientos anómalos.

2. Objeto de solicitud

2.1 Servicio de Operaciones de Seguridad.

Las tareas a realizar se llevarán a cabo mediante una VPN Site-to-Site utilizando el SIEM de TMB (Splunk). Será TMB el encargado de adquisición de licencias del producto que sustenta el SIEM (Splunk).

El Servicio englobará los ámbitos IT y OT, se realizará 24x7 y contemplará:

a) Servicio de Monitorización de Seguridad (SIEM)
b) Operación EDR
c) Vigilancia Digital
d) Coordinador Project Manager
e) Equipo de Respuesta ante Incidencias de Seguridad Informáticas - CSIRT (Computer Security Incident Response Team)

Todo lo que se desarrolle o documente dentro del servicio será propiedad de TMB.

a) Servicio de Monitorización de Seguridad (SIEM)

Tiene como principal objetivo la detección de amenazas de seguridad detectadas en el SIEM (Splunk de TMB), pero también incluye la puesta a punto y mejora continua de los paneles de la plataforma Splunk actual para mejorar la detección, alertas y fuentes de datos.
Servicio 24x7 con el soporte de un analista con una valoración de dedicación de un FTE (Full Time Equivalent) de 0,5/dia.

La lista mínima de tareas que deben ofertarse es:

- Monitorización y gestión de alertas generadas por el SIEM en 24x7.
- Las alertas serán registradas en una plataforma de ticketing de seguridad (que permita realizar el seguimiento) y gestionado en base a playbooks predefinidos con anterioridad.
- Posibilidad de integración con herramienta de ticketing de TMB.
- En caso de alertas críticas/relevantes se avisará a los responsables de TMB.
- Definición de SLAs para el tratamiento de las alertas/incidencias/peticiones
- Se atendrán todas las alertas críticas, y todas las no críticas, según SLAs acordados con TMB.
- Creación de casos de uso (IT y OT) que se consideren necesarios, tanto por parte del proveedor y su experiencia en el servicio (adaptando su catálogo estándar de casos de uso) como por parte de TMB que desee implementar casos de uso concretos por sus necesidades.
- Dentro del tiempo (FTE) asignado para este servicio de Monitorización, habrá una parte dedicada a la creación de casos de uso, que se realizará de forma continua. El proveedor deberá de realizar el máximo número de casos de uso posibles para la optimización del servicio.
- Gestión de las alertas del SIEM en 24x7 por parte de N1 (procedimientos de primera respuesta y clasificación) y escalado a nivel 2 para realizar investigación/resolución de tareas más complejas mínimo en 8x5 (siempre que no sean críticas que deberían ser 24x7).

- Elaboración y mantenimiento de los playbooks asociados a todos los casos de uso que se vayan definiendo.
- Propuestas de automatización para cada caso de uso.
- Elaboración y mantenimiento de las matrices de escalado necesarias para la gestión de alertas.
- Gestión de las peticiones sobre actividades en el sistema de ticketing.
- Carga del Threat intelligence de IOCs, para la detección de campañas de malware correlación con los datos de las fuentes disponibles dentro del SIEM.
- Análisis de muestras de malware asociados a alertas mediante una Sandbox para conocer su comportamiento y la extracción de IOCs (índices de compromiso) asociados para su aplicación en la Infraestructura. (24x7)

- Inclusión de fuentes de datos OT

  Integración de datos de OT de la parte de Bus, mediante la plataforma *Wonderware*® de donde se deberán de configurar la extracción de datos para indexarlos en Splunk y preparar los paneles y alertas para poder realizar la monitorización de OT dentro del mismo servicio.

  Integración de datos de OT de parte de Metro, posiblemente mediante la plataforma *Claroty*® Continuous Threat Detection (CTD), aunque podría tratarse de otra, con el mismo objetivo de incorporar al Servicio.

  En ambos casos se deberá de acordar qué información relevante se pretende monitorizar y realizar el servicio incorporando los casos de uso OT que se crea conveniente.

  Estos casos de uso, se realizarán mediante consumo de tiempo del servicio de Monitorización.

b) Operación EDR

Gestión de la plataforma Antimalware de TMB (actualmente McAfee) para realizar contenciones e investigaciones en caso de incidentes.

- Ajuste de políticas para poder mitigar amenazas.
- Posibilidad de contención de amenazas mediante la herramienta de EDR.
- Ejecución de tareas de análisis bajo demanda ante amenazas detectadas o de forma preventiva.
- Aplicación de los IOCs (índices de compromiso) propios de la plataforma de McAfee para prevenir posibles afectaciones.

Queda excluido de este ámbito la administración de la plataforma que ya proporciona TMB a nivel de actualización de versiones de los productos y despliegue a los clientes.

c) Coordinador Project Manager:

Project Manager que lleve todo el Servicio contratado de SOC para ver qué puntos hay que resolver, que conozca la evolución de los eventos, los casos de uso actuales y tenga la previsión de los prioritarios a añadir, gestiones la incorporación de nuevos casos de uso necesarios o de solicitudes concretas.
Valoración del servicio del coordinador con un FTE de 0,5/dia.

- Seguimiento del día a días del contrato, evaluación del servicio prestado, y seguimiento del consumo de jornadas del contrato, reportando su uso a TMB.
- Revisión de las principales incidencias y cumplimiento de los SLAs

- Informe mensual de la prestación del servicio, con las actividades ejecutadas, acciones planificadas, puntos bloqueantes o que requieran atención, así como un resumen de las incidencias gestionadas, volumetrías asociadas al servicios y próximos pasos y propuestas de mejora de servicio.
- Informes de incidentes, a petición de cliente, sobre un incidente con afectación que haya podido producirse.
- Generación y puesta en marcha de casos de uso de librería, en base a las tecnologías presentes en el SIEM.
- Puesta en marcha dentro de la mejora continua, de nuevos casos de uso (desde la recogida de fuentes de datos, creación Panales y alertas, tratamiento y sus Playbooks asociados).
- Revisión, mantenimiento e integración de fuentes de logs, revisión e indexación de las fuentes en el SIEM.
- Despliegue de nuevas piezas dentro de la infraestructura de Splunk.
- Monitorización de las fuentes, detección de fuentes que no reportan, picos y valles.
- Gestión de peticiones de cambios en SIEM (usuarios, perfiles, índices, etc)
- Reducción de falsos positivos. Identificación de eventos que no provocan una acción a realizar para minimizar/eliminar de los cuadros de mando. Proponer cambios en las configuraciones de las plataformas de TMB.
- TMB dispone de cuadros de mando de gestión de las distintas fuentes, pero se deberán proponer y crear los cuadros de mando necesarios (dentro del Splunk de TMB) para el seguimiento de eventos de todos los casos de uso.
- Reuniones trimestrales con TMB a nivel estratégico, táctico y operacional, para analizar cómo se está dando el servicio.

d) Vigilancia Digital

Aplicable como mínimo para las marcas de TMB: “Transports Metropolitans de Barcelona”, “Ferrocarrils Metropolitans de Barcelona”, “Transports de Barcelona”, “Projectes i Serveis de Mobilitat”/“Barcelona Bus Turistic”, “Fundació TMB” y “Transports Metropolitans de Barcelona, SL”.

Este servicio debe cubrir diferentes aspectos:

- Reputación de marca: Inteligencia y protección contra el fraude relacionado con el uso ilegítimo de las marcas de la organización de TMB. P.e. páginas web de Phishing, perfiles falsos, ofertas de trabajo falsas, aplicaciones móviles falsas, dominios sospechosos, etc.
- Hacktivismo: Operaciones o información relacionada con TMB, activos en listas negras, campañas dirigidas de malware, presencia en Deep Web, etc.
- Contenido confidencial: listas de usuarios y credenciales, documentos confidenciales, etc.
- Servicio de Takedown : solicitud para eliminar contenido malicioso, fraudulento o dominios que abusan de la marca de una empresa
- 10 jornadas de analista de Seguridad para búsquedas en Dark Web u otras peticiones relacionadas en el ámbito de Vigilancia digital a petición de TMB.

e) Equipo de Respuesta ante Incidencias de Seguridad Informáticas - CSIRT (Computer Security Incident Response Team)

Se contemplan 90 jornadas de especialistas para todo el periodo de vigencia del contrato, para gestión de incidentes de impacto, investigación, Threat Hunting, u otras tareas especializadas a petición de TMB.
La metodología requerida deberá ser la aprobada por el CCN-CERT, de acuerdo con el Esquema Nacional de Seguretat (ENS) y que está referenciada en las guías CCN-STIC-403 y CCN-STIC-817.

Se establecerá como SLA para las incidencias los siguientes tiempos de respuesta:

- Incidencia Crítica → 1h
- Incidencia Media → 4h
- Incidencia Baja → 8h

La definición de criticidad de los incidentes será:
- **Criticidad alta**: Incidentes que tienen un impacto considerable (afectación a la confidencialidad, disponibilidad y la integridad) a información considerada crítica para la actividad de TMB y/o sistemas TIC críticos. El incidente con capacidad de afectación a gran cantidad de información valiosa y causar la degradación de servicios vitales de TMB.
Estos incidentes pueden ser típicamente, malware destructivo, denegación de servicios, compromiso de sistemas, incidentes de hacking y violaciones de políticas que afecten a sistemas críticos o información crítica per TMB.
- **Criticidad media**: Incidentes que afectan a sistemas o información no crítica para TMB, o su impacto no repercuta directamente en servicios vitales de negocio.
Estos incidentes pueden ser típicamente, incidentes de hacking, phishing, algunas violaciones de políticas, entre otros.
- **Criticidad baja**: incidentes de seguridad en sistemas no críticos para TMB.

Este servicio debe cubrir como mínimo:

- Posible activación desde el servicio de Monitorización del SIEM y/o de la operación EDR, así como bajo petición de TMB.
- Capacidades de investigación y análisis forense.
    - Evaluación inicial y de evidencias preliminares.
    - Extracción y recolección de evidencias sobre sistemas comprometidos
    - Contextualizar la amenaza, evaluar el nivel de compromiso, posibles movimientos laterales, escalada de privilegios, etc.
- Respuesta y remediación
    - Coordinación durante el incidente con el equipo de Seguretat TIC de TMB.
    - Soporte sobre la ejecución de la contención para minimizar el impacto.
    - Soporte en la erradicación, recuperación del servicio
    - Monitorización y control post incidente
- Análisis de malware
    - Identificar el comportamiento de los artefactos
    - Identificar los IOCs aplicables a la infraestructura de seguridad de TMB para detección y bloqueo posteriores
    - Identificar sus mecanismos de propagación
- Informes técnicos del incidente
    - Informe de detalle de toda la investigación de gestión del incidente y del posible análisis del malware

- Lecciones aprendidas y propuestas de mejora

2.2 Reportes

Los reportes que se han de presentar son:

- Informe mensual de prestación del servicio, con las actividades ejecutadas, acciones planificadas, puntos bloqueantes o que requieran atención, así como un resumen de las incidencias gestionadas, volumetrías asociadas al servicios y próximos pasos y propuestas de mejora de servicio.
- Informes de incidentes, a petición de cliente, sobre un incidente con afectación que haya podido producirse.
- Notificaciones de alertas enviadas que funcionan como elementos de seguimiento de situaciones excepcionales que se estén tratando como consecuencia de un incidente de seguridad.
- Posibles riesgos detectados con la Cibervigilancia, así como propuestas de acciones preventivas.

2.3 Cuadro de mandos

Se generarán todos los cuadros de mandos que se requieran para realizar todo el seguimiento del SOC y el Estado de la Ciberseguridad en TMB, dentro de la plataforma Splunk de TMB.

Acordar el contenido de los cuadros de mando facilitando la siguiente lista a modo de ejemplo:

- **Estado general de la Ciberseguridad**
    - Filtros por tiempo, estado, tipo de ticket y prioridad
    - Mapa interactivo de geolocalización de IPs públicas correspondientes a ataques
    - Categoría de tickets, subcategoría de tickets, prioridad de tickets
    - Tipo de ataque detectado y Tabla detallada de todos los tickets.
- **SLAs**
    - Tiempo medio de vida de notificación de un incidente de seguridad
    - Número de tickets medidos para el cálculo del SLA
    - Porcentaje de cumplimiento
    - Evolución del cumplimiento de SLA de los tickets en el tiempo
    - Número de tickets que incumplen de criticidad baja y % del total
- **Volumen**
    - Filtros por tiempo, estado, tipo de ticket y prioridad
    - Distribución de tipo de tickets en el periodo
    - Número de incidentes gestionados
    - Día de máximo número de incidentes gestionados y cantidad
    - Número de peticiones gestionadas
    - Mapa de calor de atención de tickets
- **Productividad**
    - Filtros por tiempo, estado, tipo de ticket y prioridad
    - Distribución de todos los tickets gestionados en el tiempo según su tipología
    - Número de incidentes de seguridad gestionados
    - Número de incidentes de seguridad con impacto gestionados
    - Tipología de todos los tickets gestionados

En el caso de los indicadores de tickets se realizarán en colaboración con técnicos de TMB para facilitar el acceso a la información y el detalle de los campos de la Base de Datos.

2.4 Puesta en marcha, operación y entrega final

Puesta en marcha

Para poder realizar la operación, antes se requerirá un proceso de puesta en marcha del servicio donde por parte de TMB se deberá de hacer el traspaso de conocimiento del contenido del Splunk a nivel de fuentes y paneles actuales, así como documentación, acceso al SIEM desde el exterior, etc.
Toda esta fase no debería llevar más de 4 semanas.

Funcionamiento del servicio

En la siguiente fase, detallar las acciones a tomar para arrancar la monitorización, establecer si ya existen paneles que puedan cubrir casos de uso que entraran en el servicio de monitorización para su seguimiento, documentación, etc., y empezar con la labor de mejora continua donde se irán identificando y añadiendo constantemente nuevos casos de uso que se convertirán en paneles, definición de alertas, playbooks, etc. y todo lo demás que conlleva el servicio, hasta llegar a un punto donde se estabilice un nivel de seguimiento que se considere óptimo. A partir de ahí quedarían los puntos de mejora y propuestas o solicitudes nuevas.

Fin del servicio y retorno

Finalmente se debe contemplar una entrega final del SOC una vez finalizado el contrato donde se realizará el traspaso a TMB del funcionamiento del SIEM, así como de toda la documentación generada y playbooks, y desarrollos en el Splunk. Definir un plan de traspaso que garantice la correcta transmisión de conocimiento y documentación a TMB.
Esta fase de retorno del conocimiento será entre 4 y 6 semanas.

3. Características generales

3.1 Solvencia técnica del adjudicatario

El adjudicatario deberá disponer de personal para la monitorización del SIEM, atención del nivel 1 de actuación frente a incidentes y soporte experto de nivel 2.

El licitador debe contar con las siguientes certificaciones:

- Sistema de gestión de la seguridad de la información ISO 27000
- Sistema de gestión de la continuidad del negocio ISO 22301
- Certificación de conformidad con el Esquema Nacional de Seguridad (ENS) o LEET SECURITY mínimo Rating BBB
- FIRST "For Inspiration and Recognition of Science and Technology"
- CSIRT Computer Security Incident Response Team

3.2 Confidencialidad

La empresa colaboradora debe aceptar el compromiso de confidencialidad respecto a los datos a los que tendrá acceso y que son propiedad de TMB, para ello se firmará un acuerdo de confidencialidad.

Los permisos de acceso a los sistemas y aplicación, en caso de ser necesario, tendrán el nivel necesario para el trabajo a realizar y asignados a un responsable de seguridad de la empresa adjudicataria.

En caso de precisar del acceso con un usuario con privilegios elevados en el sistema se llevará a cabo a través de la herramienta que dispone TMB para este fin, de manera que queden trazadas las acciones que se realicen.

3.3 Aspectos funcionales

La prestación del servicio objeto de esta contratación debe cumplir con los siguientes ítems:

a. La realización se efectuará en remoto, aunque puede haber alguna tarea que requiera de acceso presencial.

b. La realización de las tareas presenciales, de no indicar otra cosa, se realizarán en la oficina situada en la siguiente dirección:

Centre de Suport Tecnològic
C/Josep Estivill, 47
08027, Barcelona

3.4 Contacto

El contacto con TMB para resolver cualquier duda es:

- Nombre: Ernest Costa Lluch
- Correo: ecosta@tmb.cat
- Teléfono: 932 987 198