ANUNCIO PARA LA CONTRATACIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD

Fecha de publicación: 18 de julio de 2024.

Objeto del contrato:

Dentro del proceso de implantación del ENS, SAECA se necesita contratar un Centro de Operaciones de Seguridad (Security Operations Center, SOC). El objeto de este anuncio es la contratación de un proyecto de implantación y servicio SOC, siguiendo las directrices contempladas en el Plan de Recuperación, Transformación y Resiliencia y en el CCN-CERT que permitirá garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por SAECA, así como mejorar las apacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

EL Centro de Operaciones de Seguridad será el sistema encargado de realizar un seguimiento y analizar la actividad en firewall, redes, servidores, y otros sistemas buscando actividades anómalas que puedan ser indicativas de una amenaza de seguridad, de modo que dicha información sea recogida para aplicar medidas correctivas e informar a la Plataforma Nacional de Notificación y Seguimiento de Ciber Incidentes.

La herramienta básica del Centro de Operaciones de Ciberseguridad será el SIEM (Sistema de Administración de Información y Eventos de Seguridad) que permitirá:

- Centralizar y custodiar información, es decir eventos, sobre el funcionamiento de los sistemas de información, infraestructuras tecnológicas y de comunicaciones.
- Alertar en tiempo real ante anomalías y ataques informáticos a SAECA.
- Investigar los sucesos ocurridos para poder responder y defenderse ante los ciberataques, con el objetivo de proteger los sistemas de información de SAECA

Este proyecto complementará y reforzará el proyecto de adecuación y certificación de conformidad con el ENS de los sistemas de información de SAECA.

El SOC que se despliegue en el ámbito del presente anuncio formará parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

Condiciones del servicio

Descripción del proyecto

SAECA debe hacer frente al creciente volumen y sofisticación de las amenazas que se producen en el mundo actual. La falta de visibilidad de la red, el volumen de datos a analizar de los servicios ya implantados y la necesidad de filtrado y sobre todo la rápida respuesta en forma de alertas lleva consigo que ya no es posible hacer este análisis en forma manual. Por ello, surge la

necesidad de automatizar los procesos y centralizar la gestión de seguridad de una forma que ayude a simplificar la difícil tarea de proteger la información que se maneja y el servicio que se presta.

Con la implantación de un sistema de gestión de eventos e información de seguridad se obtiene la recopilación de la información en tiempo real sobre los eventos de seguridad generados por la red para procesarla posteriormente con el fin de generar informes y/o alertas que puedan ayudar en la toma de decisiones en materia de seguridad.

Este sistema de gestión y correlación de eventos se concibe como una plataforma de gestión de seguridad lógica de la red y se enfoca principalmente en los siguientes aspectos:

- Inventario y catalogación de activos.
- Gestión centralizada de los registros y eventos de seguridad generados por los sistemas.
- Análisis y monitorización en tiempo real de los eventos de seguridad de múltiples fuentes.
- Revisión manual (humana) de los positivos detectados para una mayor criba y eliminación de falsos positivos y notificación de la alerta, cuando proceda.
- Colaboración y asesoramiento técnico en la resolución de la incidencia derivada de la alerta

Además, se desea detectar los patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos. Para ello se implantarán sondas en la red de la entidad para recolectar la información de seguridad relevante y, después de un primer filtrado, enviar los eventos de seguridad hacia el sistema central que realiza una correlación entre los distintos elementos.

Los principales objetivos del sistema de gestión de eventos son los siguientes:

- Disponer de un método efectivo para automatizar los procesos y centralizar la gestión de seguridad de una forma que ayude a simplificar la protección de la información que se maneja y el servicio que se presta.
- Identificar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos, generando alertas según corresponda.

<u>Elementos del servicio</u>

Se detallan a continuación los elementos a incluir en el servicio SOC:

- ✓ Firewall de Seguridad Perimetral Sophos SFV2C4 (SFOS 19.5.3
- ✓ 80 Endpoint con proteccion Sophos InterceptX
- ✓ 20 dispositivos móviles con Sophos Mobile - Central Mobile Advanced
- ✓ Sonda NDR para analizar tráfico de red
- ✓ 9 Servidores
- ✓ 2 cabinas de almacenamiento
- ✓ Servicio Ciber Threat Intelligence (Inteligencia de amenazas)
- ✓ Solución MFA Ironchip

Red Nacional de Centros de Operaciones de Seguridad

El Centro de Operaciones de Ciberseguridad que se despliegue en el ámbito del presente proyecto que se anuncia, debe formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad.

La coordinación de los centros integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, prevista en el artículo 11 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Centro de operaciones de ciberseguridad- SOC

Se establecerá un servicio de vigilancia proactiva 24x7x365, desde un Centro de Operaciones de Seguridad (SOC) ubicado en la Unión Europea y con soporte en castellano, con capacidad para recibir, correlacionar y gestionar eventos de seguridad en tiempo real, y que actúe en casos de ser preciso el soporte o como respuesta a un incidente de seguridad.

Este servicio permitirá que todos los dispositivos de seguridad incluidos en este anuncio sean monitorizados y gestionados por personal experto en ciberseguridad, independientemente de su ubicación, ya estén en sus dependencias (CPD) de SAECA, en un proveedor o en la cloud privada/pública. Dentro del servicio se englobarán entre otras las siguientes funciones:

- Mantenimiento y soporte de los sistemas instalados.
- Servicio de monitorización y vigilancia 24x7 de la seguridad de los dispositivos incluidos en el servicio, que permite reducir los riesgos de seguridad y acelerar la respuesta ante incidentes. Esta función está orientada a la prevención y mitigación de amenazas que pueden afectar a la seguridad de la organización.
- Seguridad Gestionada: externalizar la gestión de la seguridad de los elementos dentro del alcance del contrato.
- Correlación de eventos de seguridad: Security Information Event Management (SIEM), que sea capaz de identificar incidencias de seguridad, análisis y correlación de los logs de seguridad.
- Respuesta y análisis forense ante eventos de seguridad: se prestará un servicio 24x7x365 de mantenimiento y asistencia técnica
- Servicio de soporte ofrecido 24x7x365 por teléfono, correo electrónico y sistema de tickets, en castellano.
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, informes de ciberseguridad.
- Soporte técnico vía email o teléfono 24x7x365
- Acceso ilimitado al Helpdesk: sin límite de incidencias. Las fuentes de información que se consideran relevantes a priori incluir en el servicio serán las siguientes:

  • Logs y eventos de los controladores de dominio y otros servidores relevantes

  • Logs y eventos de los diferentes servidores de aplicaciones

  • Logs y eventos de los firewalls

  • Logs y eventos de los motores antivirus EDR

- Logs y eventos de la solución MFA de Ironchip
- Sondas de red en diferentes segmentos

Administración de eventos de información de seguridad- SIEM

La capacidad de recolección y correlación de los registros de trazabilidad (logs) necesarios para la vigilancia por parte del SOC deberá realizarse mediante productos recogidos en el catálogo CCN-STIC 105. En concreto, la solución SIEM deberá estar recogida en dicho catálogo, o haber iniciado los trámites necesarios para su inclusión habiendo superado la fase de revisión de propuesta de declaración de seguridad por parte del CCN (debe adjuntarse certificado al efecto)

El SIEM recogerá en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques sino, en la medida de lo posible, adelantarse a ellos para remediarlos antes de que sucedan.

La plataforma se alimentará igualmente de fuentes externas de vigilancia y alerta temprana, de forma que esté preparada para proteger las vulnerabilidades registradas en la Red Nacional de Centros de Operaciones de Seguridad.

La empresa adjudicataria propondrá los diferentes escenarios o caso de uso de los eventos recolectados en el SIEM, así como su posterior tratamiento.

Todas las alertas generadas por el motor SIEM deberán ser revisadas por un técnico de seguridad de la empresa adjudicataria, como paso previo a su envío a SAECA. Este método de trabajo deberá permitir con un importante nivel de acierto, la eliminación de falsos positivos en la identificación de incidentes.

Toda la información recolectada junto a las posibles alertas generadas y el estado de salud global del sistema, así como el de cada uno de los elementos, deberá ser accesible mediante una consola centralizada que permita una gestión ágil.

Sonda de red NDR

A fin de poder correlar los eventos provenientes de los endpoints y servidores con el tráfico de red, con la funcionalidad XDR, será necesario que el adjudicatario instale una sonda de red con capacidades NTSA/NDR. Este elemento se instalará en las oficinas centrales y, de modo pasivo, debe ser capaz de detectar todo tipo de ataques, tanto verticales como horizontales:

- Tráfico SPAM.
- Escaneos.
- Spiders.
- Intentos de distribución de malware.
- Ransomware.
- Conexiones con Red TOR.
- Conexiones con proxys.
- Conexiones a sitios de baja reputación.
- Conexiones con dominios nuevos o de baja reputación.
- Peticiones ilegales a DNS.

- Exploraciones masivas.
- Atacantes anónimos.

Además, sus funcionalidades de NDR deben permitir alertar a SAECA en caso de un uso sospechoso o peligroso de la red (por ejemplo, movimiento de grandes volúmenes de ficheros, fallos en la conexión al dominio, usuarios con elevado nivel de riesgo, detección de eventos como apertura masiva de ficheros, ransomware, malware, comportamiento de usuarios amenazas conocidas etc).

El adjudicatario debe indicar las características de la sonda y el modelo de licenciamiento y explotación (adquisición, alquiler ,…)

Servicio de Cybersecurity Threat Intelligence

Adicionalmente, para una mejor capacidad de detección de posibles incidentes, el SOC deberá incluir una solución para la protección contra posibles amenazas que al menos incluya:

- Protección del dominio
- Cuentas y contraseñas filtradas
- Malware
- Exfiltración de datos

Plan de instalación

El licitador presentará en su documentación técnica un plan de instalación. Una vez formalizado el contrato, y en el plazo máximo de siete (7) días naturales, se elaborará y revisará el plan de trabajo propuesto y se elaborará el plan de trabajo definitivo.

Este plan de trabajo deberá mantenerse actualizado y consensuado entre el SAECA y la empresa adjudicataria.

Este plan de instalación deberá llevarse a cabo en un plazo máximo de30 días naturales desde el siguiente a la firma del contrato.

Metodología y gestión del servicio

Se formará un Comité para la dirección del proyecto, que estará compuesto al menos por la persona Responsable del Contrato designada por SAECA, una representante de la adjudicataria y cuantas otras personas designen las partes.

La misión de la persona responsable del contrato será la siguiente:

a) Supervisar la ejecución del contrato.

b) Asegurar la correcta realización de la prestación pactada, dictando las instrucciones y adoptando las decisiones necesarias para ello dentro de las facultades otorgadas por el órgano de contratación.

c) En su caso, informar de los retrasos en la ejecución del contrato y realizar la propuesta para la aplicación de penalidades por incumplimiento parcial, cumplimiento defectuoso y demora en la ejecución.

Asimismo, SAECA designará una Dirección/Jefatura de Proyecto que tendrá entre sus funciones la planificación, seguimiento y control de los trabajos a realizar, así como la interlocución para la coordinación de los recursos humanos y disponibilidad de recursos materiales del mismo que sean necesarios en cada momento.

SAECA, mediante la figura mencionada, vigilará por el cumplimiento de los términos acordados, así como la calidad y adecuación del servicio objeto de este expediente.

Sus funciones serán las siguientes:

- Autorizar los contactos directos de las personas del equipo de trabajo de la adjudicataria con personas de SAECA

- Autorizar la entrega de documentación al Equipo de Trabajo de la adjudicataria.

- Autorizar el cambio de personas en el Equipo de Trabajo de la adjudicataria.

- Solicitar el cambio de personas del Equipo de Trabajo de la adjudicataria.

La Jefatura de proyecto o la persona en la que delegue, mantendrá reuniones de seguimiento con periodicidad como mínimo mensual.

Condiciones generales de ejecución de los trabajos

El trabajo se desarrollará en las instalaciones de la adjudicataria.

Los medios, equipos y desplazamientos necesarios del personal de la empresa adjudicataria serán a cargo de esta.

El horario del SOC será en régimen de 24x7x365 a afectos de análisis, detección e identificación de patrones de ataque.

El trabajo se desarrollará siguiendo el siguiente procedimiento:

1. La adjudicataria pondrá a disposición de SAECA una cuenta de correo genérica y un teléfono en la que se atenderán las peticiones y/o consultas que se realicen. Asimismo, pondrá a disposición de SAECA una herramienta de gestión de tickets de incidencia
2. Las incidencias podrán registrase por la empresa adjudicataria o a través de la plataforma de gestión de las incidencias por parte del personal de SAECA. La empresa adjudicataria registrará todas las acciones que se vayan desarrollando para su resolución.
3. Existirá un canal de notificación prioritaria y urgente para aquellas incidencias de especial relevancia.
4. Asimismo, realizará un seguimiento de dichas acciones a medida que la incidencia se vaya gestionando y registrará el cierre una vez que SAECA dé la aceptación de su resolución y cierre.

La adjudicataria se debe comprometer a un ANS que, como mínimo, tendrá los niveles definidos en la tabla siguiente:

	Servicio	Prioridad	Tiempo de respuesta/Soporte en remoto	Tiempo de resolución
	Apertura de incidencias 24x7x365			
Servicio de soporte y SOC	1	Critica	15 minutos	2 Horas
	2	Alta	20 minutos	4 Horas
	3	Media	4 Horas	Día siguiente laboral
	4	Baja	12 Horas	Día siguiente laboral
	5	Apertura de Solicitudes/peticiones	8 Horas	Día siguiente laboral

Solvencia técnica del adjudicatario

Requisitos mínimos de solvencia y acreditación

- Los licitadores deberán disponer de las siguientes certificaciones de calidad:
  - Acreditación de formar parte de la Red Nacional de SOC.
- Acreditación de la certificación de conformidad del Esquema Nacional de Seguridad nivel Medio o Alto para el sistema con el que se prestará el servicio de SOC.
- ISO 27001
- ISO 20000
- ISO 9000
-

Valorable:

- FIRST
- CSIRT
- TF-CSIRT

Se acompañarán a la oferta, certificados expedidos o visados por el órgano competente.

Valor estimado total del contrato: 120.000 € (sin IVA).

Duración del contrato: 4 años. El proyecto de implantación del SOC deberá realizarse en un mes, tras la contratación del proyecto. El servicio SOC tendrá una duración de 4 años.

Forma de pago: Una vez adjudicado, se firmará contrato con el proveedor seleccionado. El proveedor deberá indicar claramente el coste inicial, el coste anual de cada concepto, y el precio total a 4 años.

Criterios de adjudicación: Oferta técnica y económica más ventajosa.

En relación a los criterios de adjudicación, conforme a los artículos 145 y siguientes de la Ley 9/2017 de 8 de noviembre de Contratos del Sector público, se establece que la adjudicación se realizará utilizando una pluralidad de criterios en base a la mejor relación calidad-precio, evaluándose conforme a criterios económicos y cualitativos valorándose que la empresa adjudicataria cumpla con los aspectos medioambientales y sociales conforme a la LCSP.

Criterios medioambientales:

- Promoción de medidas de ahorro y eficiencia energética y utilización de energía procedentes de fuentes renovables durante la ejecución del contrato

Criterios sociales de adjudicación:

- Promoción de medidas para la conciliación de la vida personal y laboral. Flexibilidad y adecuación de los horarios, posibilidad de teletrabajo, no establecer reuniones en tiempo límites de descanso
- Promoción de medidas para la igualdad de trato y oportunidades para hombres y mujeres. El adjudicatario deberá elaborar un informe con las medidas de igualdad aplicadas.
- Estabilidad en el empleo. Se valorará la estabilidad de la plantilla
- Promoción de medidas para la formación, así como
- Medias de salud y seguridad en el trabajo

Procedimiento de contrato: Instrucciones Internas de Contratación.

Plazo presentación ofertas: Hasta las 15:00 horas del día 31 de julio de 2024.

Recepción de ofertas en el correo electrónico: contratacion@saeca.es

Datos de contacto para recabar información adicional:

Javier Diego

91 209 37 00

En Madrid, a 18 de julio de 2024.