cfe_calificados

CONCURSO PARA LA INSTALACIÓN, CONFIGURACIÓN, PUESTA EN FUNCIONAMIENTO Y LICENCIAMIENTO DE LA HERRAMIENTA DE SEGURIDAD PARA ANÁLISIS DE COMPORTAMIENTO DE USUARIOS Y DISPOSITIVOS.

Anexo Técnico

1. Objeto

Contar con una herramienta de Seguridad para Análisis de Comportamiento de Usuarios y Dispositivos (*User and Entity Behavior Analytics* o UEBA) para identificar y examinar el comportamiento de los usuarios y equipos de cómputo que están conectados a la red de la empresa a fin de detectar amenazas a la seguridad de la información de CFE Calificados.

2. Alcance del proyecto

Como parte de las acciones para fortalecer la seguridad de la información y tecnologías para la operación, CFE Calificados necesita adquirir una herramienta de Seguridad para Análisis de Comportamiento de Usuarios y Dispositivos (*User and Entity Behavior Analytics* o UEBA). El objetivo de la herramienta es el análisis del comportamiento de los usuarios y equipos de cómputo que están conectadas a la red de la empresa a fin de detectar amenazas a la seguridad de la información de CFE Calificados.

La solución por implementar deberá incluir:

a. Licenciamiento para software de análisis de entidades y usuarios.

b. Instalación y configuración inicial de la herramienta.

c. Capacitación para el administrador de la aplicación.

d. Servicio y mantenimiento.

Requerimiento	Descripción
Licenciamiento de herramienta	Licenciamiento aplicable para la herramienta en una instalación centralizada o distribuida.
Licenciamiento para administrador	Licenciamiento aplicable para el usuario administrador con los permisos y facultades que permitan el monitoreo del comportamiento de usuarios y dispositivos.
Licenciamiento para usuarios / dispositivos	Licenciamiento aplicable para instalación de la herramienta en 60 equipos de cómputo portátil con sistema operativo Windows 10.
Instalación, configuración y puesta en marcha	Servicio de instalación, configuración y puesta en funcionamiento de la herramienta en los dispositivos de CFE Calificados en un entorno de nube de Amazon Network Services (AWS), incluyendo desde el dimensionamiento hasta la puesta en marcha y comunicación a dispositivos. Incluir pruebas del funcionamiento correcto de todos los módulos de la herramienta, y revisar la generación de reportes y alertas en la herramienta.
Capacitación para administrador	Capacitación de la funcionalidad para tres (3) usuarios con perfil de administrador en la herramienta que asegure la transferencia del conocimiento que se necesita para administrar y operar de forma autónoma la herramienta.
Soporte Técnico	Incluir esquema de soporte 5x8 (5 días a la semana, 8 horas laborales) para: Corrección de errores. Brindar soporte técnico para corrección de errores o defectos detectados en el funcionamiento del software. Actualizaciones. Actualización del software cuando estén disponibles nuevas versiones. Asesoramiento y Soporte. Contar con una línea de soporte técnico telefónico, por correo electrónico y en caso de ser necesario en sitio, ante incidencias debidas al funcionamiento incorrecto de los productos adquiridos. En caso de haber un máximo de horas y/o eventos, indicar el número para cada tipo de evento.

3. Requerimientos Funcionales

A continuación, se describen las características y funcionalidades que se requiere como alcance del presente servicio. Con la intención de evaluar el esquema de configuración de la herramienta que mejor se adecue a las necesidades de **CFE Calificados.**

Solución UEBA de *endpoint* (analíticos de comportamiento de usuarios y otras entidades), instalado en un entorno de nube, con las siguientes características:

Funcionalidad	Descripción
Autoaprendizaje	Capacidad de autoaprendizaje del comportamiento de usuarios y otras entidades.
Línea Base de Comportamiento	Creación de líneas base de comportamiento de usuarios y otras entidades (dispositivo, aplicación, IPs, departamento, organización) basado en aprendizaje generado por la herramienta.
Comparación de anomalías	Identificación de anomalías de comportamiento de usuarios y otras entidades en comparación con las líneas base de usuarios y otras entidades.
Monitoreo en tiempo real	Monitoreo de comportamiento de usuarios y otras entidades en tiempo real a nivel del *endpoint*.
Monitoreo online y offline	Monitoreo online y offline de *endpoints* (conectados o no a la red interna de la empresa).
Identificación de comportamiento malicioso	Identificación en tiempo real de comportamientos maliciosos de usuarios (intención de generar un daño). Identificación en tiempo real de fraude interno.
Identificación de comportamiento negligente	Identificación en tiempo real de comportamientos negligentes de usuarios (se identifica un evento de posible riesgo, aunque no haya intención de generar un daño).
Identificación individual de usuarios y dispositivos	Identificación en tiempo real de cuentas de usuario o dispositivos comprometidos (infiltración a la red por parte de hackers externos).
Identificación de salida de información	Identificación en tiempo real de exfiltración de información, ocultamiento de actividad maliciosa, salteo de controles de seguridad, riesgo por renuncia del empleado.
Identificación de descargas y aplicaciones no autorizadas	Identificación en tiempo real de descarga de aplicaciones y medios piratas, apuestas en línea, compartición de archivos en línea, web mail, activación y desactivación de la red.
Identificación de actividad de *ransomware*	Identificación en tiempo real de agregación inusual de datos, escalación de privilegios, movimientos laterales, actividad de *ransomware* y otros tipos de malware.
Bibliotecas de referencia	Incorporación de biblioteca de patrones de comportamiento malicioso conocido que se pueden utilizar sin necesidad de aprendizaje.
Alertas	Alerta en tiempo real de comportamientos anómalos de usuarios y otras entidades.
Auditoría	Auditoría de la actividad de usuarios y otras entidades. Consola de investigación y auditoría de la actividad de usuarios y otras entidades.
Tableros	Tableros de monitoreo preconfigurados. Debe permitir el enmascaramiento de datos con fines de privacidad. Consola de visualización de alertas. Consola de visualización, personalización y creación de tableros.
Reportes	Consola de creación de reportes.
Interfaces	Capacidad de conexión con un sistema de gestión de información y eventos de seguridad (*Security Information and Event Management* o SIEM) y otras soluciones UEBA. Capacidad de conexión personalizada con otros sistemas para envío de datos, reportes e indicadores.
Uso de recursos	El agente colector instalado en cada *endpoint* debe generar menos de 10 MB por usuario por día. Capacidad para que el agente sea desplegado de manera silenciosa a través del Directorio Activo.
Recolección de metadatos	El agente sólo debe recolectar metadatos (información no sensible). El agente debe recolectar metadatos como mínimo de aplicaciones ejecutadas, archivos manipulados, sitios web, interacciones con ventanas de usuarios, nombres de los procesos, directorio de procesos, procesos padres, hash de los procesos, tiempo de actividad, cuentas de usuario que ejecuta un proceso, nombre del dispositivo, modo de ejecución de un proceso (con privilegios o no), tiempo de ventana activa, tiempo de actividad de un proceso, parámetros de la línea de comandos enviados a un proceso, uso de USBs, eventos de inicio de sesión, entre otros.

4. Condiciones generales de la prestación del servicio

i. La funcionalidad mencionada en este documento deberá cumplirse en su totalidad por el proveedor seleccionado, también se deberá asegurar que la configuración del sistema permita integrar la funcionalidad futura mencionada en este documento.

ii. El proveedor deberá realizar la entrega del servicio dando acceso a la herramienta en la cede que CFE Calificados defina en el área metropolitana y de acuerdo con el número de licencias definidas en el anexo técnico.

iii. Proporcionar una garantía que asegure la calidad de los productos entregados y que en el caso de requerir corrección de errores deberá atenderlos máximo en dos (2) días hábiles a partir del reporte que se realice mediante los canales establecidos por el proveedor.

iv. El proveedor deberá tener un canal de comunicación para proporcionar servicio de asistencia técnica vía telefónica o presencialmente de acuerdo con la severidad del problema.