Implementación y gestión de una solución de seguridad de EDR eficaz

Protección de los puestos de trabajo corporativos y servidores a través de una solución de seguridad de EDR centralizada y la gestión eficiente de la misma.

Igenomix®

sothis

www.sothis.tech

Reto

Cuando Igenomix contacta con Sothis, se encuentra en un momento en el que ha experimentado un gran crecimiento orgánico, tanto por apertura de filiales en diferentes localizaciones como por la integración de filiales independientes, cada una con su propia solución de protección del puesto de trabajo desplegada. Esta situación da como resultado un conjunto heterogéneo de soluciones de protección para unos 450 puestos de trabajo muy complejo de gestionar y poco efectivo.

Además, Igenomix detecta la necesidad de dotarse de una protección avanzada contra el ransomware debido a la explosión de ciberataques de este tipo en todo el mundo.

En un entorno con datos sensibles como es el sanitario, la solución debía garantizar una protección eficaz de los mismos que no tuviera impacto alguno en su alta disponibilidad.

Valor de la solución

Tras el estudio de las soluciones de EDR más reconocidas del mercado, la elegida es SentinelOne.

Sentinel One es una solución de protección basada en la nube con una respuesta eficaz y probada contra el malware y en particular, contra el ransomware, capaz de integrarse con los principales SIEM/SOAR del mercado y con entorno VDI y la gran mayoría de OS, cualidad importante en el entorno heterogéneo que presentaba este reto.

Sothis propone a Igenomix un despliegue de SentinelOne diseñado para que pueda ser ejecutado por el equipo especializado de Sothis sin impacto alguno en el rendimiento del sistema corporativo, de forma que Igenomix pueda seguir operando durante el proceso sin alteraciones. Además, también le propone el posterior servicio gestionado asociado a la solución de protección.

¿Por qué Sothis?

Igenomix elige a Sothis para llevar a cabo el proyecto por su larga y contrastada experiencia en la implementación de soluciones de protección, así como por su trayectoria y recursos propios desarrollados en la oferta de servicios gestionados relacionados con la ciberseguridad. Entre ellos y en especial, el Centro de Operaciones de Seguridad SOC Sothis ERIS-CERT®, desde el que Sothis realiza las actividades de seguridad analítica y seguridad operativa y que puso a disposición de Igenomix para la entrega del servicio de ciberseguridad asociado a la gestión de la solución elegida.

Además de la experiencia y prestigio, la visión de hacer solo aquello que aporta valor al cliente y adaptarlo a sus necesidades y posibilidades han sido elementos clave para la toma de decisión sobre el partner escogido para este proyecto.

IGENOMIX, organización pionera en genética reproductiva

Igenomix es una organización que trabaja por un mundo en el que la infertilidad no sea más una barrera. En colaboración con las clínicas de fertilidad y doctores de todo el mundo, Igenomix investiga la reproducción humana para cambiar las vidas de parejas que intentan concebir.

La división Investigación Igenomix está centrada en proporcionar soluciones a los profesionales de la medicina reproductiva. La Fundación Igenomix tiene como misión el desarrollo de conocimiento científico para esta rama de la medicina.

Objetivo del proyecto

El objetivo del proyecto es la protección de los puestos de trabajo de Igenomix a través de una solución de seguridad de EDR centralizada y la gestión efectiva de la misma.

La variedad de soluciones de protección del puesto de trabajo después del crecimiento orgánico deriva en ineficacia por la complejidad de gestión.

El objetivo del proyecto es unificar esa gestión implantando una solución de EDR que logre la homogeneización y la centralice.

Junto a este objetivo principal, también se marcan los siguientes:

- Que la solución sea líder en las pruebas de evaluación de The MITRE Engenuity ATT&CK® Evaluations.
- Que la solución se base en la nube.
- Que la solución tenga una respuesta eficaz y demostrada frente a cualquier tipo de malware y en especial frente al ransomware.
- Que la solución disponga de un mecanismo de respuesta y restauración rápida para los equipos afectados por ransomware.
- Que la solución se integre con los principales SIEM/SOAR del mercado para esquivar la heterogeneidad de las filiales incorporadas.
- Que la solución sea fácilmente integrable con entornos VDI y la gran mayoría de OS.
- Que la solución produzca el mínimo impacto sobre los endpoints y servicios de Igenomix y la disponibilidad de los datos.
- Que la gestión de la solución se realice a través de un servicio gestionado.

Solución propuesta

La solución que lideramos desde Sothis ha sido la implantación y despliegue en Igenomix de la solución de EDR SentinelOne y la gestión de la misma a través de nuestro Centro de Operaciones de Seguridad SOC Sothis ERIS-CERT®.

SentinelOne es una plataforma de protección avanzada endpoint basada en la nube que previene, detecta, responde y atrapa amenazas en todos los recursos de la organización.

Desde Sothis, lideramos la implantación y el despliegue de SentinelOne en Igenomix a través de un proceso diseñado para tener un impacto mínimo en la operatividad normal de la compañía y su rendimiento.

Una vez realizado el despliegue y la puesta en funcionamiento de la solución, la gestión de la misma pasa al Centro de Operaciones de Seguridad SOC Sothis ERIS-CERT®, desde el que se realiza la evaluación, monitorización y el análisis continuos de los eventos generados en el SIEM/SOAR por parte de los analistas de seguridad de Sothis.

Además, se activa el servicio de alertas de comportamiento y actividad y el de reporte mensual de la actividad de la plataforma SentinelOne al equipo de IT de Igenomix.

Todo ello ofrecido a través de un sistema de facturación de la solución alineado con el uso realizado por parte de Igenomix.

Resultados

Igenomix cuenta ahora con un sistema de protección del puesto de trabajo unificado y centralizado, gestionado desde un SOC que proporciona monitorización, análisis y reportes continuos y garantiza un sistema de alertas en tiempo real y una protección efectiva frente al ransomware, además de:

- Funcionalidad total con entorno VDI.
- Funcionalidad total sobre las plataformas de laboratorio de Igenomix.
- Funcionalidad total sobre las plataformas de Bio-IT.
- Disponibilidad de comandos para su implementación automatizada.
- Protección sin impacto en la funcionalidad dentro de un entorno de alta disponibilidad de datos.

Según palabras del cliente

«Nos ha sorprendido el hecho de que, durante la fase de integración inicial, no hemos tenido casi impacto en nuestros sistemas en cuanto a rendimiento o bloqueos en servicios críticos se refiere».

«Gracias al sistema de facturación ad-hoc y el consumo bajo demanda, podemos crecer o decrecer en el número de agentes de una manera sencilla. Si bien partimos una volumetría mínima establecida por nuestro equipo de tecnología en el arranque del proyecto, hemos podido ampliar nuestra capacidad sin ningún tipo de flujos administrativos menos agiles».

Xavier Benavides - IT Security Specialist

IGENOMIX

CASO DE ÉXITO

En Sothis dedicamos tiempo y esfuerzo a entender de forma detallada cómo definen nuestros clientes el éxito; con ello les ayudamos a utilizar los avances tecnológicos, simplificar la complejidad de TI y a definir la arquitectura de transformación que mejor encaje con su estrategia de negocio, y que les lleve a estar mejor protegidos y a ser más eficientes y más productivos mediante la integración de los tres principales activos de las organizaciones: Personas, Procesos e Información.

www.sothis.tech