Los servicios de Entelgy Innotec Security, avalados por Ingram Micro, refuerzan la protección de la infraestructura de Fintonic en la nube

Fintonic ha mejorado la seguridad de su infraestructura que descansa sobre la nube de AWS gracias a los servicios de seguridad gestionada que le proporciona Entelgy Innotec Security, *partner* de AWS, que contó con el apoyo de Ingram Micro para su capacitación y desarrollo *cloud*. A través del servicio SmartSOC y su SIEM *as a service*, Entelgy Innotec Security ha puesto en marcha una estrategia de seguridad preventiva.

Rosa Martín

Fintonic es una *fintech* que está centrada en mejorar la salud financiera de sus clientes por medio de la agregación de sus cuentas bancarias y la recomendación de productos personalizados para su ahorro. Ofrece también formación financiera para que los usuarios puedan tomar mejores decisiones económicas. Cuando comenzó su actividad, hace más de una década, apostó por la infraestructura de AWS por su flexibilidad y su escalabilidad.

Enrique Cervantes Mora, CISO de Fintonic, señala que "disponer de los servicios de AWS supone para nosotros la capacidad de abstraernos de la parte física de la infraestructura para centrarnos en crear valor a través de nuestras aplicaciones y procesos de negocio".

La compañía utiliza servicios PaaS y SaaS de AWS que su equipo de *cloud engineering* automatiza con infraestructura como código, lo que le proporciona "un buen nivel de resiliencia, confianza en las configuraciones y repetibilidad de todo lo relacionado con la infraestructura", según indica el CISO de Fintonic.

Al mismo tiempo, el uso de los servicios de AWS le permite limitar el coste de la infraestructura a las necesidades de cada momento de una manera flexible.

Más seguridad y visibilidad

A pesar de estas ventajas, hace un año la *fintech* decidió reforzar su seguridad y la de sus usuarios con un enfoque preventivo. Según explica Cervantes Mora, "la gestión de configuraciones, la importancia de las identidades, el inventario de activos y la monitorización tanto del plano de gestión de la infraestructura como de los propios activos es algo que debe ser gestionado 24/7 por un equipo con experiencia en entornos *cloud*, ya que el nivel de exposición en algunos ámbitos es superior que en entornos más clásicos o "estáticos" y es necesario conocer las capacidades de los *public cloud providers* y los riesgos asociados".

Para acometer esta tarea necesitaba un compañero de viaje que le diera confianza, tuviera la capacidad de adaptarse a su ritmo de innovación y no se acomodase en los servicios "clásicos" de SOC. La compañía confió en Entelgy Innotec Security porque cumplía con estos requisitos gracias su profundo conocimiento de la tecnología de AWS y su experiencia contrastada.

Enrique Cervantes Mora, CISO de **Fintonic**

Alejandro Entrenas, *Monitoring & MDR manager* en **Entelgy Innotec Security**

Servicio de monitorización y gestión de incidentes

Alejandro Entrenas, *Monitoring & MDR manager* en Entelgy Innotec Security, indica que antes de poner en marcha los servicios de monitorización Fintonic tenía una visibilidad muy limitada sobre las amenazas que afectaban a su arquitectura y tenía menos agilidad a la hora de enfrentarse a los posibles riesgos que podrían afectar a la infraestructura.

Para monitorizar y gestionar los incidentes Entelgy Innotec Security ha puesto en marcha su servicio de Smart SOC y el sistema de SIEM *as a service*.

Por tanto, la solución comienza cuando se recogen los eventos o *logs* de seguridad directamente del *cloud* de AWS, es decir de las soluciones que tiene la compañía que son CloudTrail, Elastic Load Balancer y WAF, para integrarlos en el SIEM que es un software que facilita el análisis de cientos de eventos de seguridad por segundo. Así se realizan correlaciones y se despliegan casos de uso o consultas. "Se busca un patrón concreto para

Ingram Micro, pilar para el desarrollo del proyecto

El papel desempeñado por Ingram Micro en el desarrollo del proyecto ha sido decisivo para cumplir con los objetivos que quería alcanzar Fintonic. La *fintech* necesitaba un *partner* con un conocimiento profundo de la tecnología de AWS y experiencia para proporcionarle servicios de seguridad contrastados y diferenciales. Entelgy Innotec Security reunía todos los requisitos para ofrecer estos servicios gracias a la capacitación y la formación que le proporcionó Ingram Micro. "Ayudamos a nuestros *partners* con la gobernanza de los proyectos de AWS y a generar el máximo valor posible para garantizar el éxito de los proyectos *cloud*", según indica Manuel Vázquez, *IaaS Sales manager* de Ingram Micro.

Esta ayuda se concretó en diversos beneficios desde el punto de vista de *assessment cloud*, *compliance*, seguridad y *FinOps*. A través de la solución Cloudcheckr le permite optimizar costes sobre la infraestructura desplegada, detectar y revolver problemas de seguridad y recopilar las evidencias para estar lo más alineados con las normativas internacionales como ISO27002 para seguridad de la información.

"Ingram Micro proporciona una capa extra de valor sobre AWS para que los *partners* construyan sus propuestas *cloud* más completas hacia sus clientes finales", recalca Vázquez.

Entelgy Innotec Security ha participado en el programa de aceleración, siendo uno de los *partners* más destacados, lo que le ha permitido reducir los tiempos habituales de los *partners*. Ha sido capaz de pasar por todos los estatus en menos de un año.

"Uno de los puntos claves ha sido la formación y certificación de su personal en AWS, donde han estado participando en nuestros cursos de Cloud Practitioner y a través de nuestro programa IMbrace para obtener las certificaciones técnicas avanzadas sin coste para ellos", destaca el responsable de Ingram Micro.

entender cuándo sucede un evento y generar alertas de seguridad que ayuden a detectarlo en el futuro", destaca Entrenas.

Entelgy Innotec Security también aporta recomendaciones correctivas en base a la información generada durante el proceso. Según señala el *Monitoring & MDR manager* en Entelgy Innotec Security, su experiencia y conocimiento le permite detectar ataques IMDS (*Instance Metadata Service*), que es un tipo de amenaza específica en entornos AWS que puede extraer datos sensibles.

Manuel Vázquez,
IaaS Sales manager de **Ingram Micro**

Desde el SmartSOC, Entelgy puede identificar a través de los *logs* de AWS peticiones de acceso a IMDS que hayan tenido un resultado satisfactorio, diferenciando entre peticiones legítimas, escaneos desde una aplicación automática o intentos de intrusión reales que pretenden acceder a datos sensibles.

Entelgy Innotec Security ha contado con el respaldo de Ingram Micro a la hora de llevar a cabo este proyecto. Manuel Vázquez, *IaaS Sales manager* de Ingram Micro, destaca que "Ingram Micro proporciona una capa extra de valor sobre AWS para que los *partners* construyan sus propuestas *cloud* más completas hacia sus clientes finales". En este caso a través del "Programa de Aceleración" se le ha orientado de una manera consultiva para avanzar en su conocimiento sobre la tecnología de AWS y como subraya Vázquez se le ha ayudado a "generar valor reduciendo el *time to market*".

> *"Ingram Micro proporciona una capa extra de valor sobre AWS para que los partners construyan sus propuestas cloud"*

Resultados y beneficios

Para Entrenas, una de las claves principales del proyecto ha sido "la solución SIEM *as a service*, que permite dar un servicio de monitorización y respuesta a incidentes de seguridad especializado por un menor coste del que hubiera significado para Fintonic montar su propio SOC".

Entelgy también se comprometió a notificar los incidentes de seguridad en un plazo máximo de 30 minutos y, al mismo tiempo, activar al equipo de Digital Forensics and Incident Response (DFIR) disponible 24x7, lo que permite contener los incidentes con agilidad, coordinando a todos los equipos especializados del SmartSOC con el cliente.

Fintonic cuenta con un control constante de su plataforma, lo que le permite tener una visión más amplia y anticiparse a los riesgos y amenazas.

En palabras de Enrique Cervantes Mora "el resultado ha sido positivo. Disponer de las personas y la experiencia de Entelgy guardándonos la espalda 24/7 ha supuesto una mejora exponencial en cuanto a las capacidades de monitorización y ha mejorado nuestra postura de seguridad".

La cooperación entre Entelgy Innotec Security e Ingram Micro ayuda a Fintonic a reforzar su ciberseguridad

Fintonic eligió la nube de AWS para alojar su infraestructura hace más de 10 años, por lo que a la hora de elegir un *partner* para reforzar su seguridad y adoptar un enfoque preventivo necesitaba un especialista en ciberseguridad con un alto nivel de conocimiento y experiencia para complementar el trabajo de su equipo de TI. Entelgy Innotec Security, en calidad de *partner* de AWS y gracias al apoyo de Ingram Micro, ha acompañado a Fintonic en este proyecto. Le ha proporcionado servicios de seguridad gestionada con el fin de que disponga de las mejores prácticas de seguridad, vigilancia y triaje de eventos de seguridad.

VER VÍDEO