Fintonic asegura su infraestructura sobre AWS con los servicios de Entelgy Innotec Security

Fintonic quería reforzar la seguridad de su infraestructura que descansa sobre la nube de AWS. Necesitaba anticiparse ante los posibles incidentes y llevar a cabo una estrategia de seguridad preventiva. Para lograr este objetivo contó con los servicios de seguridad de Entelgy Innotec Security, que aportó su conocimiento y *expertise* a través del servicio de su SmartSOC y su SIEM *as a service*. Este trabajo contó con el respaldo de Ingram Micro.

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.

"Disponer de los servicios de AWS nos permite centrarnos en crear valor a través de nuestras aplicaciones"

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

Enrique Cervantes Mora, CISO de Fintonic

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 cono-

cer 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.

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

"La solución SIEM as a service permite dar un servicio de monitorización y respuesta a incidentes de seguridad especializado"

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

Claves del proyecto

El conocimiento de la tecnología de AWS ha sido una de las claves para lograr un resultado positivo en el desarrollo de este proyecto. Entelgy Innotec Security cuenta con una completa preparación gracias a su participación en el "Programa de Aceleración" que desarrolla Ingram Micro. En un periodo de un año ha conseguido pasar por los *status de registered, select y advanced y advanced* con competencia, lo que le ha permitido reducir los tiempos habituales del *time to market* en más de un 50 %.

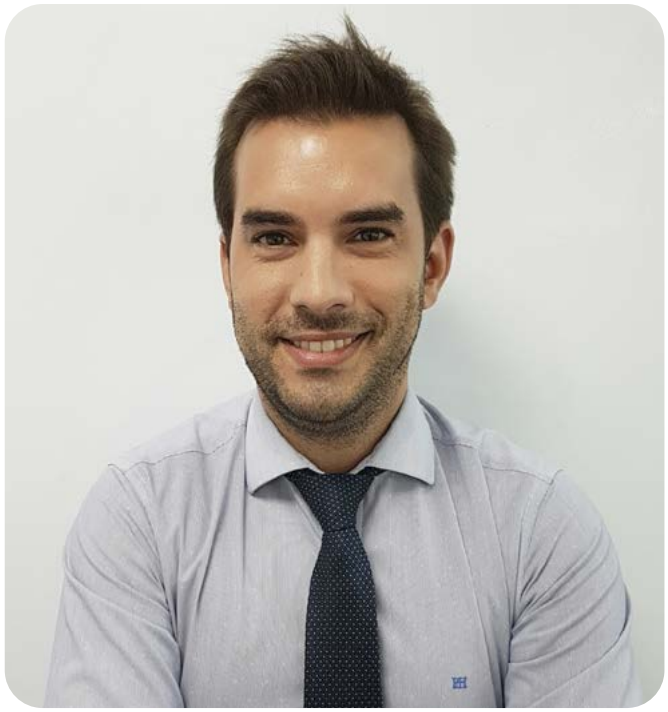
A juicio de Manuel Vázquez el desarrollo óptimo de este proyecto ha sido posible por el desarrollo de un plan *cloud* a la medida de las necesidades, focalizando el esfuerzo en la capacitación, la certificación del personal y el suministro de herramientas de valor añadido.

La experiencia y el alto nivel de conocimiento han generado confianza a Fintonic que no dudó en elegir a Entelgy Innotec Security para desarrollar este proyecto que sigue evolucionando. "Seguimos trabajando mano a mano con Entelgy para mejorar los casos de uso, adaptarlos a las nuevas funcionalidades que lanzamos y a nuevos vectores de ataque que no dejan de aparecer", destaca Cervantes Mora.

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 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

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

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. Desde el SmartSOC, Entelgy puede identificar a través de los *logs* de AWS peticiones de acceso a IMDS que hayan tenido un resultado satisfactorio,



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

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".

Los servicios de Entelgy Innotec Security, respaldados por Ingram Micro, permiten a Fintonic blindar su infraestructura en la nube de AWS

Fintonic necesitaba contar con un equipo experto para un nivel 1 de monitorización y, a la vez, un *partner* que entendiese lo que implica tener una infraestructura 100 % *cloud* como la suya que se encuentra en la nube de Amazon Web Services (AWS). En Entelgy Innotec Security, especialista en servicios de ciberseguridad y *partner* de AWS, que a su vez ha contado con el apoyo de Ingram Micro, ha encontrado el compañero de viaje idóneo para mejorar su seguridad. El especialista en ciberseguridad le ha proporcionado servicios de seguridad gestionada para crear un ecosistema de detección y respuesta a incidentes 24 horas de los 7 días a la semana.