Ciberseguridad

Servicio de seguridad completo para la web de un organismo público

El cliente

El cliente, un organismo de la Administración, necesitaba un servicio de seguimiento de su plataforma web alojada en el entorno AWS. Por ello, requería de un servicio de seguridad completo para el tratamiento de vulnerabilidades, escaneo de archivos maliciosos, tratamiento de alertas de seguridad, así como la generación de informes mensuales con estadísticas de alertas. Otro requisito era contar con un servicio de monitoreo de seguridad 24 horas al día, 7 días a la semana, con posibilidad de escalamientos en caso de cualquier incidente.

¿Por qué NTT DATA?

NTT DATA cuenta con un equipo de profesionales especializados en el servicio AWS Security Hub. Este ofrece una gestión de seguridad cloud con chequeos periódicos de los recursos AWS. Estos indicios se trasladan a un formato estandarizado que facilita acciones reactivas planificadas a través de sus recursos AWS integrados. Entre otros, Config; Firewall Manager o GuardDuty, enfocados a controlar proyectos de seguridad.

El reto

- El reto de este organismo público es disponer de un servicio de seguridad completo para su página web, alojada en un entorno AWS, y mantenerla protegida ante cualquier amenaza.
- Uno de los requisitos es contar con un servicio de monitoreo de seguridad 24 horas al día, 7 días a la semana, con posibilidad de escalamientos de alerta en caso de cualquier incidente.

La solución

- Para este proyecto, NTT DATA ofreció al cliente una solución de monitorización de la seguridad basada en servicios nativos de AWS
- Se implementaron herramientas como Amazon AWS Security Hub y Amazon GuardDuty.
- También se incluyeron agentes antivirus McAfee y CrowdStrike para el escaneo de ficheros maliciosos.

El resultado

- Durante los primeros nueve meses, el nivel de seguridad de la plataforma AWS del cliente ha mejorado hasta un 90% según los puntos de referencia de Centro de Seguridad de Internet (CIS).
- Todas las alertas de seguridad y vulnerabilidades detectadas en la infraestructura son atendidas y procesadas por el equipo de operaciones de seguridad de NTT DATA.

Mejorar la seguridad en el entorno AWS

En un contexto de transformación digital, la seguridad de la información se ha convertido en una prioridad ineludible para las organizaciones que operan en entornos en la nube.

Las herramientas de seguridad proporcionadas por AWS, entre las que destacan los servicios de AWS Security Hub y Amazon GuardDuty, así como la adopción de las mejores prácticas en la gestión de identidad, control de acceso y monitoreo continuo, permiten a las empresas asegurar la integridad de sus datos críticos, y también convertirse en referentes de la excelencia en la salvaguarda de la información en la nube.

Amazon Security Hub, la solución para automatizar y centralizar las alertas

Para este proyecto, NTT DATA ofreció al cliente una solución de monitorización, gestión de incidentes y amenazas basada en servicios nativos de AWS, que incluye AWS Security Hub y Amazon GuardDuty.

La información recopilada por Security Hub se utilizaría para procesar las alertas de GuardDuty y las vulnerabilidades descubiertas por Amazon Inspector, con el fin de mantener la infraestructura protegida. Además, se añadió una lista de IP maliciosas, generada en el SOC de NTT DATA, como fuente al propio GuardDuty y ayudar a las detecciones debido a conexiones maliciosas.

AWS Security Hub también se utilizaría para centralizar la gestión de los hallazgos de seguridad, así como para descubrir mejoras de configuración que se pueden realizar en el entorno.

Además, y debido a las necesidades de este organismo, NTT DATA también desplegó agentes antivirus de CrowdStrike y McAfee. Concretamente se instaló el antivirus EDR CrowdStrike en las instancias EC2 Linux desplegadas en el entorno. Paralelamente a esta solución, se utilizó otra propiedad de McAfee para el escaneo de archivos en un servidor implementado en la infraestructura del cliente.

Como la solución se basa en microservicios, se propuso CrowdStrike Falcon Container para la protección de los contenedores, así como para las imágenes ECR utilizadas.

Aumento hasta un 90% la seguridad del entorno AWS de la web de un organismo público

Tras la implementación de la solución basada en servicios nativos de AWS, e cliente ha conseguido los siguientes beneficios:

- **Mejora del 90%.** El nivel de seguridad de la plataforma AWS del cliente ha mejorado hasta en un 90% según los puntos de referencia del Centro de Seguridad de Internet (CIS).
- **Gestión de las alertas**. Todas las alertas de seguridad y vulnerabilidades detectadas en la infraestructura son atendidas y procesadas por el equipo de operaciones de seguridad de NTT DATA.
- **Protección**. La infraestructura de microservicios quedó protegida gracias a CrowdStrike Falcon Container.

> “Con el objetivo de mantener la infraestructura protegida, desde NTT DATA desarrollamos una solución de seguridad completa para el, tratamiento de vulnerabilidades, escaneo de ficheros maliciosos, tratamiento de alertas, generación de reportes mensuales con estadísticas de la alerta, y también el tener un equipo de monitorización de seguridad 24/7 y con escalado en cualquier tipo de incidente

Ricardo Camargo, Cybersecurity Manager en NTT DATA

Conoce más sobre NTT DATA

es.nttdata.com

