Ciberseguridad

NTT DATA ayuda a mejorar la seguridad de la app de un operador de transporte

El cliente

El cliente, una empresa operadora de transporte, necesitaba tener visibilidad de la seguridad en el entorno Amazon Web Services de su aplicación de movilidad. Concretamente, quería poder detectar vulnerabilidades y saber quién estaba atacando su plataforma de servicio de transporte integral.

¿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

- Esta compañía de transportes de pasajeros quería proteger la aplicación de transporte integrado y tener visibilidad de quien atacaba a su plataforma.
- El cliente requería además visibilidad del tráfico que fluye a través del entorno a monitorear, de modo que se pudieran detectar posibles ataques que intentaran violar el entorno del cliente, ya que los ataques son numerosos y se producen a diario, y cada minuto.

La solución

- Para este proyecto, NTT DATA propuso como solución diversas tecnologías basadas en AWS como Amazon GuardDuty y AWS Security Hub.
- También se implementó AWS WAF, un firewall para supervisar, filtrar o bloquear el tráfico.
- Las alertas generadas por GuardDuty serán absorbidas por el SOC de NTT Data para ser tratadas por el grupo de operación de nivel 1, que escalará las alertas al equipo de nivel 2 y 3 si es necesario.

El resultado

- Visibilidad de patrones maliciosos gracias a la implementación de AWS WAF y que están atacando la aplicación del cliente.
- Mayor nivel de seguridad en base a los puntos de referencia del Centro de Seguridad de Internet (CIS).

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 de seguridad, NTT DATA ofreció al cliente una solución de monitorización, gestión de incidentes y amenazas basada en los siguientes servicios nativos de AWS:

-**Amazon GuardDuty** para la revisión de alertas maliciosas que se detectaran en el entono AWS. Es un servicio de detección de amenazas que supervisa de manera continua las cargas de trabajo y cuentas de AWS para detectar actividades maliciosas y envía hallazgos detallados de seguridad para su visibilidad y corrección

-**Amazon Inspector**: para la detección de vulnerabilidades. Es un servicio de administración automatizada de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposición involuntaria a la red.

-**AWS Security Hub**: para la integración y centralización de toda la información. Se trata de un servicio de administración de la posición de seguridad en la nube (CSPM) que realiza revisiones de las prácticas recomendadas de seguridad, agrega alertas y permite la corrección automatizada.

-**AWS WAF:** firewall de aplicaciones web que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores.

Visibilidad de patrones maliciosos gracias a la implementación del AWS WAF

Tras la implementación de las soluciones de Amazon Web Service se han conseguido los siguientes beneficios:

•**Mejora de la seguridad.** El nivel de seguridad de la aplicación AWS del cliente ha mejorado según los puntos de referencia 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.

·**Visibilidad de patrones maliciosos**. Gracias a la implementación del firewall AWS WAF se pueden visibilizar patrones que están atacando la aplicación del cliente.

> “Para este proyecto, además de los servicios de seguridad nativos de Amazon Web Service, NTT DATA implementó un firewall capaz de mostrar quien estaba atacando la apliación. Para este cliente, el equipo de expertos de NTT DATA optó por AWS WAF, un firewall que, además de proteger la app permite visibilizar quien los patrones maliciosos. Un elemento muy importante ya que en este caso, los ataques se producen de manera continua.

David Cruz, Cybersecurity Expert Engineer en NTT DATA

Conoce más sobre NTT DATA

es.nttdata.com