Ciberseguridad

NTT DATA mejora de la seguridad de la landing zone de una energética

El cliente

El cliente, una multinacional del sector energético con poca madurezen la nube pública ni en su seguridad, necesita evaluar y mejorar el estado actual de seguridad del entorno de AWS, y más concretamente, de su landing zone. Esta empresa tiene presencia en los mercados de EEUU, Brasil, Reino Unido, Noruega, Irlanda y España.

¿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 esta empresa es configurar la protección de la landing zone corporativa, e implementar un sistema para proteger la totalidad de los niveles organizativos de la compañía en todos los países en los que opera.

La solución

- Para este proyecto, NTT DATA realizó la integración de los registros de AWS Security Hub con QRadar, el SIEM designado de seguridad de la multinacional energética.
- NTT Data desplegó Amazon GuardDuty como vehículo de prevención de amenazas y de AWS Security Hub para agregar, organizar y priorizar las alertas.

El resultado

- Integración con Qradar para el tratamiento de todos los hallazgos de seguridad presentes en AWS Security Hub/GuardDuty.
- Mediante la auditoría realizada en los entornos de producción, se encontraron 521 recursos que no estaban configurados correctamente desde el punto de vista de seguridad.
- Generación de reportes relacionados con los hallazgos de seguridad encontrados gracias a Security Hub.
- Unificación de la gestión de los sistemas integrales, así como la creación de una operativa para el despliegue de servicios de seguridad en AWS.

Mejorar la seguridad de la landing zone

La compañía operadora en el sector energético quería evolucionar hacia un nuevo modelo tecnológico que modernizase la infraestructura, facilitando su mantenimiento e incrementando la seguridad global.

La compañía necesitaba establecer un conjunto de normas seguridad sobre el conjunto de su arquitectura cloud y que abarca distintos negocios nacionales e internacionales.

Esta estrategia debía ir en concordancia con los métodos de seguridad de AWS, configurado en términos globales. De ahí surge la exigencia de recurrir a una Control Tower para orquestar, desde ella, las distintas cuentas y posibilitar que se agregue toda información de forma centralizada.

Los criterios técnicos de confección de la arquitectura de cuentas integradas deben seguir los máximos niveles de seguridad tanto en el diseño de las fases como en la ejecución de decisiones colectivas. Siempre desde una concepción global y mediante sinergias permanentes con QRadar, el SIEM (Security Information and Event Management) de la empresa.

AWS SRA, la solución para alinear los requerimientos legales de protección

Para este cliente, NTT DATA logró adaptar el proyecto y su ensamblaje al diseño multi-país de la landing page de la compañía y a su plataforma abierta e híbrida. La plataforma exigía una estructura de seguridad que abarcara todos los servicios de su arquitectura, además de la implantación constante de configuraciones.

Bajo estas premisas, NTT DATA desarrolló un prototipo organizativo con los servicios de seguridad de AWS multi-cuenta, multi-país, tanto a nivel empresarial como de escala; y además, una adecuación permanente a los requerimientos de seguridad durante el rediseño de la landing zone.

La revisión de la infraestructura de seguridad se realizó a través de la guía prescriptiva AWS SRA que amplía el espectro de protección de los servicios AWS y las opciones de trabajo conjunto en ambientes multi-cuentas.

Resultados

Tras la implementación de la solución basada en servicios nativos de Amazon Web Service, se han conseguido los siguientes beneficios:

- **Integración.** Se han puesto en funcionamiento varios soportes técnicos para el despliegue, la configuración y la operativa de los servicios de seguridad AWS con objeto de organizarlos mediante criterios probados e integrarlos así de una forma efectiva.

- **Estrategia unificada**. A través de la landing zone, se dispone de una estrategia unificada en los distintos mercados.

- **Alineación de requerimientos legales**. Alineación de los distintos y numerosos requerimientos legales de protección a los que debe responder de manera obligada una compañía energética.

- **Gestión de sistemas integrales**. La concepción de seguridad en una arquitectura global no puede estar basada en localizaciones individuales. En consecuencia, si un equipo necesita actuar localmente un incidente deberá acceder a la información precisa desde la consola integral con una cuenta OU –unidad organizativa– de servicios compartidos de seguridad.

> “Las respuestas a incientes en la nube con arquitecturas AWS requieren que los usuarios de las plataformas tengan nociones básicas de seguridad y respuesta ante posibles anomalías y sobre el uso de procedimientos de protección para lograr una gestión efectiva. De ahí que sea recomendable activar planes formativos, simulaciones e itinerarios operativos en ejecución en cloud.
>
> **Ricardo Camargo, Cybersecurity Manager en** NTT DATA

Conoce más sobre NTT DATA

es.nttdata.com

