Seguridad en la nube de AWS para una landing zone comercial

Una multinacional energética necesitaba una estrategia de compliance para su landing zone, lista para mercados globales

Perfil del cliente

Una multinacional de la energía necesitaba una redefinición de su arquitectura de seguridad AWS al cumplirse el primer aniversario de la puesta en marcha de su Landing Zone. Esta trabajaba para mercados en EEUU, Brasil, Reino Unido, Noruega, Irlanda y España. Con unas rigurosas normas de compliance de seguridad exigidas, NTT DATA pudo solventar el proyecto de manera ágil para proteger la landing zone.

¿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.

> **"Era imprescindible configurar la protección de la landing zone corporativa e implementar, desde AWS Control Tower un sistema que permita proteger la totalidad de los niveles organizativos de la compañía"**

Sumario de necesidades

- Identificar y gestionar los accesos con herramientas centralizadas en cuentas múltiples, permisos privilegiados y credenciales auditadas desde el AWS IAM Identity Center con las pertinentes salvaguardas acreditativas.
- Red de protección. Controles de tráfico de capas siguiendo los referentes operativos de la compañía.
- Vulnerabilidades de administración. Desarrollo de servicios homologados de reducción de incidencias en arquitecturas en Nube con sistemas de protección: AWS GuardDuty, AWS Security Hub
- Seguridad de datos. Mediante los mecanismos de encriptado y aislamiento y de detección de accesos no identificados usando el servicio AWS Key Management Service (encriptado) y AWS GuardDuty (detección de eventos)

Sumario de soluciones

- Configuración de servicios de registro de aplicaciones y de auditoría sobre todas las cuentas.
- Provisión de AWS CloudTrail para disponer de historiales de actividad, análisis de registros, hallazgos y métricas de forma centralizada.
- Integración de los registros de AWS Security Hub con QRadar, el SIEM designado de seguridad de la multinacional energética.
- Definición de las configuraciones de protección, seguimiento de cambios y utilización de *conformance packs* predefinidos por AWS.

Resultado

- Habilitación de servicios nativos para detectar y responder a sucesos de seguridad.
- Despliegue de Amazon GuardDuty como vehículo de prevención de amenazas y de AWS Security Hub para agregar, organizar y priorizar las alertas.
- Un carrusel de alarmas responde ante comportamientos anómalos.
- Disponibilidad de análisis forense.
- Amazon Detective facilita la investigación e identifica con rapidez la causa originaria de las fallas de seguridad o de actividades sospechosas

Necesidades

La compañía necesitaba establecer un conjunto de normas seguridad sobre el conjunto de su arquitectura cloud. Esta 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.

Alto nivel de seguridad en todas las fases

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.

Solución

NTT DATA logró la adopción del proyecto y su ensamblaje al diseño multi-país de la Landing Zone de la compañía y a su Plataforma Abierta e Híbrida. Esta exige una estructura de seguridad que abarque todos los servicios de su arquitectura, además de la implantación constante de configuraciones.

Dos líneas de ejecución

Bajo estas premisas, el replanteamiento de NTT DATA siguió dos trayectorias operativas:

- La realización de un prototipo organizativo con los servicios de seguridad de AWS multi-cuenta, multi-país, tanto a nivel empresarial como de escala.
- Una adecuación permanente a los requerimientos de seguridad durante el rediseño de la Landing Zone.

El arranque de 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.

Un proyecto llave en mano

A través de la Torre de Control que hospeda la AWS SRA se refuerzan las funcionalidades de gestión e intervención en entornos multi-cuenta como las que demanda la empresa energética y, al mismo tiempo, se acompasan las actuaciones en puntos específicos con respuestas agregadas.

Las service Control Policies (SCP) son un buen ejemplo de políticas preventivas y el CloudTrail de monitorización de eventos en cuentas corporativas.

Beneficios

NTT Data ha 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. Esto permite tener una estrategia unificada en los distintos mercados, a través de la landing zone.

La AWS Security Reference Architecture (SRA) ha sido el instrumento de 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 incidentes en 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 de ejecución en Cloud”