AWS Control Tower como baluarte de seguridad en cloud

NTT Data activa los controles de varios frameworks de seguridad para dotar de más protección a la arquitectura AWS de una firma energética.

Perfil del cliente

Una importante compañía eléctrica española ha decidido realizar una evaluación integral de seguridad de sus entornos en cloud, aplicaciones y datos. El objetivo es revisar los riesgos y el estado de sus servicios para la identificación de posibles vulnerabilidades y amenazas en su infraestructura y la consiguiente aplicación de medidas de mitigación. Esta empresa desea modernizar con tecnologías de vanguardia AWS su infraestructura en cloud para facilitar su gobernabilidad y reforzar sus capacidades de protección.

¿Por qué NTT DATA?

Las herramientas NTT Data de gestión de arquitecturas cloud detectaron la necesidad de instaurar métodos específicos de ciberseguridad y de despliegues de controles del CIS y NIST. Para, con posterioridad, aplicar una revisión global con Security Hub sobre las diferentes cuentas de la compañía. NTT DATA tiene un equipo de ciberseguridad cloud especialista en AWS. Compuesto de profesionales que abarcan todas las capacidades necesarias para la ciberseguridad desde el diseño de las medidas de seguridad hasta la monitorización de los eventos de seguridad en la

> "Security Hub y los diferentes servicios AWS como Config, System Manager o GuardDuty aportan una visión centralizada de la seguridad en un negocio altamente sensible como el eléctrico. Mientras que AWS Organizations permite concentrar los flujos de comunicación en una cuenta única y gestionar desde ella toda la estructura corporativa de forma armonizada y con vigilancia específica. Además de propiciar el despliegue de cuentas de manera unificada mediante Services Catalog y su gobierno mediante Control Tower."

Sumario de necesidades

- El proyecto Cloud Arq 2.0 pretende culminar la fase de reconstrucción actual y elevar el grado de explotación de la plataforma.
- El cliente necesita cimentar y consolidar las bases de su arquitectura y definir metodologías de trabajo que ayuden a ejecutar con eficiencia y seguridad las cargas operativas en cloud.
- Realización de los procesos de migración y movilidad de datos y servicios con los máximos niveles de seguridad que requieren los entornos AWS.

Sumario de soluciones

- Evaluaciones de gestión de identidades y acceso, de almacenamiento, de registro, de monitoreo y de redes a partir de los controles CIS AWS Foundations Benchmark v 1.4.0.
- La gravedad de las vulnerabilidades encontradas se somete a un cálculo de riesgos utilizando una tabla de criticidad que las cataloga en cuatro estadios de peligrosidad: crítico, alto, medio y bajo.
- La solución Control Tower ha permitido que el equipo de NTT DATA despliegue dos cuentas -log archive y audit account- con configuraciones predefinidas que, junto a otros servicios AWS, cubren todo el stack de seguridad y compliance que es exigido

Resultado

- Las cuentas nuevas se incluyen automáticamente en la organización que utilizará sus controles para la supervisión de los requerimientos sobre seguridad y buen gobierno corporativo.

Necesidades

La compañía busca crear entornos seguros en cloud con herramientas AWS para disponer de una plataforma Cloud eficiente, bien para la migración de sus sistemas actuales o para el despliegue de futuros servicios.

En paralelo, la empresa exige plenas garantías de control sobre la totalidad de la infraestructura mediante configuraciones AWS que generen entornos escalables, elásticos y protegidos.

Ajustes significativos en tiempo y operatividad

El proyecto debe obtener, además, mayores parámetros de automatización de tareas con los consiguientes ahorros operativos, de forma que el incremento de la seguridad en Cloud posibilite poner más énfasis en otras áreas del negocio.

Así como la programación de nuevas actualizaciones amparadas en la agilidad y la fiabilidad de las herramientas AWS.

La reestructuración de su plataforma y de sus procesos debe contribuir a aumentar sus niveles de operabilidad y a integrar convenientemente sus servicios transversales.

Solución

NTT DATA ha aportado una visión global de la seguridad cloud, teniendo en cuenta aquellos aspectos que pueden representar un mayor riesgo para los activos del cliente

La revisión de la arquitectura cloud siguió un exhaustivo itinerario que se inició con la desactivación de las credenciales no utilizadas en 45 días o más y la rotación de claves de acceso cada 90 días o menos.

En una segunda fase de actuación, se asignaron permisos de IAM -grupos de usuarios- solo a través de equipos de ayuda para evitar accesos individuales desmesurados y actualizaciones de la política de buckets de S3 para denegar solicitudes HTTP.

El objetivo de este último paso era el de impedir que posibles atacantes aprovechen las vulnerabilidades del protocolo HTTP para poder capturar los datos que se transmiten entre el bucket y la aplicación o persona que accede.

Restricciones de tráfico por seguridad

La hoja de ruta de NTT Data contempla cifrado de volúmenes Elastic Block Store (EBS) -almacenamiento de nivel de bloques- para proteger datos sensibles y restricciones de tráfico

Un proyecto llave en mano

La evaluación manual de NTT Data encontró 521 recursos desconfigurados en 16 ámbitos de producción, mientras el examen automático de la herramienta AWS Security Hub durante 30 días en 75 cuentas corporativas arrojó 27.442 anomalías.

Con estos datos, se confecciona una calculadora de precios para cifrar un coste mensual estimado de Security Hub, según la información disponible del área de facturación de la cuenta raíz de la empresa.

Beneficios

Tras el diágnostico inicial del equipo de NTT DATA, se procede a realizar un análisis que permite hacer un seguimiento de la gestión, el compliance y la seguridad desplegada en la plataforma de AWS.

Modernización arquitectónica de impacto

El proyecto Cloud Arq 2.0 tendrá un elevado impacto y provocará una notable gestión de riesgos sobre futuras iniciativas, que deberán adaptarse a su marco general y asumir las funcionalidades generadas.

En consecuencia, la compañía debe avisar de su cumplimiento, trasmitir a los equipos intervinientes en sus servicios esta advertencia y generar alarmas o diques que impidan ejecutar acciones de despliegue que creen incidencias.

La Control Tower es el vehículo de detección y corrección de estas anomalías.

> “Una mejora de la seguridad en entornos cloud exige un diagnóstico integral que analice todos los servicios. Ese diagnóstico permite generar un inventario de vulnerabilidades desde el que emprender su mitigación a partir de actuaciones de supervisión. Esta actuación podría generar sistemas con altas capacidades defensivas en arquitecturas corporativas.”