Automatización de gestión y monitoreo de seguridad bajo una estrategia de SOCLESS

Simón Becerra
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
Bogotá, Colombia
s.becerrau@uniandes.edu.co

Carlos Castro
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
Bogotá, Colombia
ca.castroc12@uniandes.edu.co

Sergio Quevedo
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
Bogotá, Colombia
se.quevedo3306@uniandes.edu.co

***Resumen* — Este trabajo aborda la situación en una organización que presta servicios de seguridad de la información, donde se gestionan sus activos en la nube, de los cuales un número significativo presentan riesgos de seguridad, en su mayoría de gravedad baja y media, pero también críticos y altos. A medida que aumenta la cantidad de cargas de trabajo, se observa un incremento en las alertas no resueltas, lo que sugiere una falta de gestión adecuada. Estos activos han generado alertas de seguridad, incluyendo varios incidentes y riesgos latentes. Los principales incidentes y configuraciones se relacionan con exposiciones a Internet, actividades maliciosas e intentos excesivos de inicio de sesión, entre otros.**

Para abordar esta problemática, se propone la implementación de una solución SOCLess con enfoque en entornos en la nube. Esta solución busca mejorar la eficiencia y automatizar la respuesta a incidentes de seguridad, facilitando la detección, investigación y mitigación de amenazas de manera efectiva, reduciendo al mínimo la intervención humana. Además, se propone un modelo de pago Pay As You Go para garantizar que se pague solo por las acciones realizadas, lo que agrega valor a la solución de incidentes de la organización y promueve la mejora continua.

Keywords—SOCLess, AWS, Amazon Web Services, Alertas.

I. CONTEXTO

Esta organización es una entidad de servicios profesionales de ciberseguridad con certificación ISO 27001:2013, que atiende a clientes en sectores regulados, como el financiero, industrial y seguros. Recientemente, optaron por una infraestructura alojada en la nube de AWS para mantener su rápido crecimiento. Utilizaron diversas metodologías de creación de infraestructura en la nube, lo que resultó en una variedad de configuraciones y enfoques en su infraestructura.

Este crecimiento y descentralización interna han creado desafíos en la gestión de riesgos en la nube, que incluyen problemas de configuración, vulnerabilidades y gestión de identidades. La ciberseguridad en la nube es un tema crítico, ya que el tiempo promedio de resolución de alertas en la nube es de 4-8 días, mientras que los atacantes pueden aprovechar oportunidades en cuestión de horas.

Además, se destaca que la mayoría de las alertas se generan a partir de un pequeño conjunto de reglas, lo que lleva a repeticiones frecuentes de alertas, esto de acuerdo con la imagen 1. El informe "The State of Cloud Native Security Report 2023" de Palo Alto Networks (Networks, s.f.) revela que el 39% de las organizaciones que utilizan herramientas de seguridad en la nube informan un aumento en las brechas de seguridad. Además, la mayoría de las organizaciones tienen dificultades para detectar y responder a incidentes de seguridad de manera rápida y eficiente.

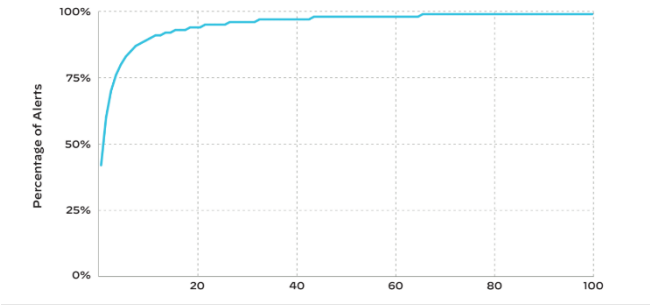

Imagen 1: Número de reglas de seguridad únicas que contribuyen al porcentaje de alertas recibidas por una organización.

En vista de estos desafíos, esta organización busca un enfoque que integre la automatización, la detección y la respuesta con tecnologías de inteligencia artificial para garantizar una supervisión, prevención, detección y respuesta eficaz a las amenazas cibernéticas en todo momento. Esto es esencial para cumplir con los requisitos de seguridad, ya sea por cumplimiento normativo o mejores prácticas de gestión de riesgos, y para mantenerse al día con la velocidad de la transformación digital.

II. JUSTIFICACIÓN DEL PROBLEMA

La información provista se recopiló de manera directa desde el entorno productivo de esta organización utilizando una herramienta de demostración con capacidades de Cloud Security Posture Management (CSPM). Esta herramienta se conecta a través de API para auditar la postura de seguridad en un entorno en la nube y presenta los resultados en informes fáciles de analizar. El objetivo principal de esta metodología es obtener datos cuantificables sobre el estado de los riesgos relacionados con la gestión en la nube.

En esta organización, se gestionan varios activos en la nube, de los cuales un porcentaje de estos presentan riesgos de seguridad, principalmente de baja y mediana gravedad, pero también críticos y altos. A medida que el número de cargas de trabajo ha aumentado, las alertas no se han gestionado adecuadamente y, de hecho, han aumentado en los últimos meses. Estos activos han generado múltiples alertas de seguridad. Los principales incidentes y configuraciones problemáticas están relacionados con exposiciones a Internet, actividades maliciosas e intentos excesivos de inicio de sesión, entre otros.

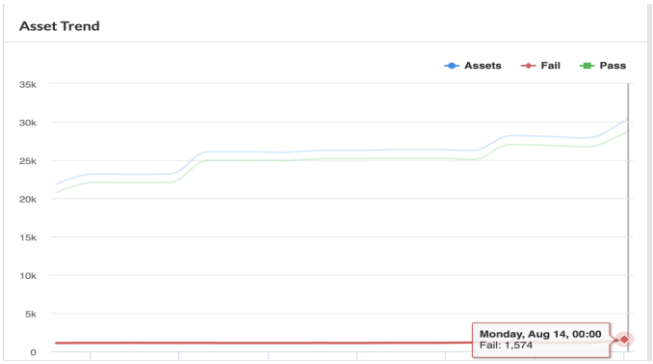

Imagen 2: Tendencia de activos y activos alertados

Tal como se evidencia en la imagen 2, muchas alertas se generan debido a configuraciones inseguras por defecto en la nube, lo que se repite en cada implementación. Además, se menciona que más de un tercio de los activos no cumplen con los controles aplicables de la norma ISO 27001:2013, y esta cifra está en aumento. La falta de procesos y controles de gestión se refleja en estos resultados descritos en la imagen 3.

Imagen 3: Tendencia de activos y su evaluación ante los controles de ISO/IEC 27001:2013

En resumen, la expansión de las aplicaciones en la nube de esta organización ha generado una gran cantidad de activos que generan alertas en grandes cantidades, lo que representa un riesgo de incumplimiento de la norma ISO/IEC 27001:2013 y posibles brechas de seguridad. El crecimiento constante de estas alertas indica que esta organización no está siguiendo el ritmo actual del mercado en cuanto a detección y respuesta a riesgos en entornos de nube. Sin embargo, se reconoce que muchas organizaciones a nivel mundial, especialmente las pequeñas y medianas, enfrentan desafíos similares debido a la complejidad técnica, la inversión económica y la falta de automatización en estas implementaciones.

III. PROPUESTA

Implementar una solución SOCLess, con un alcance enfocado a un entorno nube, que permita mejorar la eficiencia y la automatización de la respuesta a incidentes de seguridad que se puede presentar, facilitando la detección, investigación y mitigación de amenazas de forma efectiva, y con la menor intervención posible por parte del ser humano, y generando un valor agregado a la solución de incidentes de la organización, en búsqueda de la mejora continua. Así mismo, una modalidad de pago Pay As You Go, garantizando que solo se pague por las acciones realizadas.

IV. OBJETIVOS ESPECÍFICOS

- Implementar una solución que se caracterice por contar con el cumplimiento de los requerimientos y controles aplicables de la norma ISO/IEC 27001:2013.
- Garantizar que la solución cumple con las buenas prácticas del Framework del Cloud Provider.
- Garantizar y seleccionar elementos de detección que permitan validar la configuración de los recursos, así como datos y anomalías que se puedan presentar.
- Diseñar e implementar algoritmos de triage y clasificación de alertas de forma automatizada, de tal forma que la solución pueda clasificar por severidad las mismas.
- Configurar la solución implementada enfocada a que genere y almacene registros de eventos, y notifique si encuentra alguna anomalía dentro de los mismos.
- Asegurar que la solución puede garantizar una respuesta automatizada a la información del estado de la nube, esto enfocado a nivel de configuración.
- Desarrollar una solución que disminuya lo máximo posible las interacciones humanas con la aplicación, buscando que esta sea lo más automatizada posible.
- Garantizar que la solución implementada genere rastros auditables para mantener trazabilidad de sus acciones.
- Garantizar que la solución implementada requiera el menor costo monetario posible, y dar a conocer el beneficio que tiene la inversión en esta implementación.

Respecto a la metodología seleccionada para trabajar este proyecto, y tras evaluar con el equipo de proyecto y considerar los objetivos establecidos, se optó por una metodología ágil debido a la incertidumbre técnica y la naturaleza dinámica de los requisitos del negocio. Se formó un equipo multidisciplinario para tomar decisiones rápidas, obtener feedback inmediato y validar prototipos. Se estableció un plan de trabajo basado en sprints, con actividades a corto plazo y una verificación continua del valor en función de los objetivos del proyecto.

V. DISEÑO DE LA ARQUITECTURA

La arquitectura de alto nivel definida para este proyecto se evidencia en la figura 4:

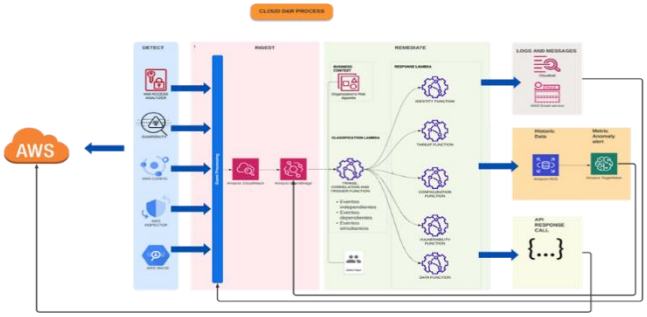

Imagen 4: Diagrama de arquitectura de alto nivel

Entre los requisitos funcionales se encuentran los siguientes:

- El sistema deberá obtener información del estado de la nube a través de conexiones API, sin el uso de agentes.
- Los elementos de detección deberán validar aspectos de Identidad, Configuración, y anomalías. En su primera fase, nos concentraremos en la configuración de los elementos de la nube.
- Las alertas generadas se organizarán en tiempo real en forma de flujos.
- El sistema debe tomar las alertas y realizar de manera automática el triage y clasificación de la alerta basada en severidades críticas, altas, medias, bajas e informacionales.
- Basado en la clasificación el sistema debe tomar la decisión de forma automática sobre cuál playbook se requiere ejecutar de acuerdo con la alerta encontrada.
- Los playbooks deberán ser ejecutados de manera automatizada, sin la necesidad de la intervención de un agente humano.
- La autenticación y autorización de los playbooks para realizar sus acciones deberá ser programática.
- El sistema deberá generar registros de las acciones tomadas, y de igual forma enviar un mensaje a los responsables en tiempo real.
- El sistema deberá tomar acciones sobre los recursos de la nube a través de conexiones API, sin necesidad de algún agente.

Entre los requisitos no funcionales se encuentran los siguientes:

- El sistema deberá ser compatible con la nube de Amazon Web Services.
- El criterio de clasificación de alertas debe estar basado en los controles del estándar ISO 27001:2013 y las buenas prácticas del Well architected framework de AWS.
- Las respuestas del sistema deberán ejecutarse en un tiempo máximo de cinco minutos.
- El sistema debe tratar de seguir una filosofía de 'Pay as you go" (PAYG), tratando en lo posible reducir los gastos solo a las acciones que se realicen.
- La autenticación y autorización de los playbooks debe seguir el principio de mínimo privilegio, garantizando que los accesos y permisos que se brinden sean los mínimos necesarios.

Entre los requisitos técnicos se encuentran los siguientes:

- La nube deberá permitir la conexión vía REST API de sus configuraciones.
- La nube deberá tener registros de los cambios realizados sobre la infraestructura a ser consultados.
- La nube deberá tener registros de sus flujos de red generados por las cargas de trabajo a ser consultados.
- Los servicios de detección deberán ser nativos de la nube.
- Se deberá contar con un servicio 'Event Stream Processing' (ESP) en modalidad SaaS capaz de integrarse con las alertas generadas.
- Las alertas deberán ser generadas en formato JSON.
- Se deberá contar con funciones que procesen los eventos en tiempo real, basado en arquitectura 'Serverless' para evitar cargos pasivos de procesamiento.
- El lenguaje de las funciones deberá ser Python por su facilidad en la integración de sistemas web, el procesamiento de datos y su facilidad de entendimiento.
- El sistema deberá guardar logs en un sistema de registros SaaS de manera no estructurada.
- Se deberá tener un sistema de relay de correo electrónico en modalidad SaaS para enviar las notificaciones de las acciones.

Los elementos de alto nivel de la arquitectura anterior son:

- Cloud Provider: Proveedor de nube pública donde se encuentran las cargas de trabajo.
- Detect: Elementos que se conectan con el proveedor de nube para detectar anomalías o malas prácticas en diferentes elementos de interés a la ciberseguridad, estos servicios crean alertas a ser analizadas.
- Ingest: Un servicio de ESP que permita organizar y procesar las alertas en tiempo real mientras se generan. Sirve como punto de entrada y disparador de las funciones.
- Remediate: Funciones que se disparen para cada evento que realizan funciones de normalización, clasificación, elección de playbook, recolección de metadata y ejecución de acciones de respuesta basado en la información de entrada.
- Logs and Messages: Servicios para dejar registro de las acciones tomadas por los playbooks y notificaciones a los administradores humanos.
- API Response: Conexiones hacia el proveedor de nube publica para realizar acciones sobre sus cargas de trabajo.

VI. ALCANCE DEL PROYECTO

Debido a limitaciones de tiempo y recursos, el proyecto se enfocará en implementar un prototipo que aborde los siguientes aspectos:

- Despliegue de AWS Config e IAM Access Analyzer para abordar los principales riesgos en la nube de esta organización.
- Creación de una capa de Ingest para integrar futuras fuentes de detección.
- Desarrollo de una capa de Remediate que clasifique riesgos según eventos independientes y dependientes, considerando el apetito de riesgo de la organización y permitiendo acciones reactivas y proactivas.
- Implementación de una capa de salida para registrar eventos, tomar acciones preventivas, crear una base de datos de métricas para futuros modelos de machine learning en Sagemaker y cerrar riesgos identificados.

Se aprovecharán las capacidades de automatización y velocidad de respuesta, reconociendo que la seguridad de los datos en AWS es una responsabilidad compartida entre el proveedor de la nube y el cliente.

Se identifican cuatro tipos de controles a nivel Cloud:

- Controles directivos: definen modelos de gobernanza, riesgos y cumplimiento.
- Controles preventivos: protegen cargas de trabajo y reducen amenazas y vulnerabilidades.
- Controles de detección: ofrecen visibilidad total sobre las implementaciones en AWS.
- Controles de respuesta: destinados a remediar desviaciones del marco de seguridad.

Dentro de los entregables generales de proyecto se encuentran los siguientes:

- Arquitectura detallada para el desarrollo de una plataforma de respuesta y gestión de incidentes de seguridad.
- Informe escrito que incluye justificación, objetivos, metodología, resultados y conclusiones relacionados con la implementación de un prototipo funcional, integraciones, aplicaciones e indicadores de eficiencia y eficacia del sistema implementado.
- Informe escrito que aborda la metodología de desarrollo del SOCLESS, un análisis de costo-eficacia y técnico comparativo con un modelo de SOC tradicional, así como un análisis DOFA de la plataforma.

Teniendo en cuenta lo anterior, la arquitectura que tendrá el primer entregable de este proyecto se define en la figura 5:

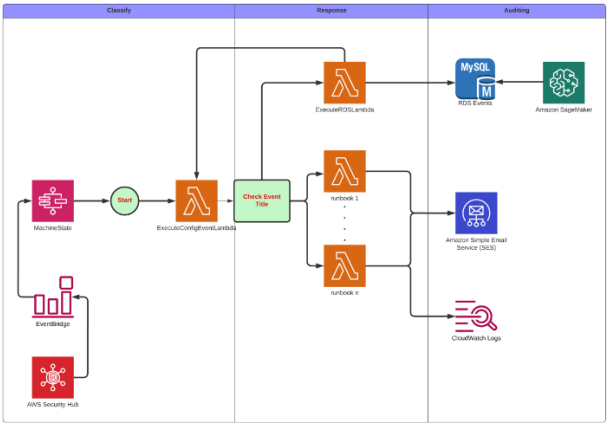

Imagen 5: Arquitectura del alcance el proyecto

Dentro de los beneficios que tendrá esta organización con la implementación de este proyecto serán los siguientes:

- Mayor visibilidad de eventos de seguridad y cumplimiento en configuraciones en la nube, con correcciones automáticas en AWS.
- Recepción de notificaciones continuas a lo largo del año por medidas de seguridad y buenas prácticas implementadas en la capa de remediación.
- Mejora en la postura de seguridad y cumplimiento normativo.
- Capacidad para presentar resultados de la gestión de seguridad de la información y cumplir con normativas como la ISO/IEC 27001:2013.
- Gestión eficiente de eventos de seguridad, reduciendo riesgos por falta de respuesta oportuna.
- Notificaciones de medidas de seguridad automáticas.
- Mayor certeza en el cumplimiento y mitigación de riesgos en AWS.
- Optimización del tiempo de analistas de seguridad.
- Mayor confianza para accionistas y clientes en el cumplimiento normativo y mejoría en la seguridad de la información.

Para el manejo del proyecto hemos definido un equipo interdisciplinario que trabaja en conjunto con el equipo interno de esta organización para alinear las expectativas y prioridades del proyecto. De este modo se definen:

- Equipo de proyecto UNIANDES
    - Sponsor
        - Gerente de Proyecto
            - Controlador de proyecto
        - Oficial de Seguridad
            - Analista de seguridad
        - Operador de Sistemas y desarrollo
- Equipo de proyecto CLIENTE
    - Sponsor
        - CISO
        - Gerente de Infraestructura

- Analista de respuesta a incidentes senior

VII. Sistema de Triage y Priorización de las Alertas

En el proceso de triage de esta organización, se determinaron factores clave para priorizar alertas de seguridad, incluyendo:

- Impacto o severidad de la alerta.
- El ambiente en el que se encuentra el activo.
- El tipo de activo.
- El sistema operativo del activo.
- Si el activo tiene conexión a redes sensibles.
- La criticidad de la operación relacionada con el activo.

De acuerdo con los requerimientos de la organización, alineados con la estrategia de seguridad de la información, se consideró ordenar estos factores según su criticidad, y para esto se asignaron puntajes a estos factores para calcular la priorización, con el mayor peso en el impacto o severidad (30%), seguido de la criticidad de la operación (25%), el ambiente (20%), el tipo de activo (15%), el sistema operativo (5%), y la conexión a redes sensibles (5%). Los puntajes van de 5 a 10.

Se definió una calculadora de priorización basada en estos puntajes y se creó una función para procesar alertas. Las alertas se reciben de diversas fuentes de detección, como AWS Config, IAM Access Analyzer, AWS GuardDuty y AWS Inspector. Las alertas se normalizan a través de AWS Security Hub.

Se configuró un sistema de orquestación con AWS Step Functions para clasificar y priorizar las alertas según los puntajes de los factores mencionados.

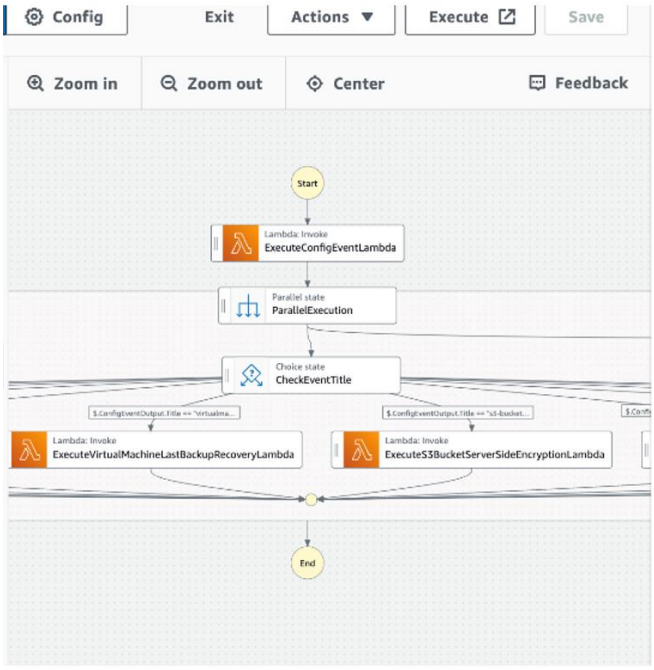

Imagen 6: Configuración del flujo de eventos a través del ASL

De acuerdo con lo evidenciado en la figura 6, la función es un script en Python que utiliza el framework de Lambda y el paquete boto3, con nueve acciones principales:

- process_security_hub_event: Extrae datos específicos de eventos de SecurityHub para el cálculo de riesgo y envía el JSON completo por correo.
- calculate_risk_score: Calcula el riesgo de eventos utilizando pesos definidos y porcentajes asignados.
- classify_event: Clasifica eventos en categorías (INFORMATIONAL, LOW, MEDIUM, HIGH, CRITICAL) según el riesgo calculado.
- get_severity_score: Determina la severidad del evento basándose en la información predeterminada de AWS o el número "normalizado" de SecurityHub.
- get_criticality_score: Valida la criticidad de recursos en la alerta, consultando un archivo .csv gestionado por esta organización en un Bucket S3.
- get_ambient_score: Verifica la región de AWS y compara con un archivo .csv en un Bucket S3 para determinar el ambiente (PRD, QA, PRUEBAS).
- get_resource_score: Calcula el riesgo basándose en el tipo de recurso involucrado en la alerta.
- get_os_score: Calcula el riesgo según el sistema operativo del evento.
- get_sensible_network_score: Evalúa la sensibilidad de la subnet o IP del evento comparándola con un archivo .csv gestionado por esta organización en un Bucket S3.

Los playbooks de respuesta se utilizan para ejecutar acciones de remediación basadas en el tipo de alerta. Las alertas se procesan y se les asigna una severidad, un riesgo y una clasificación, lo que permite priorizar las acciones de respuesta.

En cuanto a las funciones del runbook, estas funciones comparten una estructura común centrada en la interacción con servicios de AWS, el procesamiento de eventos, la evaluación de riesgos y la ejecución de acciones específicas basadas en esos riesgos. Además, mantienen una gestión de errores y notifican el estado de las operaciones a través de correos electrónicos.

Los runbooks, los cuales son implementados en Python, siguen una lógica general, aunque varían en la acción específica realizada en los servicios de AWS, dependiendo del recurso asociado al evento de SecurityHub. Utilizan librerías como 'boto3' para interactuar con servicios como CloudTrail, EC2, S3 y SES.

Las funciones establecen conexiones con los servicios de AWS, extraen información mediante 'json', definen variables y configuraciones específicas para cada caso de uso, y ejecutan acciones como la creación de CloudTrails, revocación de reglas en security groups y habilitación de cifrado en buckets S3.

Las acciones también incluyen la notificación de eventos mediante correos electrónicos en caso de fallos en las operaciones y para informar sobre la gestión de casos de uso. En particular, las excepciones se implementaron para los casos de rotación de secretos y activación de MFA de usuarios, donde se optó por enviar correos notificando la alerta al recurso que pertenece al departamento de seguridad en lugar de una remediación directa.

El sistema sigue en desarrollo, con planes de introducir un manejo probabilístico de eventos correlacionados y un registro de eventos en una base de datos. El objetivo es tomar medidas de seguridad de manera automática y eficiente en función de las alertas recibidas.

El enfoque se centra en mejorar la seguridad de los activos de esta organización y reducir el riesgo de incidentes de seguridad de la información.

Dentro de las funciones de apoyo, parte de las acciones paralelas dentro del MachineState es que una vez la función principal procese los eventos de SecurityHub lo envía a la función de RDS, esta función implementa la conexión a una base de datos RDS MySQL alojada en AWS, y al mismo tiempo crea una base de datos y una tabla (en caso de que no exista), y maneja las operaciones de inserción y actualización de los datos de los eventos utilizando la librería 'PyMySQL' y 'boto3' para el manejo de la conexión con la base de datos y los servicios de AWS.

- Conexión con DB: Se utiliza la librería PyMySQL para establecer y gestionar la conexión con la base de datos MySQL desde la función de Python.
- Creación de Base de Datos: Se crea una base de datos si no existe y se establece como base de trabajo.
- Creación de Tabla: Se crea una tabla llamada 'EventData' con columnas específicas para almacenar datos.
- Operaciones de Datos: Se ejecutan operaciones SQL para insertar o actualizar registros de los eventos en la tabla 'EventData'.

De igual forma, la base de datos que esta función manipula es la que se utiliza dentro del sistema para guardar el histórico de eventos, concurrencia y en el futuro porcentaje de probabilidad basado en el teorema de Bayes. Así mismo, en los próximos pasos se debe conectar el servicio Sagemaker de AWS para aplicar AI para la identificación y alerta de tendencias en los eventos ocurridos que podrían indicar otros riesgos dentro de la infraestructura.

VIII. Selección de reglas para cumplimiento de la norma ISO/IEC 27001:2013

Amazon Web Services ofrece un conjunto de reglas para evaluar el cumplimiento de la seguridad de la información y los controles de la norma ISO/IEC 27001:2013 en los activos de AWS. El CISO y CTO de esta organización han seleccionado las siguientes reglas clave:

- iam-password-policy: Evalúa las políticas de contraseñas seguras para garantizar la complejidad adecuada en longitud y tipos de caracteres.
- s3-bucket-logging-enabled: Verifica si se han habilitado los registros de auditoría en los buckets de S3, ya que es necesario mantenerlos habilitados siempre.
- secretsmanager-rotation-enabled-check: Comprueba si la rotación de credenciales o secretos configurados en AWS Secrets Manager está habilitada.
- vpc-sg-open-only-to-authorized-ports: Enfocado en la seguridad de red, verifica que el tráfico sin restricciones solo se permita a través de puertos autorizados.
- virtualmachine-last-backup-recovery-point-created: Asegura que cada activo cuente con un punto de restauración y copias de respaldo.
- s3-bucket-server-side-encryption-enabled: Verifica que los buckets utilicen cifrado predeterminado a través de protocolos seguros.
- iam-user-mfa-enabled: Comprueba si los usuarios que acceden a la consola utilizan la autenticación de múltiples factores además de la contraseña.
- cloudtrail-security-trail-enabled: Garantiza que los registros de eventos en AWS CloudTrail cuenten con claves de cifrado y administración de registros para validar la integridad de los registros.

- ec2-instances-in-vpc: Valida que las instancias estén en una nube privada virtual, lo que evita que estén expuestas en redes públicas.

Estas reglas se utilizan para asegurar que los activos en AWS cumplan con los estándares de seguridad y la norma ISO/IEC 27001:2013 de acuerdo con los siguientes riesgos identificados:

- s3-bucket-logging-enabled:
  - Control de Acceso (A.9):
    - A.9.2.1: Falta de capacidad para rastrear y registrar el acceso al sistema de información.
  - Gestión de Activos (A.8):
    - A.8.1.2: Ausencia de un inventario actualizado de activos de información, incluyendo registros de acceso a objetos en el bucket.
  - Seguridad en la Información (A.12):
    - A.12.4.1: Insuficiencia en el seguimiento y revisión regular de registros de eventos de seguridad, complicando la evaluación de eventos.
  - Gestión de Incidentes de Seguridad (A.16):
    - A.16.1.1: Dificultad para identificar y manejar incidentes debido a la falta de registros.
  - Riesgos:
    - Falta de monitoreo impide la detección y respuesta a ataques.
    - Auditoría deficiente dificulta la demostración de cumplimiento.
    - Riesgo de incumplimiento de regulaciones y pérdida de confianza.
- secretsmanager-rotation-enabled-check:
  - Control de Acceso (A.9):
    - A.9.1.2: Falta de implementación de medidas de control de acceso basadas en políticas, especialmente en la rotación de secretos.
  - Gestión de Activos (A.8):
    - A.8.1.2: Ausencia de un inventario actualizado de activos, incluyendo gestión adecuada de secretos y credenciales.
  - Seguridad en la Información (A.12):
    - A.12.4.1: Falta de políticas y procedimientos para la gestión segura de la información, incluyendo la rotación periódica de registros.
  - Gestión de Incidentes de Seguridad (A.16):
    - A.16.1.1: Dificultad para identificar y manejar incidentes relacionados con la exposición no autorizada de secretos.
  - Riesgos:
    - Exposición prolongada de credenciales sensibles.
    - Mayor riesgo en caso de compromiso, facilitando acceso no autorizado a largo plazo.
- vpc-sg-open-only-to-authorized-ports:
  - Control de Acceso (A.9):
    - A.9.1.2: Falta de implementación de medidas de control de acceso basadas en políticas, especialmente en las reglas de seguridad de la VPC.
  - Seguridad en la Información (A.13):
    - A.13.2.1: Falta de políticas y procedimientos para la gestión segura de la información, incluyendo la configuración de seguridad de los recursos de red.
  - Riesgos:
    - Exposición de servicios no autorizados debido a puertos abiertos innecesarios.
    - Mayor riesgo de ataques de escaneo de puertos sin restricciones.

IX. Análisis de resultados

Se crearon diez funciones de respuesta (runbooks) basadas en políticas definidas junto con el equipo de trabajo de esta organización. Estas funciones se aplican a eventos tomados del servicio AWS Config. Para probar la ejecución de la StateMachine y cada caso de uso, se utilizaron eventos JSON directamente de las reglas de AWS Config.

Se presenta un caso de prueba específico, "vpc-sg-open-only-to-authorized-ports", utilizando eventos JSON que indican un grupo de seguridad con puertos no restringidos (0.0.0.0/0). La simulación en StepFunctions muestra resultados exitosos, manejando eficientemente los eventos en cada paso.

La ejecución demuestra el procesamiento de 'ConfigEventLambda', asignando un riesgo medio (risk score: 3.4) al evento, clasificando el tipo de recurso y el ambiente (desarrollo), entre otros. Los logs incluyen la ejecución del runbook y la función de RDS enviando el SQL statement a la base de datos.

Se validan las integraciones de los runbooks con SES para correos, el registro en CloudWatch logs y los cambios en los recursos de AWS para notificar sobre las modificaciones.

Los demás casos de uso pueden manejarse de manera autónoma, reduciendo el riesgo inherente de las configuraciones en la nube y acercando a la organización al cumplimiento normativo.

Se busca cumplir con los controles de la norma ISO/IEC 27001:2013, priorizando la implementación de tecnologías para abordar 83.33% de los controles relacionados con activos tecnológicos. Esta primera fase excluye controles de criptografía, que podrían integrarse en futuras implementaciones, alcanzando así un 100% de cumplimiento en controles tecnológicos.

Considerando que el 37.5% de los controles en el Anexo A son tecnológicos, la implementación proyectada contribuirá al cumplimiento del 31.25% del Anexo A total. La solución aborda la mayoría de los grupos de controles tecnológicos, demostrando efectividad en el cumplimiento.

En cuanto a los activos en el entorno AWS, se proyecta que en 24 meses solo el 1% no cumplirá con los controles tecnológicos. Este margen se reserva para la integración de nuevos activos a lo largo del tiempo. Se espera una reducción significativa de activos no conformes en los próximos meses, permitiendo que esta organización cumpla con la norma ISO/IEC 27001:2013, crucial para operar con información sensible como la financiera y de salud.

X. Paso a producción

Para el paso a producción se realizarán tareas previas de dimensionamiento de riesgo, alistando los casos de uso que se pondrán en producción y mapeando los activos definidos. Luego se considerarán cuales activos son más críticos y qué aplicaciones o servicios se podrían ver afectados producto de las medidas correspondientes.

Se considera una sola ventana de puesta en producción, donde se debe generar un documento de control de cambio donde un comité conformado por miembros de Customer Support, Seguridad de La información, IT y Helpdesk para evaluar riesgos de los cambios, plan de acción, y plan de rollback.

Una vez aprobado, se genera el documento Acceptance test procedure (ATP) para verificar el plan de pruebas y sus responsables.

El día de la ventana de cambio se corre el ATP antes de los cambios, se ejecuta el CDC, y luego nuevamente el ATP luego de los cambios. De ser exitoso y sin problemas se aprueba y se cierra la ventana de cambio.

En caso de tener inconvenientes con aplicaciones críticas se tendrá hasta 1 hora para remediar incidentes de acuerdo con el Business Impact Analysis (BIA), de no lograr mitigar los incidentes dentro de ese tiempo se deberá aplicar el plan de rollback.

XI. Pasos futuros del proyecto

Se recomienda incorporar funcionalidades avanzadas de Machine Learning en un nuevo entorno definido de AWS para mejorar las capacidades de seguridad. Esto incluiría la creación de un bucket específico utilizando Sagemaker para implementar técnicas como correlación cruzada, detección de anomalías y entrenamiento de modelos. La integración de correlación cruzada con machine learning permitiría un análisis más profundo y contextualizado de los datos de seguridad, mejorando la detección en tiempo real de patrones complejos y comportamientos anómalos.

XII. Referencias

- Palo Alto Networks Inc. (2023). *Cloud Threat Report, Volume 7.* Santa Clara, CA.
- ISO. (10 de 2013). ISO/IEC 27001:2013. Obtenido de ISO/IEC 27001:2013: https://www.iso.org/contents/data/standard/05/45/54534.html
- Roberto Martinez, Incident Response with Threat Intelligence: Practical Insights into Developing an Incident Response Capability through Intelligence-Based Threat Hunting. Mexico, Nuevo Leon: Packt Publishing; 1er edición , 2022
- “2023 State of Cloud Native Security Report”. Palo Alto Networks. Accedido el 11 de diciembre de 2023. [En línea]. Disponible: https://www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2023