Cuando la nube se defiende sola

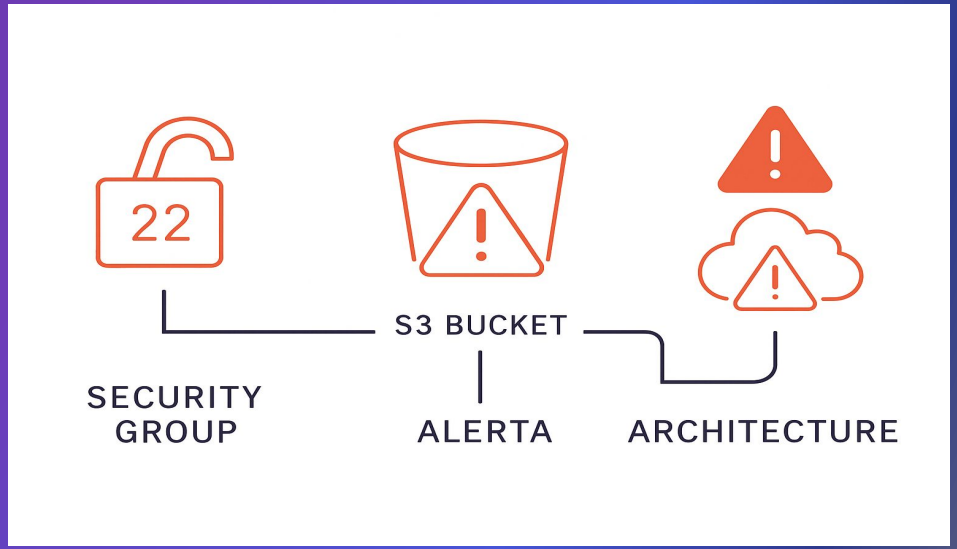
Remediación automática en **AWS** con eventos y funciones Lambda

Luis Lunar (Luis Eduardo)
Noviembre 19, 2025

El conflicto: cuando la nube NO se defiende sola

El conflicto, cuando una mala configuración abre la puerta

- Un puerto 22 expuesto sin querer
- Un bucket S3 creado sin autorización
- Una regla insegura que nadie ve
- Un cambio que pasa “debajo del radar”

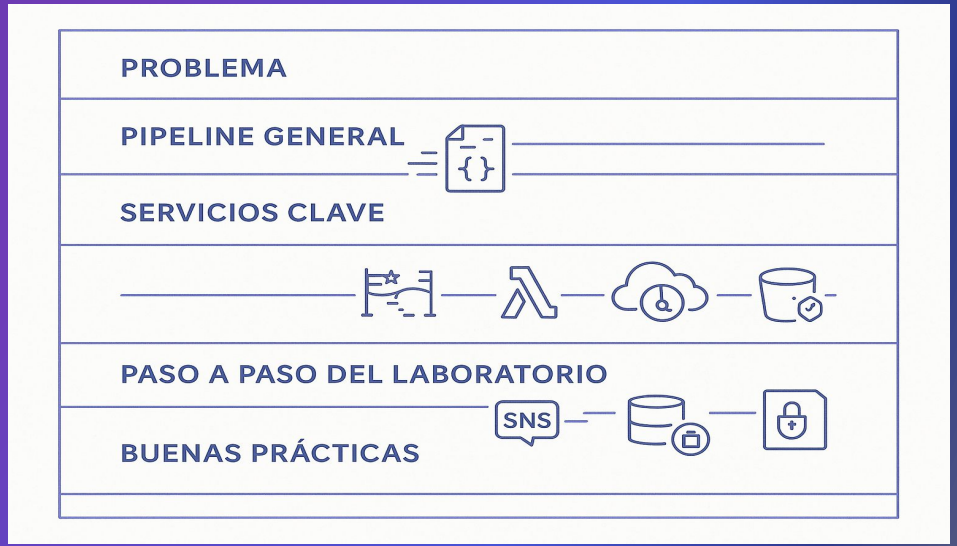


“¿Qué pasa si nadie corrige este error… y nadie se da cuenta?”

Qué vas a aprender hoy (Objetivos + Mapa de ruta)

Objetivos de aprendizaje

- Entender cómo AWS detecta acciones sensibles en tiempo real.
- Aprender a diseñar un pipeline de remediación automática.
- Conocer el rol de CloudTrail, EventBridge, Lambda, S3, SNS y CloudWatch.
- Revisar un laboratorio paso a paso sin hacer demo en vivo.
- Llevarte un modelo replicable para tu propia cuenta de AWS.

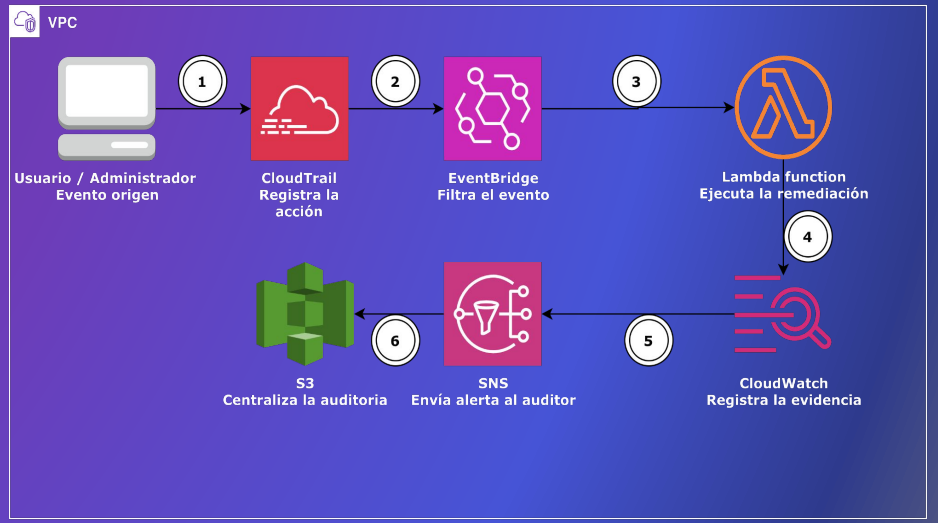


Visión global del pipeline de remediación automática

Pipeline de seguridad automatizada flujo completo:

1. CloudTrail registra la acción.
2. EventBridge filtra el evento
3. Lambda ejecuta la remediación.
4. CloudWatch Logs registra la evidencia.
5. SNS envía la alerta.
6. S3 centraliza la auditoría.

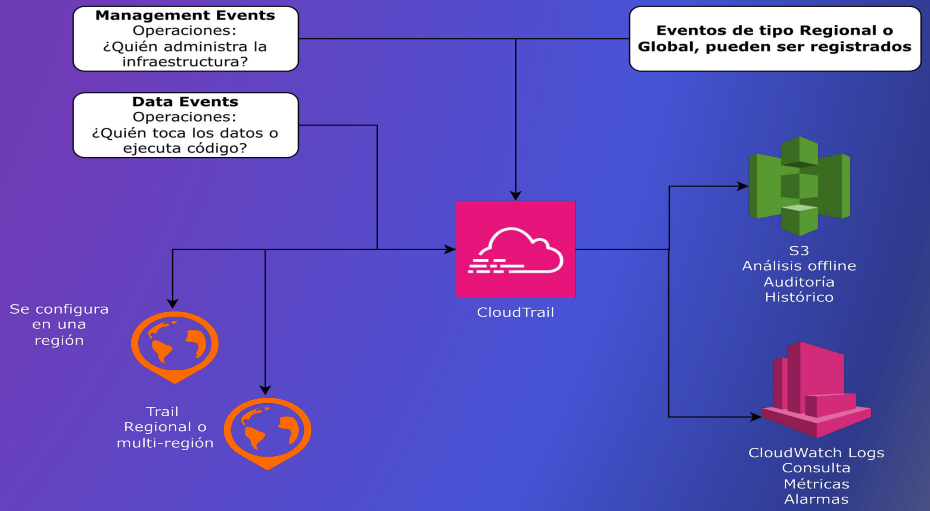
Resultado: La nube detecta, corrige y notifica sin intervención manual.



CloudTrail: ojos y memoria de la nube

CloudTrail: registro y trazabilidad total

- Registra cada acción API en tu cuenta.
- Captura *quién*, *cuándo*, *desde dónde* y *qué hizo*.
- Fuente primaria de eventos para seguridad y auditoría.
- Alimenta a EventBridge en tiempo real.

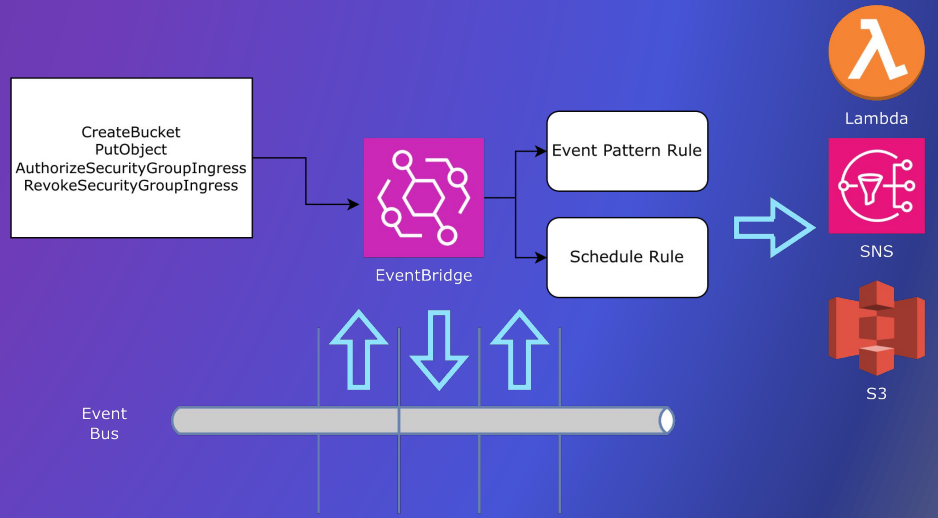


"Si pasó en tu cuenta, CloudTrail lo sabe."

EventBridge: el motor que detecta y dispara acciones

EventBridge: detección inteligente en tiempo real

- Detecta eventos de CloudTrail en tiempo real.
- Filtra acciones sensibles mediante *Event Patterns*.
- Ejecuta automatizaciones vía Lambda.
- Permite reglas por servicio, acción, usuario, IP, región, etc.
- Base del modelo event-driven en seguridad.



"EventBridge convierte eventos en acciones."

Lambda: el cerebro de la remediación

Lambda toma el evento que detectó EventBridge y aplica la corrección necesaria.

- EventBridge, no corrige nada.
- SNS, no corrige nada.
- CloudWatch Logs, no corrige nada.

“Solo Lambda ejecuta la **remediación**”

¿Qué tipo de remediaciones hace Lambda en tu laboratorio?

Lambda realiza dos acciones críticas:

a) **Remediación 1**: Bucket no autorizado

Ante un CreateBucket:

- Verifica si el bucket cumple las reglas esperadas.
- Si NO cumple → elimina automáticamente el bucket.
- Registra evidencia.
- Envía notificación vía SNS.

"Este es un control preventivo + correctivo inmediato."

b) **Remediación 2**: Regla SSH 22 abierta

Ante un AuthorizeSecurityGroupIngress:

- Analiza el contenido del evento.
- Si detecta algo como 0.0.0.0/0 + puerto 22.
- Elimina la regla insegura.
- Registra evidencia en CloudWatch Logs.
- Envía alerta via SNS.

"Aquí Lambda te protege de un riesgo de alto impacto."

¿Qué contiene el evento que recibe Lambda?

El evento que recibe Lambda es un JSON 100% igual al evento original de CloudTrail filtrado por EventBridge.

Contiene:

- Nombre del servicio: "eventSource": "s3.amazonaws.com".
- Operación: "eventName": "CreateBucket".
- Identidad del usuario: userIdentity.
- Dirección IP: sourceIPAddress.
- Recurso afectado: requestParameters.
- Hora exacta, región y cuenta.

Este JSON es suficinte para:

- Identificar el bucket creado.
- Identificar la regla de seguridad agregada.
- Decidir la acción automática.

"Lambda no adivina nada, simplemente lee el evento."

Lambda necesita permisos (y por eso el rol IAM es clave)

Lambda NO puede corregir nada si no tiene permisos, debes darle un rol que permita:

Para S3:

- s3:DeleteBucket
- s3:ListBucket
- s3:GetBucketPolicy
- etc.

Para Security Groups:

- ec2:RevokeSecurityGroupIngress
- ec2:DescribeSecurityGroups

Para logs:

- logs:CreateLogGroup
- logs:PutLogEvents.

Y para SNS:

- sns:Publish.

“Lambda es la pieza que convierte un evento en una acción concreta, es donde ocurre la remediación automática.
Sin Lambda, detectaríamos el problema… pero no haríamos nada al respecto.”

CloudWatch Logs, S3 y SNS: evidencias y alertas

CloudWatch Logs es donde Lambda deja todo registrado:

- Qué acción ejecutó.
- Qué recurso afectó.
- Qué decisión tomó.
- Qué valores encontró en el evento JSON.
- El resultado de la remediación.
- Errores, advertencias y detalles internos.

"CloudWatch Logs es donde queda la **evidencia técnica del proceso**.
Si quieres saber qué hizo Lambda exactamente, lo ves aquí."

S3 → “El repositorio de auditoría”

S3 funciona como almacenamiento histórico. Mientras CloudWatch Logs guarda evidencia técnica temporal, S3 guarda evidencia permanente.

En el laboratorio, S3 sirve como:

- Repositorio de evidencia.
- Archivos históricos.
- Punto de control para auditoría

“CloudWatch Logs te dice qué pasó. S3 te **guarda** el registro histórico para auditoría.”

SNS → “La alerta inmediata”

SNS no guarda nada.
SNS no analiza nada.
SNS no ejecuta nada.
SNS notifica lo que pasó.

En el pipeline:

- Lambda remedia.
- Labda publica en SNS.
- SNS envía un correo al equipo técnico o de seguridad.

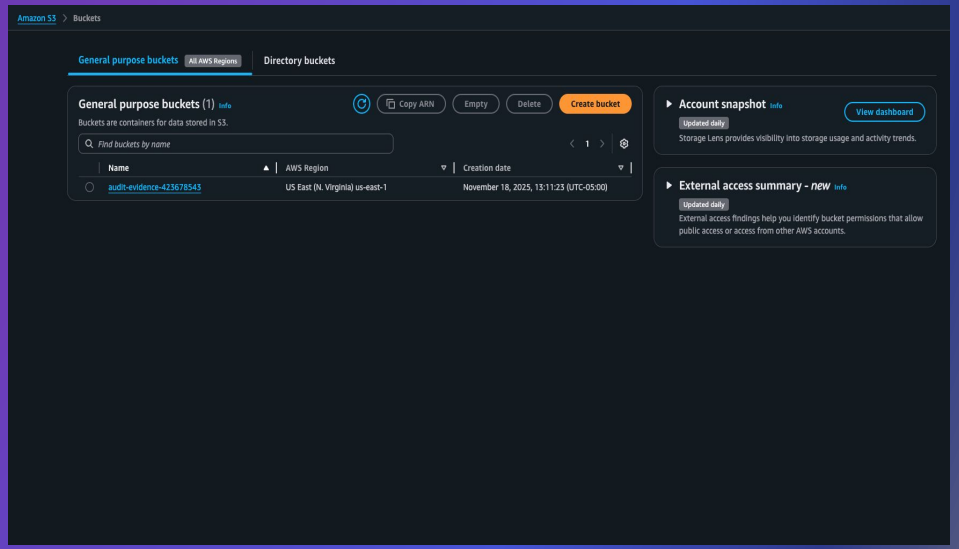
“SNS no forma parte de la remediación, forma parte de la **comunicación**, es la voz del pipeline.”

Laboratorio – Pasos

PASO 1 — Crear bucket S3 de evidencias

PASO 1 — Crear bucket de evidencias en S3

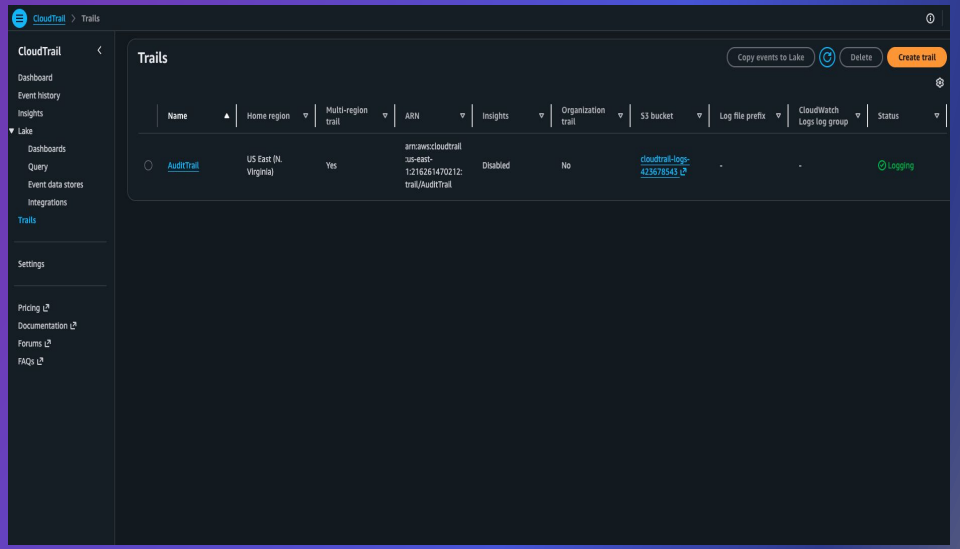
Ir a S3 → Buckets - Clic en Create bucket
Configurar:
Bucket name: audit-evidence-<randomkey>
Región: us-east-1 (N. Virginia)
Block Public Access: Activado (por defecto)
Object Ownership: ACLs disabled
Ejemplo:audit-evidence-a92fbd
Nota:No cambiar encryption, versioning ni configuraciones avanzadas.



PASO 2 — Crear Trail en CloudTrail

PASO 2 — Habilitar el registro de eventos con CloudTrail

Ir a CloudTrail → Trails - Clic en Create trail
Configurar:
Trail name: AuditTrail
S3 bucket: Crear nuevo: cloudtrail-logs-<randomkey>
Management events: Read/Write (activado)
Data events: Opcional (dejar apagado para este lab)
Log file SSE-KMS Encryption: Dejar por defecto (opcional)
Clic en Create trail
Ejemplo de bucket:
cloudtrail-logs-a41dcb

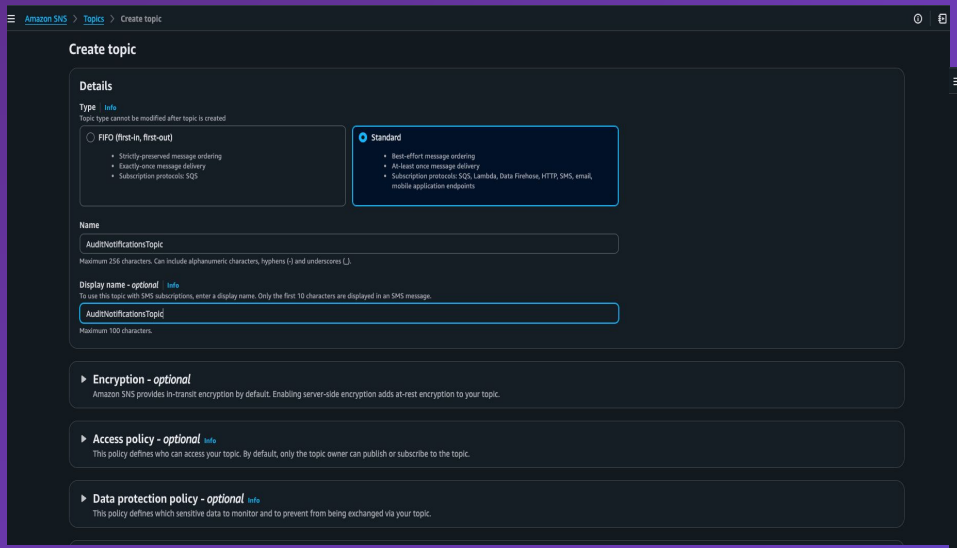


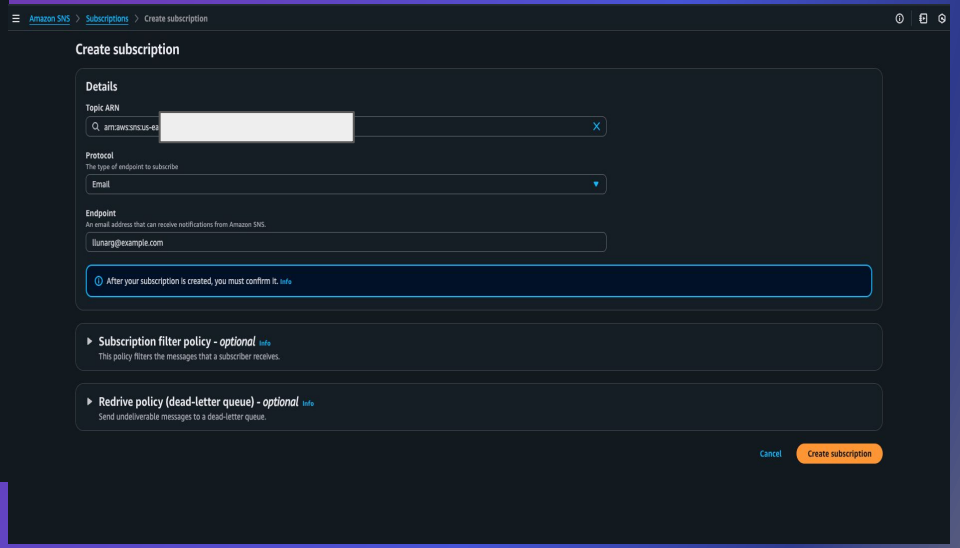
PASO 3 — Crear SNS Topic + Suscripción por Email

PASO 2 — Habilitar el registro de eventos con CloudTrail

Ir a SNS (Simple Notification Service)
Configurar:
*Menú izquierdo → *Topics*
Clic en Create topic
Tipo: Standard
Nombre: AuditNotificationsTopic
Dejar el resto por defecto→Clic en Create topic
Configurar:
*Crear suscripción por correo
Dentro del Topic → *Subscriptions*
Clic en Create subscription
Protocol: Email - **Endpoint**: (tu correo real, ej: miemail@gmail.com)
Clic en Create subscription

PASO 3 — Crear SNS Topic + Suscripción por Email





PASO 4 — Crear la función Lambda de remediación - Parte 1

PASO 2 — Habilitar el registro de eventos con CloudTrail

Ir a Lambda → Create function
Configurar:
Name: ProcessAuditEvent
Runtime: Python 3.12
Architecture: x86_64 (o ARM si lo prefieres)
Execution role:
Usar rol existente:
ProcessAuditEventExecutionRole

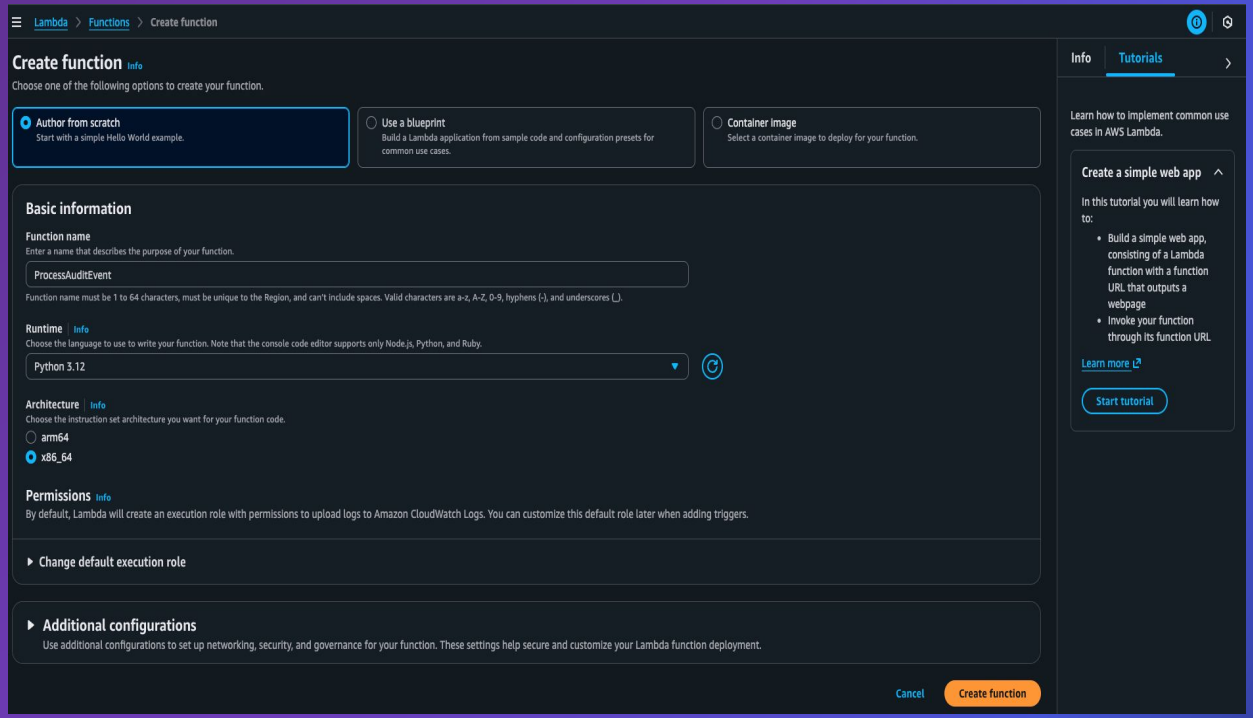
Verificar permisos del rol
El rol debe incluir (previamente creado):

- AWSLambdaBasicExecutionRole
- AmazonS3FullAccess
- AmazonEC2FullAccess
- AmazonSNSFullAccess
- CloudWatchLogsFullAccess

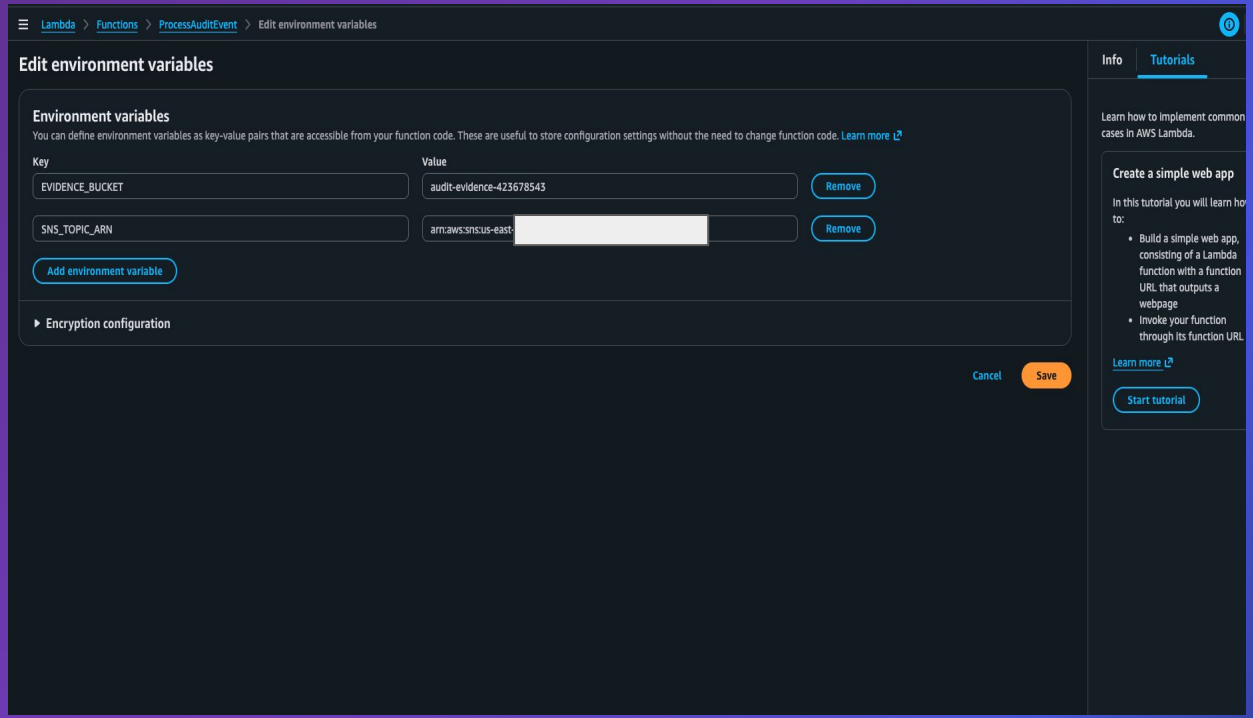
Configurar variables de entorno

EVIDENCE_BUCKET = audit-evidence-<id>
SNS_TOPIC_ARN = arn:aws:sns:us-east-1:<id>:AuditNotificationsTopic
Finalmente **pegar el código** compartido por la comunidad.

PASO 4 — Crear la función Lambda de remediación – Parte 2



PASO 4 — Crear la función Lambda de remediación – Parte 3



PASO 5 — Crear reglas en EventBridge - Parte 1

PASO 5 — Configurar reglas EventBridge para activar Lambda

Regla: CreateBucket
Detecta cuando se crea un bucket sin autorización.

- **Rule name**: DetectCreateBucket
- **Service**: S3
- **Event type**: CreateBucket
- **Target**: ProcessAuditEvent
- **Event Pattern JSON**:

```
{
  "source": ["aws.s3"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["s3.amazonaws.com"],
    "eventName": ["CreateBucket"]
  }
}
```

PASO 5 — Crear reglas en EventBridge - Parte 2

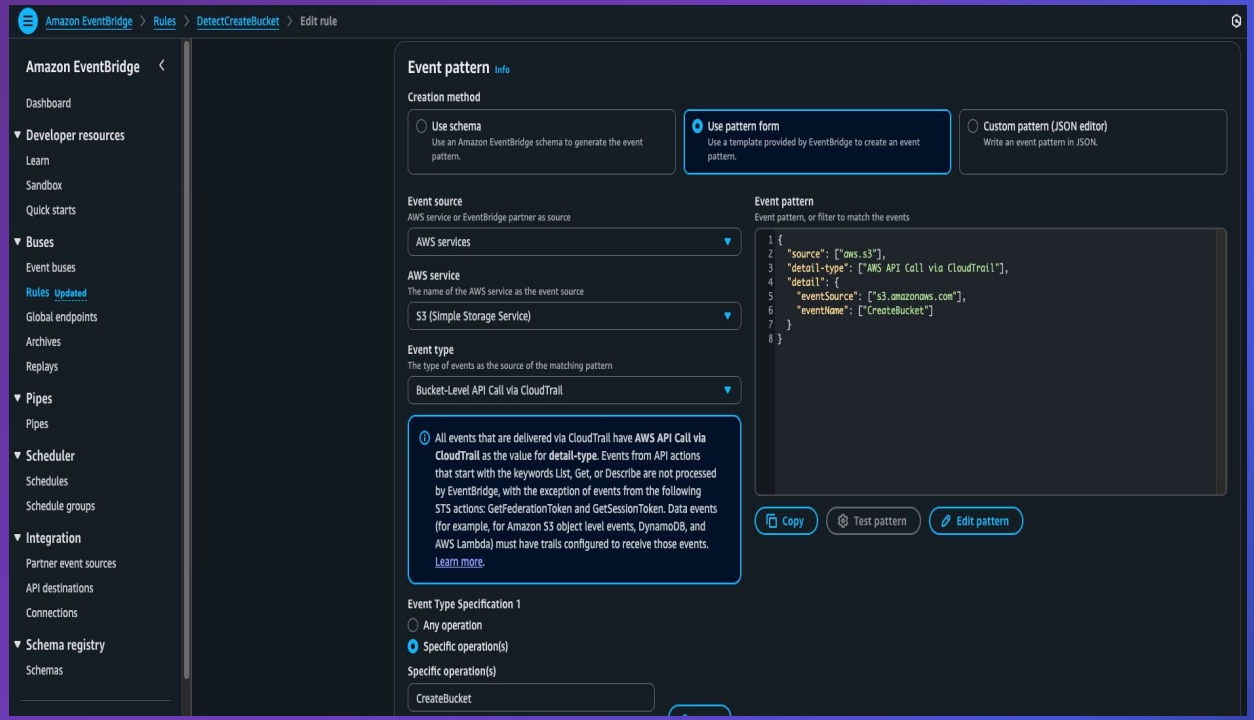
PASO 5 — Configurar reglas EventBridge para activar Lambda

Regla: CreateBucket
Detecta cuando se crea un bucket sin autorización.

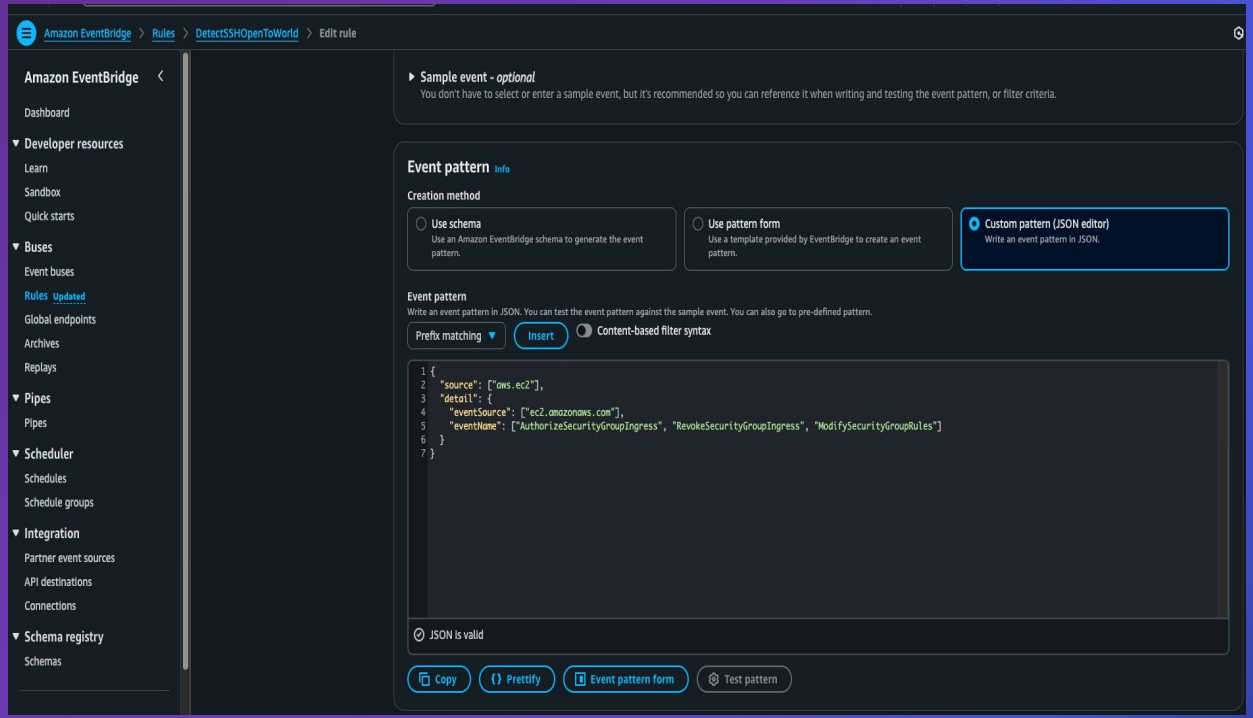
- **Rule name**: DetectInsecureSSH
- **Service**: EC2
- **Event** : Reglas de SG modificadas
- **Target**: ProcessAuditEvent
- **Event Pattern JSON**:

```
{
  "source": ["aws.ec2"],
  "detail": {
    "eventSource":
["ec2.amazonaws.com"],
    "eventName": [
      "AuthorizeSecurityGroupIngress",
      "RevokeSecurityGroupIngress",
      "ModifySecurityGroupRules"
    ]
  }
}
```

PASO 5 — Crear reglas en EventBridge - Parte 1



PASO 5 — Crear reglas en EventBridge - Parte 2



PASO 6 — Pruebas Reales del Pipeline

Escenario S3: Bucket no autorizado
Crear un bucket temporal (cualquier nombre).
Esperar 5–10 segundos mientras EventBridge procesa el evento.
Confirmar que el bucket se eliminó automáticamente.
Revisar CloudWatch Logs → buscar log de Lambda:

- Acción detectada: CreateBucket
- Bucket marcado como no autorizado
- Acción realizada: DeleteBucket

Verificar correo SNS confirmando la remediación.

Escenario Security Group: SSH inseguro
Crear o seleccionar un Security Group de prueba.
Agregar la regla:

- Port 22
- Source: 0.0.0.0/0

Esperar 5–10 s: Lambda debe eliminar automáticamente la regla insegura.
Validar en CloudWatch Logs:

- Evento: AuthorizeSecurityGroupIngress
- Evaluación de riesgo
- Remediación ejecutada: RevokeSecurityGroupIngress

PASO FINAL — Limpieza del entorno

Limpieza del laboratorio

- Eliminar Lambda
- Eliminar reglas EventBridge
- Eliminar SG y buckets de prueba
- Eliminar SNS Topic si ya no se usa

Referencias y Documentación Oficial

AWS — Servicios utilizados en el laboratorio

CloudTrail (Registro y auditoría)
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

EventBridge (Reglas y automatización)
https://docs.aws.amazon.com/eventbridge/latest/userguide/what-is-amazon-eventbridge.html

AWS Lambda (Remediación automática)
https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

Amazon S3 (Evidencias y almacenamiento)
https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

Amazon SNS (Notificaciones por correo)
https://docs.aws.amazon.com/sns/latest/dg/welcome.html