Verificación continua de la postura de seguridad en la nube de AWS

CloudFest, 2022

Por: Sheyla Leacock

Agenda

- Presentación y objetivo
- Introducción a la seguridad en la nube
- Introducción a la postura de seguridad
- Verificación continua de la postura de seguridad en AWS
- Demostración
- Referencias

Sheyla Leacock

- Licenciada en Desarrollo de Software (UTP). Cursando un Máster en Ciberseguridad, Hacking Ético y Seguridad Ofensiva (UEMC-EIP).
- Co-fundadora de Women of Security (WoSEC) Panamá, Embajadora de la Fundación Comunidad Dojo y Community Builder de AWS.
- Oficial de Seguridad de la Transformación Digital e Instructora de cursos de Seguridad Informática, con +8 años de experiencia.
- Ponente internacional en conferencias de Ciberseguridad y Tecnologías.
- Con certificaciones y especializaciones en AWS, ciberseguridad, redes (CCNA), administración de servidores Linux, entre otras.

shey.lck@gmail.com

https://www.linkedin.com/in/sheyla-leacock/

Objetivo

Ejemplificar la importancia de conocer la postura de seguridad de nuestras aplicaciones en la nube, manteniendo una visibilidad centralizada mediante verificaciones de seguridad continuas y automatizadas utilizando como referencia servicios nativos de AWS.

Disclaimer

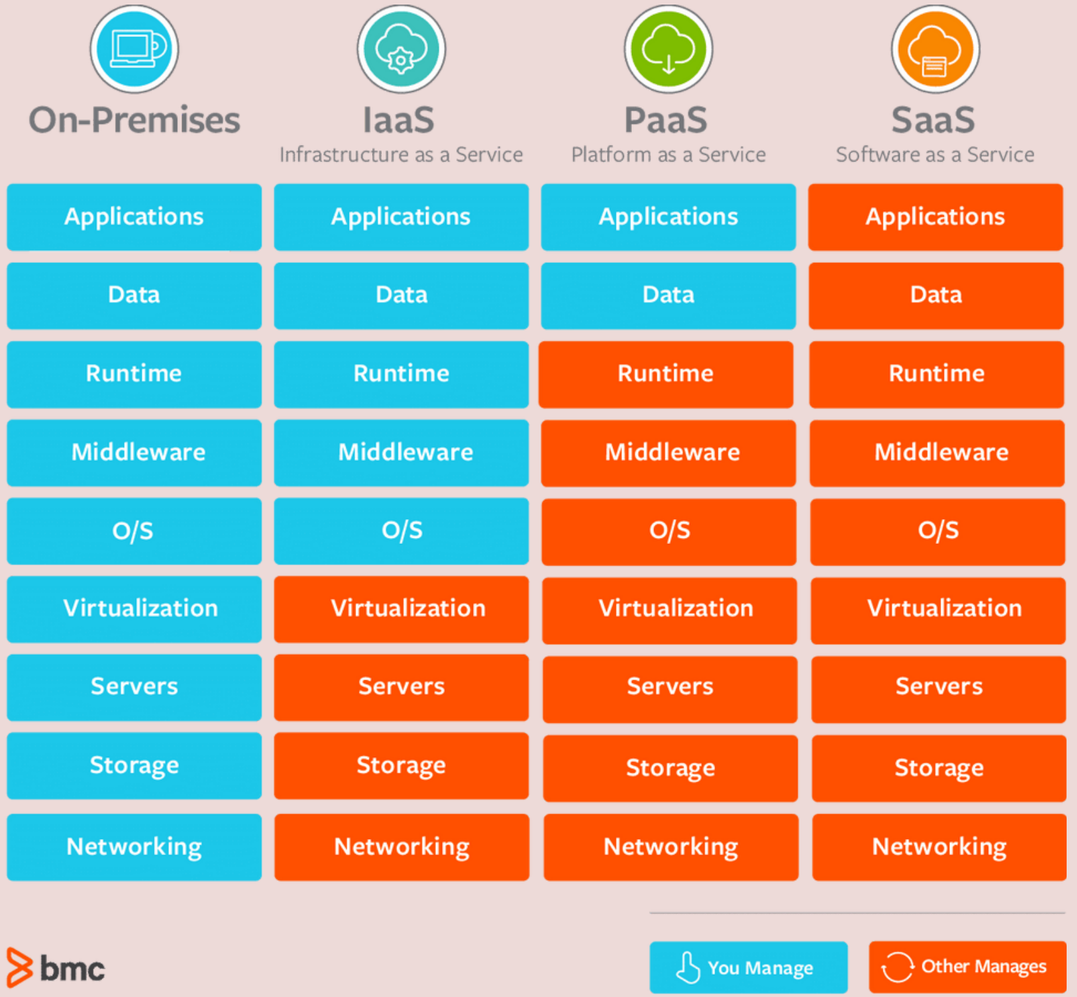
Esta presentación se realiza con fines educativos y de aprendizaje, con el fin de brindar información que permita mejorar las defensas en ciberseguridad.

Introducción a la seguridad en la nube

Seguridad en la nube

Fuente: HyTrust

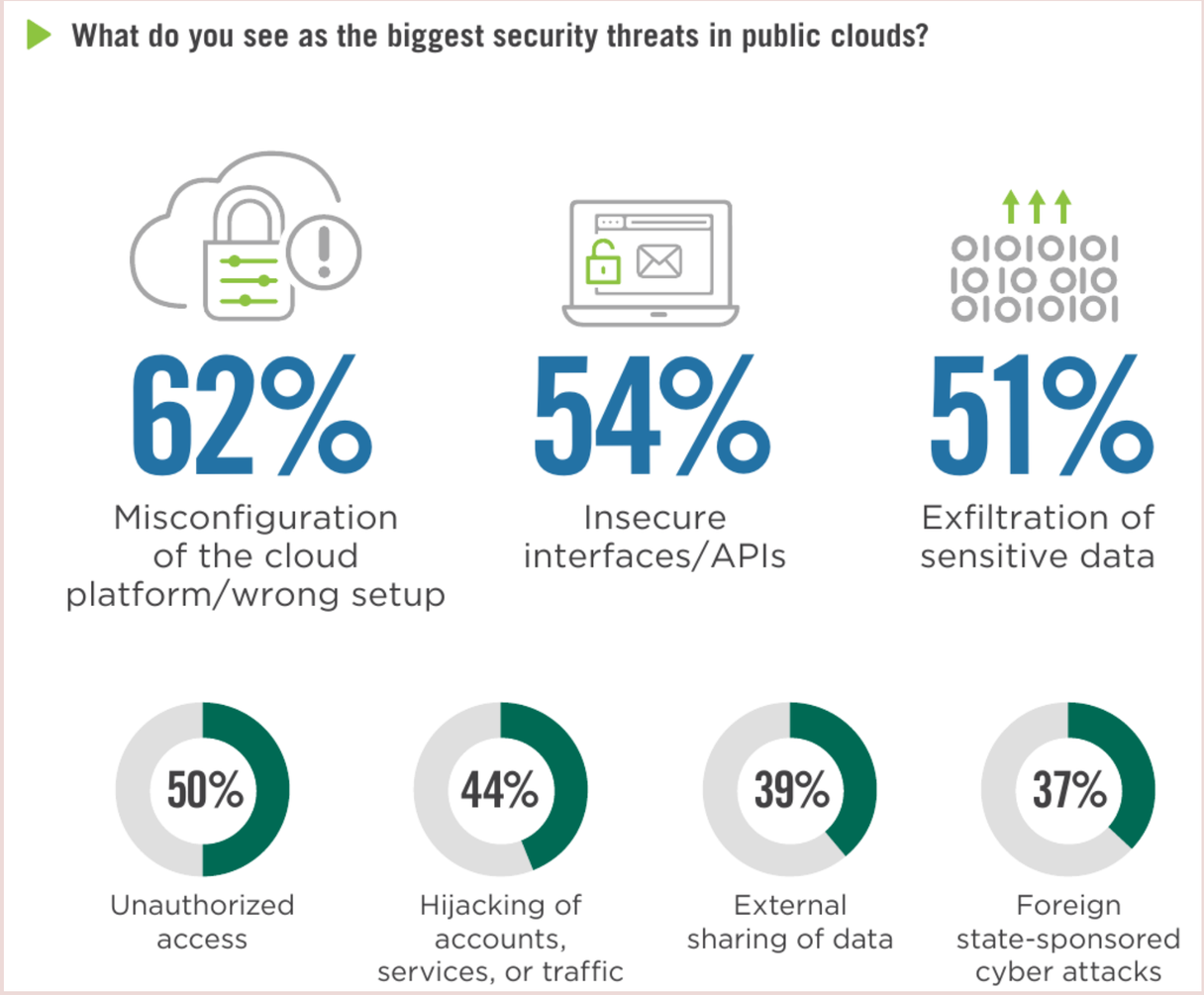
Seguridad tradicional vs seguridad en la nube



Fuente: bmc.com

Desafíos de la seguridad en la nube

Amenazas de seguridad



Fuente: Cloud Security Report 2022 - Cybersecurity Insiders & ISC2

Desafíos de la seguridad en la nube

Aseguramiento de entornos

Fuente: Cloud Security Report 2022 - Cybersecurity Insiders & ISC2

Estrategias de seguridad en la nube

Evite

Defina los permisos e identificaciones del usuario, las medidas de protección de infraestructura y de protección de datos para lograr una estrategia de adopción de AWS uniforme y planificada.

Detecte

Obtenga visibilidad de la postura de visibilidad de su organización iniciando sesión y monitoreando los servicios. Introduzca esta información en una plataforma escalable para la gestión, las pruebas y la auditoría de eventos.

Responda

Respuesta y recuperación automatizada de incidentes que le ayudan a cambiar el enfoque principal de los equipos de seguridad de responder a analizar la causa raíz.

Solucione

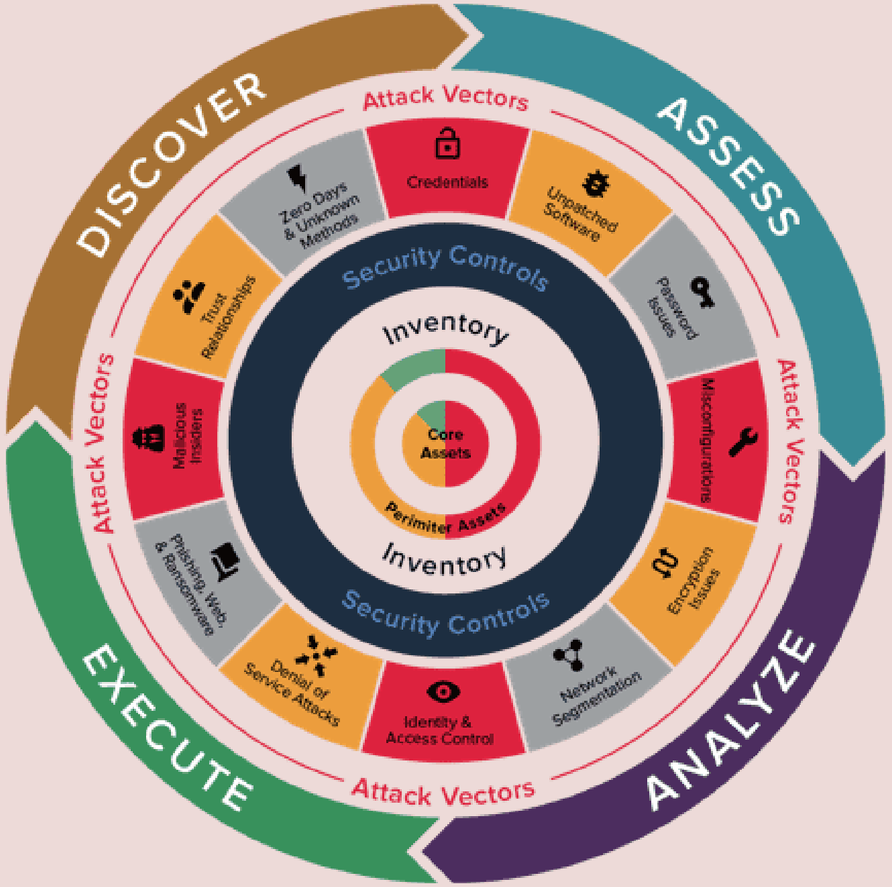
Aproveche la automatización impulsada por eventos para solucionar y asegurar rápidamente su entorno de AWS casi en tiempo real.

Fuente: aws.amazon.com

Introducción a la postura de seguridad

¿Qué es la postura de seguridad?

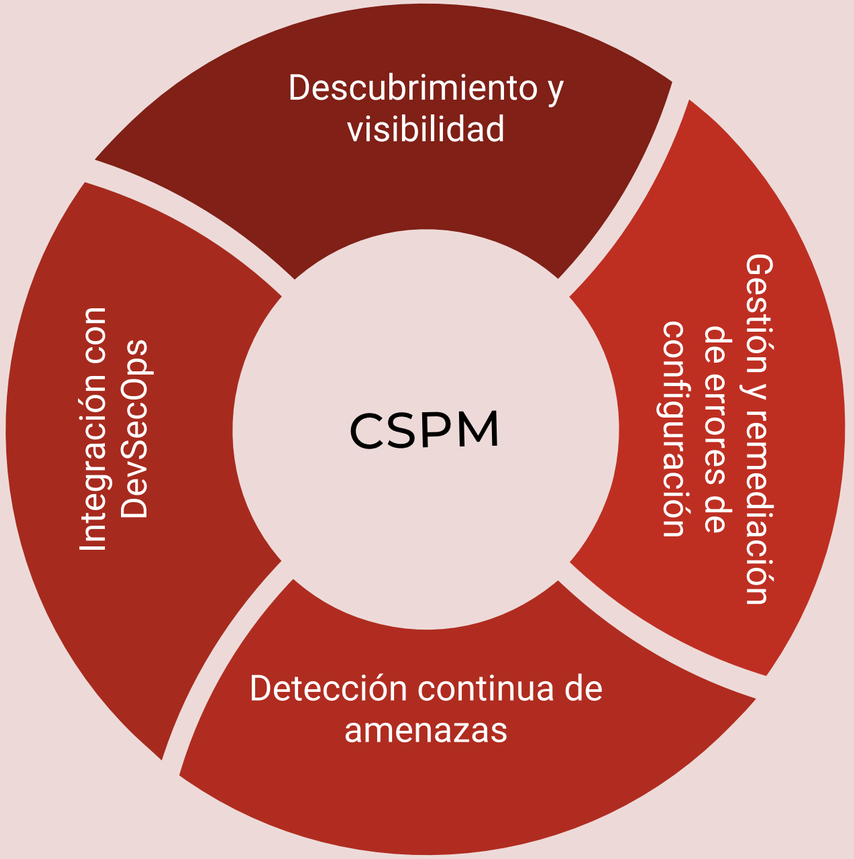
- El nivel de visibilidad de tus activos, controles y superficie de ataque.
- La habilidad de detectar, reaccionar, contener y recuperarte de un evento de seguridad.
- El nivel de respuestas automatizadas de ciberseguridad.



Fuente: balbix.com

Administración de la postura de seguridad en la nube

Un CSPM permite administrar continuamente la seguridad en la nube, ofreciendo capacidades de detección, registro, informes y remediación automatizada de hallazgos de seguridad.



Verificación continua de la postura de seguridad en AWS

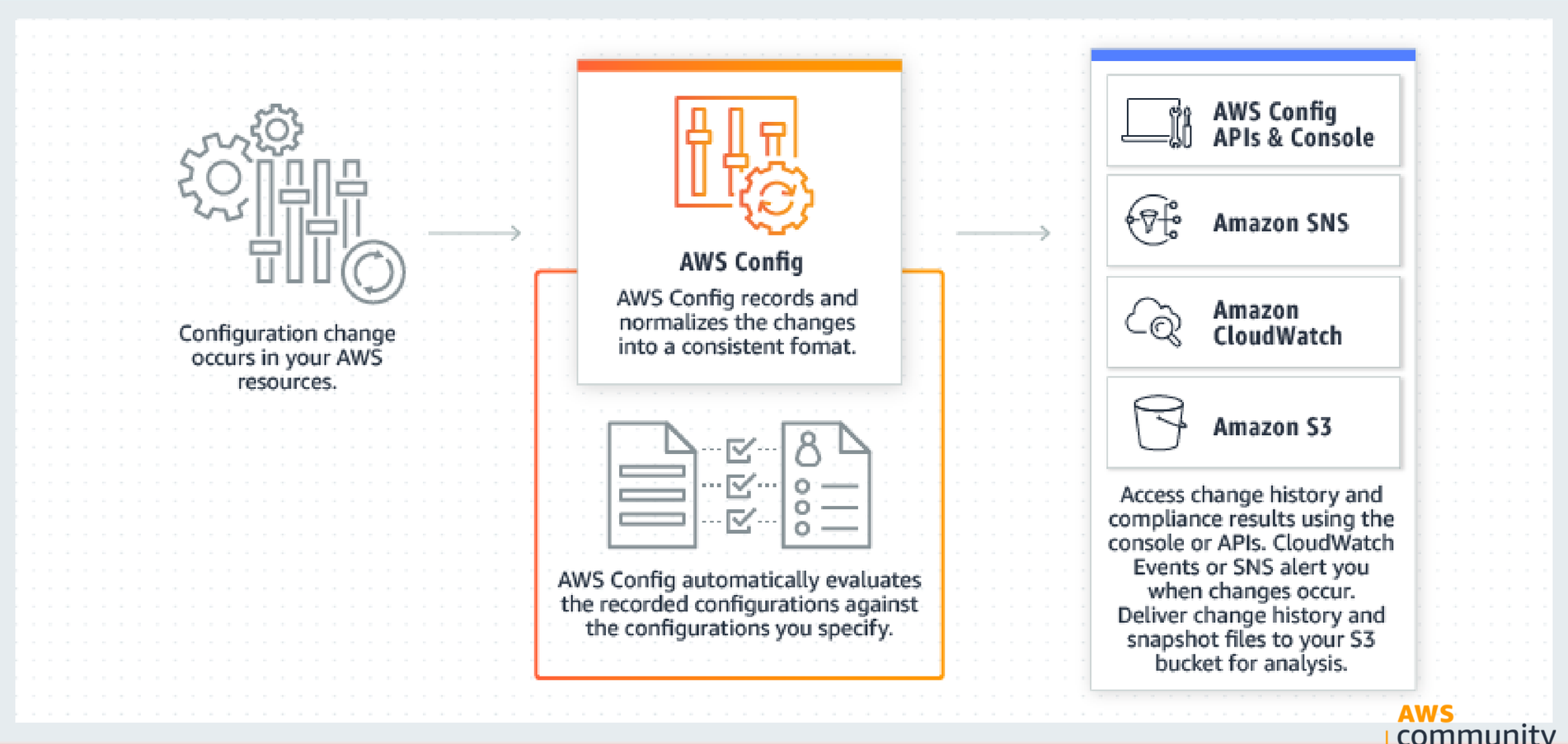
Postura de seguridad en AWS con Security Hub

AWS Security Hub es un servicio de administración de la postura de seguridad en la nube que realiza comprobaciones de las prácticas recomendadas de seguridad, agrega alertas y permite la corrección automática.

Fuente: aws.amazon.com

Evaluación continua de la configuración con AWS Config

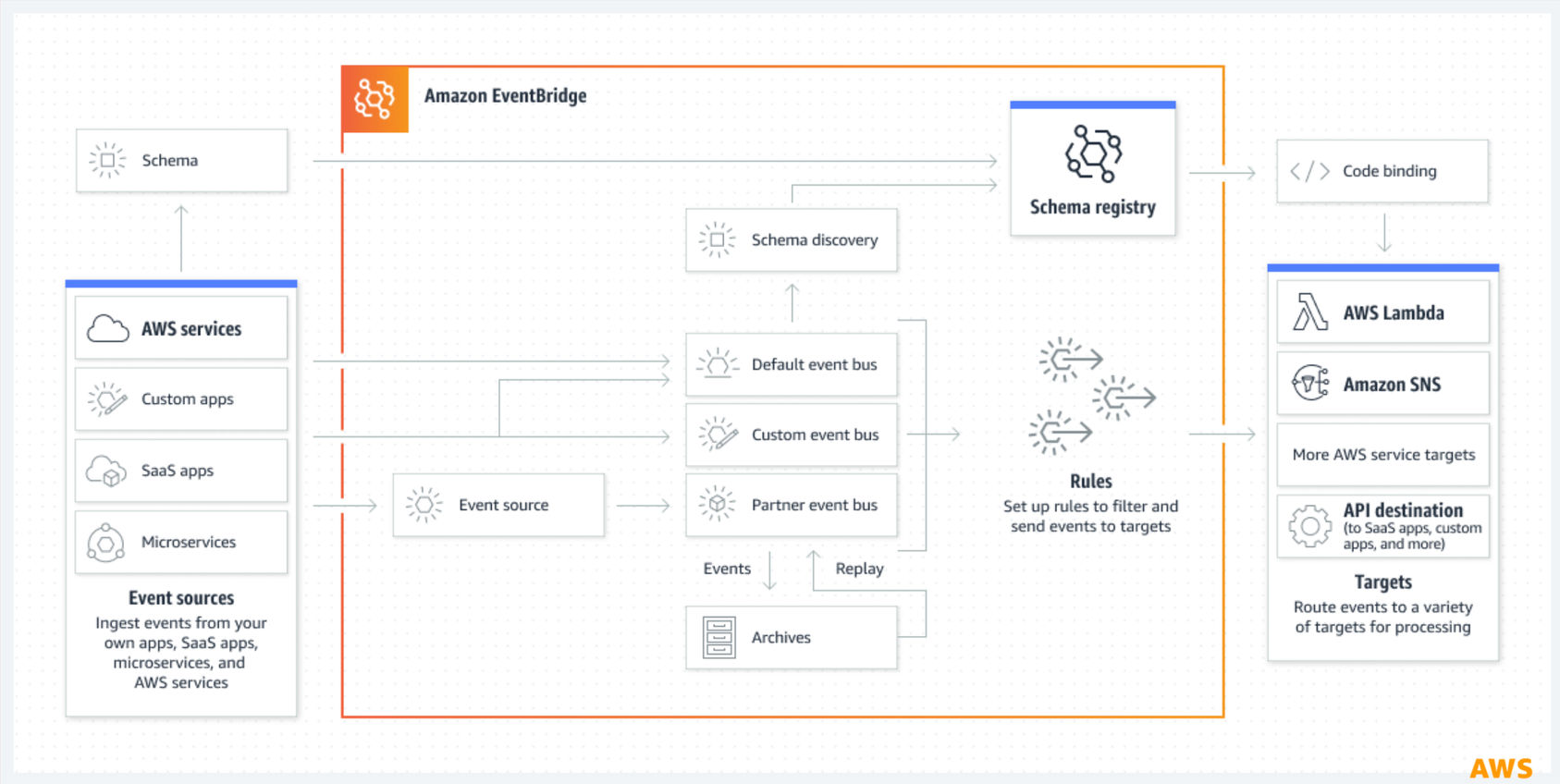
AWS Config analiza, audita y evalúa continuamente las configuraciones y las relaciones de sus recursos.



Fuente: aws.amazon.com

Respuestas en base a eventos con Amazon Eventbridge

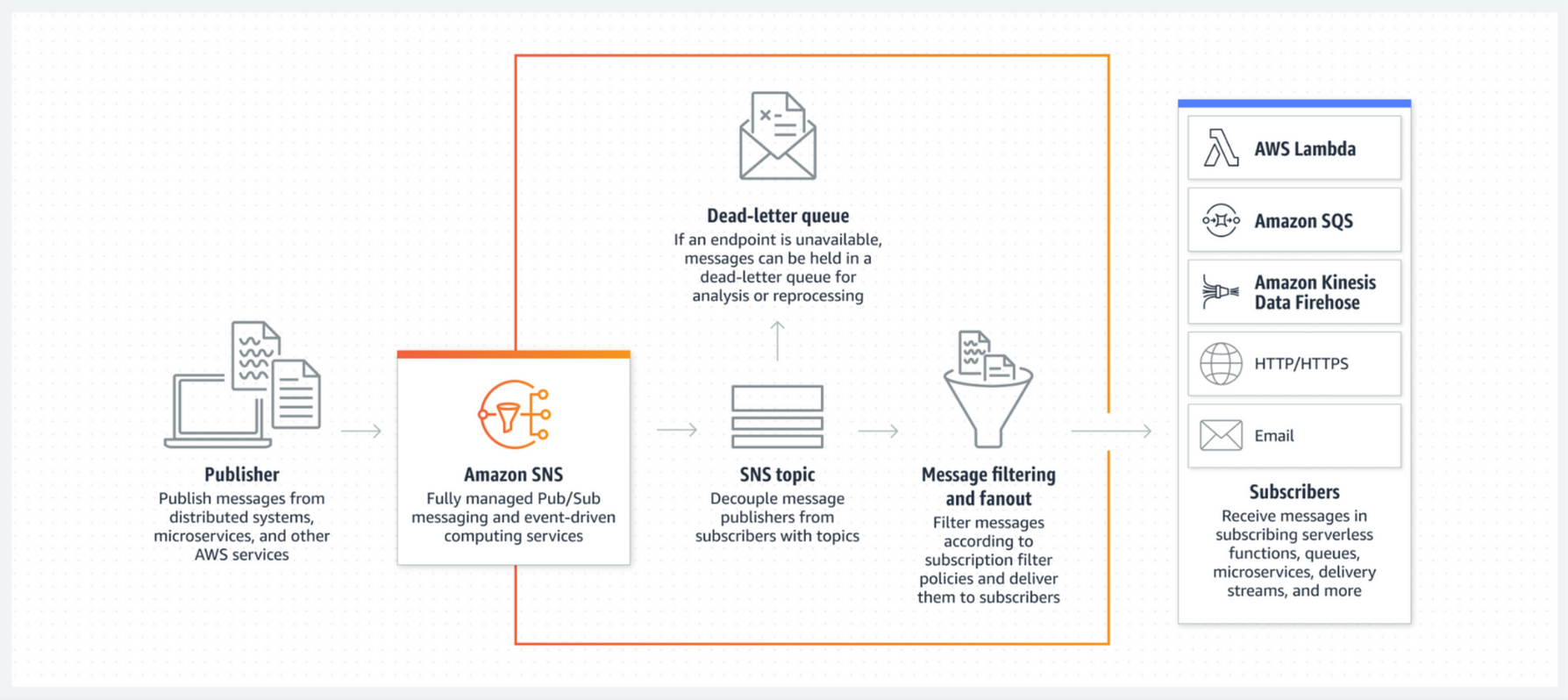
Amazon EventBridge es un bus de eventos sin servidor que le permite recibir, transformar, enrutar y entregar eventos.



Fuente: aws.amazon.com

Notificaciones automáticas con Amazon SNS

Amazon Simple Notification Service (SNS) es un servicio de publicación-suscripción totalmente administrado para mensajería A2A (aplicación a aplicación) y A2P (aplicación a persona).



Fuente: aws.amazon.com

Demostración

Referencias

Recursos de la presentación:
https://github.com/Sheynnie05/Cloudfest2022
Documentación de los servicios expuestos en la presentación:
https://aws.amazon.com/es/security-hub/
https://aws.amazon.com/es/config/
https://aws.amazon.com/es/eventbridge/
https://aws.amazon.com/es/sns/

¡Gracias!

https://www.linkedin.com/in/sheyla-leacock/

shey.lck@gmail.com

@sheynnie_mcr

https://github.com/Sheynnie05/

https://www.wosecpanama.com/

https://comunidaddojo.org/

https://backtrackacademy.com/@Sheyla_Leacock/cursos

https://aws.amazon.com/es/developer/community/community-builders/