Detección continua de amenazas con Amazon GuardDuty

AWS User Group Panamá
Mayo, 2023

Por: Sheyla Leacock

Agenda

- Presentación y objetivo
- Conociendo GuardDuty
    - Arquitectura
    - Casos de uso
    - Fuentes
    - Tipos de escaneos
- Demostración
    - Activación
    - Escaneos a demanda
    - Hallazgos generados
    - Notificación de alertas
- Conclusión
- Referencias

#WHOAMI

- Lic. en Desarrollo de Software (UTP).
- Cursando un Máster en Ciberseguridad, Hacking Ético y Seguridad Ofensiva (UEMC-EIP).
- Co-fundadora de WoSEC Panamá, Embajadora de Comunidad Dojo y Community Builder de AWS.
- Líder DevSecOps e Instructora de cursos de Seguridad Informática.
- Con +9 años de experiencia profesional.
- Ponente internacional en conferencias de Ciberseguridad y Tecnologías.
- Certificaciones en AWS, Ciberseguridad, CCNA, Linux, entre otras.

shey.lck@gmail.com

sheyla-leacock

https://linktr.ee/sheyla_lck

Objetivo

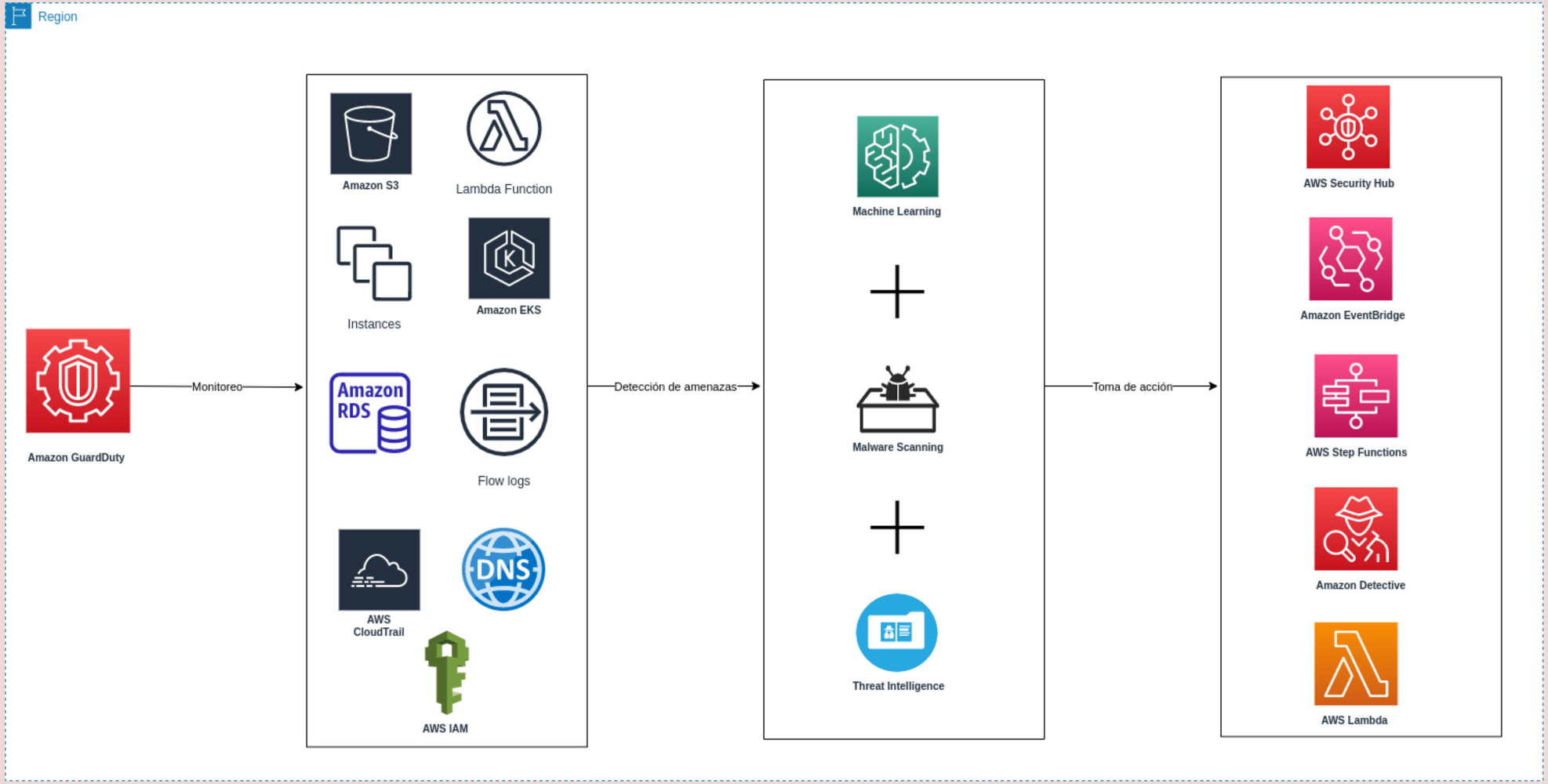
Ejemplificar las capacidades de Amazon GuardDuty para identificar y gestionar amenazas de forma continua en nuestra infraestructura de AWS. Mediante una demostración veremos cómo utilizar estas capacidades y el alcance que podemos tener sobre los diversos recursos.

Disclaimer

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

Conociendo GuardDuty

Amazon GuardDuty



Casos de uso

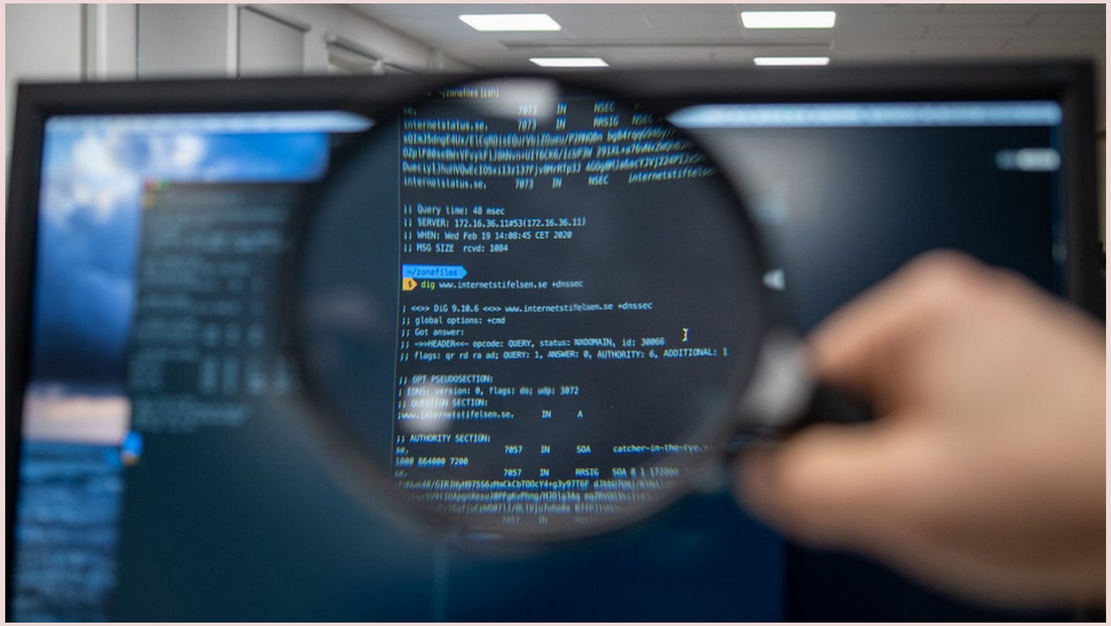
Visibilidad de las operaciones de seguridad
Análisis de investigaciones de seguridad
Identificación de software malicioso
Gestión de hallazgos de seguridad

Fuentes de GuardDuty

Fuentes Fundacionales	Fuentes Adicionales
Se activan automáticamente al habilitar GuardDuty.	Funciones de protección adicionales (no se activan automáticamente).
VPC flow logs	Protección de S3
DNS Logs	Protección de EKS (Registros y Ejecución)
Eventos globales de AWS CloudTrail (API y SDKs)	Protección de Lambda (Registros de actividad de red)
Eventos de administración de AWS CloudTrail	Protección de Malware
-	Protección de RDS

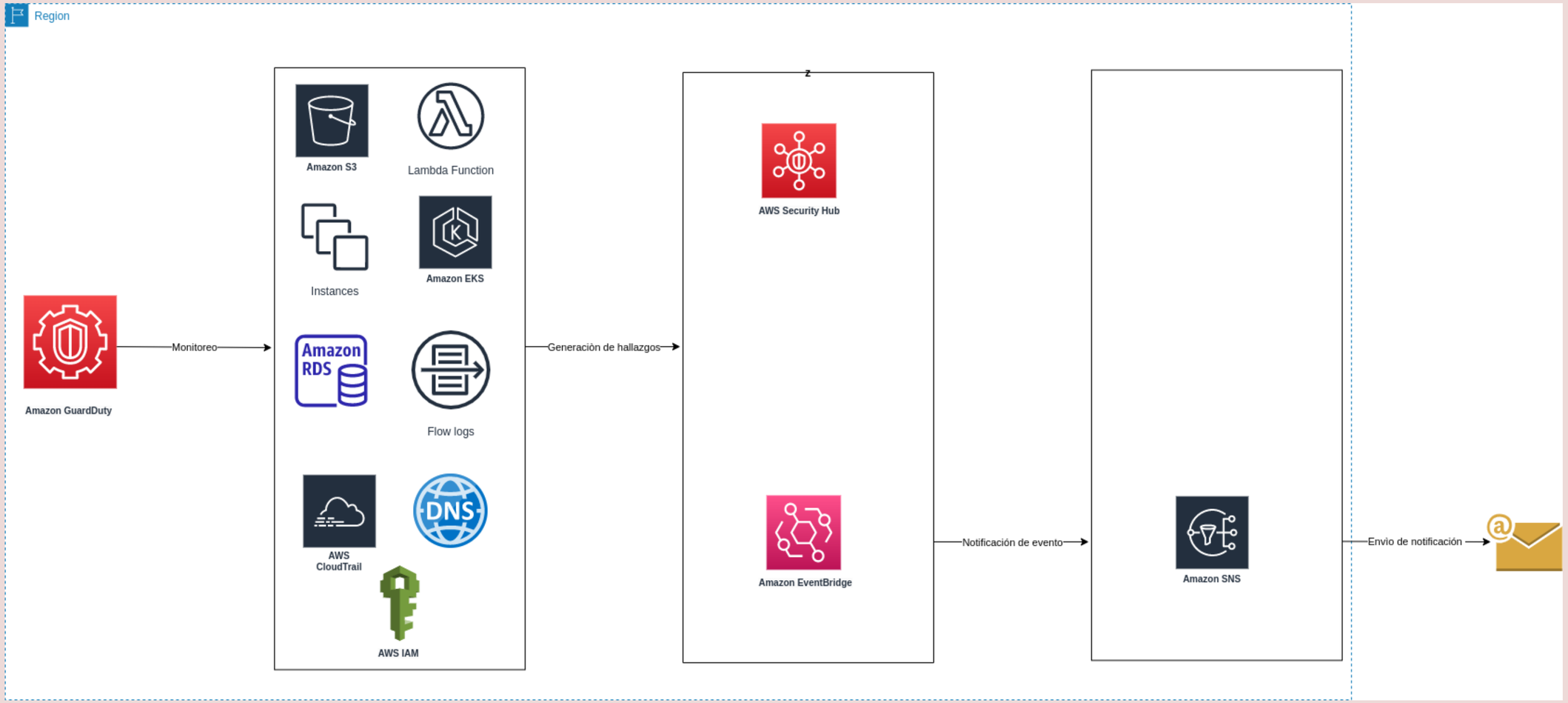
Tipos de escaneos

- Escaneos bajo demanda
- Escaneos iniciados por GuardDuty



Demostración

Arquitectura de demostración



Conclusiones

- Monitorear y auditar de manera continua
- Automatizar la gestión y remediación de hallazgos
- Implementar infraestructura como código (IaC)
- Comprender el alcance de responsabilidades del cliente y del proveedor
- Aplicar el esquema de defensa en profundidad

Referencias

Recursos de la presentación:
https://github.com/Sheynnie05/AWSUGmeetup

Documentación de los servicios expuestos en la presentación:
https://aws.amazon.com/es/guardduty/
https://aws.amazon.com/es/eventbridge/
https://aws.amazon.com/es/sns/

Calculadora de precios de Amazon GuardDuty:
https://calculator.aws/#/addService/guardduty

¡Gracias!

shey.lck@gmail.com

sheyla-leacock

https://linktr.ee/sheyla_lck