aws

COMMUNITY DAY

Introduciendo controles DAST y SAST en nuestra plataforma cloud

Daniel Nieto | 23 Septiembre 2023

aws

COMMUNITY DAY

Daniel Nieto García

Principal Cloud Architect at Axis Data

AWS Community Builder

@droomPMI

aws
COMMUNITY DAY

¿Qué vamos a ver hoy?

- Estrategias DevSecOps
- SAST vs DAST
- SAST on Pipelines: Amazon ECR on push, checkov
- DAST on Platform: Amazon Inspector, Prowler
- Monitorización y remediación: Lambda, Step functions
- Demo 1: Checkov en Pipelines
- Demo 2: Análisis de plataforma con Prowler

aws
COMMUNITY DAY

Estrategias DevSecOps

Beneficios

Reducción de gastos, seguridad y auditoría de cambios, capacidad de recuperación e inmutabilidad.

Buenas prácticas

Implementar controles de seguridad y automatizar el proceso de desarrollo, utilizar versionado de código, análisis de dependencias y utilizar SIEM.

Análisis continuo de la seguridad, tener definido un compliance y procesos y herramientas para poder aplicarlo.

aws
COMMUNITY DAY

SAST vs DAST

Disclaimer: IaC es código.

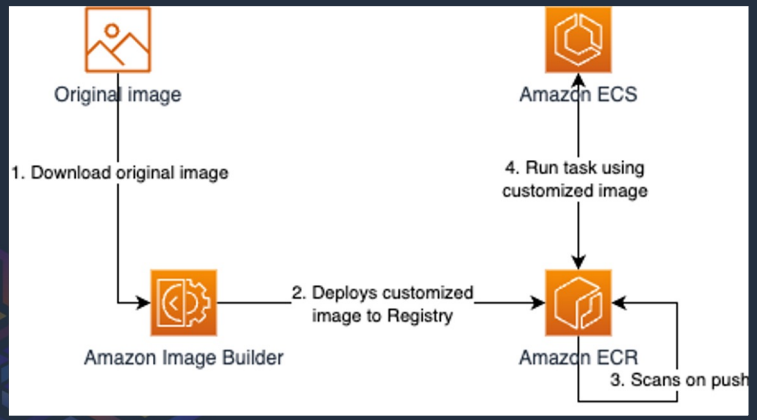
Static Application Security Testing (**SAST**). En las primeras etapas del desarrollo a nivel de código antes de la finalización de la compilación. SonarQube, snyk, ECR on push, checkov…

Dynamic Application Security Testing (**DAST**). Sin acceso al código, revisión de funcionalidades y comportamientos de una aplicación en tiempo de ejecución. sonda+, invicti, Amazon Inspector, Prowler…

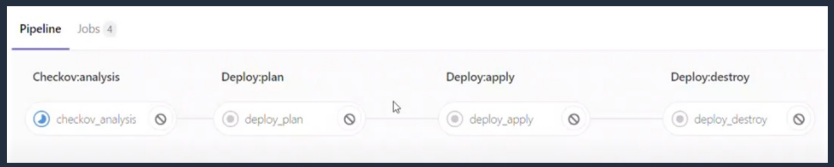
aws
COMMUNITY DAY

SAST on Platform: ECR scan on push, Checkov in pipelines

ECR scan on push



Checkov en pipelines



aws
COMMUNITY DAY

DAST on Platform: Amazon Inspector, Prowler

Amazon Inspector

- Descubrimiento automatizado de cargas de trabajo.
- Análisis continuo.
- Mantenimiento de BD de vulnerabilidades.
- Resultados casi en tiempo real.
- Contextualiza resultados y permite tomar acciones (Security Hub, EventBridge o ECR).

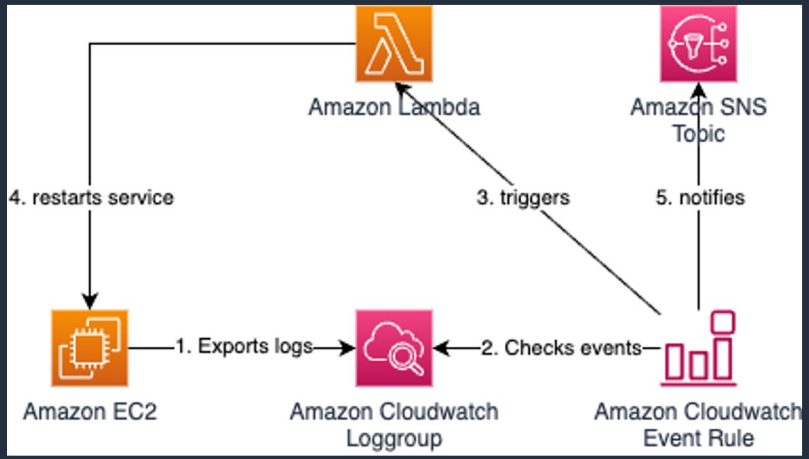
Prowler

- Controles tipo CIS, CISA, PCI-DSS, GDPR, HIPAA, SOC2, AWS Well-Architected Framework Security Pillar or others.
- Controles propios de compliance por servicios y características.
- Resultados en tiempo real.
- Exportable en json, csv, y html5.

aws
COMMUNITY DAY

Monitorización y remediación: Lambda, Step functions

- Exportar logs de sistema, seguridad y aplicación a diferentes Cloudwatch *log groups*
- Establecer roles por grupo de logs
- Crear Cloudwatch *event rules* para comprobar eventos en tiempo real
- Implementar correcciones con Lambdas



aws
COMMUNITY DAY

Demo

checkov
by bridgecrew

aws
COMMUNITY DAY

Demo prowler

aws
COMMUNITY DAY

One More Thing: Otras herramientas DAST y SAST

- **Bandit** para la revisión de la seguridad del código
- **Safety** y **Dependabot** para dependencias
- **Hadolint** y **Dockle** para analizar el código de nuestros contenedores
- **Snyk** para Docker Hub
- **Clair** en Amazon ECR
- **Vulture**, **Flake8**, **Black** y **pylint** para formateo y buenas practicas de Código
- **Intruder** para la supervisión continua de vulnerabilidades y seguridad proactiva

aws
COMMUNITY DAY

¿Preguntas?

¡Gracias!