DEVOPS SENIOR

{desafío}
latam_

CURSO:

DEVOPS SENIOR

- Módulo 1: DEVOPS ESTRATÉGICO Y GITOPS
- Módulo 2: AUTOMATIZACIÓN CON IA EN DEVOPS
- **Módulo 3: SEGURIDAD AVANZADA Y DEVSECOPS**
- Módulo 4: OBSERVABILIDAD AVANZADA
- Módulo 5: KUBERNETES AVANZADO
- Módulo 6: SERVICE MESH & NETWORKING MODERNO

Te encuentras aquí

{desafío} latam_

CURSO:

DEVOPS SENIOR

- Módulo 7: INFRAESTRUCTURA COMO CÓDIGO AVANZADA
- Módulo 8: PLATFORM ENGINEERING & INTERNAL DEVELOPER PLATFORMS (IDP)
- Módulo 9: FINOPS & COST OPTIMIZATION
- Módulo 10: AIOPS & INCIDENT MANAGEMENT
- Módulo 11: SOFT SKILLS PARA ROLES DEVOPS SENIOR
- Módulo 12: PROYECTO FINAL INTEGRADOR

{desafío} latam_

Módulo 3: Seguridad avanzada y DevSecOps.

{desafío} latam_

OBJETIVO ESPECÍFICO DEL MÓDULO

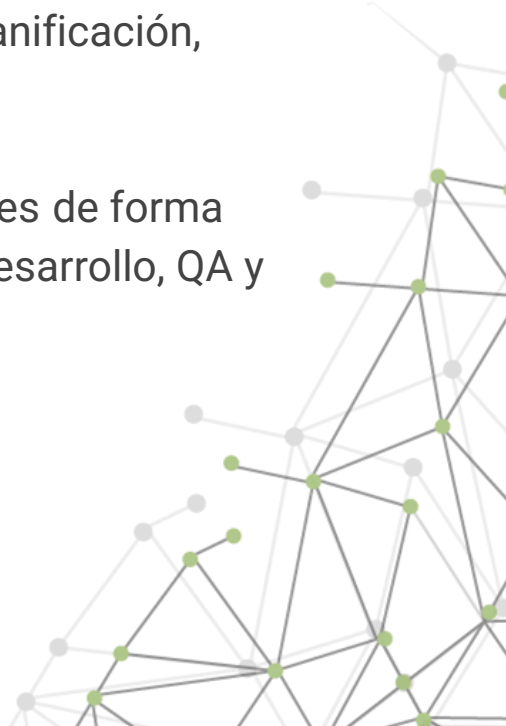
- DEFINIR CONCEPTOS DE SEGURIDAD AVANZADA Y DEVSECOPS, SEGUN LAS PRACTICAS AVANZADAS DE GITOPS, DEVSECOPS, KUBERNETES, OBSERVABILIDAD, IAC, FINOPS Y AIOPS.

¿Qué aspectos de seguridad cree que se deben automatizar en el ciclo de vida del software para evitar vulnerabilidades antes de que lleguen a producción?

DEVSECOPS

- DevSecOps es la evolución del modelo DevOps con enfoque en incorporar la seguridad desde el inicio del ciclo de desarrollo. En lugar de aplicar controles al final, se integran escaneos, validaciones y auditorías en las etapas de planificación, codificación, pruebas y despliegue.

- Este enfoque reduce la superficie de ataque, detecta vulnerabilidades de forma temprana y promueve una cultura de seguridad compartida entre desarrollo, QA y operaciones.



SNYK, TRIVY, CHECKOV, VAULT

- Existen herramientas clave que permiten automatizar la seguridad en diferentes capas del ecosistema DevOps:

- Snyk analiza dependencias de código y contenedores en busca de vulnerabilidades conocidas.

- Trivy permite escanear imágenes, repositorios y archivos de configuración como Dockerfiles y Kubernetes YAML.

{desafío} latam_

- Checkov evalúa IaC (Infrastructure as Code) en busca de errores de seguridad y malas prácticas.

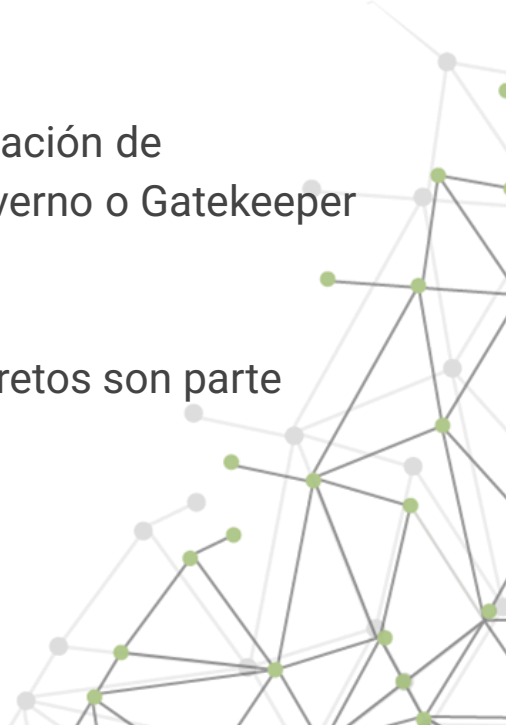
- Vault gestiona secretos y credenciales de forma centralizada, cifrada y con control de acceso, evitando filtraciones accidentales.

SEGURIDAD EN KUBERNETES

- La seguridad en clústeres Kubernetes incluye la configuración de RBAC (control de acceso basado en roles), políticas de red, escaneo de imágenes y restricciones a nivel de pods.

- También se aplican mecanismos como namespaces aislados, validación de manifiestos con Open Policy Agent (OPA), y herramientas como Kyverno o Gatekeeper para imponer reglas de seguridad.

- El monitoreo continuo del clúster y la rotación de certificados y secretos son parte esencial de una arquitectura segura en producción.



{desafío} latam_

No olvide desarrollar los ejercicios que contiene el Módulo…

{desafío} latam_

¿Cómo integraría herramientas de análisis de seguridad como Snyk, Trivy, Checkov y Vault en su flujo DevOps sin afectar la velocidad de despliegue ni la experiencia del equipo de desarrollo?

{desafío} latam_

Éxito en la evaluación parcial y en la Prueba Final...

{desafío}
latam_

Academia de
talentos digitales