CURSO: DEVOPS SENIOR

Módulo 3: Seguridad avanzada y DevSecOps

Ejercicio Práctico 1

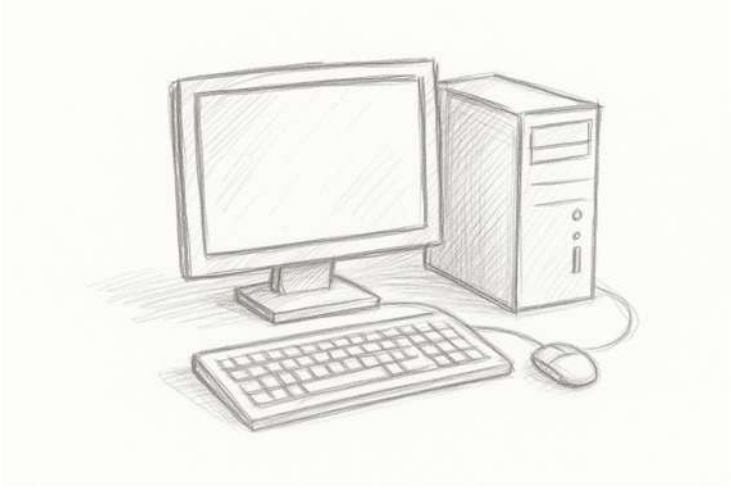
Auditoría y Corrección de Vulnerabilidades en Imágenes y Manifiestos Kubernetes con Trivy, Snyk y Checkov

Objetivo:

Aplicar herramientas DevSecOps para detectar y corregir vulnerabilidades en contenedores, dependencias y configuración de infraestructura como código (IaC), en un flujo realista de despliegue sobre Kubernetes.

Resultado esperado:

Integrar herramientas reales en un flujo seguro de revisión de contenedores, IaC y código fuente, aprendiendo a interpretar reportes, priorizar riesgos y corregir vulnerabilidades en un entorno real.



INSTRUCCIONES:

Preparación del entorno:

- Instale Docker Desktop o usa Play with Kubernetes.
- Cree cuenta gratuita en Snyk y configura el CLI (npm install -g snyk).
- Instale Trivy (brew install aquasecurity/trivy/trivy) y Checkov (pip install checkov).

Escenario:

- Clone este repo vulnerable:
  https://github.com/snyk-labs/node-goof
  (contiene fallas de seguridad en Node.js y configuración de Docker y Kubernetes).

Actividad práctica:

Escanea la imagen del contenedor con Trivy (trivy image node-goof).

- Escanee el código fuente con Snyk (snyk test) e integre el proyecto en el dashboard de Snyk para seguimiento.
- Audite los manifiestos YAML con Checkov (checkov -d ./k8s-manifests).
- Registre los hallazgos principales (CVEs, errores de configuración, secretos expuestos, uso de latest, etc).
- Aplique al menos 3 correcciones efectivas en el repositorio local y vuelva a escanear para verificar que desaparecen.

Feedback técnico esperado:

- Comparación entre resultados antes y después de los fixes.
- Análisis de qué tipos de errores son comunes: ¿paquetes desactualizados?, ¿configuraciones permisivas?, ¿secretos hardcodeados?
- Evaluación del nivel de cumplimiento de buenas prácticas DevSecOps.