

Resumen Módulo 4 - Seguridad en Contenedores y Kubernetes

Este documento forma parte del portafolio profesional de Nadia Arellano, participante del Bootcamp "Seguridad Cloud" otorgado por Talento Digital y SENCE, impartido por OTEC EDUTECNO.

Objetivos del módulo 4:

- Comprender y aplicar conceptos clave de seguridad en contenedores y clústeres de Kubernetes.
- Identificar riesgos y buenas prácticas al ejecutar contenedores.
- Implementar herramientas de escaneo y monitoreo como Trivy, Falco, Kube-bench y OPA Gatekeeper.
- Gestionar políticas de red, RBAC, secretos y configuraciones seguras dentro de un entorno Kubernetes.

Contenidos clave:

- Aislamiento y control de recursos mediante namespaces y cgroups.
- Escaneo de vulnerabilidades con Trivy y cumplimiento CIS con Kube-bench.
- Monitoreo de actividad en tiempo real con Falco y visualización con Prometheus y Grafana.
- Gestión de secretos, RBAC, políticas de red y mínimos privilegios.
- Aplicación del enfoque GitOps y uso de herramientas como Renovate y Anchore.
- Análisis estático de código (SAST) en pipelines CI/CD.

Evidencias incluidas en este módulo:

- Actividades resueltas de las seis sesiones del módulo.
- Evaluación final con respuestas justificadas.
- Este mismo resumen, que incluye una reflexión sobre el impacto del módulo en el desarrollo profesional.

Reflexión personal:

Este módulo 4 me permitió afianzar mis conocimientos en la seguridad de entornos basados en contenedores, adquiriendo habilidades prácticas en la detección, prevención y monitoreo de amenazas en Kubernetes. La integración de herramientas como Falco y Trivy fortaleció mi capacidad de respuesta ante incidentes, y la implementación de políticas con OPA Gatekeeper me dio una visión más avanzada sobre el control de acceso y cumplimiento. Este aprendizaje refuerza mi perfil profesional en DevSecOps y me posiciona para asumir nuevos desafíos en la protección de infraestructuras modernas.