Nadia Arellano
Ingeniera en Informática

Actividad Práctica – Sesión 5 – Módulo 4

Pregunta 1

¿Qué es el monitoreo de ductos en CI/CD?
Respuesta correcta: a. Un proceso para detectar fallos de seguridad y accesos no autorizados en tiempo real.

Explicación: El monitoreo de pipelines en CI/CD permite identificar incidentes y garantizar la integridad del sistema, detectando fallos o accesos indebidos en tiempo real.

Pregunta 2

¿Cuál de las herramientas se utiliza para recopilar métricas en tiempo real en tuberías de CI/CD?
Respuesta correcta: b. Prometeo

Explicación: Prometheus recopila métricas y permite configurar alertas basadas en umbrales definidos para entornos cloud-native.

Pregunta 3

¿Qué tipo de actividad puede detectar Falco en una tubería de CI/CD?
Respuesta correcta: c. Actividades sospechosas o comportamientos anómalos en contenedores.

Explicación: Falco detecta comportamientos no esperados en contenedores, como accesos indebidos o comandos maliciosos.

Pregunta 4

¿Qué significa SAST en el contexto de la seguridad de ductos?
Respuesta correcta: b. Análisis estático del código fuente sin ejecutarlo.

Explicación: SAST revisa el código en reposo para detectar vulnerabilidades sin necesidad de ejecutarlo.

Pregunta 5

¿Qué herramienta se utiliza para visualizar métricas recopiladas por Prometheus?
Respuesta correcta: a. Grafana

Explicación: Grafana permite crear dashboards con métricas monitoreadas por Prometheus, facilitando la observación del pipeline.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Cuál de las siguientes afirmaciones describe mejor el propósito de las políticas de revisión en imágenes de contenedores?
Respuesta correcta: b. Asegurar que solo imágenes validadas y seguras se desplieguen en producción.

Explicación: Las políticas de revisión permiten prevenir el uso de imágenes vulnerables o mal configuradas en entornos de producción.

Pregunta 7

¿Qué es RBAC en el contexto de pipelines de CI/CD?
Respuesta correcta: a. Un mecanismo para controlar quién puede realizar qué acciones en el pipeline.

Explicación: RBAC asigna permisos por rol, limitando las acciones según el perfil del usuario, aplicando el principio de menor privilegio.

Pregunta 8

¿Qué herramienta se utiliza para detectar vulnerabilidades en imágenes de contenedores antes de su despliegue?
Respuesta correcta: a. Trivy

Explicación: Trivy escanea imágenes de contenedor para identificar vulnerabilidades en bibliotecas o paquetes antes del despliegue.

Pregunta 9

¿Qué tipo de alerta generaría Prometheus si se detecta un fallo crítico en el pipeline?
Respuesta correcta: a. Una alerta basada en reglas predefinidas, como un umbral de fallos excedido.

Explicación: Prometheus puede generar alertas automáticas cuando se exceden condiciones críticas, como tiempos de ejecución o errores acumulados.

Pregunta 10

¿Qué es GitOps en el contexto de la gestión de cambios en imágenes de contenedores?
Respuesta correcta: b. Una metodología que utiliza repositorios de control de versiones como fuente única de verdad.

Explicación: GitOps gestiona la infraestructura y aplicaciones desde Git como fuente única, aplicando automatización con herramientas como Argo CD.