Nadia Arellano
Ingeniera en Informática

Actividad Práctica – Sesión 6 – Módulo 4

Pregunta 1

¿Cuál es el propósito principal de analizar informes de seguridad generados por herramientas como Falco o Trivy?
Respuesta correcta: a. Identificar vulnerabilidades en tiempo real y tomar medidas correctivas.

Explicación: El análisis de informes de seguridad permite detectar actividades sospechosas, vulnerabilidades y configuraciones inseguras en entornos de contenedores.

Pregunta 2

¿Qué acción es recomendable cuando Falco genera una alerta sobre la apertura de un shell interactivo en un contenedor?
Respuesta correcta: c. Investigar si el acceso fue autorizado y ajustar políticas de control de acceso.

Explicación: La apertura de un shell interactivo puede ser legítima o indicar un intento de escalada de privilegios. Es crucial investigar el contexto y restringir el uso de kubectl exec en entornos productivos.

Pregunta 3

¿Qué herramienta se utiliza para escanear imágenes de contenedores en busca de vulnerabilidades conocidas?
Respuesta correcta: b. Trivy

Explicación: Trivy es una herramienta especializada en escanear imágenes de contenedores para identificar vulnerabilidades conocidas (CVE).

Pregunta 4

¿Qué significa aplicar el principio de "mínimo privilegio" en Kubernetes?
Respuesta correcta: b. Restringir permisos y capacidades a lo estrictamente necesario.

Explicación: Este principio implica otorgar solo los permisos necesarios para que un contenedor funcione correctamente, reduciendo así la superficie de ataque.

Pregunta 5

¿Qué herramienta se utiliza para verificar si un clúster Kubernetes cumple con las CIS Benchmarks?
Respuesta correcta: d. Kube-bench

Explicación: Kube-bench evalúa la configuración de un clúster Kubernetes contra las mejores prácticas de seguridad definidas en las CIS Benchmarks.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Qué política de red en Kubernetes permite segmentar el tráfico entre contenedores?
Respuesta correcta: d. Políticas de red

Explicación: Las Políticas de Red permiten definir reglas de comunicación entre pods, asegurando que solo los contenedores autorizados puedan interactuar entre sí.

Pregunta 7

¿Qué acción es recomendable para proteger secrets en Kubernetes?
Respuesta correcta: c. Montar secrets como volúmenes de solo lectura.

Explicación: Esta opción reduce el riesgo de exposición accidental en comparación con el uso de variables de entorno.

Pregunta 8

¿Qué herramienta se utiliza para automatizar la actualización de dependencias en Dockerfiles?
Respuesta correcta: d. Renovate

Explicación: Renovate automatiza la actualización de dependencias en Dockerfiles, Helm charts y archivos de configuración, manteniéndolos actualizados y seguros.

Pregunta 9

¿Qué perfil de Pod Security Standards en Kubernetes es más restrictivo?
Respuesta correcta: c. Restricted

Explicación: El perfil Restricted aplica políticas más estrictas, prohibiendo contenedores privilegiados, eliminando capacidades y forzando sistemas de archivos de solo lectura.

Pregunta 10

¿Qué herramienta se utiliza para definir políticas de seguridad personalizadas en Kubernetes usando el lenguaje Rego?
Respuesta correcta: b. OPA Gatekeeper

Explicación: OPA Gatekeeper permite definir políticas de seguridad personalizadas en Kubernetes usando el lenguaje Rego, restringiendo el uso de imágenes no aprobadas, limitando recursos, entre otras reglas.