Kubernetes Security Specialist (CKS)

Temario

1. Configuración del clúster
   - 1.1 Usar directivas de seguridad de red para restringir el acceso a nivel de clúster
   - 1.2 Utilice el benchmark CIS para revisar la configuración de seguridad de los componentes de Kubernetes (etcd, kubelet, kubedns, kubeapi)
   - 1.3 Configurar correctamente los objetos de entrada con control de seguridad
   - 1.4 Proteger los metadatos y los puntos finales del nodo
   - 1.5 Minimice el uso y el acceso a los elementos de la GUI
   - 1.6 Comprobar los archivos binarios de la plataforma antes de implementar

2. Cluster Hardering
   - 2.1 Restringir el acceso a la API de Kubernetes
   - 2.2 Usar controles de acceso basados en roles para minimizar la exposición
   - 2.3 Tenga cuidado al usar cuentas de servicio, por ejemplo, deshabilite los valores predeterminados, minimice los permisos en los recién creados
   - 2.4 Actualice Kubernetes con frecuencia

3. System Hardering
   - 3.1 Minimice la huella del sistema operativo del host (reduzca la superficie de ataque)
   - 3.2 Minimizar los roles de IAM
   - 3.3 Minimizar el acceso externo a la red
   - 3.4 Utilice adecuadamente herramientas de protección del kernel como AppArmor, seccomp

4. Minimice las vulnerabilidades de los microservicios
   - 4.1 Configurar dominios de seguridad apropiados a nivel de sistema operativo, por ejemplo, utilizando PSP, OPA, contextos de seguridad
   - 4.2 Administrar secretos de kubernetes
   - 4.3 Usar entornos aislados de tiempo de ejecución de contenedores en entornos multiinquilino (por ejemplo, gvisor, contenedores de kata)
   - 4.4 Implementar el cifrado pod to pod mediante el uso de mTLS

5. Seguridad de la cadena de suministro
   - 5.1 Minimice la huella de imagen base
   - 5.2 Asegure su cadena de suministro: incluya en la lista blanca los registros de imágenes permitidos, firme y valide imágenes
   - 5.3 Utilice el análisis estático de las cargas de trabajo de los usuarios (por ejemplo, recursos de kubernetes, archivos Docker)
   - 5.4 Escanear imágenes en busca de vulnerabilidades conocidas

6. Supervisión, registro y seguridad en tiempo de ejecución
   - 6.1 Realizar análisis de comportamiento de las actividades de archivos y procesos syscall a nivel de host y contenedor para detectar actividades maliciosas
   - 6.2 Detecte amenazas dentro de la infraestructura física, aplicaciones, redes, datos, usuarios y cargas de trabajo

6.3 Detecte todas las fases del ataque, independientemente de dónde ocurra y cómo se propague
6.4 Realizar una investigación analítica profunda y la identificación de malos actores dentro del entorno
6.5 Garantice la inmutabilidad de los contenedores en tiempo de ejecución
6.6 Usar registros de auditoría para supervisar el acceso