Seis prácticas recomendadas de DevSecOps para desarrolladores

1 Reduzca los riesgos de las dependencias de las aplicaciones

Es posible que haya puntos vulnerables en los elementos de software utilizados para diseñar las aplicaciones que necesitan gestión. Para reducir los riesgos de la cadena de suministro del software, en particular con los elementos de software open source, pueden usarse herramientas del análisis de composición del software (SCA). Asegúrese de que las herramientas de SCA que utilice:

- Analicen las dependencias de las aplicaciones para garantizar que no tengan puntos vulnerables conocidos.
- Permitan automatizar el cumplimiento de las licencias de software al identificar los elementos y sus licencias y advertir sobre aquellas que podrían no ser compatibles.
- Confirmen que las dependencias de las aplicaciones sean actuales y que provengan de una comunidad activa que produce actualizaciones.
- Sean una parte automatizada del proceso de diseño de las aplicaciones, así como del entorno de desarrollo, lo cual les da a los desarrolladores la oportunidad de resolver problemas antes de la integración y, de esta manera, reducir la cantidad de fallos en el proceso.

2 Unifique el código y la gestión de la configuración

En el paradigma de GitOps, que es muy usado en Kubernetes y en los entornos en contenedores, se incluyen prácticas capaces de mejorar en gran medida la estrategia de seguridad desde el desarrollo:

- Aplique las prácticas recomendadas de desarrollo para la gestión del código fuente (SCM) a la configuración. El uso de las mismas herramientas para el ingreso, la fusión y la aprobación permite conocer la persona y la hora específicas asociadas a los cambios en la configuración de la infraestructura.
- En lugar de confiar en las operaciones, los desarrolladores deben considerar la configuración en una etapa temprana del proceso y establecer un panorama para el entorno de producción previsto de la aplicación. Al usar el mismo tipo de entorno y controles para la seguridad en el desarrollo, las pruebas y la producción, resulta más sencillo gestionar la configuración en todo el ciclo de vida.
- Utilice un canal automatizado para crear las imágenes de contenedores y los elementos binarios para la integración y la distribución continuas (CI/CD). No deben necesitarse cambios específicos al momento de implementar estas imágenes en la producción.
- No almacene datos confidenciales en un sistema de SCM. Utilice herramientas que analicen la configuración y las imágenes de contenedores para asegurarse de que no contienen secretos integrados.

3 Proteja los secretos de las aplicaciones

Es importante gestionar las identidades y los secretos como las contraseñas, los tokens y las claves en todo el ciclo de vida de las aplicaciones. El acceso a los sistemas de SCM, los registros de contenedores y los repositorios binarios deben supervisarse. También es necesario proteger las credenciales que utilizan las aplicaciones para acceder a las bases de datos y los servicios, así como aquellas necesarias para los diseños automatizados y los procesos de pruebas. Los secretos pueden divulgarse por accidente si están almacenados en sistemas de SCM o archivos de configuración. Para proteger los secretos de las aplicaciones:

- Establezca una infraestructura de gestión de las identidades y control de acceso en una etapa temprana del ciclo de vida.
- Considere el uso de un almacén de secretos o un módulo de seguridad de hardware (HSM) para gestionar y proteger los secretos cuando están en reposo o en tránsito. Los almacenes de secretos suelen ser soluciones de software, mientras que los HSM utilizan hardware especializado para aumentar la protección. Ambos se deben integrar en la infraestructura de gestión de las identidades.

4 Elija imágenes de base confiables

Las imágenes de base de contenedores son distribuciones de Linux® sumamente ligeras. Se pueden preinstalar cientos de paquetes, los cuales pueden contener posibles puntos vulnerables. Para reducir el riesgo de las imágenes de contenedores:

- Elija imágenes confiables con actualizaciones conocidas, periódicas y debidamente probadas. Investigue las fuentes de la imagen y las opciones de soporte disponibles.
- Utilice herramientas de imágenes para verificar si hay puntos vulnerables conocidos. Las imágenes también deben analizarse para comprobar que las configuraciones sean seguras y que no haya secretos integrados.
- Reduzca los vectores de ataque mediante la eliminación de archivos binarios innecesarios, como las herramientas del sistema operativo (OS), que podrían utilizarse durante un ataque.

5 Aborde el cumplimiento normativo y los problemas de auditoría de forma anticipada

Para reducir los riesgos al momento del traslado a la producción, es importante entender que los marcos de cumplimiento y los controles técnicos se requieren en una etapa temprana del desarrollo. Las verificaciones automatizadas para aplicar el cumplimiento y los requisitos de seguridad se pueden integrar en el canal de diseño.

Comience a documentar los procedimientos y las políticas con antelación, ya que esta documentación puede abarcar el 50 % de una auditoría como mínimo. La documentación sobre las políticas debe incluir los controles de acceso y de cambios, los backups y la retención de datos. Las verificaciones de seguridad, como las pruebas de seguridad de las aplicaciones y los SCA, se deben incluir al momento de documentar los procedimientos.

6 Comience con una plataforma y un ecosistemas sólidos

Con el aumento permanente de las amenazas de seguridad, es fundamental usar una plataforma con un ecosistema de seguridad completo que ofrezca soluciones integradas y con soporte. Red Hat® OpenShift® es una plataforma de Kubernetes empresarial con muchas funciones para respaldar el desarrollo y las operaciones. Los potentes canales de diseño e implementación en Red Hat OpenShift brindan un entorno ideal para implementar verificaciones y controles de seguridad automatizados. Las verificaciones de seguridad pueden integrarse en cualquier parte del proceso, desde el diseño de imágenes con código fuente hasta la implementación de la producción.

Red Hat tiene un ecosistema de partners que optimizan y amplían las funciones de seguridad en Red Hat OpenShift. Estos partners trabajan con Red Hat para ofrecer soluciones compatibles que se integran con Red Hat OpenShift. Puede elegir de entre una variedad de soluciones aquellas que se adapten a sus requisitos específicos empresariales y de seguridad.

Red Hat CodeReady Workspaces es un entorno de desarrollo de Kubernetes que se ejecuta en Red Hat OpenShift y le permite agilizar el desarrollo de las aplicaciones basadas en contenedores. Red Hat Universal Base Images y Red Hat Runtimes proporcionan una base sólida para sus aplicaciones que proviene de una fuente confiable.

Marco de DevSecOps de Red Hat

Obtenga un panorama integral del ciclo de vida de la seguridad y conozca la manera en que las funciones de desarrollo de seguridad se adaptan al marco de DevSecOps de Red Hat. Visite red.ht/DevSecOps.

Conozca las soluciones de desarrollo de seguridad

Vea webinars de Red Hat y sus partners de seguridad para conocer la manera de incorporar la seguridad en todo el ciclo de vida de las aplicaciones.

Acerca de Red Hat

Con Red Hat, los clientes pueden llevar la estandarización a todos los entornos; desarrollar aplicaciones directamente en la nube; e integrar, automatizar, proteger y gestionar los entornos complejos a través de servicios galardonados de soporte, capacitación y consultoría.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

Argentina
+54 11 4329 7300

Chile
+562 2597 7000

Colombia
+571 508 8631
+52 55 8851 6400

México
+52 55 8851 6400

España
+34 914 148 800

es.redhat.com
#F29682_0921