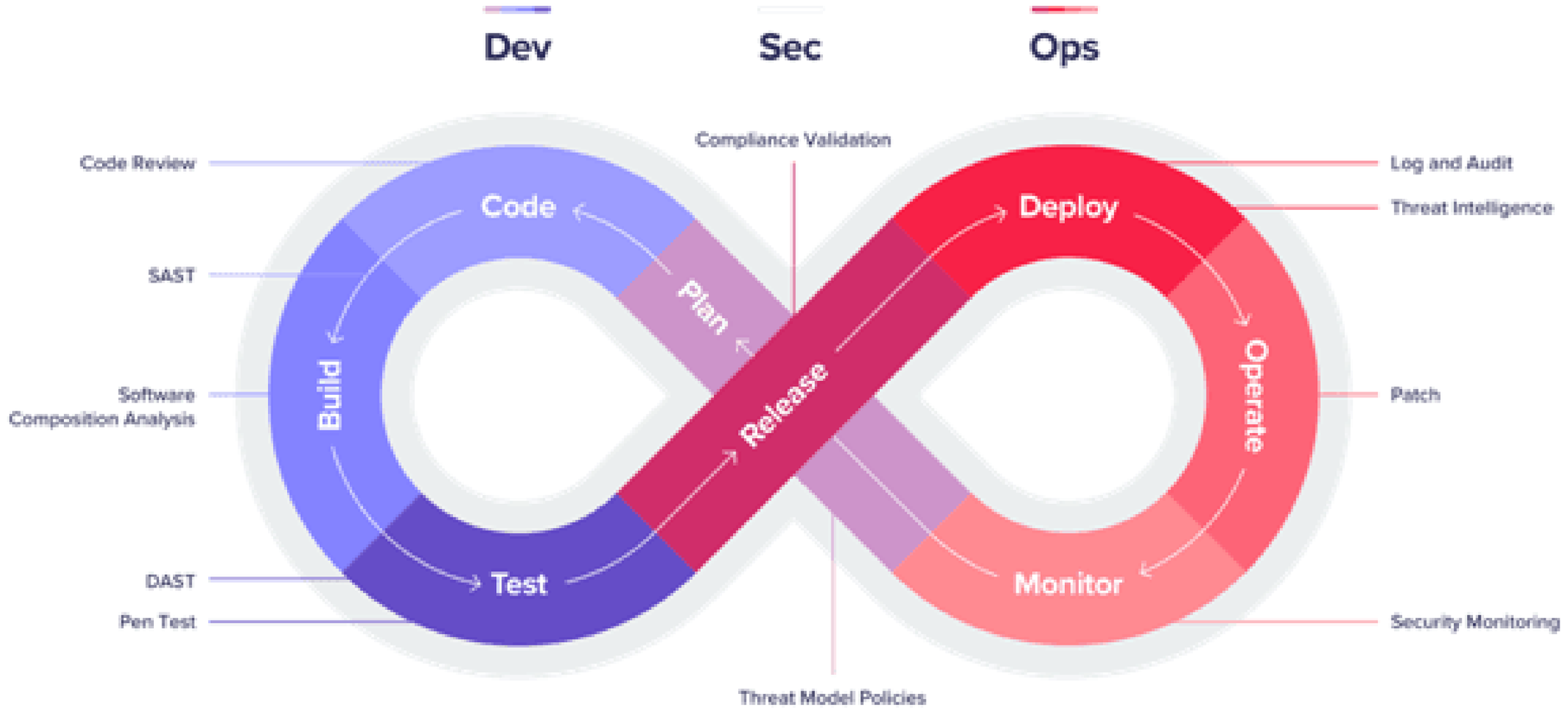
Análisis automático de vulnerabilidades de código abierto

Daniel Castellanos

Debricked - Que es

Debricked es una plataforma de seguridad para desarrolladores que ayuda a garantizar la seguridad y la calidad del software en todas las etapas del ciclo de vida del desarrollo de software. Ofrece una amplia gama de herramientas, desde escaneos automatizados de vulnerabilidades hasta análisis de código fuente, lo que permite a los desarrolladores detectar y solucionar problemas de seguridad en sus aplicaciones antes de que lleguen a producción. La plataforma también proporciona informes detallados y recomendaciones para ayudar a los equipos de desarrollo a mejorar continuamente la seguridad de sus productos.

DevSecOps Life Cycle



CyberRes

Fortify

Debricked - Ventajas

- La inteligencia y la seguridad de código abierto con la tecnología del aprendizaje automático de vanguardia le permiten obtener resultados más rápidos y precisos.
- Una solución de análisis de composición de software nativa de la nube que los desarrolladores prefieren utilizar y que, además, aumenta la productividad.
- Un enfoque global con integraciones sin fisuras en el ciclo de vida de DevOps para gestionar los riesgos de la cadena de suministro del software.

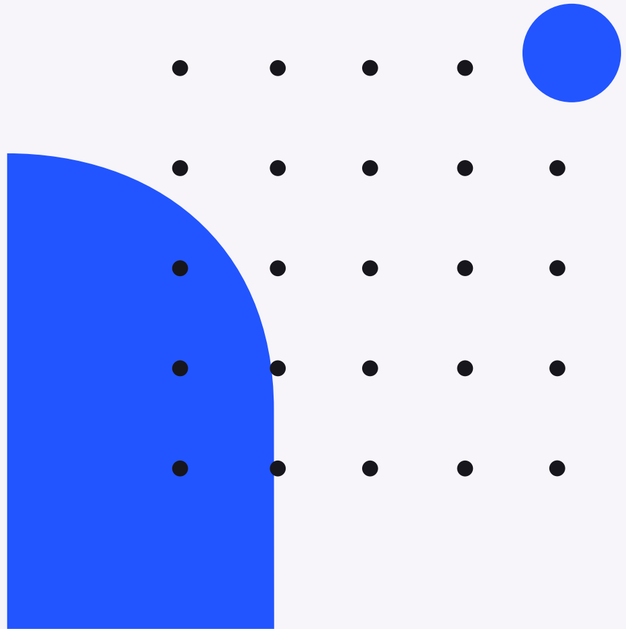
Debricked - Desventajas

- El costo puede ser una desventaja, aunque Debricked ofrece una versión gratuita para el análisis de firmware, también tienen planes de pago para empresas que requieren análisis de firmware a gran escala.
- Debricked se especializa en analizar vulnerabilidades de dependencias y librerías de código abierto al ser un área tan especifica no cobre otras posibles fuentes de vulnerabilidades en el código
- Al usar a Debricked como la fuente principal para el análisis de las vulnerabilidades dependemos del servicio, y en caso de algún fallo con la herramienta se vera interrumpida la cadena de trabajo

Vulnerabilidades en el código abierto

Las librerías de código abierto se utilizan ampliamente y son muy populares, por lo que los atacantes a menudo buscan vulnerabilidades en ellas. Si una librería tiene una vulnerabilidad conocida, es posible que un atacante pueda explotarla y comprometer la seguridad del software.

Al utilizar librerías de código abierto, los desarrolladores deben asegurarse de cumplir con las licencias de software que las rigen. Algunas licencias pueden requerir que los desarrolladores publiquen el código fuente de su software, lo que puede no ser deseable.



Vulnerabilidades en el código abierto

Los desarrolladores utilizan versiones antiguas de las librerías de código abierto porque son estables y han sido probadas. Sin embargo, esto puede ser problemático si una versión antigua tiene una vulnerabilidad conocida que se ha corregido en versiones posteriores. Si el desarrollador no actualiza la librería, el software puede ser vulnerable a ataques.

Las librerías de código abierto suelen ser desarrolladas por terceros, lo que significa que los desarrolladores no tienen control directo sobre su calidad y seguridad. Si una librería tiene una vulnerabilidad que el desarrollador no es consciente, puede ser explotada por los atacantes.

Bitbucket - Que es

Bitbucket es una plataforma de alojamiento de código fuente y gestión de proyectos basada en la nube que permite a los desarrolladores colaborar en equipos y mantener un seguimiento de las versiones del software en un solo lugar. Además, Bitbucket ofrece integración con otras herramientas populares de desarrollo, como Jira, Trello, Bamboo, Debricked y muchas más. La plataforma también brinda una amplia variedad de opciones de seguridad, control de acceso y autenticación para garantizar la protección del código fuente y la información confidencial del proyecto.

Bitbucket - Ventajas

- Bitbucket tiene integraciones con muchas herramientas populares de desarrollo, como Jira, Bamboo, Trello y Debricked. Estas integraciones permiten a los equipos de desarrollo sincronizar sus herramientas y aumentar la eficiencia en el proceso de desarrollo.

- Bitbucket utiliza Git como su sistema de control de versiones, lo que permite a los desarrolladores trabajar en diferentes ramas del proyecto y fusionar cambios fácilmente.

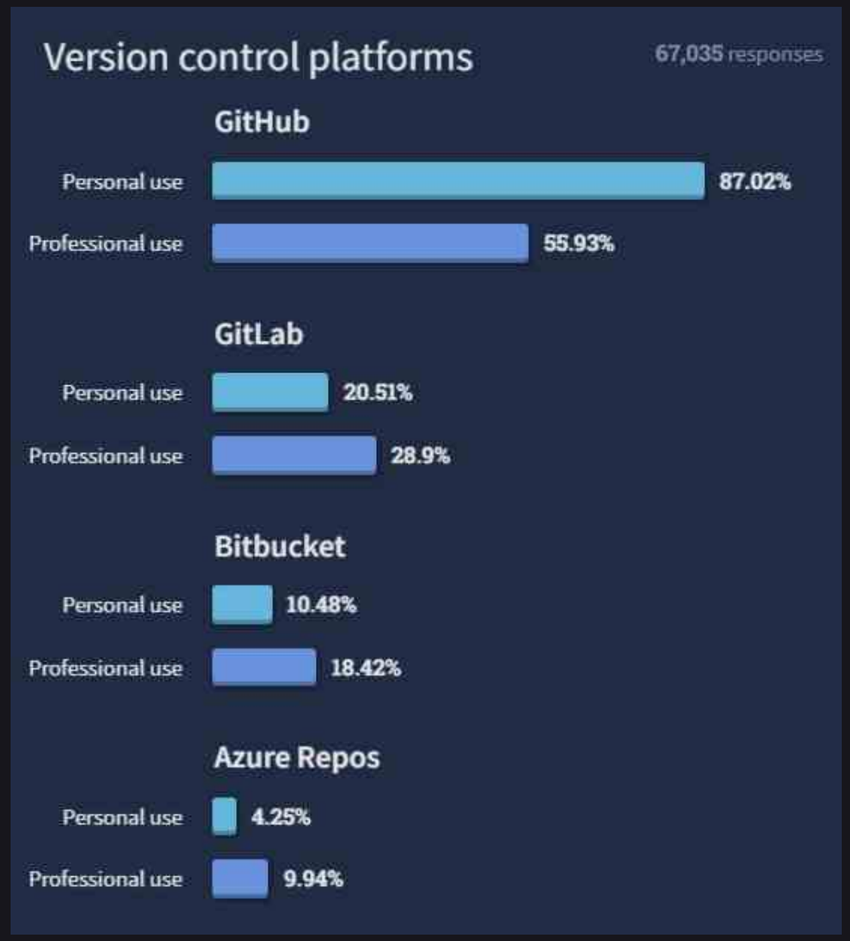
- Bitbucket permite a los equipos de desarrollo colaborar en proyectos de forma eficiente. Los desarrolladores pueden trabajar juntos en el mismo código. Además, Bitbucket proporciona características de seguimiento de problemas y tareas.

Bitbucket - Desventajas

- Aunque Bitbucket ofrece planes gratuitos para usuarios individuales y pequeñas empresas, también tiene planes de pago para empresas que requieren más características y capacidad de almacenamiento.
- A diferencia de otras plataformas de alojamiento de repositorios de código fuente, como GitLab, Bitbucket tiene opciones de personalización limitadas.
- Aunque Bitbucket tiene integraciones con muchas herramientas populares de desarrollo, algunas de las integraciones pueden no ser tan robustas como en otras plataformas.

Gartner 2022 Aplication Security Testing

Estadísticas de uso: Plataformas de control de versiones



Aprendizajes

- Las diferentes vulnerabilidades a las que se esta expuesto cuando se utilizan librerías y dependencias de código abierto
- Manejo e Intergracion de debricked como herramienta de analisis de dependencias y librerías de codigo abierto
- Automatización y diferentes reglas que se pueden establecer en un pipeline de manejo de versiones para evitar ataques a un código vulnerable