BASE4 SECURITY

Ayudando a construir un ecosistema digital más seguro.

Application Security

DATA SHEET

Aspectos generales del área

Base4 Security acompaña a las empresas hacia la automatización en los controles de seguridad dentro del SDLC de sus proyectos donde acompañamos a integrar seguridad en DevOps a través de la colaboración continua entre los equipos de desarrollo, operaciones y seguridad. Incorporando seguridad al ciclo de vida de desarrollo de software.

Es un método que se enmarca dentro del desarrollo ágil de software y supone una evolución hacia una responsabilidad compartida de la seguridad. Implica tener en cuenta la seguridad del software desde el principio, así como automatizar procesos para no ralentizar el flujo de trabajo de DevOps dentro del pipeline de desarrollo de aplicaciones según su nivel de madurez.

Objetivo

Nuestro objetivo es conseguir entregas más rápidas y seguras de software, sin convertir la seguridad en un cuello de botella. Es decir, DevSecOps trata de garantizar una entrega rápida y segura resolviendo problemas habituales entre el desarrollo y la seguridad. Y, para ello, se apoya en herramientas como Veracode.

Visibilidad

Realizamos GAP Análisis basándonos en el framework OWASP SAAM como una forma efectiva y medible para que su organización

analice y mejore su postura de seguridad de software.

Beneficio

• Obtener visibilidad del estadío de madurez actual de la seguridad de su pipeline de desarrollo dentro SDLC.
• Obtenga un plan certero de crecimiento e inversión en seguridad sobre las aplicaciones cubriendo niveles de criticidad.
• Cobertura de las últimas vulnerabilidades mundiales constantemente subidas a su nube y sin necesidad de instalar parches.

Puntos de Control

Realizamos servicios One Shot como puntos de control de la seguridad en su aplicación como Ethical Hacking Agile, Escaneo de Código Estático, Análisis de librerías de tercero y Análisis Dinámico.

Beneficio

• Servicios acotados y veloces para medir el grado de riesgo de su aplicación tanto de forma externa como desde el código fuente.
• Encuentre las vulnerabilidades más importantes y sepárelas por nivel de criticidad para poder corregirlas de manera rápida y obtener un mejor time-to-market.
• Seguimiento en la remediación hasta que la aplicación marca el 100% de estabilidad antes de salir a producción.
• Implementación de políticas centralizadas da un mayor enfoque y orientación al análisis, así como control desde Seguridad Informática sin influir en el proceso de desarrollo.
• Analizar todo el proyecto compilado a nivel de código además de tener integraciones con los IDE más relevantes en el mercado, herramientas de integración continua y gestión de proyectos.
• Mostrar un grado de la severidad encontrada bajo la restricción de política aplicada es más severo en el sentido de indicar las vulnerabilidades e incidencias encontradas.vulnerabilidades e incidencias encontradas.

Personal

Realizamos OutSourcing de perfiles DevSecOps 5x8 para que se encarguen de brindar una mejora continua de la seguridad en el pipeline de desarrollo, así como visibilidad de las mejoras al negocio.

Beneficios

- Contar con una persona dentro del mundo de DevOps con experiencia y capacidad en ciberseguridad.
- Evitar la rotación de personal en puestos similares.
- Mejora de puntos de control de seguridad en aplicaciones.
- Mayor integración con área de ciberseguridad.
- Capacitación al equipo de desarrollo.
- Apoyo en Implementación de tecnologías he integraciones
- Creación y automatización de análisis
- Presentaciones de vulnerabilidades y recomendación de buenas prácticas.
- Creación de Métricas he Indicadores.

Tecnología

Comercializamos tecnología para brindar una seguridad automatizada cross en todo tipo de aplicaciones con control independiente desde el área de desarrollo bajo las políticas de ciberseguridad.

Beneficios

- Mejora el time-to-market
- Reduce costos de tiempos de Desarrollo
- Reduce costos de Ethical Hacking.
- Automatización de los procesos
- Optimizar los procesos de seguridad y desarrollo.
- Enseñar buenas prácticas de seguridad a los diferentes equipos.
- Evaluar riesgos y definir planes de contingencia.
- Identificar amenazas y vulnerabilidades antes de salir a producción.

¿Por qué aplicar DevSecOps?

Integrar la seguridad en todo el proceso de desarrollo y no solo al final permite a los profesionales DevOps y de seguridad sacar el máximo partido a las metodologías ágiles, eliminando obstáculos a la hora de garantizar un código seguro.

Estos son los principales beneficios de adoptar DevSecOps:

- Desarrollar software seguro desde el diseño.
- Identificar vulnerabilidades en el código y ataques antes.
- Aplicar la seguridad de forma más rápida y ágil.
- Responder a los cambios y requisitos rápidamente.
- Mejorar la colaboración y comunicación entre equipos.
- Generar una mayor conciencia sobre seguridad entre todos los miembros.
- Enfocarse en generar el mayor valor de negocio.

Buenas prácticas de DevSecOps

Estas serían buenas prácticas a la hora de poner en práctica DevSecOps:

- Optimizar los procesos de seguridad y desarrollo.
- Enseñar buenas prácticas de seguridad a los diferentes equipos.
- Gestionar y mejorar los controles de acceso.
- Automatizar procesos repetitivos.
- Evaluar riesgos y definir planes de contingencia.
- Utilizar herramientas de seguridad.
- Identificar amenazas y vulnerabilidades proactivamente.
- Llevar a cabo auditorías de seguridad periódicamente.

Recomendaciones de Gartner

La integración de la seguridad en DevOps exige un cambio de mentalidad, procesos y tecnologías. Así, Gartner hace una serie de recomendaciones para practicar de forma exitosa DevSecOps:

- Adaptar las herramientas y los procesos a los desarrolladores y no al revés.
- No tratar de eliminar todas las vulnerabilidades durante el desarrollo.
- Centrarse en identificar y eliminar primero las vulnerabilidades de código abierto conocidas.
- Adaptar los análisis de pruebas estáticos y dinámicos (SAST /SCA/ DAST) a la nueva realidad.
- Capacitar a los desarrolladores en materia de seguridad, sin esperar que se conviertan en expertos.
- Adoptar un modelo de Security Champion (especialista en seguridad que hace de mentor para el resto de equipos) e implementar una herramienta sencilla para la recogida de requisitos.
- Asegurar y aplicar la misma disciplina operativa a los scripts de automatización y la infraestructura de seguridad.

Implementar un control de versiones sólido en todos los códigos y componentes.

- Implementar la gestión de secretos.
- Adoptar una mentalidad de infraestructura inmutable.
- Repensar cómo se manejan los incidentes de prestación de servicios, incluida la seguridad
- Utilizar aprovisionamiento de acceso dinámico para los desarrolladores en DevSecOps.

Auditoria OWASP DEVOPS

Audite los riesgos en el proceso, arquitectura y comunicaciones de desarrollo, para conocer el grado de madurez de ciberseguridad del pipeline.

El proceso se realiza vía reuniones para poder ver el GAP entre las mejores prácticas del mercado y lo que está realizando el cliente bajo un plan de trabajo detallado. Posteriormente, la ejecución involucra la revisión de una o varias aplicaciones, entrevistas con los desarrolladores, revisión de inventarios de herramientas, pipelines, buenas prácticas, resultados de pentesting anteriores, entre muchas otras.

Se le entregará un informe con detalle de los controles, estadísticas, y recomendaciones de implementaciones y buenas prácticas del uso de herramientas, documentos, checklist de validación, wiki online con recomendaciones de prácticas de desarrollo en la organización, asesoría posterior, entre otras.

El servicio está orientado a poder obtener un mejor ROI, elevando la seguridad de las aplicaciones desde su propio desarrollo, automatizando la misma, ganando time-to-market contra su competencia y evitando riesgos en producción que puedan tener un impacto negativo en la economía e imagen del cliente.

Modelado de amenazas

Proteja sus aplicaciones desde el inicio de las mismas para evitar futuros riesgos. El objetivo es que la seguridad de dicha aplicación se implemente desde su comienzo, modelando las futuras amenazas.

La implementación del modelado de amenazas se da en etapas tempranas de diseño del Software. La misma está orientada a que el área de desarrollo tenga en claro las posibles amenazas que podrá tener dicha aplicación desde la concepción e idea del negocio hasta su ejecución en células de desarrollo, así como la arquitectura validada desde un punto de ciberseguridad para la misma.

Mediante reuniones con los interlocutores validados, se diseñará un documento con la topología de la aplicación y las recomendaciones de mejores prácticas a tener en cuenta en el momento de comenzar su desarrollo, tanto por áreas de desarrollo como de infraestructura.

La finalidad del servicio es contemplar los mayores riesgos que podrá tener dicha aplicación según su uso, conexiones, arquitectura, diseño y lenguaje. Con ello se disminuirán durante el proceso de desarrollo dichos riesgos para que su paso a producción sea acelerado, poder ganar time-to-market, reducir tiempos del desarrollo de la misma e involucrar al área de ciberseguridad desde el primer momento.

BASE4 Security también comercializa tecnología de Modelado de Amenazas para automatizar el proceso dentro de las compañías.

Escaneo de código

Obtenga visibilidad de las vulnerabilidades actuales en su código fuente con este servicio One Shot, que ayudará a prever y ponderar riesgos previos el paso a producción.

Mediante herramientas cloud de primer nivel, BASE4 Security provee el servicio de Escaneo de Código Estático y Dinámico para descubrir las vulnerabilidades actuales en el mismo.

El servicio cuenta con una corta duración y ayuda a prever amenazas y riesgos previo al paso a producción de las aplicaciones, siendo una herramienta muy productiva para reducir ataques sobre las mismas.

Se entregará a los clientes un reporte de las vulnerabilidades segregadas por criticidad, así como una recomendación sobre la remediación de las mismas.

BASE4
SECURITY

www.base4sec.com