18_devsecops_y_owasp_top_10

October 15, 2020

1 DevSecOps.

- La razón de ser de DevOps es orientar los esfuerzos de la organizacion hacia el ciclo de vida desarrollo de software, permitiendo compartir responsabilidades y esfuerzos de los diversos integrantes de un equipo de trabajo.
- La premisa básica de DevSecOps es: "*Todos somos responsables de la seguridad*". De este modo, no sólo es necesario integrar y entregar software de calidad, sino seguro desde su concepción.
- De forma similar a los ámbitos de infraestructura, gestión de bases de datos, pruebas y calidad; los especialistas en seguridad deben formar parte integral en el ciclo de desarrollo del software, mientras que los desarrolladores deben de tener nociones básicas y herramientas automatizadas para crear, integrar y entregar software seguro.
- Es importante recalcar que la seguridad no viene en una caja, sino que es un fin a alcanzar.

1.1 El manifiesto de DevSecOps.

Fuente: https://www.devsecops.org/

Mediante *Seguridad como Código*, deberemos aprender que simplemente existe una manera de hacer las cosas para los expertos en seguridad, como nosotros, para operar y añadir valor con menores fricciones. Sabemos que debemos adaptarnos rápidamente y adoptar la innovación para asegurarnos de que la seguridad de los datos y la privacidad se dejen de lado debido a que fuimos muy lentos para cambiar.

Al desarrollar *Seguridad como Código*, nos avocaremos en crear productos y servicios asombrosos, ofrecer retroalimentación directamente a los desarrolladores y favorecer la iteración por encima de siempre buscar la mejor solución antes de un despliegue. Operaremos como desarrolladores para hacer que la seguridad y la conformidad a estándares sean consumidas como servicios. Abriremos y facilitaremos nuevas formas para ayudar a los demás y ver a sus ideas hacerse realidad.

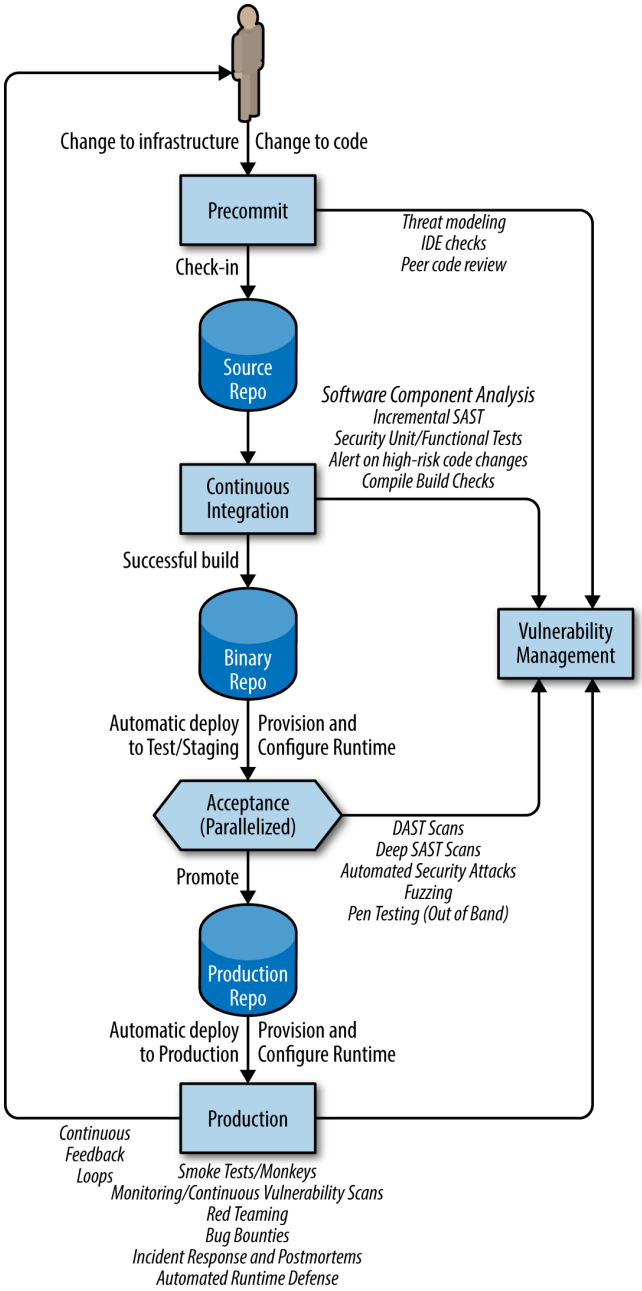
No dependeremos exclusivamente de reportes y "scanners" para mejorar el código. Atacaremos a los productos y servicios como a un intruso para defender lo que han creado. Exploraremos los huecos y buscaremos debilidades, y tabajaremos con ustedes para proveer acciones correctivas en vez de asignarles con una larga lista de problemas que deben de ser resueltos a costa suya.

No esperaremos a que las organizaciones sean víctimas de errores y atacantes. No nos conformaremos con encontrar lo que ya es sabido; en cambio, buscaremos anomalías que no han sido detectadas. Buscaremos ser mejores compañeros valorando lo que ustedes valoran:

- **Flexibilidad** por encima de decir “No”.
- **Apertura a la colaboración y contribución** por encima de requerimientos exclusivos de seguridad.
- **Servicios de seguridad con APIs** por encima de controles de seguridad obligatorios y papeleo.
- **Entregables de seguridad orientados al negocio** por encima de Seguridad basada en Sellos.
- **Pruebas de *Red Team* y *Blue Team*** por encima de depender de “scanners” y de vulnerabilidades téoricas.
- **Monitoreo proactivo 24x7** por encima de reaccionar después de ser informados de un incidente.
- **Compartir información sobre de las amenazas** por encima de quedarnos con la información.
- **Operaciones de conformidad** por encima de listas de requerimientos y reportes.

1.2 La seguridad como componente en la entrega continua.

Fuente: https://www.oreilly.com/library/view/devopssec/9781491971413/ch04.html



1.3 Automatización de pruebas de seguridad.

1.3.1 Aproximaciones.

- Caja blanca.
  - Inspección de código seguro.
  - Inspección de configuración segura.
- Pruebas de API.
  - Pruebas de seguridad Web/RESTFul API.
  - Pruebas de orientada a datos.

- Pruebas de la interfaz de usuario (web).
  - Ingreso con diferentes usuarios o cuentas incorrectas.
  - Salida del sistema para gestión de sesiones.
  - Creación de cuentas nuevas.
  - Ataques de ingreso por fuerza bruta.

1.4 *OWASP* Top Ten.

El Proyecto Abierto de Seguridad de Alicaciones Web (OWASP por sus siglas en inglés) es una organización sin fines de lucro dedicada a mejorar la seguridad del software mediante la creación de proyectos de código abierto y la apertura de capítulos locales en todo el mundo.

Una de sus actividades más conocida es la publicación de lo 10 riesgos de seguridad más importantes en el medio.

https://owasp.org/www-project-top-ten/

La versión en español del OWASPTop Ten puede ser consultada en la siguiente liga:

https://www.dragonjar.org/owasp-top-ten-project-en-espanol.xhtml

1. **Inyección** es la acción de poder filtrar código malicioso como parte de una consulta o un comando, el cual sería interpretado y ejecutado por el sistema para ganar acceso a recursos restringidos.
2. **Autenticación rota** ocurre cuando las herramientas de gestiónde sesiones y autenticación se implementan de forma incorrecta, permitiendo a los atacantes vulnerar credenciales o suplantar usuarios.
3. **Exposición de datos sensibles** ocurre cuando las aplicaciones no son capaces de proteger adecuadamente la exposición de información sensible de tal forma que el atacante acceda a ella o sea capaz de modificarla.
4. **Entidades XML Externas (XXE)** ocurre cuando ciertos procesadores de documentos XML son viejos o están mal configurados, perimtiendo a "entidades externas" realizar diversos ataques.
5. **Control de acceso roto** ocurren cuando los usuarios autenticados cuentan con permisos que no les corresponden.
6. **Mala configuración de seguridad** ocurren cuando se utilizan configuraciones por defecto, se habilitan modos de depuración en producción, se da accceso a recursos en las nube si restricciones o los sistemas no están parchados y actualizados.
7. **Ejecución de scprits de sitios cruzados (XSS)** ocurre cuando del lado del cliente/navegador se ingresa información no confiable dentro de una página web, lo que permitiría ejecutar scripts en el manegador de usuario.
8. **Deserialización insegura** ocurre cuando se intenta reconstruir un objeto de forma impropia a partir de sus datos serializados.
9. **Uso de componentes con vulnerabilidades conocidas** ocurre cuando se utilizan en un entrono producvtivo bibliotecas con fallas conocidas.

10. **Monitoreo y uso de bitácoras insuficiente.** la falta de un sistema de bitácoras y monitoreo robusto difuclta la detección de anomaías y ataques.