Caso de estudio

CYBOLT
Security Innovation

Empresa: Banco Santander

2019 - actual

Application Security

Soluciones que se implementaron

VERACODE

Plataforma de Seguridad Aplicativa (Veracode)

Servicios que se implementaron

Soporte, seguimiento y consultoría para la implementación de la plataforma e integraciones.

Transferencia de conocimiento en el uso de la plataforma de seguridad aplicativa.

Sesiones de seguimiento quincenales para atención de dudas, sesiones de trabajo y/o presentación de nuevas características de la plataforma.

La situación

El objetivo del banco se focalizó en contar con aplicaciones seguras que protegieran la información tanto de sus clientes como sus colaboradores con el objetivo de ser una institución de confianza y que se preocupa por la seguridad.
Para esto se requiere contar con una plataforma robusta y segura que permita identificar huecos de seguridad, así como vulnerabilidades para poder remediarlas basándose en el impacto al negocio, riesgo y criticidad, todo esto de forma automatizada para agilizar los tiempos ya que se contaba con diversas fabricas de software y un equipo de seguridad compacto que debía gestionar la seguridad de todas esas fabricas y aplicaciones que se desarrollaban día a día, por ello la necesidad de una aplicación que brindará visibilidad y gestión centralizada era un factor clave para el éxito del proyecto.

El problema

No se contaba con visibilidad de la cantidad de aplicaciones ni la postura de seguridad de estas, por ello se requería:

- Contar con **políticas centralizadas.**
- Implementar una herramienta que brindará una tasa baja de falsos-positivos **(para enforcarse en amenazas reales).**
- **Automatización del pipeline** del ciclo de desarrollo (agilidad).
- **Alinear a equipos de desarrollo** interno y fábricas de software con **políticas de código seguro**.
- **Optimizar el tiempo de liberación** de aplicaciones seguras.
- Contar con una consola central que **provea KPIs y métricas para toma de decisiones.**
- Identificar las **tendencias de vulnerabilidades** para **capacitar** a los equipos de trabajo en **desarrollo seguro y buenas prácticas.**

El análisis

Una vez realizado el análisis de la situación se determinó que la plataforma de seguridad aplicativa que ayudaría a cumplir con las necesidades requeridas.
Además de proporcionar un análisis de seguridad en el código y conocer la postura de seguridad de las aplicaciones contarían con métricas e insumos para tomar acciones en la mejora de los procesos de desarrollo seguro orientándose a una metodología DevSecOps, todo esto automatizando la integración de la seguridad en el ciclo de desarrollo y siendo gestionada desde un único punto de acceso, el cual, por medio de tableros, proporcionaría la información de valor para identificar áreas de oportunidad, puntos de mejora y tener un seguimiento detallado de los avances respecto a un programa de seguridad aplicativa.

La solución:

Por medio de la implementación de la plataforma de **Veracode** para el **análisis de seguridad en el código** se tuvieron los siguientes hitos:

- **Integración al pipeline** del ciclo de desarrollo (con **Jenkins**).
- **Implementación** de la plataforma de análisis de código estático.
- **Definición de políticas** acorde a las necesidades específicas del cliente.
- **Automatización completa** del ciclo de desarrollo para **análisis estático**.
- **Reducción de tiempos** de liberación de aplicaciones seguras.
- **Creación de tableros** personalizados para el seguimiento de tendencias y atención a hallazgos.
- **Control y gestión** centralizada que provee la visibilidad, KPIs y la postura de seguridad de las aplicaciones.

Retos en la implementación

El principal reto fue el tiempo ya que se requería una implementación ágil, sin embargo, derivado de la participación conjunta se realizaron sesiones de trabajo presenciales en las cuales se definió un plan de trabajo agresivo, pero alcanzable para poder realizar las integraciones en los plazos establecidos.
Las integraciones nativas de la plataforma ayudaron a que este proceso fuera ágil, contando con análisis de seguridad y resultados desde la primera semana.

Los beneficios:

- Menor tiempo para liberar las aplicaciones (seguras) al mercado.
- Contar con aplicaciones seguras en el mercado.
- Menor tasa de cambios al código (por temas de seguridad), una vez que el aplicativo está en producción.
- Gestión centralizada de cientos de aplicaciones que puede ser operadas por un equipo compacto.
- Automatización de la seguridad de las aplicaciones en el ciclo de desarrollo.
- Mejora en la atención de vulnerabilidades (baja tasa de falsos-positivos).
- Capacidad de priorizar atención de huecos de seguridad basados en riesgo y criticidad.
- Medición de atención de remediación o corrección de vulnerabilidades por los equipos de desarrollo.
- Homologación de políticas de seguridad para los desarrollos (internos y por fábricas de software).
- Mejora en los procesos para atención de hallazgos o vulnerabilidades.
- Equipos de trabajo operando bajo una metodología DevSecOps.

Los resultados:

- Crecimiento de análisis de aplicaciones de decenas a cientos.
- 90% de cobertura de análisis de seguridad en aplicaciones.
- 95% de las aplicaciones con cumplimiento satisfactorio con base en las políticas, estándares de seguridad y prácticas definidas por el cliente.
- 40% de reducción de tiempo en atención de vulnerabilidades por parte de los equipos de desarrollo.
- 30% menos vulnerabilidades inyectadas en las etapas tempranas de desarrollo.

Equipo participante en el proyecto:

Farith Baltazar
Account Manager

Emanuel Valle
Consultor Sr. de
Seguridad Aplicativa

WE ARE ONE,
WE ARE CYBOLT