PLATINUM
CIBER-SEGURIDAD

Servicios de APPLICATION SECURITY

PENETRATION TEST, VULNERABILITY ASSESSMENT Y SOURCE CODE ANALYSIS.
Proteja sus sistemas y aplicaciones sometiéndolas a las pruebas que realizan los atacantes. Conozca sus vulnerabilidades mediante las mismas técnicas utilizadas por ellos, y sepa cómo solucionarlas para evitar sufrir por esos ataques.
A través de nuestros servicios, simulamos ataques reales sobre los sistemas, obteniendo pruebas concretas de hasta dónde podría llegar un atacante evidenciando la vulnerabilidad y recomendando una posible solución a cada hallazgo.

ANÁLISIS DE VULNERABILIDADES

Mediante esta técnica, se efectúa una búsqueda de vulnerabilidades presentes en los sistemas analizados. Se verifica que cada vulnerabilidad exista, sin efectuar la explota- ción de la misma. Este servicio tiene como ventajas que en un corto tiempo, se hallan casi todos los posibles puntos de entrada para un atacante. Se lleva a cabo con herramientas automáticas específicas del tipo World-Class y mediante los conocimientos de nuestro equipo de consultores.

PRUEBAS DE PENETRACIÓN

En este caso, cada vulnerabilidad hallada se explota para ingresar a los sistemas del cliente y se intenta seguir penetrando hasta donde sea posible técnicamente. Esta técnica tiene la ventaja de permitir demostrar fehacientemente los daños que podría causar un atacante. Si bien para el desarrollo del servicio se utilizan herramientas automáticas, es fundamental y determinante el expertise de nuestro técnico.

ANÁLISIS DE CÓDIGO

Para determinar las posibles vulnerabilidades de una aplicación, se analiza su código fuente, buscando fallas de seguridad que podrían resultar puertas de acceso para los atacantes. Para este servicio se utilizan las herramientas automáticas, pero debido a que aún las mejoras herramientas sólo detectan un muy bajo porcentaje de las fallas de seguridad, en este caso es fundamental y determinante el conocimiento y experiencia de nuestro equipo técnico especializado.

MODALIDADES

BLACK BOX

El cliente elige no dar absolutamente ninguna información sobre los sistemas a verificar, por lo que el equipo debe incialmente explorar, encontrar e identificar los posibles blancos relacionados con la empresa o negocio al que se le debe efectuar el análisis. Posteriormente, el equipo técnico lleva a cabo la búsqueda de vulnerabilidades y/o explotación de las mismas, exactamente de la forma en que lo haría un atacante externo que no conoce la compañía. La ventaja de esta modalidad consiste en que es la más cercana a la realidad, pero tiene como desventaja que la duración del proyecto es necesariamente mayor.

GREY BOX

Es un intermedio entre Black Box y White Box, es decir la empresa brinda parte de la información técnica al equipo que va a llevar adelante el proyecto. Esta modalidad se asemeja a lo que haría un atacante que conoce en parte la compañía blanco del ataque, por ejemplo, un ex-empleado.

WHITE BOX

El equipo técnico cuenta con toda la información sobre el entorno, interface, equipos de conectividad, etc., de forma de acortar drásticamente los tiempos de proyecto, enfocándose sólamente en el análisis.
Esta modalidad es la utilizada para el Análisis de Código en la que se entrega el código fuente completo de la aplicación para su análisis.