



Aumente la seguridad de sus redes

Las principales preocupaciones de las organizaciones, se centran en la protección de la infraestructura tecnológica, incluido su activo más importante, la información, así mismo el incremento de amenazas ya sea internas o externas, la búsqueda de las organizaciones de todos los sectores económicos de altos estándares de seguridad y la incorporación de nuevas tecnologías para gestión de la información, entre otros, se torna de gran importancia y obligación para la adopción de estrategias que permitan implementar soluciones que auditen la seguridad de los sistemas de información.

Frente a esta problemática, ofrecemos a las organizaciones soluciones fundamentadas en “mejores prácticas” y lineamientos nacionales e internacionales, que apoyen el aseguramiento razonable de los Riesgos relevantes y de gran impacto para la empresa.

Principales beneficios

La realización del Análisis de Vulnerabilidades proporciona una lista detallada de debilidades en torno a la información contenida dentro y fuera de sus sistemas de información, estableciendo en cada caso el nivel de riesgo.

- 🔒 Conocer el estado actual de riesgo de la información corporativa, analizando: redes, comunicaciones, aplicaciones críticas, bases de datos y seguridad física .
- 🔒 Generación de patrones de posibles ataques al crear escenarios de explotación sobre conjuntos de vulnerabilidades encontradas.
- 🔒 Establecimiento de un correcto orden de prioridades en la implementación de parches y soluciones, ya sean temporales o permanentes.
- 🔒 Centralización de la información de vulnerabilidades, procesamiento y producción de reportes, clasificando de acuerdo con la CVE, a las direcciones IP afectadas.

Black Falcon, Net security suite

Completa familia de servicios que permite gestionar y auditar la seguridad de la información, la cual consta de las siguientes soluciones.



Cumplimiento de estándares, dirigidos a clientes de sectores específicos

FAV

Falcon Análisis de Vulnerabilidades es una herramienta para la auditoría de los sistemas de información, especializada en el análisis, clasificación y custodia de los datos que indican las vulnerabilidades de los dispositivos presentes en las redes informáticas, esta solución permite gestionar y monitorear las vulnerabilidades, amenazas, falsos positivos y generar informes.

Específicamente, se exploran las vulnerabilidades mediante ataques controlados, homologados por el programa de compatibilidad del **CVE (Common Vulnerabilities and Exposures)**, adicionalmente permite automatizar diferentes tareas de análisis tales como:

- 🔒 Correlación de resultados de la exploración de red, asegurando el cumplimiento de normas de Seguridad
- 🔒 Búsqueda, seguimiento y evaluación automática de posibles falsos positivos.
- 🔒 Comparación de resultados de un mismo segmento en dos momentos distintos, de un segmento con una red o de dos



Pruebas e Informes.

Nuestro servicio se basa en el estándar de facto de la CVE (Vulnerabilidades y Exposiciones Comunes) y el appliance que trabaja dentro de las instalaciones de nuestros clientes. Usamos solo componentes homologados por la CVE, cumpliendo de esta manera con la nomenclatura de vulnerabilidades a nivel mundial (<http://cve.mitre.org>), lo que a su vez permite a las entidades cumplir con normas de calidad en seguridad.

Nuestra plataforma diagnostica más de 15.000 vulnerabilidades de seguridad en entornos de red, evitando gastos indirectos provocados por virus, gusanos y crackers.

Con el uso del servicio, la aplicación de soluciones sugeridas y la retroalimentación del sistema, se introduce a la seguridad de la organización un elevado proceso de aprendizaje y conocimiento de sus sistemas, quedando registrado el historial de sucesos en una base de conocimiento que se convierte en uno de los pilares para la estructura de seguridad de la red.

En los reportes se comparan los estados actual y anterior, se ven gráficos ilustrativos y se obtienen hojas de trabajo que permiten al administrador de la red y a los auditores, un efectivo seguimiento de los logros en cuanto a las vulnerabilidades resueltas, pendientes o nuevas de sus infraestructuras.

Otros productos

PCI

Esta solución permite validar el cumplimiento de las normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS), identificando las vulnerabilidades y errores en la configuración e infraestructura tecnológica contra listados CVE. Estas pruebas son realizadas a nivel ASV.

DR

Descubrimiento de redes, esta solución permite realizar la toma de información pormenorizada sobre dispositivos de red, clientes, servidores y OS.

HIPPA

Configuración de chequeos para verificar el cumplimiento de la Health Insurance Portability and Accountability Act (HIPAA) para el sector salud.



Nuestra Solución

El servicio comprende la implementación de un appliance, el cual identifica las vulnerabilidades al interno de la organización y a su vez recibe los informes de una herramienta similar externa.

Esta herramienta centraliza la información de vulnerabilidades, los informes, las soluciones sugeridas y permite realizar los correspondientes comparativos de seguimiento sobre soluciones aplicadas. Específicamente, se exploran mediante ataques controlados, las vulnerabilidades registradas en <http://cve.mitre.org/cve/downloads/full-allitems.html>



Intel® Xeon® X3430 (4 Core, 2,40 GHz, 8 MB L3, 95W)
16 GB DDR3 PC3-10600E

Servicios

Nuestra área de consultoría, con alto grado de conocimiento, experiencia y especialización está en capacidad de aplicar una metodología que permite conocer al cliente en sus necesidades, formas de operación y aplicación de la tecnología, análisis de posibles ataques, organización estructural, rapidez y tiempos de respuesta, controles y tiempos de uso, posibilidades de ampliación y utilización adecuada de equipos y programas.