

# “Pentera es como tener un ejército de hackers atacando durante un año, pero concentrado en dos horas y con seguridad”

**Ramón Lucini** Pentera Regional Sales Manager Iberia

Pentera es una nueva forma de validar y reducir la exposición a la ciberseguridad basada en la emulación continua de ataques

La plataforma Pentera utiliza un algoritmo para escanear y desafiar toda la superficie de ataque (interna y externa), proporcionando validación de seguridad en tiempo real a escala.

Al no requerir agentes ni preinstalaciones, la plataforma brinda a los equipos de seguridad una vista completa de la operación de ataque que proporciona una evaluación real de su resiliencia frente a ataques reales, priorizando los esfuerzos de remediación con una perspectiva frente a la amenaza.

Con Pentera, una empresa puede reducir continuamente la exposición a ataques y mantener seguro su sistema mediante la realización de pruebas de validación continua. Esto brinda a las organizaciones una mejor comprensión que también les permite probar la eficiencia de los sistemas de seguridad implementados y mantener la coherencia en toda la organización. Hoy conversamos con Ramón Lucini, Pentera Regional Sales Manager Iberia.

**Han pasado casi dos años del boom de las tecnologías producido como consecuencia de la pandemia de la COVID-19, ¿nos hemos adaptado bien en términos de seguridad?**

Es cierto que estos dos años han acelerado muchos los proyectos, tanto de migración a la nube como de trabajo en remoto. Este incremento de actividad ha aumentado la superficie de ataque y, dada la urgencia con la que se han implantado estos nuevos entornos, estamos viendo cómo la seguridad vuelve a primera línea.

Las empresas necesitan estar en constante alerta y asegurar que tanto su red interna como externa no queden comprometidas. En otras palabras, deben validar la superficie de ataque en su totalidad.

**Proteger nuestros datos es como un mantra que todos repetimos y pocos conseguimos. ¿Cuáles son los retos que tiene actualmente el mercado?**

Hay muchos fabricantes en el marco de la ciberseguridad que ofrecen soluciones que van cubriendo ciertos riesgos. Pero es muy complicado para cualquier empresa saber si realmente está protegida frente a los ataques, o bien tiene una falsa

sensación de seguridad sin haber hecho pruebas reales de ataques.

Todos los días, los líderes de seguridad de las empresas aceptan la tarea casi imposible de identificar los riesgos reales a los que se enfrentan sus organizaciones en una superficie de ataque en constante crecimiento. Sin una lectura actualizada de su verdadera exposición a la seguridad, los equipos de seguridad no pueden estar seguros de que están preparados. Sin una visión precisa de qué vulnerabilidades son reales y cuáles son solo asumidas, el riesgo empresarial aumenta.

Puedes tener todas las herramientas de seguridad del mercado, pero la única manera de validar al 100% si estos sistemas están implementados correctamente es validando tus controles de seguridad constantemente.

**Así, la ciberseguridad es un trabajo diario, ¿verdad?**

Desde luego. Nuestras redes cambian continuamente. Compañeros que se incorporan, otros que dejan la empresa, equipamiento nuevo, cambios de configuraciones y más. Todo ello es como un ente vivo que cambia constantemente. Lo que ayer era perfectamente seguro, puede que hoy no lo sea.

Además, los atacantes también están evolucionando: los hackers están desarrollando nuevos métodos que ponen en riesgo los datos de las empresas. Por ello, y es algo que hace que Pentera sea única, es que su equipo interno de investigación está constantemente descubriendo nuevos vectores de ataque.

**¿Y estos procesos se pueden automatizar?**

En una gran mayoría de los casos, sin lugar a duda, la automatización es la clave. Nadie tiene los recursos humanos y económicos para gestionar entornos cambiantes de forma manual. Tenemos que ser capaces de automatizar y priori-



zar cada iniciativa de seguridad para que tenga el máximo impacto.

**¿Qué ofrece Pentera en este sentido?**

Pentera ofrece validación automática de seguridad. Esto implica que cualquier empresa puede verificar cómo sus sistemas de seguridad se enfrentan a ataques reales (pero seguros), tanto en su red interna como en su exposición en Internet. De esta forma descubre cómo un hacker puede progresar en sus ataques en su red, qué vulnerabilidades son las que tiene un mayor impacto en su ciberseguridad y cómo arreglarlas. Y todo de forma automática y periódica. Como definió un CISO, es como tener un ejército de hackers atacando durante un año, pero concentrado en un par de horas.

**“Las empresas necesitan estar en constante alerta y asegurar que tanto su red interna como externa no queden comprometidas”**

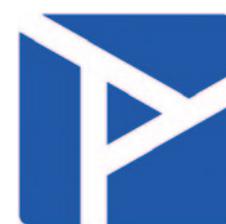
**“Es muy complicado saber si realmente se está protegido frente a los ataques, o bien tiene una falsa sensación de seguridad sin haber hecho pruebas reales de ataques”**

**Sois una multinacional puntera en el sector, ¿qué servicios ofrecéis al mercado español y con qué equipo?**

Pentera es líder en la categoría de Validación Automatizada de la Seguridad™. Tenemos una amplia cartera de clientes en todas las industrias.

En España nos hemos establecido con un equipo de 6 personas para ayudar a las empresas españolas a mejorar su seguridad. Contamos igualmente con una amplia red de partners que integran Pentera en sus ofertas para dar un servicio.

De esta forma ofrecemos la plataforma Pentera a todos los clientes, permitiendo validar tanto la seguridad interna de sus empresas, como la seguridad de su exposición en Internet.



**PENTERA**

www.pentera.io