Gestión de la exposición con Ivanti

Amplía tus prácticas de gestión de vulnerabilidades para prevenir proactivamente las brechas de seguridad

Las prácticas tradicionales de gestión de vulnerabilidades no fueron diseñadas para gestionar el volumen y la variedad de activos de exposiciones que son hoy el pan de cada día. A causa de ello, las organizaciones no son conscientes de muchas ciberamenazas. La solución de gestión de la exposición de Ivanti resuelve este problema, proporcionando una visibilidad completa de los activos y de las exposiciones, además de efectuar una priorización basada en el riesgo para guiar un enfoque estratégico de la resolución.

¿Qué es CTEM?

La gestión continua de la exposición a amenazas (CTEM), introducida por Gartner, consiste en un conjunto de procesos y capacidades que permiten a las organizaciones evaluar de forma continua y coherente la accesibilidad, la exposición y la explotabilidad de los activos digitales y físicos de una empresa. Las prácticas de CTEM se ejecutan en gran medida a través de las capacidades que ofrece la nube, como las de la solución de gestión de la exposición de Ivanti.

Las superficies de ataque crecen constantemente en cuanto a tamaño y complejidad. Las prácticas tradicionales de gestión de vulnerabilidades rara vez se ajustan en respuesta, lo que provoca que se queden cortas a la hora de proteger los entornos informáticos modernos:

- Observar únicamente el perímetro tradicional (servidores y puntos finales) ignorando dispositivos móviles, páginas web, aplicaciones y otros activos que introducen riesgos en un entorno.
- Enfocarse estrictamente en las Vulnerabilidades y Exposiciones Comunes (CVE, por sus siglas en inglés) mientras se dejan sin comprobar otros tipos de exposiciones, como los errores de configuración, que exponen a una organización al riesgo.
- Priorizar los esfuerzos de corrección con el Sistema de Puntuación de Vulnerabilidad Común (CVSS, por sus siglas en inglés), que mide la gravedad de la vulnerabilidad, pero no el riesgo que atañe; en otras palabras, la facilidad con que una vulnerabilidad podría ser explotada, pero no si ya lo ha sido.

En definitiva: a pesar de realizar un esfuerzo encomiable, las organizaciones que utilizan métodos tradicionales de gestión de vulnerabilidades corren un mayor riesgo de sufrir una brecha, y de ser víctimas de periodos de inactividad, daños a su reputación y otros perjuicios derivados de las brechas. Tampoco están propensas a quedarse varadas en un carácter reactivo, ya que intentan solucionar miles de vulnerabilidades de alta gravedad en lugar de las pocas y selectas que les suponen un riesgo real.

La gestión de la exposición resuelve las deficiencias de la gestión de vulnerabilidades. Así, representa una evolución de la gestión de vulnerabilidades que moderniza los métodos tradicionales para garantizar una visibilidad completa de los activos y las exposiciones, además de una adecuada priorización. Según Gartner, para 2026, las organizaciones que prioricen las inversiones en seguridad basándose en un programa de gestión continua de la exposición a amenazas (CTEM, por sus siglas en inglés) reducirán las brechas en dos tercios[1].

Presentamos la gestión de la exposición con Ivanti

Mediante una visibilidad completa de la superficie de ataque y una priorización basada en el riesgo, la solución de gestión de la exposición de Ivanti garantiza que las organizaciones sean conscientes de todos sus activos y exposiciones (incluyendo aquellos que a menudo se pasan por alto en la gestión tradicional de vulnerabilidades) y del riesgo real que plantean.

Funciones principales

Obtén visibilidad completa

Amplía tu perspectiva para incluir activos más allá de los servidores y puntos finales conocidos, para tener una visión completa de la superficie de ataque que debes defender, puesto que basta un punto ciego para que un ciberadversario se infiltre en tu organización. La gestión de la exposición de Ivanti detecta todos los dispositivos que se conectan a la red (incluyendo los nuevos y los desconocidos) y el software instalado mediante escaneos activos y pasivos y conectores de terceros.

La monitorización sin agentes descubre activos externos que normalmente eluden la vigilancia de los equipos de seguridad, como los entornos de Control de Calidad (QA), los entornos de desarrollo y las páginas web de marketing que nadie usa ya. La solución Ivanti busca también más allá de los CVE para detectar exposiciones de activos externos en los siguientes vectores:

- Seguridad de las aplicaciones
- Fugas de datos
- Salud del DNS
- Seguridad del correo electrónico
- Seguridad de la red
- Ingeniería social

Contabiliza el riesgo

Despídete del CVSS y de los inconvenientes asociados. Ivanti ofrece dos metodologías propietarias de puntuación de riesgos que centran los esfuerzos de remediación de exposiciones donde más sentido tiene, para que puedas prevenir la explotación y sus consecuencias.

La Clasificación de Riesgos de Vulnerabilidad (VRR) califica las exposiciones en función de sus atributos intrínsecos y del contexto de amenazas del mundo real, no solo de su gravedad. Al proporcionar evaluaciones precisas de cada exposición, VRR muestra cuáles requieren atención inmediata y cuáles no suponen ningún riesgo.

El VRR se combina con la criticidad de los activos, la inteligencia de amenazas y el acceso externo para calcular las puntuaciones RS^3 de Ivanti que señalan qué activos presentan mayor riesgo. También se integran en una vista cuantificada del perfil de riesgo de una organización que muestra el éxito de los esfuerzos de gestión de la exposición a lo largo del tiempo.

Toma acción

¿Cuál es el punto de evaluar las exposiciones si no puedes hacer nada a partir de tu análisis? Con Ivanti, podrás adoptar medidas tangibles para reducir el riesgo corrigiendo las exposiciones críticas antes de que sean explotadas.

Una integración API te permite entregar listas de exposiciones priorizadas directamente desde nuestra solución de gestión de exposiciones a nuestro módulo de gestión de parches para su remediación. Gracias a su compatibilidad con Windows, macOS, Linux y aplicaciones de terceros, podrás corregir un alto porcentaje de las exposiciones que encontradas en la mayoría de los entornos modernos.

Ivanti también puede actuar por ti a través de bots automatizados que detectan, diagnostican y solucionan problemas de forma proactiva en endpoints y dispositivos periféricos.

Acerca de Ivanti

Ivanti elimina las barreras entre TI Seguridad, para que el «Everywhere Work» pueda prosperar. Ivanti ha creado la primera plataforma tecnológica diseñada específicamente para los CIO y los CISO, ofreciendo a los equipos de TI y Seguridad soluciones de software integrales que se adaptan a las necesidades de sus organizaciones para habilitar, proteger y elevar las experiencias de los empleados. La plataforma Ivanti cuenta con el potencial de Ivanti Neurons, una capa de hiperautomatización inteligente a escala en la nube que permite remediar los problemas y aplicar seguridad de forma fácil y proactiva en toda la organización, proporcionando una experiencia de empleado que encanta a los usuarios. Más de 40.000 clientes, incluidos 85 de las 100 empresas de la lista Fortune, han elegido Ivanti para hacer frente a los retos con sus soluciones end-to-end. En Ivanti, nos esforzamos por crear un entorno en el que se escuchen, respeten y valoren todas las perspectivas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta. Para más información, entre en www.ivanti.com/es y sigue a @GoIvanti.

Copyright © 2024, Ivanti. All rights reserved. IVI-2856 09/24 RW/NH

ivanti neurons

Para obtener más información o ponerse en contacto con Ivanti, por favor visita www.ivanti.com/es.

1. Gartner, «Top Trends in Cybersecurity for 2024» (Principales tendencias en ciberseguridad para 2024), 2 de enero de 2024.