ivanti neurons

DATASHEET

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

Ampliar la gestión de vulnerabilidades basada en riesgos de aplicaciones

Evolucione la gestión de vulnerabilidades de sus aplicaciones hacia un enfoque basado en riesgos con Ivanti Neurons para ASOC. Esta oferta SaaS le permite tomar decisiones rápidas e informadas sobre hacia dónde dirigir el desarrollo para mejorar la seguridad de las aplicaciones internas y de cara al cliente.

La gestión de vulnerabilidades basada en el riesgo debe incluir aplicaciones

El número de aplicaciones escaneadas por trimestre se ha triplicado en 10 años. La cadencia de los escaneos se ha multiplicado por 20 en el mismo periodo. No es de extrañar que identificar la rara vulnerabilidad o debilidad de aplicaciones que plantea un riesgo significativo sea un proceso lento para las organizaciones que utilizan enfoques tradicionales para la gestión de vulnerabilidades: se están ahogando en datos.

Antes de que estas organizaciones puedan siquiera comenzar a priorizar las vulnerabilidades y debilidades para su corrección, primero deben recopilar una serie de datos dispares - SAST, DAST, OSS y hallazgos de escáneres de contenedores, inteligencia de amenazas y más - normalizar esos datos y prepararlos para su uso. Cuando se hacen manualmente, estos procesos tardan semanas en completarse y son propensos al error humano.

El proceso de priorización no es mejor. Consideremos las vulnerabilidades del ransomware. El setenta y cuatro por ciento no están clasificadas como Críticas en CVSS v3 y 156 faltan en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de CISA. Además, tres escáneres muy populares todavía no han añadido plugins y firmas de detección para un total de 20 vulnerabilidades de ransomware.[2]

Además de todo esto, la falta de cooperación entre los equipos implicados se ha citado como el principal reto en la defensa contra los ciberataques.3 Esta fricción entre las partes interesadas en la gestión de vulnerabilidades puede ralentizar la corrección y dejar a la organización expuesta a los ataques.

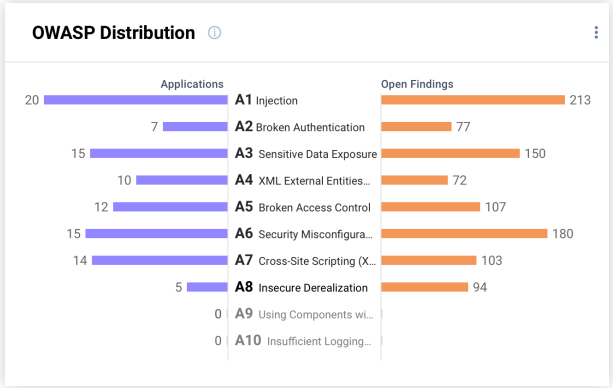
Presentación de las neuronas Ivanti para ASOC

Adopte un enfoque basado en riesgos para la gestión de vulnerabilidades para su pila de aplicaciones con las capacidades que se encuentran en Ivanti Neurons para ASOC. Estas capacidades vienen empaquetadas en una sola interfaz para que pueda eliminar gradualmente el enfoque de “silla giratoria” que ha definido las prácticas de gestión de vulnerabilidades del pasado.

Funciones clave

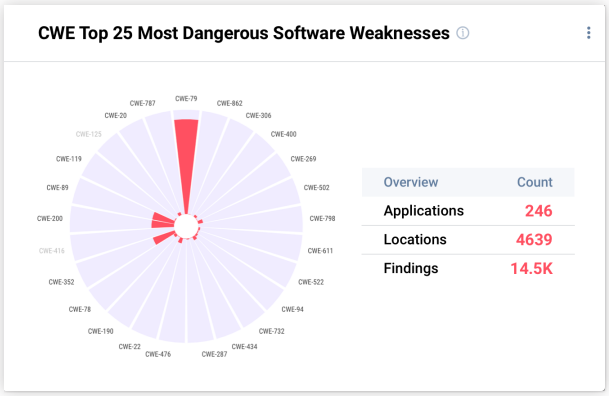
Obtenga una visibilidad completa de la exposición al riesgo de las aplicaciones

Obtenga visibilidad completa de la exposición al riesgo de las aplicaciones, desde el desarrollo hasta la producción. Ivanti Neurons for ASOC unifica todos los datos de análisis de aplicaciones (SAST, DAST, OSS y contenedores) para localizar vulnerabilidades y puntos débiles y priorizar la corrección.



Ivanti Neurons for ASOC es independiente del escáner, lo que permite a DevOps seleccionar las diversas herramientas de escaneado necesarias en las distintas partes del ciclo de vida de desarrollo. El producto normaliza todos los hallazgos de vulnerabilidades y escaneos de aplicaciones y luego los correlaciona continuamente con las amenazas activas de tendencia en la naturaleza, lo que permite a los usuarios saber de inmediato qué hallazgos son el mayor riesgo para su organización. Los usuarios también pueden desglosar las ubicaciones exactas del código donde residen esos hallazgos dentro de las aplicaciones.

Además, el panel de Seguridad de Aplicaciones del producto permite a los usuarios ver el progreso del desarrollo de aplicaciones en el tratamiento de la deuda de seguridad, ofreciendo una visión completa de las vulnerabilidades, CWEs y hallazgos OWASP que exponen las organizaciones, junto con el balance de nuevos hallazgos de escaneo y el ritmo en que se remedian.



Priorizar las acciones inmediatas en función del riesgo de amenaza

Pase de la detección de vulnerabilidades y debilidades a la remediación en minutos -no meses- con una visión contextualizada y basada en riesgos de la postura de ciberseguridad de su organización. Ivanti Neurons for ASOC mide el riesgo y prioriza las actividades de corrección a través de un proceso que implica la correlación continua de las aplicaciones de una organización con::

- Datos sobre vulnerabilidades internas y externas.
- Inteligencia sobre amenazas.
- Pen test manuales y hallazgos basados en la investigación.
- Criticidad de los activos empresariales.

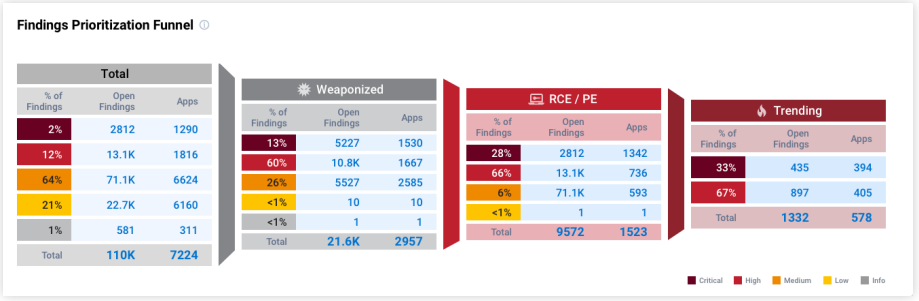
Y lo mejor de todo: se llega a un plan de ataque totalmente informado sin apenas esfuerzo manual.

Además, a diferencia de CVSS, la calificación de riesgo de vulnerabilidad (VRR) propiedad de Ivanti permite a las organizaciones medir con precisión el impacto y determinar la probabilidad de que se explote una vulnerabilidad. Ivanti Neurons for ASOC también identifica específicamente la ejecución remota de código, la escalada de privilegios, el ransomware y las vulnerabilidades activas y en tendencia. Esta información ayuda a las organizaciones a centrarse en aquellas vulnerabilidades que les suponen un mayor riesgo.

Centrarse en la corrección, no en la administración

Mejore su postura de ciberseguridad sin todo el tiempo, esfuerzo y errores tradicionalmente asociados a ello mediante una serie de automatizaciones y otras funciones que mejoran la eficacia:

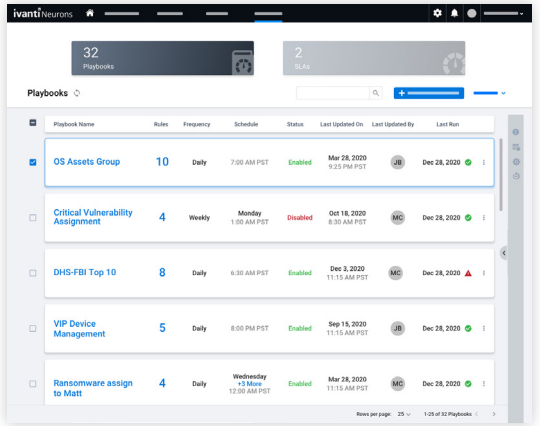
- Cree playbooks para automatizar tareas comunes o repetitivas que tradicionalmente realizan los analistas de seguridad.
- Establezca automáticamente fechas de vencimiento para el cierre de vulnerabilidades si lo desea con automatizaciones de acuerdos de nivel de servicio.
- Reciba alertas casi en tiempo real fuera del producto que enlacen a una página del producto que contenga información relacionada con el evento suscrito.
- Filtre fácilmente aplicaciones y hallazgos de aplicaciones por criterios de tendencias que revelen su exposición a las principales vulnerabilidades críticas -como ransomware y CVE de tendencias- mediante vistas del sistema impulsadas por el equipo de seguridad Ivanti.



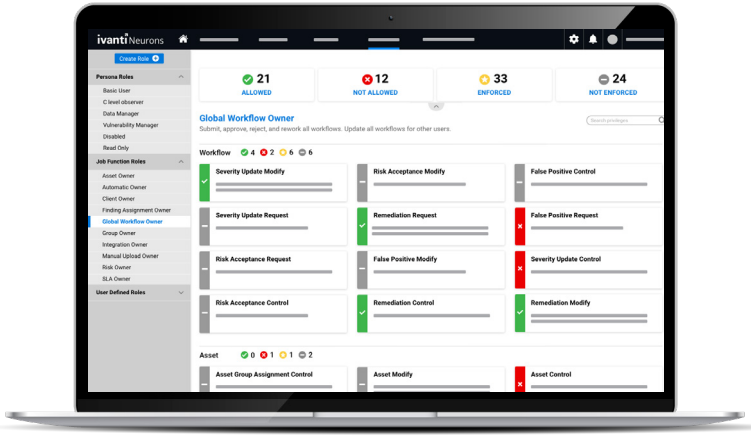
Mejorar la colaboración entre las partes interesadas en la seguridad

Cultive la comunicación y la cooperación entre las partes interesadas en la seguridad de toda la organización proporcionándoles información oportuna y relevante para sus funciones. Ivanti Neurons para ASOC emplea el control de acceso basado en roles (RBAC) para que el acceso al producto se pueda proporcionar de forma segura a todo el personal aplicable.

Una vez dentro del producto, los usuarios tienen acceso a cuadros de mando diseñados para personal desde el SOC hasta la C-suite. Pueden modificar estos cuadros de mando para adaptarlos a casos de uso más específicos, o incluso aprovechar los widgets de usuario para crear cuadros de mando personalizados que satisfagan las necesidades exactas de las distintas funciones y equipos.



Además, el producto cuantifica el perfil de riesgo de una organización en forma de una puntuación Ivanti RS^3. Esta puntuación garantiza que todas las partes interesadas en la seguridad estén de acuerdo con el nivel de seguridad general de la organización. Las integraciones bidireccionales con sistemas de tickets como Ivanti Neurons para ITSM mejoran la coordinación entre quienes trabajan para mejorar ese nivel de seguridad.



Caracteristicas y funcionalidades

Funcionalidades	Función
Diversas fuentes de datos	Obtenga una visión amplia del riesgo cibernético con un producto que ingiere datos de escáneres de aplicaciones (SAST, DAST, OSS, contenedor), hallazgos de vulnerabilidades de más de 100 fuentes, hallazgos manuales de equipos de investigación y pruebas de penetración, y fuentes de datos personalizadas.
Motor de amenazas	Obtenga información inigualable sobre vulnerabilidades, como las relacionadas con el ransomware, a través de inteligencia sobre amenazas generada por humanos e impulsada por IA y procedente de Ivanti Neurons for Vulnerability Knowledge Base.
Calificación del riesgo de vulnerabilidad (VRR)	Determine rápidamente el riesgo que plantea una vulnerabilidad con puntuaciones numéricas de riesgo que tienen en cuenta sus atributos intrínsecos y el contexto de amenaza del mundo real.
Ivanti RS³	Obtenga una visión cuantificada del perfil de riesgo de su organización mediante una metodología de puntuación propia que tiene en cuenta el VRR, la criticidad empresarial de los activos, la información sobre amenazas y la accesibilidad externa.
Automatización	Sustituya una serie de tareas manuales por la automatización para que los empleados puedan centrarse en acciones correctoras e iniciativas estratégicas en lugar de en la administración.
Alertas y notificaciones	Conozca al instante los acontecimientos pertinentes mediante alertas casi en tiempo real enviadas desde un motor de notificaciones. Del mismo modo, dirija a otros usuarios a información importante dentro del producto mediante enlaces profundos.
Organización de datos personalizable	Descubra información práctica con widgets de usuario que permiten la creación de cuadros de mando personalizados, además de la posibilidad de pivotar datos en vistas de listas.
Paneles	Obtenga capacidades superiores de consulta visual y descubrimiento de riesgos en activos e infraestructuras a través de cuadros de mando listos para usar y personalizables, equipados con capacidades de desglose.
Puntos de vista basados en las amenazas	Descubra rápidamente cómo se manifiestan en su entorno las principales vulnerabilidades críticas, como Log4j y las asociadas a las versiones del martes de parches, utilizando vistas basadas en amenazas. Cree y comparta también sus propias vistas personalizadas.
Integraciones a Neurons	Empareje Ivanti Neurons for ASOC con Ivanti Neurons for RBVM para ampliar la gestión de vulnerabilidades basada en riesgos a un área mayor de su superficie de ataque. Aproveche una integración lista para usar con Ivanti Neurons para ITSM para permitir que los profesionales de gestión de vulnerabilidades de toda la organización realicen sus tareas de manera más eficiente y eficaz.

About Ivanti

Ivanti eleva y asegura el trabajo en todas partes para que las personas y las organizaciones puedan prosperar. Hacemos que la tecnología trabaje para las personas, no al revés. Los empleados de hoy en día utilizan una amplia gama de dispositivos corporativos y personales para acceder a aplicaciones y datos de TI a través de múltiples redes para seguir siendo productivos donde sea y como sea que trabajen. Ivanti es una de las únicas empresas tecnológicas que encuentra, gestiona y protege cada activo de TI y punto final de una organización. Más de 40.000 clientes, incluidos 88 de las 100 empresas de Fortune, han elegido Ivanti para que les ayude a ofrecer una excelente experiencia digital a sus empleados y a mejorar la productividad y eficiencia de los equipos de TI y seguridad. 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, visite ivanti.com
y siga @GoIvanti.

Copyright © 2023, Ivanti. All rights reserved. IVI-2674 11/23 NH

ivanti

For more information, or to contact Ivanti, please visit ivanti.com

1. Veracode, "State of Software Security v12", 2021. https://info.veracode.com/report-state-of-software-security-volume-12.html
2. Cyber Security Works, Cyware, Ivanti, Securin, "2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management", 16 February 2023. https://www.securin.io/ransomware/
3. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/