Principios para un uso ético de sistemas IA en ciberseguridad

kaspersky bring on the future

kaspersky.com

Machine Learning:

https://www.kaspersky.com/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

Nuestro mundo está cambiando rápidamente a medida que las tecnologías avanzadas desempeñan un papel cada vez más crucial. En particular, estamos presenciando el desarrollo activo de la inteligencia artificial (IA), que ya está aportando muchos beneficios al mundo, incluida una mejora en la ciberseguridad. Con la proliferación de nuevas amenazas, resulta imposible detectarlas todas de manera manual. Durante años, los algoritmos IA se han aplicado para automatizar y acelerar el proceso de detección, reconocer anomalías y mejorar la precisión en la identificación de malware. Es importante destacar que Kaspersky ha estado utilizando el aprendizaje automático (ML), que puede considerarse como una subdisciplina de la IA, en sus soluciones. Pero, el uso de la IA no está libre de riesgos y, por lo tanto, requiere un enfoque responsable de todas las partes involucradas.

Por ello, con el fin de liderar la innovación en beneficio de todos, Kaspersky establece los siguientes principios éticos para el desarrollo y uso de la IA/ML en ciberseguridad. También invitamos a otras empresas de ciberseguridad a unirse y seguir estos principios.

#1
Transparencia

Los clientes tienen derecho a estar informados sobre el uso de tecnologías IA/ML por parte de una empresa en sus productos y servicios. Por lo tanto, **nos comprometemos a explicar los principios de cómo operan y se utilizan las tecnologías IA/ML en nuestras soluciones**. Dentro de la Iniciativa Global de Transparencia, operamos un creciente número de Centros de Transparencia en todo el mundo, donde nuestros clientes y otras partes interesadas pueden revisar los procesos de desarrollo de Kaspersky, incluyendo aquellos que usan las tecnologías de IA/ML, y examinar la integridad y confiabilidad de los productos y soluciones de Kaspersky. Siguiendo el principio de transparencia, **nos comprometemos a desarrollar sistemas de IA/ML lo más interpretables posible y a introducir las salvaguardias necesarias para garantizar la validez de los resultados proporcionados por estos sistemas**.

#2
Seguridad

Cómo securizar el Machine Learning en sistemas de seguridad

https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/machine-learning-cybersecurity-whitepaper.pdf

Cómo confundir las redes neurales antimalware. Ataques adversarios y prottección:

https://securelist.com/how-to-confuse-antimalware-neural-networks-adversarial-attacks-and-protection/102949/

Una vez inroducidos en el mundo real, los algoritmos IA/ML podrían ser vulnerables a diversas formas de ataques diseñados para forzar a estos sistemas a cometer errores deliberados. En ciberseguridad, el coste de cometer errores en la detección de amenazas es alto, por lo tanto, es crucial centrarse en la seguridad y la resiliencia en lo que respecta a posibles amenazas. **Para nuestros sistemas de IA/ML, nos comprometemos a dar prioridad a la seguridad en el desarrollo y uso de estos sistemas.** Esto se logra mediante la implementación de medidas rigurosas para garantizar la calidad de todos los sistemas de IA/ML. Los pilares clave de estas medidas incluyen la realización de auditorías de seguridad específicas para ML/AI y 'red teaming'; minimizar la dependencia de conjuntos de datos de terceros en el proceso de entrenamiento; un funcionamiento conjunto basado en un diseño de protección multicapa; dar preferencia a las tecnologías de ML basadas en la nube con las salvaguardias necesarias en lugar de modelos instalados en las máquinas de los clientes.

#3
Control Humano

A medida que el malware muta con trucos como la ofuscación de código, el empaquetado, el cifrado, la generación de código dinámico, etc., se necesita una opinión experta, especialmente para el análisis de APTs (Amenazas Avanzadas Persistentes) y otras amenazas complejas. Con el fin de proporcionar la mejor protección, n**os comprometemos a mantener el control humano como un elemento esencial en todos nuestros sistemas IA/ML**. Aunque nuestros sistemas IA/ML están diseñados para funcionar de manera autónoma, su rendimiento es supervisado de forma continua por especialistas. Con acceso en tiempo real a información sobre amenazas de en curso y entrantes, los expertos utilizan su conocimiento para corregir el funcionamiento de nuestros sistemas IA/ML si es necesario y adaptarlos para enfrentar las nuevas amenazas emergentes. Para proporcionar una protección integral contra amenazas cibernéticas en constante evolución, Kaspersky combina algoritmos de ML con la experiencia humana, respaldada por datos de inteligencia de amenazas a gran escala.

#4
Privacidad

Procesamiento de datos: https://www.kaspersky.com/about/data-protection

El big data desempeña un papel vital en la implementación de sistemas IA/ML, donde parte de los datos que se pueden utilizar pueden calificarse como información personal. Por ello, un enfoque ético para el uso de tales datos debe tener en cuenta de manera integral la privacidad de las personas. Por lo tanto,**nos comprometemos a respetar los derechos de las personas a la privacidad**. Desde una perspectiva de ciberseguridad, esto puede suponer desde limitar el procesamiento, reducir la composición de datos, seudonimizar o anonimizar siempre que sea posible, garantizar la integridad de los datos y aplicar otras medidas técnicas y organizativas para proteger datos y sistemas, y asegurar el ejercicio significativo de los derechos, todo con el objetivo de proteger la privacidad de las personas.

#5
Desarrollada para ciberseguridad

Construir y mantener la confianza dentro de la comunidad de ciberseguridad y entre los usuarios es fundamental. En línea con los valores fundamentales de Kaspersky centrados en proteger a individuos y organizaciones y en construir un mundo seguro,**nos comprometemos a utilizar sistemas IA/ML exclusivamente con fines defensivos.**Para nosotros, la reputación e integridad de una empresa son activos vitales. Al centrarnos exclusivamente en tecnologías defensivas, seguimos nuestra misión y demostramos nuestro compromiso de proteger a los usuarios y sus datos, mejorando así nuestra reputación como proveedor de ciberseguridad responsable. Creemos en un futuro en el que la tecnología mejora la vida de todos nosotros. Es por eso que la aseguramos, para que todos, en todas partes, puedan beneficiarse de las innumerables oportunidades que ofrece.

#6
Abiertos al diálogo

Contribución al diálogo en el Grupo de Trabajo sobre seguridad de y en el uso de las TIC:

https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Kaspersky_SUBMISSION_OEWG_MAY_22.pdf

Estamos comprometidos en promover el diálogo con todas las partes interesadas para compartir las mejores prácticas en el uso ético de la IA. En este sentido, Kaspersky está dispuesta a entablar conversaciones con todas las partes, incluyendo el seno de las Naciones Unidas (Pacto Digital Global, Grupo de Trabajo de Ciberseguridad de la ONU, Foro de Gobernanza de Internet, etc.) y otras plataformas a nivel mundial. Nuestra posición es que solo a través de la colaboración continua podemos superar obstáculos, impulsar la innovación y abrir nuevos horizontes.

Kaspersky estará encantado de compatir opiniones sobre el uso de la IA en ciberseguridad. En caso de estar interesado en recibir información adicional sobre estos principios, no dude en contactar con nosotros: TransparencyCenter@kaspersky.com

Cyber Threats News: securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com