An AI allows companies to collaborate on cybersecurity without sharing sensitive data

Risk Advisory Firm

Persistent

Digital Case Study Awards 2022

Technology

North America

ISG

Opportunity

The client is a cybersecurity advisor seeking to develop a new tool to better detect cyberattacks. They devised a concept for a sandbox that would allow multiple companies to collaborate without exposing their private or confidential data with one another.

Their goal was to use machine learning to study cyberattack attempts against multiple companies and improve the ability for all participating organizations to detect similar attacks. As a cybersecurity advisor, this capability would be a basis to create significant value for their clients and improve their own leadership position as a leading advisor in this market.

Imagining IT Differently

The client started with a vision and Persistent Systems helped them define specific goals and translate the vision into an actionable roadmap.

To address the privacy requirements of every organization, the solution designed by Persistent Systems uses a federated learning model to decentralize how the machine learning algorithm studies each set of information.

This design allows the AI to be trained using insights from each organization without risking the exposure of the raw data.

Future Made Possible

This new solution significantly altered the client's cybersecurity offerings, helping them reach new customers and markets.

According to the client, this new capability improved the accuracy of cybersecurity attack detection by 38%, compared to other methods. And all of the companies involved were able to mutually benefit from that accuracy without compromising their privacy.

According to ISG, this work is an excellent example of the power of a co-creation ecosystem, enabled by a provider.

ISG