Investing in cyber security innovation

Client story

Client
Diversified financial services firm

Sector
Financial services

Project
Cyber security transformation

Client challenge

When your entire brand is built on trust, you have to know you can weather a surge in cyber crime – especially when you're a financial services household name and your customers' money is at stake. And when you're competing for millennial customers in particular, you have to make it easy to do business through a variety of digital channels and platforms – even if doing so raises the risk of data breaches. What's the solution? Proactively leverage the latest technologies in artificial intelligence (AI) and machine learning to detect, counter, and prevent sophisticated cyber attacks in real time.

Benefits to client

KPMG's solution combines the client's existing cyber security toolkit with customized machine learning and AI capabilities to help eradicate risks in a scientific, repeatable, and proactive way. By automating manual processes, the prototype:

- Increases cyber-security accuracy, based upon analysis of one billion records per week from six data sources. During initial two-month adoption period, more than 2,000 account-takeover attempts identified.
- Improves forensic and predictive capabilities: 50 previously unknown detection signals now ranked by importance, and attack-probability percentiles used to prioritize manual review cases.
- Quickly identifies high-volume and under-the-radar attack patterns for immediate remediation; faster reporting of significant account deviations.
- Maps physical access to digital location to spot trends faster.
- Launches a reusable machine learning architecture – with engineering, workflows, and embedded roadmaps to support additional cyber-use cases and remediation steps.

KPMG response

Having worked with the client on numerous strategic initiatives, we were deeply familiar with its technology, operations, strategic direction, and business priorities. That's why we offered to co-innovate with the firm on one of its most pressing issues: the transformation of its cyber security capabilities.

Combining expertise from our cyber, forensics technology, financial services, and data and analytics teams, we proposed a visionary solution: an enterprise-wide cyber risk platform that learns from datasets. The framework triggers alerts and responses, by compares the top cyber-attacks in real time against the company's customized tolerance levels. As the model evolves, it is even expected to start providing predictive recommendations for pre-emptive action.

KPMG's solution takes available open-source libraries, big-data platforms and machine learning tools, then ties them together with client-specific machine learning and AI capabilities. The machine-learning capabilities cross-references relevant data, traditionally siloed in each tool and acts on them in real time. The organization gains insights it didn't know existed.

Unlike organizations that can only react to incidents, the client can monitor itself and respond to risks and anomalies before they become problematic. One example: A login session with uncharacteristic behavioral identifiers can be automatically flagged when someone attempts to update bank account activity or perform a high-risk transaction.

As more of these transactions occur apart from the physical branch – through the mobile and web channels that digital-native millennials prefer, for instance – these detection capabilities become especially important. Over time, the customer security experience can be continually enhanced, with additional analytics drawn from select data attributes and key risk indicators.

By identifying both high-volume and under-the-radar cyber attack patterns, this KPMG prototype can protect the company's core business, allowing the firm to pursue new opportunities with agility and confidence.

KPMG insights

Data brings with it great power, and great responsibility.
AI and machine learning can transform an organization's cyber security initiatives if the client leverages a multi-dimensional team (data scientists, cyber security experts, forensic specialists, and security architects) and takes a holistic perspective rather than focusing on point solutions.

What sounds impossible is really possible. It's about manageable steps.
Implementing intelligent cyber security measures involves three phases. The first phase describes how you want to prioritize your problem statement, second determines use of your data and what you want to learn, and the third provides the intelligence at scale.

We're here to help with the behavioral implications of data transformation.
KPMG frameworks s allows you to retrain existing resources to take on new responsibilities and also attract new talent excited to work with next-generation technology.

If you are interested in learning more about this case study, or if you are experiencing similar issues, please contact us.

Vijay Jajoo
vjajoo@kpmg.com
415-963-8698

Anthony Gawron
agawron@kpmg.com
312-665-3379

For more information on how KPMG can help turn cyber risk into opportunity, go to: kpmg.com/us/cyber.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.