KPMG Intelligent Cyber Analytics Program (kiCAP)

Powered by **KPMG Ignite**

Cyber criminals are winning in the arms race of enterprise network security.

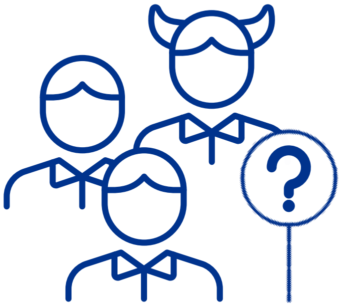
As digital channels increase and the demands on the organizations grow, the quantity of threat exposures and complexity of the attacks are growing significantly.

Cyber criminals capitalize on static and incomplete controls that still define the security landscape for many businesses.

Organizations need to ask themselves some vital questions

How consistently are we protecting our customer across channels and products?

Do we have the data insight and infrastructure to identify, measure and respond to threats in real life?



What are my cyber risks and how do I know they're within our tolerance?

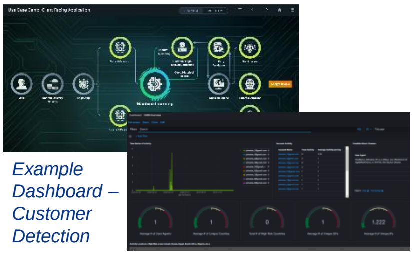
How can we proactively detect attacker activity before it affects the business?

What would be the impact of leveraging your existing technology and data to their full potential?

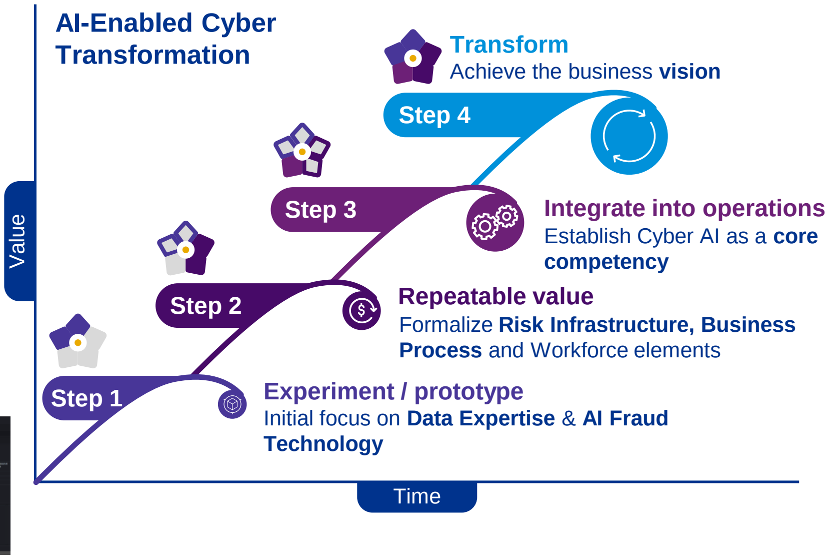
It is a journey to transform to next generation cyber defense with Advanced Analytics and Machine Learning.

Many organizations take a step-by-step approach, with discrete projects building AI capabilities along the way.

KPMG Intelligent Cyber Analytics Program (kiCAP) can enable and accelerate your Security Organization in the adoption of AI-enabled cyber enterprise security.



Example Dashboard – Customer Detection



AI-Enabled Cyber Transformation

Transform
Achieve the business **vision**

Integrate into operations
Establish Cyber AI as a **core competency**

Repeatable value
Formalize **Risk Infrastructure, Business Process** and Workforce elements

Experiment / prototype
Initial focus on **Data Expertise** & **AI Fraud Technology**

Example KPMG Intelligent Cyber Analytics Program (kiCAP) offerings

KPMG provides client-deployable accelerators to solve top security challenges using AI/ML

Example solutions supported by over 120 KPMG developed features.

IAM Provisioning

Insufficiently structuring Identity Access Management can allow an attacker to efficiently navigate the network of an organization, gaining permissions and access.

Component Firmware

Some adversaries employ mature means to compromise PC components and install malicious firmware that will execute adversary code outside of the operating system.

Ransomware Attacks

The deployment of ransomware within an environment has the potential to cripple or halt core business processes if executed in the right place of a company's infrastructure.

Process Exploitation

With an in-depth understanding of company procedures, an attacker may be able to exploit these for monetary gain like having the company call an attacker-owned Toll number.

Rogue Access Points

An adversary adds an unauthorized Access Point to the corporate network. This can give the attacker access to company networks, information, or databases as if a legitimate employee.

Credential Stuffing

Large numbers of leaked credentials are entered into websites until they are potentially matched with an existing account.

Domain Impersonation

Without proper domain monitoring, attackers may purchase domains similar to a legitimate business in order to impersonate them.

Cryptominers

Malware-infected systems are increasingly being infected with Cryptomining software to use valuable company resources to mine cryptocurrencies.

Account Takeover (for O365)

Using credentials found elsewhere, an attacker can attempt to log into a legitimate user's account and use their account for nefarious purposes.

File-less Malware

An ever growing form of malware no longer uses executable files to run and leave forensic artifacts in the process. The malware instead executes in browser plugins / within programs themselves.

Email Escalation

Email is being weaponized to steal user credentials and deliver malware. As security teams review many sophisticated messages, there is a need to integrate existing tools.

C2 Detection

Malware routinely imbeds command-and-control (C2) ability, enabling attackers to control compromised machines in a client's environment. ML can detect C2 activity to identify infected hosts.

Exfiltration (via Malware)

Once inside environments, attackers often install malware that can send information that they have stolen back to a server that they can access outside of the company's environment.

Distributed Denial-of -Service Attacks

Like a Denial-of-Service Attack, a Distributed Denial -of-Service Attack aims to flood systems, servers, or networks with traffic to attempt and exhaust resources and bandwidth.

kiCAP Deployment Options

There are several deployment options available, in order to cater to a client's specific need, scope, size and business challenge.

Option 1 ● ○ ○

Proof of Value (POV)
4-6 weeks ~$150K

Non-scalable, smaller-scale use case / analysis and reporting.

Non-production analysis leveraging a VM / single server platform (For prototyping, development and proof-of-value).

Option 2 ○ ● ○

Minimal Viable Product (MVP)
6-12 weeks ~$400K

AI backbone build and solve for an initial cyber challenge

Deploy on cloud or on-prem infrastructure.

Option 3 ○ ○ ●

Program Implementation
6-12 months ~$2-4M

Complete AI capability transfer

Scalable production environment with people, process, and technology training solving for 6 top security threats

Scale of Transformation delivered through the program

KPMG intelligent Cyber Analytics Program (kiCAP) | Powered, connected and trusted

We have outstanding Cyber fraud risk and data science/ analytics credentials and bring to bear strong alliance relationships with leading cloud providers.

Services

- Cyber analytics strategy, roadmap and readiness
- Security data lake – target state architecture design
- Front/middle/back office data store, data quality, data normalization and infra design (Cloud or on-prem)
- POC and MVP accelerators
- Cyber analytics governance and operating model
- Transformation and Integration(Platform Architecture, data model design, integration and enforcement with security / fraud tools)
- KRI dashboards with real-time insights
- Integration within POWERED and CONNECTED initiatives
- Managed Services (Run "OUTCOME" as a Service)

Value proposition / How KPMG can help

KPMG's cross functional experts from Cyber Security, Data Science, Fraud analytics, Customer solution, AML, Digital Experience, and Risk and Compliance, among other practices, help you establish / maintain TRUST with your stakeholders, by connecting KEY data sets / metrics, to identify threats/anomalies and transform security/risk capabilities using advanced analytics / automation

Contact

Vijay Jajoo
vjajoo@kpmg.com

Sreekar Krishna
sreekarkrishna@kpmg.com

Anthony Gawron
agawron@kpmg.com

Yiwen Zhang
yiwenzhang1@kpmg.com

Tangential services

Fraud / forensic
Security monitoring
Threat hunting
Security intelligence
Access mgmt

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. The KPMG name and logo are registered trademarks or trademarks of KPMG International.