BLACK KITE

Arranged by

Black Kite Research
Led by: Gokcen Tapkan

ARTIFICIAL INTELLIGENCE IN TPRM

The Need, The Use, and The Challenges , Volume 1

INTRODUCTION

While AI reminds us of self-driving cars and robots from the movies, the reality of it all goes much deeper - thanks to ChatGPT and generative AI. Those tools have been the go-to options for creating content, whether it be a piece of code or writing.

AI technologies have been adopted in a variety of verticals for a while – and cybersecurity and compliance are no exception. This ebook focuses on the applications of AI to the TPRM workspace. Our goal is to provide insights into what Black Kite has been doing in the last couple of years (with a sneak peek into its own TPRM AI model.)

According to the IBM Cost of a Data Breach Report 2022, one-fifth of breaches are caused by third parties. The report, conducted by IBM and the Ponemon Institute, is a survey-based report that studies 550 organizations impacted by data breaches occurring between March 2021 and March 2022.

On the other hand, Black Kite's yearly report focuses specifically on third-party breaches that were publicly revealed in the preceding year. The fourth annual Third Party Breach Report by Black Kite revealed that the number of breaches decreased with respect to previous years - while the affected number of companies and cascading individuals increased. This implies that hackers are getting smarter, successfully conducting multi-victim attacks with the cascading effect of said attacks continuing to grow.

Digitalization is now at the core of company operations, giving data access to third parties. Threat actors know this too, often preying on the 'usual suspects:' third parties that will create the biggest impact.

In TPRM, AI allows organizations to seal every single gap in all risk management efforts. Context-aware AI technology tells security experts where to look, specifically among hundreds of thousands or millions of control points.

The Cost of a Data Breach Report 2022 report revealed that breaches at organizations with fully deployed security AI and automation typically cost $3.05 million **less** than breaches at organizations with no security AI and automation deployed. Read further to learn how new AI technologies can further benefit supply chain and third-party risk programs. In saying further, we refer to fine-tunable language models, context-aware models, attack susceptibility models, cleaner alarms, and curated intelligence.

MACHINE LEARNING, LLMS, AND AI: DIFFERENCES

AI is an umbrella term, not one single technology. It refers to all kinds of computer-related technologies that are capable of decision-making – from smart chess algorithms to evolved forms of deep learning (Large Language Models/LLMs).

Unlike the common perception, AI technologies do not always involve machine learning processes. Deep Blue, the IBM chess computer that gained fame in the late 90s and early 2000s, made headlines by defeating world chess champion Garry Kasparov. It utilized an alpha-beta search algorithm and custom hardware that allowed it to analyze up to 200 million positions per second. Rather than a learning technology, Deep Blue's development relied on a search and decision-making algorithm.

In contrast, AlphaGo, a more advanced AI compared to traditional chess engines, employed a general reinforcement learning algorithm. It garnered significant attention in 2017 for its exceptional accomplishments in board games, particularly chess. AlphaGo learns and improves through self-play and training against itself, utilizing various reinforcement learning techniques. In a series of 100 games against Stockfish, a leading chess engine, AlphaZero emerged victorious. This success highlighted AlphaGo's ability to rapidly learn and adapt without any prior human knowledge or pre-programmed strategies.

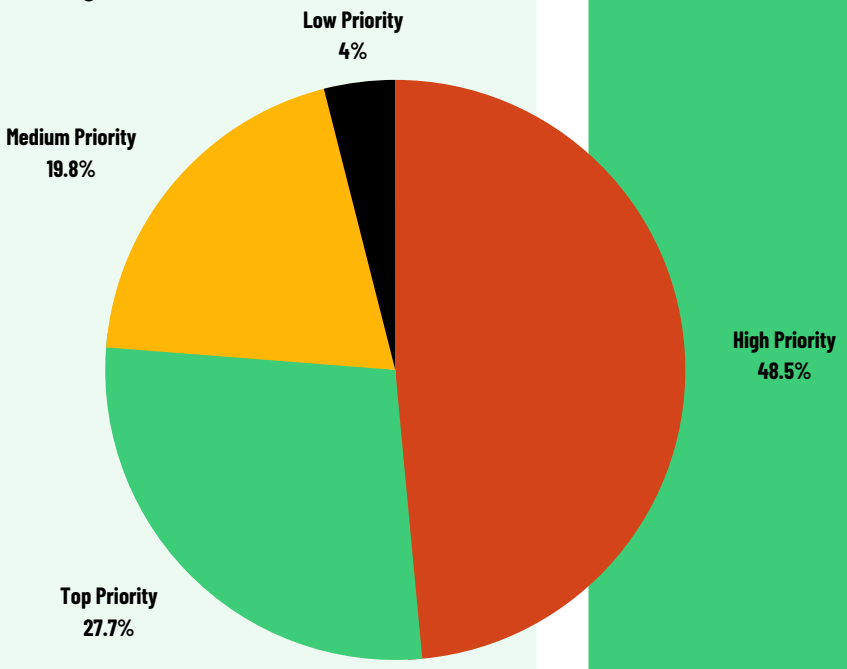
The word "AI" serves as a catch-all for a number of related but separate subfields. This includes, but is not limited to:

- **Machine learning** (ML), a branch of artificial intelligence in which algorithms are trained on data sets to generate machine learning models that can carry out particular tasks.
- **Artificial neural networks** (AANs), which simulate the human brain. These are utilized in deep learning to carry out more sophisticated reasoning tasks autonomously.
- **NLP** is a subfield of computer science, artificial intelligence, linguistics, and machine learning that focuses on developing software that can decipher human communication.
- **Robotics** is a branch of artificial intelligence, computer science, and electrical engineering that focuses on building robots that can learn and carry out difficult tasks.

THE ADOPTION OF AI IN TPRM: THE NEED, THE USE AND THE CHALLENGES

The Need

According to *Forbes*, 76% of enterprises have prioritized AI and machine learning in their IT budgets. This trend is driven by the increasing volume and complexity of data that needs to be analyzed to identify and mitigate cyber threats, among other reasons.



The rationale is the same for the TPRM domain.

Here are a few reasons why an AI-focused TPRM is crucial for organizations:

- Today's security experts invest extensive hours manually carrying out TPRM operations by combining various platforms and knowledge sources. These arduous monitoring duties carry an increased risk of bias or human error as data volume rises. AI-driven tools can streamline risk assessment processes and improve decision-making.

- Traditional approaches to third-party risk management struggle to handle the increasing data volume and variety, hindering effective risk identification and mitigation. However, AI can collect and analyze data from diverse sources, enabling comprehensive risk assessments, continuous monitoring, and effective mitigation throughout the third-party relationship lifecycle.

- AI-powered technologies offer the potential to revolutionize third-party risk management by leveraging advanced algorithms to analyze vast amounts of data, detect patterns, and make more accurate risk predictions.

- By harnessing the power of machine learning, natural language processing, and network analysis, AI can enable organizations to proactively identify and address risks associated with their third-party relationships.

The Use

Question: What is the best TPRM program?
Answer: The one that is scalable and sustainable!

The need for automation in TPRM is undebatable. Automation is the key to scalability and sustainability in a successful TPRM program.

Gartner recognizes the potential of AI in enhancing TPRM practices. Here are a few points that Gartner has highlighted as potential areas where TPRM can benefit from AI:

- **Risk Assessment:** AI can help automate the risk assessment process by analyzing large amounts of data from third-party sources, identifying potential risks, and providing risk scores or rankings.

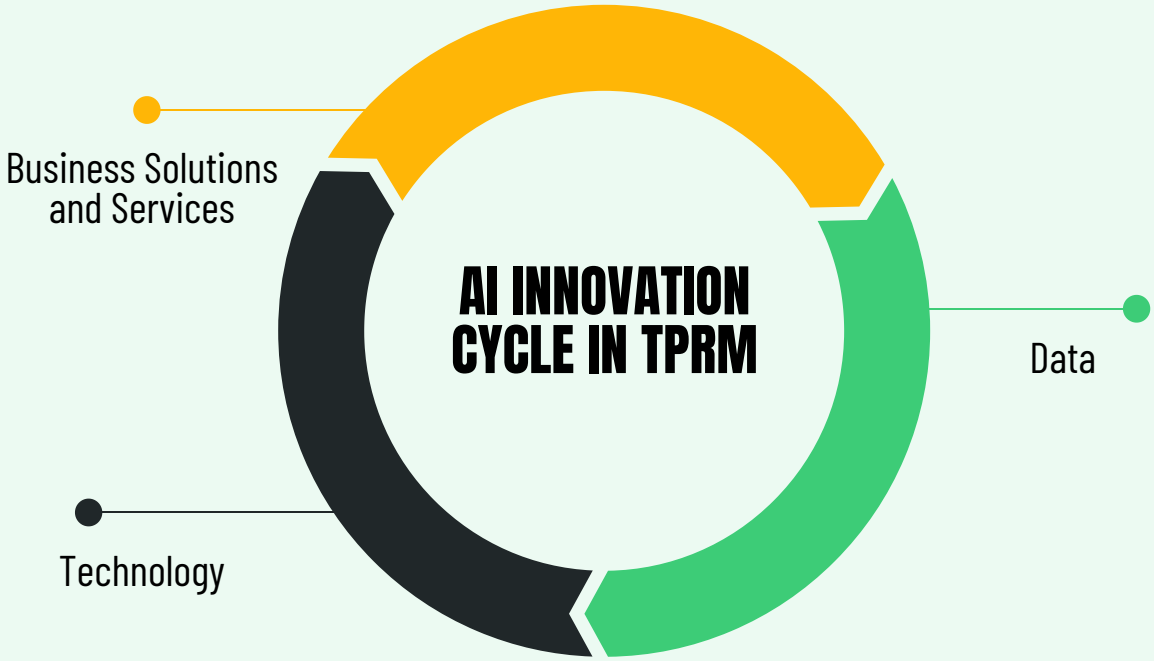
- **Due Diligence:** AI can assist in conducting due diligence on third-party entities by analyzing information from various sources, such as financial records, legal databases, news articles, and social media, to identify any red flags or potential risks.

- **Monitoring and Alerting:** AI-powered systems can continuously monitor third-party activities and detect any abnormal or suspicious behavior. These systems can provide real-time alerts to TPRM teams, enabling them to take immediate action.

- **Natural Language Processing (NLP):** NLP algorithms can be used to extract and analyze unstructured data from contracts, agreements, and other documents, helping TPRM teams to identify contractual risks, compliance issues, and obligations.

- **Predictive Analytics:** AI algorithms can analyze historical data and patterns to predict future risks associated with third-party relationships. This can help organizations proactively address potential issues before they occur.

The Challenges



- **Business Solutions & Services**: Quality vs. delivery time is always an issue in the business world. Today delivery-time constraints are even shorter in order to adapt to shifts in technology. This part becomes critical, where feasibility must be considered, prior to taking data, human resources, and available technology into account. The right time and right place make a huge difference in fueling this circle.
  - **Set-Backs:** Immature technology (for some workspaces), lack of context in TPRM, customer adaptation
  - **Opportunities:** Ready-to-use AI tools and technology, dynamic AI landscape, the share of know-how on AI tools, the need for (further) supply-chain automation

- **Data:** Data is the key to developing technology and business solutions. Remember - garbage in, garbage out. AI models typically require high-quality and well-labeled data. Unfortunately, data labeling requires significant human resources. Most businesses solely give up on AI applications for this reason. Business solutions enrich the data in return by creating feedback from users.
  - **Set-Backs:** Lack of initial data, data usage restrictions, consent issues, data quality
  - **Opportunities:** More data when in production, finer applications with more data

- **Technology:** Technology is a solution & service enabler. However, technology competition makes it necessary to keep its adaptation process and time-to-market shorter. The learning curve in the technology is a game-changer in fueling the innovation cycle
  - **Set-Backs:** Learning curve, competition, often shifts, explainability
  - **Opportunities:** Learning curve, more applications

UNIQUE PARSER 2.0, A SMARTER PARSER WITH A FINE-TUNED NLP ALGORITHM

In general, compliance means abiding by a set of rules. Compliance in corporate and organizational management environments refers to ensuring that your business and its personnel comply with all applicable laws, rules, regulations, standards, and ethical guidelines. It also includes abiding by local, state, and federal laws and corporate policies.

Regarding Information and Cyber Security Compliance, there are different standards and best practices depending on the company's geography, sector, and business environment.

Let's shift to the perspective of a vendor. Each company, the vendor, is in a business deal that requires a different standard. For each business, typically that vendor has to fill in a separate questionnaire shaped around a different standard, framework, or regulation.

The original Black Kite Unique Parser (1.0) was an intelligent parser that read and mapped documents to various industry standards and Black Kite cybersecurity controls. The purpose was to reduce time spent on compliance efforts while reducing errors and subjectivity. From a supply chain security management viewpoint, this level of automation has the potential to save companies a considerable amount of human effort.

An AI with a Security Certification

Black Kite Research recently launched Unique Parser 2.0, a document parser and a natural language processing model now fine-tuned for the cybersecurity domain. The former parser, Unique Parser 1.0 utilized a generic language model as the AI engine.

To better understand the difference between Unique Parser 2.0 from 1.0, let's consider the following analogy.

> Consider an individual who can read, understand, and speak English. Someone randomly picked from the crowd. They read information sources such as Wikipedia and know basic concepts. When you say to them, “Abraham Lincoln is a Hollywood actor living in LA,” they can say, “You are wrong!” They have a certain level of “intelligence.”
>
> The individual's cybersecurity and TPRM knowledge is average, as is the case for many other domains. When you talk about “physical security” and “cloud access control,” he can say, “You are talking about security, right? Those two mean the same”. **Is it?**

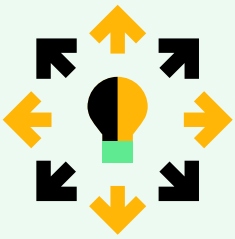
While a generic AI might miss the nuances between the confidentiality of data at rest and in transit, an AI specifically tuned to the cybersecurity and TPRM domain understands that those two concepts are different. You can think of it as the “training of an English-speaking individual in the cybersecurity and TPRM domain.”

UNIQUE 2.0 now correlates compliance documentation to industry standards, best practices, regulations, and even vendor’s custom frameworks in an ad-hoc fashion. It is an automated compliance solution on its own.

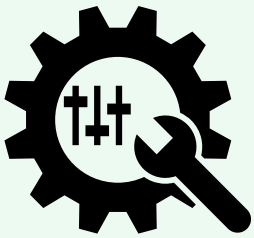
Some of the key features that have improved in Unique Parser 2.0 are:

Less Human Effort

Scalability through Intelligence



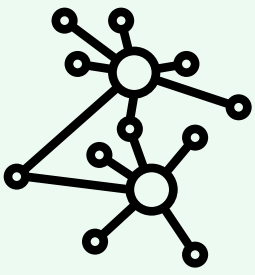
Customizable to your TPRM needs



Less Error

Context Awareness through Tuning

Full correlation within the platform
(+your custom framework)



HOW IT COMPARES TO CHATGPT AND ALL OTHER AI MODELS

Unique Parser 2.0 utilizes a fine-tuned language model. This model is specifically tuned in embedding and deriving similarities between texts in the TPRM and cybersecurity domains. While it is not a generative AI such as ChatGPT or Google's PALM engine, it can be considered an embedding engine that maps text to vectors in an N-dimensional universe. The similarity score is the cosine distance between vectors – the closer the higher the similarity score.

WHAT IS FINE-TUNING?

Fine-tuning is a transfer learning approach where a model is initially trained on one dataset and then trained again on a smaller domain-specific dataset. To avoid disrupting the adjusted weights of the underlying language, a lower learning rate is typically used. Additionally, it is possible to utilize a base model for a similar task, freezing certain layers to retain prior knowledge while training with new data. The output layer can also be modified, with some portions frozen during the training process.

The following benchmark shows cosine similarity scores coming from UNIQUE 2.0 embedding engine, and Ada embedding engine: text-embedding-ada-002.

Model Name	Spearman Correlation	F1 score	Precision
Unique 2.0 engine	0.61	0.67	0.74
Ada engine	0.58	0.59	0.71

For a similarity task, all sentence/text pairs are either labeled 0 or 1, directly translating into dissimilar/similar. The models label the text pairs based on the model threshold. Model thresholds are optimized for the best f1 score with maximum tolerance for false positivity.

Therefore, we have true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) based on the AI model outcome.

Text 1	Text 2	Similarity	True Label	Model_X Outcome	FN,TN,TP,FP
Do Incident Response Plan notification procedures require notifying any required government self regulatory or other supervisory bodies within hours from the determination that Cybersecurity Event with reasonable likelihood of materially harming any material part of normal business operations has occurred?	Incident Response Assistance. The organization provides an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Similar	1	0	False Negative
Is a website, mobile, or digital service privacy policy developed, maintained, published, and communicated to users on devices or applications that have access to client-scoped privacy data?	Does your company utilize MFA for access to systems that contain private confidential proprietary data?	Dissimilar	0	1	False Positive

The Metrics used in Model Evaluation

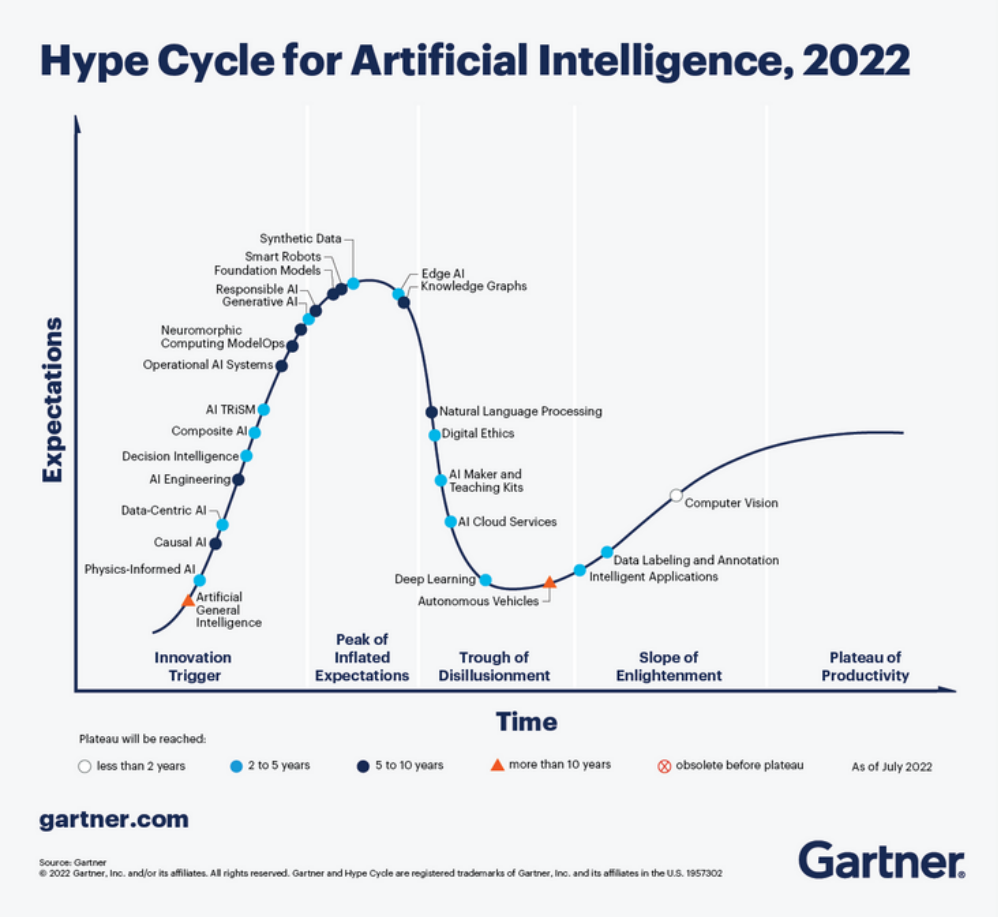
- **Spearman:** The Spearman correlation between two variables is equal to the Pearson correlation between the rank values of those two variables; while Pearson's correlation assesses linear relationships, Spearman's correlation assesses monotonic relationships.

- **F1 score:** F1 score is an evaluation metric for classification problems. It is a harmonic mean of precision and recall, where precision is the ratio of true positives to all positive results, and recall is the ratio of true positives to all relevant results. A high F1 score indicates a high accuracy of the model.

- **Precision:** The precision is the ratio TP / (TP + FP) where TP is the number of true positives and FP is the number of false positives. The precision is intuitively the ability of the classifier not to label as positive a sample that is negative.

AI APPLICATIONS IN TPRM

According to *Gartner*, they see generative AI as ""“becoming a general-purpose technology with an impact similar to that of the steam engine, electricity, and the internet. The hype will subside as the reality of implementation sets in, but the impact of generative AI will grow as people and enterprises discover more innovative applications for the technology in daily work and life."



The ease of application building fueled the other markets to integrate AI into their workspace. AI will be crucial in addressing cybersecurity challenges in the TPRM domain by detecting and responding to threats in real-time, identifying vulnerabilities, and helping teams strengthen overall security measures.

TPRM and cybersecurity are such domains where there will be more “Intelligent Automation” in the future. Supply-chain threat forecasting, customer-tuned artificial intelligence, and customer experience are just a few areas that will impacted by AI in TPRM and cybersecurity workspaces.

FINAL WORDS

BOB MALEY, CISO OF BLACK KITE

Artificial Intelligence (AI) holds immense potential to revolutionize Third Party Risk Management. As we navigate an increasingly interconnected world, the complexity and scale of managing third-party risks have grown exponentially.

AI, with its ability to analyze vast amounts of data and identify patterns beyond human capacity, can be a game-changer in this field. It can enhance our agility, enabling us to respond swiftly and effectively to emerging threats. By leveraging AI, we can gain a strategic advantage, staying ahead of potential risks and getting inside the adversary's OODA (Observe, Orient, Decide, Act) loop.

However, it is crucial that we approach this technological advancement with a discerning eye. The market is saturated with AI-related products and services, each accompanied by its own set of promises and hype. While some of these offerings may be transformative, others may fall short of their claims. It is our responsibility to sift through the noise, critically evaluate each solution, and identify those that truly have the potential to elevate our risk management capabilities.

Moreover, our commitment to AI must extend beyond mere adoption. We must continually strive to improve and refine these technologies, tailoring them to our unique needs and challenges. AI is not a one-size-fits-all solution; it is a tool we can and should mold to serve our specific objectives. This requires ongoing investment in research, development, and training and a culture that encourages innovation and learning.

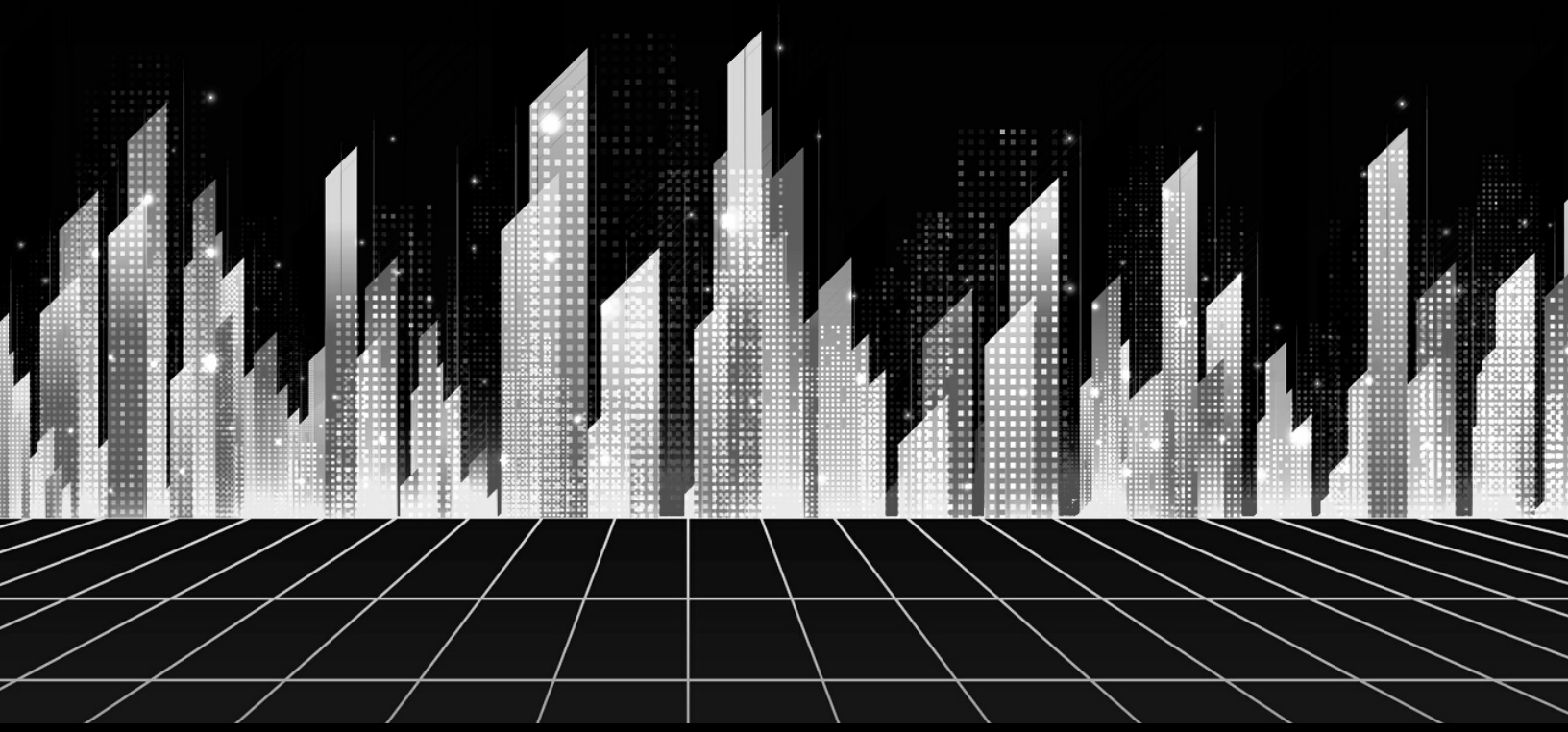
AI represents a powerful tool in our arsenal for Third Party Risk Management. Embracing it can significantly enhance our agility and effectiveness in managing risks. However, we must approach it with a critical eye, avoiding the trap of marketing hype, and commit to its continual improvement. By doing so, we can harness the full potential of AI, transforming our risk management capabilities and staying ahead of the curve in an ever-evolving threat landscape.

ABOUT BLACK KITE

Our deep insights help you ease the stress of cyber ecosystem risk management. We do this by giving you more than a risk score. Our automated system provides real-time and accurate risk intelligence. Our data is accurate, reliable and detailed so you can improve business resilience by making informed risk decisions across your entire ever-changing cyber ecosystem.

With Black Kite you get More than a Score™.

EXPERIENCE THE BLACK KITE PLATFORM YOURSELF WITH A FREE CYBER ASSESSMENT



CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston St. Suite 2905
Boston, MA 02199