BLACK KITE
Third Party Risk Platform

Black Kite offers the most trustworthy and comprehensive platform for risk detection and response in your supply chain

Black Kite gives companies a comprehensive, real-time view into cyber third-party risk so they can make informed and proactive risk decisions that help avoid business disruption, building resilience within their supply chain. With one-of-a-kind collaboration capabilities, companies can work directly with their vendors to report, mitigate, and minimize risk, improving their own business resilience as well as their vendors' organizations.

BLACK KITE IS CHANGING THE WAY COMPANIES MANAGE CYBER THIRD-PARTY RISK

Black Kite is building a world where security professionals have scalable tools that provide trustworthy and complete data to illuminate supply chain risk. What makes us different? It is our commitment to offering trustworthy data that can be operationalized to make better business decisions.

Data You Can Trust:

- Black Kite false positive target rate is less than 5%. In practice this is achieved by relying on multiple data sources in evaluating each TTP control point. Typically, there is a requirement that 2 of 3 data sources must agree in order for a finding to be presented. This helps to eliminate noise in findings results as well as improve accuracy as the observed systems change over time.
- Black Kite employs a standards-based methodology in development of the threat matrix and scoring of the controls based on MITRE's CTSA, CWSS and FIRST's CVSS. This standards-based approach facilitates better risk prioritization, which has the downstream impact to help minimize remediation time expenditures.
- Black Kite recognizes that in providing an OSINT outside-looking-in hacker's reconnaissance view of a company, there can be no visibility to compensating controls. To help alleviate this gap, Black Kite utilizes a shared responsibility model for ensuring findings accuracy. Findings may be directly challenged within the platform without delay and without the need for human intervention. The challenges are immediately trusted, however, finding challenges are subject to Black Kite audit review so that the integrity and consistency of Black Kite scoring is maintained.

BLACK KITE
Third Party Risk Platform

TECHNICAL INNOVATION - A MULTI-DIMENSIONAL VIEW OF RISK:

CYBER RATING:

- Black Kite employs a robust approach, utilizing 1,000+ sources and over 300 control points. This results in an unparalleled data pool, delivering 2-4 times more data than competitors.
- Out of the Box Black Kite cross-references data and findings to two independent sources which contributes to an industry low false positive rate of below 5%.
    - In addition, Black Kite allows its customers and its vendors to verify and contribute to findings and digital footprints in real-time. This further improves Black Kite's data quality and false positive rate to below 3%.
- The scoring methodology leverages industry standards MITRE & NIST, enhancing transparency and objectivity when evaluating vulnerabilities. MITRE TTPs and NIST vulnerabilities are used to objectively show the severity level of our findings, making sure your analysts can prioritize the findings for each company.

RANSOMWARE SUSCEPTIBILITY INDEX® (RSI™):

- Black Kite is the only solution in the market to offer a predictive indicator that highlights potential ransomware risks within your supply chain. Black Kite's data is collected from a variety of OSINT sources such as internet-wide scanners, hacker forums, the deep/dark web, and more. The data is also curated from our own research and intelligence team at Black Kite. By using the data and machine learning, Black Kite identifies the correlation between control items in the Cyber Risk Assessment and access methods used by ransomware groups to provide these approximations.
- RSI™ is leveraged by enterprises around the world as a probabilistic measure of a future breach. RSI™ monitors vendors in near real-time, understands vendors' exposure to weaponized vulnerabilities
- Understand which vendors are most prone to ransomware with a tool that calculates attack susceptibility within seconds.

FOCUSTAGS™:

- Black Kite leverages automated discovery and tagging supported by a research team that combs the public and dark web to proactively identify products affected by new Zero-Days and vulnerabilities, with that information they create what we call FocusTags™. FocusTags™ are an immediate way for your organization to understand its level of exposure to critically emerging cyber events across your vendor ecosystem.
- Critical supply chain information and vulnerabilities are presented in a user-friendly format, simplifying comprehension and decision-making.
- FocusTags™ are created and assigned for significant events such as ransomware attacks, data breaches, and zero-day vulnerabilities.
- In instances like the MoveIT and Citrix vulnerabilities, Black Kite introduced the focus tags within 24 hours of detection.
- This allows you to be alerted on specific vulnerabilities by which your ecosystem may be affected, allowing you to act faster than manually sending out a questionnaire asking if each vendor is impacted.

SUPPLY CHAIN RISK MODULE:

- With the new Supply Chain module, Black Kite aims to illuminate risks to your organization beyond direct vendors.
- Black Kite simplifies assessing risk in your organization or your vendors' supply chains through automating the detection of 3rd, 4th, and Nth party suppliers. Black Kite detects software products your supply chain is over-reliant on and could present a single point of failure, assessing how security incidents in 4th and 5th parties could disrupt operations by cascading back through your 3rd parties, and much more
    - For example, customers can set up alerts where they can be notified if any 4th party faces a ransomware or data breach event

SUPPLY CHAIN RISK MODULE (CONT.):

- Automatic discovery of both digital and physical suppliers out to 5th parties, for both your organization AND your vendors.
- Out-of-the-box concentration risk metric to identify vendors, products, and geolocations that could have an outsized impact on the supply chain.
- Preempt disruptions from the cascading risks of cyber events using vendor link intelligence to identify how 4th parties link back to your organization to coordinate a response to your 3rd parties.
- Verify vendors are upholding contractual obligations disclosing subprocessors and security incidents in their supply chains.
- Respond to geo-political risks by identifying vendors and their assets located in conflict zones or sanctioned countries.

COLLABORATION CENTER:

- Black Kite's Collaboration Center is a cyber intelligence sharing platform that can identify both immediate and emerging risk, while acting as a centralized system of record for 3rd party incident management. Black Kite is the only system that allows you to invite your vendors into the platform to collaborate with them at unprecedented scale and with incredible precision down to the finding.
- Customers invite vendors to access Black Kite intelligence for free, inclusive of critical vulnerabilities and findings. Black Kite reports also include documents and emerging security incidents through Black Kite FocusTags™ (e.g., MOVEit, Log4j, KEVs). Further, customers will be able to communicate with vendors directly on findings and reports, and importantly track and report on remediation progress across all of their monitored companies, all in an auditable and centralized dashboard.

RISK QUANTIFICATION - UNDERSTAND AND COMMUNICATE THE IMPACT RISK HAS ON YOUR ORGANIZATION:

Risk in Dollars and Cents:

- Implementing the Third-Party FAIR methodology, Black Kite provides a vendor-specific risk estimation that is based on your unique relationship with each vendor.
- Black Kite leverages information from our standardized technical findings in conjunction with compliance mappings of the documents uploaded from the UniQuE Parser to help hone in on the residual risk of working with a vendor.
- Risk quantification covers three scenarios:
- Business Interruption: Gauges the impact if a vendor's services were unavailable.
- Confidentiality: Assesses the impact of a vendor breach based on shared records and internal network access.
- Ransomware: Evaluates the impact of ransomware affecting a vendor.

BLACK KITE
Third Party Risk Platform

COMPLIANCE DIFFERENTIATORS - REDUCE THE TIME TO ASSESS AND ONBOARD VENDORS :

FRAMEWORKS:

- Black Kite seamlessly aligns with 14 distinct Standards and Frameworks and is able to take uploaded documents and apply them to these frameworks, so your team never needs to read and parse information out from SOC2, privacy policy, and questionnaires again. In addition, Black Kite has recently mapped and automated regional/ Industry frameworks such as DORA (EMEA), HECVAT, B10, ITSG-33 and the OSFI Self-Assessment as examples.

UNIQUE PARSER:

- Universal Questionnaire and Policy Examiner (UniQuE) is designed in a way that it can consume a wide variety of questionnaires and internal policies, e.g., Information Security Policies, SOC2 reports, and map the contents of these different documents to well-known standards/frameworks like NIST 800-53, ISO27001, or CMMC. If a customer has a custom questionnaire or the information security policy of a vendor, UniQuE Parser will parse and process the document and map the results to the controls in each relative framework. This means your vendors can share their security policy in its original format e.g., DOCX or PDF, or the results from any standard or custom questionnaire, and upload them into the Black Kite platform. This is an effort to automate your vendor review/due diligence process.
- Automates consumption of a wide variety of questionnaires, internal policies and security artifacts. Parse and process custom questionnaires and documents instantly while mapping content to 14 well-known standards and frameworks within minutes.

GAP ANALYSIS:

- Request compliance documents first, and use the Gap Analysis to instantly identify unanswered controls or unsatisfactory responses based on UniQuE Parser results.
- Send drastically reduced questionnaires and/or follow ups to increase vendor response rates.
- Manually sifting through frameworks is minimized, with unmapped controls conveniently presented in an exportable Excel Document.

ENTERPRISE FRAMEWORK:

- Black Kite's Enterprise frameworks enable teams to craft Custom Frameworks tailored to their organization's pertinent controls.
- Organizations can merge controls from our 17 standardly supported frameworks or create their own custom questionnaire to design a suitable framework for due diligence reviews.

By utilizing the Unique Parser, Enterprise Framework, and Gap Analysis tools, organizations can significantly slash vendor due diligence review times from weeks to hours.

- The assessments that Black Kite provides both a letter grade and a data drill-down for each risk category so that vulnerability remediation and risk mitigation can be assessed, prioritized, and acted upon.
- In most third-party risk programs, the rating serves as the only outlet for understanding a risk posture of a vendor or partner. It's Black Kite's role and mission to not only give the rating for the company, but to also give the granular reasoning why.
- In each of our ratings we present an option to either investigate the technical findings standardized to MITRE and NIST, the compliance control and result or a mixture of both when dealing with third party FAIR. Which is why it's safe to say Black Kite is more than a run of the mill security ratings service. It is a risk intelligence platform that houses more than 35 million companies and has best in class detection capabilities (detection of the MoveIT vulnerability towards those companies in less than 24 hours from when the vulnerability was announced).
- https://cwe.mitre.org/cwss/cwss_v1.0.1.html

ADDITIONAL FEATURES:

- Platform Access Sharing: The platform permits the sharing of access with vendors, facilitating collaborative risk management.
- Unlimited Seats: Users can enjoy unrestricted access for their team members.
- Customer Success: Onboarding includes a dedicated Customer Success Manager, who assists with best practices, workflow setup, and alerts.
- Ongoing Support: Regular meetings with the Customer Success Manager, post-onboarding, ensure continuous assistance.
- Open API: The platform's Open API allows for seamless integration with other systems and applications. (app.blackkitetech.com/ApiDocs/v2/swagger/)
- DBI: The Data Breach Index (DBI) is a key performance index that tracks data breaches and past incidents (e.g., leaked credentials, botnet infections, etc.), measuring their severity based on the number of records compromised and when the data was breached.
- Ransomware Susceptibility Report - The resulting report is designed to be clear, concise, and easy to understand, providing vendors with the necessary information to identify and remediate vulnerabilities that are seen as key vectors of a ransomware attack.
- Strategy Report- A step by step improvement plan that provides explicit information that will allow you to make strategic mitigation decisions that will have the greatest impact on your overall risk from a technical, financial, and compliance perspective. The reporting is designed to be applicable for any audience
- Dashboard Customization: Our dashboard offers extensive customization, featuring a diverse range of widgets. Tailor your view to seamlessly analyze aggregated vendor risks according to your preferences or stakeholders (e.g., executive teams).

BLACK KITE
Third Party Risk Platform

GARTNER PEER INSIGHTS CUSTOMER QUOTES, CUSTOMERS:

- 130+ Ratings, 4.9 Stars, 100% Recommended by our Customers
- “Black Kite is far the best solution in their space & has the most accurate data”
- “Black Kite works exactly as we expected it to and support has been exceptional throughout our roll out and usage.”
- “Black Kite has provided a great experience in our TPRM program. It is our go-to application when we need to investigate our vendors security posture.”
- “Product is easy to use and provides in-depth information with more details than competitors.”
- “The Black Kite team has been phenomenal to work with and the product is outstanding.”
- “The platform provides continuous threat telemetry, combining a deep, hacker-minded threat intelligence with the largest data lake among its peers.”
- “The product delivers more functionality and features than the competition and the team behind it is exceptional at responding to questions or providing support”
- “The most comprehensive, consistent, and insightful product offerings in the space. The most consistently accurate and up-to-date findings in the space. The most responsive customer service in the space.”
- “I've worked with other tools and Black Kite by far has the best data in the space.”
- “We have tried other products in this space, but Black Kite has been the easiest to adopt with little or no user training, and the most impressive in terms of overall capability and features.”
- “BlackKite differentiates itself in a saturated market with exceptional detection capabilities that are significantly better than any other third-party risk rating service I've seen. They have an excellent team behind the product that is invested in your success.”
- “The Black Kite team has been super responsive and continues to improve the tool. I've seen customer requests become part of the tool.”
- “Best Security And IT Risk management Platform: This platform helps in generating quality data by screening data from all the vendors of my organization. Overall experience is wonderful. This platform Provides best team support with well knowledge and skills. My company has been using this platform since 3 years now and their are no major complaints. Strongly recommended platform”
- "For us, as a banking group, it is crucial to manage 3PRM, CyberSecurity Rating and Benchmarking. For several years we used other big well known vendor. But the service providers improved a lot in the last 2 years. We did new PoCs with almost all of the vendors, went thru all our use cases, compared data and functionalities available and identified Black Kite as the best one. After several months of operation, we are super happy we selected Black Kite”
- “Black Kite is the leader in the Cyber Risk monitoring space. Their innovation when it comes to assessing risk coming from our vendors is simply not found anywhere else. From the confidence and transparency of their data to quantifying ($$) the risk of working with a vendor is fantastic. Not much is not working.”
- “The best Third Party Risk Intelligence Platform we have ever implemented. It provides us with significant (technical) details; as well it gives us financial (risk) impact that not many could do.”