BLACK KITE

2022 | Data Sheet

BEHIND THE CYBER RATING

THE MOST COMPREHENSIVE AND ACCURATE TECHNICAL INTELLIGENCE

At Black Kite, we're redefining and disrupting vendor risk management with the world's first global third-party cyber risk monitoring platform built from a hacker's perspective. Adversaries attack companies through third parties, island-hopping their way into target organizations. **We aim to help you be as agile as the adversary.**

Companies that provide security ratings employ strategies that include a combination of data points. Whether they are gathered organically or purchased from public and private sources, the data translates organizational security effectiveness into numerical ratings. While other security ratings services narrow the scope, our non-intrusive, powerful scans tap our vast data lake, accessing information on **34 million companies – 4x that of our competitors.** We tell the full story, providing a multidimensional view of your entire attack surface from a technical, financial impact and compliance perspective.

100%

STANDARDS-BASED SCORING

A-F

TRANSPARENT GRADING

CONTINUOUS GLOBAL COVERAGE

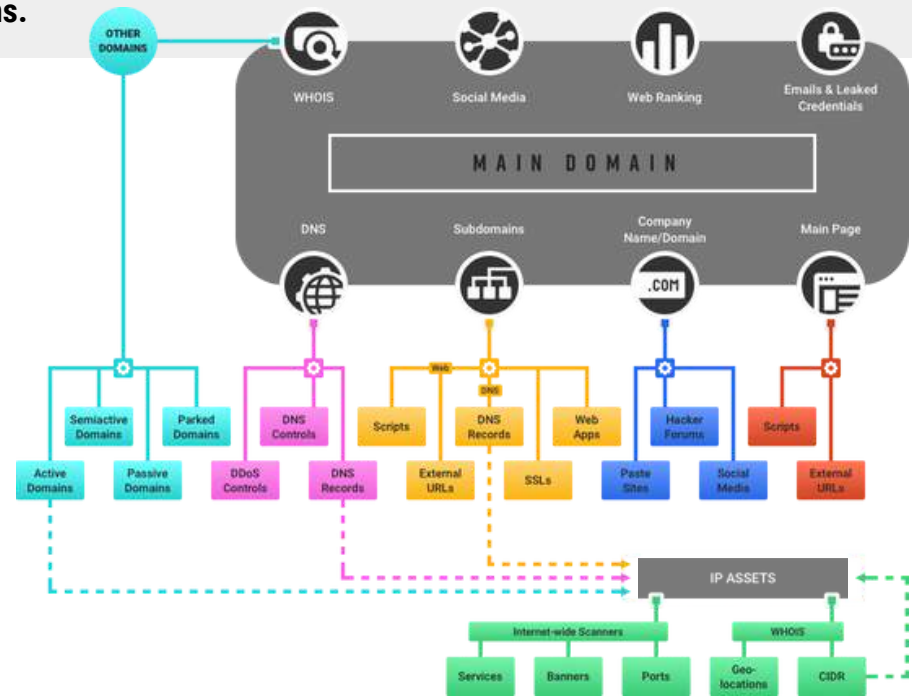
- 400 million domain names
- 4 billion subdomains
- 4 billion service fingerprints
- 10 billion SSL certificates
- 100 billion DNS & Whois
- 100 billion web pages

34+ million companies

1 DATA COLLECTION

The baseline of data collection is asset discovery. Domains, IP addresses, DNS records, social media, emails and leaked credentials are all valuable assets of a company in the digital space. Black Kite uses **passive, non-intrusive scans.**

Black Kite does not use intrusive vulnerability scanners like Nessus, Netsparker, Acunetix, Nexpose, Nmap, openvas, etc. The passive scan doesn't touch the target company's assets. Instead, the platform finds required data from the internet, including search engine caches, archive[.]org, internet-wide scanners, VirusTotal, PassiveTotal, hacker sites, paste sites & deep/dark web.



2 STANDARDS-BASED SCORING

Once collected, the **data is categorized into 20 categories, graded according to MITRE Cyber Threat Susceptibility Assessment (CTSA) and NIST.** Black Kite has over 500 control points corresponding to MITRE's TTPs. These standard scoring models eliminate false positives.

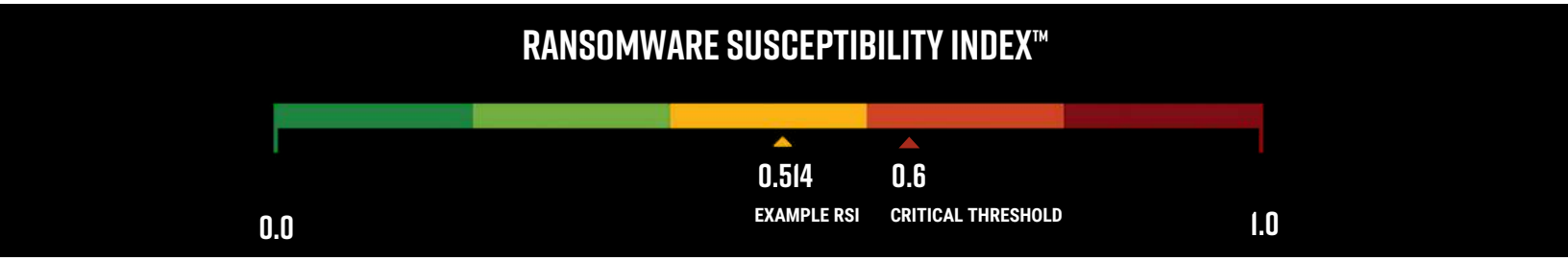
290 **CONTROL ITEMS**

The technical rating is a weighted average of 20 risk categories, providing unmatched breadth and insight into detected vulnerabilities. Each category, as well as each control point, has a different weight in the overall grade.

FULL TRANSPARENCY INCLUDES:

PREDICTIVE RANSOMWARE INTELLIGENCE

Black Kite is the only cyber risk rating platform with a ransomware indication tool. Using data and machine learning, Black Kite's Ransomware Susceptibility Index™ (RSI™) discovers the likelihood that an organization will experience a ransomware attack. By becoming aware of your risk, you can avoid business interruption and data loss by using our reliable data to develop informed policies around all emerging threats.



COMPLIANCE CORRELATION & RISK QUANTIFICATION USING OPEN FAIR™

Black Kite estimates the external compliance of target companies, saving you time and effort. The classification allows you to measure the compliance level of any organization across various well-known frameworks, including NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR, Shared Assessments, and others.

Using the Open FAIR™ model, Black Kite calculates the probable financial impact if a third-party vendor, partner, or supplier experiences a breach. Using this model, you can effectively communicate risk in quantitative, easy-to-understand business terms.

SPEAK A COMMON LANGUAGE WITH STANDARDS-BASED RESULTS

Black Kite leverages MITRE frameworks to communicate cyber risk in a common language. After aggregating hundreds of data sources from open-source intelligence (OSINT), MITRE CTSA is the foundational scoring matrix to map all vendors in our system using a well-known industry standard.

3 STRATEGY & REMEDIATION

Black Kite provides an automated remediation plan for each one of your vendors. In our Strategy Report, we **highlight the vendor's current posture and outline a set of prescriptive steps** that are designed to advise them on increasing their cyber risk and reducing financial risk.

EASILY VALIDATE FINDINGS

Black Kite has a built-in case management system to facilitate interacting with your vendors. Vendors can quickly review findings assigned to them and ensure data points are remediated appropriately.

ELIMINATE FALSE POSITIVES

This standard scoring model eliminates more false positives and removes those findings from the data set. Ratings are adjusted accordingly and those findings will not be present in subsequent updates.

COMPLETE GUIDANCE ALONG THE WAY

Black Kite's Strategy Report helps you improve your cyber posture by making strategic remediation suggestions for compliance and financial impact improvements. Tasks are prioritized based on criticality.

EVERY ORGANIZATION IN YOUR ECOSYSTEM, MONITORED CONTINUOUSLY

This automated platform is built to scale alongside your digital supply chain– without sacrificing time or efficiency. Black Kite reduces assessment times from weeks to minutes. In turn, you can cost-effectively embrace full supply chain monitoring – as all third-party vendors pose a risk to your organization, not just the ones that appear most risky.

+1 (571) 335-0222 | **800 Boylston St Suite 2905**
info@blackkite.com | Boston, MA 02199