

CAPABILITIES STATEMENT



DUNS: 08-1054873
CAGE: 81FG0
UEID: DWU8TLAVC1G5

CONTACT INFORMATION

8609 Westwood Center Dr. Ste 110
Vienna, VA 22182
p. 571-335-0222
w. www.blackkite.com

AWARDS

- CISOs Choice Award, Risk Management 2020, 2021, 2022, 2023, Partner in Success 2022, Visionary Company 2023
- Gartner Customer First Technology Provider 2023
- Forrester Wave Strong Performer Cybersecurity Risk Ratings Platform 2024
- Red Dot Interface Design Award 2024

Forrester WAVE 2024 Strong Performer

"Black Kite's unique focus on standards-based ratings tackles the industry's ratings integrity problem head-on. It's the only vendor in this evaluation whose customers were unanimously satisfied with its rating accuracy."

NAICS

513210 - Software Publishers



DHS/CISA
Continuous
Diagnostics and
Mitigation Approved
Products List

Black Kite Illuminates Risk in Your Supply Chain



Improve Visibility

Preempt Disruptions

- Automatic **3rd, 4th, and 5th party detection**
- Respond to security incidents beyond 3rd parties to prevent cascading impacts to your operations
- **Concentration Risk** of suppliers, software products, and geographies
- Address supply chain risks in Geo-Political hot zones

Multidimensional View of Third-Party Risk

MITRE

FAIR
INSTITUTE

NIST



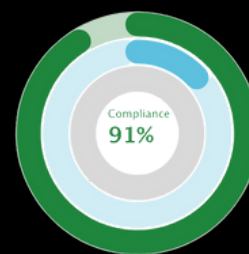
Technical Cyber Rating

- Easy-to-understand letter grades with risk intelligence beyond a rating
- Real-time continuous attack surface monitoring
- Powerful performance behind 20 technical categories
- Trusted, standards-based intelligence



Cyber Risk Quantification

- Understand the potential financial impact (risk) to your organization in the case of a cyber breach
- Cost-effectively achieve and maintain an acceptable level of loss exposure
- Effectively communicate risks to business stakeholders



Questionnaire & Compliance Correlation

- Automates consumption of a wide variety of questionnaires and internal policies
- Map content to well-known standards and frameworks within minutes, including CMMC, NIST 800-171 and 800-53

Large Data Lake:

- 500M Domain Names
- 6B Subdomains
- 4B Service Fingerprints
- 10B SSL Certificates
- 100B DNS & Whois
- 100B Webpages
- **34M+ Organizations**

Reporting & Tools:

- Dashboards
- Scheduled Reports
- Workflow Engine
- Ticketing & Audit Logs
- Integrations
- VendorMap™

Results in Minutes:

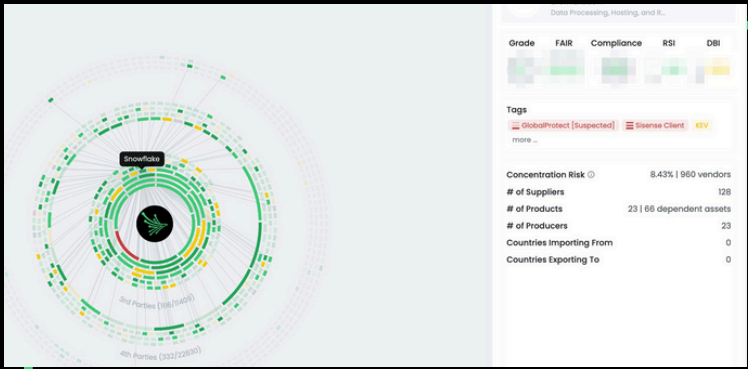
- Summary View Dashboards
- Letter Grade Cyber Ratings
- Standards-Based Risk Quantification
- Automated Compliance Mapping
- Benchmark & Strategy Reporting
- Ransomware Susceptibility

Technical Categories:

- Digital Footprint
- Patch Management
- Application Security
- CDN Security
- Website Security
- SSL/TLS Strength
- Credential Management
- Hactivist Shares
- Social Network
- Information Disclosure
- Attack Surface
- DNS Health
- Email Security
- DDoS Resiliency
- Network Security
- Brand Monitoring
- IP Reputation
- Fraudulent Apps
- Fraudulent Domains
- Web Ranking

GET INSTANT VISIBILITY INTO YOUR CYBER ECOSYSTEM

FocusTags™



DATA BREACHES & RANSOMWARE

Ransomware Ransomware (90+ days)
Data Breach Data Breach (90+ days)

- Get instant alerts on data breaches and ransomware attacks happening in your Nth party ecosystem
- Arm yourself with solid data and information before approaching vendors

HIGH PROFILE CYBER EVENTS

PAN-OS [Suspected] Snowflake Client Citrix ADC/Gateway

- Know about exploited vulnerabilities and impactful third-party breaches, often before your third-party vendor
- Icons show the confidence level of the product identification
- Filter your ecosystem by FocusTags™ to see the breadth of the event

Potential impact due to CrowdStrike Update Issue

Telstra has a vendor relationship with CrowdStrike

A recent incident involving CrowdStrike, a leading cybersecurity firm, resulted in a significant outage affecting businesses worldwide. This was caused by a defect found in a single content update for Windows hosts. Mac and Linux hosts were not affected. The defect led to a widespread Blue Screen of Death (BSOD) issue and disrupted various services, including Microsoft 365 and Azure.

The issue was not a result of a cyberattack but a defect in the CrowdStrike update, which has since been identified and isolated. CrowdStrike has deployed a fix and is working actively with customers to resolve the issue. This incident has affected many organizations, including financial institutions, airlines, and other critical infrastructure entities, causing operational disruptions globally.

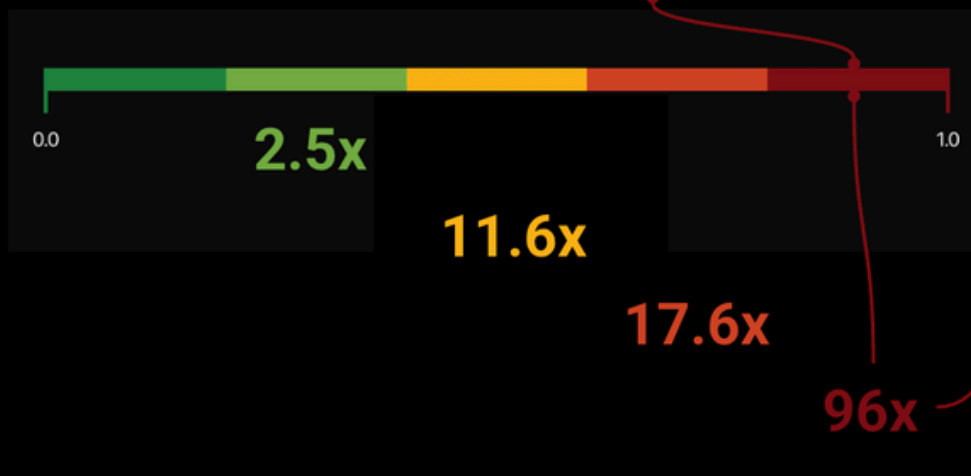
This issue might affect Telstra's operations and cause business disruption. Immediate actions include implementing CrowdStrike's update recommendations.

Recommended Actions:

Ransomware Susceptibility Index® (RSI™)

See where you or a vendor ranks to assess the likelihood of a ransomware attack.

The companies with an RSI value in this range are



more likely to experience a ransomware attack than the companies with an RSI value below 0.2.

SEE THE EARLY WARNING SIGNS. The World's First & Only Ransomware Indication Tool.