BLACK KITE

STANDARDS-BASED SCORING SPOTLIGHT

Letter grades designed for transparency and accuracy.

OPEN STANDARDS YOU CAN TRUST

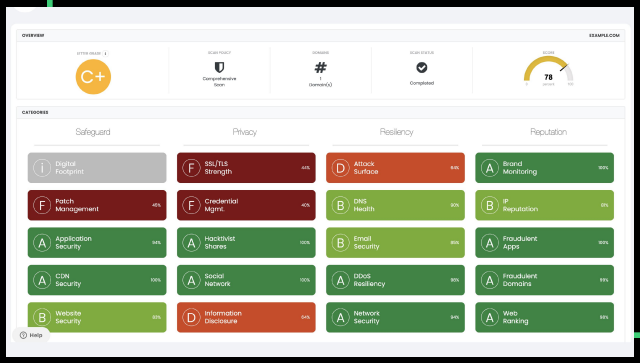
Helps to eliminate false positives.

- Non-intrusive scans using open-source intelligence (OSINT) techniques collect detailed external data without ever touching the target.
- Once collected, the data is categorized and graded according to MITRE Cyber Threat Susceptibility Assessment (CTSA) methodology.

BE AS AGILE AS ADVERSARIES

See risk from a hacker's perspective.

- Hackers also use OSINT resources to target victims.
- We perform contextualization and analysis to convert the same data into risk intelligence.
- Black Kite has more than 500 control points corresponding to MITRE's Tactics, Techniques, and Procedures (TTP).



MORE THAN MITRE

Black Kite maps its data to many trusted frameworks:

- Common Weakness Risk Analysis Framework (CWRAF)
- Common Weakness Scoring System (CWSS)
- Common Vulnerability Scoring System (CVSS)
- Open FAIR™ (Factor Analysis of Information Risk)
- Exploit Prediction Scoring System (EPSS)

Learn more about our methodology.