BLACK KITE

CYBER RISK ASSESSMENT

PREPARED FOR

EXAMPLE COMPANY

REPORT GENERATED ON

2023-12-12

How to read this report?

This report evaluates the security posture for 4 main groups namely Safeguard, Privacy, Resiliency, Reputation, and 20 unique categories. This data is compiled into a simple, readable report with letter-grade scores to help identify and mitigate potential security risks. Each category has summary or top riskiest assets and technical details along with mitigation, compliance, standards & regulation details can be found at the bottom of the each category and the Knowledge Base.

About Black Kite

In 2016, Black Kite began its journey to redefine third-party risk management (TPRM), building the world's first security ratings service designed from a hacker's perspective. With 200+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence.

While other security ratings service (SRS) providers try to narrow the scope, our non-intrusive, powerful scans tell the full story. Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: **technical, financial and compliance.**

Sections

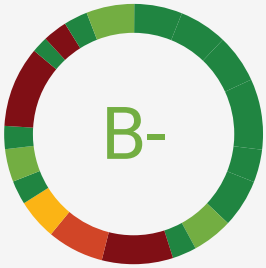
OVERVIEW

Example Company

PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES (NAICS: 54)

You have **7% worse** cyber risk rating than industry average

Cyber Rating



Probable Financial Impact Rating

Risk
(Annualized)

4.1K MINIMUM | **268.8K** MOST LIKELY | 71.6M MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

Compliance Rating

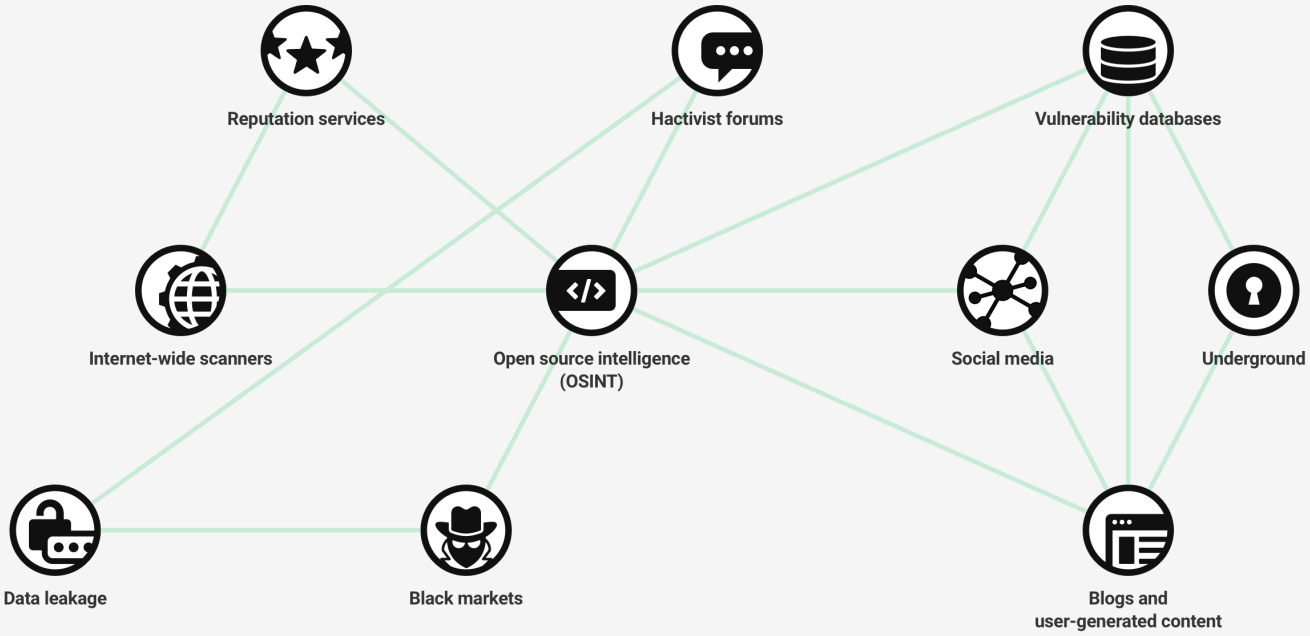
Black Kite follows and applies commonly-used frameworks developed by the MITRE Corporation to calculate ratings in a consistent, flexible, and transparent manner, converting highly technical terms into simple letter grades with +/- ranges.

C+ Safeguard	C Privacy	A- Resiliency	B Reputation
i Digital Footprint	A SSL/TLS Strength	B Attack Surface	A Brand Monitoring
F Patch Management	F Credential Management	A DNS Health	D IP Reputation
A Application Security	C Hacktivist Shares	A Email Security	A Fraudulent Apps
A CDN Security	A Social Network	A DDoS Resiliency	B Fradulent Domains
B Website Security	F Information Disclosure	A Network Security	A Web Ranking

METHODOLOGY

Cyber Risk Scorecard uses Open Source Intelligence services to collect, analyze and report security related events and findings. Security companies and hackers are always scanning publicly accessible networks and share their data on the internet. This commonly referred to as Open-Source Intelligence (OSINT).

Following mindmap shows how hackers can leverage their attack vectors by using OSINT services like hacker forums, social networks, Google, leaked database dumps, paste sites or even legitimite security services like VirusTotal, Censys, Cymon, Google Safe Browsing etc.



Black Kite Cyber Risk Scorecard is a service that reports your business's public access methods for possible security risks, such as known but unpatched vulnerabilities or open network ports. Black Kite also scans social media, darkweb forums, and other sources of information leaks, looking for information about your company such as compromised passwords, emails, or network structure details, as well as other attack methods such as fake websites or programs masquerading as legitimate sites or products of your business.

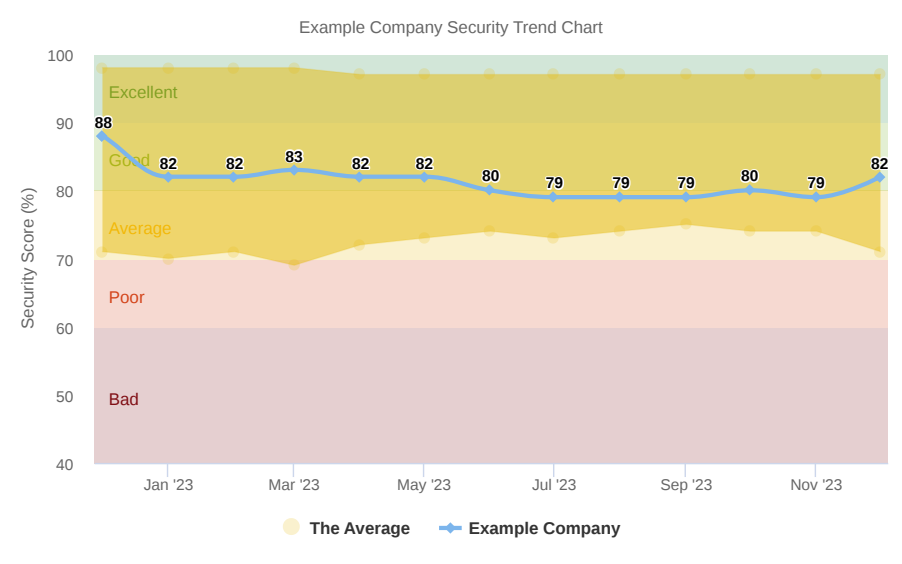
This data is compiled by Black Kite into a simple, readable report with letter-grade scores to help identify and mitigate potential security risks. Black Kite does all of this without scanning or modifying any of the company's business assets.

Black Kite uses what is called open-source intelligence (OSINT) to gather information. Both hackers and legitimate security companies are continually publishing to, and scanning, social media websites and networks for information on vulnerabilities. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites or even legitimate security services like VirusTotal, Censys, Cymon, Shodan or Google Safe Browsing. Black Kite's Passive Scorecard assesses an organization in these areas using the techniques described above.

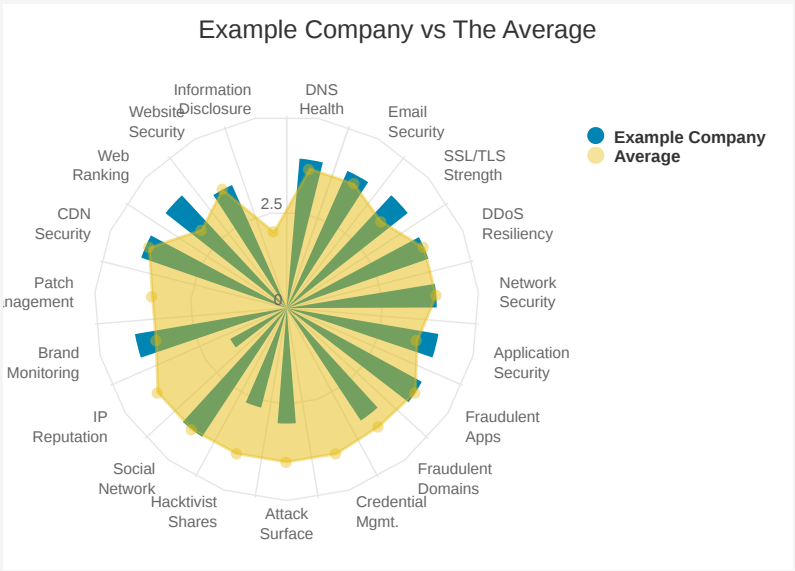
To generate the scorecard, Black Kite needs only the company domain. The asset discovery engine collects the related information from VirusTotal, PassiveTotal, web search engines and other Internet wide scanners. Black Kite has one of the largest IP & Domain Whois databases which holds more than 1 billion historic items. The asset discovery engine searches the database in order to find all IP address ranges and domain names that belong to the company. The result of the asset discovery engine is the company assets, which is used as the input for passive vulnerability scanner, configuration scanner, threat intelligence agent and reputation engine.

BENCHMARK

The Cyber Risk Benchmark begins with a multi-tiered risk analysis. The scorecard provides insight into the current security posture based on 20 core pillars of a successful security strategy. Black Kite benchmark report provides comperative visibility for cyber risk posture, and is a collection of global standard and best practices for securing IT systems and data against attacks. Black Kite evaluates an organization in a set of 20 security categories "which map to many compliance standards".



The following chart is the radar map compares Example Company with the average of other companies in the same industry. The chart evaluates the company in nineteen security-related categories and one informational category, as shown below. Each category provides specific information about an aspect of a firm's cyber security posture.



RESULTS
FROM PUBLIC-FACING ASSETS

Digital Footprint

Digital Footprint is determined by open ports, services and application banners. This information is gathered from Black Kite crawlers, Censys, VirusTotal, Robtext, Alexa, Shodan etc.

DNS Health

1 issues

The DNS Health report is generated from 40+ control items which are collected from online services like IntoDNS, Robtex, Netcraft, and HackerTarget. Since DNS queries are recursive, it is almost impossible to detect a hacker's footprints from the DNS servers.

Email Security

3 issues

Potential email servers and SMTP misconfigurations like open relay, unauthenticated logins, restricted relay, and SMTP 'Verify' vulnerabilities are collected from the online services like MxToolbox and eMailSecurityGrader.

SSL/TLS Strength

0 issues

SSL/TLS configurations and vulnerabilities are provided by several third-party online services. The results come from various online SSL grading services like Qualys SSL Labs scanner, HTBridge, Mozilla Website Observatory etc.

Application Security

5 issues

The contents of each web application are collected from various internet-wide scanners and are analyzed for application level weaknesses i.e. Cross Site Request Forgery, Cross Content Mixing, Plain Text Transmission of Sensitive Information etc. The results are also correlated with MITRE CWE database to detect the severity level of each finding.

Network Security

2 issues

This section analyzes network level problems and detects any open critical ports, unprotected network devices, misconfigured firewalls, and service endpoints on public-facing assets.

Attack Surface

50 issues

Attack surface is the technical analysis of open critical ports, out-of-date services, application weaknesses, SSL/TLS strength, and any misconfigurations. This information is gathered from Censys and Shodan databases and service/application versions are correlated with other subcategories' results.

Patch Management

719 issues

Company asset system versions are collected from internet-wide scanners like Censys, Shodan, Zoomeye etc. These version numbers are converted into the corresponding common platform enumeration number (CPE-ID) and are correlated with NIST NVD and MITRE CVSS databases to detect and approximate any unmitigated known vulnerabilities.

Website Security

1 issues

This is a special analysis of the company's main website. The findings are collected from the SSL/TLS Strength, Patch Management, Application Security, Web Ranking and Brand Monitoring sub-categories.

RESULTS

FROM CYBER SPACE (HACKER SITES, SOCIAL MEDIA, ETC.)

A DDoS Resiliency — 3 issues

This section shows the result of 15 different potential DDoS checks and detects any potential DrDoS amplification endpoints. The data is collected from non-intrusive scanners and other internet-wide scanners.

B Fraudulent Domains — 59 issues

Fraudulent domains and subdomains are extracted from the domain registration database. The registered domains database holds more than 300M records.

A Fraudulent Apps — 0 issues

Fraudulent or pirate mobile or desktop applications are used to hack or phish employee or customer data. Possible fraudulent or pirate mobile or desktop apps on Google Play, App Store and pirate app stores are provided.

F Credential Mgmt. — 31 issues

There are 5+ billion hacked emails and passwords available on the internet and underground forums. This section shows the leaked or hacked emails and passwords that were discovered. * Only the findings that have upper than low severity levels are shown.

D IP Reputation — 77 issues

The asset reputation score is based on the number of IPs or domains are blacklisted or that are used for sophisticated APT attacks. The reputation feeds are collected from VirusTotal, Cymon, Firehol, BlackList DNS servers, etc.

C Hacktivist Shares — 348 issues

Hackers publicize their targets in underground forums or on the darkweb. Black Kite collects information from hundreds of darkweb forums, criminal sites, and hacktivist sites and filters the results for information pertaining to the company.

A Social Network — 0 issues

Hackers publicize their targets or victims on social network sites to motivate other hackers to attack the same target. The results are filtered from billions of pieces of social media content.

A Brand Monitoring — 1 issues

Brand monitoring is a business analytics process concerned with monitoring various channels on the web or other media to gain insight about the company, brand, and anything explicitly connected to the company in cyberspace.

A Web Ranking — 1 issues

Cisco, Alexa, and Majestic track web sites and rank them according to popularity, back-links, references, etc. This subcategory shows Alexa and Majestic trends, Google Page insight speed test results as well as Web Content Accessibility Guidelines (WCAG) 2.0 parsing compliance findings.

F Information Disclosure — 108 issues

Misconfigured services or other public assets may disclose local IPs, email addresses, version numbers, whois privacy records, and other sensitive information to the internet.

A CDN Security — 0 issues

A content delivery network (CDN) is a large distributed system of servers deployed in multiple data centers across the Internet. Companies use CDNs for online libraries like JQuery. This section analyzes the CDN content to detect possible vulnerabilities.

i Compliance — 15 regulations

Cybersecurity standards and regulations provide policy frameworks of computer security guidance for private and public-sector organizations. They provide a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes. Major regulations within this section include NIST 800-53, GDPR, ISO 27001, PCI-DSS, HIPAA, COBIT

FAQ

FREQUENTLY ASKED QUESTIONS

What types of data does Black Kite collect to inform its cybersecurity ratings?

Black Kite uses open-source intelligence (OSINT) techniques to collect data from 400+ OSINT resources via a span of internet-wide scanners. As an authorized IP zone transferer with one of the largest IP & Domain Whois databases, we hold more than one billion historical items. The asset-discovery engine detects all company-related IP address ranges and domain names.

How does the Black Kite provide transparency to rated companies about how their rating was derived?

Black Kite utilizes the MITRE Cyber Threat Susceptibility Assessment (CTSA) as a foundational scoring matrix to map every vendor in the system. Black Kite uses additional standard scoring models like the Common Weakness Risk Analysis Framework (CWRAF), Common Weakness Scoring System (CWSS), Common Vulnerability Scoring System (CVSS), and Factor Analysis of Information Risk (FAIR). Mining data from other sources enables customers to eliminate false positives and audit results. See https://blackkitetech.com/black-kites-methodology for more information

How many suppliers are currently in your portal?

We collect data on all companies which are added to our data lake. Our data lake comprises information on over 34 million companies which allows our customers to add and start monitoring any company within a few hours. If the company is previously monitored by another customer, the company's data will be available in minutes.

Is any of the data proactively provided by the suppliers?

No. Suppliers can share their policies, such as their information security policy, or questionnaires if necessary.

Do you get permission, acknowledgment, etc. from the companies you monitor?

No, all information is publicly available and curated from open sources.

What are your Data Sources?

Black Kite collects data from 400+ resources. There are several categories that Black Kite collects data from:

- Threat Intelligence
- Exploits & Advisories
- Dark Web
- Archives
- Forums / Blogs / IRC
- Search Engines
- Business Records
- Public Records
- Social Networks
- Internet Wide scanners

GLOSSARY

- **Botnet:** A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- **Brute Force:** A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.
- **Cryptanalysis:** The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the ciphertext to plaintext without knowing the key.
- **Denial of Service:** The prevention of authorized access to a system resource or the delaying of system operations and functions.
- **Domain Name:** A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.
- **Domain Name System (DNS):** The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
- **Encryption:** Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
- **Fingerprinting:** Sending strange packets to a system in order to gauge how it responds to determine the operating system.
- **Hardening:** Hardening is the process of identifying and fixing vulnerabilities on a system.
- **Internet Protocol (IP):** The method or protocol by which data is sent from one computer to another on the Internet.
- **IP Address:** A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.
- **Network Mapping:** To compile an electronic inventory of the systems and the services on your network.
- **Patching:** Patching is the process of updating software to a different version.
- **Penetration Testing:** Penetration testing is used to test the external perimeter security of a network or facility.
- **Phishing:** The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.
- **Plaintext:** Ordinary readable text before being encrypted into ciphertext or after being decrypted.
- **Port:** A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.
- **Port Scan:** A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- **Ransomware:** A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.
- **Reverse Lookup:** Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.
- **Secure Sockets Layer (SSL):** A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.
- **TCP Fingerprinting:** TCP fingerprinting is the use of odd packet header combinations to determine a remote operating system.
- **WHOIS:** An IP for finding information about resources on networks.

- END OF REPORT -