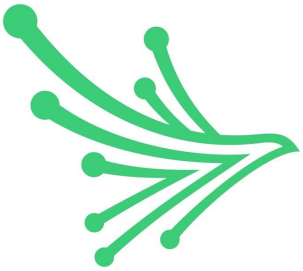


BLACK KITE

Cyber Risk Assessment Documentation

March 29th, 2021

Contents

Copyright Black Kite 2021

Cyber Risk Assessment

Introduction

The purpose of this white paper is to detail how the Black Kite risk rating system works and the comprehensive data and analysis behind letter grades.

Risk Ratings

“The world is divided into two groups: those that have been hacked and know it, and those that have been hacked but don’t know it yet.” This old saying in the cyber security industry indicates a simple truth: *you are being targeted right now*. Hackers can range from young-age newbies a.k.a. “script kiddies” to sophisticated state-sponsored agents. They all have one thing in common: they are looking for a way to disrupt your business. No business is immune; all are vulnerable.

This white paper has two goals:

1. Helping organizations understand the importance of having access to timely, accurate, and to-the-point information required to act proactively against imminent threats in cyber security.
2. Explaining how Black Kite Cyber Risk Assessments can help with its simple-to-use yet powerful letter-grade mechanism.

We will also cover the comprehensive data behind the letter-grade scores and delve into the details of some of the algorithms and methods used to compute these scores.

A cyber attack is one of the biggest threats confronting any business today. Attacks can have devastating and lasting impacts including lost assets & data, systems damage & downtime, negative impacts to partners & customers, and harm to the organization’s reputation. Defending against cyber attacks requires systems in place to enable a company to identify and eliminate security vulnerabilities.

Black Kite Cyber Risk Assessments deliver the information necessary to proactively protect businesses from cyber attacks. The assessments provide 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.

Copyright Black Kite 2021

There are five main reasons to know your organization's risk scores.

1. PROVIDE INTELLIGENCE FOR DECISION-MAKING

Business and security leaders make decisions on how to allocate resources best to protect the organization. Risk scoring provides a guide to allocate those resources to the most critical points of failure first. Decision-makers can measure their results and adjust rapidly.

2. HELP DETERMINE ROI

Organizations spend large sums improving their cyber security infrastructures, but often CEOs and IT directors cannot effectively determine the return on investment (ROI) of these efforts — how much improvement they are achieving for a given expenditure (and over what time period). Risk-scorecard metrics can help businesses assess the quality and completeness of their cyber security infrastructure and thereby determine the ROI of their cyber investments.

3. JUSTIFY CYBER BUDGETS

Uniform risk scoring across an industry provides a benchmark for organizations within that industry to compare and contrast their risk mitigation goals and progress. This comparison can be used for justifying cyber security investments, identifying priority areas, and measuring success against appropriate benchmarks.

4. MANAGE VENDOR RISK

Companies working with third-party vendors often share valuable information with these vendors or give them system access as a necessary function of business. Any cyber vulnerability within a vendor's organization may affect the principal organization: *a chain is only as strong as its weakest link*. The Cyber Risk Scorecard provides a letter grade and data drill downs specifically for a principal's vendors and sub-vendors.

A survey conducted by Ponemon Institute reveals that 59% of respondents experienced a 3rd-party breach in the last year. The fines paid because of the breaches are quite large: more than 7 million $US *per breach.* Target paid more than $116 million in civil settlements related to its 2013 breach caused by an HVAC company, but Target's total cost of this breach exceeded $290 million. With GDPR requirements and penalties, risk associated with higher fines for each breach related to EU citizens will increase. The GDPR fines can go up to 20 million Euros or 4% of a business's annual global turnover (whichever is the highest).

5. EVALUATE CYBER INSURANCE SUBSCRIBERS

The cyber risk assessment works for both cyber insurers and for their subscribers. Previously cyber insurers determined the insured organization's security infrastructure risk profile by

Copyright Black Kite 2021

submitting a long list of questions, but these extensive questionnaires were inadequate. Penetration test reports are often used as a way to discover vulnerabilities, but they reflect only a point-in-time assessment and are not designed to show improvement unless repeatedly performed - *a continual high cost*. Risk scoring over time shows insurers the dynamic changes in subscribing firms' security infrastructures. In turn, the insured organizations benefit from knowing how they are evaluated by the insurer and can take defined and concrete steps to reduce their risk.

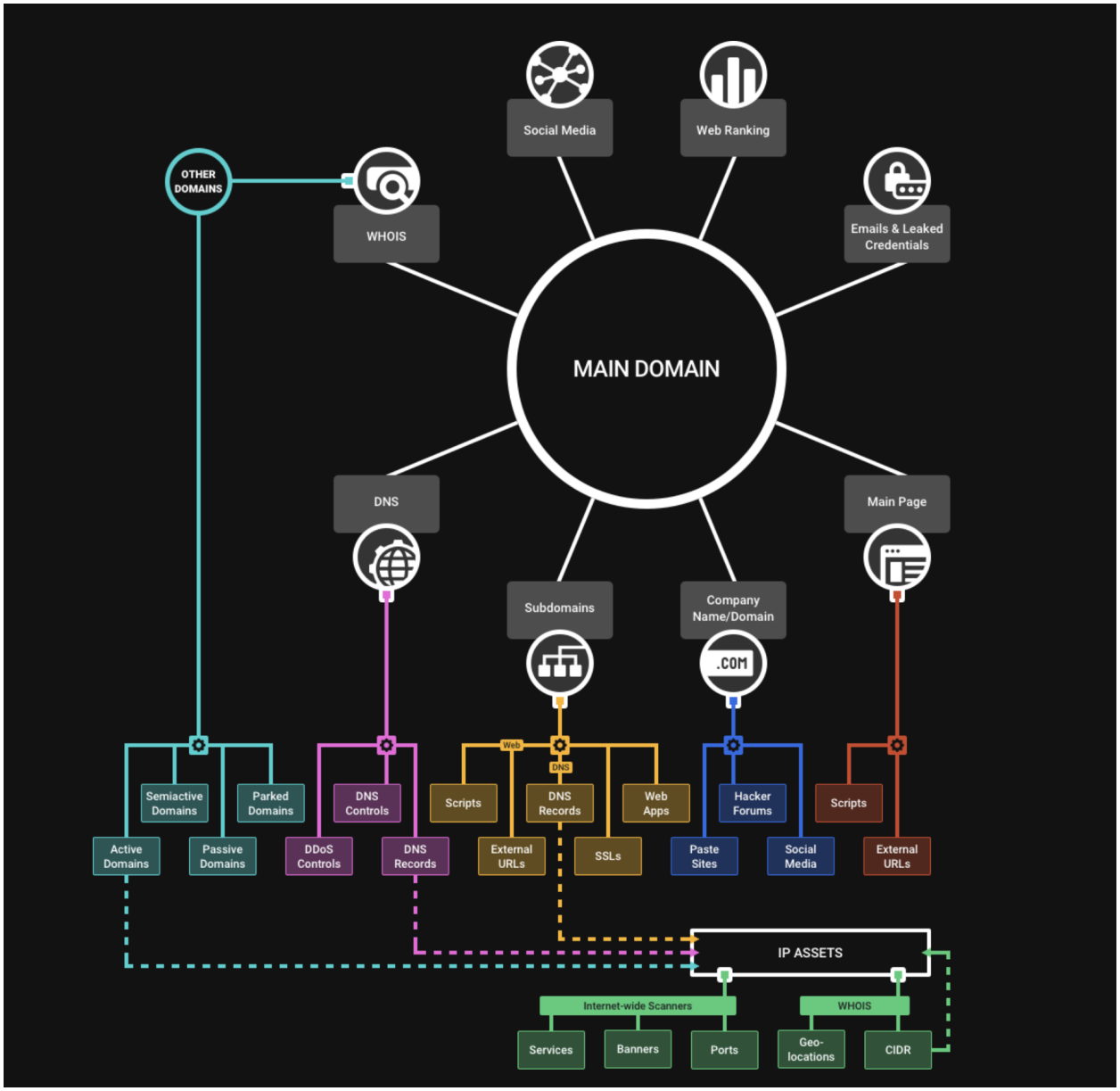
How the Black Kite Cyber Risk Assessment Works

Black Kite provides a service that scans your business's public access methods for possible security risks, such as known but unpatched vulnerabilities, or open network ports. Black Kite also monitors social media, dark-web forums, and other sources of information leaks, searching for company information such as compromised passwords, email addresses, or network structure details. Other potent attack methods such as fake/fraudulent websites or programs and/or services masquerading as legitimate sites, or a business's products are also hunted down.

Black Kite uses open-source intelligence (OSINT) techniques to gather information. Both hackers and legitimate security companies continually scan social media websites and networks for information on vulnerabilities and publish their findings on the internet. The map below shows how hackers can leverage their attack vectors by using OSINT resources, namely hacker forums, social networks, Google, leaked database dumps, paste sites, and even legitimate security services like VirusTotal, Censys, Cymon, Shodan, and Google Safe Browsing. Black Kite's cyber risk assessment gathers data from all these sources and performs contextualization and analysis to convert data into risk intelligence presented in rating format.

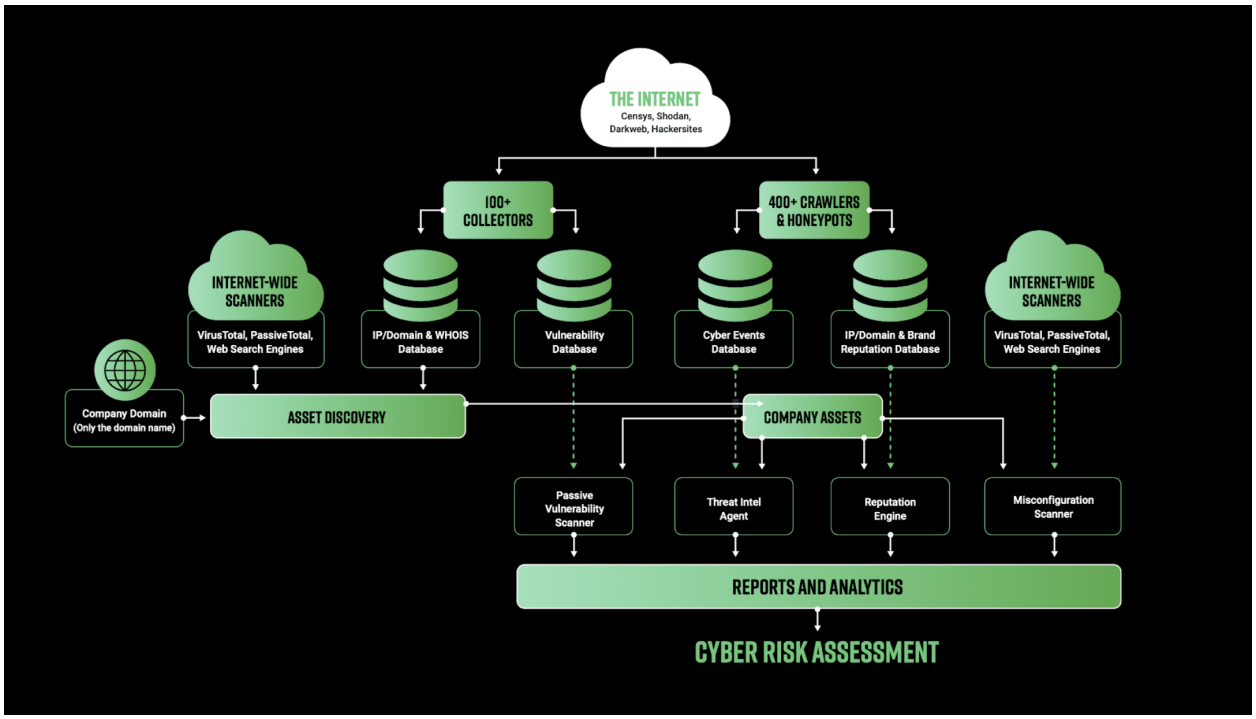
To generate the assessment, Black Kite only requires a company's domain name. Black Kite's asset-discovery engine collects the related information from VirusTotal, PassiveTotal, web search engines, and other Internet-wide scanners. Black Kite has one of the largest IP & Domain Whois databases holding more than one billion (1B) historical items. The asset-discovery engine searches the database to find all company-related IP address ranges and domain names.

Copyright Black Kite 2021



The results generated by the asset-discovery engine are used as the input for passive vulnerability and configuration scanners, threat intelligence agent, and reputation engine.

Copyright Black Kite 2021



Black Kite has more than 100 data collectors, 400 crawlers, and tens of honeypots. The crawlers and collectors continuously collect IP & domain reputation feeds, cyber events, hacker shares, social-media shares, and known vulnerabilities. They also collect internet-wide scanner (Censys, Shodan) databases and put the results into the corresponding data stores. The reports and analytics agent then analyzes the findings and generates the categorized and letter-graded assessment.

This data is analyzed and compiled by Black Kite into a simple, readable report with letter-grade ratings to help identify and mitigate potential security risks and to present technical data as readily understandable business concepts. Black Kite does all of this information gathering and analysis in a non-intrusive way, i.e., without scanning or modifying any of the company's business assets.

Grading Methodology

In our grading methodology, we follow and apply well-known and commonly-used Cyber Threat Susceptibility Assessment (CTSA) and Common Weakness Risk Analysis Framework (CWRAF™), both developed by the MITRE Corporation. CTSA and CWRAF provide a framework for scoring software weaknesses in a consistent, flexible, open manner, while accommodating context for various business domains. Black Kite's assesses the risks vis-a-vis CTSA and CWRAF, and converts that risk into rankings and easy-to-understand letter grades.

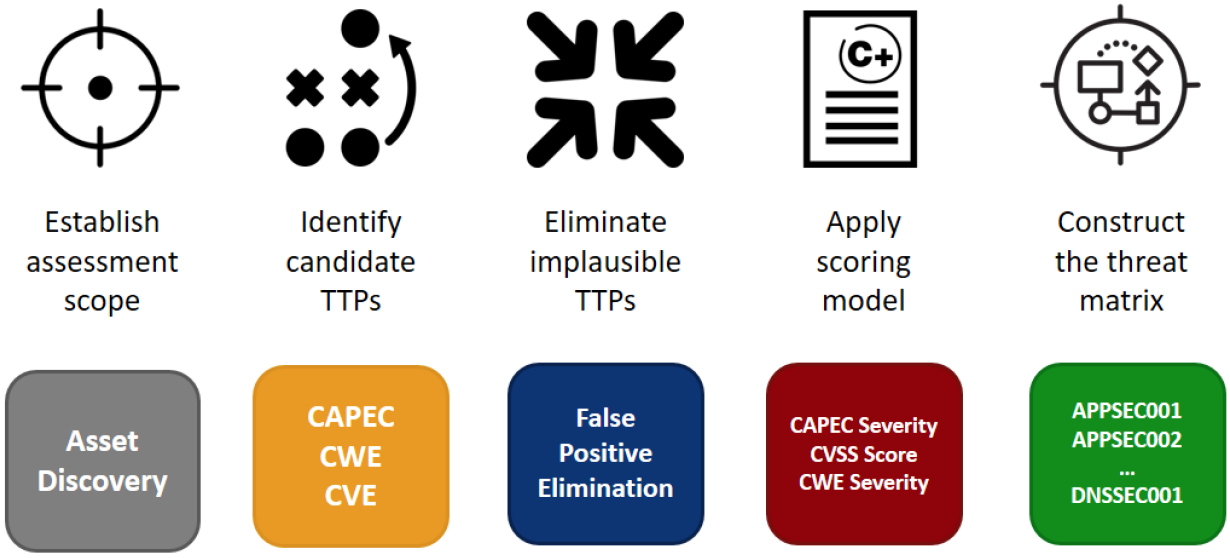
Copyright Black Kite 2021

CTSA and CWRAF benefits:

- Includes mechanisms for measuring risk of security errors ("weaknesses") in a way that is closely linked with the risk to an organization's business or mission.
- Supports the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the organization's business or mission.
- Can be used by organizations in conjunction with the Common Weakness Scoring System (CWSS™) to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance.

Cyber Threat Susceptibility Assessment (CTSA)

Cyber Threat Susceptibility Assessment (CTSA), developed by MITRE, is a methodology for evaluating the susceptibility of a system to cyber-attack. CTSA quantitatively assesses a system's [in]ability to resist cyber-attack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). CTSA consists of the following five (5) steps:



Step 1: Establish Assessment Scope:

The first step in CTSA is to establish the scope of the evaluation, which can be characterized in terms of:

- The set of system assets being evaluated
- The range of attack TTPs being considered
- The types of adversaries

Black Kite establishes the assessment scope during the asset discovery process, which discovers all publicly visible/accessible domains, subdomains, IP/CIDR ranges, etc.

Step 2: Identify Candidate TTP

Once the scope of CTSA is established, the next step is to evaluate the cyber asset's architecture, technology, and security capabilities against TTPs in the Mission Assurance Engineering (MAE) Catalog. Unclassified sources of adversary TTPs in the catalog include MITRE-hosted resources such as Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), and Common Vulnerability Enumeration (CVE). CAPEC is a compilation of attack patterns derived from specific real-world incidents. CWE is a catalog of software weaknesses and defects that adversarial TTPs may exploit. CVE catalogs vulnerabilities found in Commercial off-the-shelf (COTS) hardware and software products.

Step 3: Eliminate Implausible TTPs

The initial set of candidate TTPs undergoes a narrowing process to eliminate TTPs considered implausible. Several factors can make a TTP an implausible method of cyber attack. Many TTPs have prerequisites or conditions that must hold true in order for that TTP to be effective.

Apply Scoring Model: Candidate TTPs that cannot be eliminated are ranked using a scoring model. The TTP scoring model assesses the risk associated with each TTP relative to other plausible TTPs considered in the assessment. This ranking helps set priorities on where to apply security measures to reduce the system's susceptibility to cyber attack. CAPEC severity levels, CVSS scores and CWE severity ranks are the main parameters to calculate the TTP risk scores.

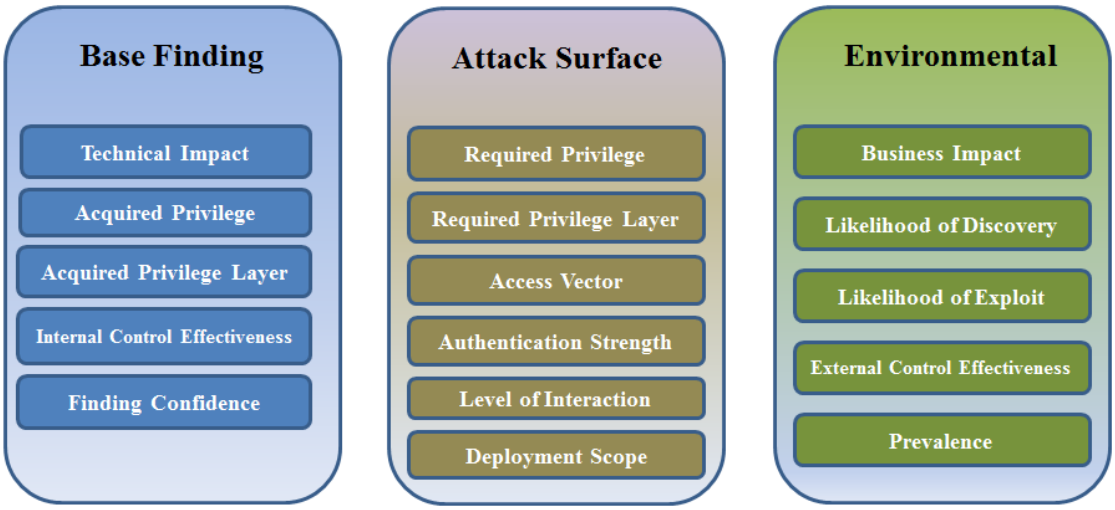
Construct a Threat Matrix: CTSA produces a Threat Matrix, which lists plausible attack TTPs ranked by decreasing risk score and their mapping to cyber assets as a function of adversary type. Black Kite has over 500 TTPs (APPSEC001, APPSEC002, … DNS001, DNS002,… etc.) with different risk scores.

The Black Kite threat matrix is calculated by using the Common Weakness Scoring System (CWSS™) that provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry. When used in conjunction with the Cyber Threat Susceptibility Assessment (CTSA) or Common Weakness Risk Analysis Framework (CWRAF™), organizations are able to apply CWSS to those CWEs that are most relevant to their own specific businesses, missions, and deployed technologies.

Copyright Black Kite 2021

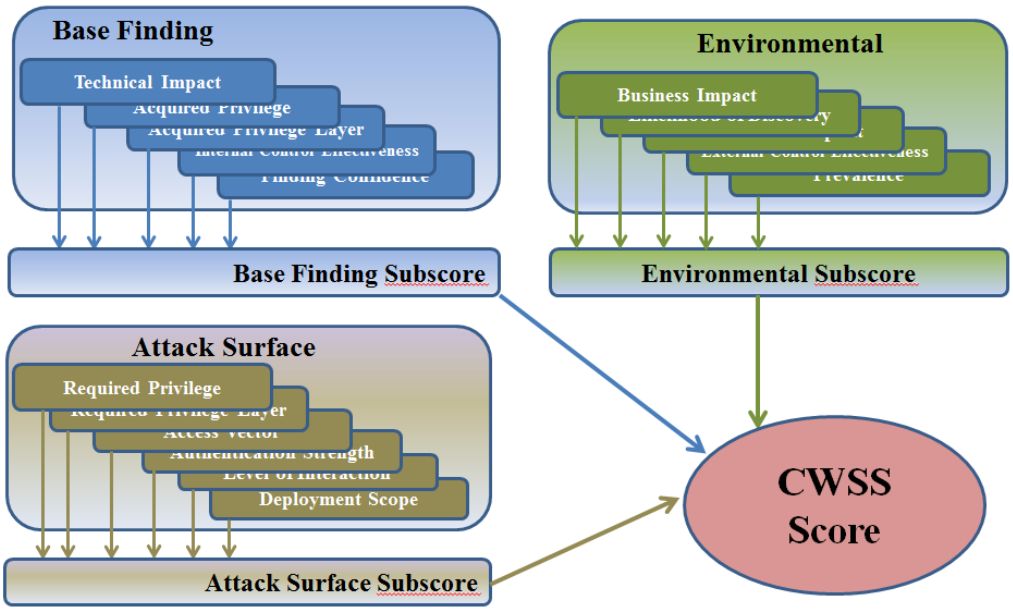
How does CWSS work?

CWSS scores CWEs using 18 different factors across three metric groups: (1) the Base Finding group, which captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls; (2) the Attack Surface group, which captures the barriers that an attacker must cross in order to exploit the weakness; and (3) the Environmental group, which includes factors that may be specific to a particular operational context, such as business impact, likelihood of exploit, and existence of external controls.



Each factor in the Base Finding metric group is assigned a value. These values are converted to associated weights, and a Base Finding subscore is calculated. The Base Finding subscore can range between 0 and 100. The same method is applied to the Attack Surface and Environmental metric group; their subscores can range between 0 and 1. Finally, the three subscores are multiplied together, which produces a CWSS score between 0 and 100.

Copyright Black Kite 2021



CWSS contains the following factors, organized based on their metric group:

Group	Name	Summary
Base Finding	Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.
Base Finding	Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.
Base Finding	Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.
Base Finding	Internal Control Effectiveness (IC)	The ability of the control to render the weakness unable to be exploited by an attacker.
Base Finding	Finding Confidence (FC)	The confidence that the reported issue is a weakness that can be utilized by an attacker.
Attack Surface	Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.
Attack Surface	Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.
Attack Surface	Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.
Attack Surface	Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.
Attack Surface	Level of Interaction (IN)	The actions that are required by the human victim(s) to enable a successful attack to take place.
Attack Surface	Deployment Scope (SC)	Whether the weakness is present in all deployable instances of the software or if it is limited to a subset of platforms and/or

Copyright Black Kite 2021

		configurations.
Environmental	Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.
Environmental	Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness.
Environmental	Likelihood of Exploit (EX)	The likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.
Environmental	External Control Effectiveness (EC)	The capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.
Environmental	Prevalence (P)	How frequently this type of weakness appears in software.

A CWSS 1.0 score can range between 0 and 100. It is calculated as follows:

`BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore`

The Base Finding subscore (BaseFindingSubscore) is calculated as follows:

```
Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer)
+ 5*FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness ] *
4.0

f(TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f(TechnicalImpact) =
1.
```

The AttackSurfaceSubscore is calculated as:

```
[ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) +
20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0
```

The EnvironmentalSubscore is calculated as:

```
[ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit +
3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0

f(BusinessImpact) = 0 if BusinessImpact == 0; otherwise f(BusinessImpact) = 1
```

Using the Codes as specified for each factor, a CWSS score can be stored in a compact, machine-parsable, human-readable format that provides the details for how the score was generated. This is very similar to how CVSS vectors are constructed.

Example: Business-critical application

Consider a reported weakness in which an application is the primary source of income for a company, thus has critical business value. The application allows arbitrary Internet users to sign up for an account using only an email address. A user can then exploit the weakness to obtain administrator privileges for the application, but the attack cannot succeed until the administrator

views a report of recent user activities - a common occurrence. The attacker cannot take complete control over the application, but can delete its users and data. Suppose further that there are no controls to prevent the weakness, but the fix for the issue is simple, and limited to a few lines of code.

This situation could be captured in the following CWSS vector:

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:L,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C,0.9/DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

The vector has been split into multiple lines for readability. Each line represents a metric group.

The factors and values are as follows:

Factor	Value
Technical Impact	High
Acquired Privilege	Administrator
Acquired Privilege Layer	Application
Internal Control Effectiveness	None
Finding Confidence	Proven True
Required Privilege	Guest
Required Privilege Layer	Application
Access Vector	Internet
Authentication Strength	None
Level of Interaction	Typical/Limited
Deployment Scope	All
Business Impact	Critical
Likelihood of Discovery	High
Likelihood of Exploit	High
External Control Effectiveness	None
Prevalence	Not Applicable

The CWSS score for this vector is 92.6, derived as follows:

- BaseSubscore:
    - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`
    - `f(TI) = 1`
    - `= 96.0`
- AttackSurfaceSubscore:
    - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0`
    - `= 0.965`

- EnvironmentSubscore:
    - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20.0`
    - `f(BI) = 1`
    - `= 1.0`

NormShield uses 0-to-10 scale and the CWSS score is divided by 10. The final score is:

```
96.0 * 0.965 * 1.0 / 10 = 92.64 / 10 ~= 9.2
```

Category Grades

The Black Kite category (Patch Management, SSL/TLS Strength, DNS Security etc.) grades are calculated based on the following equation:

`TheSuccessPoint = 100 - [Sum( CWSS * SeverityLevel * Status * (1/AgeOfFinding) * (1/DenseOfFinding) / (1 or sqrt(TheSizeOfTheCompany)))] * CategoryMultiplier`

Parameter	Description
`TheSuccessPoint`	This is the success percent of the category which can be translated into letter grades based on the American Grading System shown below.
`CWSS`	The CWSS score of each finding in the category. The calculation of CWSS score is given above. It could be between 0.0 (min) to 10.0 (max)
`SeverityLevel`	This is the Severity level of the finding and could be Info (0), Low(1), Medium (2), High (3) or Critical (4). This parameter is used to amplify the high severity weaknesses.
`Status`	This is the status of a finding and it could be Passed (0), Warning (0.5) or Failed (1). This parameter is used to fine tune the impact of some findings if there are other countermeasures.
`AgeOfFinding`	Each finding has a date and the age may reduce the impact on the grade. For example a leaked credential or a blacklisted IP lose the impact over time.
`DenseOfFinding`	Some findings may frequently show up in each of the scorecards. Over the time the density of a finding inversely impact the grade since these types of findings become unimportant.
`TheSizeOfTheCompany`	Small and larger companies have different constraints. As a company grows it becomes harder to keep it secure. This parameter allows the scorecard to optimize the difficulty of keeping the company secure due to growth.
`CategoryMultiplier`	Since the number of control items in each category are different, this parameter allows the scorecard to scale each category from 0-to-100.

Once the category grades are calculated based on the equation given above, the grades are translated into GPA and Letter grades based on the American Grading system. Below is the grading system used by Black Kite.

Letter Grade	Percentage	GPA
A+	97%+	4.00/4.00
A	93%-96%	3.90/4.00
A-	90%-92%	3.67/4.00
B+	87%-89%	3.50/4.00
B	83%-86%	3.33/4.00
B-	80%-82%	3.00/4.00
C+	77%-79%	2.67/4.00
C	73%-76%	2.33/4.00
C-	70%-72%	2.00/4.00
D+	67%-69%	1.67/4.00
D	63%-66%	1.33/4.00
D-	60%-62%	1.00/4.00
F	0%-59%	0.00/4.00

The Grading Scale Table

Category Weights

The category grades are calculated once assessments on all the categories are completed. Each category has different weight in the overall grade as shown below.

Category Name	Weight (Total 100)		Category Name	Weight (Total 100)
Digital Footprint	0/100		IP Reputation	7/100
DNS Health	6/100		Hacktivist Shares	5/100
Email Security	6/100		Social Network	3/100
SSL/TLS Strength	6/100		Attack Surface	4/100
Application Security	9/100		Brand Monitoring	3/100
DDoS Resiliency	4/100		Patch Management	10/100
Network Security	6/100		Web Ranking	2/100
Fraudulent Domains	5/100		Information Disclosure	3/100
Fraudulent Apps	3/100		Website Security	6/100
Credential Mgmt.	9/100		CDN Security	3/100

Copyright Black Kite 2021

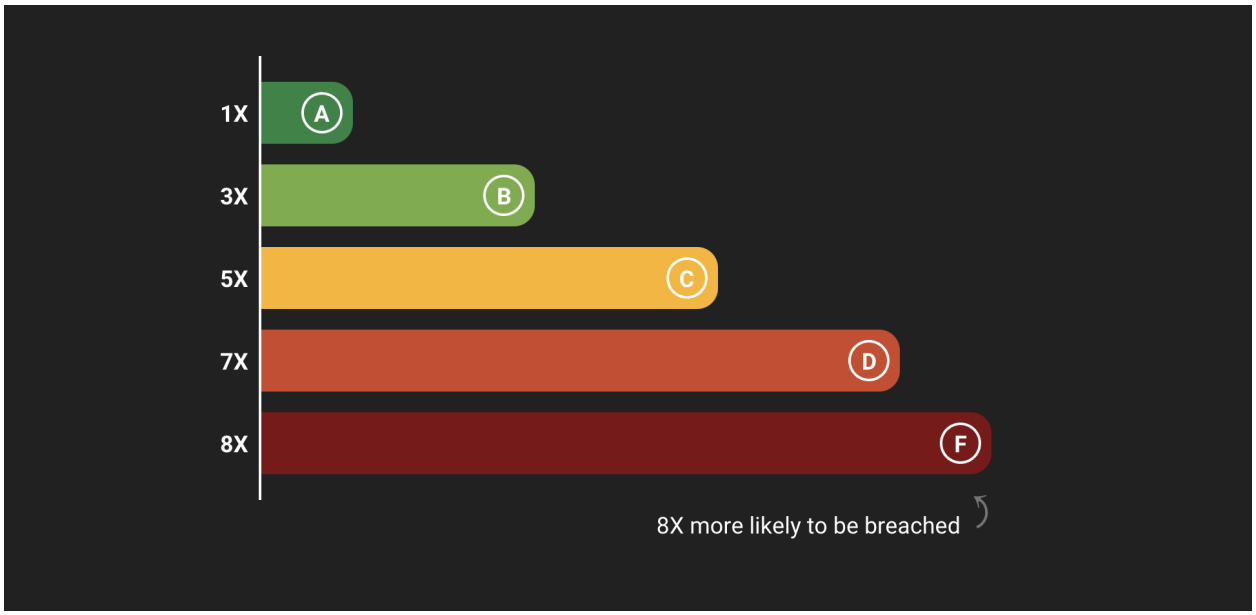
The overall grade is calculated by the weighted arithmetic mean, which is similar to an ordinary arithmetic mean (the most common type of average), except that instead of each of the data points contributing equally to the final average, every category contributes proportionally with the weights.

So the final grade is calculated by:

```
TheOverAllGPA = Sum(TheGPAofTheCategory * WeightOfTheCategory)
```

The overall GPA is translated into a letter grade and percentage again using the same table (The Grading Scale Table) given above.

Black Kite analyzes data in different risk categories from over 1,000,000 servers for hundreds of companies and calculated letter grades for the results. For example, a grade of 'B' indicates an organization has opened the door to a sophisticated hacker, a grade of 'F' means there are significant risks which hackers of all types may exploit. The overall grade shows *how easy it is to hack the corresponding environment*.



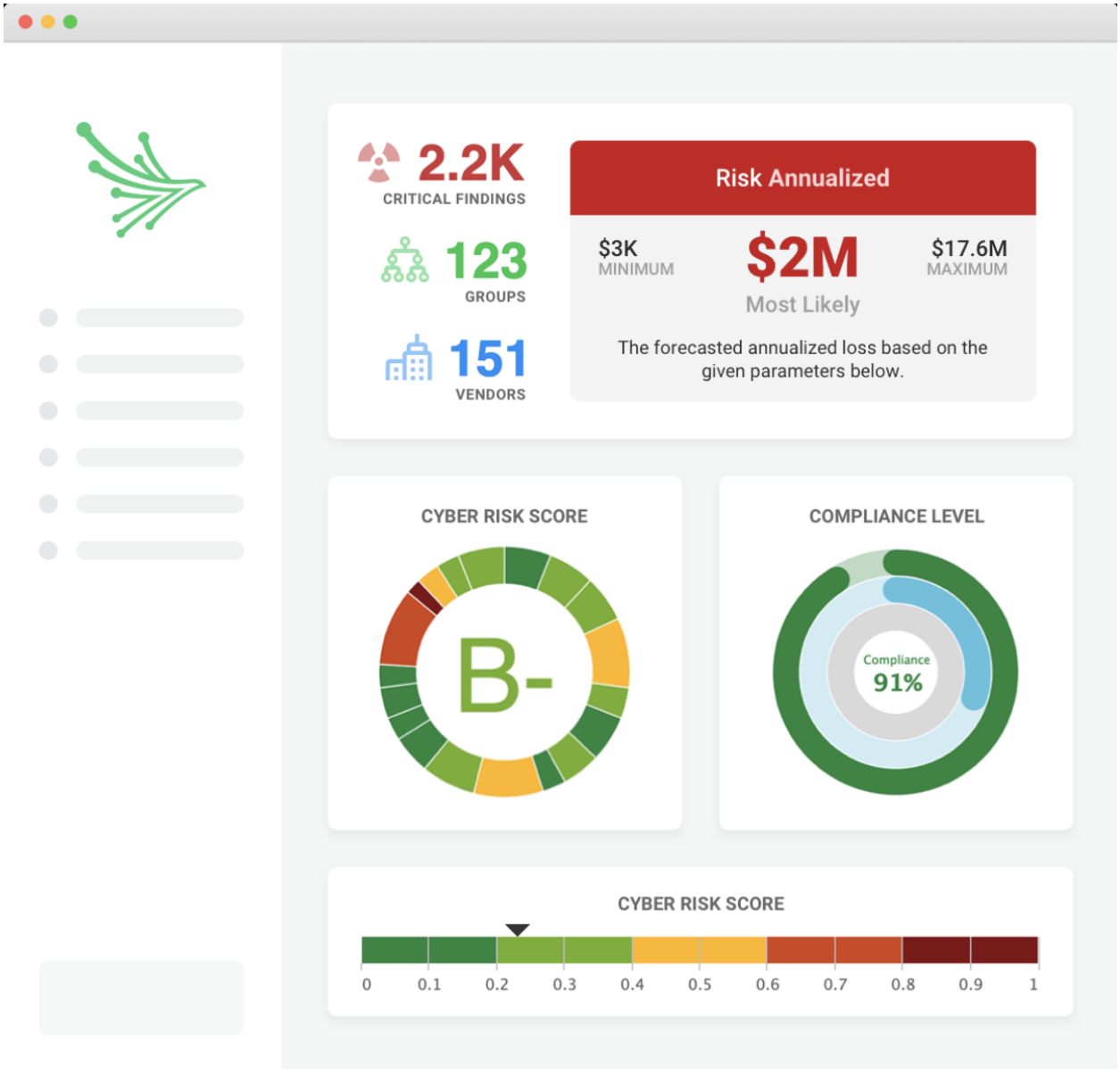
References:

https://cwe.mitre.org/cwss/cwss_v1.0.1.html
https://cyber.riskscore.cards/grades
https://www.mitre.org/sites/default/files/pdf/11_4982.pdf
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/cyber-threat-susceptibility-assessment
https://nvd.nist.gov/

Product Description

Black Kite Cyber Risk Assessment

Black Kite is the only cyber risk rating platform focused on alerting your business to third party risks. Black Kite's cyber risk assessments deliver easy-to-understand letter grade ratings, with additional financial impact estimations and cross-correlated compliance metrics.



Copyright Black Kite 2021

Technical Cyber Risk Rating

Black Kite uses open-source intelligence techniques to gather data, perform contextualization and analysis to convert data to risk intelligence in the form of a risk assessment. Black Kite's assessment is an objective, external measure of an organization's cyber risk posture. The risk ratings provide easy to understand cyber risk information for executives while providing detailed technical data and mitigation strategies to frontline engineers.

Technical Categories

The passive Black Kite assessment evaluates a company in twenty 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.

Patch Management: Keep software on computers and network devices up to date and capable of resisting low-level cyber attacks. Criminal hackers can take advantage of known vulnerabilities in operating systems and third-party applications if they are not properly patched or updated.

Application Security: Security measures at the application level aim to prevent data or code within the app from being stolen or hijacked. Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities.

DNS Health: A DNS attack is an exploit in which an attacker takes advantage of vulnerabilities in the domain name system (DNS).

Email Security: Open-sourced techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise.

SSL/TLS Strength: The SSL/TLS protocol encrypts internet traffic of all types, making secure internet communication (and therefore internet commerce) possible.

Leaked Credentials: Risk detection indicates that the user's current credentials have been leaked, which are valid and can be used to sign-in.

IP/Domain Reputation: Identify IP addresses that send unwanted requests. Using the IP reputation list you can identify if an IP address has a bad reputation or member of a botnet.

Social Network: Social media is part of a larger ecosystem of publicly available platforms that make up a new attack surface for threat actors to leverage.

Copyright Black Kite 2021

Hacktivist Shares: Hacktivism is the act of misusing a computer system or network for a socially or politically motivated reason. An example of hacktivism is denial of service attacks (DoS) which shut down a system to prevent customer access.

Fraudulent Domains: Domains registered by fraudsters plan to launch phishing attacks, sell knock-off goods on spoofed sites, or use "typo-squatting" domains to make money off unintentional traffic for other sites.

Fraudulent Applications: Fraudulent applications are used to hack/phish employee or customer data. This category identifies possible fraudulent or pirate mobile/desktop apps on Google Play, App Store, and pirate app stores.

Digital Footprint: Your digital footprint refers to a digital collection of data that can be traced back to you. This includes IPs, domains, subdomains, email addresses and server fingerprints.

Information Disclosure: When a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, such as usernames or financial information.

Attack Surface: The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter or extract data.

Brand Monitoring: A business analytics process that monitors various channels on the web or media to gain insight about the company, brand, and anything explicitly connected to cyberspace.

Network Security: Analyze network-level problems and detect any critical ports, unprotected network devices, misconfigured firewalls, and service endpoints.

DDoS Resiliency: Detect malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

Web Ranking: Cisco, Alexa and Majestic track web sites and rank them according to popularity, backlinks, and references. This subcategory shows trends, page speed test results, and Web Content Accessibility Guidelines (WCAG) 2.0 parsing compliance findings.

CDN Security: Companies use content delivery networks (CDNs) — large distributed systems of servers deployed in multiple data centers across the Internet — for online libraries like JQuery. Detect vulnerabilities in services like edge caching, SSL offloading and edge routing.

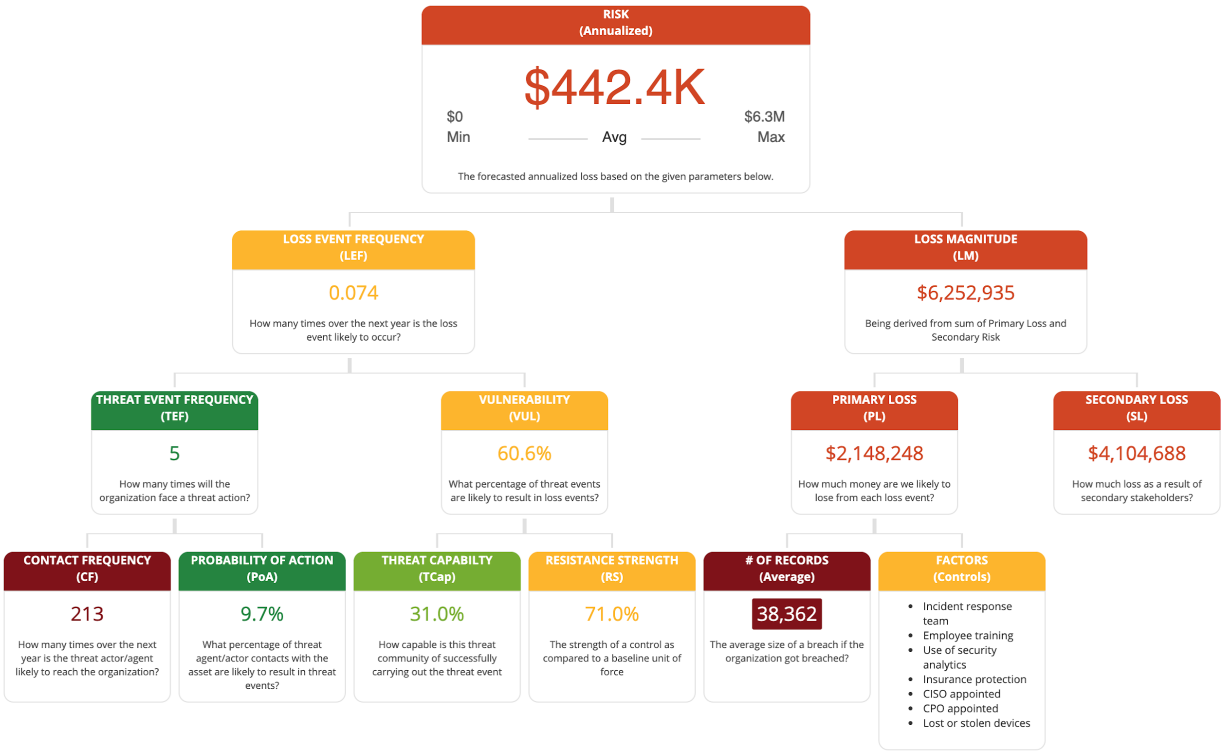
Website Security: The main website of an organization is one of the most important assets. Detecting any code or server level vulnerabilities is crucial for a company's reputation.

Copyright Black Kite 2021

Risk in Financial Terms with FAIR

For the first time, CISOs, CROs, and CFOs have an automated tool that measures the probable financial impact of cyberattacks against your company or your vendors, suppliers, and trading partners — and communicates risks in quantitative, easy-to-understand business terms.

Having the capacity to use an Open FAIR™ assessment at scale for third-party risk management will elevate your risk management program. This tool will help attain the goal of cost-effectively achieving and maintaining an acceptable level of loss exposure, while also clearly conveying the breadth of risk factors across the organization.

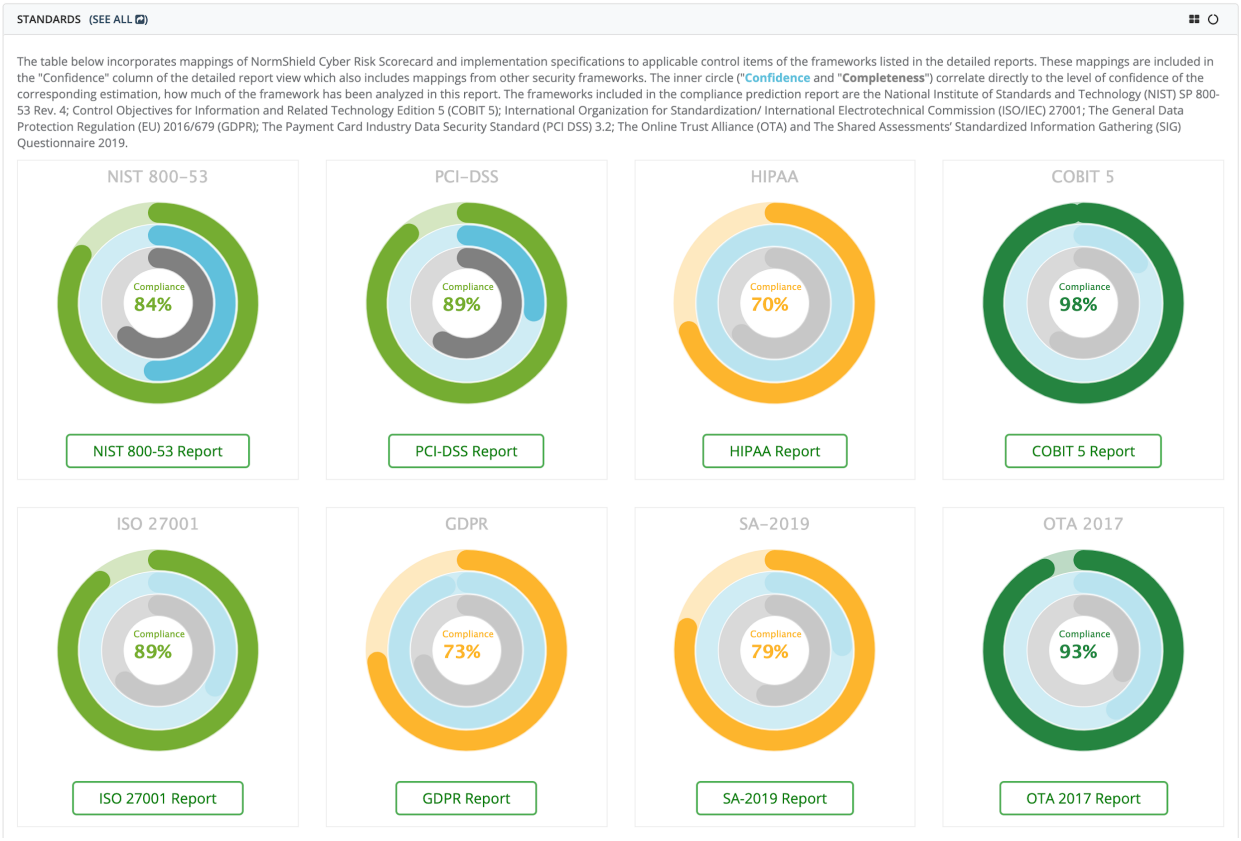


Copyright Black Kite 2021

Questionnaire & Compliance Correlation

Black Kite correlates cyber risk findings to industry standards and best practices. The classification allows you to measure the compliance level of any company for different regulations and standards, including NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR, Shared Assessments, and others. Black Kite's platform estimates the external compliance of target companies. The cross-correlation capability measures the compliance level of a target company based on the standard input, saving time and effort for both you and your vendors.

You can share compliance control items/questions with vendors using Black Kite's Strategy Report, or by directly inviting them to the Black Kite platform. Vendors can then fill out the control items/questions, and Black Kite can map the answers to other regulations and frameworks available in the system.



Conclusion

Black Kite is led by a team of innovative thinkers and cybersecurity experts. Our goal is to provide you with the most accurate and comprehensive cyber rating results, with the fewest false positives.

Our people and platform do the work for you, highlighting risk areas that require attention and automating feedback on how to address them. We're committed to serving our customers — and we're proud of our five-star customer service rating.

Black Kite is the only rating system that gives a complete view of cyber risk across three dimensions – technical, financial, and compliance. Companies choose our patented rating technology over legacy rating services every day, as our platform continues to prove superior technically, systematically, and at scale.

For more information visit www.blackkitetech.com

Copyright Black Kite 2021