Making the case to use Black Kite for third party cyber risk monitoring

Abstract

Conducting third party cyber risk assessments can be complex, resource intensive and expensive. With Black Kite, it does not have to be. This document outlines how Black Kite is used to automate much of this process.

Ronan Lavelle
ronan@elasticito.com

Contents

Making the case to use Black Kite for third party cyber risk monitoring

About Black Kite

Black Kite is a cyber risk assessment and monitoring platform that is used to rapidly assess the cyber risk profile of any company. The Black Kite platform uses open standards, like MITRE's CTSA methodology to provide a reliable cyber risk rating for any company.

Using Black Kite to assess and monitor third party cyber risk

As business becomes more digital and third parties are increasingly used to deliver services, cyber criminals are increasingly targeting what they consider to be potentially weaker victims; the vendors and third parties of larger companies.

It is becoming critical therefore, to understand and monitor the cyber risk that a third party poses to your business and to work with the external party to remediate issues and problems to ensure that your company's data and IP is better protected.

These are some of the key cyber risk qualification questions that you should be asking to establish the inherent risk that a third party brings to your business:

- Do we share data with the third party?
- Does the third party have access to our network?
- Does the third party have access to our facilities, offices and premises?
- Is the third party operationally critical to us?

We strongly recommend that you continuously monitor any vendor where you answer in the affirmative to one or more of these questions.

Here is an example of a HR and recruitment platform that is commonly used by enterprise customers to process recruitment and HR related data:

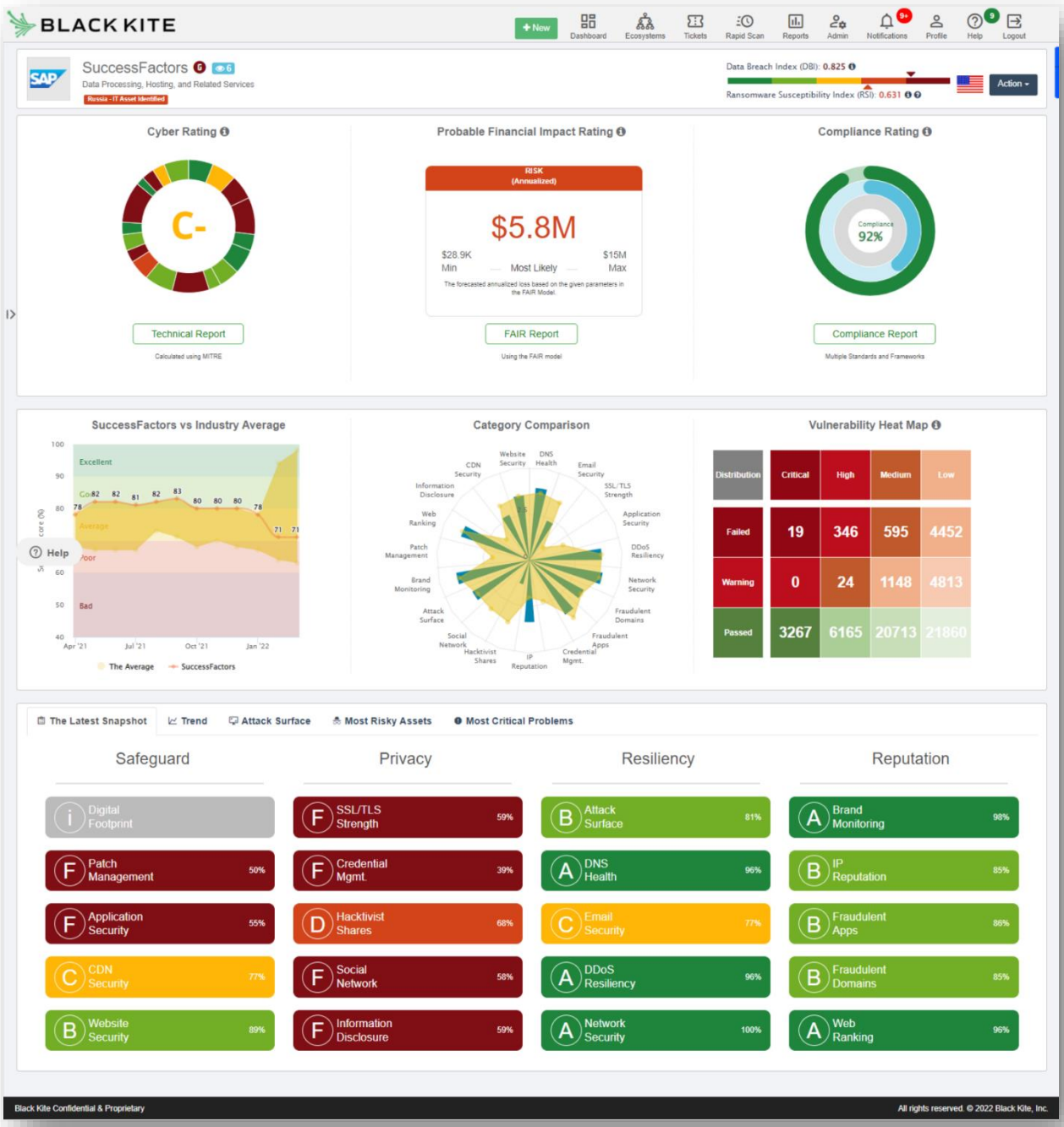


Figure 1: Black Kite cyber risk assessment report for SuccessFactors

Reducing the time and effort to assess third party cyber risk

Cyber risk assessments can be a complex, slow and expensive process – but it does not have to be. The risk assessment process is typically made up of risk assessment questionnaires that are sent to vendors and third parties with much manual prompting and reminders to encourage external parties to complete the questionnaires.

Black Kite presents a revolutionary new way to gather evidence-based cyber risk data in a fraction of the time, allowing customers to assess more vendors and third parties with a fraction of the effort.

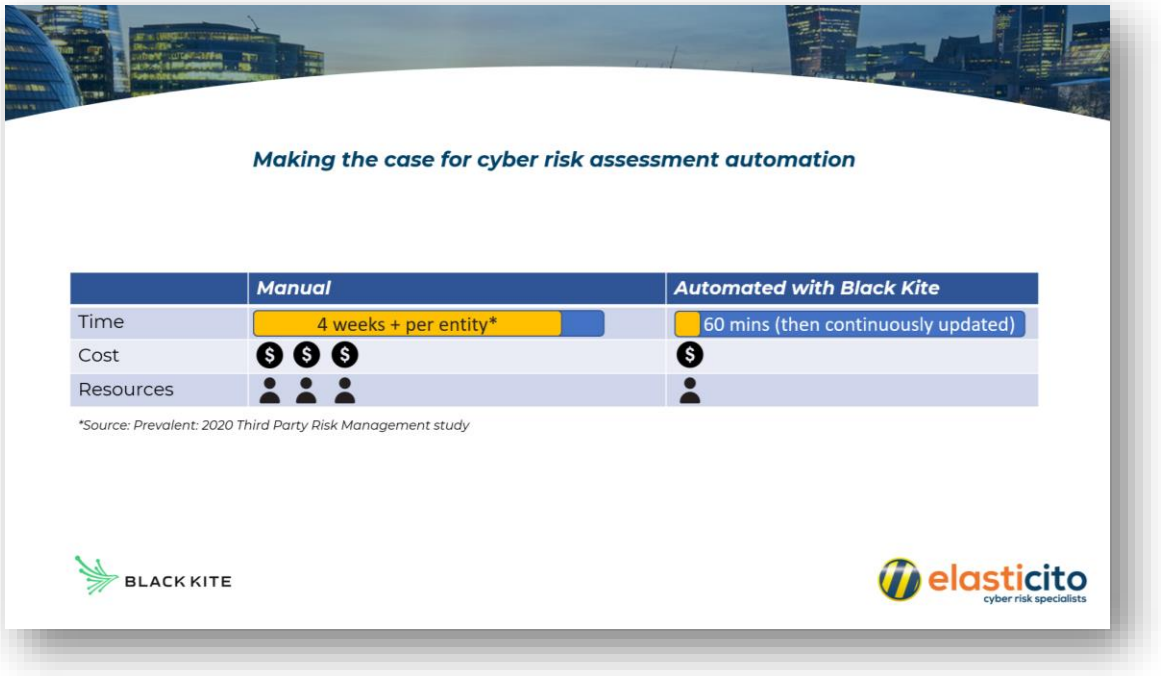


Figure 2: Automating cyber risk assessments with Black Kite

Quantifying third party cyber risk to the Board

Rapid identification of third parties affected by Log4j

Black Kite users are able to instantly identify any vendors or third parties who may have been affected by the Log4j vulnerability; or indeed, whether they have resolved the issue.

This is a useful feature to generate an instant 'long list' of potential third party candidates that can be followed up using risk based questionnaires for critical or high risk third parties.

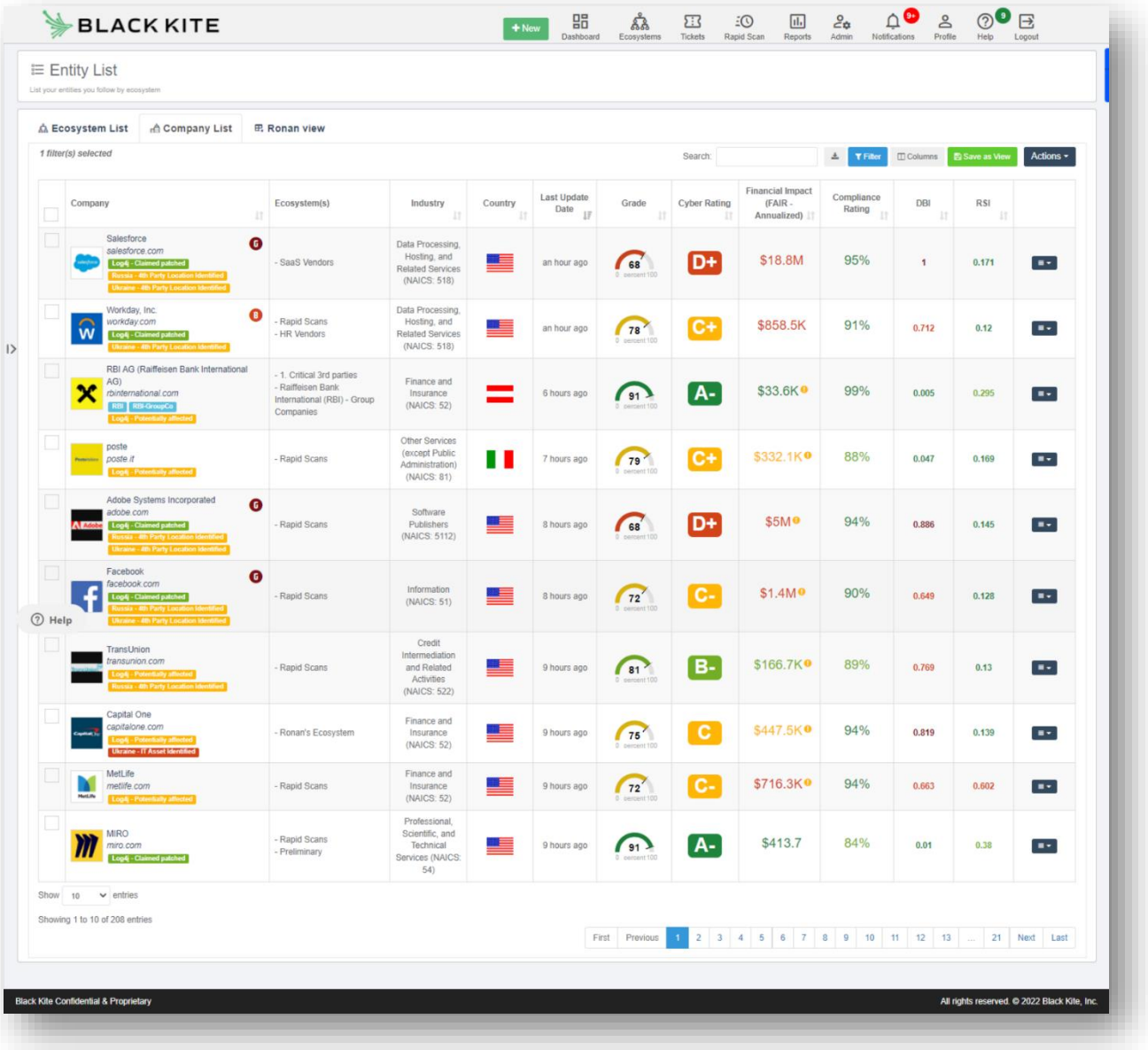


Figure 3: Identifying vendors and third party Log4j vulnerability status

Rapid identification of third parties located in Russia, Ukraine or Belarus

Equally, Black Kite has added the capability to perform similar instant searches for companies that have operations or assets in particular countries.

In the example below, this could be to identify third parties who may be affected by the conflict in Ukraine; or companies that may be affected by sanctions against countries like Russia.

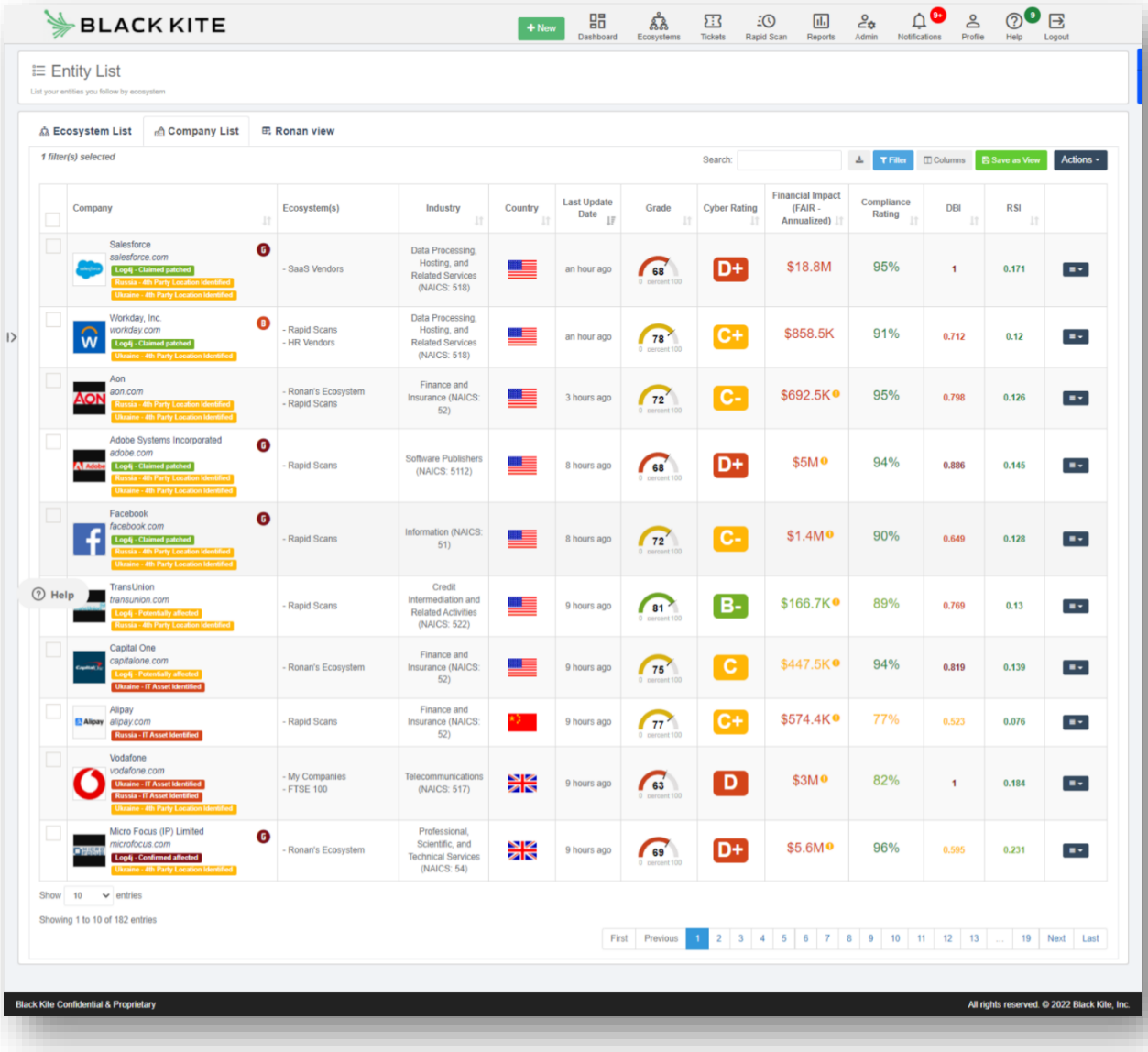
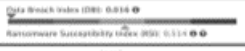
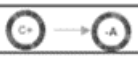


Figure 4: Identifying vendors and third parties with assets or operations in conflict zones or under sanctions

How is Black Kite different to other cyber risk ratings tools, like Bitsight?

While similar solutions, here is a table of six unique capabilities that cannot be found with other risk ratings tools:

1	*Cyber Risk Rating*	MITRE
2.	*Probable Financial Impact*	FAIR INSTITUTE
3.	*Cross-reference to 10+ Compliance Frameworks*	NIST ISO GDPR.EU
4.	*Ransomware Susceptibility Index (RSI)*	
5.	*Universal Parsing Engine*	
6.	*Strategy Report: Step-by-step remediation plan*	

Summary

With Black Kite, you can scale a third party cyber risk management programme to include all key vendors and third parties without having to significantly scale up internal resources. For a fraction of the cost of a manual risk assessment, Black Kite can produce a technically detailed cyber risk analysis of any company and continuously monitor for changes to the cyber risk posture of that company afterwards.

We hope that you will join over 5,000 other enterprise customers around the world and use Black Kite as your cyber risk monitoring platform of choice.