**Cyber Risk API Description**

**Background**

Numerous Partners have successfully used the APEX Analytix Cyber Risk API for many years. In the last several months, the Cyber Risk solution has seen considerable changes (not least a name change), reflected in the API. This and feedback from Partners has led us to create different API versions according to the Partners' needs.

“Partner” is a Customer of APEX Analytix, LLC (“we” or “us”) and has entered into an End-User Services Agreement for Cyber Risk solutions, including one or more of the APIs described herein.

**API Versions**

Development API

This is a fully functioning version of the API to allow Partners to develop the integration of Cyber Risk functionality into their applications. This version provides access to:

- All third-party vulnerability reporting data, including the new “Digital Footprint” category.
- Cyber Threat Intelligence allows the API to query Cyber Risk’s wide range of dark web crawlers to identify threats against third parties.
- Breached credentials, which enables real-time searches for any stolen credentials associated with a domain.

This version also provides access to a new feature, the API widgets. There are 2 widgets:

- Vulnerability Widget—This allows the Partner to integrate the Cyber Risk Vulnerability Report page in the Partner application using our CDN. The widget is fully customizable in terms of design so that the Partners can include their own styles.
- Threat Intelligence Record Widget—This widget provides the same functionality as the Vulnerability Widget but for Cyber Threat Intelligence records.

These widgets benefit the Partner by giving them great flexibility regarding how Cyber Risk reports are embedded in their applications.

Usage

Partners may only use the development API in their sandbox environments for development or demonstration purposes. We monitor the API's usage and will notify the relevant Partner account manager if there is any noticeable upward trend in usage that could indicate that it is being used for commercial purposes.

Freemium API

This version of the API is intended for Partners to enable all their clients to see summary cyber risk vulnerability data for all their Third Parties. The Freemium API is available to all Partners as part of their agreement with us.

The API provides access to the following endpoints:

- Overall Cyber Risk score
- Scores for all 7 vulnerability categories
- The number of high, medium, and low-risk items. These are indicators of which individual tests carried out during a Cyber Risk vulnerability scan need to be addressed in order of priority.

The Freemium API does not provide access to the full vulnerability report, threat intelligence, or breached credential data. Hence, the

widgets do not apply to this version of the API.

Usage

Depending on the commercial agreement between the Partner and us, this version of the API can be used freely by all customers and their associated third parties.

The API provides a quick and easy way to add third-party cyber risk data to the Partners application and provides a route to upgrade to the Premium APIs.

Premium APIs

There are 3 versions of the Premium API:

- Vulnerability Premium-This version provides full access to all detailed third-party vulnerability data but no access to any threat intelligence data
- Threat Premium-This version provides full access to threat intelligence data and only summary access to vulnerability data.
- Full Premium-This version provides unrestricted access to all Cyber Risk data, including:
    - All third-party vulnerability reporting functions, including the new “Digital Footprint” category;
    - Cyber Threat Intelligence, which allows the API to query Cyber Risk’s wide range of dark web crawlers to identify threats against third parties; and,
    - Breached credentials, which enables real-time searches for any stolen credentials associated with a domain.

Usage

The Premium APIs are only available for Partner clients who pay for this functionality. Hence, a commercial agreement must be in place between you and us that specifies the customer's name and level of access, plus all standard commercial terms.

We will issue a new API key for each premium-use customer. This allows us to monitor key usage, review trends, and notify account managers of anomalous usage.

**API keys and upgrades**

Once the End-User Services Agreement is in place, all Partners who require it will be provided with two API keys, one for Freemium and one for Development usage. Partners will also be provided access to the developer's Documentation for the API.

Once the keys have been issued, we will start monitoring their usage. This is particularly true for the Development API, where any use considered outside expected patterns will be notified to the relevant account manager.

To gain access to Premium functionality, the Cyber Risk Product Management team should be provided with details of the commercial agreement with the Partner that licenses premium access by the relevant account manager. On confirmation of this agreement, a new Premium API will be issued to the Partner based on the access allowed. A new API will be provided for each client based on the license agreements provided.

If a Partner's client wishes to upgrade from either the Vulnerability or Threat Premium APIs to the Full Premium, the product management team should provide proof of the new commercial agreement and a new API key will be issued.