Product Specification - KYND Signals Portfolio

Document Creation Date	18 Feb 2025
Document Version	6.0

1. Definitions

a) **Partner** - The KYND customer who is using the KYND Signals service to monitor and or assess the Cyber risk profiles of a portfolio of organisations

b) **Organisations** - The businesses that the Partner is monitoring and or assessing using the KYND Signals Portfolio service

2. Product Description

KYND Signals Portfolio is a report-based Cyber risk analysis service, with each report representing an analysis across a portfolio of Organisations as supplied by the Partner.

Customisable Aggregate Risk Indicators

KYND will, in collaboration with the Partner, define the subset of the cyber risk data points (Aggregate Risk Indicators) to be included in the Partner's Signals Portfolio analysis.

Aggregate Risk Indicators:

Based on Partner-defined criteria (in collaboration with KYND), each Organisation within a portfolio is rated as Red, Amber or Green. Criteria are defined such that:

- The presence of one risk matching a Red criterion rates the Organisation as Red
- If no risks matching Red criteria are present, then the presence of one risk matching an Amber criterion rates the Organisation as Amber
- If no risks matching Red or Amber criteria are present, then the Organisation is rated as Green

KYND provides to the Partner:

- The overall rating of each Organisation within the Signals portfolio
- The criteria which have been matched by risks for each Organisation
- The risks (and details of these) which matched each criterion for each Organisation

The following data points can be included within the KYND Signals product:

Service Risks - Identify the risks associated with the Organisation's services.

Email Security Risks - Analyse how the Organisation has configured its email security and identify impersonation, spoofing and business email compromise risks associated.

Phishing and Malware Risks - Identify whether domains owned by the Organisation are being used or impersonated to host malware or phishing attacks.

Certificate Risks - Identify risks associated with the security certificates associated to the domains and subdomains owned by the Organisation.

Domain Risks - Identify risks associated with Internet Domain registrations.

Proactive Scanning - Identify potential risks in the Organisation relating to specific vulnerabilities, particularly those highlighted in the CISA Known Exploited Vulnerabilities Catalog. This is not included by default and is an optional service. It is the responsibility of the Partner to obtain all the necessary permissions from the scanned Organisations.

Reactive (Zero-Day) Scanning - Driven by KYND's knowledge of real-world Zero-Day exploits. Identify whether an organisation is potentially exposed to specific Zero-Day vulnerabilities. This is an optional supplementary service that is not included by default.

3. Delivery

Signals Portfolio reports can be delivered as:

1. Data in .xlsx or .csv format delivered via a secure mechanism
2. Data in JSON format accessed via the API

4. Support Services

KYND will provide Support Services to the Partner to address issues related to the production of reports. Support will be available from Monday to Friday, between 09:30 and 17:30 UK time, excluding national holidays.

Level 1 - Support will be provided via email in English and covers:

- Assistance with account access and activation
- Basic guidance on the use of the KYND Signals product

Level 2 - Support will be an escalation from Level 1, where an issue requires further investigation by KYND's cyber analysts or engineers.

Level 1 and 2 Support is available to all KYND Partners.

KYND will aim to respond to all queries within one working day.

5. Service Availability

KYND will use reasonable endeavours to maintain an application availability measure of 95%, excluding planned downtime. Partners will be given notice of any planned downtime where possible.