# PRODUCT SPECIFICATION - KYND Signals analysis and report

## Definitions

1. **User:**  
   The end user or customer who is using the KYND Signals service to monitor and/or assess the cyber risk profile of an Organisation
2. **Organisation:**  
   The business that the User is monitoring and/or assessing using the KYND Signals service

## Core information

* 1. **Product Release Date:** February 2023
  2. **Version:** KYND Signals v5
  3. **Product deployment options:**
     1. PDF report per-Organisation, requested by and delivered to the User via signed URLs in the webapp and/or API
     2. Data in .xlsx or .csv format delivered via email or uploaded to a secure cloud location
     3. API access for adding Organisations and retrieving data in JSON format

## Product description:

KYND Signals is a cyber risk analysis service. It is a report-based service, with each report representing a single analysis of one or more Organisations at the date and time the Signals analysis was performed.

### Data

The following data is included within KYND Signals to support its analysis:

|  |  |
| --- | --- |
| **Domain discovery** | Identify domains owned by the Organisation |
| **Domain Risks** | Identify risks that exist in the Organisation’s domains |
| **Service Discovery** | Identify external Internet facing services being run by the Organisation |
| **Service Risks** | Identify risks that exist in the Organisation’s services |
| **Proactive scanning for vulnerabilities** | Identify risks in the Organisation relating to specific vulnerabilities, as highlighted in the CISA [Known Exploited Vulnerabilities Catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog), and identified by KYND’s proactive scanning of the Organisation |
| **Phishing & Malware Risks** | Identify whether domains owned by the Organisation are being used or impersonated to host phishing or malware |
| **Website and Certificate Risks** | Identify risks associated with the configuration of the websites owned by the Cyber Client and the certificates associated with these |
| **Service location** | Identify the location(s) of the Organisation’s services through IP data |
| **Service hosting** | Identify the hosting provider(s) and/or Cloud Service Provider datacentre(s) and service(s) for 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 |

### Analysis

Two core analyses are performed on the data which KYND gathers:

1. Aggregate risk indicator:
   1. Based on User-defined criteria (in collaboration with KYND), each Organisation is rated as Red, Amber or Green
   2. Criteria are defined such that:
      1. The presence of one risk matching a Red criterion rates the Organisation as Red
      2. If no risks matching Red criteria are present, then the presence of one risk matching an Amber criterion rates the Organisation as Amber
      3. If no risks matching Red or Amber criteria are present, then the Organisation is rated as Green
   3. KYND provides to the User:
      1. The overall rating of each Organisation
      2. The criteria which have been matched by risks for each Organisation
      3. The risks (and details of these) which matched each criterion for each Organisation
2. Accumulation insights:
   1. The assets and risks identified within the Signals analysis are aggregated according to a User-defined set of relevant features
   2. These assets are presented as:
      1. Line-item raw data for each asset
      2. A table detailing the proportion of Organisations which have assets with particular (combinations of) features
      3. A table detailing, for particular (combinations of) features, the Organisations with relevant assets, and the proportion those assets represent for each Organisation
      4. A table detailing, for a particular Organisation, the proportion of assets with particular (combinations of) features

### Delivery

1. Signals aggregate risk indicator reports can be delivered as:
   1. PDF report per-Organisation via webapp and/or API
   2. Data in .xlsx or .csv format delivered via email or uploaded to a secure cloud location
   3. Data in JSON format accessed via API
2. Signals accumulation reports can be delivered as:
   1. Data in .xlsx or .csv format delivered via email or uploaded to a secure cloud location

## Support Services

KYND will provide Support Services to the User to resolve any issues with the production of the reports. Support will be available from Monday to Friday, between 9:30 and 17:30 UK time, excluding national holidays.

Level 1 Support will be provided via email or web chat in English. Level 1 support covers:

* account access and activation support
* basic “how to” questions about the KYND Signals

Level 2 Support will be an escalation from Level 1, where an issue or support question requires detailed investigation by the KYND cyber analysts or engineers and/or where more detailed information is required by the User. In some instances, at KYND’s sole discretion, KYND may provide a call-me-back capability.

Level 1 and 2 Support is available to all KYND Users using KYND Signals. KYND will aim to respond to all queries within 1 working day.

## Service Availability

KYND will use reasonable endeavours to maintain an application availability measure of 95% excluding planned downtime. Users will be given at least 48 hours’ notice of any planned downtime where possible.

## Product Price to include

* 1. Product access via webapp and API
  2. Level 1 Support in English
  3. Level 2 Support in English