# **PRODUCT SPECIFICATION - KYND Start**

## **Definitions**

1. **User:**
The end user or customer who is using the KYND Start 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 Start service

## **Core information**

* 1. **Product Release Date:** December 2022
	2. **Version:** KYND Start v3
	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. API access for adding Organisations and retrieving data in JSON format

## **Product description:**

KYND Start is a cyber risk management report service.

It is a report-based service, with each report representing a single scan for an Organisation, discovering the infrastructure that belongs to the Organisation, and analysis of the cyber risk that may affect it.

Each report represents a snapshot in time, when the report was requested.

Multiple documents can be created from a single report. Each document based on the same report will be based on the same underlying data, but will comprise a different collection/representation of that data.

### **Data**

The following data is included within KYND Start 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 |
| **Comparative Risk Profile** | Compare the Organisation versus its peers in the same industry sector. The comparison covers:1. The percentage of services using out-of-date/vulnerable software
2. The percentage of services which are misconfigured
3. The percentage of certificates that have or are in danger of expiry/distrust
4. The percentage of domains with domain protection risks

The comparison places the Subject either “In the group”, “Off the back” or “Straggling” versus its peers on each of these measures |
| **Recommendations** | Prioritises the 5 most important actions that a subject should take to begin to mitigate the cyber risks that have been identified |

### **Documents**

The following components are available for inclusion in a KYND Start document on an Organisation:

* 1. Summary page:
		1. The total number of red, amber, and green risks for the Organisation
		2. Whether the Organisation’s primary domain is vulnerable to email spoofing
		3. Whether the Organisation has any issues which are particularly associated with the risk of ransomware
		4. The comparative risk profile for the Organisation, as described above
	2. Recommendations page:
		1. The five recommended actions for the Organisation, as described above
	3. Methodology section:
		1. A brief and high-level description of KYND’s process of discovery, scanning and analysis
	4. High risks:
		1. A list of all red risks identified for the Organisation, with relevant details and advice
	5. Risks for consideration:
		1. A list of all amber risks identified for the Organisation, with relevant details and advice
	6. Domains list:
		1. A list of all domains discovered for the Organisation, with their registrant details

The User can create any number of documents based on a single report “scan” on an Organisation. These documents can be any of the below formats:

* 1. Start Summary document, comprising of the Summary page only
	2. Start Full document, comprising all of the above components, in the above order
	3. Custom configuration, comprising any combination of the above components, in the above order

## **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 Start

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 Start. 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