Product Specification - KYND ON

Document Creation Date	20 Feb 2025
Document Version	6.0

1. Definitions

a) **User** - The end user or customer who is using the KYND ON product to monitor and or assess the Cyber risk profile of an organisation. Multiple Users can be added to the account for a single Organisation

b) **Organisation** - The business that the User is monitoring and or assessing using the KYND ON product

2. Product Description

KYND ON is a web-based cyber risk monitoring service, which periodically performs an analysis of an Organisation. This monitoring starts from the date on which the customer activates their service.

Data

The following data points are included within the KYND ON product:

Domain Discovery - Identify additional domains owned by the Organisation.

Domain Risks - Identify risks associated with Internet Domain registrations.

Service Discovery - Identify external Internet-facing services being run by the Organisation.

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

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.

Proactive Scanning - Identify potential risks in the Organisation relating to specific vulnerabilities, particularly those highlighted in the CISA Known Exploited Vulnerabilities Catalog. This is an optional service and it is the responsibility of the customer to obtain

all the necessary permissions from the scanned organisation (if accessing their KYND ON dashboard directly the User can directly opt-in and provide those permissions).

Reactive (Zero-Days) 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.

Service Location - Identify the location(s) of an Organisation's assets through the IP data.

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

Data Breach Risks - Identify any risks to the security of the customer data being held by the Organisation. This involves KYND creating unique synthetic identities which the User can insert into their Organisation's databases. KYND will then monitor for and alert to any use or attempt to use these identities.

Ransomware risks - Focuses on a subset of the Organisation's risk factors to identify specific risks that would enable a ransomware attack. Prompts the User to provide additional information to add further data for KYND's analysis of the Organisation's ransomware risk. Presents the User with actions to take to mitigate the Organisation's ransomware risk.

Recommendations - Accessible to KYND ON Users by downloading their on-demand Start report PDF export (see Functionalities below). Prioritises up to five of the most important actions that a subject should take to begin to mitigate the cyber risks that have been identified.

Comparative Risk Profile - Comparison of the Organisation to others in the same industry sector. The comparison covers:

1. The percentage of services using out-of-date and or vulnerable software
2. The percentage of services which are misconfigured
3. The percentage of certificates that have or are in danger of expiry and or distrust
4. The percentage of domains with domain protection risks

Functionalities

Domain Suppression - Allows the User to suppress new and previously identified assets for any domain and corresponding risks.

Start Report Export - Allows the User to generate an on-demand Start Full PDF document based on their Organisation's current risks.

CSV Data Export - Allows the User to generate an on-demand CSV download with the data for all their Organisation's current risks.

Mark As Resolved - Allows the User to mark an individual risk as fixed. This will remove the risk from being shown among other red/amber/green risks. In the subsequent hours, KYND will verify whether the risk has been resolved, and update the risk to the appropriate risk level.

3. Delivery

Data can be exported in the following forms:

1. **CSV Data** - An export of all risks
2. **Start Full PDF** - Includes all the selectable components

4. Support Services

KYND will provide Support Services to the User to address issues related to the KYND web application. 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 web application
- Clarification regarding the KYND analysis results or alerts, to the extent necessary for the User to relay relevant information to their IT support or cybersecurity provider

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

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

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. Users will be given notice of any planned downtime where possible.