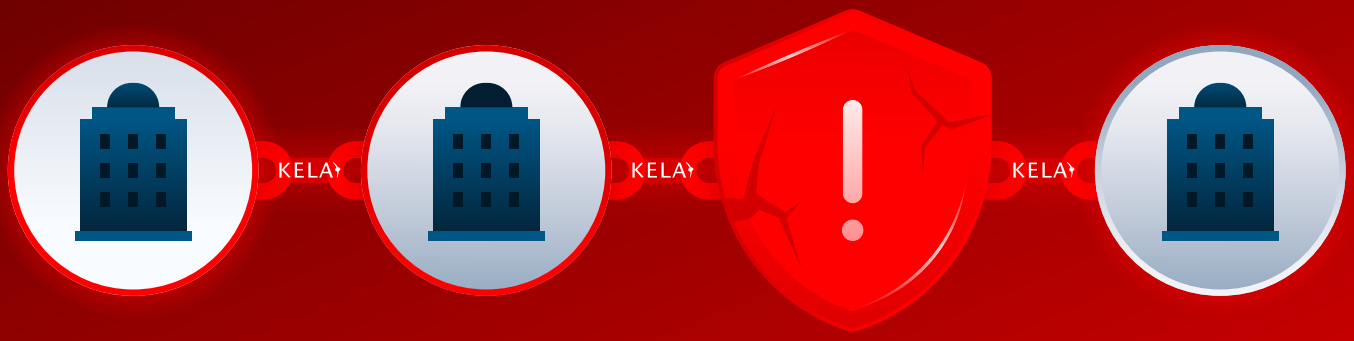
KELA

Essential Guide

TPRM Technical Process Overview



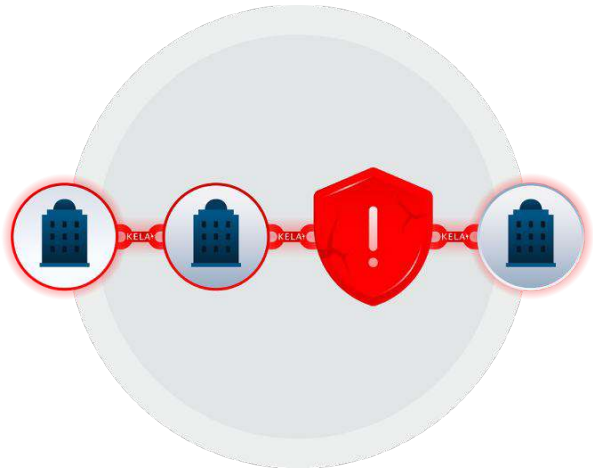
KELA

The leading provider of real, actionable intelligence

TPRM Technical Process Overview

Introduction To Kela TPRM

Kela's cutting-edge Third-Party Intelligence solution empowers organizations to assess and make informed decisions regarding the businesses within their supply chain by taking into account their cyber exposure. This module is dedicated to delivering trustworthy intelligence, minimizing the risk of inaccuracies, and leveraging a wealth of reliable information sources to ensure precise calculations of cyber risk. Our solution integrates Cyber Threat Intelligence (CTI) from the depths of the Darknet and Cybercrime sources, seamlessly merging with our comprehensive Attack Surface Monitoring (ASM).



Module Architecture Overview

This solution is built on a multiple-layer technical solution, from quick vendors onboarding to risks remediation recommendations. This document introduces each of the layers systematically and details the actions performed by the platform in each of the stages.

Automated Asset Discovery › Risks Collection › Score Calculation › Portfolio Analysis › Actionable Output

1

Asset Discovery

In the onboarding process, Kela detects digital assets related to a company's network using multiple mechanisms and capabilities.

2

Risk Collection

The platform collects cyber risks from 3 main categories; Threat Intelligence Exposure, Attack Surface Management and Technical Intelligence. The risks are collected using Kela's in-house capabilities.

3

Score Calculation

Score Calculation: By combining the collected risks on the detected assets in a proprietary scoring algorithm, a score calculation process in enabled per company. The score is a prediction mechanism, assessing the probability of a company to be effected by a cyber incident.

4

Portfolio Analysis

Kela's portfolio dashboard includes overview information about the vendors with trends, distribution information and aggregated data.

5

Actionable AI-powered Output

Reports and an AI assistant that include recommendations for issues remediation.

Discovery Process

The TPRM discovery process is aimed at detecting all the digital assets related to a specific, required organization online. The discovery mainly includes 2 logics (horizontal discovery and vertical discovery), while each stage includes different mechanisms. The following explanations details the high-level process, while each stage consists of multiple sub-stages.

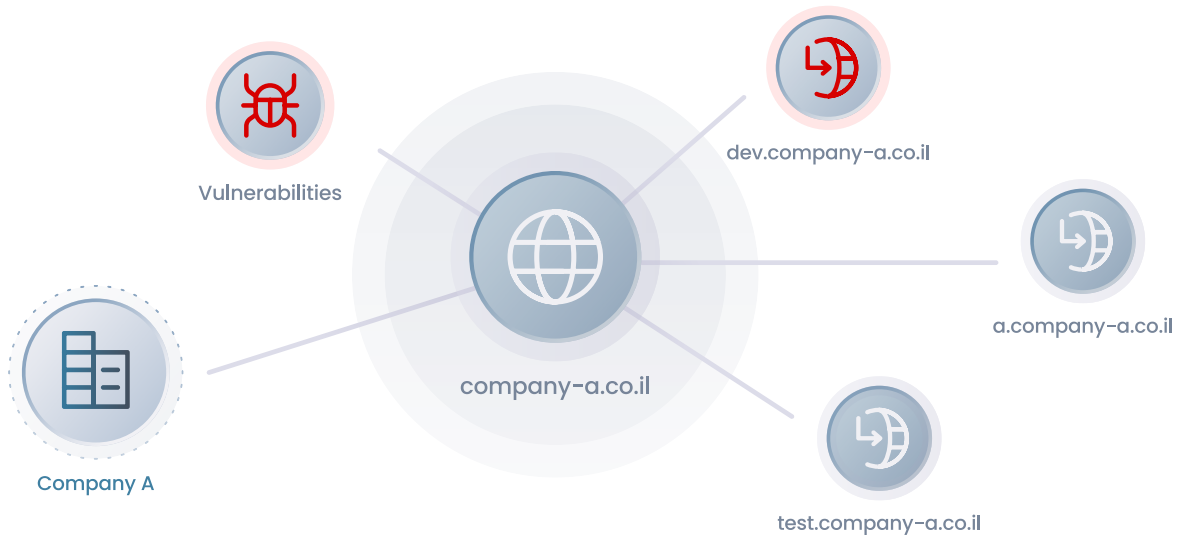
Horizontal Discovery

In the first stage, kela discovers all assets related to the initial asset on the same level, including domains and subdomains. There are several methods enabled in this stage.

Vertical Discovery

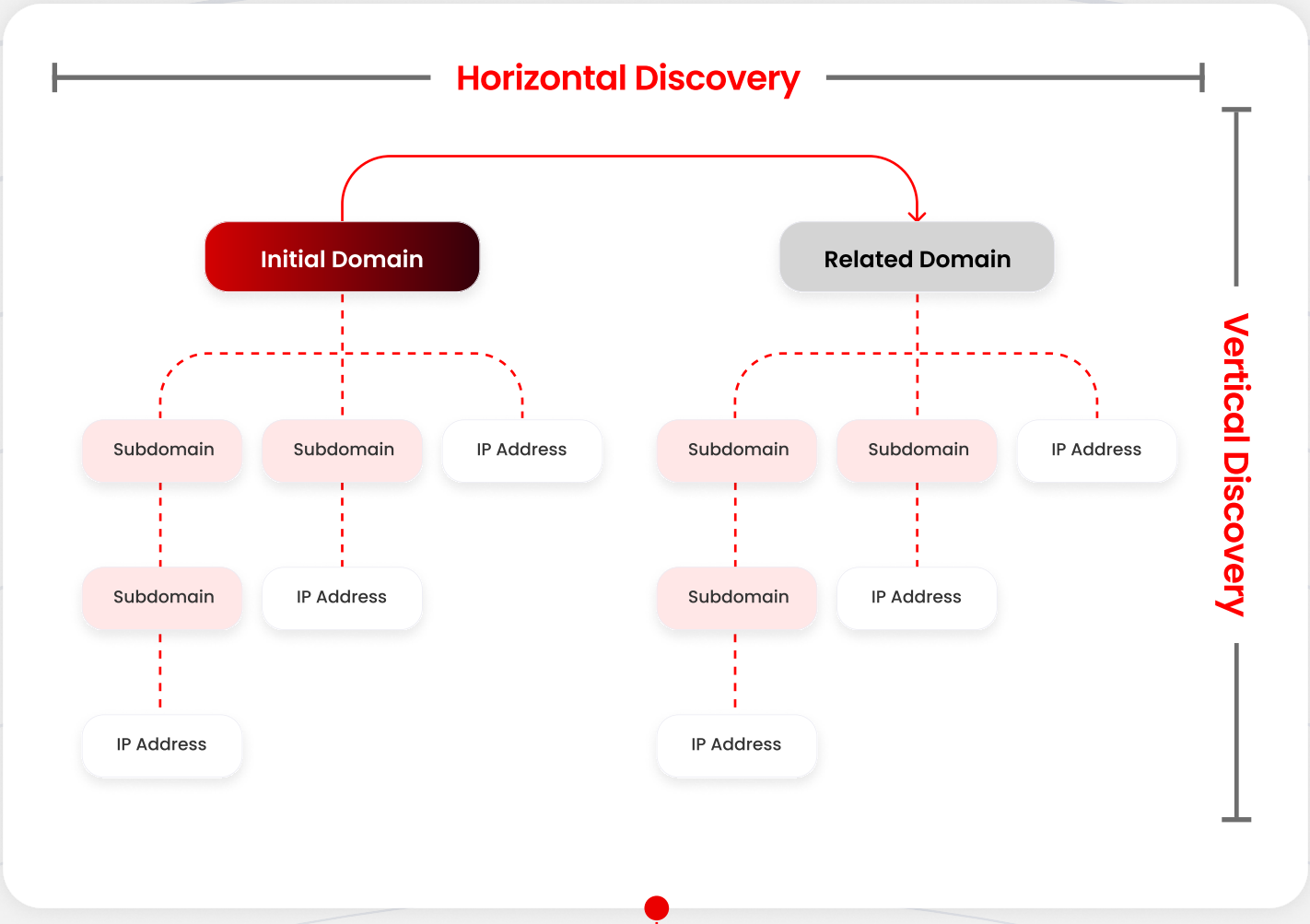
The following stages are performed by a combination of tools and methods, including in-house developed capabilities.

I. **In the second stage**, all subdomains related to a domain are collected.
II. **In the third stage**, all detected assets are tested for their resolving IPs.



Company's detected assets presented in Kela's visual module

The visual below present the discovery stages:



Risk Collection

To calculate an accurate score, Kela collects intelligence from multiple sources, relying on in-house developed capabilities. The intelligence is collected from Darknet & Deep Web sources, as well as technical/configuration tests. When combined, the intelligence collected per company supports the score calculation process, aimed at assessing the probability of a cyber incident.

Threat Intelligence Exposure

Leaked Credentials: These results include exposed user login credentials from various sources, offering high value to hackers, as password reuse is common, and such leaked data often appears first on the dark web after successful application breaches.

Compromised Accounts: Stolen data from banking Trojan botnets, including credentials taken by password stealers or form injectors, with each result representing a single stolen account from an infected machine and including the GUID of the infected machine, associated service, username, password (if available), and data source.

Initial Access: Initial Network Access refers to remote access to a computer in a compromised organization. They play a crucial role in the ransomware-as-a-service economy, as they significantly facilitate network intrusions by selling remote access to a computer in a compromised organization and linking opportunistic campaigns with targeted attackers, often ransomware operators. Kela monitors the initial network access listings published for sale on various cybercrime underground forums. Based on Kela's research, companies with initial access listing published is highly likely to suffer a cyber incident.

Ransomware Attack: Kela monitors for ransomware victims in ransomware actors' blogs and negotiation portals, data leak sites and public reports. Ransomware listings impact the Risk Score for a long period, as most companies suffering a ransomware incident are highly likely to experience significant damage in business continuity, or an additional incident.

Database Leak: A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information. Kela monitors listings of recent leaks of popular, global services.

Technical Intelligence

Outdated Technologies: Outdated technologies are older software, operating systems, and hardware used for a while, and "outdated" means newer versions have likely been released with improved security, efficiency, and results.

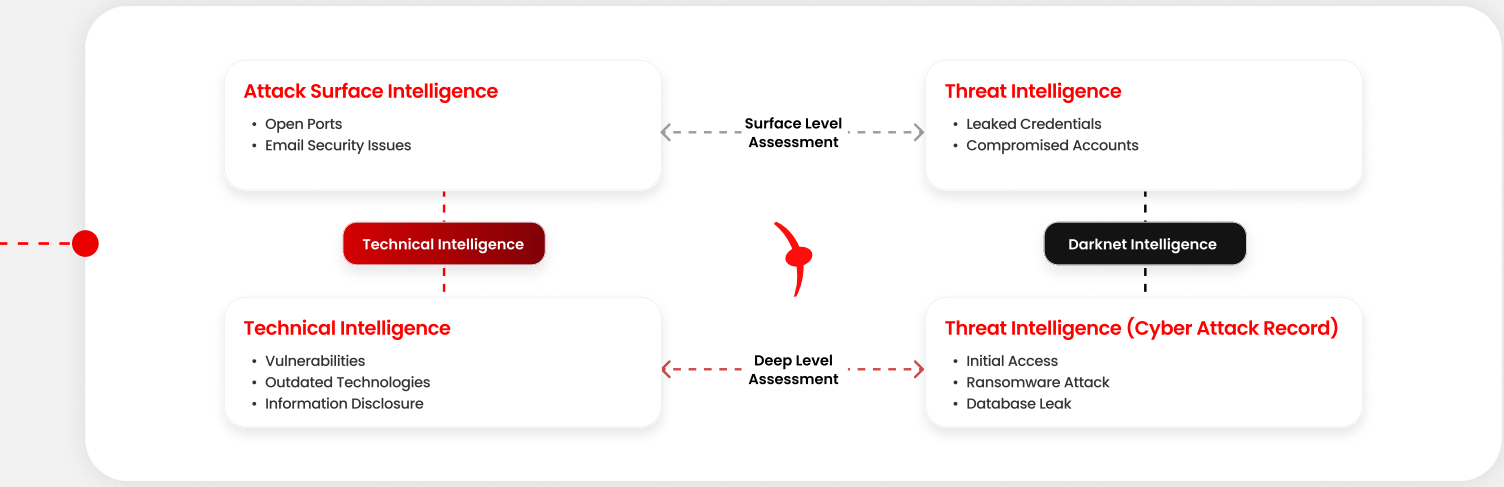
Vulnerabilities: Continuously scanning for and patching vulnerabilities in web applications and networks is crucial to reduce the risk of critical exploits that could lead to server takeovers, website defacement, session cookie theft, and more, helping companies proactively safeguard their businesses against cyberattacks.

Information Disclosure: Information disclosure occurs when sensitive data, like SSH private keys, API keys, and clear text credentials, is unintentionally exposed through the source code or publicly accessible endpoints, which may happen if an attacker gains access to improperly secured configuration files like /.git or /db.php.

Attack Surface Management

Open Ports: Ports are crucial for Internet communication, where actively accepting packets open ports can pose security risks if not properly managed, potentially leading to unauthorized access and system compromise.

Email Security Issues: Email data in transit can be intercepted by cybercriminals for attacks, including data theft and malware delivery, and advanced social engineering tactics via email can bypass traditional security measures, making secure email servers essential to reduce the risk of various attacks, such as phishing and spoofing.



Cyber Risk Score

The TPRM module's cyber risk score was created to solve the current issue of incomplete risk assessments and the critical oversight of risks with a proprietary scoring algorithm, created by analyzing a database of more than +2k cases of confirmed ransomware.

The score operates on a scale of 0 to 100, representing the risk of the company being attacked. It leverages a distinctive Attacker's Perspective to analyze accumulated risks. This predictive tool empowers you to proactively manage third-party cyber risks, safeguarding organizations from potential cyber attacks that could result in various consequences, including but not limited to ransomware infections, disruptions to business continuity, and the leakage of confidential data.

Algorithm Overview

- Built on a decade+ Darknet & cybercrime database.
- Developed with Threat Intelligence experts, considering attackers' view
- Functions as cyber incidents prediction tool

Score Calculation Process

Actionable Assets Discovery

- Automatically verify assets' discovery domains, subdomains, and IP's.

Intelligence Collection

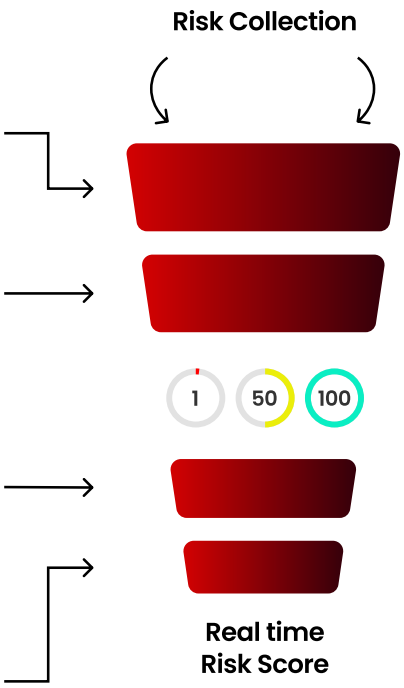
- Advanced intelligence analysis uncovers attackers' motivations through in-depth knowledge of Darknet and open sources.

Noise Reduction & Risk Prioritization

- Exclusively focusing on verified data with the potential to affect the vendor's network, an advanced ranking procedure is applied to each risk and threat, ensuring maximum accuracy in the overall scoring.

Cyber Risk Score

- A cumulative risk score for a company's vendors is provided.

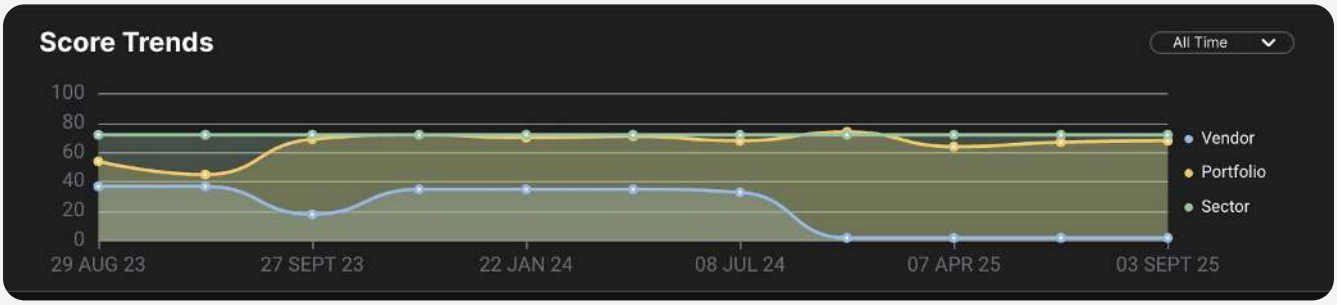


Portfolio Analyis

Following a setup of the portfolio with vendors intelligence & score, Kela's TPRM provides users high-level analysis of the portfolio, including trends and data distribution.

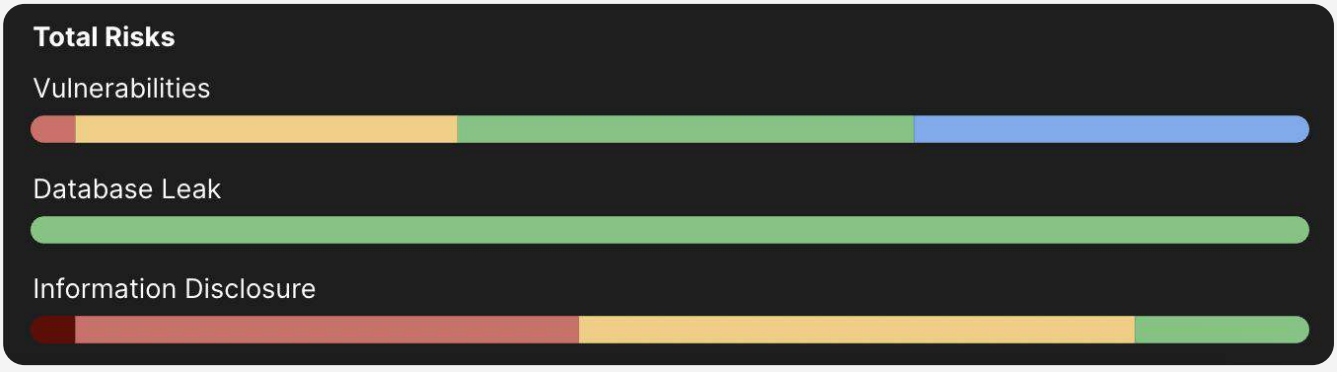
Score Trends

This graph presents the change in the portfolio average score over time. By examining it, users can view whether their portfolio exposure level is improving over time or if there's a decrease in the status. This graph supports Kela's vision to maintain portfolio with +75 average score, representing a lower exposure level and potential to experience a cyber incident.



Total Risks

This component includes summary information of all risks collected in the portfolio by Kela. The data is presented by Intelligence Type, with a distribution to severity: Critical, High, Medium, Low and Informational. When hovering over any section in the bar, the number of total risks is presented.

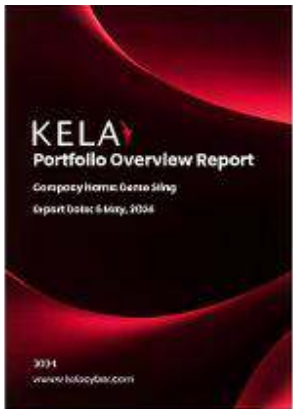


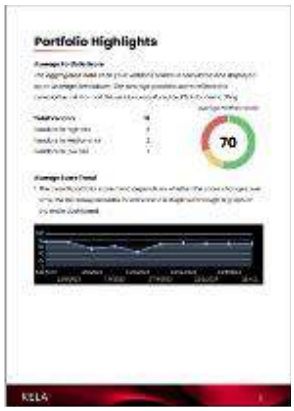
Reports

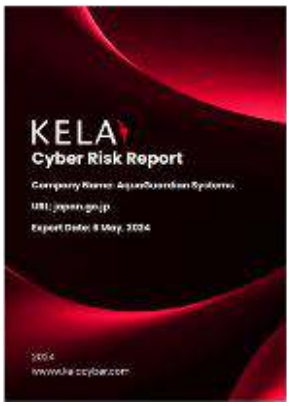
The TPRM module provides companies with the flexibility to generate 2 types of reports; Portfolio Report & Vendor Overview report. These reports include high level and in-depth information about intelligence collected by Kela. These reports can be used to share information with vendors or within organizations and support prioritization and remediation processes.

Portfolio Report

The **Portfolio Report** offers a comprehensive perspective on the overall security posture of vendors, showcasing essential insights into how your portfolio's cyber posture evolves based on vendors' risk profiles & scores.







The **Cyber Risk Report** offers an in-depth view of a specific vendor, providing insights into their cybersecurity posture and the risks that led to the risk score.

Recommendations & Remediation

Kela's reports include recommendations to resolve the detected cyber risks. It provides actionable steps for improving security and guidance on addressing each identified issue.

Reccomendations

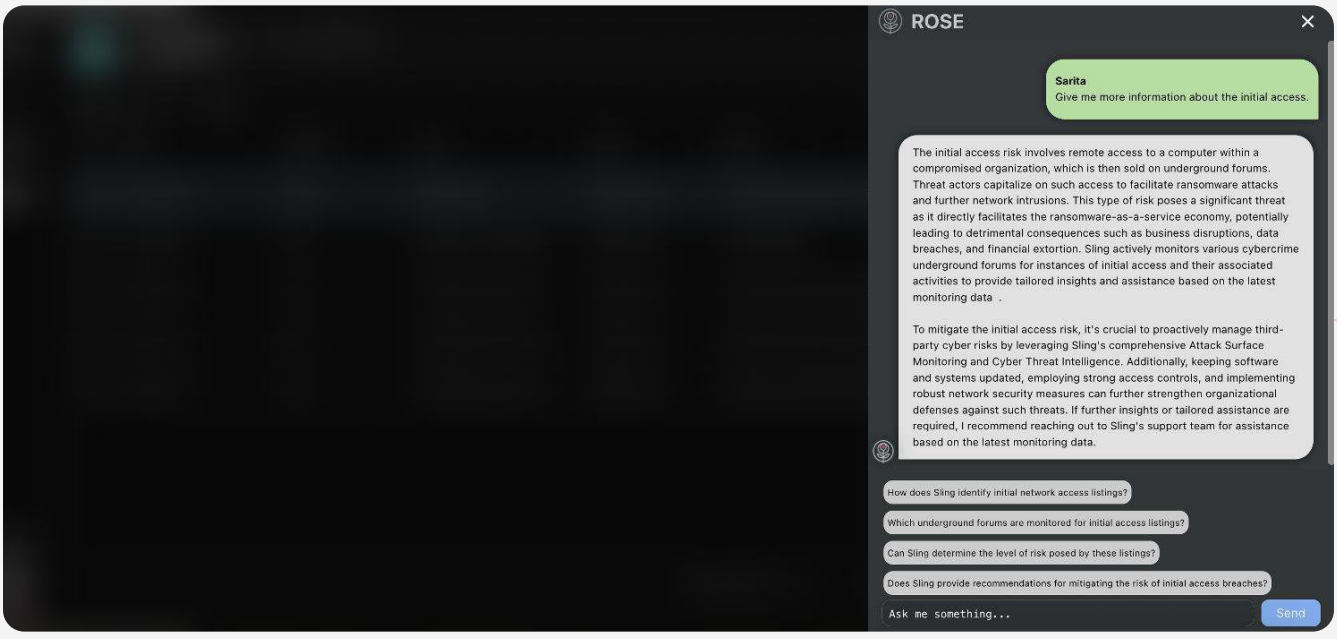
Review the potential exposure of the vulnerability and address the unique parameters required.

For any assistance or clarification, do not hesitate to reach out to us at: **info@sling.insure**

An example of a "Recommendation" as seen in the Cyber Risk Report

AI Actionable Output - ROSE AI

Kela's TPRM AI virtual assistant, ROSE, delivers both high-level and in-depth insights into specific risks and detections, along with real-time context and enriched remediation guidance.



An example of a "Recommendation" as seen in the Cyber Risk Report

Next Steps

Following a setup of the portfolio with vendors intelligence & score, Kela's TPRM provides users high-level analysis of the portfolio, including trends and data distribution.

1 Onboarding Process

Kela ensures an efficient onboarding process, by following these steps:

- Requires only vendors domain for score calculation.
- Support hundreds of vendors onboarding in parallel.

2 Ongoing Services

By using Kela's technology, the following services are provided:

- Risk assessment is triggered every 24 hours.
- Live Score Change, based on risks detection and remediation.
- Real time alerts based on pre-define thresholds.
- Ongoing new related assets discovery.
- Data export to reports per demand.

3 Technical Support

Kela can provide customers with support based on different use cases.

- Technical support per risk.
- Ongoing, scheduled status meetings.
- Dedicated communication with vendors for issues remediation.