RiskAuto: Third-Party Risk Assessment Automation

- A web-based SaaS solution for Third-Party Risk Assessment with Cloud security capability.

Note for: Visitors & Contributors:

This is a learning-focused weekend project to help the broader community of Cybersecurity professionals, and newbies learn and identify mistakes in design, code, or overall approach. That's intentional to some extent — I'm using this space to experiment, try new ideas, and improve over time.

This project is a work in progress. If you notice something that could be better, I'd genuinely appreciate your help:

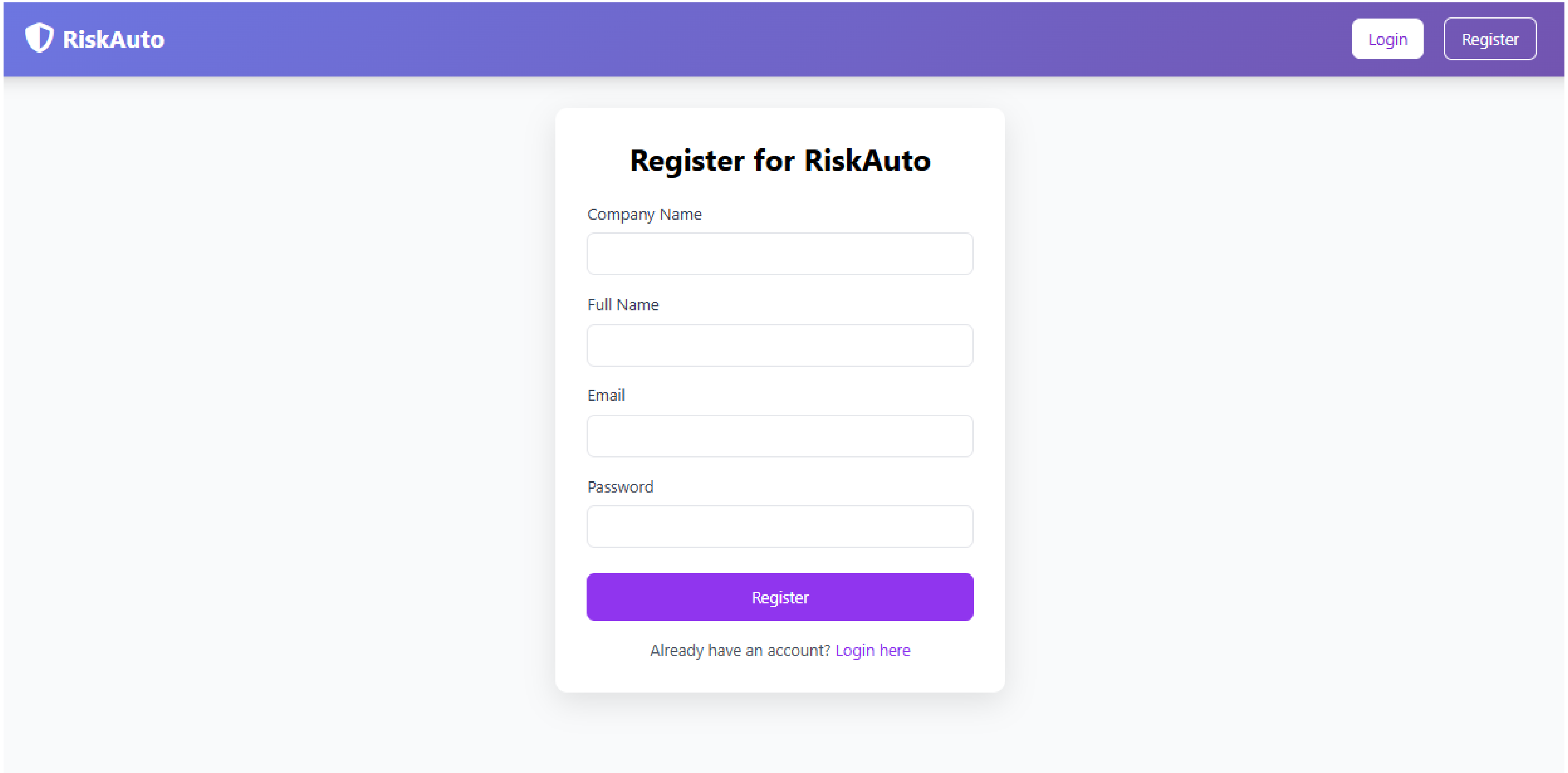
- Please feel free to open an issue to share suggestions or ask questions.
- Submit a pull request with improvements.
- Share best practices, alternative designs, or helpful resources.

I'm always keen to learn from others, so if you're interested in collaborating or giving feedback, you're very welcome here.

GitHub Link: RiskAuto

RiskAuto Processes	Description
User Registration	New user registration.
Dashboard	User dashboard showing third-party risk assessment automation options.
Passive Scanning	Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.
Questionnaires	Create customizable security questionnaires to share with third parties for risk assessment.
Risk Assessments	View completed questionnaires by third-party and the risk ratings.
Reports	Auto-generated risk assessment reports with detailed analysis based on risk assessment questionnaires.

User Registration



Register for RiskAuto

Company Name

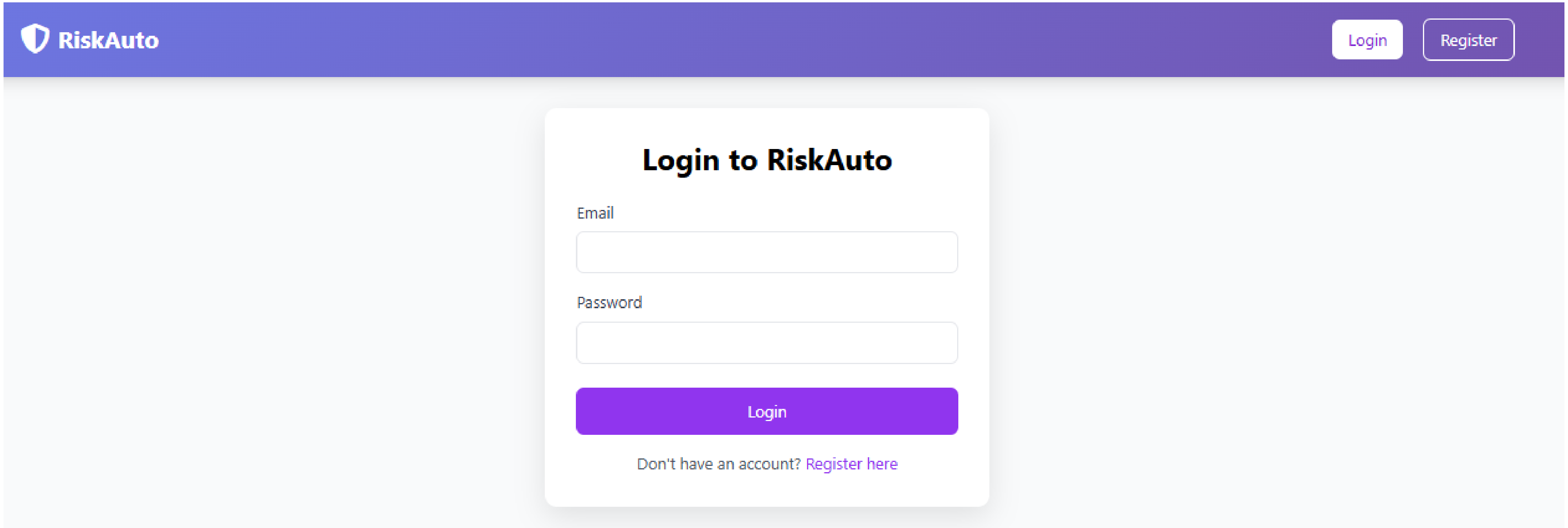
Full Name

Email

Password

Already have an account? Login here

User Login



Login to RiskAuto

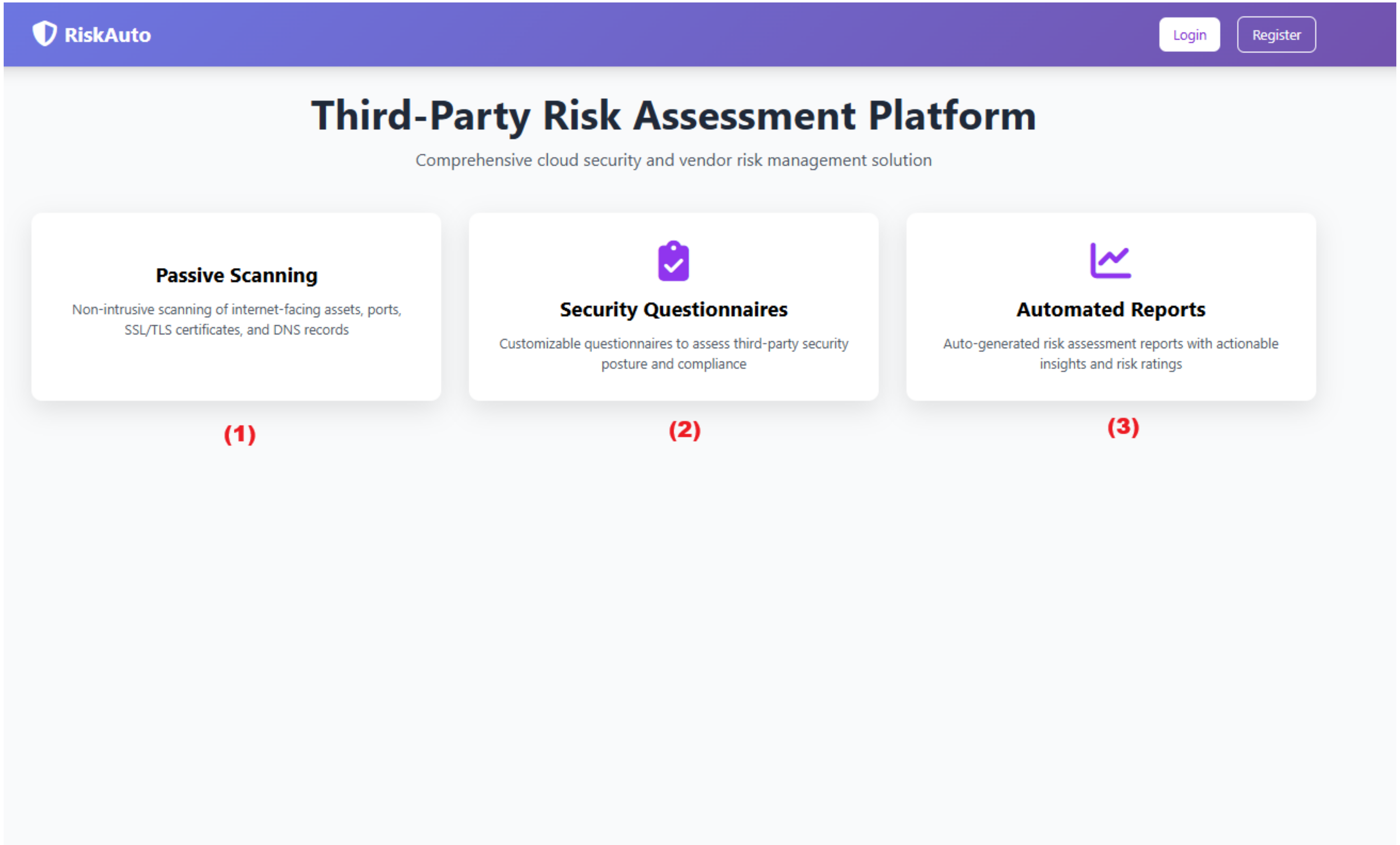
Email

Password

Don't have an account? Register here

RiskAuto has 3 options.

(1) Passive Scanning.
(2) **Security Questionnaires** for third-party risk assessment.
(3) **Automated Reports** for risk assessment.



Third-Party Risk Assessment Platform

Comprehensive cloud security and vendor risk management solution

Passive Scanning

Non-intrusive scanning of internet-facing assets, ports, SSL/TLS certificates, and DNS records

Security Questionnaires

Customizable questionnaires to assess third-party security posture and compliance

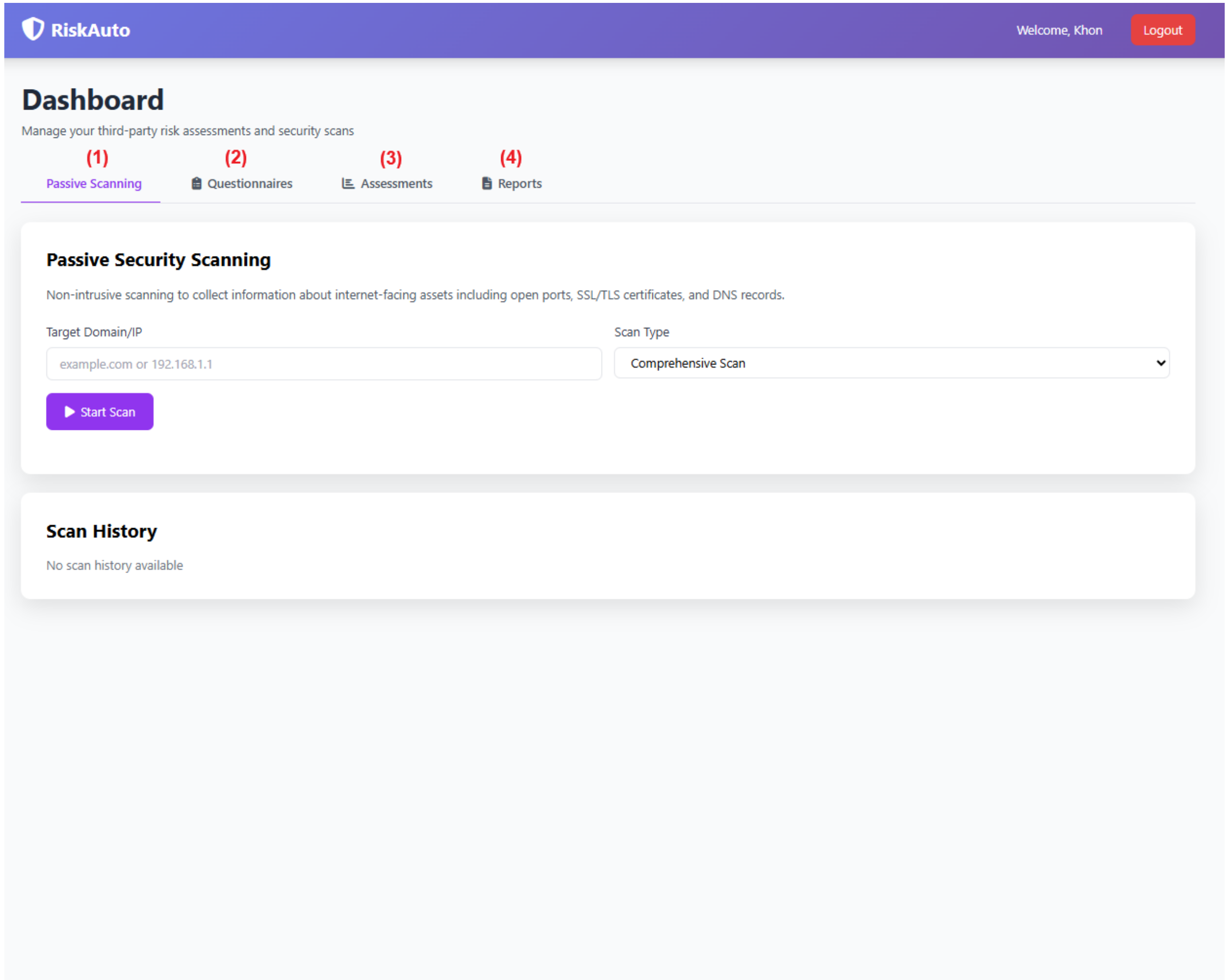
Automated Reports

Auto-generated risk assessment reports with actionable insights and risk ratings

Dash Board:

There are 4 sections.

1. **Passive scanning.**
2. **Questionnaires.**
3. **Assessment.**
4. **Report.**



Dashboard

Manage your third-party risk assessments and security scans

Passive Security Scanning

Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.

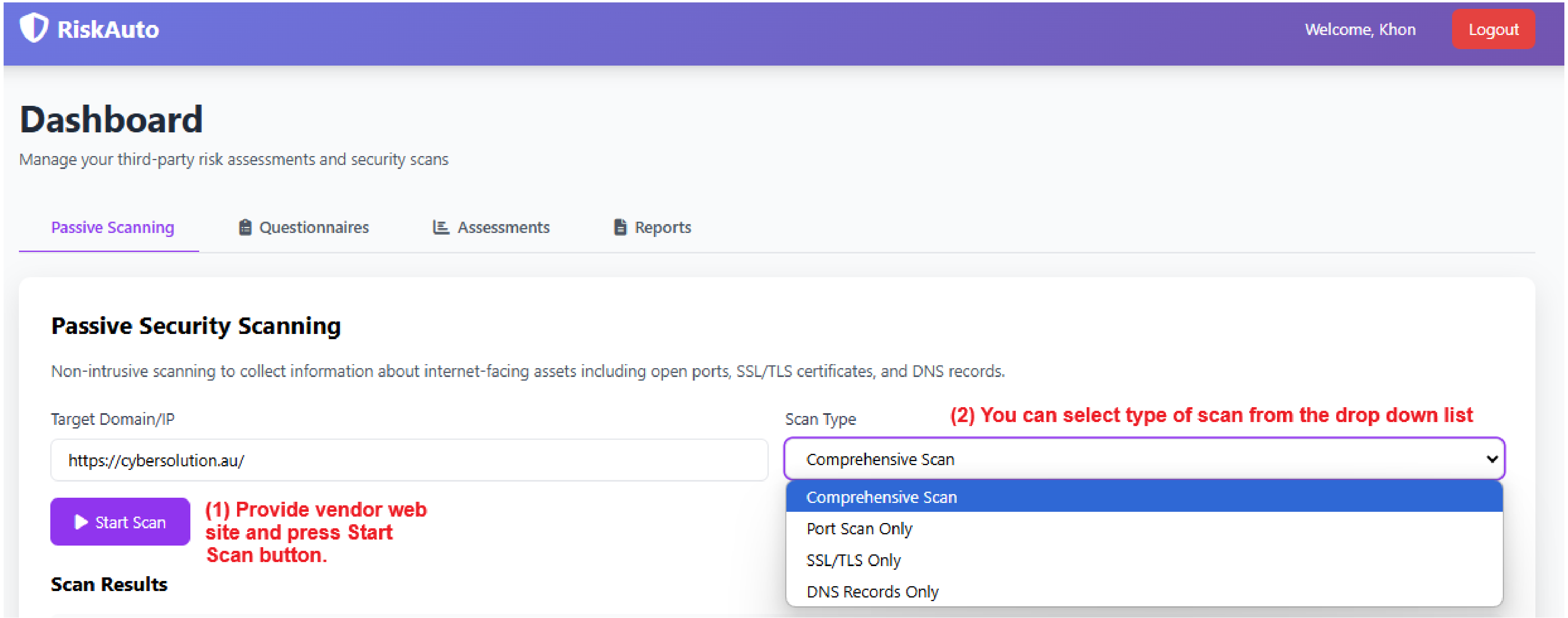
Target Domain/IP: example.com or 192.168.1.1

Scan Type: Comprehensive Scan

Scan History

No scan history available

1. Passive Scanning:



Dashboard

Manage your third-party risk assessments and security scans

Passive Security Scanning

Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.

Target Domain/IP: https://cybersolution.au/

Scan Type: Comprehensive Scan

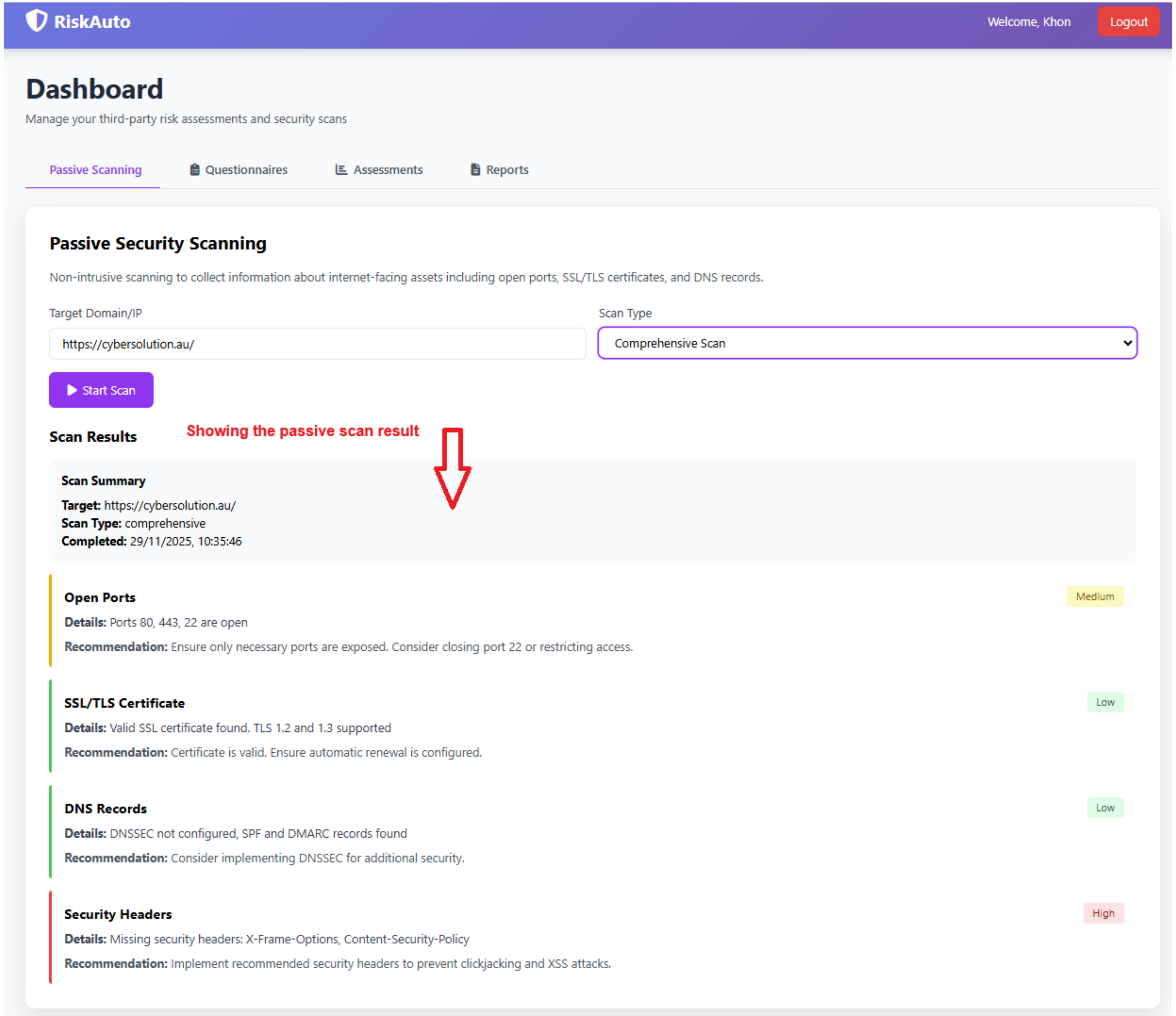
(1) Provide vendor web site and press Start Scan button.

(2) You can select type of scan from the drop down list

(1) Select third-party's business web-site for passive scan. This is non-intrusive scanning to collect information about internet facing assets including open ports, SSL/TLS certificates and DNS records.

(2) Scan type: User can select various scanning process depends on the business requirements.
   a. Comprehensive Scan.
   b. Port Scan.
   c. SSL/TLS Scan.
   d. DNS Records.

Scan Result



Dashboard

Manage your third-party risk assessments and security scans

Passive Security Scanning

Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.

Target Domain/IP: https://cybersolution.au/

Scan Type: Comprehensive Scan

Scan Results

Showing the passive scan result

Scan Summary

Target: https://cybersolution.au/
Scan Type: comprehensive
Completed: 29/11/2025, 10:35:46

Open Ports Medium

Details: Ports 80, 443, 22 are open

Recommendation: Ensure only necessary ports are exposed. Consider closing port 22 or restricting access.

SSL/TLS Certificate Low

Details: Valid SSL certificate found. TLS 1.2 and 1.3 supported

Recommendation: Certificate is valid. Ensure automatic renewal is configured.

DNS Records Low

Details: DNSSEC not configured, SPF and DMARC records found

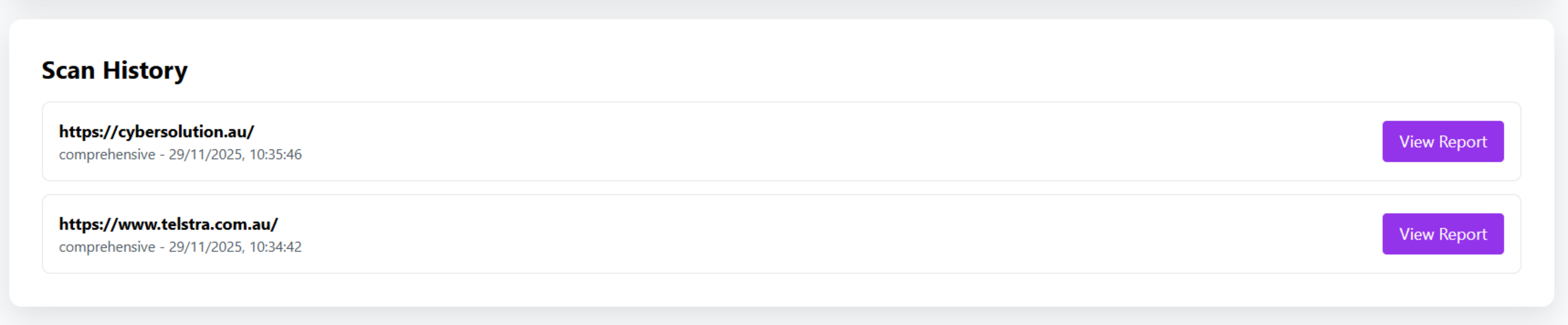
Recommendation: Consider implementing DNSSEC for additional security.

Security Headers High

Details: Missing security headers: X-Frame-Options, Content-Security-Policy

Recommendation: Implement recommended security headers to prevent clickjacking and XSS attacks.

Scan history



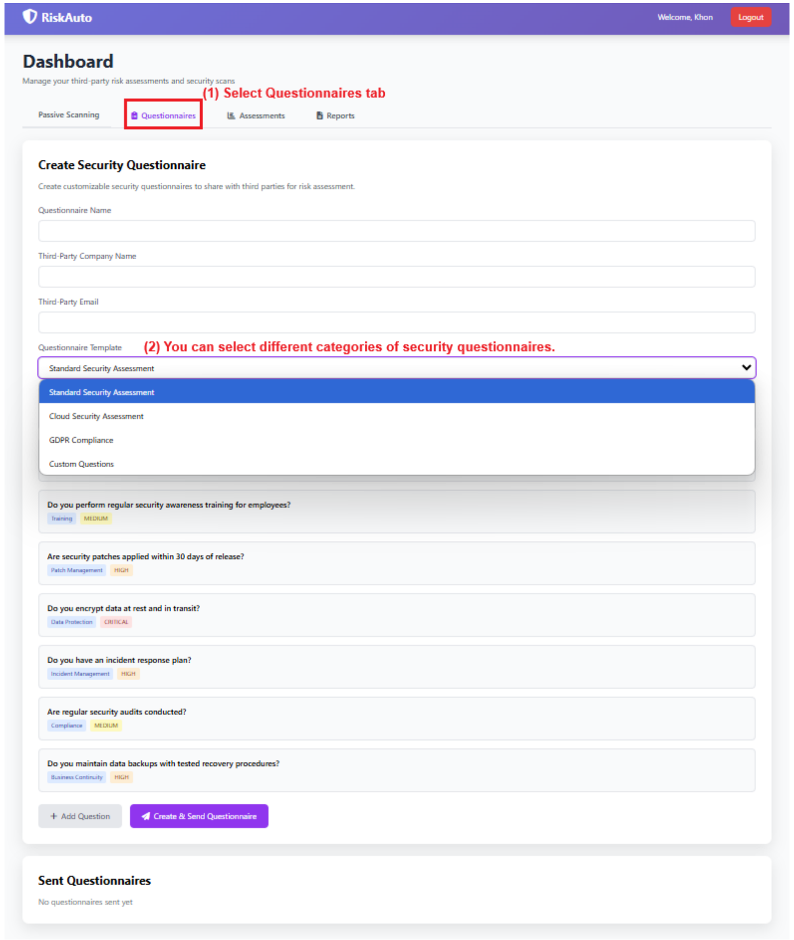
Scan History

https://cybersolution.au/
comprehensive - 29/11/2025, 10:35:46

https://www.telstra.com.au/
comprehensive - 29/11/2025, 10:34:42

2. Questionnaires

- User can complete all the necessary information as shown in the screenshot.
- Questionnaire Template: User can select questionnaires type according to the business need and scope of the risk assessment.
  - a) Standard Security Assessment.
  - b) Cloud Security Assessment.
  - c) GDPR Compliance.
  - d) Custom Questions.



Dashboard

Manage your third-party risk assessments and security scans

(1) Select Questionnaires tab

Create Security Questionnaire

Create customizable security questionnaires to share with third parties for risk assessment.

Questionnaire Name

Third-Party Company Name

Third-Party Email

Questionnaire Template

(2) You can select different categories of security questionnaires.

Standard Security Assessment

- Standard Security Assessment
- Cloud Security Assessment
- GDPR Compliance
- Custom Questions

Do you perform regular security awareness training for employees? Training MEDIUM

Are security patches applied within 30 days of release? Patch Management HIGH

Do you encrypt data at rest and in transit? Data Protection CRITICAL

Do you have an incident response plan? Incident Management HIGH

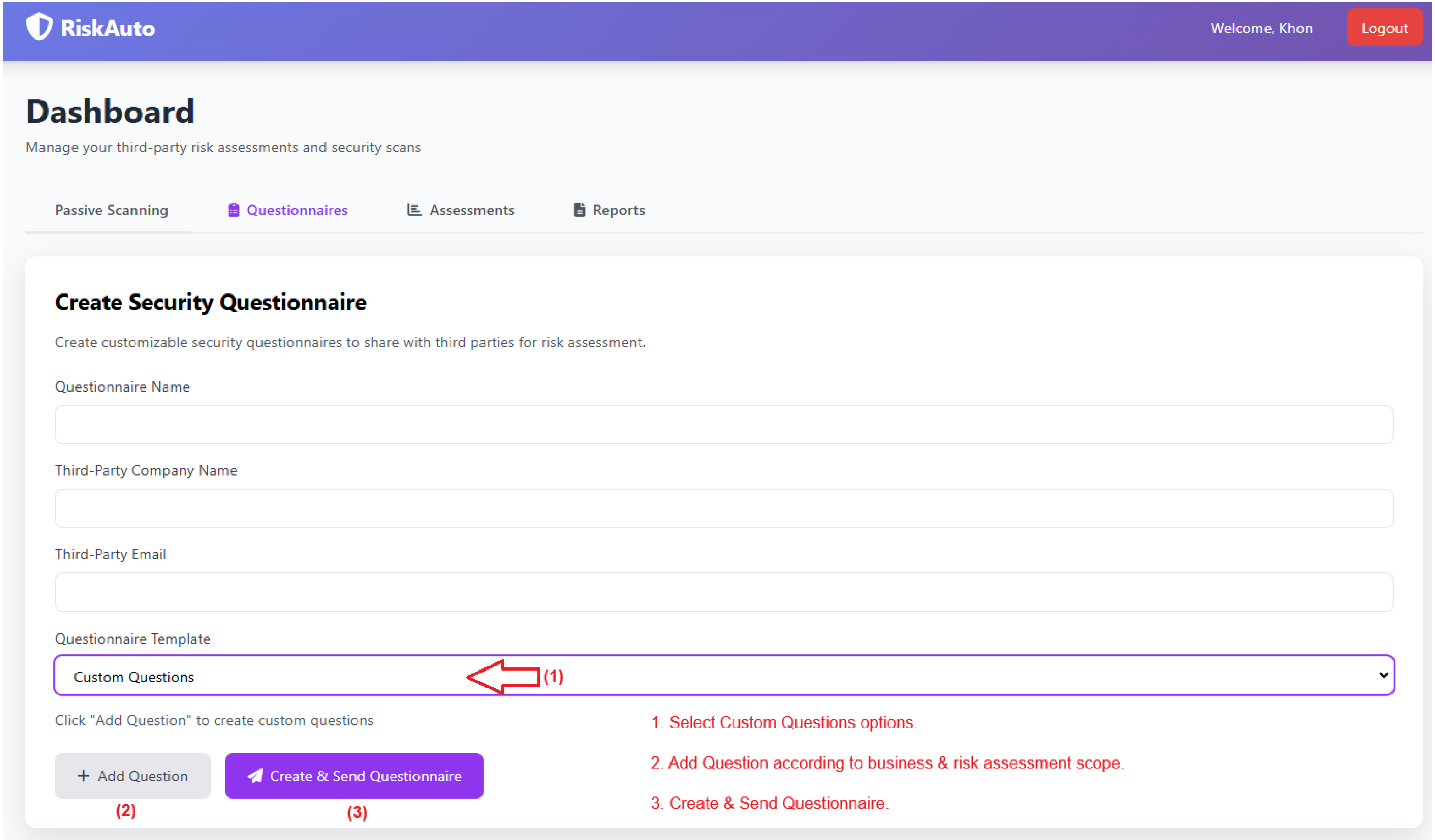
Are regular security audits conducted? Compliance MEDIUM

Do you maintain data backups with tested recovery procedures? Business Continuity HIGH

Sent Questionnaires

No questionnaires sent yet

Custom Questions



Dashboard

Manage your third-party risk assessments and security scans

Create Security Questionnaire

Create customizable security questionnaires to share with third parties for risk assessment.

Questionnaire Name

Third-Party Company Name

Third-Party Email

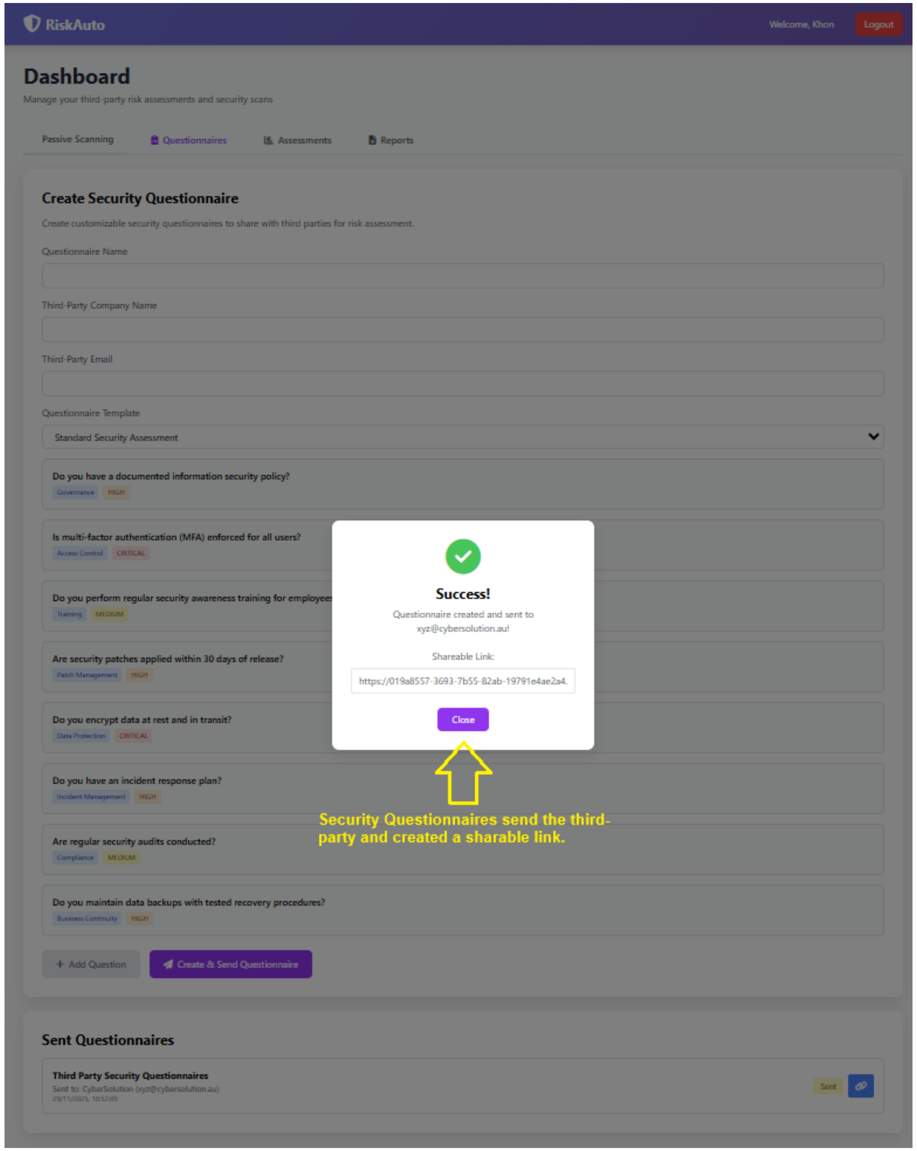
Questionnaire Template: Custom Questions (1)

Click "Add Question" to create custom questions

1. Select Custom Questions options.
2. Add Question according to business & risk assessment scope.
3. Create & Send Questionnaire.

Questionnaires Sent Notification:

- Questionnaires can be sent to the vendor’s email.
- A sharable link also generated.



Dashboard

Manage your third-party risk assessments and security scans

Create Security Questionnaire

Create customizable security questionnaires to share with third parties for risk assessment.

Questionnaire Name

Third-Party Company Name

Third-Party Email

Questionnaire Template: Standard Security Assessment

Do you have a documented information security policy?

Is multi-factor authentication (MFA) enforced for all users?

Do you perform regular security awareness training for employees

Are security patches applied within 30 days of release?

Do you encrypt data at rest and in transit?

Do you have an incident response plan?

Are regular security audits conducted?

Do you maintain data backups with tested recovery procedures?

Success!

Questionnaire created and sent to xyz@cybersolution.au!

Shareable Link:

https://019a8557-3693-7b55-82ab-19791e4ae2a4.

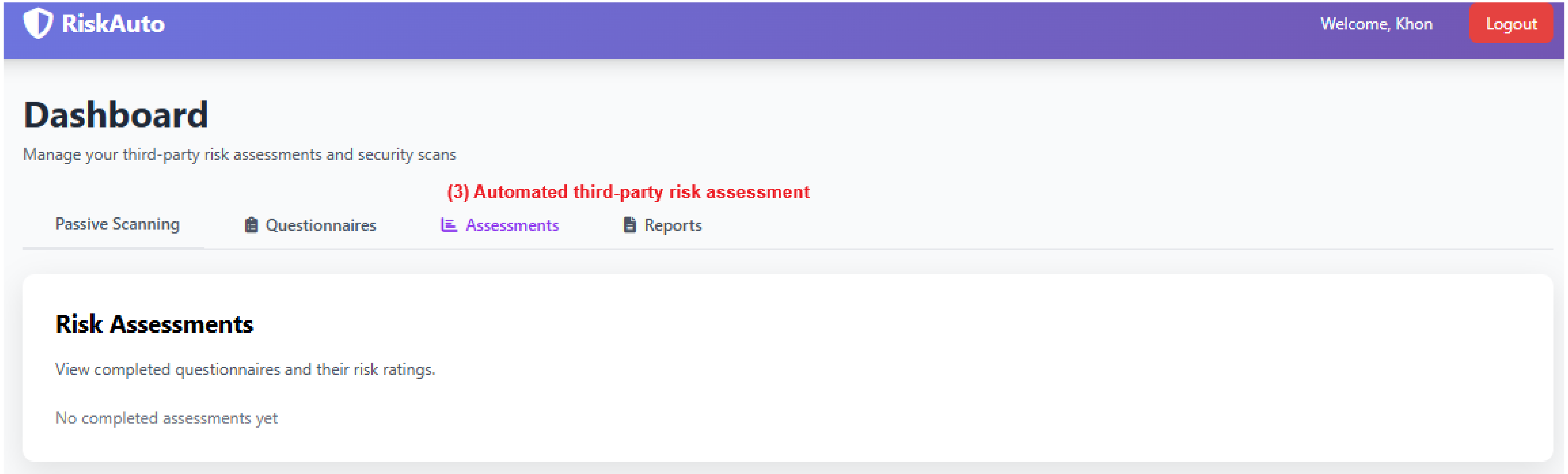
Security Questionnaires send the third-party and created a sharable link.

Sent Questionnaires

Third Party Security Questionnaires
Sent to: CyberSolution (xyz@cybersolution.au)
29/11/2025, 10:52:09

3. Assessments

- Select Assessments tab for the risk assessment.



Dashboard

Manage your third-party risk assessments and security scans

(3) Automated third-party risk assessment

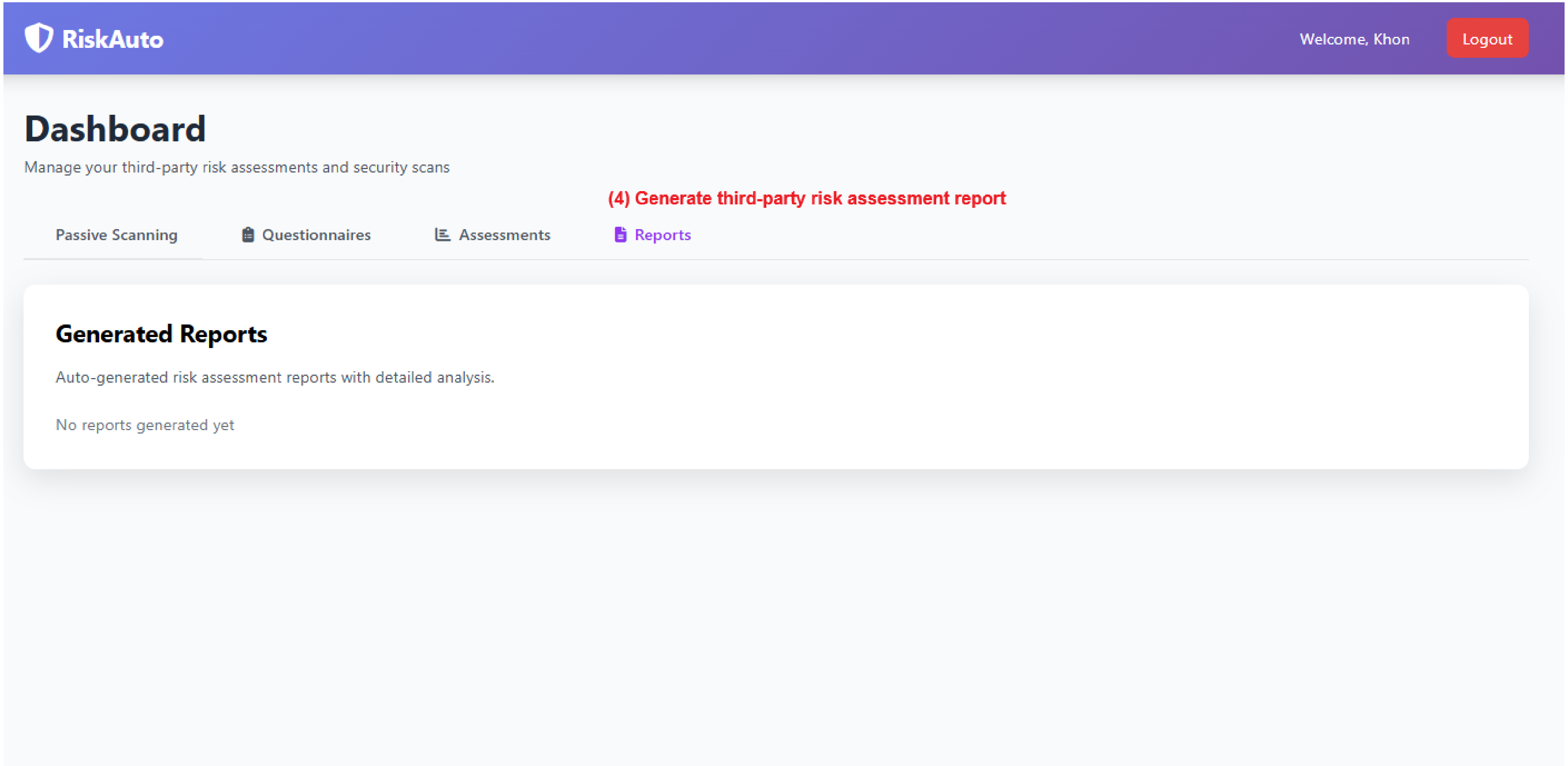
Risk Assessments

View completed questionnaires and their risk ratings.

No completed assessments yet

4. Reports

- Based on the security answers from third-party, the risk assessment report will be generated.



Dashboard

Manage your third-party risk assessments and security scans

(4) Generate third-party risk assessment report

Generated Reports

Auto-generated risk assessment reports with detailed analysis.

No reports generated yet