University of Southampton

Cybersecurity Southampton

A Methodology for Cybersecurity Risk Assessment in Supply Chains

CPS4CIP: **Cyber-Physical Security for Critical Infrastructures Protection**

28th of September 2023

betul.gokkaya@soton.ac.uk

Betul GOKKAYA, Leonardo ANIELLO, Erisa KARAFILI, Basel HALAK

Content:

- Motivation and Contribution
- Methodology
- Implementation
- Evaluation
- Results

A Methodology for Cybersecurity Risk Assessment in Supply Chains

- ➢ Motivation and Contribution
- Methodology
- Implementation
- Evaluation
- Results

Motivation

Cyber Security Breaches Survey (2023) Highlights:

- **51%** of medium businesses perform security risk assessments
- **63%** of large businesses conduct these assessments

Supply Chain Risk Assessments:

- Only **27%** of medium businesses actively engage
- **55%** of large corporations participate

Main Challenges:

- **High cost** of risk assessment (cited by 50% of organizations)
- **Uncertainty** on what checks to perform (noted by 25% of organizations)

There is a clear **necessity** for a **free and readily available online tool** that is not only **cost-effective** but also provides **a systematic approach to assessing supply chain risks**.

Note: The survey was conducted with 2,263 UK businesses, 1,174 UK registered charities and 554 education institutions from 27 September 2022 to 18 January 2023.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

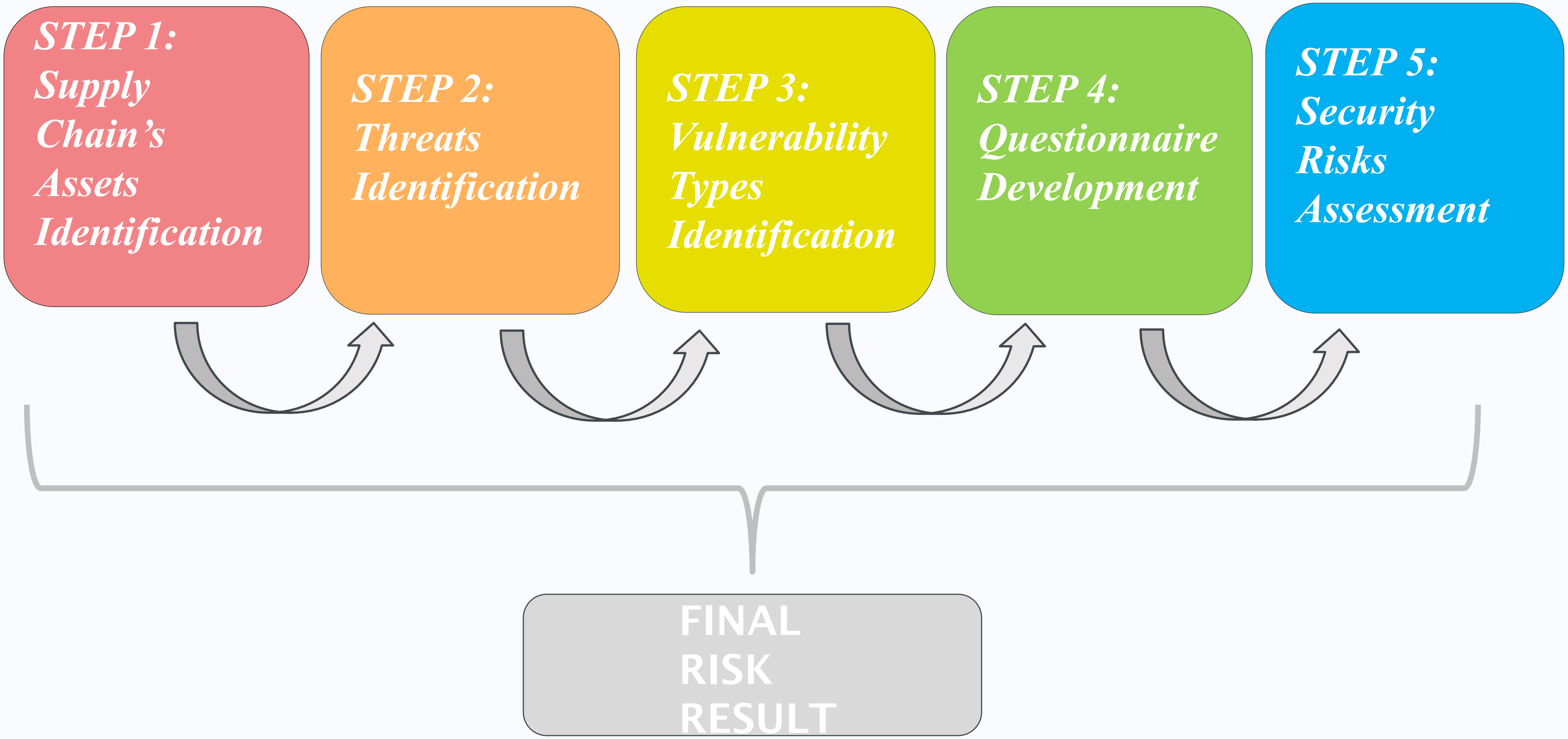
Contribution

1. Addressing the existing needs of supply chain risks in cybersecurity, we've developed a free, online tool offering a systematic approach to analyzing supply chain risks.
2. The research foundation of the proposed tool identifies 9 distinct security threats and 37 relevant vulnerabilities directly linked to supply chain risk. The tool includes 164 carefully crafted questions that cover all potential threats and vulnerabilities.

A Methodology for Cybersecurity Risk Assessment in Supply Chains

- Motivation and Contribution
- ➢ Methodology
- Implementation
- Evaluation
- Results

Methodology



STEP 1: Supply Chain’s Assets Identification

STEP 2: Threats Identification

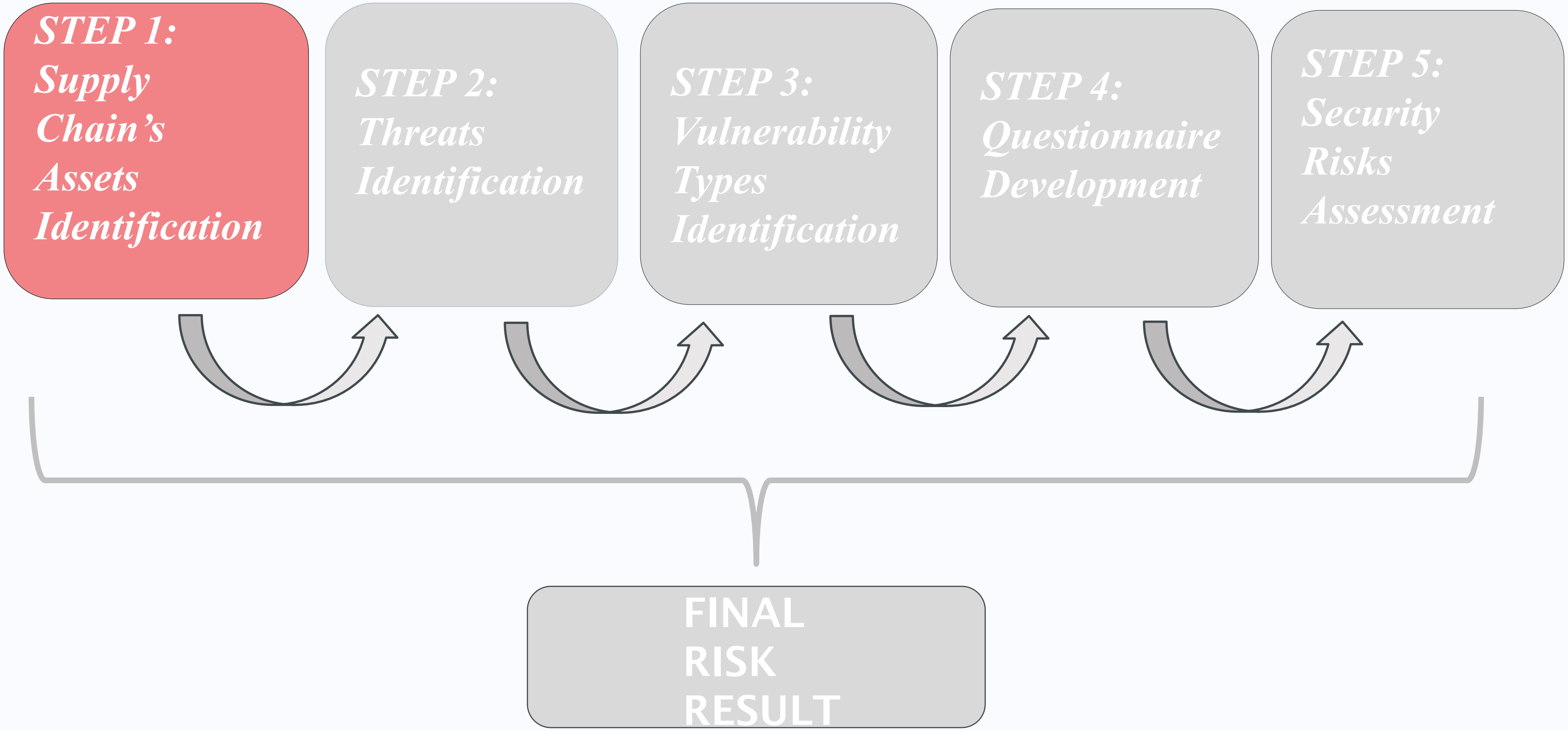
STEP 3: Vulnerability Types Identification

STEP 4: Questionnaire Development

STEP 5: Security Risks Assessment

FINAL RISK RESULT

Methodology



STEP 1: Supply Chain's Assets Identification

STEP 2: Threats Identification

STEP 3: Vulnerability Types Identification

STEP 4: Questionnaire Development

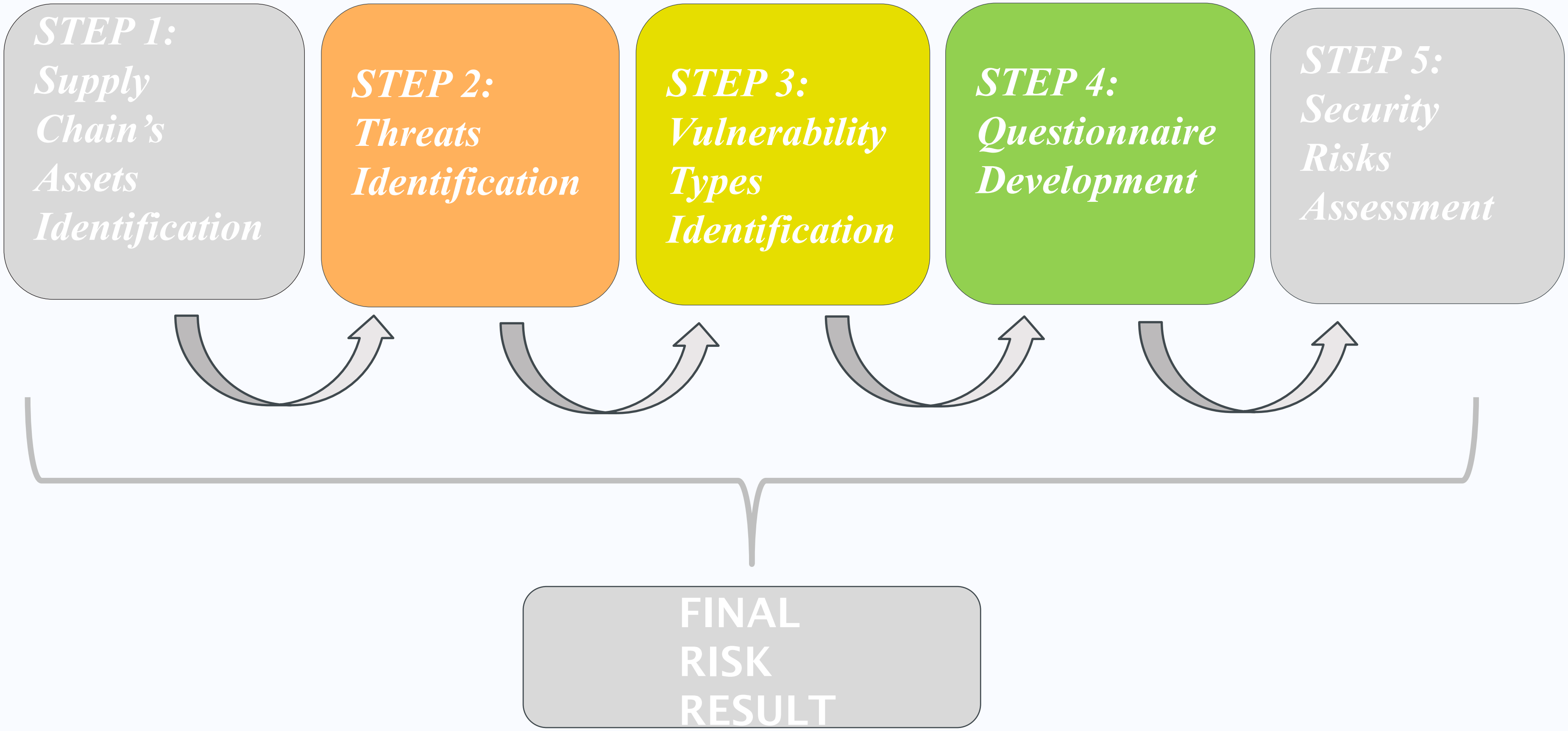
STEP 5: Security Risks Assessment

FINAL RISK RESULT

Methodology

- Hardware Assets
  - *User Electronics*
  - *Organizational Hardware*
  - *Internet of Things (IoT) Devices*
- Software Assets
  - *Third-party software*
  - *Organizational Software*
- User Assets
  - Internal User
  - External User

Methodology



STEP 1: Supply Chain's Assets Identification

STEP 2: Threats Identification

STEP 3: Vulnerability Types Identification

STEP 4: Questionnaire Development

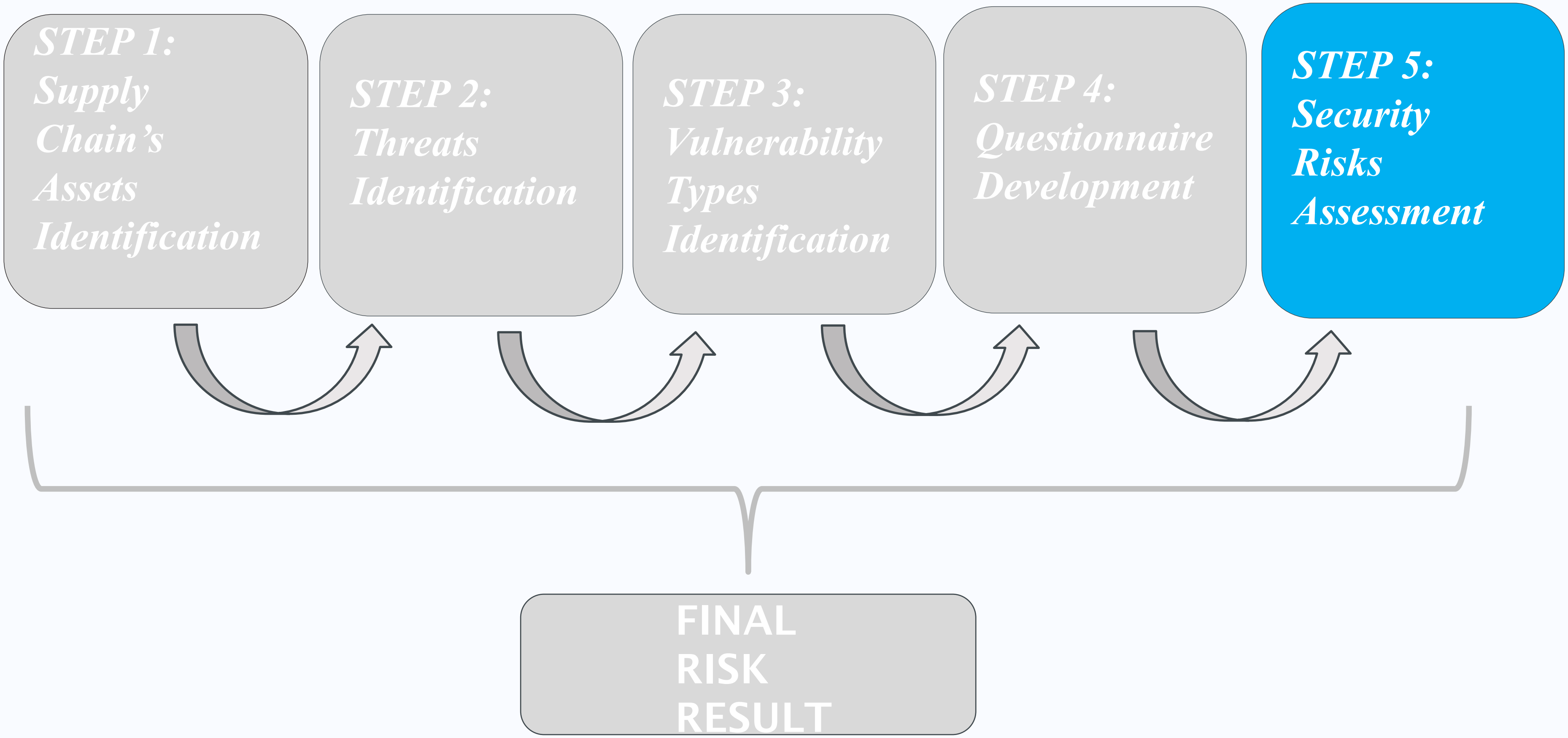
STEP 5: Security Risks Assessment

FINAL RISK RESULT

Methodology

- The research foundation of the proposed tool identifies **9 distinct security threats** and **37 relevant vulnerabilities** directly linked to **supply chain risk**.
- The tool includes 164 carefully crafted questions that cover all potential threats and vulnerabilities. It is a comprehensive resource for organizations to strengthen their supply chain risk assessments and security strategies.
- For each relevant asset sub-type a, questions are included to obtain estimates about
  - The likelihood of a presenting a vulnerability; **(e.g., How likely is it that your organization would lack a secure update mechanism for IoT devices?)**
  - The likelihood of a being targeted by a threat; **(e.g., How likely is it that a cyber actor could compromise IoT devices used for tracking goods in your supply chain, potentially leading to inaccurate data or loss of visibility?)**
  - The impact of a being targeted by a threat; **(e.g., If a cyber actor successfully compromises IoT devices used for tracking goods in your supply chain, how significant would the potential impact on your organization's ability to manage its supply chain effectively?**)

Methodology



STEP 1: Supply Chain’s Assets Identification

STEP 2: Threats Identification

STEP 3: Vulnerability Types Identification

STEP 4: Questionnaire Development

STEP 5: Security Risks Assessment

FINAL RISK RESULT

Methodology

Security Risks Assessment

Risk = (Vuln_likelihood ● Threat_likelihood) ● Impact

The scale we use and the values and labels associated to each rating are defined as follows:

– very low (value: 1, label: VL)
– low (value: 2, label: L)
– medium (value: 3, label: M)
– high (value: 4, label: H)
– very high (value: 5, label: VH)

Table 1. Semantics of the ● operation.

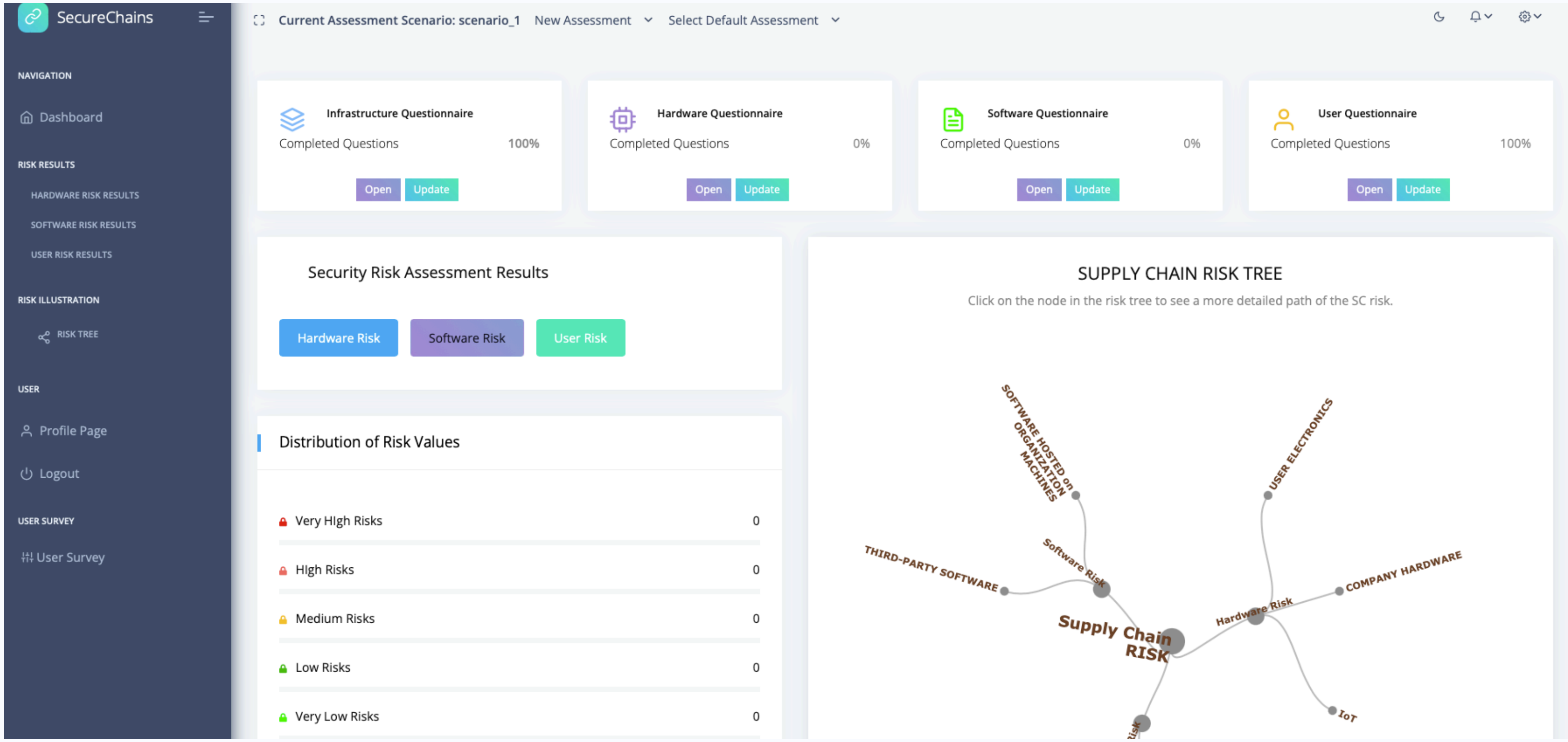
VH	M	H	H	VH	VH
H	L	M	M	H	VH
M	L	M	M	M	H
L	VL	L	M	M	H
VL	VL	VL	L	L	M
	VL	L	M	H	VH

A Methodology for Cybersecurity Risk Assessment in Supply Chains

- Motivation and Contribution
- Methodology
- ➢ Implementation
- Evaluation
- Results

Implementation

https://www.securechains.co.uk



Current Assessment Scenario: scenario_1

Infrastructure Questionnaire	Completed Questions	100%
Hardware Questionnaire	Completed Questions	0%
Software Questionnaire	Completed Questions	0%
User Questionnaire	Completed Questions	100%

Security Risk Assessment Results

SUPPLY CHAIN RISK TREE

Click on the node in the risk tree to see a more detailed path of the SC risk.

Distribution of Risk Values

Very HIgh Risks	0
HIgh Risks	0
Medium Risks	0
Low Risks	0
Very Low Risks	0

A Methodology for Cybersecurity Risk Assessment in Supply Chains

- Motivation and Contribution
- Methodology
- Implementation
- ➢ Evaluation
- Results

Evaluation

Method: Engaged cybersecurity experts with multi-year experience in risk assessments for companies.

Expert Panel

Expert #1: Chief of Cybersecurity, large UK institution, 10+ years experience

Expert #2: Consultant, large UK international enterprise, 5+ years in risk assessment

Expert #3: Specialist, small UK company, 20+ years in risk planning

Scenario Basis: Real-world supply chain cyberattacks, including the SolarWinds attack and the 'Big Hack' incident.

Note: Experts' identities and affiliations are confidential

Findings

Key Findings:

- **Average Score Deviation:** Up to 8% from the expert panel's average scores.
- **Likelihood Scores:** Closer to expert scores (5%) compared to impact scores (8%).

Highest Discrepancies:

- **Likelihood:**
  - **Company A:** Data and cloud breaches (13.4%)
  - **Company C:** Malicious third-party software (13.4%)
- **Impact:**
  - **Company A:**
    - Malicious third-party software (13.4%)
    - Cloud breaches (13.4%)
    - Data breaches (25%)
- **Overall Risk:**
  - **Company A:**
    - Malicious third-party software (25%)
    - Cloud breaches (13.4%)

A Methodology for Cybersecurity Risk Assessment in Supply Chains

- Motivation and Contribution
- Methodology
- Implementation
- Evaluation

➢ Results

Conclusion

Major alignment with expert judgments, showcasing the robustness of our methodology. Efficient risk assessment without detailed supplier and asset information.

Future Work

- **Extend the validation of the methodology:**
  - Involving a larger number of experts
  - Exploring different evaluation scenarios

- **Enhance the web-based tool:**
  - Improve the tool based on feedback
  - Increase the reliability of the scores generated by the tool

- **Integrate the tool with other existing risk assessment tools.**

- **Enable custom weighting for the impact of different assets:**
  - Allow organizations to tailor their risk assessments to their specific requirements and priorities.

YOUR QUESTIONS

Tool demo

Contact:
betul.gokkaya@soton.ac.uk