Intro

This survey contains a list of pre-screening questions to gauge the participant's eligibility to participate in a study to measure the usefulness of analysis materials for threat validation.

Eligible candidates will receive an invitation to participate in the paid study with a compensation of $100.

You can also get more information about the study by contacting k.tuma@vu.nl or w.mbaka@vu.nl
Click this link to access the full informed consent form.

By clicking next, you agree to participating in this pre-screening survey.

Concept understandability

First, we would like to gauge your knowledge on some of the basic concepts on software engineering and threat analysis

Which of the following best describes what a pseudocode is?

○ A detailed set of instructions written in a programming language that can be executed by a computer.

○ A high-level description of an algorithm or program, written in a format that resembles plain language, which is not intended to be executed.

○ A type of graphical representation used to illustrate the flow of a program, similar to a flowchart.

○ A specific programming language used primarily for developing quick prototypes of software applications.

Which of the following best describes what security threat analysis and risk assessment is?

○ Process of analyzing software performance and efficiency to optimize coding practices and reduce execution time.

○ Process of analyzing security threats to software performance and the risk they pose to application efficiency.

○ Process of identifying, evaluating, and prioritizing potential security threats and vulnerabilities to an organization, in order to implement appropriate measures to mitigate or manage the risks.

○ Process of identifying security threats in user interface design and assessing the risk they pose to user engagement.

Background

In this next part of the survey, you will be asked to answer questions on your background (professional and demographics) and on assessing security threats

What is your current role (professional occupation)?

○ System Administrator

○ Devops Engineer

○ Software Architect

○ Software Engineer

○ Product Manager

○ Quality Assurance/Tester

○ Security Manager

○ Other (Please specify)

How long have you been working in this role?

○ Less than a year

○ 1- 5 years

○ 6 - 10 years

○ 10 - 20 years

○ More than 20 years (Please specify)

What gender do you identify with?

○ Male

○ Female

○ Non-binary

○ Prefer not to say

What is your Nationality? Choose the country that coincides with your ethnic/cultural background

Experience with secure design techniques

Thank you for answering the questions so far. In this next phase, we are going to ask you questions on your experience with cybersecurity risk assessment

Do you have experience assessing security risks in a software project?

○ I do not have any experience assessing security risks in a software project

○ I have attended some sessions where security risks were assessed and discussed, but only as a spectator (did not contribute)

○ I have attended and contributed in some sessions where security risks were assessed and discussed

○ Assessing security risks of software projects is part of my professional tasks (I do it frequently)

○ Assessing security risks of software projects my job description (I do it everyday)

Do you participate in security practices at your organization?

○ Yes

○ No

In which of the following secure activities do you participate in? and how frequently? (Multiple answers allowed)

	Never	Rarely	Sometimes	Often	Always
Security requirements engineering	□	□	□	□	□
Threat Modeling and Design Review	□	□	□	□	□
Static Analysis	□	□	□	□	□
Security Testing and Code Review	□	□	□	□	□

	Never	Rarely	Sometimes	Often	Always
Security Assessment and Secure Configuration	□	□	□	□	□
Use dynamic monitoring tools (e.g., for monitoring network traffic)	□	□	□	□	□
Other (please specify)	□	□	□	□	□

Have you ever participated in a threat modeling sessions?

○ Yes

○ No

In which stage of the secure SDLC process did you participate? (Multiple answers allowed)

□ Risk Assessment

□ Threat Modeling and Design Review

□ Static Analysis

□ Security Testing and Code Review

□ Security Assessment and Secure Configuration

□ Use dynamic monitoring tools (e.g., for monitoring network traffic)

□ Other (please specify)

While participating in the threat modeling session(s), which technique was used? (You can choose more than one answers)

□ TARA

□ CORAS

□ STRIDE

□ NIST

□ OCTAVE

□ Attack trees

□ In-house adoptation

□ Other (please specify)

During the threat analysis and risk assessment sessions, what was being prioritised?

○ Asset identification

○ Threat scenarios/description

○ Impact rating and attack feasibility

○ Risk assessment (impact x feasibility)

○ Recommending appropriate mitigations

○ Other (please specify)

What was the most challenging part of assessing security risks of a software project/system?

○ Defining the scope of the analysis

○ Determining the abstraction level of the representation of the system (DFD, Component diagram, e.t.c)

○ Manual resources spent on discussing threats

○ Precision- identifying threats correctly

○ Identifying and discussing all possible threats

○ Definition of done (when to consider the the task-assessing security risks- as complete)

○ Other (please specify)

Exp object experience

In this last phase of the survey, you will be asked questions based on the core concepts of the study

Do you have any experience working with cloud deployment platforms like Kubernetes, AWS?

○ None- I do not have any experience working with cloud deployment platforms

○ Beginner- I have a certification on cloud deployment platforms (attended a course with hands-on experience)

○ Intermediate- I have some experience with cloud deployment platforms (I have used it before/ use it infrequently in my professional capacity)

○ Advanced- I have substantial experience with cloud deployment platforms (I use them regularly as additional resources in my professional role)

○ Expert- I possess extensive expertise in cloud deployment platforms (I use them on a daily basis in my professional duties)

Do you have any experience working with GitHub?

○ None- I do not have any experience working with GitHub

○ Beginner- I have a certification on GitHub (attended a course with hands-on experience)

○ Intermediate- I have some experience with GitHub (I have used it before/ use it infrequently in my professional capacity)

○ Advanced- I have substantial experience with GitHub (I use them regularly as additional resources in my professional role)

○ Expert- I possess extensive expertise in GitHub (I use them on a daily basis in my professional duties)

How often do you use Large language Models (e.g., chatGPT, Bard)?

○ Never

○ Daily basis

○ Couple of times a week

○ Couple of times a month

○ Other (Please specify)

What do you use Large Language Models for? (multiple answers alllowed)

□ Writing code

□ Debugging code

□ Writing reports

□ Writing emails

□ Other (Please specify)

think-aloud

Are you willing to participate in a think-aloud study, where you will be asked to voice your thoughts as you are carrying out a security threat validation task?

○ Yes

○ No

Invite to survey

Thank you for your participation. If you are eligible, we would like to invite you to participate in the paid survey. Kindly leave your personal email address below. We will contact you with details (zoom link, date and time)

Here is an example of the task to be expected during the actual study.

You will receive a scenario (two in total), and ten security threats to each scenario. Each threat contains a threat description, assumption(s), STRIDE threat type (that will be compromised if the threat is realistic), and affected data flow diagram components, as can be seen below. You will then be asked to assess the correctness of each threat. That is, mark each threat as either realistic (likely to occur) or bogus (unlikely to occur).

> **Scenario: updating a remote repository on GitHub**
>
> **Threat description: Exploit a vulnerability in the code in the remote repository to attack the server running the code.**
>
> **Assumptions: Remote repository and running server reachable by the attacker. The source code has security vulnerabilities.**
>
> **STRIDE threat type: Information disclosure**
>
> **Affected DFD components: Victim’s server**