Config SAST User Study

1. How many years of software development experience (writing code) do you have?

   Mark only one oval.

   ○ 0 – 2
   ○ 3 – 5
   ○ 6 – 9
   ○ 10+

2. What is your experience with security vulnerabilities?

   Mark only one oval.

   ○ No experience at all
   ○ I am beginner
   ○ I am knowledgeable in the topic
   ○ I am an expert

3. Have you ever attended a training on secure software development?

   Mark only one oval.

   ○ Yes
   ○ No

4. If yes, which topics/areas did you cover?

____

____

____

____

____

Section 2: SAST Tools

The questions in this section are related to your experience with Static Application Security Testing (SAST) tools that analyze source code to find security vulnerabilities. For example, Checkmarx, SonarQube, FindBugs, CheckStyle, etc.

5. Do you use SAST tools in your everyday workflow?

Mark only one oval.

○ Yes

○ No

6. If yes, which tools?

____

____

____

____

____

7. How often do you use these tools?

Check all that apply.

□ Before each commit
□ When a new functionallity is implemented
□ On milestones (e.g. new release)

□ Other: ________________________

8. Do you use the SAST tools or integrated SAST features within your IDE?

Mark only one oval.

○ Yes

○ No

9. If yes, which tools or features?

____

10. Do you configure the tools?

Mark only one oval.

○ Yes

○ No

11. List the top 3 configuration options that you like.

____

____

____

____

____

12. List the top 3 configuration options that you dislike.

____

____

____

____

____

13. Have you used any Domain Specific Languages (DSL) to adapt the existing rules in a tool you used?

Mark only one oval.

○ Yes

○ No

14. If yes, for which tool(s)?

____

15. How would you describe the experience?

____

____

____

____

____

16. How confident are you when you adapt the existing rules?

Mark only one oval.

	1	2	3	4	5	
not at all	○	○	○	○	○	very confident

17. Have you written new rules in the DSL?

Mark only one oval.

○ Yes

○ No

18. If yes, for which rules or what kind of rules?

19. How confident you are when you write new rules?

Mark only one oval.

	1	2	3	4	5	
not at all	○	○	○	○	○	very confident

20. Are there any processes, polices, and/or regulations for using SAST in your company?

Mark only one oval.

○ Yes

○ No

21. If yes, what processes, policies and/or regulations are in place?

22. Are you allowed to configure the rules of the SAST tools used in your company?

Mark only one oval.

○ Yes

○ No

23. Who is allowed to configure the rules of the SAST tools?

____

24. For each statement, please rate how relevant it is on a scale from 1 to 5.

Mark only one oval per row.

	1 - not at all	2	3	4	5 - highly relevant
The issues reported by the tool should be available immediately (fast analysis).	○	○	○	○	○
The issues reported by the tool should be easy to understand.	○	○	○	○	○
The issues reported by the tool should be relevant for me (the context I am currently focused on).	○	○	○	○	○
The issues reported by the tool should be grouped according to my preferences.	○	○	○	○	○
The tool should have continuous reporting. (reports individual issues as soon as they are found)	○	○	○	○	○

25. When should the analysis run?

Check all that apply.

- □ Automatically, on file save.
- □ Automatically, on file change.
- □ Automatically, on project build.
- □ Automatically, on commit to “main” branch.
- □ Manually

Section 3: SecuCheck Feedback

The questions in this section are related to your experience using SecuCheck.

26. On what level would you prefer the entry points selection option to be?

Mark only one oval.

○ Method level

○ Class level

○ Package level

○ Other: ______________________

Discussion Question 1: What did you like or didn't like? What changes and improvements should be made?

Discussion Question 2: Are there any options you miss or that you would like to see? Additional things you would want to configure? For example, algorithm, output format, timeout, etc.

27. Is configuring the analysis in the browser ideal?

Mark only one oval.

○ Yes

○ No

Discussion Question 3: Would you prefer an alternate configuration approach?

28. Where should the notifications from the tool be shown?

Mark only one oval.

○ IDE

○ Configuration Page

Section 4: Tool 1 Configuration Options

Read the configuration options available in a commercial SAST tools (Tool 1) and evaluate if they are understandable and useful. These are options used to configure different properties of the SAST tools, similar to the configurations performed for SecuCheck.

[F1] filter

Apply a filter using a filter file

[F2] disablesource-bundling

Exclude source files from the FPR file

[F3] disable-language

To disable specific languages.

[F4] analyzers

To disable specific analyzers, include this option at scan time with a colon- or comma-separated list of analyzers you want to enable. The full list of analyzers is: buffer, content, configuration, controlflow, dataflow, findbugs, nullptr, semantic, and structural.

[F5] incremental-base

Specifies that this is the initial full scan of a project for which you plan to run subsequent incremental scans. Use this option for the first scan when you plan to run subsequent scans on the same project with the incremental option

29. F1-F5 Options

Check all that apply.

	Understandable	Useful
F1	□	□
F2	□	□
F3	□	□
F4	□	□
F5	□	□

[F6] no-default-issue-rules

Disables rules in default Rulepacks that lead directly to issues. Still loads rules that characterize the behavior of functions. Note: This is equivalent to disabling the following rule types: DataflowSink, Semantic, Controlflow, Structural, Configuration, Content, Statistical, Internal, and Characterization:Issue.

[F7] no-default-rules

Specifies not to load rules from the default Rulepacks.

[F8] no-default-sink-rules

Disables sink rules in the default Rulepacks.

[F9] rules

Specifies a custom Rulepack or directory. You can use this option multiple times to specify multiple Rulepack files. If you specify a directory, includes all of the files in the directory with the .bin and .xml extensions.

[F10] EnableInterproceduralConstantResolution

Use constant resolution.

30. F6-F10 Options

Check all that apply.

	Understandable	Useful
F6	□	□
F7	□	□
F8	□	□
F9	□	□
F10	□	□

[F11] DataflowMaxFunctionTimeMinutes

Set a threshold to limit the dataflow analysis time of a single function.

[F12] MaxFunctionVisits
Set a threshold for the number of times a function is analyzed.

[F13] MaxTaintDefForVar
dimensionless value expressing the complexity of a function

[F14] MaxTaintDefForVarAbort
the upper bound for MaxTaintDefForVar

[F15] MaxChainDepth
Set a threshold for depth of functions chain.

31. F11-F15

Check all that apply.

	Understandable	Useful
F11	□	□
F12	□	□
F13	□	□
F14	□	□
F15	□	□

[F16] alias.EnableInterprocedural
Enable interprocedural alias analysis.

[F17] MaxFieldDepth
Set a threshold for the depth of the analyzed fields.

[F18] MaxPaths
Set a threshold for the number of analyzed paths.

32. F16-F18 Options

Check all that apply.

	Understandable	Useful
F16	□	□
F17	□	□
F18	□	□

Section 4: Tool 2 Configuration Options

Read the configuration options available in a commercial SAST tools (Tool 2) and evaluate if they are understandable and useful. These are options used to configure different properties of the SAST tools, similar to the configurations performed for SecuCheck.

[C1] EXCLUDE_PATH
Semicolon separated list of file names to exclude from the scan (e.g. file1;file2;file3). Include only file names, not paths.

[C2] MAX_QUERY_TIME
Defines part of a formula to calculate the maximum execution time allowed for a single query. After the set time, the query execution is terminated, the result is empty and the log indicates that its execution failed.

[C3] USE_ROSLYN_PARSER
Enable the use of Roslyn parser to scan C# files.

[C4] LANGUAGE_THRESHOLD
Sub-setting of MULTI_LANGUAGE_MODE. The minimal percentage of complete number of files required to scan a language. Should be set to 0.0 (and MULTI_LANGUAGE_MODE=2) to match the Portal_s Multi-language mode. See MULTI_LANGUAGE_MODE parameter for more details.

[C5] MULTI_LANGUAGE_MODE
Defines which languages the application should scan. 1 = One Primary Language, 2 = All Languages, 3 = Matching Sets, 4 = Selected Languages.

33. C1-C5 Options

Check all that apply.

	Understandable	Useful
C1	□	□
C2	□	□
C3	□	□
C4	□	□
C5	□	□

[C6] SCAN_BINARIES
Whether or not to scan binary files (only available for .jar files – Java – and for .dll files – C#). *Note*: Requires Java to be installed on the machine.

[C7] SUPPORTED_LANGUAGES
Sub-setting of MULTI_LANGUAGE_MODE. If MULTI_LANGUAGE_MODE = 1 or 2 ignore/meaningless. If MULTI_LANGUAGE_MODE = 4 then languages are separated by commas. See MULTI_LANGUAGE_MODE parameter for more details.

[C8] TYPES_TO_DECOMPILE
When SCAN_BINARIES is set to true, this flag should be used to specify which packages/namespaces should be decompiled and then included in the scan. Format x.y.* can be used to specify that all the types under package/namespace x.y should be decompiled and scanned. The list of packages/namespaces should be separated by a semicolon (;).

[C9] MAXFILESIZEKB
Files exceeding the set size (in KB) will not be scanned.

[C10] MAX_PATH_LENGTH
Defines the maximum amount of flow elements allowed in an influence flow calculation. Paths with length exceeding this number are ignored.

[C11] MAX_QUERY_TIME_PER_100K
Sub setting of MAX_QUERY_TIME. Defines part of formula to calculate the maximum execution time allowed for a single query. See MAX_QUERY_TIME parameter for more details.

34. C6-C11 Options

Check all that apply.

	Understandable	Useful
C6	□	□
C7	□	□
C8	□	□
C9	□	□
C10	□	□
C11	□	□