

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Lint

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: CI

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

- Yes
- No

If yes, which tools or features?

Lint

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

Checkstyle

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

KTLint

How would you describe the experience?

Good and easy to use. You apply your config directly in an editor file (IntelliJ).

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all



very confident

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

Yes

No

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

Quality Gate regulations on Sonarqube

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

Yes

No

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

Lead Developer / Architects

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: Why not everything

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CogniCrypt

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

CogniCrypt

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

I have only tested the tool.

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all



very confident

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

Yes

No

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

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

Yes

No

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

At the moment every developer in our team

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input type="checkbox"/>	<input type="checkbox"/>
F8	<input type="checkbox"/>	<input type="checkbox"/>
F9	<input type="checkbox"/>	<input type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
 - When a new functionality is implemented
 - On milestones (e.g. new release)
 - Other: Randomly
-

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

- Yes
- No

If yes, which tools or features?

CogniCrypt

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

1

2

3

4

5

not at all



very confident

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

Yes

No

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

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

Yes

No

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

Everybody

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Secure Software Engineering, Cryptography, Static Code Analysis

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CogniCrypt

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: Comparison of static analysis tools

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

- Yes
- No

If yes, which tools or features?

CogniCrypt_SAST and CogniCrypt_Gen

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

Introducing rules

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

CogniCrypt - CrySL (DSL)

How would you describe the experience?

Straight forward

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

Rule for proper use of cryptographic API, e.g. Cipher

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
 - When a new functionality is implemented
 - On milestones (e.g. new release)
 - Other: I never used a SAST Tool before
-

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

- Yes
- No

If yes, which tools or features?

I never used a SAST Tool before

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

I never used a SAST Tool before

List the top 3 configuration options that you dislike.

I never used a SAST Tool before

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

Yes

No

If yes, for which tool(s)?

I never used a DSL Tool before

How would you describe the experience?

I never used a DSL Tool before

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

I never used a DSL Tool before

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

We don't have a policy but theoretically we are allowed to use it

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

Yes

No

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

The Developers

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

CogniCrypt

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Java Crypto API misuses (JCA)

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CogniCrypt

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: at least one time

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

- Yes
- No

If yes, which tools or features?

detection of crypto API misuses

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

Yes

No

If yes, for which tool(s)?

CogniCrypt (CrySL rules)

How would you describe the experience?

good

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

I wrote rules for EC encryption

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

How confident are you when you adapt the existing rules?



Have you written new rules in the DSL?

- Yes
 No

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

How confident you are when you write new rules?



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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

CogiCrypt

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

1

2

3

4

5

not at all



very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

1

2

3

4

5

not at all



very confident

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

- Yes
- No

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

Cognicrypt used for developing new features that could potentially involve security vulnerabilities

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

- Yes
- No

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

product management, senior software engineers

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Software attacks (Man In the Middle, Denial of Service, etc), Memory/Buffer overflows, Misuse of cryptography

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

CogniCrypt

How would you describe the experience?

Used it in eclipse IDE. It works good and finds out the misuses of cryptographic API used in Java.

How confident are you when you adapt the existing rules?



Have you written new rules in the DSL?

- Yes
- No

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

CrySL rules for few Bouncy Castle API in Java

How confident you are when you write new rules?



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

- Yes
- No

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

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

- Yes
- No

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

Developer using the tools

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Secure coding and analysis; vulnerability checks

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Checkstyle, SonarQube (previously used), Findbugs

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

SonarLint

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

Ensure that state-of-art tools are used

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

Yes

No

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

Team but it must be logged who performed the changes

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Topics of Eric's Secure Software Engineering Lectures (a bit extended to fit industrial purposes)

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Sonarlint, Checkstyle

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: During Coding

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

- Yes
- No

If yes, which tools or features?

Sonarlint, Checkstyle

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

1. Turn on/off rules that fit or don't fit my style / use case. 2. Add "xyz" as rule (like turn a coding pattern into a rule) 3.

List the top 3 configuration options that you dislike.

In checkstyle especially the configuration format - I believe it's xml...

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

Everybody

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: Class or Package level, depending on project size

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

soot

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: I only use them when needed

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

-cp

List the top 3 configuration options that you dislike.

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input type="checkbox"/>	<input type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Encryption

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CheckStyle and Findbugs, OWASP Dependency Checker

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

.....

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

Build is broken when dependency problems are found (OWASP), use identical code format (CheckStyle),
.....

List the top 3 configuration options that you dislike.

OWASP - too easy to suppress the OWASP findings. This is done globally - no finding that stops the process.
.....

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

Yes

No

If yes, for which tool(s)?

.....

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

Build pipeline - development, QA, and production stages. Program doesn't move to next phase when there are findings

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

Yes

No

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

All developers - developers sit together and decide how the security check should be implemented.

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input type="checkbox"/>	<input type="checkbox"/>
C3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

None so far

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

ISO 27000, Threat Modeling, Defensive Coding, DevOps

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CogniCrypt, Roslyn

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: While Coding

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

- Yes
- No

If yes, which tools or features?

Roslyn

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

Suppressing, Severity changing

List the top 3 configuration options that you dislike.

idk,

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

Some knowledge in general DSLs

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

.....

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

Yes

No

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

prob. anyone

.....

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: Class and/or package.

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Secure web development

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CheckStyle, FindBugs, SonarQube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: after each commit

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

- Yes
- No

If yes, which tools or features?

CheckStyle and FundBugs

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

Mark things as hints and not errors. Rules not enforced but presented as hints.

List the top 3 configuration options that you dislike.

Too many options configure

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

SonarQube - company supplied rule set

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

- Yes
- No

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

SonarQube - cannot be changed. But for other tools it's possible

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Security Champion Training offered by Fraunhofer

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

SonarQube Scan

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: integrated in CI/QA

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

- Yes
- No

If yes, which tools or features?

OWASP Dependency Check

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

Recommendations - every team should have security champion and a belt. PenTest, integrating security and SAST tools in the pipeline.

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

Yes

No

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

Every team is responsible for this

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: Possible to select all combinations

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Security Champion program taught by Fraunhofer

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Sonarqube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

Everybody who is part of the DevOps team and showing interest in doing that.

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

SSE and DeCA

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Soot

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

E.g. SAST of IntelliJ IDEA

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

Null assertions, type casts, if conditions

List the top 3 configuration options that you dislike.

Hints for members that could be private

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

basic sonar qube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

lead dev / architect / it-ops

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: hierarchical starting at package level

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Crypto, Hashing, PKI, Symmetric and asymmetric crypto

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

SonarQube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

lint rules

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

SonarQube for each project, basic set of rules

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

- Yes
- No

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

The team of developers

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Secure Design, Security vulnerabilities, OWASP, tools for finding vulnerabilities, laws/regulations, secure code

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

FindBugs and SonarQube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

SonarQube - choose which checks should be execute, easily apply them, apply to all projects, inheritance of rulesets that can be used

List the top 3 configuration options that you dislike.

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

Policies require automatically using SAST tools during the build process

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

- Yes
- No

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

All development team members

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all



very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

-
- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input type="checkbox"/>	<input type="checkbox"/>
F8	<input type="checkbox"/>	<input type="checkbox"/>
F9	<input type="checkbox"/>	<input type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Secure Software Engineering, Designing code analyses for large-scale software systems

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

CogniCrypt, SecuCheck

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: For research purposes

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

- Yes
- No

If yes, which tools or features?

CogniCrypt, SecuCheck

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

1. Choosing the desired crypto API rulesets.
2. Choosing the desired version of these ruleset.
3. Choosing the checkbox option for provider detection analysis.

List the top 3 configuration options that you dislike.

-

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

Yes

No

If yes, for which tool(s)?

CogniCrypt, SecuCheck

How would you describe the experience?

CogniCrypt - it needs a little more time to learn the syntax on how the crypto API rules are done. But once I learned this, it was easier and convenient to specify the rules the way they are specified.

SecuCheck - I found it easier to understand the syntax faster and start with implementing the taint flow queries right away.

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

For CogniCrypt only. I have written a new ruleset called BouncyCastle-JCA and also updated and upgraded existing rules in the other ruleset in CogniCrypt.

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

-

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

- Yes
- No

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

Usually my supervisors.

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

General security overview (Lectures like SSE)

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

SonarQube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

SonarQube / SonarLint

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

False Positives, Temporal Suppression, Choosing specific analysis rules

List the top 3 configuration options that you dislike.

Configurations about unsure reports, Handling of Errors where the SAST misses information, current implementations of filter features

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

Yes

No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

A branch can't be merged, if there are too severe issues detected by the SAST

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

- Yes
- No

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

The leader of the project or somebody assigned to the configuration

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

SonarCube

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: I have previously used when a new functionality was implemented

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1 2 3 4 5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1 2 3 4 5

not at all

very confident

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

Yes

No

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

There is team specialized for finding vulnerabilities and everything that is tracked is brought back to the development teams.

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

Yes

No

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

The security department

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....
1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....
1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input type="checkbox"/>	<input type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

general IT Security / Secure Software Engineering

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

shellcheck, intellij integrated, checkstyle, ... depends on language

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other:

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

- Yes
- No

If yes, which tools or features?

intellij, shellcheck, checkstyle

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

-

List the top 3 configuration options that you dislike.

-

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

Yes

No

If yes, for which tool(s)?

-

How would you describe the experience?

-

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

-

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

ci integration with modified templates (breaking pipeline)

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

- Yes
- No

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

developers, team discussion

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

TLS, Basic C-style exploitation (buffer overflows, format...), Architectures, networking, encryption, useable security,

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other:

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

- Yes
- No

If yes, which tools or features?

Basic IntelliJ,

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

checkstyle

How would you describe the experience?

Somewhat works

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

Yes

No

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

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

Yes

No

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

Whoever is interested

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

1

2

3

4

5

not at all



very confident

Have you written new rules in the DSL?

Yes

No

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

1

2

3

4

5

not at all



very confident

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

Yes

No

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

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

Yes

No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input type="checkbox"/>	<input type="checkbox"/>
C9	<input type="checkbox"/>	<input type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
 - When a new functionality is implemented
 - On milestones (e.g. new release)
 - Other: NA
-

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1 2 3 4 5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1 2 3 4 5

not at all

very confident

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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Xanitizer

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: SAST Tool Developer / Vendor

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

Yes

No

List the top 3 configuration options that you like.

Analyzed Classes, Checked Problem Types/Vulnerabilities, Matched Patterns

List the top 3 configuration options that you dislike.

Start Methods

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

Yes

No

If yes, for which tool(s)?

Xanitizer

How would you describe the experience?

I prefer adapting with a GUI, but it can be handled this way, too.

How confident are you when you adapt the existing rules?



Have you written new rules in the DSL?

Yes

No

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

Added new problem types/vulnerability checks, enhanced existing checks

How confident you are when you write new rules?



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

- Yes
- No

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

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

- Yes
- No

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

Everybody, because we are the tool vendor

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input type="checkbox"/>	<input type="checkbox"/>
C5	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

basics, vulnerability of the day from owasp

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

findbugs, checkstyle (covero/ "google grammar"...)
.....

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other:

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

(code style - "self applied")

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Portswigger Burp, Coursera Security Software Development, Workshop at conferences OWASP, ...

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Findbugs

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: CI/CD Pipeline

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

Best practices / recommendations, we use SAST in our pentest if it is in scope or demanded

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

- Yes
- No

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

depends on the project, normally developers

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input type="checkbox"/>	<input type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C11	<input type="checkbox"/>	<input type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Security Champion Training

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

Contrast, SpotBugs

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: Code Reviews

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

How would you describe the experience?

.....

How confident are you when you adapt the existing rules?

1

2

3

4

5

not at all

very confident

Have you written new rules in the DSL?

Yes

No

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

.....

How confident you are when you write new rules?

1

2

3

4

5

not at all

very confident

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

- Yes
- No

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

SAST tools are integrated into build pipeline - fix reported problems are mark as FP

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

- Yes
- No

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

DevOps team

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

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)

When should the analysis run?

- 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.

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

- Method level
- Class level
- Package level
- Other: package and annotations

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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input type="checkbox"/>	<input type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input type="checkbox"/>	<input type="checkbox"/>
F17	<input type="checkbox"/>	<input type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms

Config SAST User Study

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

- 0 – 2
- 3 – 5
- 6 – 9
- 10+

What is your experience with security vulnerabilities?

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

Have you ever attended a training on secure software development?

- Yes
- No

If yes, which topics/areas did you cover?

Static Code Analysis

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.

Do you use SAST tools in your everyday workflow?

- Yes
- No

If yes, which tools?

How often do you use these tools?

- Before each commit
- When a new functionality is implemented
- On milestones (e.g. new release)
- Other: _____

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

- Yes
- No

If yes, which tools or features?

Do you configure the tools?

- Yes
- No

List the top 3 configuration options that you like.

List the top 3 configuration options that you dislike.

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

- Yes
- No

If yes, for which tool(s)?

CodeSharpenerCryptoAnalyzer

How would you describe the experience?

Not developer friendly as of now, as it still a prototype.

How confident are you when you adapt the existing rules?



Have you written new rules in the DSL?

Yes

No

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

CrySL Rules

How confident you are when you write new rules?



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

- Yes
- No

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

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

- Yes
- No

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

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

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)

When should the analysis run?

- 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.

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

- 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.

Is configuring the analysis in the browser ideal?

- Yes
- No

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

Where should the notifications from the tool be shown?

- 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] disable-source-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

F1-F5 Options

	Understandable	Useful
F1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F2	<input type="checkbox"/>	<input type="checkbox"/>
F3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F5	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[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.

F6-F10 Options

	Understandable	Useful
F6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
F9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

F11-F15

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.

F16-F18 Options

	Understandable	Useful
F16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

C1-C5 Options

	Understandable	Useful
C1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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.

C6-C11 Options

	Understandable	Useful
C6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
C7	<input type="checkbox"/>	<input type="checkbox"/>
C8	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C10	<input type="checkbox"/>	<input type="checkbox"/>
C11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Google Forms