CERT C Compliance

The Parasoft CERT C Compliance extension is a set of assets for your DTP infrastructure that enable you to demonstrate compliance with CERT C Coding Standard guidelines. The extension is shipped as part of the Security Compliance Pack for DTP 5.4.2. Contact your Parasoft representative to download and license the Security Compliance Pack.

In this section:

Background

The CERT C Coding Standard was developed by the CERT Coordination Center to improve the safety, reliability, and security of software systems. CERT coding standards consist of "rules" and "recommendations" and are organized into a set of categories. Rules provide code requirements for adhering to the standard, whereas recommendations are intended to provide guidance that improves the safety, reliability, and security of software systems.

Rules and recommendations are collectively referred to as "guidelines." Guidelines in the CERT C Secure Coding Standard are cross-referenced with Common Weakness Enumeration (CWE) entries. A programming pattern that fails to meet CWE's guidelines are called "weaknesses."

In terms of risk analysis, CERT uses three metrics to help quantify weaknesses:

- the *severity* of the consequences associated with a failure to comply with the rule
- the *likelihood* that a coding flaw introduced by ignoring the rule will result in an exploitable vulnerability
- the *remediation cost* associated with complying with the rule

The metrics are used to prioritize violations into three levels: L1 (highest priority), L2, and L3. The CERT C Compliance extension configures your DTP implementation to show static analysis violations according to their CERT C priority, guideline, type, and guideline category.

See https://wiki.sei.cmu.edu/confluence/display/c/Introduction to learn more about the standard.

Prerequisites

C/C++test 10.4.2 (desktop or plug-in edition) with the Flow Analysis license feature enabled. See Security Compliance Pack for DTP 5.4.2 for additional information.

Process Overview

1. Install the Security Compliance Pack for DTP 5.4.2 into DTP Extension Designer.
2. Deploy the CERT C Compliance artifact into your DTP environment. This also deploys the CERT C Compliance extension assets.
3. Analyze code with C/C++test using the SEI CERT C Standard test configuration and report violations to DTP. You can configure C/C++test to use the local test configuration or the test configuration shipped with the Security Compliance Pack.
4. Add the CERT C Compliance dashboard and widgets to your DTP interface to view the reported violations within the context of CERT C guidelines.
5. Interact with the widgets and reports to identify code that needs to be fixed, as well as print out the reports for auditing purposes.

CERT C Compliance Extension Assets

This section describes the assets shipped with the CERT C Compliance artifact.

Category and Guideline Definition Files

The following configuration files provide CERT C-oriented compliance categories in DTP interfaces:

- CERT_C-Categories.xml
- CERT_C-Guideline-Recommendation.xml
- CERT_C-Guideline-Rule.xml
- CERT_C-Guideline.xml
- CERT_C-Priority.xml

Test Configurations

You can configure C/C++test to run the test configurations shipped with the tool or with the Security Compliance Pack. Refer to the C/C++test documentation for details. The following test configurations are included with the pack:

- CERT_C [10.4.2]. properities
- CERT_C_RULES [10.4.2].properties

SEI_CERT_C_Compliance.json

This file adds the CERT C compliance dashboard template to DTP. See Custom Dashboard Templates for additional information about understanding dashboard templates.

CERT Compliance.json

This is the DTP Workflow you must install and deploy in Extension Designer. It extends DTP's data processing functionality to produce CERT-specific dashboard widgets and reports. It helps you track compliance status and document guideline enforcement, deviations, and rule re-categorization.

Model and Profiles

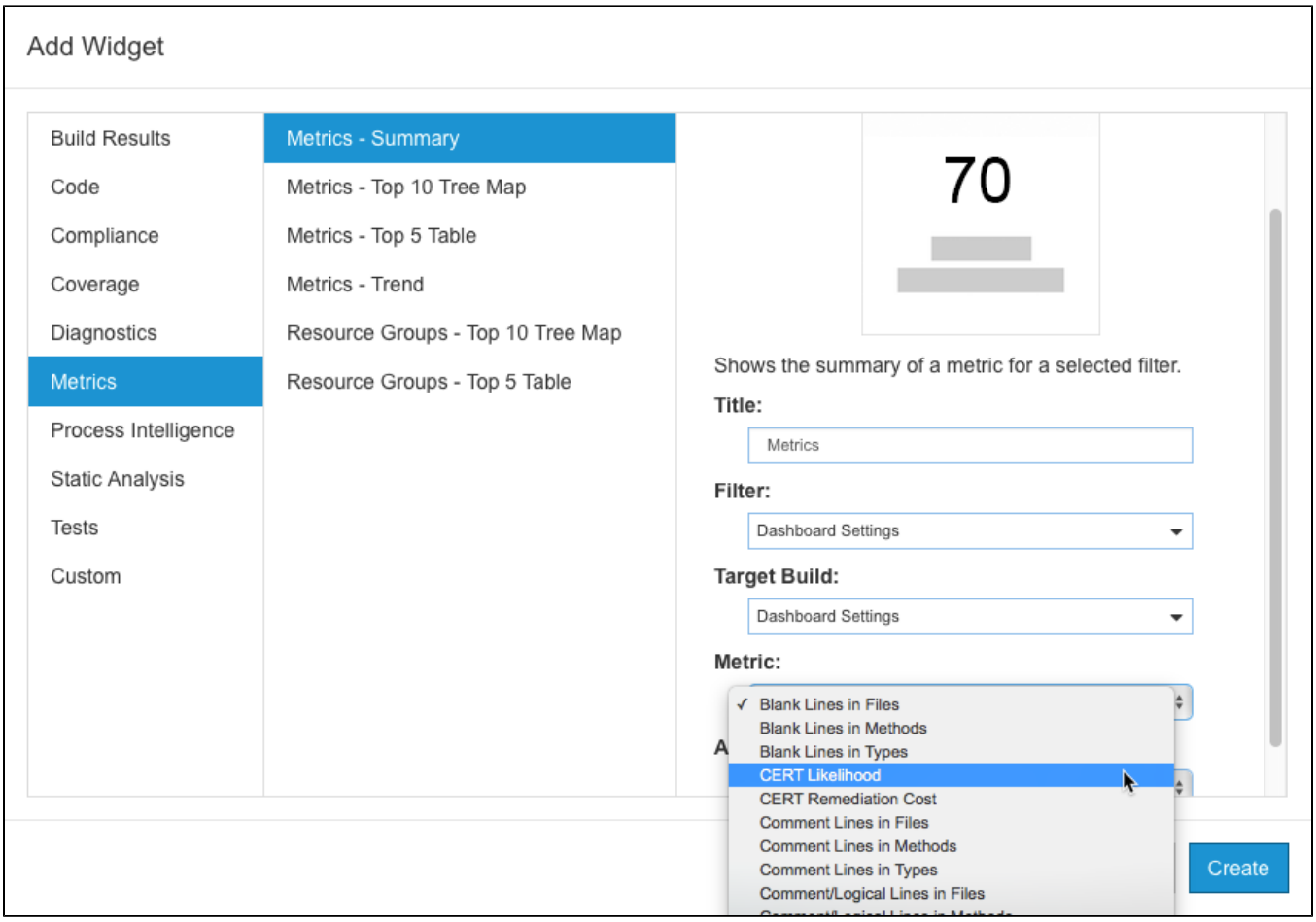
You can apply profiles to DTP Enterprise Pack extensions that perform custom calculations and drive reporting mechanisms in DTP.

- cert-compliance.json: This is the model file that describes how the cert-c-2018.json profile renders the data. The same model is used for CERT C++ Compliance.
- cert-c-2018.json: This is the default profile that renders data according to the cert-compliance.json model. This profile should be enabled to generate compliance audit reports.
- cert-c-likelihood.json: This profile provides metric information for key performance indicator (KPI) calculations. It renders data according to the KPI.json model.
- cert-c-remediation-cost.json: This profile provides metric information for KPI calculations. It renders data according to the KPI.json model.

See Working with Model Profiles for information about understanding profiles in DTP Enterprise Pack.

KPI.json

This profile extends the Key Performance Indicator artifact so that metrics widgets can show metrics information related to CERT C guidelines. The profile renders the data calculated by the cert-c-likelihood.json and cert-c-remediation-cost.json profiles.



Key Performance Indicator Extension is Required

In order to leverage the metrics calculations enabled by the KPI assets, install and deploy the Key Performance Indicator artifact. This artifact ships with the Security Compliance Pack, but you can contact your Parasoft representative to download a standalone instance of the artifact.

Cross-reference PDF

For your convenience, a PDF that shows the association between Parasoft rules and CERT guidelines is located in the <PACK>/rules/cpptest directory.

package.json

This file describes the contents of the extension.

Rule Map and Test Configuration

Parasoft static and flow analysis rules normally report violations according to a category (e.g., Possible Bug, Interoperability, etc.) and severity (i.e., 1-5). In order to view code analysis violations as CERT C guideline violations, DTP requires a rule map file that realigns Parasoft rules to report violations according to CERT C guidelines. In addition, the code analysis tool (C/C++test) needs a test configuration file that ensures that only the rules related to the remapped CERT C rules are executed. These files are shipped with C/C++test.

Deploying the CERT Compliance Assets

The CERT C Compliance artifacts are installed as part of the Security Compliance Pack (see Installation for instructions). After installing the artifact, you must deploy the assets to your DTP environment.

CERT C and CERT C++

If you are already using the CERT C++ Compliance artifact, you do not need to perform this step. Both artifacts use the same DTP Workflow.

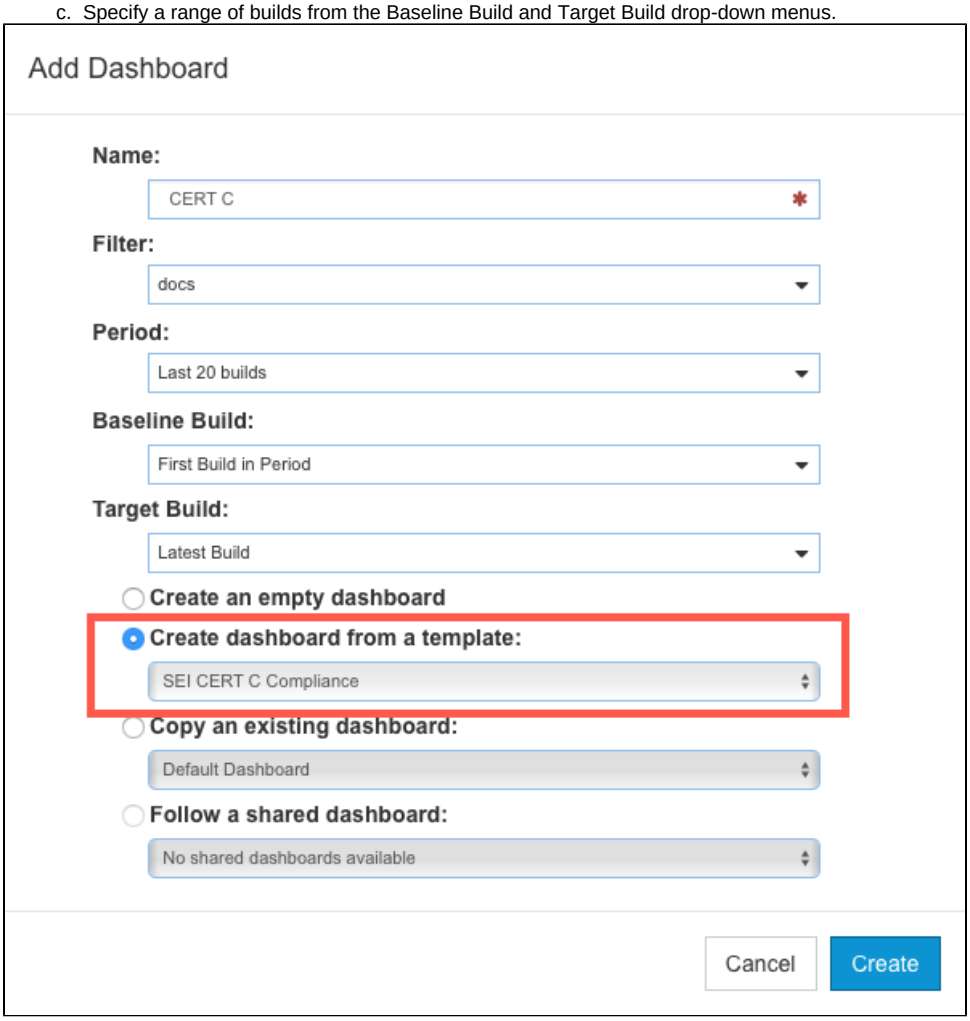
1. Choose **Extension Designer** from the DTP settings (gear icon) menu.
2. Click the **Services** tab and expand the **DTP Workflows** services category. You can deploy assets under any service category you wish, but we recommend using the DTP Workflows category to match how Parasoft categorizes the assets. You can also click **Add Category** to create your own service category (see Working with Services for additional information).
3. You can deploy the artifact to an existing service or add a new service. The number of artifacts deployed to a service affects the overall performance. See Extension Designer Best Practices for additional information. Choose an existing service and continue to step 5 or click **Add Service**.
4. Specify a name for the service and click **Confirm**.
5. The tabbed interface helps you keep artifacts organized within the service. Organizing your artifacts across one or more tabs does not affect the performance of the system. Click on a tab (or click the **+** button to add a new tab) and click the vertical ellipses menu.
6. Choose **Import> Library> Workflows> Security> CERT Compliance** and click anywhere in the open area to drop the artifact into the service.
7. Click **Deploy** and return to your DTP dashboard and refresh your browser.

You can now add the CERT C Compliance dashboard and widgets.

Adding the CERT C Compliance Dashboard

The CERT C dashboard template will be available after installing the Security Compliance Pack. If you do not see dashboard template, restart DTP (see Stopping DTP Services and Starting DTP Services).

1. Click **Add Dashboard** in the DTP toolbar and specify a name when prompted.
2. (Optional) You can configure the default view for the dashboard by specifying the following information:
    a. Choose the filter associated with your project in the filter drop-down menu. A filter represents a set of run configurations that enabled custom views of the data stored in DTP. See DTP Concepts for additional information.
    b. Specify a range of time from the Period drop-down menu.
    c. Specify a range of builds from the Baseline Build and Target Build drop-down menus.

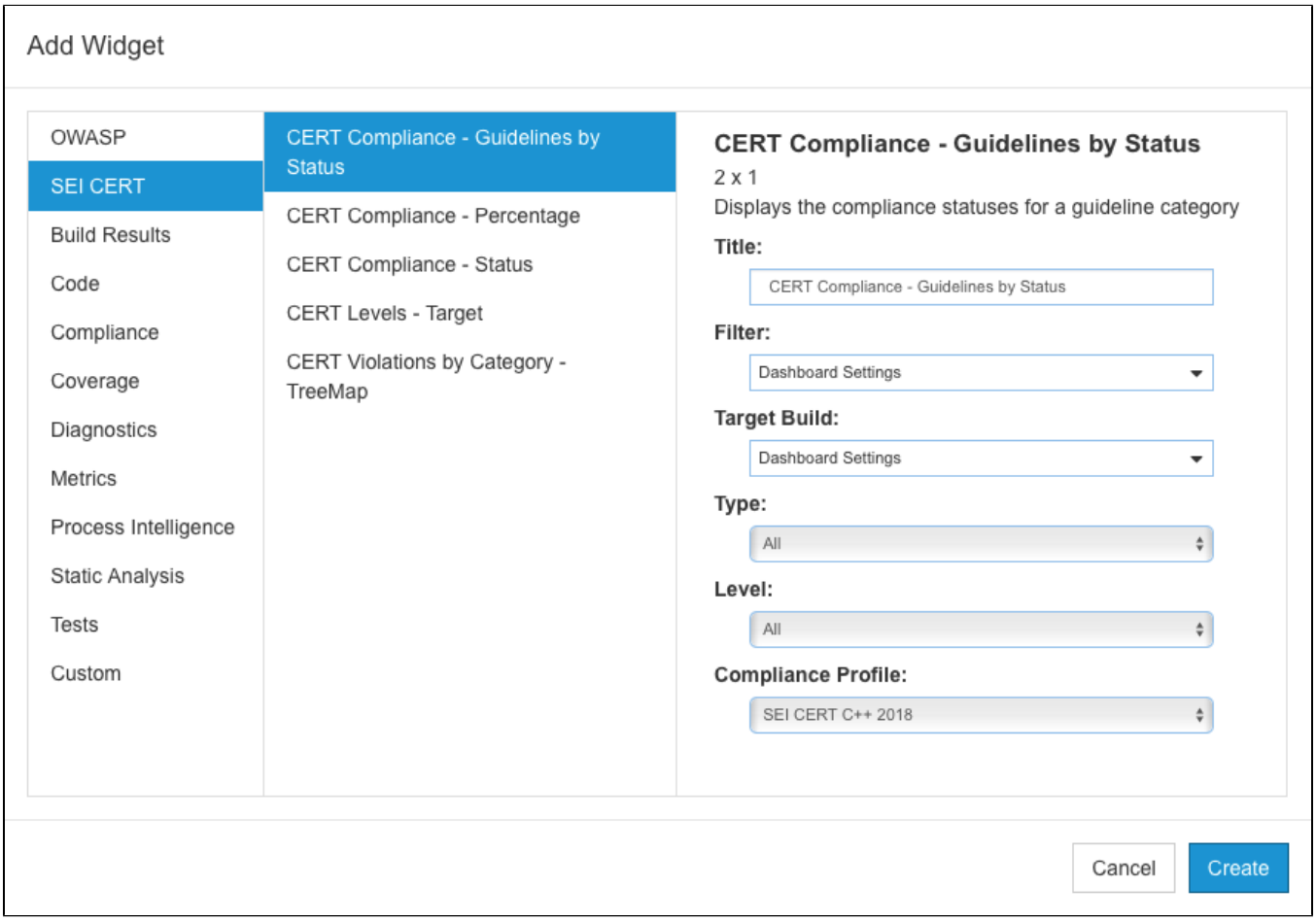


3. Enable the **Create dashboard from a template** option and choose the SEI CERT C Compliance dashboard.
4. Click **Create** to finish adding the dashboard.

If you have already executed C/C++test on your project using the SEI CERT C test configuration, most widgets will render data as soon as the dashboard is added. You can immediately begin working with the data to help you track your compliance goals (see Viewing CERT C Compliance Widgets). Additional steps, however, are necessary to use the Remediation Cost and Likelihood Score widgets, which rely on calculations executed by the KPI extension. See Enabling the CERT KPI Widgets for instructions.

Manually Adding the CERT C Widgets

You can manually add the CERT C widgets to an existing dashboard. See Adding Widgets for generation instructions on how to add widgets to a dashboard. After deploying the artifact, widgets will appear in the SEI CERT category.



The following configurations are available:

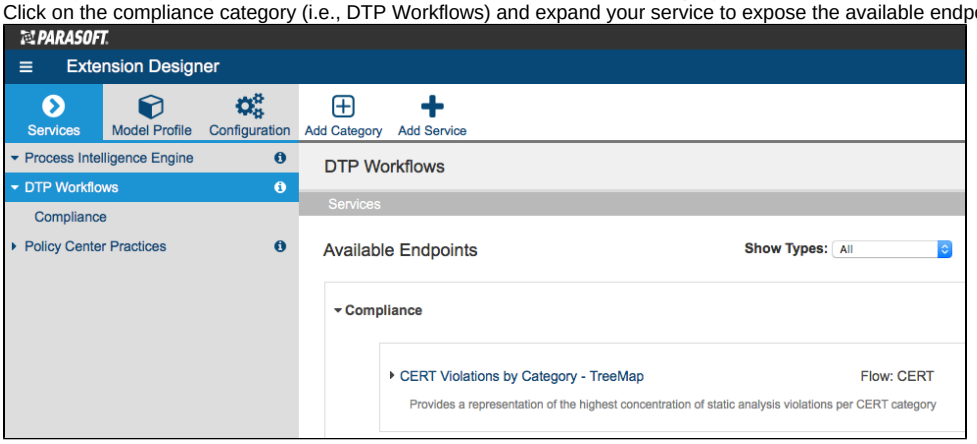
Title	You can rename the widget in the Title field. This setting is available for all widgets.
Filter	Choose a specific filter or Dashboard Settings from the drop-down menu. See Creating and Managing Filters for additional information. This setting is available for all widgets.
Target Build	Choose a specific build from the drop-down menu. The build selected for the entire dashboard is selected by default. See Using Build Administration for additional information about understanding builds. This setting is available for all widgets.
Type	This rule specifies which type of guideline you want to view in the widget. Choose either Rule, Recommendation, or All from the drop-down menu. See Background for additional information about guideline types. This setting is available for the following widgets: • CERT Compliance - Guidelines by Status • CERT Levels - Target • CERT Violations by Category - TreeMap
Level	This rule specifies which priority level you want to view in the widget. Choose either L1, L2, or L3 from the drop-down menu. See Back ground for additional information about guideline priorities. This setting is available for the following widgets: • CERT Compliance - Guideline by Status • CERT Compliance - Percentage • CERT Violations by Category - TreeM
Compliance Profile	Specify the compliance profile you want to use to view the data. In most cases, this should be the default profile shipped with the extension (see About the CERT Compliance Profile). This setting is available for all widgets.

Enabling the CERT KPI Widgets

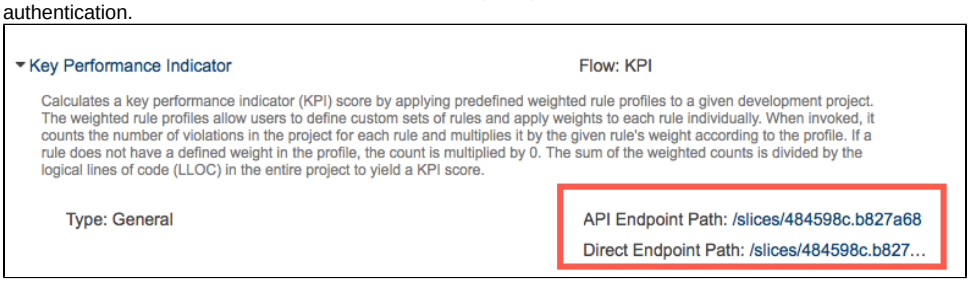
The Remediation Cost and Likelihood Score widgets are instances of the native Metrics - Summary DTP widget configured to present CERT-specific metrics data. When invoked, the KPI extension performs custom calculations according to the SEI CERT C Remediation Cost and SEI CERT C Likelihood KPI profiles and reports the processed data in the widgets.

The build must have static analysis and metrics analysis data for the KPI extension to perform the calculation. Be sure that C/C++test has been executed with the Metrics and SEI CERT C Guidelines test configurations under the same build ID. The metrics analysis must also include data for the Logical Lines of Code metric (metricId METRIC.NOLLOCIF). The guidelines test configuration will run analysis that provides violations for both rules and recommendations. You can also run the SEI CERT C Rules test configuration if do not need to gather data for recommendations. Refer to the C/C++test documentation for details about setting the build ID and executing the Metrics test configuration.

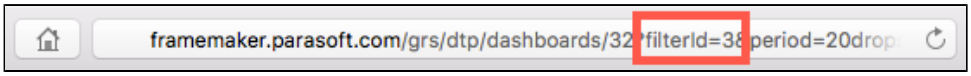
1. Choose **Extension Designer** from the DTP settings (gear icon) menu and click the **Services** tab.
2. Choose a service category and a service for the extension. We recommend deploying the KPI extension to the DTP Workflows category.
3. Open the vertical ellipses menu and choose **Import> Library> Workflows> Security> Key Performance Indicator**.
4. Click anywhere in the space to drop the flow into the service tab and click **Deploy**.
5. Click on the compliance category (i.e., DTP Workflows) and expand your service to expose the available endpoints.

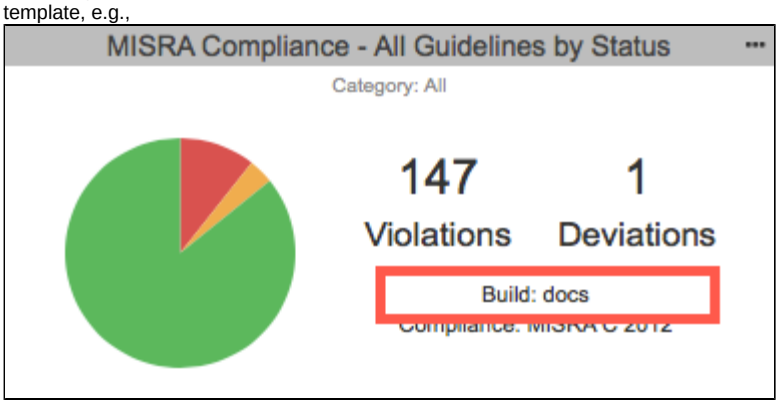


6. Expand the Key Performance Indicator section and copy the endpoint. Extension Designer presents two paths for the endpoint. The API Endpoint Path includes all API directories and can be used for exercising the endpoint in most cases. The Direct Endpoint Path is the direct path to the endpoint on the server and can be used if the API endpoint path is blocked or inaccessible, such as in some third-party integrations that require authentication.



7. Send a REST request to the endpoint along with the required parameters. For example, you can execute the request in a browser, a cURL command, or add it to a script. The following table describes the required parameters:

filterId	The filter ID for the project that the calculations will be performed on. You can quickly get the filter ID from URL of your dashboard.  You can also get the filter ID from the the Filters settings in DTP administration (see Creating and Managing Filters).
profile	Profile name with the rules and weights to use for the calculations, i.e., `SEI CERT C Remediation Cost` or `SEI CERT C Likelihood`.

buildId	The build ID for which the calculations will be performed on. If no build id is provided, this parameter defaults to the latest build. You can get the build ID from the dashboard URL. The build ID is also shown in several widgets that appear in the CERT C Dashboard template, e.g., 

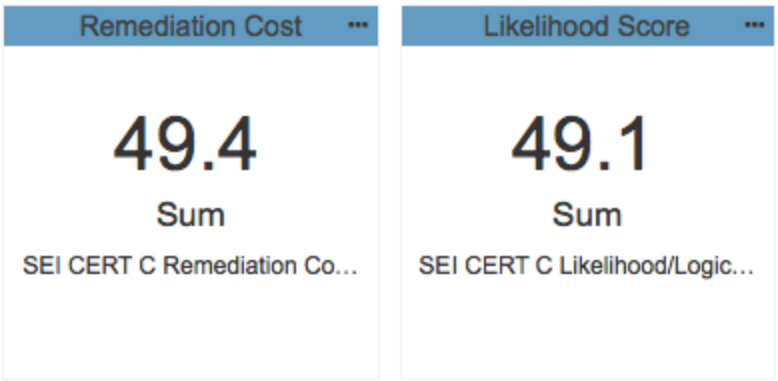
Example API Call URL

```
http://framemaker:8314/categories/5ae39f928550880f5026fc80?filterId=3&profile=SEI%20CERT%20C%20Likelihood
```

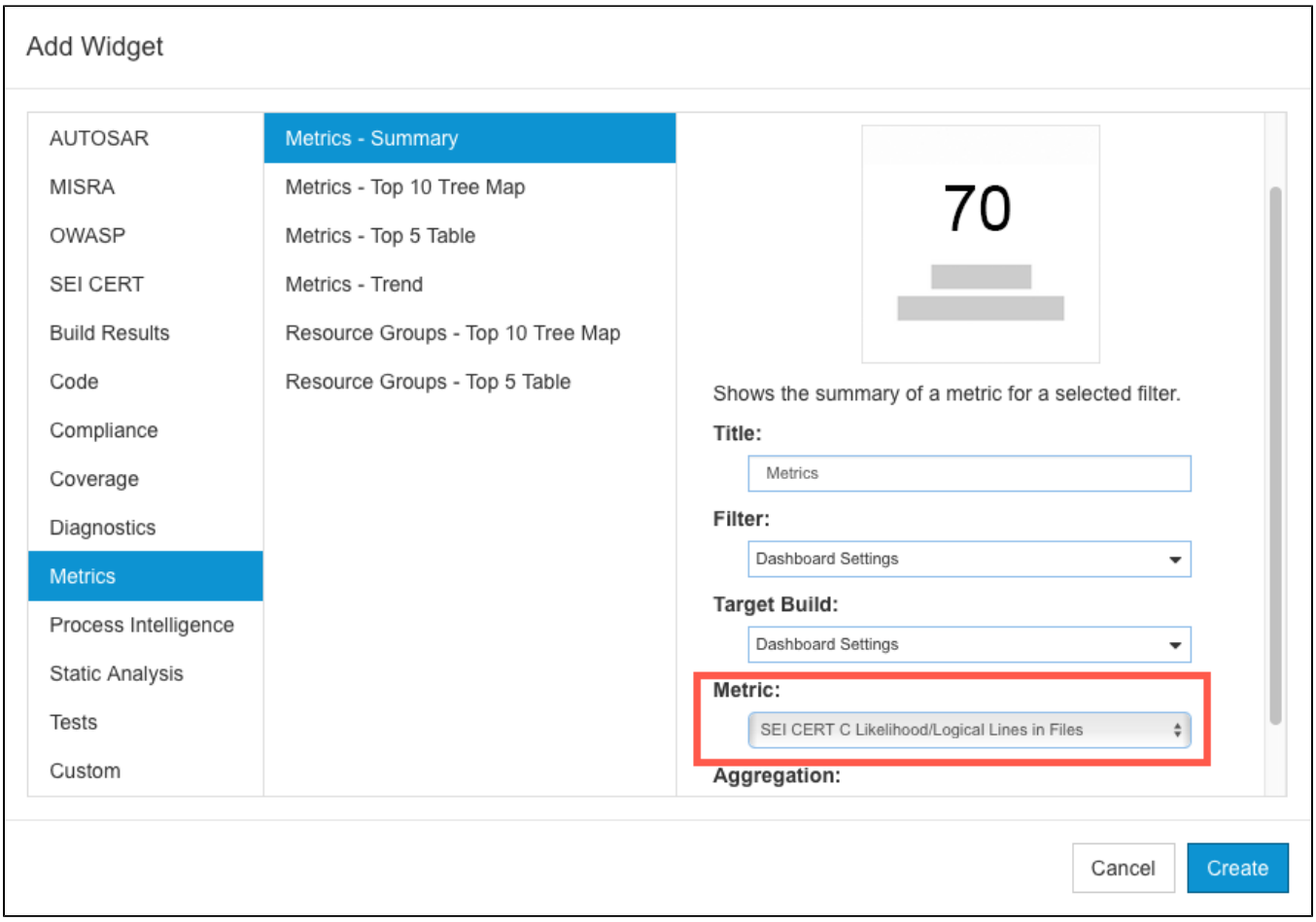
Example of Successful Response

```
{"success":{"title":"KPI","message":"Calculation has started for filter 'docs' using profile 'SEI CERT C
Likelihood'. Check debug output for any errors during calculation."}}
```

Metrics-related calculations are long-running processes and may take several minutes to execute depending on how much data you have to process. After the calculation completes, add the widgets to your dashboard to view the data. The KPI extension only needs to be deployed once, but you must invoke the API separately for each profile, i.e., SEI CERT C Likelihood and SEI CERT C Remediation Cost.



If you are not using the CERT C dashboard template or want additional views of the metrics, you can manually add instances of the native Metrics - Summary DTP widget to your dashboard and configure them to use the SEI CERT C Likelihood and SEI CERT C Remediation Cost metrics, as well as set the aggregation value:



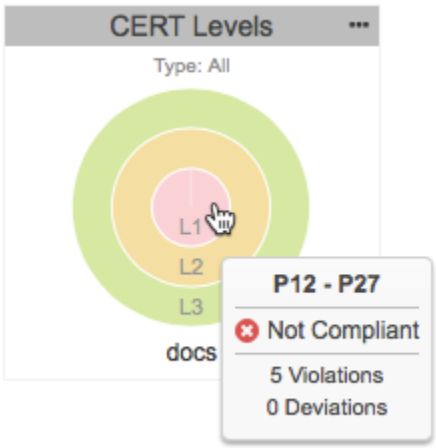
You can click on a widget to open the Single Metric Overview Report.

Viewing CERT C Compliance Widgets

The following widgets are shipped with the CERT C Compliance DTP Workflow to help you achieve CERT C compliance goals.

CERT Levels - Target

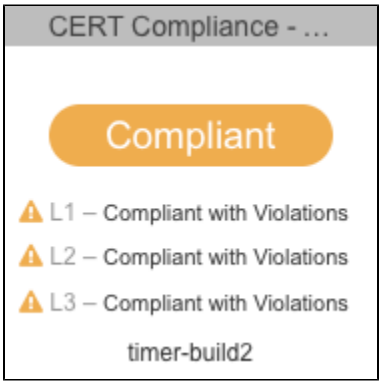
This widget provides an overview of the compliance status for each priority level in a tooltip for the target build. The tooltip also includes applicable deviations. Click on the widget to open the CERT C Compliance Report.

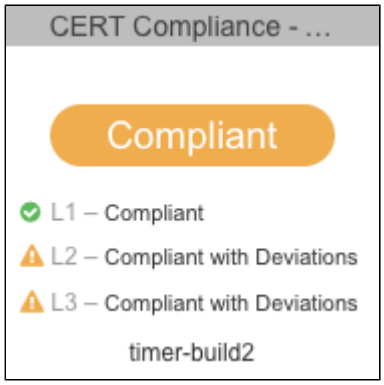


CERT Compliance - Status

The widget shows the overall compliance status, as well as the compliance status for each CERT C level. You can add multiple instances of the widget configured to use a different profile, e.g., a profile with disabled guidelines, to view your current compliance status. Click on the widget to open the CERT C Compliance Report.

The code can be compliant with deviations and violations that have been deemed acceptable. See Deviation Report for additional information about deviations.

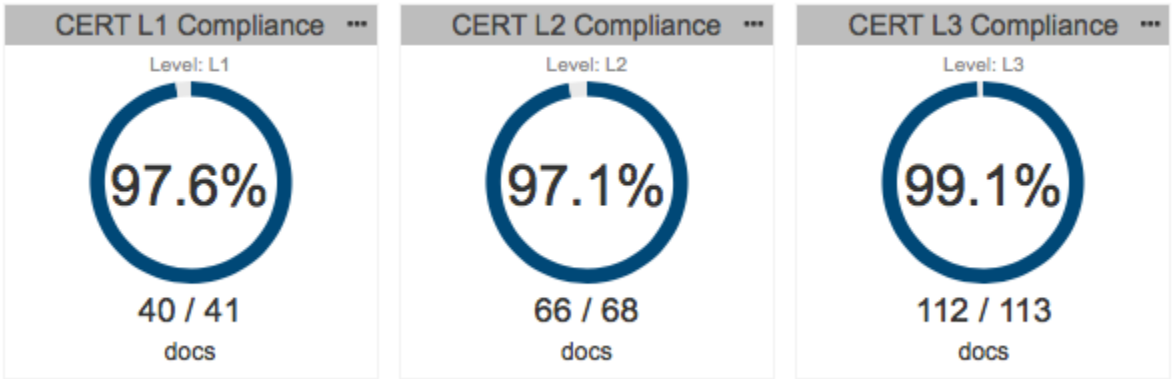




The status will be set to Not Compliant if Parasoft code analysis rules documented in your profile were not included in the specified build or if unacceptable violations have been reported. Make sure all rules are enabled in C/C++test and re-run analysis.

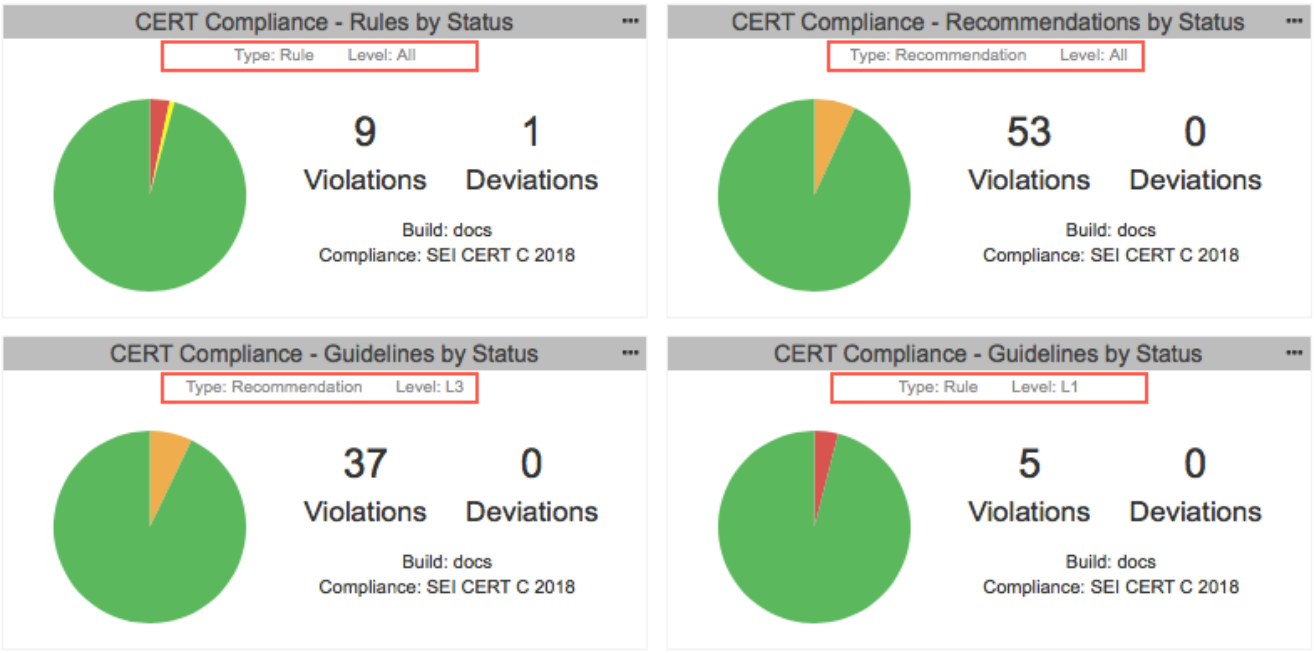
CERT Compliance - Percentage Widget

This widget shows the completeness of CERT compliance as a percentage. Completeness is based on the number of guidelines being enforced in the profile. Click on the widget to open the CERT C Compliance Report.



CERT Compliance - Guidelines by Status

This widget shows the compliance status for a specific Rule or Recommendation per priority level. You can add multiple instances of the widget configured to different type/priority level combinations to help you understand your compliance status from different perspectives.



The pie chart can represent up to four different guideline statuses for the selected category:

Green	Guidelines your code is in compliance with for the selected type and level.
Yellow	Guidelines that your code is deviating from but are still considered compliant. A deviation is when the guideline is not being followed according to the Parasoft static analysis rule, but is considered acceptable because it does not affect the safety of the software. Deviations represent Parasoft static analysis rules that have been suppressed.
Orange	Guidelines that your code is considered compliant with, even though the static analysis rules that enforce them contain violations. **Only Recommendations can have this status.**
Red	Guidelines that your code is not compliant with.

You can perform the following actions:

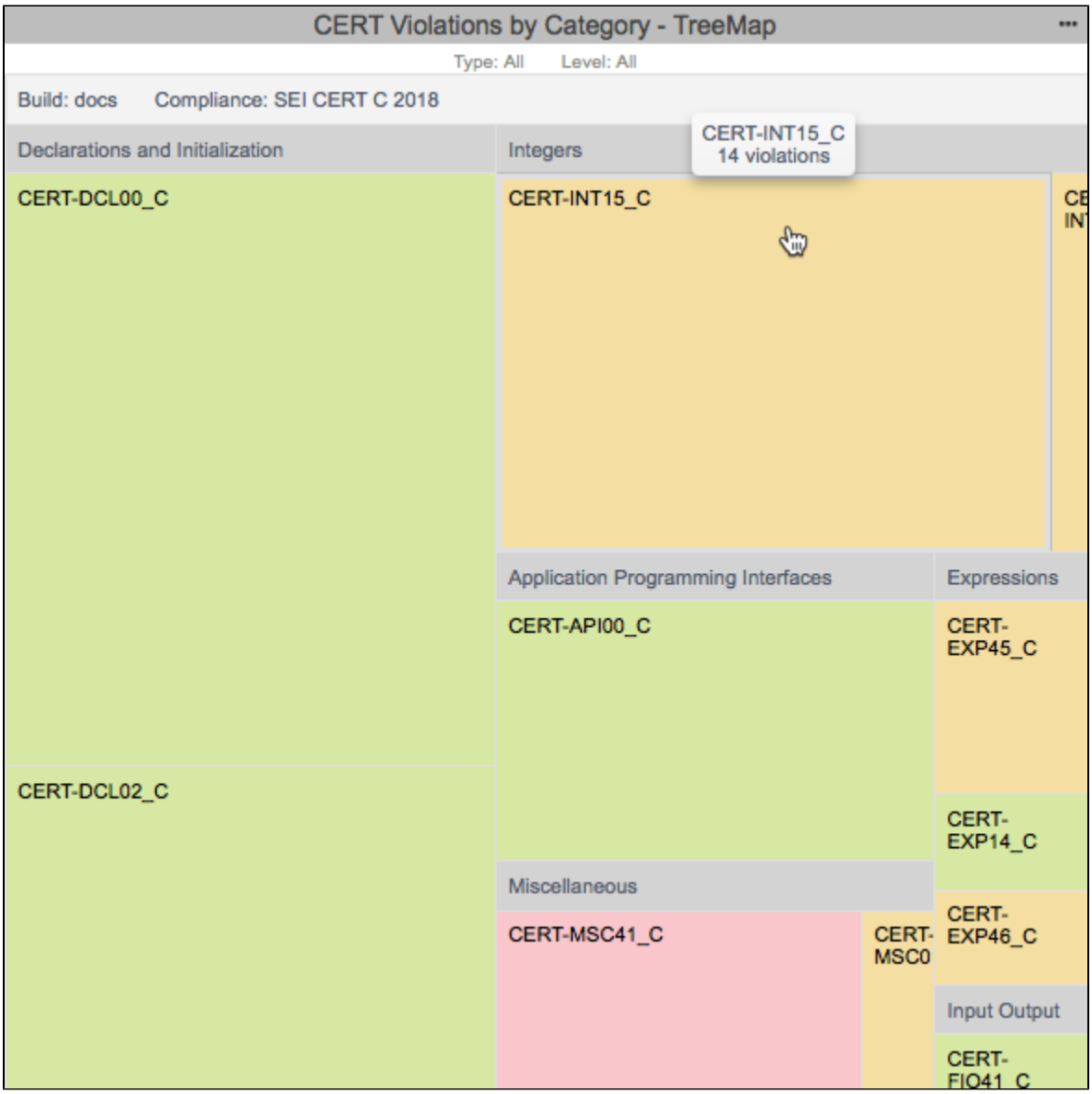
- Mouse over a pie slice to view details.
- Click on a section to open the CERT C Compliance Report filtered by the type, priority, and compliance status.
- Click on the number of violations counter to open the CERT C Compliance Report filtered by the type, priority, and compliance status.
- Click on the number of deviations counter to open the Deviation Report filtered by the type and priority.

CERT Violations by Category - TreeMap Widget

This widget provides a representation of the highest concentration of static analysis violations per type and priority level. Tiles are color-coded according the priority level:

- red tiles represent L1 violations
- yellow tiles represent L2 violations
- green tiles represent L3 violations

The Parasoft rule(s) enforcing compliance with the guidelines are also presented. Tiles are proportional to the number of static analysis violations reported for each rule.

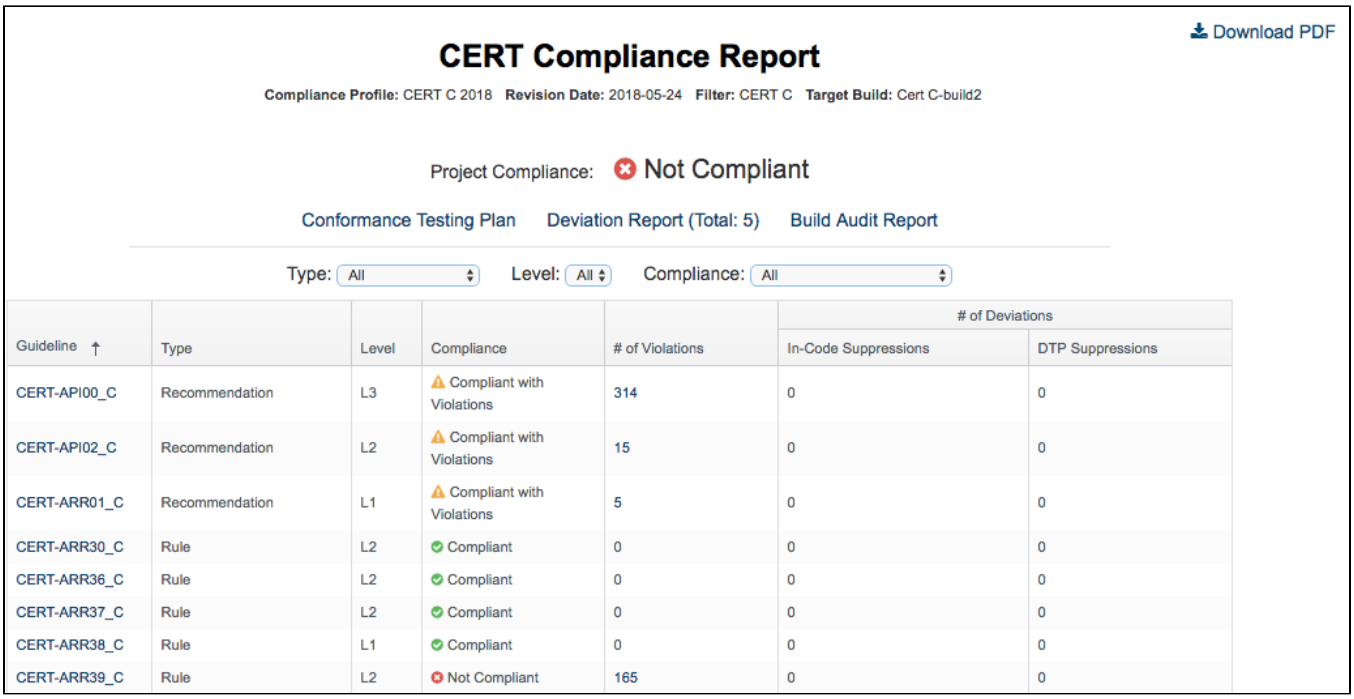


The widget uses the hierarchy established in the model profile to correlate Parasoft rules with CERT rules, recommendations, and priorities. You can mouse over a tile in the widget to view the number of violations associated with each rule-guidline-category.

Click on a rule to see the violation in the Violations Explorer.

Viewing CERT C Compliance Reports

The CERT Compliance Report provides an overview of your CERT compliance status and serves as the primary document for demonstrating compliance.



Download PDF

CERT Compliance Report

Compliance Profile: CERT C 2018 **Revision Date:** 2018-05-24 **Filter:** CERT C **Target Build:** Cert C-build2

Project Compliance: Not Compliant

Conformance Testing Plan | Deviation Report (Total: 5) | Build Audit Report

Type: All Level: All Compliance: All

Guideline	Type	Level	Compliance	# of Violations	# of Deviations	
					In-Code Suppressions	DTP Suppressions
CERT-API00_C	Recommendation	L3	Compliant with Violations	314	0	0
CERT-API02_C	Recommendation	L2	Compliant with Violations	15	0	0
CERT-ARR01_C	Recommendation	L1	Compliant with Violations	5	0	0
CERT-ARR30_C	Rule	L2	Compliant	0	0	0
CERT-ARR36_C	Rule	L2	Compliant	0	0	0
CERT-ARR37_C	Rule	L2	Compliant	0	0	0
CERT-ARR38_C	Rule	L1	Compliant	0	0	0
CERT-ARR39_C	Rule	L2	Not Compliant	165	0	0

You can perform the following actions:

- Use the drop-down menus to sort by the following criteria:
  - Guideline type: Rule, Recommendation, or All
  - Priority level: L1, L2, L3, or All
  - Compliance status: All, No Rules Enabled, Compliant, Compliant With Deviations, Compliant With Violations, Not Compliant, Missing Rule(s) in Analysis
- Click on a guideline link in the Guideline column to open the Conformance Enforcement Plan. The link goes directly to the specific guideline so that you can review the Parasoft code analysis rule or rules enforcing the guideline.
- Click on a link in the # of Violations, In-Code Suppression, or DTP Suppressions column to view the violations in the Violations Explorer.
- Open one of the CERT Compliance sub-reports.
- Click **Download PDF** to download a printer-friendly PDF version of the report data. If you added a custom graphic to DTP as described in Adding a Custom Graphic to the Navigation Bar, the PDF will also be branded with the graphic.

The CERT Compliance Report contains four supporting reports:

- Conformance Testing Plan
- Deviation Report
- Build Audit Report

Conformance Testing Plan

The Conformance Testing Plan cross-references CERT guidelines with Parasoft static analysis rules using the data specified in the compliance profile. You can change the severity, likelihood, remediation cost, and other values to meet your project goals by configuring the profile.

CERT Conformance Testing Plan

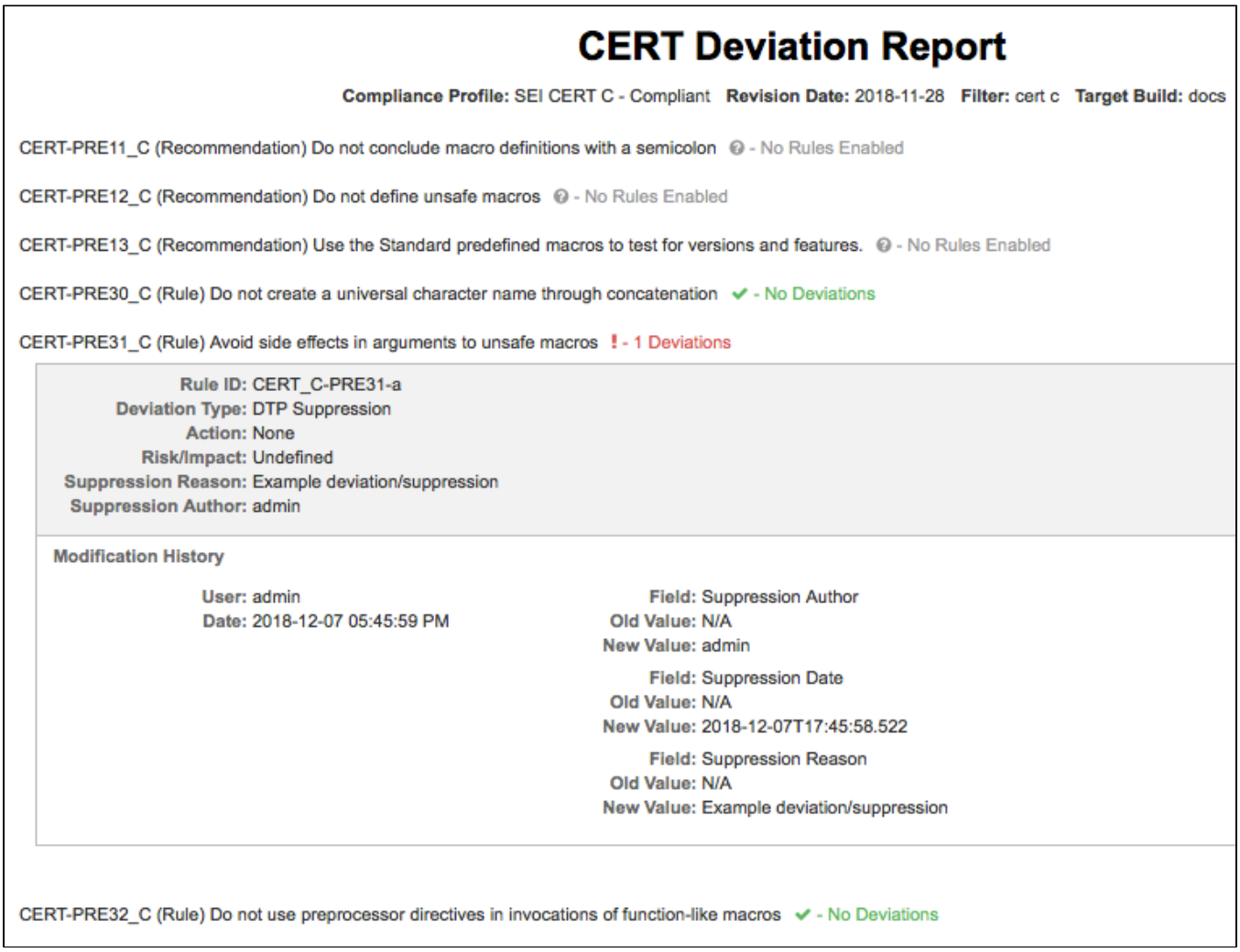
Compliance Profile: SEI CERT C 2018 **Analysis Tool:** Parasoft C++test 10.4.2 **Revision Date:** 2019-04-22

Guideline	Type	Description	Category	Severity	Likelihood	Remediation Cost	Priority	Level	Parasoft Rule Ids
API00-C	Recommendation	Functions should validate their parameters	Application Programming Interfaces	Medium	Unlikely	High	P2	L3	CERT_C-API00-a
API01-C	Recommendation	Avoid laying out strings in memory directly before sensitive data	Application Programming Interfaces	High	Likely	High	P9	L2	CERT_C-API01-a CERT_C-API01-b
API02-C	Recommendation	Functions that read or write to or from an array should take an argument to specify the source or target size	Application Programming Interfaces	High	Likely	High	P9	L2	CERT_C-API02-a CERT_C-API02-b
API03-C	Recommendation	Create consistent interfaces and capabilities across related functions	Application Programming Interfaces	Medium	Unlikely	Medium	P4	L3	
API04-C	Recommendation	Provide a consistent and usable error-checking mechanism	Application Programming Interfaces	Medium	Unlikely	Medium	P4	L3	
API05-C	Recommendation	Use conformant array parameters	Application Programming Interfaces	High	Probable	Medium	P12	L1	

Deviation Report

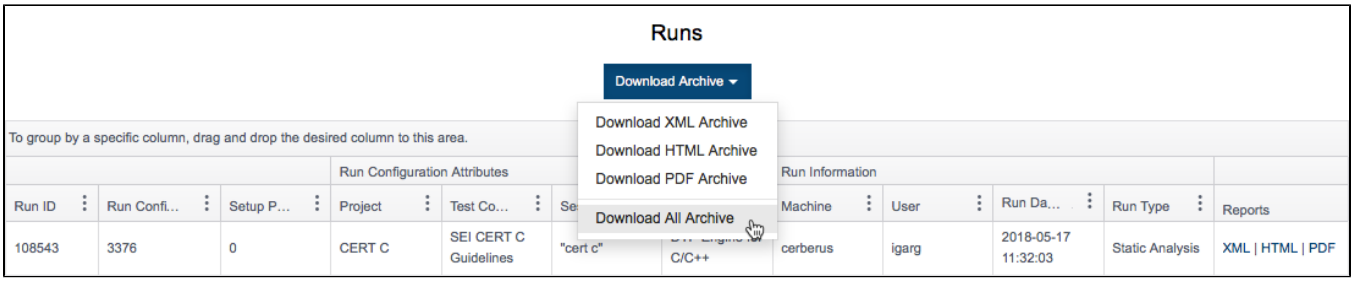
Your code can contain violations and still be CERT-compliant as long as the deviations from the standard are documented and that the safety of the software is unaffected. Deviations are code analysis rules that have been suppressed either directly in the code or in the DTP Violations Explorer. See the C/C++test documentation for details on suppressing violations in the code. See Suppressing Violations in the Violations Explorer documentation for information about suppressing violations in DTP.

Click on the **Deviation Report** link in the CERT Compliance Report to open the Deviation Report. You can filter the report by guideline type and level. You can also filter out violations that have not been suppressed by enabling the **Only Deviations** option.



Build Audit Report

The Build Audit Report is native functionality in DTP. It shows an overview of code analysis violations, as well as test results and coverage information, associated with the build. This report also allows you to download an archive of the data, which is an artifact you can use to demonstrate compliance with CERT during a regulatory audit.



In order to download an archive, the build has to be locked. See Build Audit Report for additional details about this report.

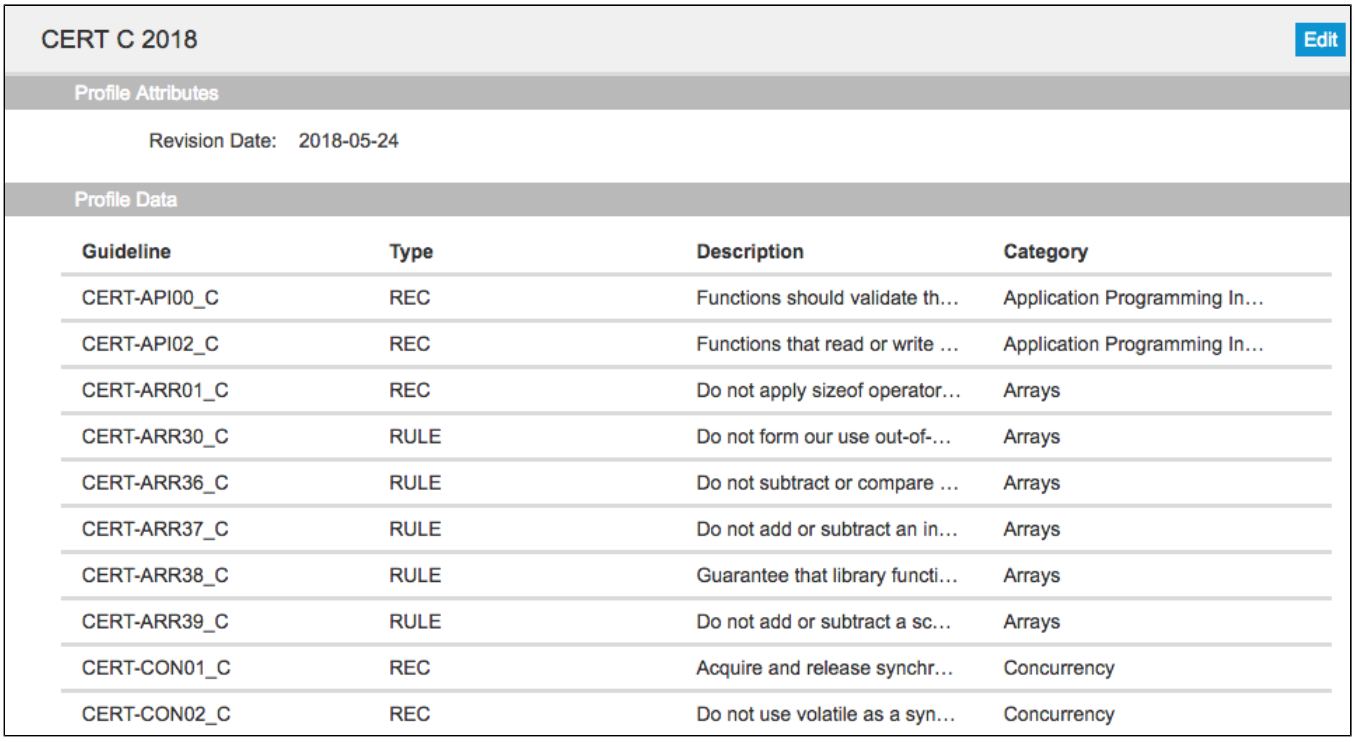
Profiles

The Security Compliance Pack for DTP 5.4.2 includes a profile associated with the core CERT C workflow and a set of profiles associated with calculating the SEI CERT C Remediation Cost and SEI CERT C Likelihood KPI metrics. See Working with Model Profiles for additional information about profiles.

About the CERT Compliance Profile

The CERT C Compliance DTP Workflow ships with a default profile that includes information necessary for generating CERT compliance reports. The default profile shows the correlation between CERT guidelines and Parasoft code analysis rules and is suitable for most normal use cases.

> **Do not modify the CERT profile**
>
> We strongly advise against altering the default CERT C 2018 profile because doing so will affect any reports you may need to generate for auditing purposes.



CERT C 2018 — Edit

Profile Attributes

Revision Date: 2018-05-24

Profile Data

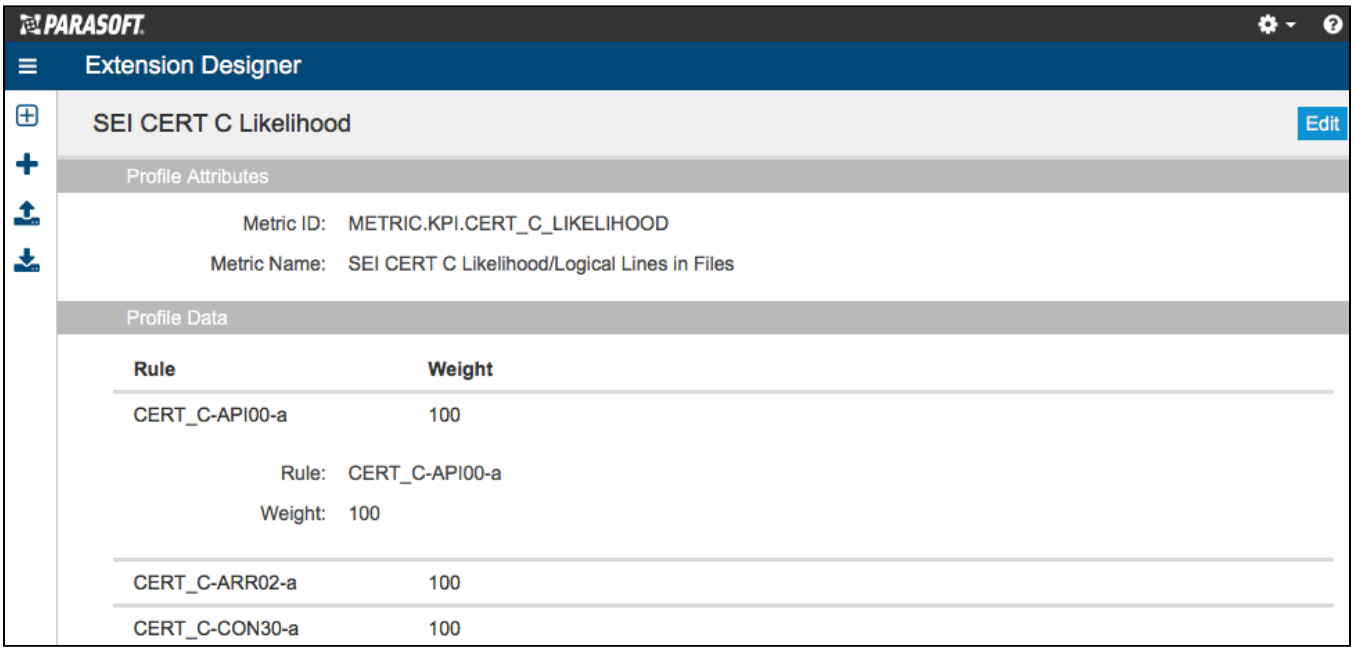
Guideline	Type	Description	Category
CERT-API00_C	REC	Functions should validate th…	Application Programming In…
CERT-API02_C	REC	Functions that read or write …	Application Programming In…
CERT-ARR01_C	REC	Do not apply sizeof operator…	Arrays
CERT-ARR30_C	RULE	Do not form our use out-of-…	Arrays
CERT-ARR36_C	RULE	Do not subtract or compare …	Arrays
CERT-ARR37_C	RULE	Do not add or subtract an in…	Arrays
CERT-ARR38_C	RULE	Guarantee that library functi…	Arrays
CERT-ARR39_C	RULE	Do not add or subtract a sc…	Arrays
CERT-CON01_C	REC	Acquire and release synchr…	Concurrency
CERT-CON02_C	REC	Do not use volatile as a syn…	Concurrency

If necessary, you can make a copy of the default profile and adjust the correlation between Parasoft code analysis rules and CERT C guidelines to achieve your software quality and compliance goals.

1. Open Extension Designer and click the **Model Profile** tab.
2. Expand the CERT Compliance model and choose the **SEI CERT C 2018** profile.
3. Click **Export Profile** to download a copy.
4. Click **Add Profile** and enter a name.
5. Click **Confirm** to create an empty profile.
6. Rename the copy of the default profile you exported and click **Import Profile**.
7. Browse for the copy and confirm to upload.
8. Click **Edit** and make your adjustments.
9. Click **Save.**

CERT C KPI Profiles

The KPI artifact shipped with the Security Compliance Pack includes the SEI CERT C Likelihood and SEI CERT C Remediation Cost profiles. The profiles assign weights to the metrics analysis rules in order to calculate a KPI value for the build.



The default profile is suitable for most normal usage, but you can adjust the weights for each metrics rule if necessary.

1. Open Extension Designer and click the **Model Profile** tab.
2. Expand the KPI model and choose either the **SEI CERT C Likelihood** or **SEI CERT C Remediation** profile.
3. Click **Export Profile** to download a copy.
4. Click **Add Profile** and enter a name.
5. Click **Confirm** to create an empty profile.
6. Rename the copy of the default profile you exported and click **Import Profile**.
7. Browse for the copy and confirm to upload.
8. Click **Edit** and make your adjustments.
9. Click **Save.**