CWE Compliance

In this section:

Introduction

The Parasoft CWE Compliance artifact is a set of assets for your DTP infrastructure that enable you to readily demonstrate compliance with CWE Top 25 and CWE List Version 2.11 development guidelines. The artifact is shipped as part of the Security Compliance Pack for DTP 5.4.0. Contact your Parasoft representative for download and licensing information.

About CWE Top 25 2011

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. They are often easy to identify and exploit by attackers, allowing them to completely take over the software, steal data, or prevent the software from working at all.

Visit http://cwe.mitre.org/top25/ to learn more about the CWE Top 25 standard.

About CWE List Version 2.11

The Common Weakness Enumeration (CWE) is a list of software weaknesses types. It is an ongoing community-driven effort to capture the specific effects, behaviors, exploit mechanisms, and implementation details affecting software development. The items on the list are created with input from many organizations and individuals. The position on the list is chosen based on real-world criteria, such as prevalence, ease-of-exploit, etc.

Visit https://cwe.mitre.org/data/ to learn more about the CWE List.

Prerequisites

- DTP (with enterprise license) and DTP Enterprise Pack 5.4.0
- A code analysis tool (i.e., Jtest, C/C++test, or dotTEST) version 10.4.0 or later with the Flow Analysis license feature enabled.

Process Overview

1. Install the Security Compliance Pack (see Security Compliance Pack for DTP 5.4.0 for installation instructions).
2. Connect your code analysis tool to DTP and configure the report settings, such as project name, build ID, etc. See the documentation for your analysis tool for details. This enables the tool send code analysis data to the correct project in DTP for processing.
3. Deploy the DTP artifact, which includes widgets for viewing compliance status on your DTP dashboard, as well as configurations for reorienting Parasoft static analysis rules to display as CWE IDs. This process is performed in DTP Extension Designer.
4. Analyze the project with your code analysis tool using the configuration and report violations to DTP.
5. Run the KPI Process Intelligence slice as part of your automated build process to generate the compliance data.
6. Use the DTP dashboard template, widgets, and reports to monitor compliance with security standards.

CWE Compliance Assets

The CWE Compliance extension helps you create the documentation required for demonstrating compliance with CWE guidelines. The following artifacts are included in the package.

Category and Guideline Definition Files

The pack ships with four sets of compliance categories that enable CWE-centric views of the static analysis data reported by the code analysis tools:

File	Description

compliance_cweid_all.xml	MITRE CWE 2.11 This set of compliance categories re-maps the static analysis violations so that they are grouped and displayed as CWE List Version 2.11 errors in widgets and reports.
compliance_impact_all.xml	MITRE CWE 2.11 - Technical Impact This set of compliance categories re-maps the static analysis violations so that they are grouped and displayed in widgets and reports by their technical impact according to CWE List Version 2.11 guidelines. The "technical impact" is a weakness categorization in CWE. See https://cwe.mitre.org/cwraf/ti_scorecard.html for additional information.
compliance_cweid_top25.xml	2011 CWE/SANS Top 25 This set of compliance categories re-maps the static analysis violations so that they are grouped and displayed as CWE/SANS Top 25 Most Dangerous Software Programming Errors in widgets and reports.
compliance_impact_top25.xml	2011 CWE/SANS Top 25 - Technical Impact This set of compliance categories re-maps the static analysis violations so that they are grouped and displayed in widgets and reports by their technical impact according to CWE/SANS Top 25 Most Dangerous Software Programming Errors guidelines. The "technical impact" is a weakness categorization in CWE. See https://cwe.mitre.org/cwraf/ti_scorecard.html for additional information.

See Custom Compliance Categories for additional information about rule categories in DTP.

CWE Top 25 Dashboard Template

The template adds security compliance-related widgets to your DTP dashboard (see Custom Dashboard Templates for additional information about dashboard templates).

DTP Workflows

The extension ships with the following DTP Workflows (also called 'slices').

Violations by Compliance

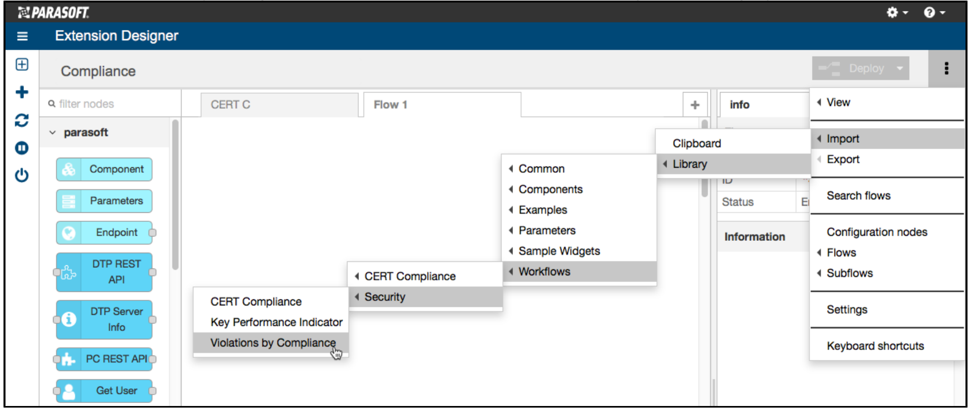
This slice contains a set of widgets that you can configure to show CWE violations. See Security Compliance Widgets for OWASP.

Key Performance Indicator

In order to leverage the metrics calculations enabled by the KPI assets, the Security Compliance Pack ships with the Key Performance Indicator (KPI) artifact. This artifact is also available separately from the Parasoft. Contact your Parasoft representative for details.

Installation

1. The CWE Compliance assets are automatically installed when you in stall the Security Compliance Pack. See Installation for installation instructions.
2. Import the Violations by Compliance and KPI slices into Extension Designer and deploy them to DTP. See Working with Flows for instructions.

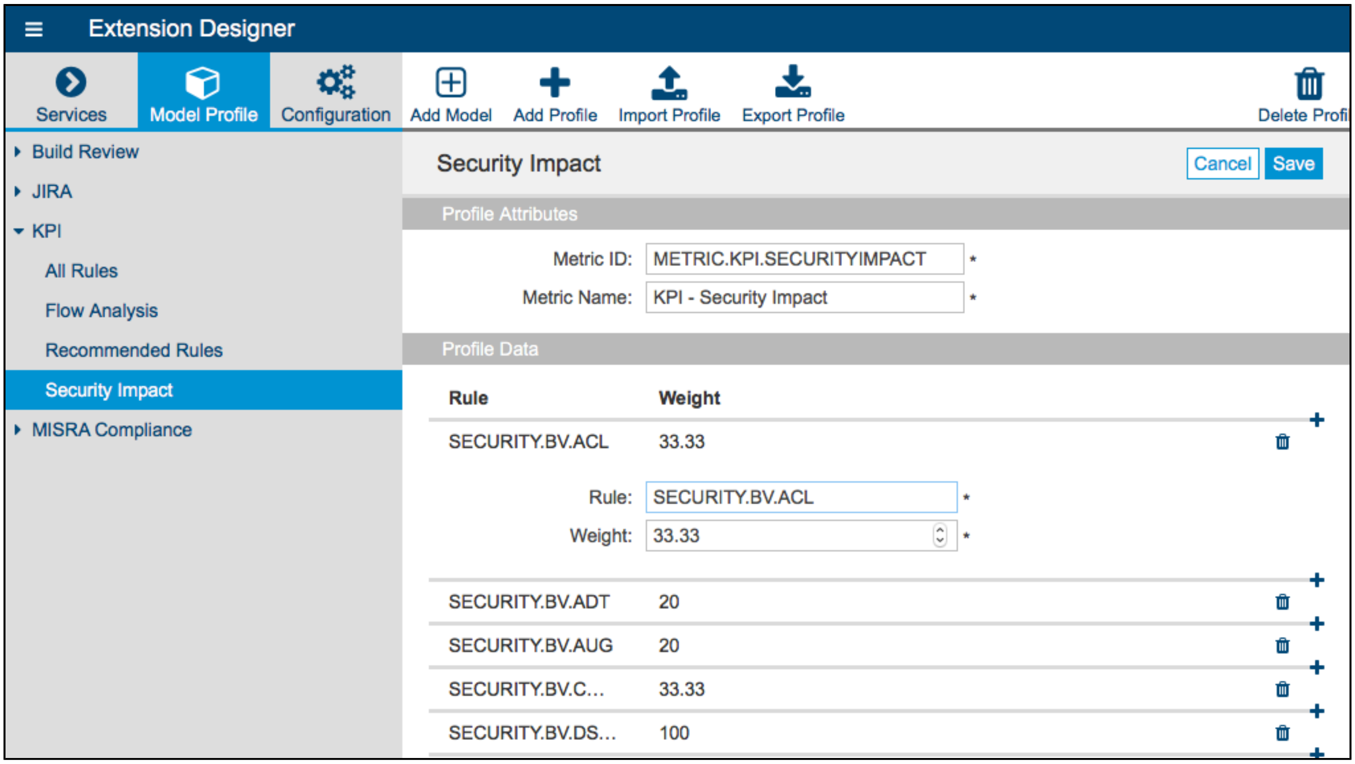


In order to view CWE code metrics, you will need to run the KPI artifact with the Security Impact profile enabled. See Running the KPI Slice.

Running the KPI Slice

The Key Performance Indicator (KPI) Process Intelligence slice defines a KPI associated with static analysis rules so you can measure and quantify results. The KPI slice uses model profiles to perform custom calculations (see Working with Model Profiles). You can adjust the calculations by modifying the profile.

KPI ships with an example model profile called “Security Impact” that demonstrates how you can adjust the weight of static analysis rules to define your own KPIs, such as the impact of a rule on security.



Security Impact

Profile Attributes

Metric ID: METRIC.KPI.SECURITYIMPACT *

Metric Name: KPI - Security Impact *

Profile Data

Rule	Weight
SECURITY.BV.ACL	33.33

Rule: SECURITY.BV.ACL *

Weight: 33.33 *

Rule	Weight
SECURITY.BV.ADT	20
SECURITY.BV.AUG	20
SECURITY.BV.C...	33.33
SECURITY.BV.DS...	100

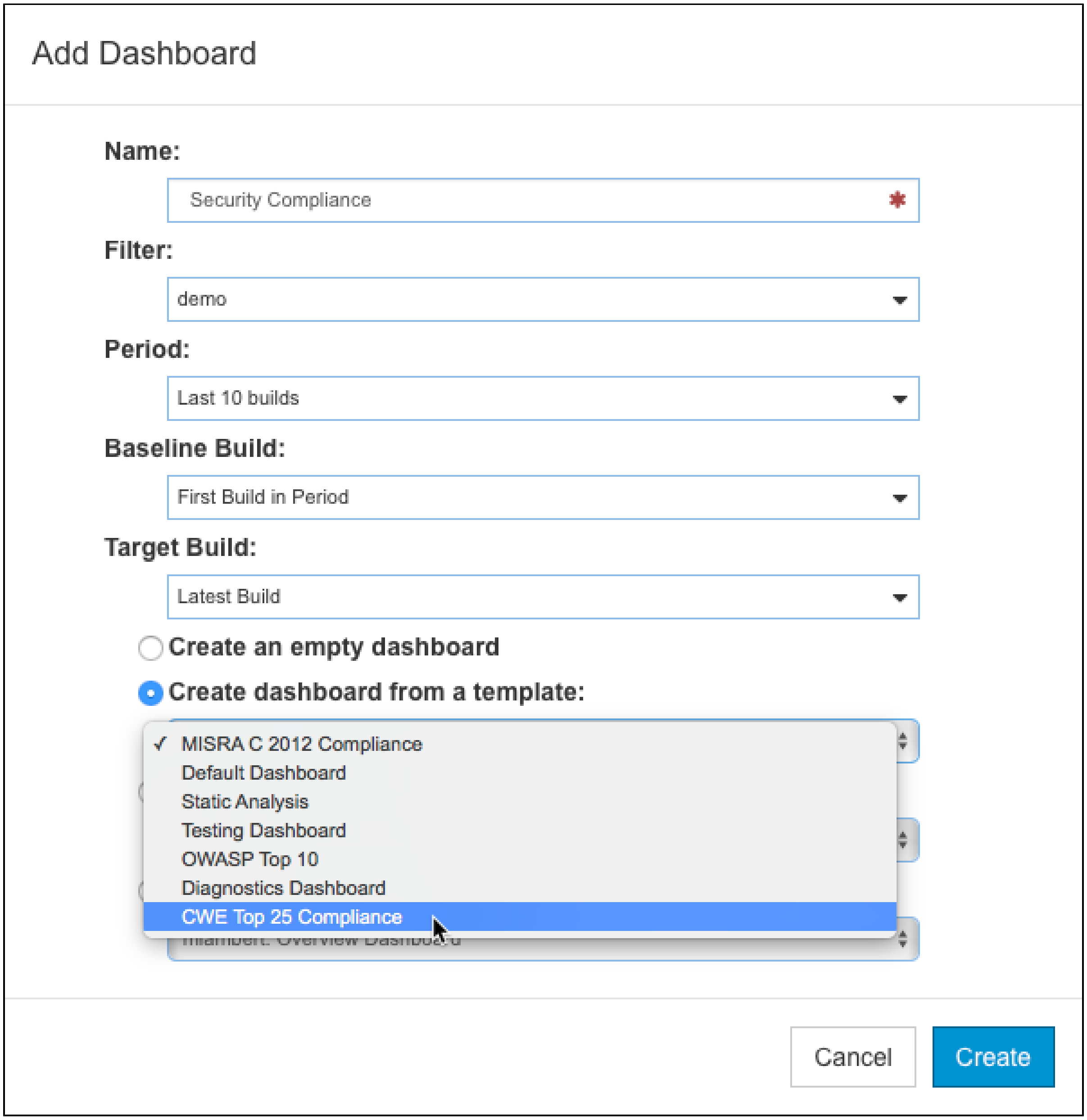
Every rule can have a different weighting, and not every rule has to be in the profile, which enables you to run different KPIs for different purposes and different profiles for different subsets of rules.

> **Run KPI as part of your automated build process**
>
> Depending on the volume of data being analyzed, KPI calculation may require multiple runs to acquire the core data and may take significant time, therefore triggering KPI calculation should be done as part of your build process or by manually using a trigger node in the KPI slice.

After configuring the profile, it must be passed when invoking the KPI slice to run the calculation. See Invoking the Calculation for instructions on invoking KPI with the Security Impact profile enabled.

Viewing CWE Widgets

After deploying the DTP Workflows and running the KPI slice, add the CWE Top 25 template to your dashboard (see Adding Dashboards).



Add Dashboard

Name: Security Compliance

Filter: demo

Period: Last 10 builds

Baseline Build: First Build in Period

Target Build: Latest Build

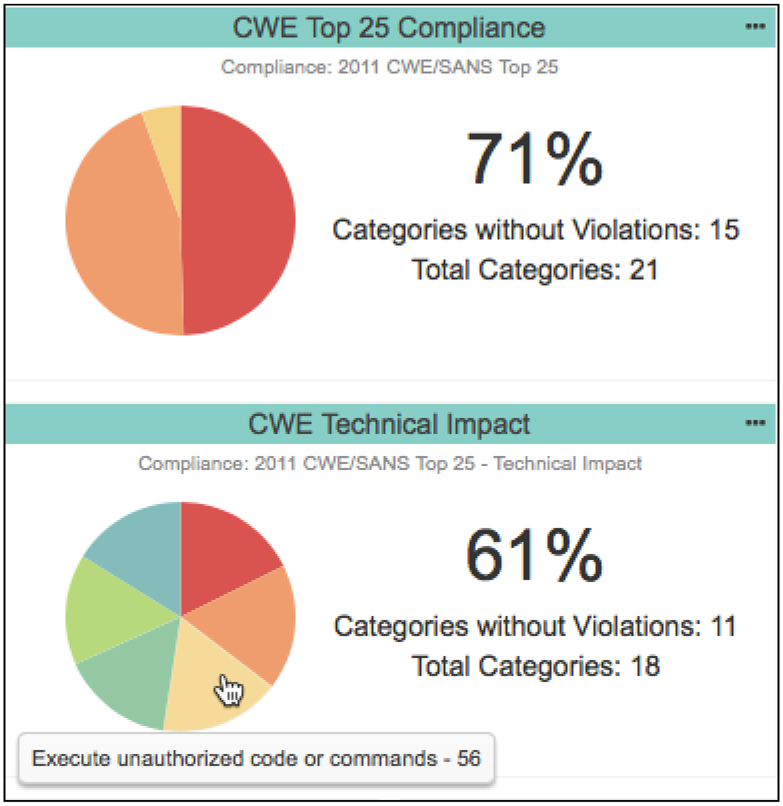
○ Create an empty dashboard

● Create dashboard from a template:

The following widgets are added when you installed.

Violations in Compliance - Pie

This widget shows the overall compliance status as a percentage. Each pie chart segment represents a compliance category that the code violates. The widget also shows the total number of compliance categories being applied and the number of categories with which the code is compliant. The dashboard adds an instance of the widget for each set of compliance categories. See Configuring CWE Widgets for details on configuring the widget.


CWE Top 25 Compliance
Compliance: 2011 CWE/SANS Top 25
71%
Categories without Violations: 15
Total Categories: 21
CWE Technical Impact
Compliance: 2011 CWE/SANS Top 25 - Technical Impact
61%
Categories without Violations: 11
Total Categories: 18
Execute unauthorized code or commands - 56

You can perform the following actions:

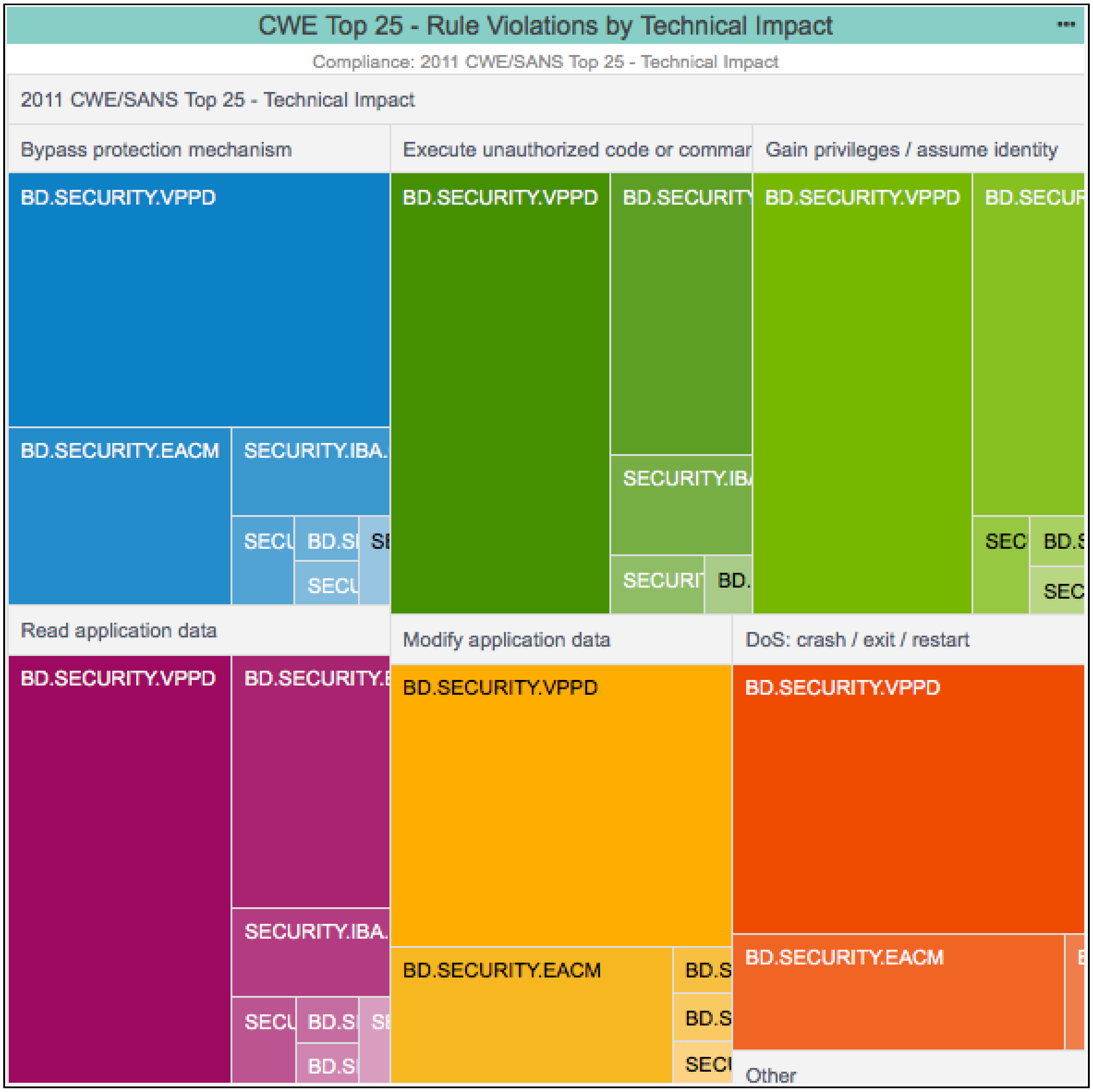
- Mouse over a segment in the chart to view the number of violations associated with a specific category.
- Click on a segment to open the Violations by Rule report.
- Click on the compliance percentage to open the Violations by Compliance Category report.

Reusing the Widget

You can use this widget with any compatible compliance category in your DTP system. See Adding Widgets for instructions on how to manually add the widget to your dashboard.

Violations in Compliance - Treemap

This widget shows the violations grouped by compliance in a tree map. Each tile is assigned a color and represents a compliance category. The dashboard includes an instance of the widget configured to show the 2011 CWE/SANS Top 25 - Technical Impact compliance category. See Configuring CWE Widgets for details on configuring the widget.



You can perform the following actions:

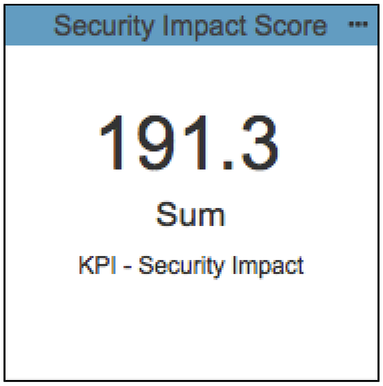
- Mouse over a tile in the to view the number of violations associated with a specific category.
- Click on a tile to open the Violations Explorer.

Reusing the Widget

You can use this widget with any compatible compliance category in your DTP system. See Adding Widgets for instructions on how to manually add the widget to your dashboard.

Security Impact Score

The dashboard adds an implementation of the Metrics - Summary widget configured to show metric data based on the running KPI slice. See Metrics - Summary for details on how to use this widget.



Security Impact Score

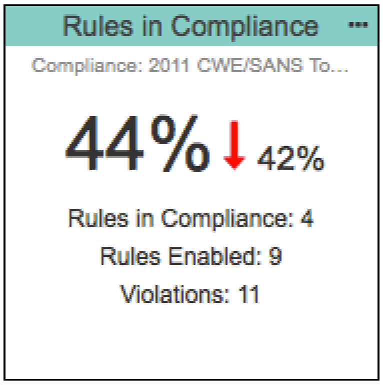
191.3

Sum

KPI - Security Impact

Rules in Compliance

The dashboard adds an implementation of the Rules in Compliance - Summary widget configured to show metric data based on the running KPI slice. See Rules in Compliance - Summary for details on how to use this widget.



Rules in Compliance

Compliance: 2011 CWE/SANS To...

44% ↓ 42%

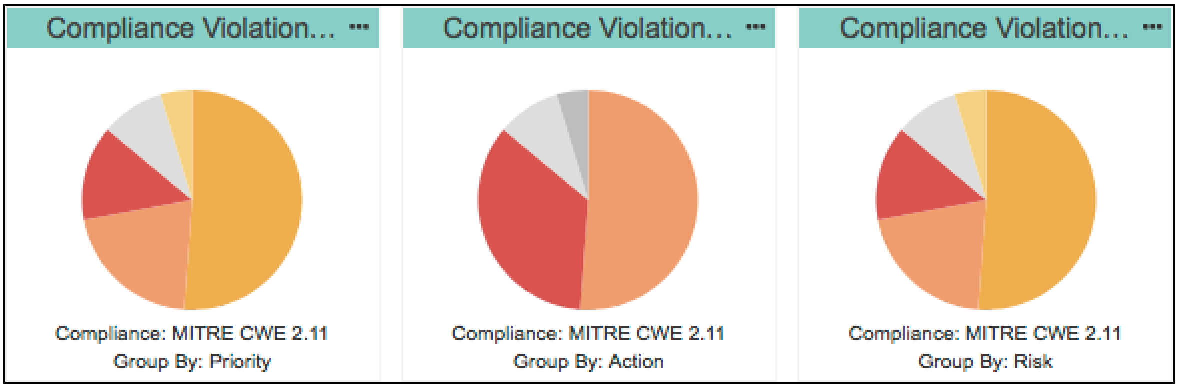
Rules in Compliance: 4

Rules Enabled: 9

Violations: 11

Compliance Violations by Metadata

This widget shows the distribution of Parasoft metadata (priority, action, and risk impact) associated with the violations reported in the filter. You can add an instance of the widget for each type of metadata. See Configuring CWE Widgets for details on configuring the widget.



Compliance Violation...

Compliance: MITRE CWE 2.11
Group By: Priority

Compliance Violation...

Compliance: MITRE CWE 2.11
Group By: Action

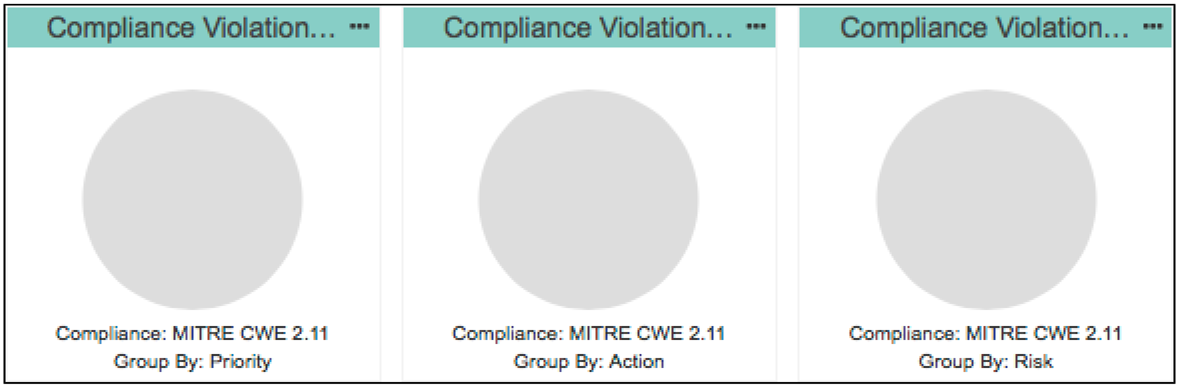
Compliance Violation...

Compliance: MITRE CWE 2.11
Group By: Risk

You can perform the following actions:

- Mouse over a segment in chart to view the number of violations tagged according to a specific metadata category.
- Click on a section to open the Compliance Violations by Metadata Report filtered by type of metadata.

For new projects or for projects in which the metadata has not been set, the chart will show undefined metadata for the violations reported.



You can manually set the metadata in the Violations Explorer (see Addressing Violations) or implement a flow as part of your build automation process to automatically set the metadata (see the How to Update Violations Metadata tutorial for additional information).

Reusing the Widget

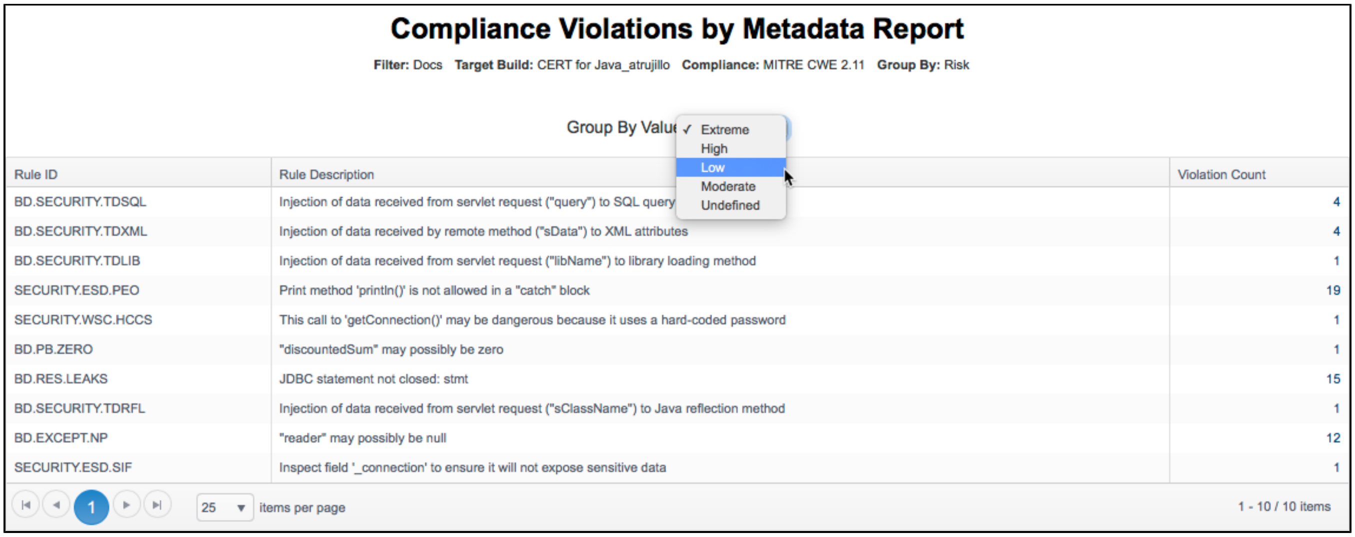
You can use this widget with any compatible compliance category in your DTP system. See Adding Widgets for instructions on how to manually add the widget to your dashboard.

Configuring CWE Widgets

Title	Enter a new title to replace the default title that appears on the dashboard.
Filter	Choose Dashboard Settings to use the dashboard filter or choose a filter from the drop-down menu.
Target Build	Choose a build from the drop-down menu. Only the data for this build will appear in the widget.
Compliance	Choose one of the following compliance category groups (see CWE Compliance Rule Categories for details): • MITRE CWE 2.11 • MITRE CWE 2.11 - Technical Impact • 2011 CWE/SANS Top 25 - Technical Impact • 2011 CWE/SANS Top 25 You can also choose any other compliance category available in DTP.
Group by	Choose a type of metadata to group by in the widget (priority, action, and risk impact). This settings is only available for the Compliance Violations by Metadata widget.

Compliance Violations by Metadata Report

This report shows the violations grouped by priority, risk, or action depending on the configuration of the widget you clicked to open the report.



Compliance Violations by Metadata Report

Filter: Docs **Target Build:** CERT for Java_atrujillo **Compliance:** MITRE CWE 2.11 **Group By:** Risk

Group By Value

Rule ID	Rule Description	Violation Count
BD.SECURITY.TDSQL	Injection of data received from servlet request ("query") to SQL query	4
BD.SECURITY.TDXML	Injection of data received by remote method ("sData") to XML attributes	4
BD.SECURITY.TDLIB	Injection of data received from servlet request ("libName") to library loading method	1
SECURITY.ESD.PEO	Print method 'println()' is not allowed in a "catch" block	19
SECURITY.WSC.HCCS	This call to 'getConnection()' may be dangerous because it uses a hard-coded password	1
BD.PB.ZERO	"discountedSum" may possibly be zero	1
BD.RES.LEAKS	JDBC statement not closed: stmt	15
BD.SECURITY.TDRFL	Injection of data received from servlet request ("sClassName") to Java reflection method	1
BD.EXCEPT.NP	"reader" may possibly be null	12
SECURITY.ESD.SIF	Inspect field '_connection' to ensure it will not expose sensitive data	1

items per page

1 - 10 / 10 items

The report is filtered by the widget segment you clicked, but you can use the Group By drop-down menu to filter the report by different metadata values.

You can also click on a link in the Violation Count column to open the Violations Explorer.