# Static Application Security Testing Process

## Introduction

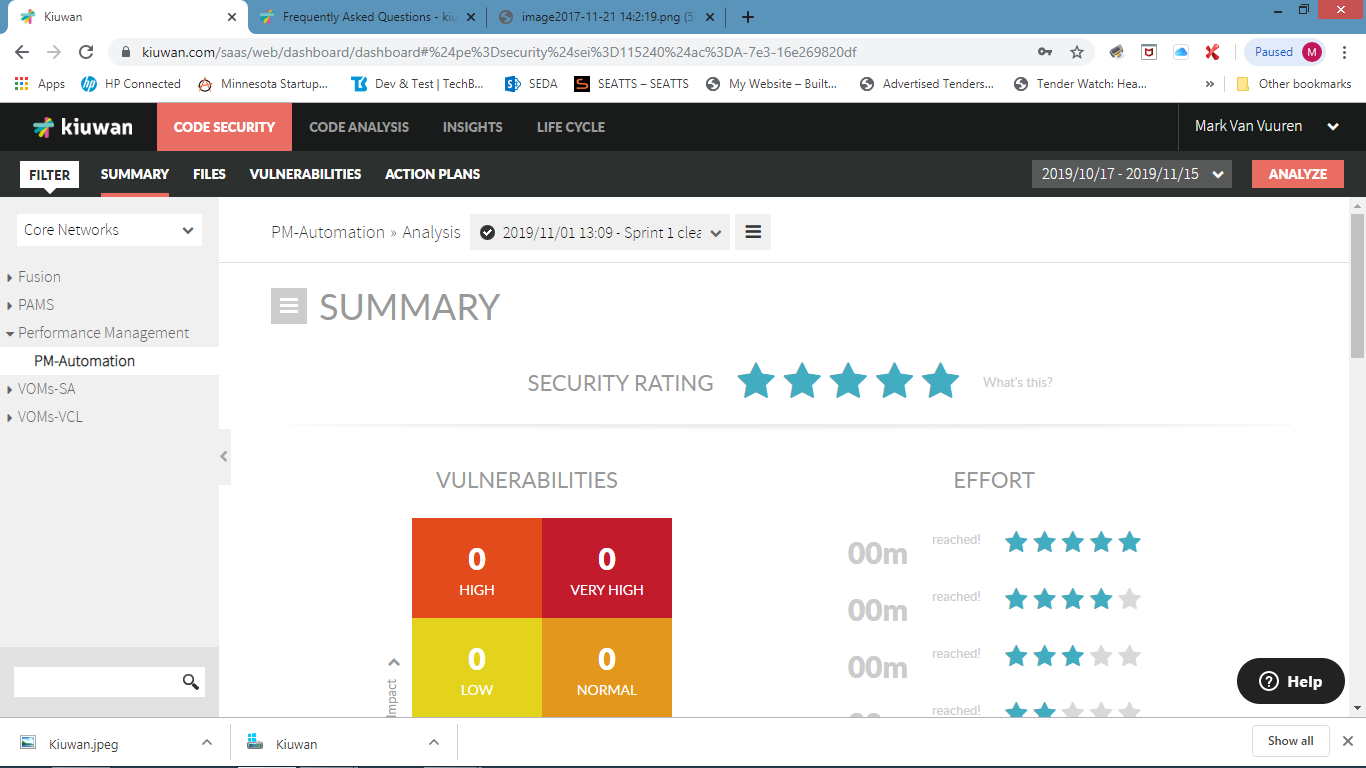
https://www.kiuwan.com/docs/display/K5/Security+and+Quality+Indicators

Vodacom have implemented Kiuwan in the Core Networks division in order to:

* To detect security vulnerabilities early and fix them before they are deployed;
* To reduce the number of bugs affecting the performance and efficiency of their software;
* To manage the costs associated with development and maintenance properly;
* To gain greater control of their application development.

This document provides a guideline to new users for the Security Analysis component, however the Code Analysis component operates in a very similar manor.

The SDLC has been modified to incorporate the scanning and remediation of source code before the code is handed to Testing and a final scan before operations will accept the application for deployment. Vodacom will not accept an application with High or Very High vulnerabilities and it is important to build the use of Kiuwan into the developers coding process as early as possible. Estimated effort to fix vulnerabilities is calculated enabling decisions to be made about how much can be fixed based on time constraints of developers.

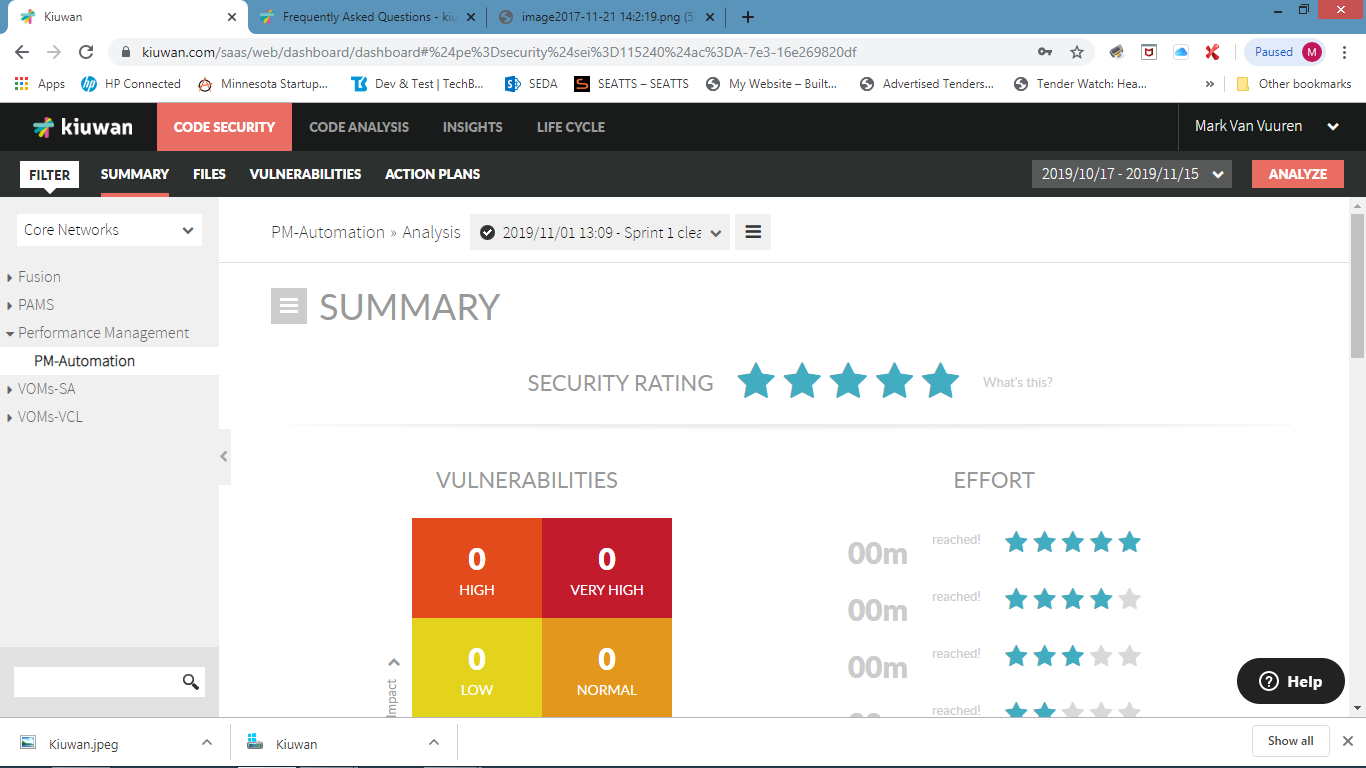


Scan - Deploy

Penetration Testing



Develop – Scan - Remediate



## On Boarding New Users

In order to gain access to Kiuwan, an email request should be sent to the administration team namely:

Phiko Genge - Phikolomzi.Genge@vodacom.co.za

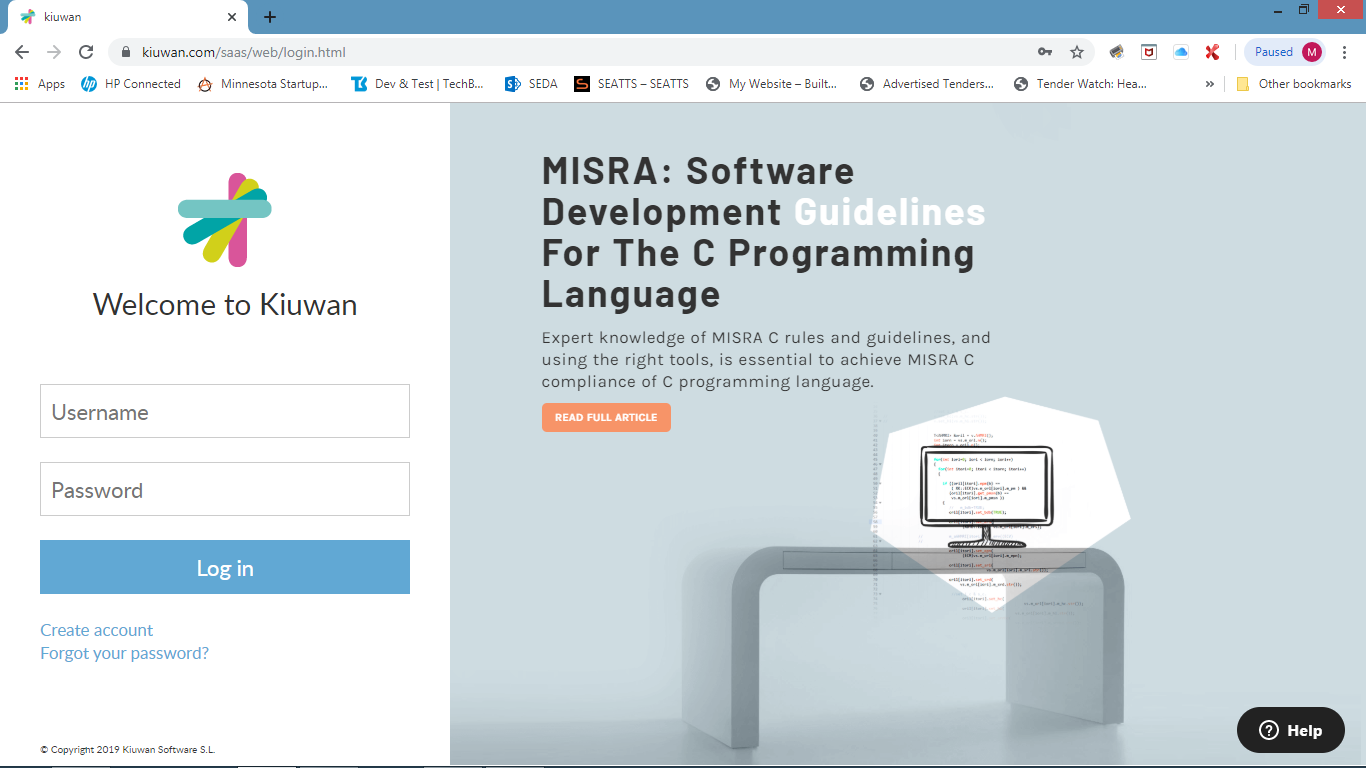
Eliah Mulaudzi, - Eliah.Mulaudzi@vcontractor.co.za

The request should contain your name and email address, Division and Business Unit and the names of the applications to scan.

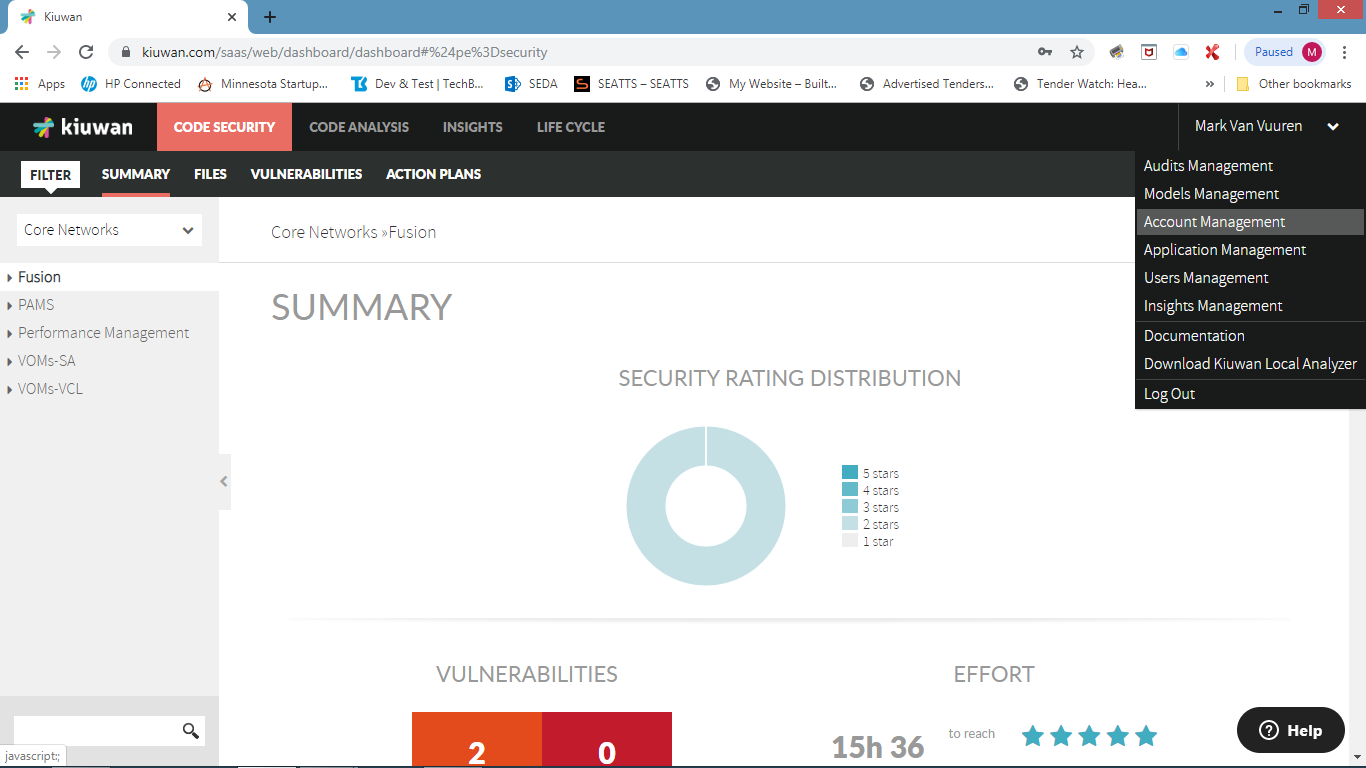
The Kiuwan administrators will add users as well as applications and a notification will be emailed to new users and will contain user name, password as well as a link to the Vodacom Kiuwan implementation.

## How to Use Kiuwan

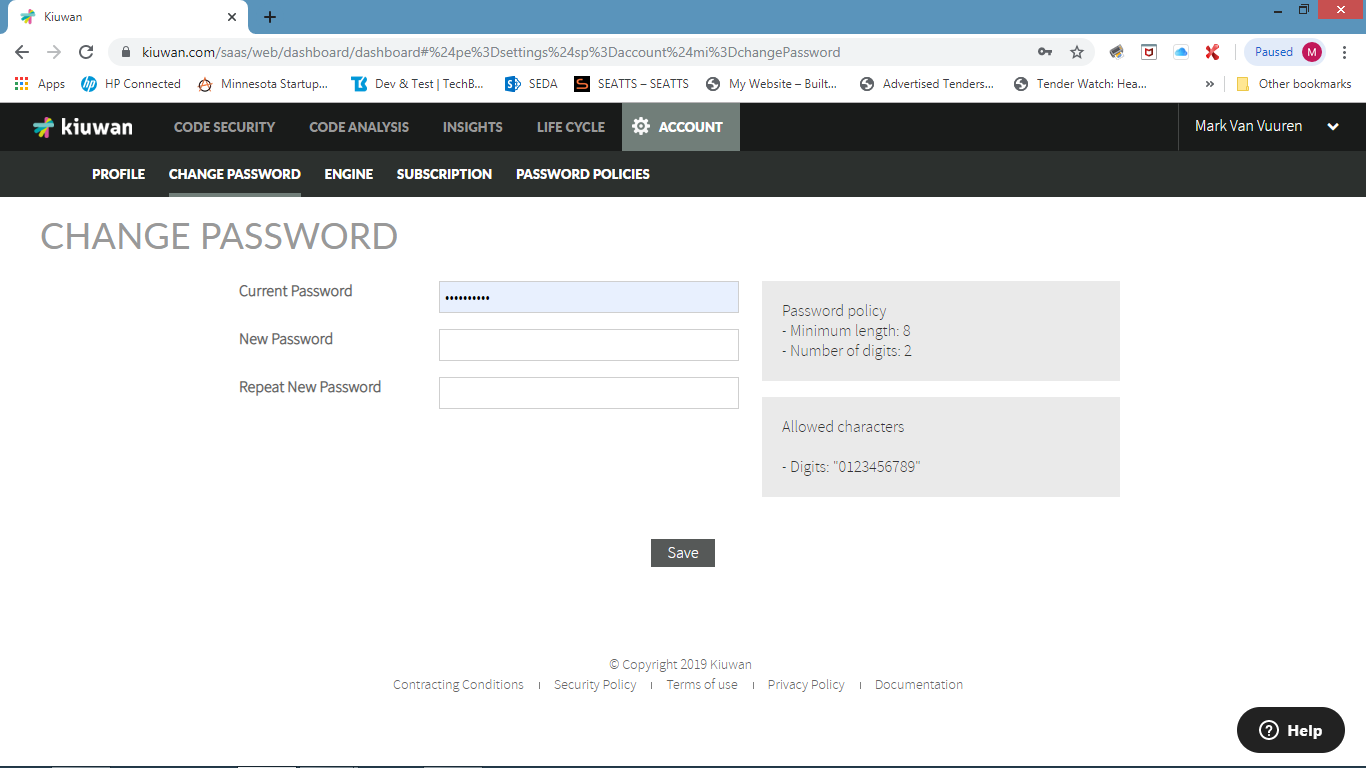
Click on the [www.kiuwan.com](http://www.kiuwan.com) link and log in.



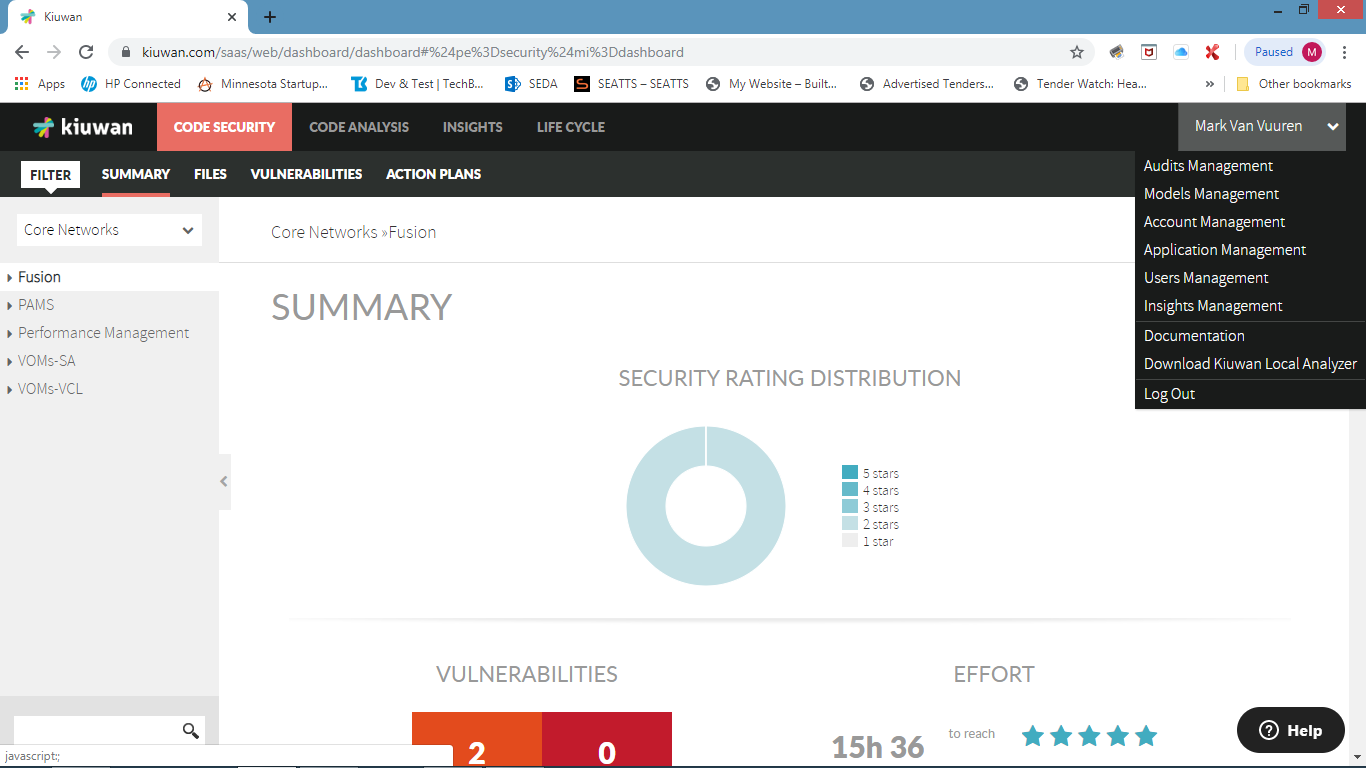
Once logged in, a user can change their password by clicking on the name at the top right of the screen and selecting Account Management.



Select Change Password and enter a new password



The next step is to select Download Kiuwan Local Analyzer (KLA) from the menu.



Once the KLA has downloaded, ensure you have a recent or latest JDK / JRE installed and unpack the download on your local machine

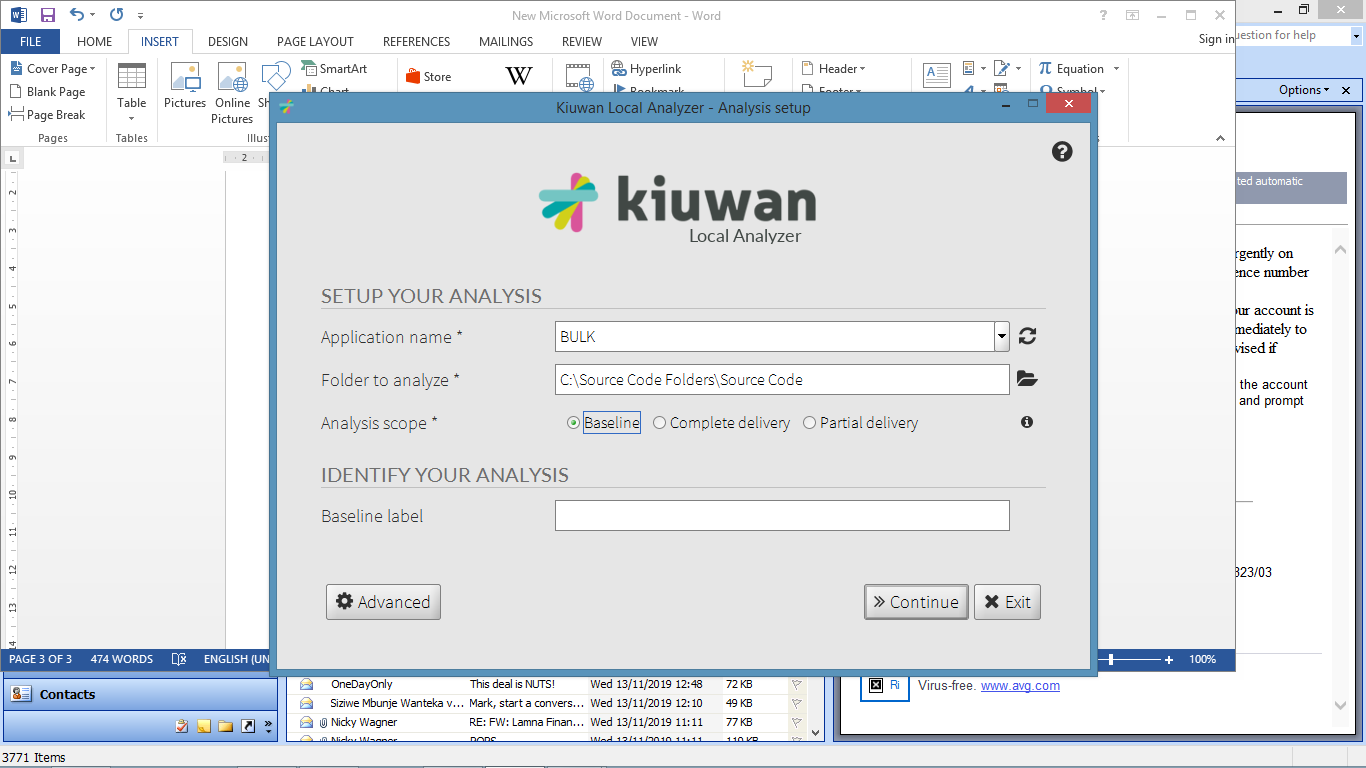
Start the KLA by running \install directory\KiuwanLocalAnalyzer\kiuwan.cmd and log in.



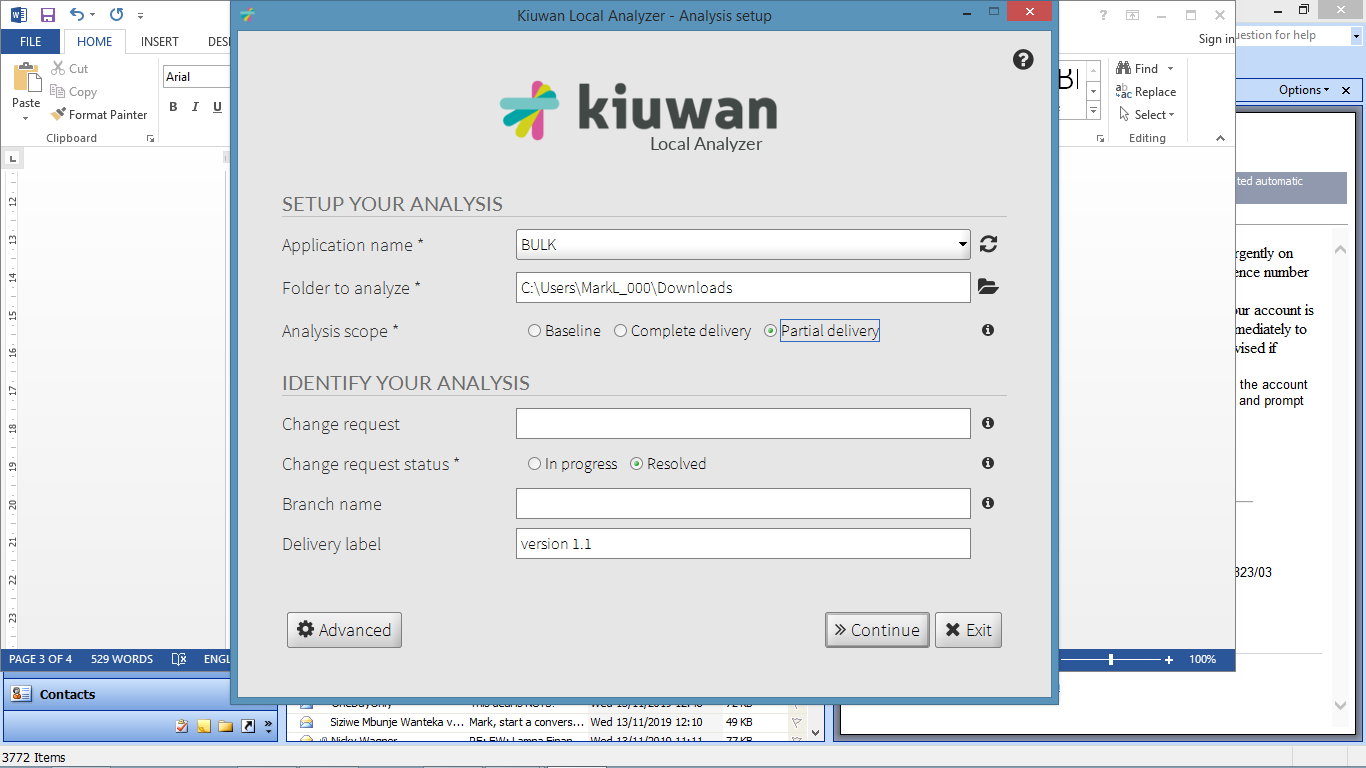
Once logged in select the application which was set up by the Kiuwan administrator.



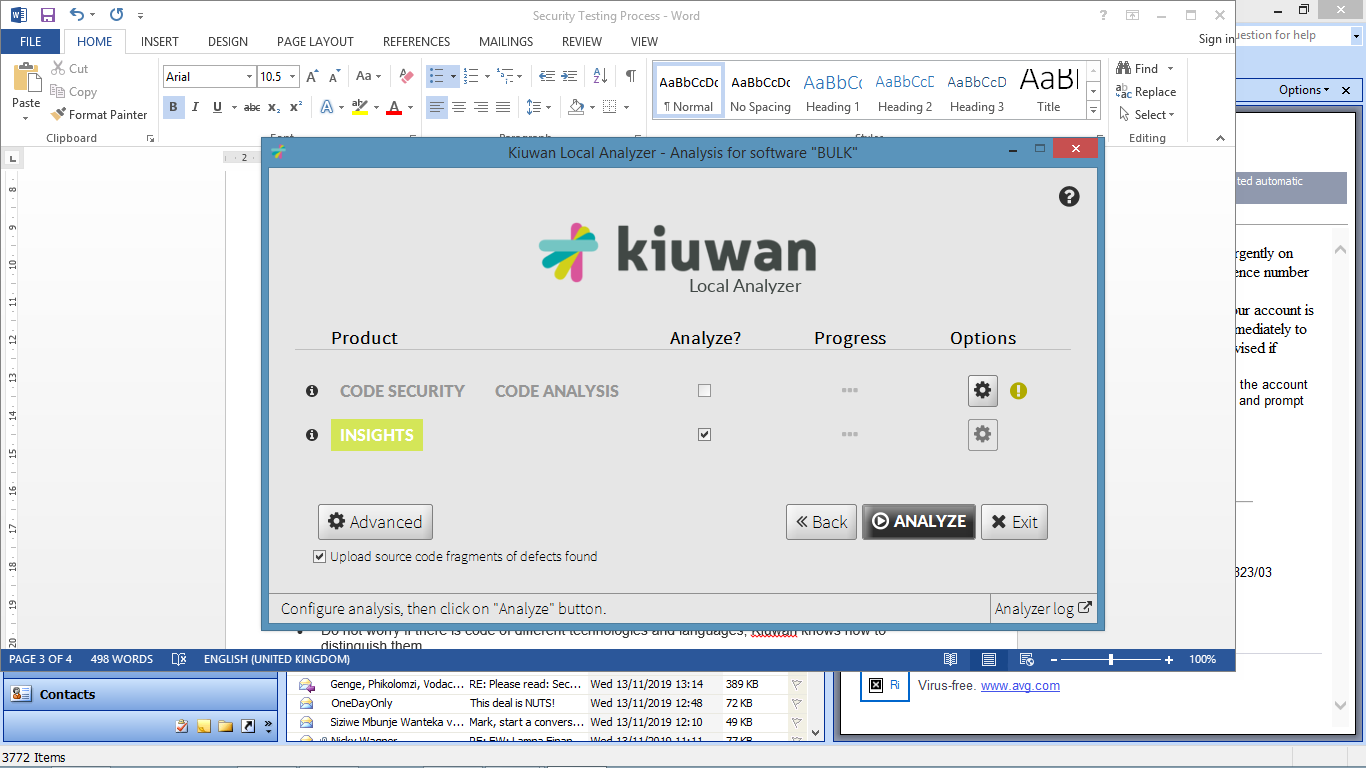
Point to the directory that contains the source code. If this is your the scan select Baseline and provide a label that is meaningful e.g. the version of the application, then select Continue



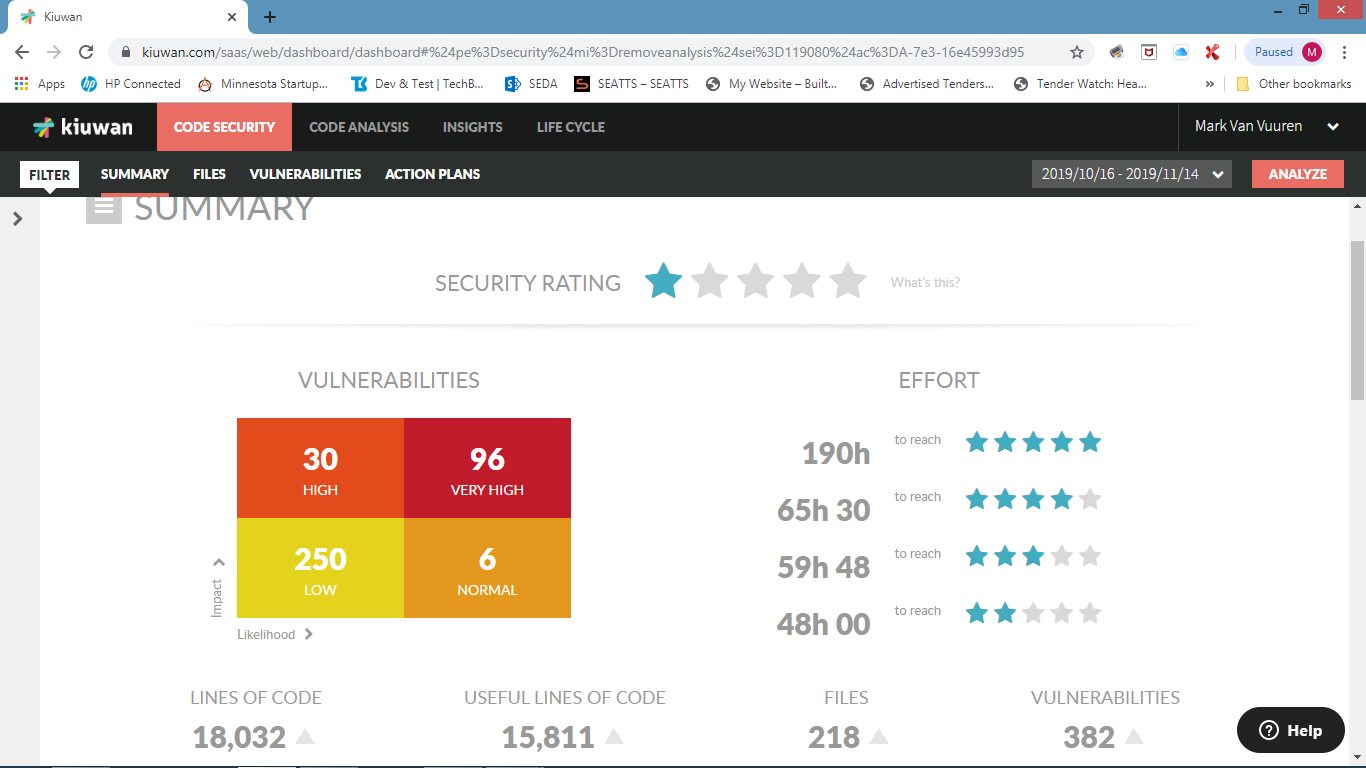
Kiuwan provides the ability to do partial analysis to enable developers to run scans when developing blocks of code. When partial delivery is selected Change request, Branch name and Delivery label can be inputed.



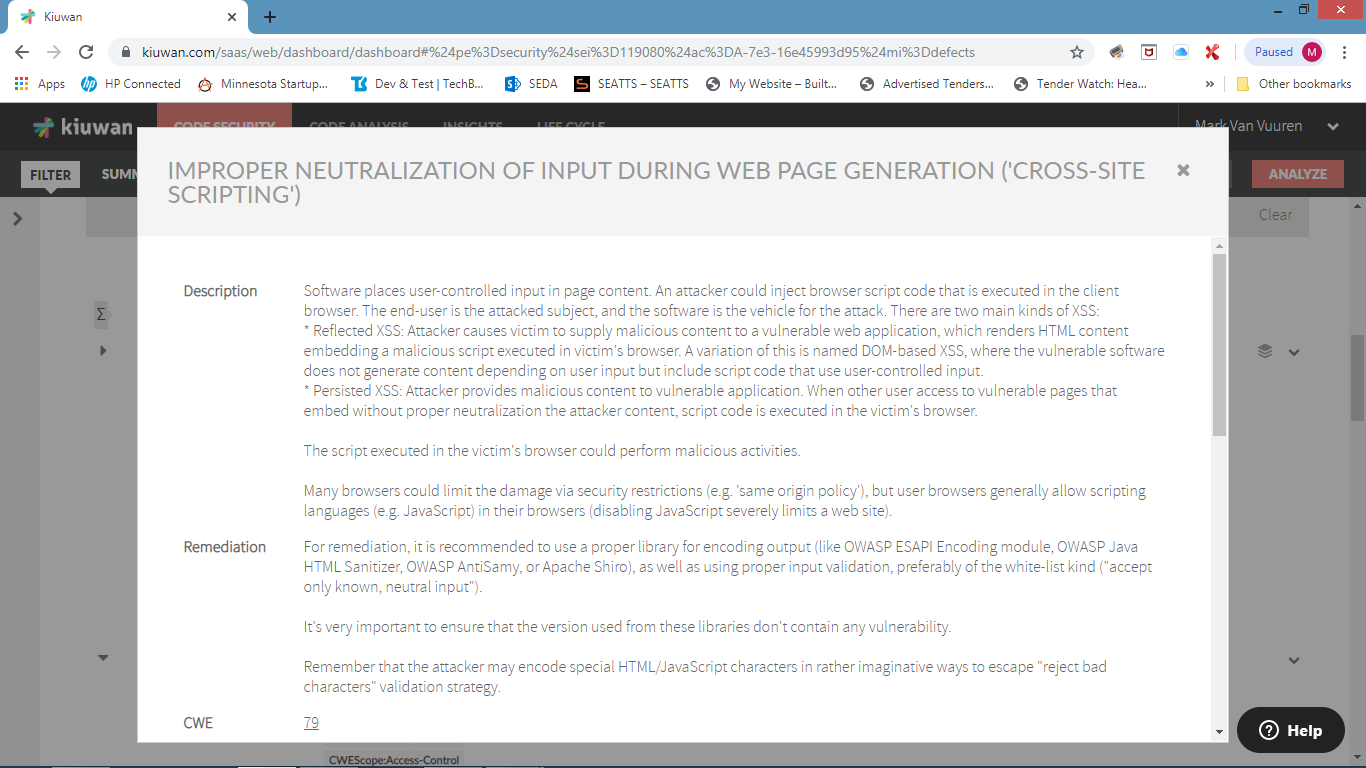
Select Code Security Code Analysis checkbox. If the application includes open source and/or third party libraries Select the Insights check box and click ANALAYSE

.

The results can then be viewed from the Dashboards.

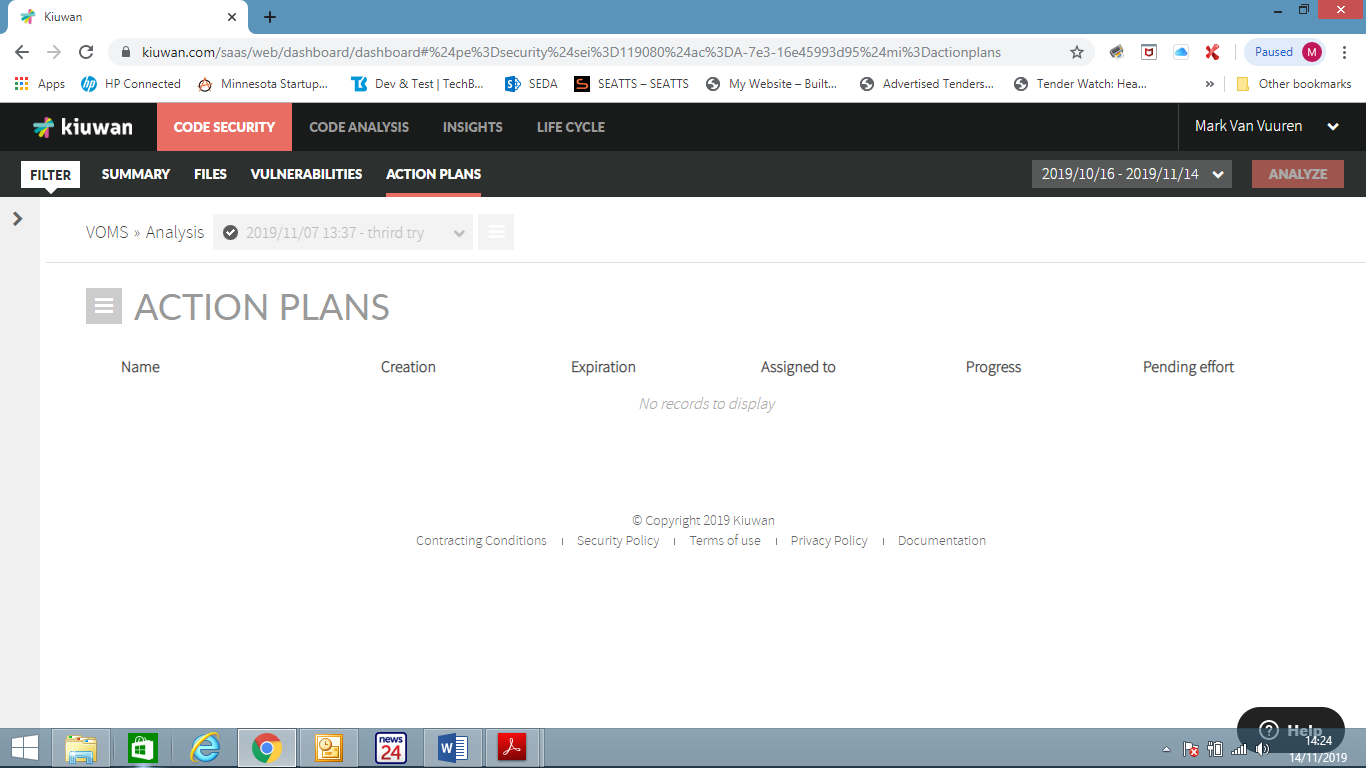


Select Vulnerabilities to analyse each vulnerability. Kiuwan provides a detailed description of each vulnerability as well as an example of how to fix it. You access this by clicking on the question mark next to each vulnerability.

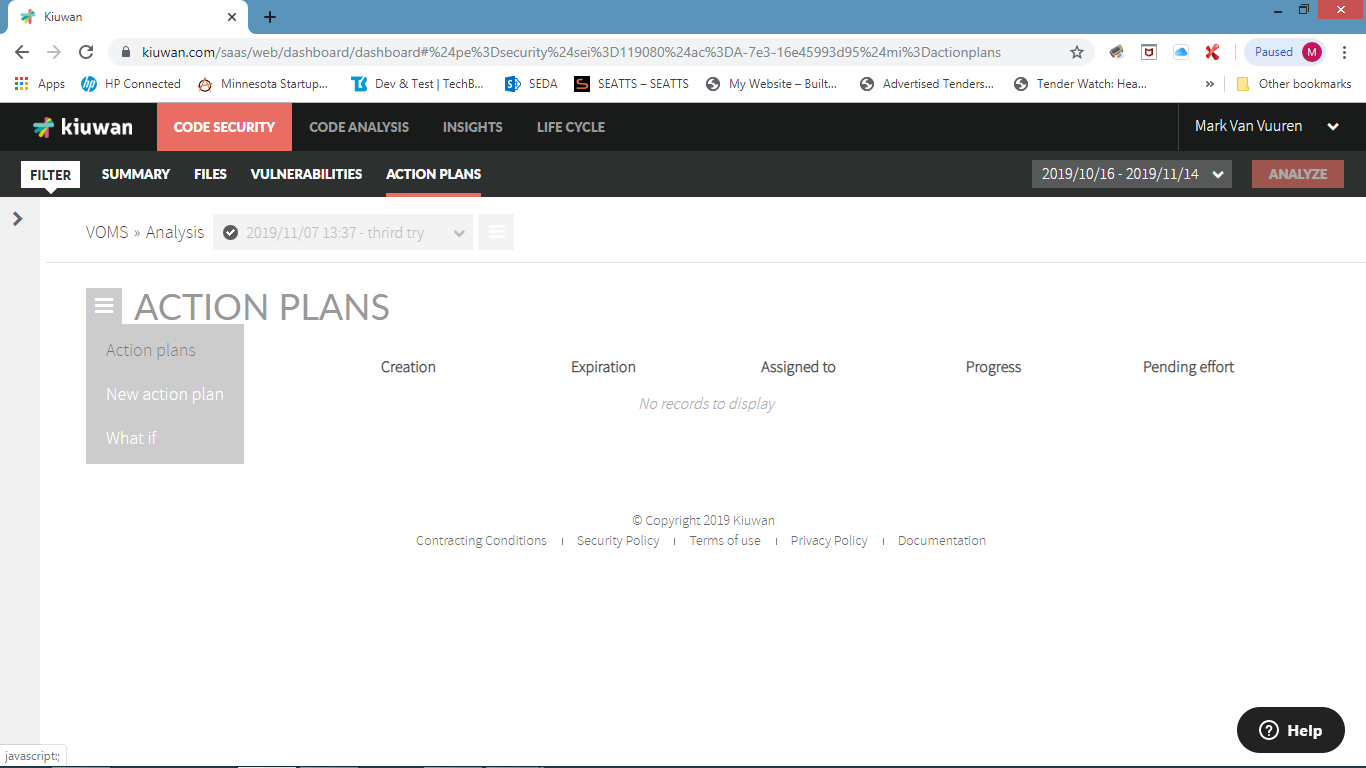


 The ability is provided to mute vulnerabilities should it be established they are not applicable or are duplicates.

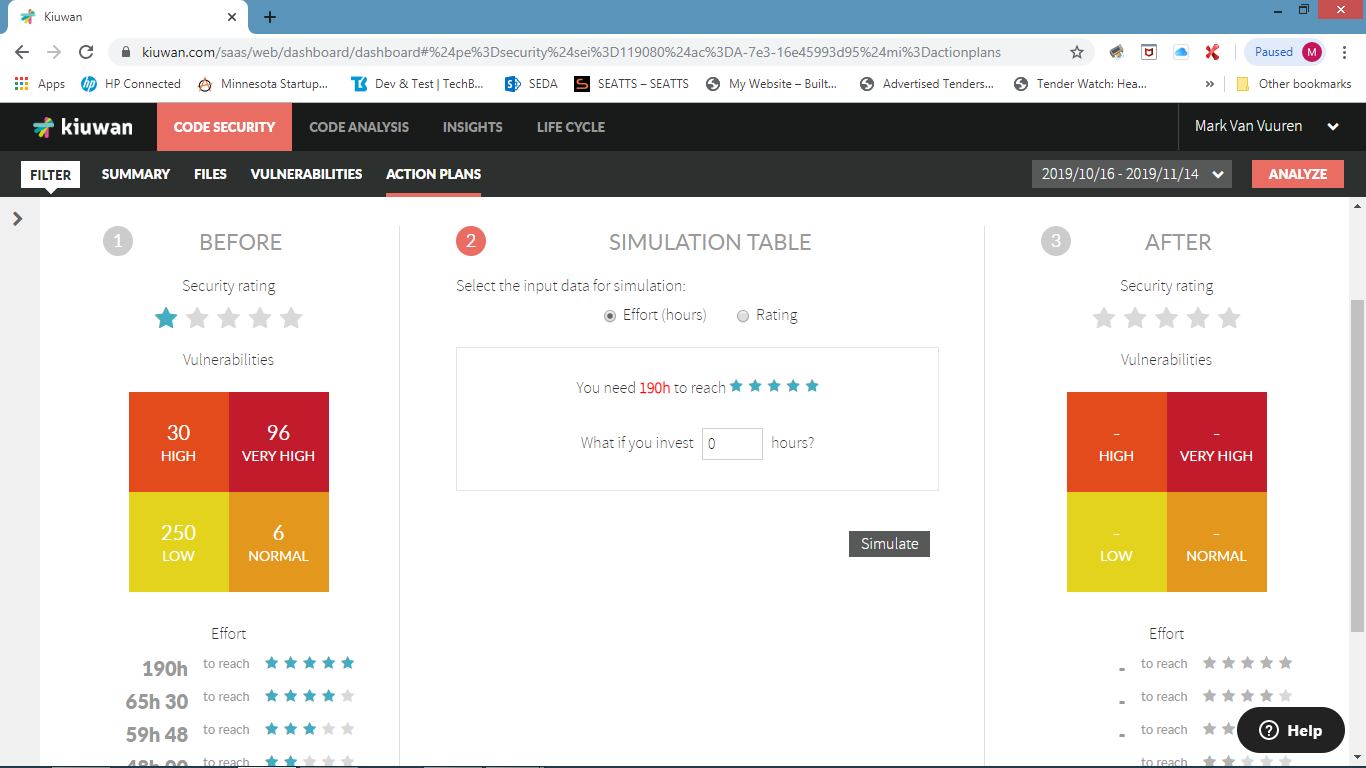
Once analysis has been completed the ability is provided to create Action Plans for remediation. Click on Action Plans.



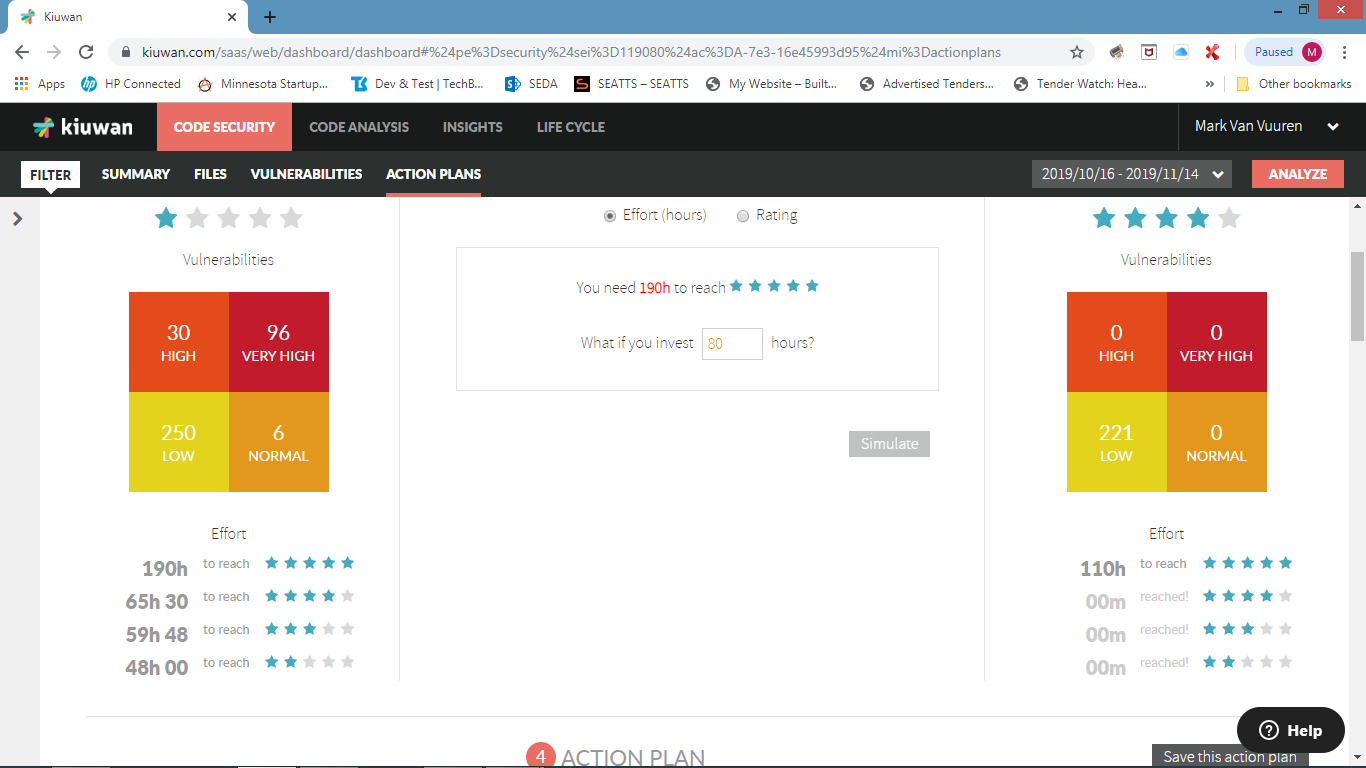
 Select What If from the menu to establish the most efficient action plan give time and effort constraints.



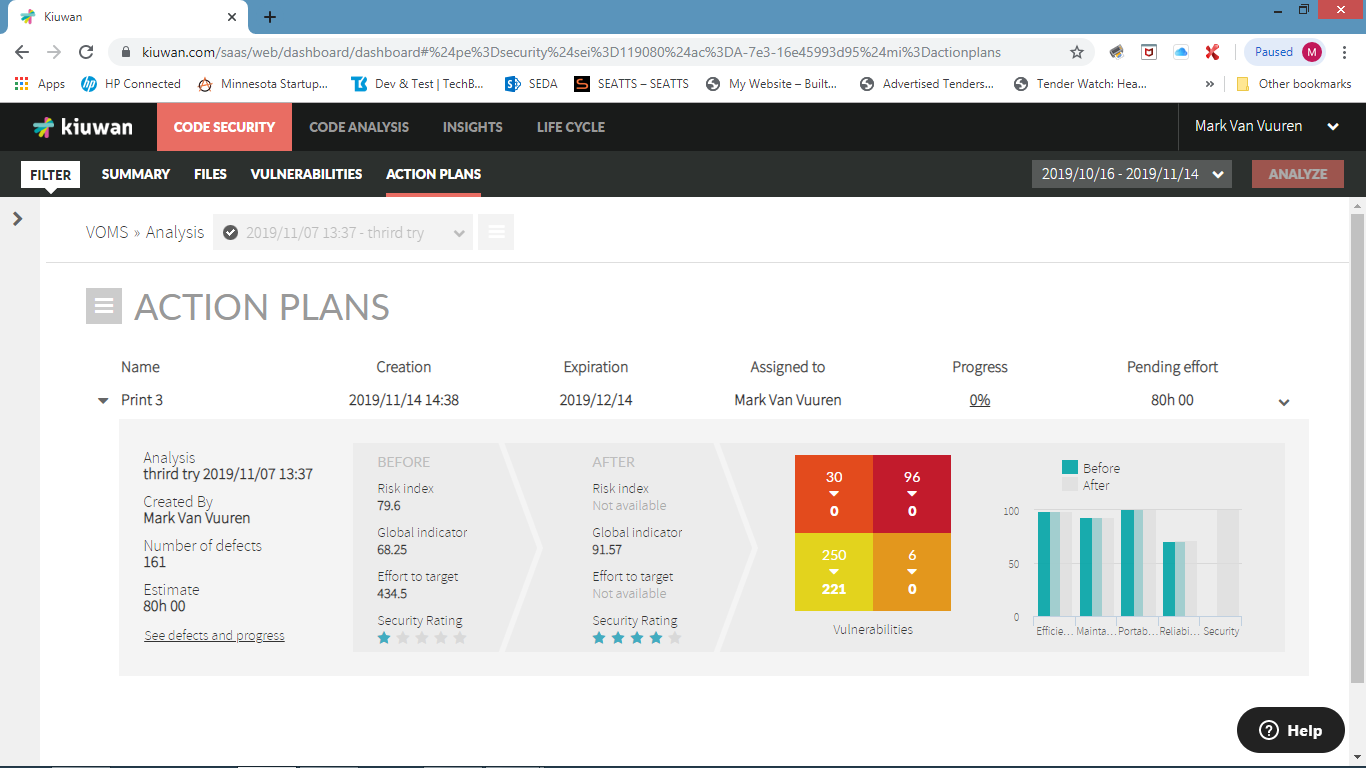
The simulation table allows for Effort, where you plug in available hours, or Rating where you select a particular star rating ranked from 1 to 5. When the simulate button is pushed Kiuwan will select as many vulnerabilities within the parameters provided as possible, beginning with the very high items.



In this example 80 hours was inputted and the After picture details the vulnerability count after all issues are addressed.



Select Save the Action Plan and Kiuwan will then group all vulnerabilities that need to be fixed and will track the progress as the vulnerabilities are fixed and further scans are run.



Once the Action Plan is complete the application can then be handed over to Testing together with the Report. Vodacom will not accept the hand over if there are very high and high vulnerabilities.