Wymagania w zakresie systemu SAST:

1. Oprogramowanie SAST może być  dostarczone w modelu usługi SaaS

2. Narzędzie musi oferować funkcjonalność Static Application Security Testing (SAST).

**3. Wspierane języki programowania i framework**

3.1. Oprogramowanie SAST musi umożliwiać analizę kodu źródłowego pod kątem występujących podatności, minimum dla wskazanych języków programowania: C, C++, C#, Objective-C, Java, JavaScript, Python, Ruby, PHP, HTML 5, ASP, PL/SQL, VBScript, Kotlin, VB, APEX, Perl, [VB.NET](http://vb.net/), SCALA, Go.

3.2. Oprogramowanie SAST musi umożliwiać analizę zewnętrznych bibliotek Opensource pod kątem znanych podatności.

3.3  Narzędzie powinno wspierać biblioteki i frameworki takie jak: React, React Native, Apache Cordoba, Xamarin, .NET, Ionic, Unity, Spring, AngularJS

**4.  Wykrywane podatności**

Oprogramowanie SAST musi:

4.1. pozwalać na analizowanie kodu aplikacji pod kątem występowania podatności wymienionych w rankingach OWASP TOP 10 oraz rankingach CWE TOP 25 dla wskazanych w pkt. 3.1 jezyków programowania;

4.2. minimalizować liczbę wyników fałszywie pozytywnych (tj. wyników błędnie uznanych za szkodliwe) oraz udostępniać mechanizmy pozwalające na weryfikację wykrytych podatności automatycznie lub z minimalnym nakładem pracy;

4.3 kategoryzowanie oraz priorytetyzowanie znalezionych podatności;

4.4. wspierać automatyzację wykrywania podatności oraz udostępniać możliwość modyfikacji polityk skanowania, reguł oraz powiadomień;

4.5. umożliwiać skanowanie kodów aplikacji mobilnych pod kątem podatności;

4.6. umożliwiać skanowanie kodów aplikacji mobilnych, desktopowych oraz webowych;

4.7. umożliwiać skanowanie wielu gałęzi repozytorium kodu jednocześnie;

4.8. umożliwiać skanowanie aplikacji podzielonych na mikroserwisy.

**5. Generowanie raportów**

Oprogramowanie SAST musi :

5.1. umożliwiać eksport wyników skanowań co najmniej w formatach pdf, csv, html;

5.2. umożliwiać generowanie raportów poprzez interfejs API;

**6. Aplikacje mobilne**

Oprogramowanie SAST musi umożliwiać przeprowadzanie skanów aplikacji mobilnych pod kątem podatności bezpieczeństwa dla platform iOS oraz Android

**7. Automatyzacja w procesach CI/CD**

Narzędzie powinno łączyć się z systemami CI/CD: Jenkins, Bitbucket Pipelines, Github Actions, Azure DevOps, inne niewymienione przez REST API

**8. Analizy kodu źródłowego**

Oprogramowanie SAST musi:

8.1. umożliwiać skanowanie kodów źródłowych oraz plików binarnych z nich wynikających

8.2. umożliwiać skanowania kodu źródłowego z repozytoriów GIT;

8.3. pozwalać na konfigurację kryteriów do analizy kodu źródłowego  
 **9. Polityki skanowania**

Oprogramowanie SAST musi:

9.1. umożliwiać modyfikację reguł skanowania dostarczonych przez producenta.

9.2. umożliwiać wykonywanie skanów inkrementalnych i różnicowych po wprowadzeniu zmian

9.3. umożliwiać konfigurację różnych polityk i reguł dla różnych aplikacji

9.4. filtrować wyniki skanów, dodawać własne reguły oraz wykluczać niektóre podatności na podstawie filtrów

**10. Zarządzanie**

Oprogramowanie SAST musi posiadać co najmniej następujące interfejsy administracyjne:

10.1. Zarządzanie poprzez GUI przy wykorzystaniu protokołu HTTPS, pozwalające na pełne zarządzanie aplikacją;

10.2. Zarządzanie poprzez API REST za pomocą, którego możliwe jest również uruchomienie skanowania.

**11. Wyniki skanowania**

Oprogramowanie SAST musi umożliwiać:

11.1. filtrowanie wyników skanów, dodawanie własnych reguł oraz wykluczać niektóre podatności na podstawie filtrów

11.2. udostępnianie dokumentacji o wykrytych podatnościach oraz możliwościach ich usunięcia wraz z przykładami

11.3. wskazanie miejsca, w którym występują błędy bezpieczeństwa

**12. Zgodności z  standardami**

Oprogramowanie SAST musi pozwalać na konfigurację polityk oraz raportów dla zgodności ze standardami OWASP TOP 10.

**13. Repozytoria kodu**

Narzędzie powinno łączyć się z repozytoriami kodów: Bitbucket Github, Gitlab..

**14. Integracje**

14.1. Oprogramowanie SAST powinno umożliwiać integrację z IDE (ang. Integrated Developer Environment);

14.2. Narzędzie powinno łączyć się ze zintegrowanymi środowiskami deweloperskimi: Visual Studio Code, Visual Studio, IntelliJ, Eclipse, Xcode, Android Studio

14.3. Oprogramowanie SAST powinno umożliwiać integrację z oprogramowaniem JIRA firmy Atlassian.