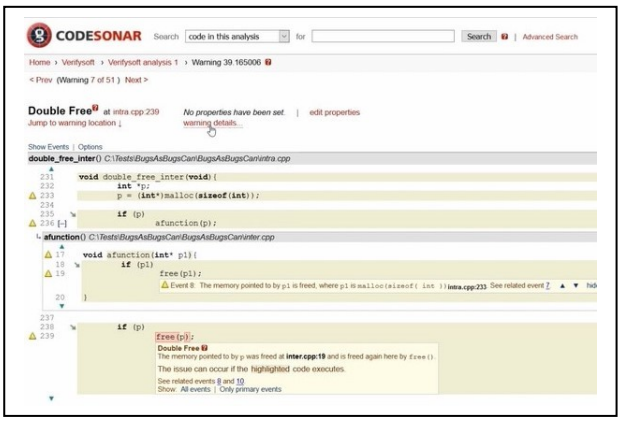
Statische Codeanalyse mit Grammatech CodeSonar

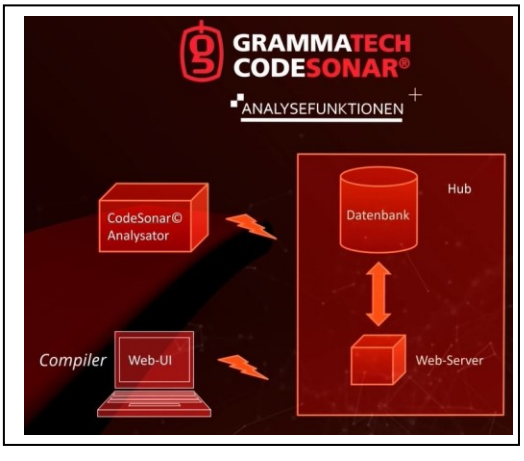
Software-Entwicklungsteams stehen unter ständigem Zeitdruck. Mehr Funktionalitäten mit immer höherer Komplexität, Qualität und Sicherheit zu liefern steht auf der Tagesordnung. Fehler im Software-Code können drastische Auswirkungen haben und zu Vermögens- und Personenschäden führen.
Software-Fehler so früh wie möglich in der Entwicklungsphase aufzuspüren ist deshalb essentiell, denn die Kosten für Fehlerkorrekturen steigen im weiteren Verlauf der Entwicklung fast exponentiell an.

Static Application Security Testing (SAST) ist eine bewährte “Best Practice”-Methode, um hochwertigen Code in kurzen Zeiträumen zu entwickeln. Um Fehler früh in der Entwicklung aufzuspüren haben sich Statische Analysetools bewährt, die sich jedoch stark in Leistungsfähigkeit und Qualität unterscheiden.



GrammaTech CodeSonar klinkt sich in Compilerprozesse ein, analysiert dabei das Projekt und erstellt einen aussagekräftigen Report. Auf einer benutzerfreundlichen Oberfläche kann anschließend jede Fehlermeldung separat angesteuert werden. Mit umfangreichen Informationen zum Codeverständnis die helfen Probleme und potenzielle Sicherheitslücken schnell zu finden und zu beheben. Die Ergebnisse können danach in verschiedenen Formaten exportiert und weiterverarbeitet werden. GrammaTech CodeSonar ist somit nicht nur ein führendes statisches Codeanalysetool für Entwickler, sondern auch eine Lösung für Manager sowie Verantwortliche für funktionale Sicherheit und Angriffssicherheit.

Analysefunktionen / statische Codeanalyse



Grammatech CodeSonar unterstützt die Quellcodeüberprüfung der wichtigsten Programmiersprachen wie C, C++, C#, Java, Python sowie die Prüfung von Quellcode für Android.
CodeSonar besteht aus einem Hub, welcher die Ergebnisse aufnimmt. Der Hub bestehend aus Webserver, auf den wir uns aufschalten können, um die Ergebnisse ansehen zu können, sowie einer Datenbank, welche die entsprechenden Findings persistiert. Weiter haben wir - unabhängig davon - den eigentlichen Analysator, der sich über das Netzwerk mit dem Hub verbindet, um dann die Analyseergebnisse aufzuspielen. Wichtig ist, dass die Analyse dort stattfinden muss, wo das Bildsystem installiert ist, d.h.es muss auf der Maschine, auf der ich analysiere ein Compiler vorhanden sein, da CodeSonar sich in den Compilerprozess einklinkt, um Informationen zu sammeln, wo der Quellcode für das Projekt liegt. Durch die Compilerabfrage ist es dann auch möglich Makrosettings mitauszulesen, die wichtig sind für CodeSonar um den Quellcode parsen zu können.

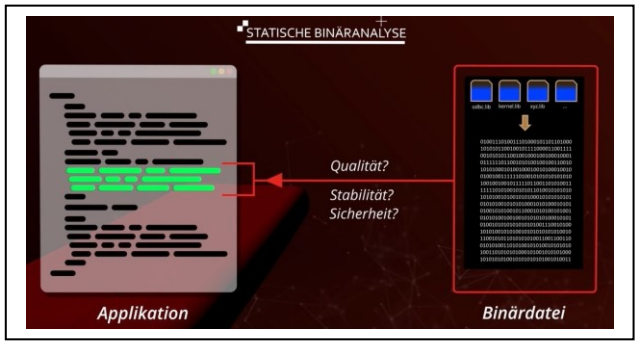
Code Sonar in Action

GrammaTech Code Sonar scannt nach Compiler-Prozessen. Wenn diese zugelassen sind, klinkt sich Code Sonar in den Compiler-Prozess ein und parst die ausgeführte Datei analog zum Compiler. CodeSonar erstellt intern Modelle, analysiert das Projekt und erstellt einen Report.

Breite Compilerabdeckung

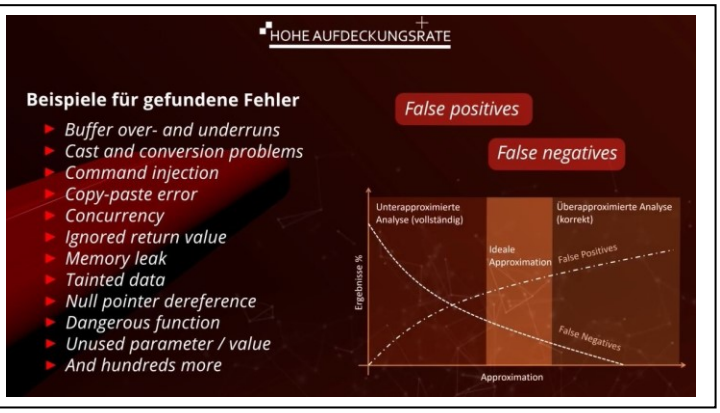
CodeSonar bietet für die Analyse der unterschiedlichen Programmiersprachen eine breite Compilerabdeckung. Weitere Compiler bzw. werkseitig nicht unterstützte Typen und Derivate können in einfachen Schritten schnell und unkompliziert hinzugefügt werden.

Statische Binäranalyse



Vielfach werden in Applikationen von Drittanbietern gelieferte Komponenten (Bibliotheken) eingebunden. Da diese oft nur als Binärdateien vorliegen, lassen sich Zweifel an deren Qualität nur schwer ausräumen und die Stabilität und Sicherheit der Gesamtapplikation steht in Frage. CodeSonar for Binaries geht mit seiner Analyse über den Quellcode hinaus und detektiert kritische Fehler auch in Binärdateien, die auf C oder C++ Quellcode basieren und die Instruction Sets x86 und ARM verwenden.

Hohe Aufdeckungsrate



Als führendes Werkzeug zur statischen Quellcodeanalyse weist CodeSonar im Vergleich zu vielen anderen statischen Analysetools nicht nur eine bessere Fehlererkennung auf, es zeichnet sich zudem durch eine vergleichsweise geringe Rate an Fehlwarnungen (False Positives & False Negative) aus. Code Sonar bietet also eine hohe Aufdeckungsrate bei hoher Genauigkeit und Vollständigkeit und somit eine ideale Approximation.

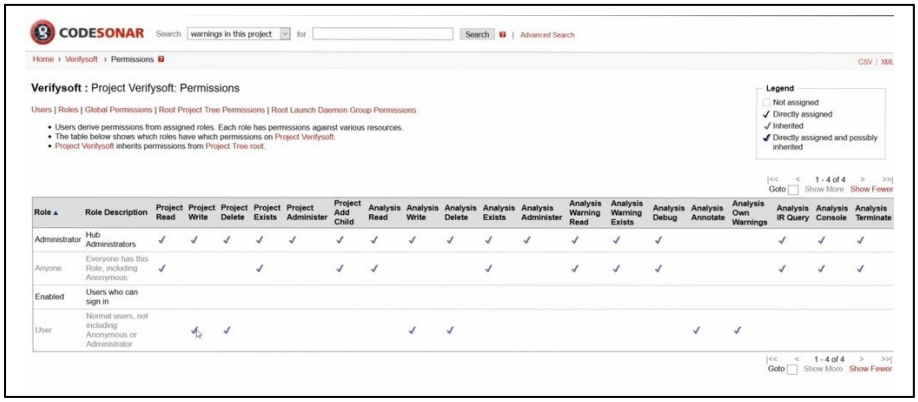
Hohe Anzahl von Prüfungen

Die sich beschleunigenden M2M- und IoT-Trends vernetzter Systeme erhöhen die Gefahr möglicher Angriffe durch Cyberkriminelle. Code Sonars große Anzahl von Checkern ermöglicht das Auffinden einer Vielzahl von kritischen Fehlern, so dass Sie die Risiken von Sicherheitsverletzungen durch Cyberkriminalität präzise und effizient beseitigen können. Die Warnklassen von CodeSonar unterstützen auch mehrere Coding-Initiativen, darunter die CWE, um die Einhaltung von Industriestandards bei der Softwareentwicklung effizient und effektiv zu gestalten.

Nebenläufigkeitsprüfungen

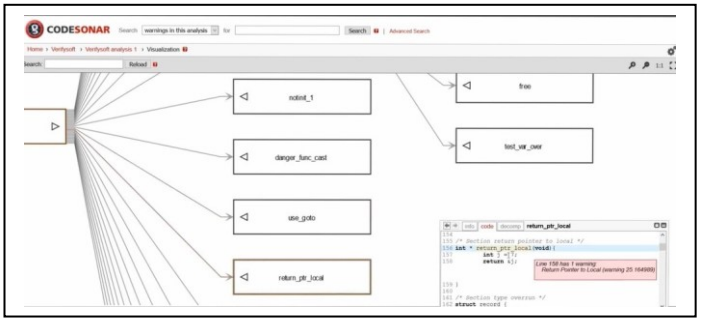
Nebenläufigkeitsprobleme wie Race-Conditions und Synchronisationsfehler wie Deadlocks deckt CodeSonar durch Verwendung interner Laufzeitmodelle zuverlässig auf.

Aussagekräftige Reports – gut dokumentierte Ergebnisse



CodeSonar zeichnet sich durch eine benutzerfreundliche Oberfläche aus, in welcher es seine Ergebnisse als Warnungen ausgibt, die durch eine gute Doku-mentation leicht ver-ständlich sind. Jede Fehlerwarnung kann separat angesteuert werden und liefert umfangreiche Informationen und Erklärungen mit Pfadinformationen. Des Weiteren bietet CodeSonar umfassende Funktionen für das Codeverständnis und hilft Entwicklern, Probleme schnell zu finden, zu verstehen und zu beheben.
Eine rechtliche Trennung durch ein rollenbasiertes Zugriffssystem (RBAC) ermöglicht die logische Trennung von Projekten und Rechtebereichen.

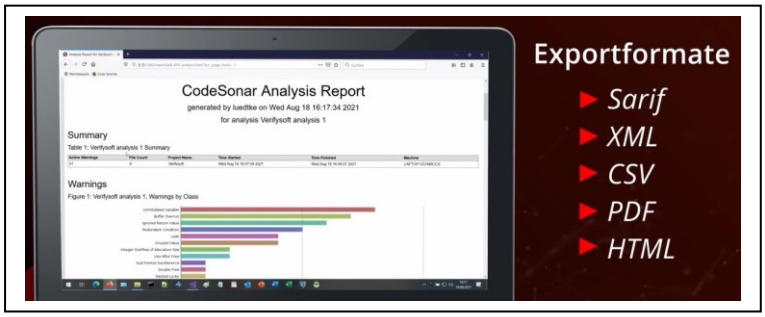
Architektur-Visualisierung



Die Architektur-Visualisierung des Call-Trees gibt für Quellcode- und Binärdateien zudem ein Verständnis dafür, wie die verschiedenen Komponenten eines Softwaresystems zusammenarbeiten, wie sich eine Funktion in eine größere Anwendung einfügt und hilft durch das gesamte Programm zu navigieren.

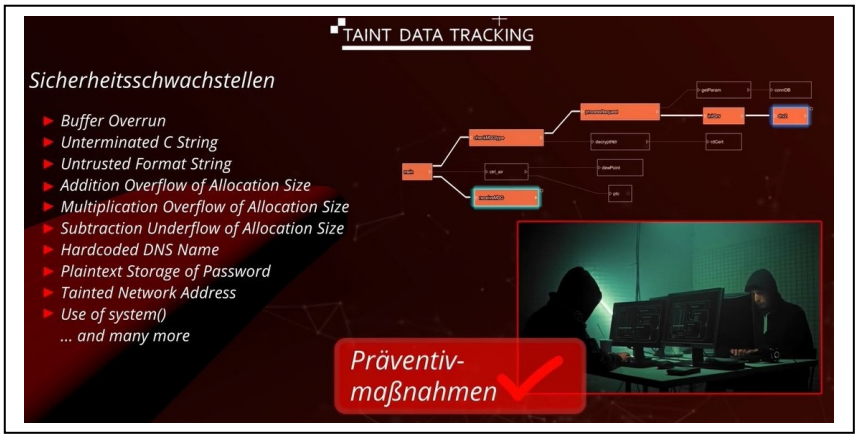
Dadurch ermöglicht CodeSonar entscheidende Aspekte von Software zu erkunden: Subsysteme, Schnittstellen, Kontrollfluss und potenzielle Taint-Quellen.

Die gefundenen Fehler können klassifiziert werden und verschiedenen Mitarbeitern zugewiesen werden.
Die Ergebnisse können anschliessend in verschiedenen Formaten wie SARIF, XML, CSV, PDF und HTML konfiguriert, weiterverarbeitet und exportiert werden.



Taint-Data-Tracking

Code Sonar ist in der Lage potenziell gefährliche Datenflüsse im Code aufzuspüren. Durch die Taint Data Tracking Analysefunktion können „verfälschte Daten“ als Overlay direkt auf dem Code angezeigt werden. Des Weiteren bietet CodeSonar eine grafische High-Level-Vistualisierung der Programm-Architektur an.



Hierdurch werden die normalerweise schwer zu findenden Datenpfade sichtbar gemacht. Durch die hohe Geschwindigkeit und Genauigkeit beim Aufspüren der betroffenen Daten-ströme hilft CodeSonar dabei, gefährliche Schwach-stellen zu finden, die ein Cyberkrimineller ausnutzen könnte. Präventivmaßnahmen sind so einfach zu treffen.

Gute Skalierbarkeit

CodeSonar ist extrem skalierbar. Schnelle Scans von kleinen Codeteilen auf den Desktops des Entwickler sind ebenso möglich wie umfangreiche Prüfungen großer Codebasen (inkl. Nebenläufigkeitsprüfungen) während der Regressionstests.

Sehr gute Performance – Möglichkeit der verteilten Analyse

Code Sonars Checker sind im Hinblick auf hohe Performance optimiert. Code Sonar skaliert gut auf Multicore- und Mehrprozessormaschinen und erlaubt zudem die Verteilung von Analysen auf mehreren Maschinen in Analysis-Clouds im eigenen Netzwerk (bis hin zu hochparallelen und verteilten Computer-Farmen). So können schnelle Analyseergebnisse auch großer Projekte von mehreren Millionen Codezeilen ermöglicht werden. CodeSonar kann an verschiedene Softwareentwicklungsumgebungen und Prozesse einfach angepasst werden.

Inkrementelle Analyse

Analysezeiten können zudem deutlich reduziert werden. CodeSonar berücksichtigt bereits bestehende Analysedaten und ermöglich es bei Projektaktualisierungen lediglich die geänderten Codeabschnitte zu bearbeiten.

Maintainance / Wartbarkeit

Code Sonar überprüft Applikationen auf die Einhaltung von Coding Standards und unterstützt eine Vielzahl von Regelwerken (u.a. MISRA-C and MISRA-C++, AUTOSAR C++-14, CERT, DISA STIG, OWASP, JPL, Power of Ten, CWE). Des Weiteren gibt es Schnittstellen zur Implementierung eigener Regeln.

Erhebung von Metriken

Zur Beurteilung der Wartungsfreundlichkeit von Quellcode berechnet CodeSonar eine Vielzahl verschiedener Metriken, wie z.B. Zyklomatische Komplexität, Halstead Metriken, Watson und McCabe und viele mehr.
Auch die Erhebung eigener, zusätzlicher Metriken lässt sich durch die API-Funktionalität von CodeSonar implementieren, bzw. durch Aggregation bestehender Metriken mittels Konfiguration realisieren.

Integrationen

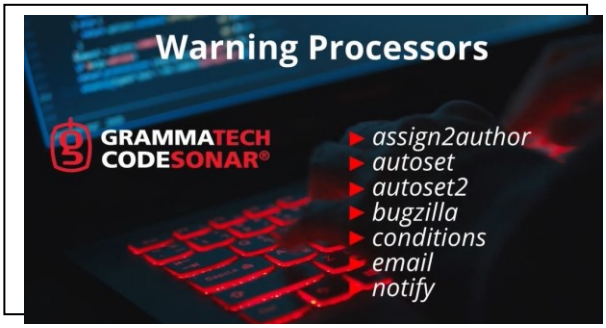
CodeSonar ermöglicht die Arbeit in großen Entwicklerteams.
Defekte sind persistent und werden über Builds hinweg verfolgt, auch wenn sich der Code ändert. Fehlermeldungen können annotiert, geordnet, an einzelne Mitarbeiter zur Bearbeitung zugewiesen, gesucht und verglichen werden.

Via Plugins kann CodeSonar in mehrere Software-Entwicklungstools integriert werden. Code Sonar kann daraufhin direkt aus der Entwicklungsumgebung heraus gestartet und die Analyseergebnisse im Anschluss direkt ausgewertet werden.

Des Weiteren gibt es die Möglichkeit die Analyseergebnisse von CodeSonar im Sarif-Format zu exportieren und mittels SARIF Importer-Plugin in eine Vielzahl von Entwicklungsumgebungen im Anschluss zu importieren.

Anbindung an Bug Tracking Tools

Mittels sog. „Warning Processors“ können diverse Bug-Tracking Tools problemlos angebunden werden, welche getriggert werden, sobald diese an den Hub übermittelt werden.



Unterstützung für Qualifizierungen nach verschiedenen Qualitätsstandards

Code Sonar wurde von der SGS TÜV Saar GmbH zertifiziert als ein geeignetes Werkzeug zur Erlangung von Zertifizierungen der höchsten Sicherheitsstufen.
Im Hinblick auf eine Zertifizierung ihrer Applikation, abhängig vom Ergebnis der Klassifizierung, ist in den meisten Fällen eine Qualifizierung von CodeSonar als Teil der eingesetzten Toolchain nötig. Hierfür bietet CodeSonar eine Reihe von Pre-Qualifizierungen und Testfällen an.

Hervorragender Support

Code Sonar zeichnet sich des Weiteren durch seinen mehrsprachigen Support aus. Ein in Deutschland basiertes deutschsprachiges Team steht Kunden und Interessenten per Telefon, E-Mail, Webpräsentation und bei Bedarf vor Ort beim Kunden auf Abruf bereit. Unser Support-Team sorgt dafür, den Kunden die Hürden bei der Einführung von Softwaretools zu nehmen.

Interessenten steht das Tool für eine kostenlose Evaluationsphase zur Verfügung.

Weitere Informationen

Webseite: https://www.verifysoft.com/de_grammatech_codesonar.html

Video: https://www.youtube-nocookie.com/embed/aCowV-zcDIM

Evalanfrage: https://www.verifysoft.com/de_grammatech_trial.html