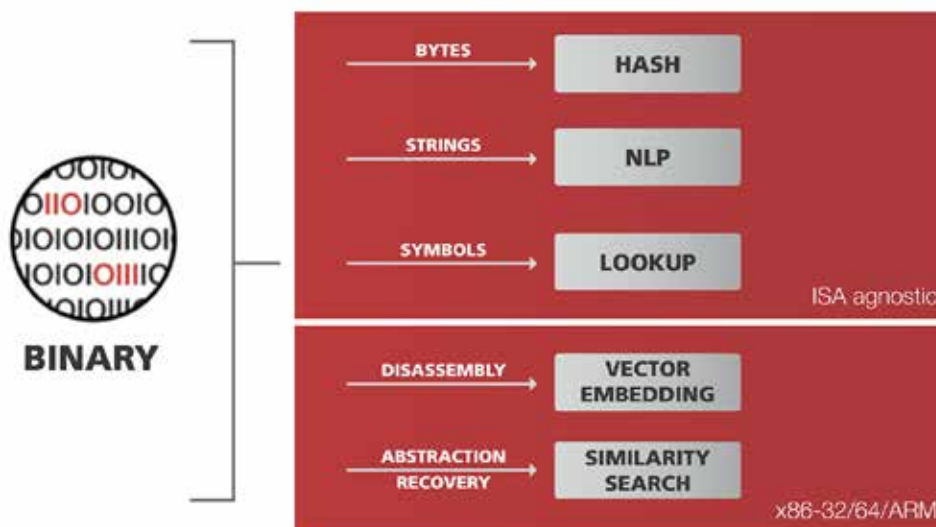


Sicherheitsrisiken mit GrammaTech CodeSentry aufdecken

Mindestens 90% der Unternehmen nutzen Third-Party-Software und 95% der von ihnen erstellten proprietären oder angepassten Softwareanwendungen enthalten Komponenten von Drittanbietern. Da diese oft unbekannt sind, besteht ein Sicherheitsrisiko.

Analyse des Binärcodes auf seine Zusammensetzung

CodeSentry verwendet Mehrkomponenten-Matching-Algorithmen, die eine schnelle und genaue Komponentenerkennung ermöglichen. Diese Algorithmen berechnen und vergleichen Codesignaturen durch die Nutzung von Eigenschaften, die von lexikalischen Informationen (z.B. Inhalt von Zeichenfolgen) bis hin zu tiefen semantischen Abstraktionen der in Funktionen enthaltenen Logik reichen.



CodeSentry führt eine Analyse der Softwarezusammensetzung durch und inventarisiert Open Source- und Drittanbieter-Code, um darin enthaltene Schwachstellen ausweisen zu können



Haupteinsatzmöglichkeiten

- ▶ Erkennung von Sicherheitslücken
- ▶ Software Re-Use Risk Management
- ▶ Software-Stücklisten

✓ CodeSentry vs. herkömmliche Software-Composition-Analysis-Tools

- ▶ CodeSentry analysiert ausschließlich den Code, der wirklich zum Ablauf gebracht wird und nicht die Build-Umgebung. Das vermag die Anzahl von False Positives signifikant zu reduzieren, da überflüssiger Code der Build-Umgebung und solcher, den die Build-Konfiguration ausschließt, in der Binärdatei nicht vorhanden ist.
- ▶ Vielfach ist der Quellcode schlichtweg nicht verfügbar.
- ▶ Sogar unter der Voraussetzung, dass der Quellcode vorhanden ist, ist das Aufsetzen einer Build-Umgebung meist nicht einfach.

✓ Eigenschaften und Vorteile von CodeSentry

- ▶ Einfache Nutzung
- ▶ Identifikation von Komponenten für die Software-Stücklisten
- ▶ Tracking und Annotation der Sicherheitslücken
- ▶ Benachrichtigungen zeigen, wo Sicherheitslücken mit einem Komponenten-Upgrade eliminiert werden können
- ▶ Diverse Einsatzmöglichkeiten (als lokale Installation oder SAAS-Lösung)
- ▶ Leichte Handhabung da kein Source Code notwendig
- ▶ Höhere Präzision (weniger False Positives, weniger entgangene Sicherheitslücken, weniger Risiko und Zeitaufwand durch exakte Warnungen)
- ▶ Mehrkomponenten-Matching-Algorithmen
- ▶ Erkennung von Drittanbieter-Komponenten

✓ Systemanforderungen

- ▶ Server: Linux-basiertes System mit 32 GB Speicher und Kubernetes
Client: jeder moderne Browser (Desktop oder mobiles Device)
- ▶ Ausgabeformat der Software-“Stücklisten“: CSV und PDF
- ▶ Sprachen: C, C++, Objective-C

Weitere Informationen finden Sie unter www.verifysoft.com/de_grammatech_codesentry.html

Vereinbaren Sie jetzt eine kostenlose Demo!

Verifysoft Technology GmbH
Technologiepark, In der Spöck 10-12
77656 Offenburg (Deutschland)
Tel. +49 781 127 8118 - 0
quality@verifysoft.com