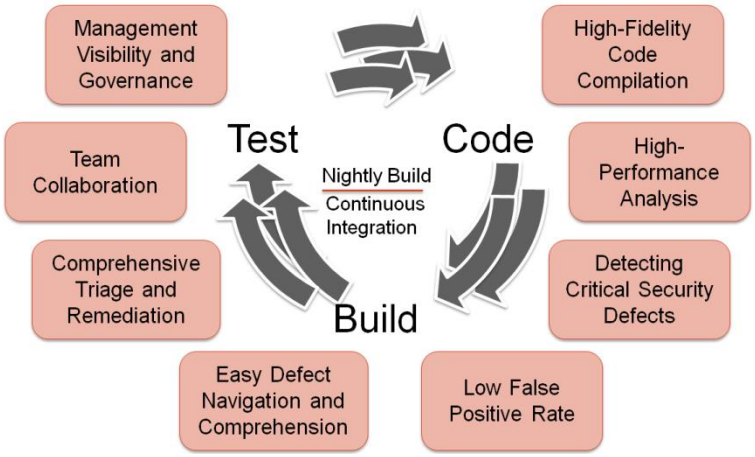
Einführung

Die **Security & Quality Software GmbH** bietet Dienstleistungen und Werkzeuge für die automatische, messbare Überprüfung und den Test der Sicherheit und Qualität der Software während der Entwicklung an. OpenSource Bestandteile werden aufgedeckt, Versionen, Exploids und rechtliche Hinweise angezeigt. In Kombination mit Verschlüsselung und Verschleierung der fertigen Applikationen gegen Angriffe und Raubkopien können Organisationen Software sicherer bauen, analysieren und ausgeben. Die zentrale, in bestehende Prozesse integrierte Gesamtlösung, spart Kosten, optimiert Vorgehensweisen, verkürzt Entwicklungszeiten und verbessert somit die Sicherheit und Qualität der Produkte messbar.

Software-Eigenentwicklung

Entwickler werden dabei unterstützt, schwer auffindbare und kritische Sicherheits- und Qualitätsprobleme automatisiert frühzeitig zu finden und zu beheben. Dabie werden Messkriterien für die Sicherheit und Qualität eingeführt und überwacht. Folgende Aufgabenstellung werden adressiert:

- Lauffähigkeit und Laufzeitverhalten der Anwendung
- Identifikation von Sicherheitsdefekte und Einfallstore für Angreifer
- Valide Messbarkeit der Software zu jedem Zeitpunkt
- Erhöhte Planbarkeit der Softwareeigen- und Fremdentwicklung



Bausteien des Softwareentwicklungsprozesses

- Schnellere Verfügbarkeit der Produkte durch Zeit- und Kostenersparnisse
- Überwachung und zeitliche Abschätzung von Abgabe- und Lieferterminen (Risikoanalyse)
- Höhere Kundenzufriedenheit durch bessere, stabilere und sicherere Produkte
- Verbesserung der Produktwartbarkeit und schnellere Produktanpassungen
- Produktivitätsverbesserung der Entwicklung und Testabteilung durch produktunterstütze Automatisierungen

Nutzen bei extern entwickelter Software

Auswahl an Fremdsoftware in Applikationen

Das Einbinden von Software von Fremdherstellern birgt ein Restrisiko mit ein. Die extern entwickelten Programme müssen mit den gleichen Metriken für Sicherheitsverwundbarkeiten, Sicherheitsrisiken, Qualität, Identifikation von OpenSource Komponenten und Wartbarkeit wie bei der Eigenentwicklung untersucht werden.

<u>Situationsbeschreibung</u>

- Viele IT Abteilungen haben nicht die Werkzeuge, Spezialisten und das Budget, um Fremdcode zu testen
- Traditionelle Bewertungsmethoden sind teuer, unvollständig, arbeitsreich und skalieren nicht
- Zulieferer geben den Quelletext nicht frei und verweigern den Zugriff in einer Cloud Umgebung

<u>Mögliche Lösungsansätze</u>

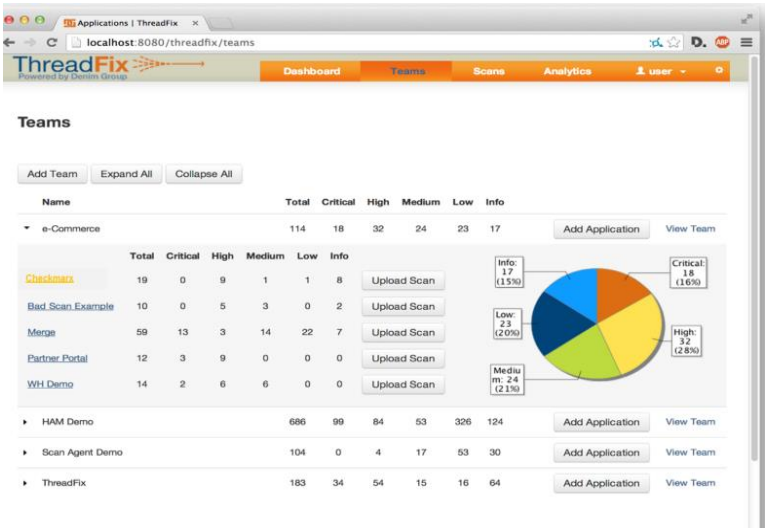
Die Zulieferer überprüfen die Software über ein Kontrollportal bei ihrem Kunden auf die Erfüllung der vorgegebenen Metriken hin. Sie können ihren Kunden auch mit entsprechenden Werkzeugen erstellte Prüfzertifikate aushändigen oder SQ Software zertifiziert beim Lieferanten die Software anhand ihrer vorgegebenen Metriken.

Software Schwachstellen finden - priorisieren – aggregieren und visualisieren

ThreadFix führt automatisch die Ergebnisse einiger Code-Scanner zusammen und unterstützt sie dabei, Sicherheitslücken in den unterschiedlichsten Progarmmiersprachen zu finden und zu schließen.

DIE AUGABENSTELLUNG

- Softwareentwickler und Sicherheitsbeauftragte nutzen Quelltextscanner wie auch Methoden zum manuellen Testen, um die Sicherheit der Anwendungen zu überprüfen.
- Jeder Test erstellt Ergebnislisten in den unterschiedlichen Formaten und mit vielen Duplikaten. Der gleiche Fehler wird verschieden beschrieben und anders bewertet.
- Die Einbindung in den Arbeitsablauf ist schwierig
- Entwickler erhalten nicht verwertbare Reports



DIE LÖSUNG

- Einlesen von dynamischen, statischen und manuellen Testergebnissen in eine zentrale Platform
- Führt Doppelnennungen zusammen und gibt eine priorisierte Liste der Fehler aus
- Verkürzt die Fehlerbehebungszeit von anfälligen Programmen
- Liest priorisierte Fehlerlisten in vorhandene „Defect Tracker" ein und rationalisiert die Fehlerbehebung
- Erzeugt Regeln für Firewalls von Webapplikationen (WAF), um die Daten während der Behebungszeit zu schützen.
- Gibt dem Mangement ein Werkzeug in die Hand, um Trendreports, Sicherheitsstati der Applikationen und Häufigkeiten von Verwundbarkeiten zu dokumentieren und zu visualisieren

Konsolidierte Ansicht der Testergebnisse
Führt Ergebnisse und Duplikate zusammen um eine Gesamtübersicht des Sicherheitsstatus der Anwendung zu erhalten.

Reporte
Ausgabe von aktuellen Sicherheitsberichten ihrer Anwendung

Einbindung in einen "Defect Tracker"
Zeigt die Sicherheits-Verwundbarkeiten und zugehörigen Defekte an

Virtuelles Patching
Stellt automatisch Regeln für die WAF auf, um heimtükischen Datenverkehr zu blocken, währedn der Fehler von den Entwicklern beseitigt wird.

Kompatibel mit Open Source und kommerziellen Produkten
Dynamische und statische Scanner, SaaS Test-Platformen, IDS/IPS, WAFs und Defect Trackers

Unterstützte Werkzeuge:
Dynamische/Statische Scanner: OWASP Zed Attack Proxy, Arachni, w3af, Skipfish, Microsoft CAT.NET, FindBugs, Brakeman, CPPcheck / *Kommerzielle Werkzeuge*: Kiuwan, Checkmarx, Virtual Forge, Coverity und andere / WAF, IDS, IPS: Mod Security, Snort, …
Regelvorgaben: PCI, OWASP, Top10, OCI DSS, HIPPA, DISA STIG und mehr
Plug-Ins: Jenkins, Sonar, BURP