Nei test di sicurezza delle applicazioni, i "falsi positivi" da soli non determinano la piena precisione, sebbene la loro bassa incidenza sia spesso considerata l'indicatore più importante che rivela la bontà del tool in esame. I falsi positivi sono solo uno dei quattro aspetti che determinano l'accuratezza di uno strumento: gli altri tre sono i "veri positivi", i "veri negativi" e i "falsi negativi". Falsi Positivi (FP): false vulnerabilità che sono non ci sono. Veri Positivi (TP): vulnerabilità reali segnalate correttamente. Falsi negativi (FN): vulnerabilità reali che non sono state correttamente segnalate. Veri negativi (TN): false vulnerabilità che correttamente non sono state segnalate. Pertanto, il tasso dei veri positivi (TPR) è il tasso con il quale sono state segnalate correttamente le vulnerabilità reali. Il tasso di falsi positivi (FPR) è il tasso con cui le vulnerabilità false sono state segnalate come reali, in modo errato. Le formule per determinare i veri e i falsi positivi: • Tasso dei veri positivi (TPR) = FP / (FP + TN) • Tasso dei falsi positivi (FPR) = TP / (TP + FN)
CONSIDERAZIONI FINALI DEL VALUTATORE
Nonostante la presenza accertata di falsi positivi e falsi negativi nei risultati delle scansioni, il prodotto si presta a una grande facilità d'uso e a una buona flessibilità, sia nella personalizzazione delle regole, sia nella reportistica. Il prodotto prevede la scansione di molti tipi di linguaggi sviluppati su diverse piattaforme e s'integra nelle pipeline di DevOps. L'interpretazione dei risultati è tuttavia d'obbligo, per valutare l'effettiva presenza delle vulnerabilità segnalate.

TEAM DI VALUTAZIONE	Software Security team

b. CodeDX

PRODOTTO	**CATEGORIA**	**FASE SSE**	**SITO WEB**
CodeDx	**SAST/DAST**	Implementation/Verification	https://codedx.com/
DESCRIZIONE			
CodeDx è un Tool commerciale che serve ad effettuare la verifica di eventuali vulnerabilità di programmi e software presi in considerazione relative al codice sorgente. CodeDx riunisce una serie di strumenti di analisi del codice (sia gratuiti, sia commerciali) che consentono a loro volta di individuare agevolmente eventuali difetti nel codice da analizzare.			
Source analysis, Pattern matching, "scan rules" (customizable).			
ANALISI DEL VALUTATORE			**SCORE**
Livello di integrazione con i seguenti prodotti			
a. IDEs	CodeDx si integra con i seguenti ide: Eclipse, IntelliJ e Visual Studio.		8

b. source repository,	CodeDx si integra i seguenti repository: Git (direttamente); Subversion, Mercurial, o Team Foundation Version Control (TFVC) (tramite zip del "source outside" di CodeDx e successivo upload verso CodeDx).	8
c. build server,	CodeDx si integra con i seguenti build server: Azure DevOps, Jenkins, Maven, TeamCity, Bamboo.	7
d. bug tracking tools	CodeDx supporta AlienVault, Git, Jira Software, Microsoft Threat Modeling, SD Elements.	
Le tipologie di applicazione supportate (Web, Mobile, Client-Server…)	Client Server, Web, Mobile (Android Studio).	7
I linguaggi di programmazione supportati	C/C++, Java, Javascript, JSP, .NET(C#, Visual Basic), PHP, Python, Ruby, Scala.	8
I framework applicativi supportati (es. Spring, Hibernate, …)	Il tool supporta i più popolari frameworks tra i quali Spring-MVC, JQuery e molti altri.	7
Gli Standard supportati (OWASP Top 10, SANS 25, …)	7PK (Seven Pernicious Kingdoms), CERT Coding Standards for C/C++ & Java, CLASP Vulnerability Lexicon, CWE/SANS Top 25 Most Dangerous Software Errors, DISA STIGs version 3.1 and 4.3, HIPAA Compliance Check, MISRA C, Mobile OWASP Top 10, NIST 800-53, OWASP Top 10 Project, PCI DSS, Software Fault Patterns (SFP), WASC Threat Classification v2	9
Le vulnerabilità riconosciute (Sql injection, Cross-site scripting, Code injection…)	Le vulnerabilità riportate dai seguenti tools, direttamente incorporati nel prodotto: Brakeman, Checkstyle, CppCheck, ESLint, SpotBugs, Find Security-Bugs, Gendarme, OWASP Dependency Check, JSHint, PHP_CodeSniffer, PHPMD, PMD, Pylint, Retire.js, ScalaStyle.	8
L'integrazione di "Custom rules"	È possibile all'interno di CodeDx creare delle regole personalizzate.	7
Possibilità di inibire la segnalazione di particolari vulnerabilità	È possibile all'interno del Tool gestire la segnalazione di una particolare vulnerabilità.	7
L'incidenza dei "Falsi positivi"	Dai riscontri, l'incidenza di falsi positivi è accettabile.	8
La capacità di analisi "raw source code" vs "need to compile"	CodeDx (a seconda dei tool embedded che vengono invocati) permette di analizzare il codice in entrambe le modalità (sia source-code che raw-code).	Entrambe
La capacità di analizzare le dipendenze da librerie esterne al fine di controllare se sono presenti vulnerabilità note	Black Duck (by Synopsys), OWASP Dependency Check, Retire.js, Synopsys Protecode, Sonatype Nexus	8