La capacità di correlare lo scan statico con l'esito di uno scan dinamico (correlazione White Box con Black Box)	Il prodotto è in grado di effettuare correlazioni tra entrambe le tipologie di scan del codice.	7
LE PERFORMANCE		
a. Full scan vs Incremental scan	Il prodotto è in grado di effettuare entrambe le tipologie di scan del codice.	8
b. Client-side scan vs Server-side scan	Il prodotto consente di effettuare scan sia lato server che client.	7
Supporto alla Remediation	Il tool guida nella localizzazione del problema ed offre supporto informativo utile per sanarlo.	6
Funzionalità di prioritizzazione delle Remediation	Il tool permete di evidenziare i bugs in base a delle priorità di intervento.	7
La facilità d'uso	Il prodotto è piuttosto facile da installare e assolutamente intuitivo da utilizzare.	8
I costi di licenza	CodeDx è un prodotto commerciale a pagamento dai costi non eccessivi rispetto a strumenti similari commerciali. L'argomento andrebbe comunque analizzato in una logica commerciale complessiva aziendale.	MEDIO
Il supporto alla reportistica	Il tool consente di produrre un'ottima reportistica in vari tipi di formato (Pdf, xml, Excel).	8
La classificazione degli errori riportati	Il Tool CodeDx permette di classificare gli errori secondo quattro tipologie di gravità: High, Medium, Low e Info.	7
CONSIDERAZIONI FINALI DEL VALUTATORE		
Dopo aver preso in considerazione tutti i punti descritti nella scheda si ritiene che il Tool CodeDx sia un ottimo strumento di facile uso e integrabile con molti altri tool sia gratuiti che a pagamento. Il tool permette agli sviluppatori di software, tester e analisti della sicurezza di individuare e gestire con modalità abbastanza semplici le vulnerabilità nel software. Il tool permette di integrare una quantità molto ampia di plugin e di altri tool che danno una copertura estesa di tutti i linguaggi più diffusi e degli IDE. L'integrazione fra i risultati di scansioni di tool differenti e la reportistica molto dettagliata e disponibile in vari formati, sono i veri punti di forza di CodeDx. Dalle evidenze riscontrate, è emerso che i tool ai quali CodeDx si appoggia forniscano risultati per lo più affidabili. Si ritiene pertanto che CodeDx sia utilizzabile proficuamente per gli scopi aziendali.		
TEAM DI VALUTAZIONE	Software Security team	

c. SonarQube

PRODOTTO	CATEGORIA	FASE SSE	SITO WEB
SonarQube	**SAST**	Implementation	http://www.sonarqube.org

DESCRIZIONE		
SonarQube è un prodotto avanzato per l'analisi statica del codice sorgente, finalizzato alla ricerca di errori di programmazione e di costrutti che costituiscono delle bad practise. I Bug rilevati sono tracciati ed evidenziati in un'interfaccia web intuitiva, in modo da poter seguire e gestire il processo di remediation. Dato che si tratta di un prodotto open source, il miglioramento dei pattern per il riconoscimento dei problemi è demandato all'ampia community in rete.		
SonarQube esegue le sue analisi attraverso appositi plugin che applicano al codice sorgente dei pattern match pre-definiti.		
ANALISI DEL VALUTATORE		**SCORE**
Livello di integrazione con i seguenti prodotti		
a. IDEs	S'integra tramite il plugin SonarLint con Eclipse, Visual Studio, IntelliJ. SonarLint è uno strumento che analizza il codice dal punto di vista della qualità, ma è possibile utilizzarlo in collegamento con SonarQube, per sfruttare le regole di sicurezza di quest'ultimo.	8
b. source repository,	S'integra, tramite plugin, a Git, Svn, CVS, TFVC, Jazz RTC, ClearCase.	8
c. build server,		
d. bug tracking tools	SonarQube comprende la gestione completa dei bug riscontrati (tracciamento incluso).	8
Le tipologie di applicazione supportate (Web, Mobile, Client-Server…)	Web, Mobile Android.	8
I linguaggi di programmazione supportati	ABAP, Apex, C#, C, C++, COBOL, CSS, Flex, Go, Java, JavaScript, Kotlin, Objective-C, PHP, PLI, PLSQL, Python, RPG, Ruby, Scala, Swift, TypeScript, TSQL, VB.NET, VB6, HTML, XML	10
I framework applicativi supportati (es. Spring, Hibernate, …)		
Gli Standard supportati (OWASP Top 10, SANS 25, …)	SonarQube comprende fra le sue rules CWE, SANS TOP 25 e OWASP TOP 10	10
L'integrazione di "Custom rules"	SonarQube offre la possibilità di creare delle regole personalizzate, attraverso dei custom templates	10
Possibilità di inibire la segnalazione di particolari vulnerabilità	Il tool consente di "sopprimere" la segnalazione di una particolare vulnerabilità in maniera agevole.	9
L'incidenza dei "Falsi positivi"	Coloro che scoprono un falso positivo possono segnalarlo alla Community. Per questo motivo l'incidenza dei falsi positivi è tenuta bassa.	7
La capacità di analisi "raw source code" vs "need to compile"	SonarQube fa le sue valutazioni su bytecode, per cui presuppone un rebuild del codice modificato.	Need to Compile

La capacità di analizzare le dipendenze da librerie esterne al fine di controllare se sono presenti vulnerabilità note	Attraverso plugin	7
La capacità di correlare lo scan statico con l'esito di uno scan dinamico (correlazione White Box con Black Box)		
LE PERFORMANCE		
a. Full scan vs Incremental scan	Il prodotto è in grado di eseguire entrambe le tipologie di scan del codice.	8
b. Client-side scan vs Server-side scan	Il prodotto consente di eseguire scan sia lato server, sia lato client.	8
Supporto alla Remediation	SonarQube offre la possibilità di organizzare e seguire la fase di correzione dei bugs.	9
Funzionalità di prioritizzazione delle Remediation	SonarQube classifica i bugs in base all'urgenza con la quale devono essere corretti.	8
La facilità d'uso	Il prodotto è piuttosto facile da installare e assolutamente intuitivo da utilizzare.	7
I costi di licenza	La Community edition di SonarQube è Open Source, con licenza GNU Lesser GPL License, Version 3, quindi non comporta alcun costo di licenza. Le edizioni Developer, Enterprise e Data Center sono commerciali.	Free
Il supporto alla reportistica	Si realizza tramite plugin open source o commerciali. La dashboard e l'interfaccia web costituiscono, di per sé, una valida reportistica.	7
CONSIDERAZIONI FINALI DEL VALUTATORE		
Sebbene l'aspetto della sicurezza non sia ancora il core delle funzionalità di SonarQube, sono stati fatti molti passi avanti per migliorare la scoperta delle vulnerabilità insite nella scrittura di codice sorgente. SonarQube ha diversi punti di forza che ne hanno fatto lo strumento preferito dai gruppi di sviluppo per il controllo statico del codice: • Un'estesa community che lavora costantemente al suo miglioramento. • Una grande disponibilità di plugin che ne ampliano le funzionalità, fino a coprire molteplici aspetti dello sviluppo sicuro. • La possibilità di utilizzarlo all'interno di una moderna pipeline di delivery DevOps-oriented, per automatizzare l'efficientamento del codice ad ogni rilascio. • Metriche sofisticate che servono a stabilire complessità e leggibilità del codice e l'adesione alle best practises di programmazione. • La gestione grafica delle vulnerabilità emerse. • L'adesione ai principali standard di sicurezza: CWE, SANS To 25 e OWASP Top 10.		
TEAM DI VALUTAZIONE	Software Security team	