DETERMINA A CONTRARRE
ART. 32 D.LGS. 50/2016

OGGETTO DELL'ACQUISIZIONE	Acquisto licenze software Checkmarx
CODICE IDENTIFICATIVO	Rda Consip n. 51247
BENEFICIARIO	Sogei
TIPOLOGIA DI PROCEDURA PRESCELTA	Affidamento diretto su MEPA (ex art. 1 comma 2 lett. a) della legge 120/2020 ed ex art. 36 comma 6 d.lgs. 50/2016)
IMPORTO MASSIMO STIMATO	€ 84.480,00
DURATA DEL CONTRATTO	6 mesi
REQUISITI DI PARTECIPAZIONE	Assenza motivi di esclusione ai sensi dell'art. 80 d.lgs. 50/2016
CRITERIO DI AGGIUDICAZIONE	Non applicabile
SUDDIVISIONE IN LOTTI	No trattandosi di un'unica fornitura di software
MOTIVAZIONI	L'affidatario sarà individuato, a seguito di valutazioni comparative dei preventivi, sulla base del minor prezzo. Il moderno processo di sviluppo del software presente in Sogei prevede, attualmente, un elevato numero di piccoli rilasci in tempi sempre più brevi. Sia in caso di nuovi sviluppi che di manutenzioni correttive e/o evolutive, il software prodotto deve rispettare elevati standard di qualità e sicurezza in linea con il flusso DevSecOps previsto in Sogei. Per la realizzazione di questo scenario è, quindi, necessario introdurre dei controlli automatici che, in tempi brevi, possano verificare e segnalare eventuali problemi di sicurezza. Inoltre i controlli, se eseguiti per ogni modifica e fin dalle prime fasi dello sviluppo del codice, permettono di intervenire sulle versioni del software non definitive abbattendo tempi e costi di ogni intervento. Tra i controlli automatici è di fondamentale importanza l'analisi SAST – Static Application Security Testing che verifica la sicurezza delle applicazioni analizzando direttamente il codice sorgente alla ricerca di problemi che possano comportare la presenza di vulnerabilità sul prodotto finale. L'azienda, per il triennio 2020/2022, ha utilizzato Checkmarx CxSAST come strumento per l'analisi statica di sicurezza ed ha avviato un'attività di analisi e sperimentazione su progetti pilota per la revisione del processo di rilascio in esercizio delle applicazioni. A partire dalla seconda metà del 2021 l'architettura dello strumento CxSAST è stata rivista per meglio adattarsi alle esigenze aziendali. L'infrastruttura, sia server che database, è stata migrata su un ambiente con risorse maggiori ed aggiornata all'ultima versione disponibile. Inoltre, per evitare che successivi aggiornamenti del prodotto possano impattare in modo imprevisto sulle applicazioni sottoposte ad analisi, è stato predisposto anche un ambiente di test sul quale è stato

	implementato un processo per la gestione degli aggiornamenti. Tale prodotto permette la riduzione dell'impatto che eventuali anomalie nelle nuove regole introdotte dagli aggiornamenti possono causare sui processi aziendali. Attualmente l'analisi con CxSAST è un passaggio obbligatorio per tutti i progetti aziendali, sia per i nuovi sviluppi sia per i progetti esistenti sottoposti ad aggiornamento o modifiche. L'introduzione dell'obbligo nell'esecuzione dell'analisi SAST è stata possibile dopo un'intensa attività di studio, sperimentazione e formazione che possono essere schematicamente suddivise in: - Individuazione dei principali linguaggi e tecnologie utilizzate in azienda e selezione delle applicazioni pilota su cui effettuare tutte le verifiche necessarie, - Onboarding delle applicazioni pilota all'interno di CxSAST ed analisi dei risultati delle scansioni per individuare pregi e difetti delle configurazioni di default del prodotto, - Definizione di nuovi policy, modifica delle query e delle regole di default del prodotto per aumentare i controlli su aree ritenute critiche e per ridurre il numero dei falsi positivi in base alla tipologia di applicazione sottoposta ad analisi, - Definizione, per ciascun linguaggio di programmazione, dei documenti "Linee guida di sviluppo sicuro" a supporto dei gruppi di sviluppo aziendali. Le soluzioni suggerite si basano sulle best practice internazionali con un focus particolare su quali funzioni sono riconosciute valide da CxSAST per la risoluzione di una vulnerabilità. Per completare il processo sopra riportato l'azienda si è avvalsa di un supporto specialistico focalizzato sull'utilizzo del prodotto CxSAST. CxSAST è uno strumento a supporto dello sviluppo e non una verifica conclusiva sul prodotto finale. I risultati dell'analisi, devono essere oggetto di verifica da parte di personale esperto di supporto ai gruppi applicativi nella valutazione dei risultati e nella scelta delle modalità più efficaci per la risoluzione dei problemi rilevati. Per evitare ritardi impedimenti, per ciascuna Unità Organizzativa aziendale sono stati individuati e formati delle figure esperte di sviluppo sicuro del codice sorgente che hanno assunto il ruolo aziendale di Security Champion. Le Unità Organizzative al momento coinvolte sono 38 per un totale di 80 Security Champions iniziali ufficialmente nominati che dovranno gestire più di 2000 progetti di sviluppo. Ogni Security Champion, in base al linguaggio ed alla tecnologia su cui è specializzato, ha seguito uno dei corsi di formazione che l'azienda ha organizzato in collaborazione con il supporto specialistico. La formazione dei SC, oltre che riguardare i principali problemi e soluzioni di sicurezza per lo sviluppo sicuro delle applicazioni, ha compreso anche una formazione specifica sull'utilizzo dello strumento. Si prevede inoltre, con l'aumentare dei clienti, una seconda fase di OnBoarding (correzione delle segnalazioni e nella selezione dei falsi positivi) per la restante parte del 2022, con l'impegno aziendale nell'individuazione e formazione di ulteriori SC. Ad Aprile del 2022 è stato pubblicato il Gartner Magic Quadrant per Application Security Testing e recentemente sono state svolte delle analisi comparative con i principali competitor di mercato riportati nella sezione Leaders del quadrante. I prodotti analizzati sono stati i seguenti: - Microfocus Fortify, - HCL AppScan, - Synopsys Coverity. Dalle analisi e dai test svolti, rispetto a tutti i competitor analizzati ed alle ultime versioni dei rispettivi prodotti, la soluzione Checkmarx CxSAST è risultata essere l'unica a soddisfare tutti i seguenti requisiti essenziali per i clienti istituzionali di Sogei: - Installazione della piattaforma OnPremise, all'interno dei sistemi aziendali, - Assenza di requisiti minimi sulla struttura del pacchetto del codice sorgente da sottoporre a scansione, CxSAST esegue l'analisi anche se il codice sorgente è parziale. - Rappresentazione grafica con analisi dei nodi comuni tra le vulnerabilità rilevate, permettendo l'identificazione del punto più conveniente in cui applicare la risoluzione, - Funzionalità di modifica e creazione di nuove regole di sicurezza per tutti i tipi di linguaggi. Tramite un apposito editor è possibile definire o modificare le query che il prodotto effettua sul codice sorgente consentendo di aggiungere funzioni per ridurre il numero dei falsi positivi. La modifica può essere anche specializzata per il singolo progetto o per tutte le applicazioni analizzate,

	- Task nativo per le pipeline di DevOps flessibile e configurabile in linea con le caratteristiche del processo SAST definito in azienda. Tramite il task di CxSAST è possibile lanciare scansioni ed impostare dei quality gate per la valutazione dell'esito in modo completamente automatico, - Integrazione diretta con il repository Git effettuare una scansione. CxSAST è in grado di collegarsi al branch del progetto e di scaricare il codice da analizzare direttamente dal repository aziendale. In conclusione, per i seguenti motivi: 1) piena ed esclusiva rispondenza delle caratteristiche tecniche del prodotto utilizzato in questi anni agli attuali requisiti tecnico-organizzativi del flusso DevSecOps adottato da Sogei ed utilizzato per fornire e aumentare il livello del servizio offerto per i clienti istituzionali, - 2) conservazione degli investimenti sostenuti nelle diverse fasi – 5) massimizzazione degli investimenti formativi già svolti sul personale, - 4) non interruzione del piano di attività di Static Application Security Testing, fondamentale per contenere i rischi di cybersecurity rispetto alle applicazioni web sviluppate da Sogei per tutti i clienti istituzionali per cui eroga servizi, si ritiene che Checkmarx CxSAST non sia sostituibile nel prossimo triennio da nessun altro software al momento presente sul mercato. Resta confermato l'impegno di Sogei a monitorare sviluppi ed evoluzioni di analoghe soluzioni disponibili sul mercato in rispondenza anche all'evoluzione delle esigenze dell'Amministrazione e dei propri clienti istituzionali e dei cicli produttivi di Sogei stessa nell'arco del prossimo triennio.	
NOMINATIVO DELL'OPERATORE ECONOMICO	Non applicabile	
ELEMENTI ESSENZIALI DEL CONTRATTO	Contratto standard Sogei	
DEROGHE AL BANDO TIPO	Non applicabile	
RESPONSABILE PROCEDIMENTO	Il Responsabile del procedimento è il Dott. Stefano Intini, ferma restando l'applicazione dell'art. 31, comma 10, del d.lgs. 50/2016. Il responsabile individuato ai sensi dell'art. 1 comma 1 del decreto legge n. 76/2020, convertito con modificazioni dalla legge n. 120/2020, ai fini di quanto previsto nella legge medesima è il Responsabile della Divisione Sourcing Operation, che nel rispetto delle deleghe a questi attualmente conferite, valida ed approva le diverse fasi procedurali.	
FIRMA DEL RESPONSABILE APPROVAZIONE DETERMINA E DATA	Gianandrea Greco (Responsabile Divisione Sourcing Operation) GIANANDREA GRECO CONSIP S.P.A 06.12.2022 17:16:29 UTC	Vale la data della firma digitale del documento

Per gli acquisti effettuati per altre Amministrazioni/Società nella determina di cui sopra sono recepite le esigenze dalle stesse manifestate