DETERMINA A CONTRARRE
ART. 17 D.LGS. N. 36/2023

OGGETTO DELL'ACQUISIZIONE	Acquisto licenze software Checkmarx
CODICE IDENTIFICATIVO	RdA Consip n°: 52163
BENEFICIARIO	Sogei S.p.A.
AVVISO DI PREINFORMAZIONE	No
TIPOLOGIA DI PROCEDURA PRESCELTA	Affidamento diretto sul MEPA (ex art. 50 D. Lgs. 36/2023, comma 1, lettera b)
IMPORTO MASSIMO STIMATO	Euro: 109.500,00
DURATA DEL CONTRATTO	Mesi: 12
REQUISITI DI PARTECIPAZIONE	Rispetto degli artt. 94 e 95 D.Lgs. 36/2023
CRITERIO DI AGGIUDICAZIONE	N.A.
SUDDIVISIONE IN LOTTI	NO - Ai sensi e per gli effetti dell'art. 58, del D.lgs. n. 36/2023, si precisa che la presente procedura non viene suddivisa in lotti in quanto le varie prestazioni oggetto del contratto fanno parte di un'unica tipologia e sono funzionalmente connesse da un punto di vista tecnico. Di conseguenza un'eventuale suddivisione in lotti potrebbe compromettere l'economicità e l'efficienza del servizio oggetto del contratto.
MOTIVAZIONI	Il moderno processo di sviluppo del software di sistemi complessi prevede 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 per la Pubblica Amministrazione deve rispettare elevati standard di qualità e sicurezza in linea con il flusso DevSecOps. Per la realizzazione di questo scenario non è possibile ricorrere esclusivamente a controlli manuali svolti da personale qualificato in quanto

	rallenterebbero in modo inaccettabile i tempi di ogni rilascio ma è necessario introdurre dei controlli automatici che, in tempi brevi, possano verificare e segnalare eventuali problemi di sicurezza. I controlli, se eseguiti per ogni modifica e fin dalle prime fasi dello sviluppo, permettono di intervenire su versioni del software non definitive abbattendo tempi e costi di ogni intervento. Al fine di effettuare lo shift left dei controlli, in ottica DevSecOps, è necessario mettere a disposizione dei gruppi di sviluppo gli strumenti necessari a spostare questi controlli nelle prime fasi dello sviluppo, riducendo il tempo e costo degli interventi ed evitando il replicarsi di vulnerabilità note nei moduli sviluppati successivamente. I controlli di sicurezza automatici possono essere divisi in due principali tipologie: • controlli statici: eseguono l'analisi a partire dal codice sorgente dell'applicazione e possono essere eseguiti fin dalle prime fasi del ciclo di sviluppo senza che l'applicazione sia in esecuzione. I principali tipi di controlli di questa tipologia sono l'analisi SAST – Static Application Security Testing e l'analisi SCA – Software Composition Analysis, • controlli dinamici: eseguono l'analisi di un'applicazione o servizi web simulando attacchi non distruttivi verso il server dove è in esecuzione il codice applicativo. I principali tipi di controlli di questa tipologia sono l'analisi DAST – Dynamic Application Security Testing e l'analisi IAST – Interactive Application Security Testing. Nell'ambito dei controlli statici Sogei ha da tempo adottato all'interno del flusso DevSecOps lo strumento per l'analisi SAST. Attualmente i risultati dell'analisi sul codice sorgente sono obbligatori per tutti gli sviluppi e propedeutici per il deploy dell'applicazione in esercizio. Tutti i gruppi di sviluppo possono eseguire le scansioni e visualizzare autonomamente i risultati in qualsiasi momento del ciclo di sviluppo. Al fine di aumentare ulteriormente il livello di qualità e sicurezza complessivo dell'applicazione, oltre l'analisi SAST che viene effettuata sul codice sorgente, è necessario attivare anche l'analisi SCA per verificare la presenza di vulnerabilità note (CVE – Common Vulnerabilities Exposure) sulle librerie di terze parti importate all'interno di tutti i progetti aziendali. L'adozione di uno strumento SCA all'interno del flusso DevSecOps permette di segnalare la presenza vulnerabilità sulle librerie sia durante la fase di sviluppo sia durante la fase operativa dell'applicazione. Infatti, anche dopo il rilascio in esercizio, potrebbero essere pubblicate nuove vulnerabilità sui componenti open source permettendo quindi un controllo di sicurezza continuo sul prodotto finale. In continuità con quanto realizzato per il processo SAST, anche per l'analisi SCA l'obiettivo è rendere autonomi i gruppi di sviluppo nell'analisi dei risultati e nella risoluzione delle segnalazioni. Al momento in Sogei sono circa 55 le L.O. che si occupano di sviluppo e che utilizzano i risultati dell'analisi SAST per verificare il codice delle loro applicazioni. Per l'analisi SCA è stato individuato il prodotto Checkmarx CxSCA che, mediante l'integrazione con Checkmarx CxSAST e dei particolari indicatori, fornisce un'ampia gamma di informazioni per supportare e guidare i gruppi di sviluppo nella risoluzione delle segnalazioni. L'esigenza è stata verificata anche sulla base delle risultanze di un'analisi di mercato comparativa basata su fonti di terze parti indipendenti (Gartner, Forrester) con altri tool di analisi SCA presenti sul mercato prodotti da fornitori come Synopsys, Veracode, Sonatype. Il prodotto Checkmarx CxSCA ha evidenziato, durante le attività di analisi comparativa condotte nei confronti delle altre piattaforme indicate, di essere l'unica soluzione a rispondere complessivamente a tutti i seguenti requisiti: - semplicità di utilizzo e flessibilità nell'adattare lo strumento all'eterogeneità delle tecnologie e software prodotti dall'azienda, - integrazione con processi aziendali DevSecOps esistenti e le relative piattaforme tecnologiche adottate, - copertura dei requisiti funzionali e logici al fine di ridurre il rischio di rilasciare in esercizio delle applicazioni affette da vulnerabilità, - integrazione con Checkmarx CxSAST, strumento già presente in azienda, con un triplice vantaggio: - Capacità di fornire allo sviluppatore un unico report contenente tutte le segnalazioni delle analisi statiche di sicurezza SAST e SCA, - Flusso di gestione delle segnalazioni di CxSCA analogo a CxSAST, rendendo lo sviluppatore fin da subito autonomo nella classificazione delle vulnerabilità,- Possibilità di mantenere il codice sorgente dell'applicazione OnPremise, inviando sulla piattaforma CxSCA esclusivamente le informazioni necessarie per risalire ai componenti di terze parti utilizzati dall'applicazione. Quest'ultimo punto è possibile solo grazie all'integrazione con CxSAST che, avendo a disposizione il codice sorgente delle applicazioni, permette di integrare le informazioni da inviare a CxSCA

	per migliorare la qualità complessiva dei risultati dell'analisi come indicato nel punto successivo, - indicazione di informazioni fondamentali a definire una priorità nell'ordine degli interventi da attivare per la risoluzione delle segnalazioni. Questo aspetto è stato ritenuto fondamentale per la scelta del prodotto in quando consente di ridurre automaticamente il numero delle segnalazioni che devono essere gestite da parte dello sviluppatore al fine di renderlo autonomo nella gestione e lavorazione delle stesse. Nel dettaglio gli indicatori forniti dal prodotto sono i seguenti: - indicazione se la libreria oltre ad essere importata è anche utilizzata all'interno del codice dell'applicazione, - indicazione se il codice dell'applicazione richiama esplicitamente il metodo o la funzionalità vulnerabile della libreria segnalato all'interno della CVE (funzionalità denominata exploitable path), - indicazione se per la CVE sono disponibili pubblicamente dei payload/script che permettono di sfruttare la vulnerabilità anche ad attaccanti non esperti, - indicazione se per la CVE sono disponibili pubblicamente informazioni e dettagli approfonditi che consentono ad un attaccante esperto di scrivere payload/script per sfruttare la vulnerabilità. Tutti i precedenti indicatori permettono di definire delle policy di sicurezza estremamente dettagliate con l'obiettivo sia di aumentare la sicurezza complessiva delle applicazioni sia di semplificare i tempi ed il costo degli interventi da parte dei gruppi di sviluppo per risolvere i problemi di sicurezza. L'analisi fornisce sia informazioni sulla presenza di CVE sia la segnalazione se la libreria non è più supportata da parte del produttore classificandola come EOL – End Of Life fornendo inoltre informazioni su quale versione più recente è possibile utilizzare. Per l'acquisto delle licenze software Checkmarx è stata effettuata preliminarmente una valutazione comparativa di preventivi tra i partner Checkmarx, indicati dal Produttore, in grado di erogare la fornitura richiesta. Il preventivo di importo più basso è stato presentato dalla Società Innovery S.p.A.	
NOMINATIVO DELL'OPERATORE ECONOMICO	Innovery S.p.A.	
ELEMENTI ESSENZIALI DEL CONTRATTO	Condizioni di contratto standard Sogei	
DEROGA AL BANDO TIPO	N.A.	
RESPONSABILE PROCEDIMENTO	Il Responsabile unico del progetto è il Dott. Gianandrea Greco. Il Responsabile del procedimento per la fase di affidamento è il Dott. Stefano Intini.	
FIRMA DEL RESPONSABILE APPROVAZIONE DETERMINA E DATA	Gianandrea Greco (Responsabile Divisione Sourcing Operation)	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