tender.sk
Doručujeme Vám zákazky

Code review informačného systému CES

I.D.: 106439697

Prílohy:
- Správa o zákazke_Codereview.doc (Pre zobrazenie príloh testujte tu)
- Link na zverejnenie.docx (Pre zobrazenie príloh testujte tu)
- Ponuka IstroSec.pdf (Pre zobrazenie príloh testujte tu)
- Záznam z prieskumu trhu_EVO_codeview.pdf (Pre zobrazenie príloh testujte tu)

Druh zákazky	Služby	Dátum publikovania	04.12.24
Typ oznámenia:	Výsledok	CPV kódy	72222100-8

Opis:

Externý proces Code Review pre Centrálny ekonomický systém (ďalej len „IS CES“) vybudovaný v zmysle zákona č. 215/2019 Z. z. – automatizovaná a manuálna kontrola kódu v súlade s požiadavkami všeobecne záväzných právnych predpisov a bezpečnostnými štandardami. 1. Predmetom zákazky je poskytnutie externých služieb na vykonanie Code Review existujúceho IS CES (CES MF SR , CES METAIS) - Tento proces bude zahŕňať kombináciu automatizovanej a manuálnej kontroly zdrojového kódu, s cieľom zabezpečiť jeho súlad s aktuálnymi požiadavkami všeobecne záväzných právnych predpisov, bezpečnostnými štandardami a osvedčenými postupmi vývoja softvéru. Úlohou dodávateľa bude identifikovať a analyzovať prípadné bezpečnostné zraniteľnosti, nekonzistencie v kóde, odporúčania pre optimalizáciu a rizikové oblasti vo vývoji IS CES v súlade s metodikou OWASP Code Review Guide. Vyžaduje sa znalosť ABAP, CDS, HTML, JSON, JS, TS (TypeScript), Java, CSS a YAML. • Bližšie informácie k počtu riadkov kódu a použitým programovacím jazykom sú uvedené v prílohe č. 6 Výzvy – príloha k OPZ na Code Review CES. 2. Špecifikácia požadovaných služieb: o Automatizované code review (Využitie špecializovaných nástrojov na automatickú analýzu zdrojového kódu, ktoré umožnia): o Detekciu bezpečnostných zraniteľností (napr. SQL injection, XSS, CSRF a ďalšie). o Identifikáciu kódových chýb (napr. zle implementované API volania, chyby v pamäťovom manažmente). o Analýzu neoptimalizovaných častí kódu z hľadiska výkonu a efektivity. o Overenie dodržiavania špecifikovaných programovacích štandardov a osvedčených postupov. o Kontrola správnosti používania knižníc a rámcov podľa požiadaviek projektu. o Manuálne code review (Detailná manuálna analýza kódu, zameraná na): o Hĺbkovú kontrolu bezpečnostných slabín, ktoré automatizované nástroje nemusia identifikovať (logické chyby, neadekvátne overenie vstupov, atď.). o Preskúmanie architektonického návrhu z hľadiska bezpečnosti a jeho konzistencie s implementovaným kódom. o Analýza dodržiavania kódovacích štandardov, najlepších postupov a odporúčaných návrhových vzorov. o Posúdenie kvality testovania a používania testovacích nástrojov. 3. Výstup - vypracovanie podrobnej správy z Code Review, ktorá bude obsahovať: o Zoznam identifikovaných chýb a bezpečnostných zraniteľností, vrátane ich závažnosti (prioritizácia nápravných opatrení, vrátane uvedenia umiestnenia všetkých zraniteľností uvedením cesty k adresáru, názvu súboru a číslo riadku). o Odporúčania pre opravu zistených chýb a návrhy na zlepšenie bezpečnosti a efektívnosti kódu (odporúčania v rozpore Best practice code quality). o Návrh krokov pre ďalší vývoj alebo úpravy IS CES.