PREGLED POSTUPKA #108933

1 PODACI O NARUČIOCU

Naziv naručioca	INSTITUT ZA JAVNO ZDRAVLJE
PIB	02015340
E-mail	ijzcg@ijzcg.me
Telefon	020/412-888
Internet adresa	ijzcg.me
Fax	020/243-728
Adresa	Džona Džeksona bb
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Antivirusni softver za korisnike
Status	U toku
Vrsta predmeta	Robe
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Dragica Pejanović
Kontakt	067/626-125
Datum objave	09.03.2026. 09:45
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Antivirusni softver za korisnike	09.03.2026 09:45	25.03.2026 10:00	25.03.2026 10:00	U toku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne
Nabavka je	
Zelena	Ne
Društveno odgovorna	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2026	**INSTITUT ZA JAVNO ZDRAVLJE** **Antivirusni softver za korisnike - Licenca** 48760000 - Softverski paket za zaštitu od virusa	8.264,46 EUR	1.735,54 EUR	-	-	-	Jednostavna nabavka

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište što se dokazuje dostavljanjem dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlašćenom licu privrednog subjekta	Uslovi za obavljanje djelatnosti
Ponuđač je dužan dostaviti Autorizaciju od strane proizvođača za prodaju i pružanje tehničke podrške u predmetnoj nabavci	Drugi uslovi
Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, data na Obrascu 2, preuzimanjem na posebnom aplikativnom dijelu elektronskog sistema javnih nabavki.	Obrazac 2
virmanski	Način plaćanja
Rok za izvršenje ugovora definiše se na sljedeći način: - Ponuđač je obavezan da izvrši isporuku, instalaciju, konfiguraciju i testiranje softverskog rešenja najkasnije u roku od 30 dana od dana potpisivanja ugovora. - Licence, tehnička podrška ponuđača i podrška proizvođača moraju trajati 12 mjeseci od dana aktivacije licenci. - Period podrške obuhvata redovne nadogradnje, otklanjanje kvarova i osiguranje nesmetanog rada.	Rok izvršenja ugovora
Rok važenja ponude je 60 dana od dana otvaranja	Rok važenja ponude
Rok plaćanja: do 30 dana od dana prijema fakture nakon uspješno izvršene isporuke i testiranja softverske platforme. Faktura prije plaćanja, mora biti ovjerena od strane odgovornog lica naručioca.	Rok plaćanja
Garantni rok: Garantni rok za ispravnost i funkcionalnost softverskog rješenja iznosi 12 mjeseci od dana aktivacije licenci, odnosno od dana puštanja u rad. Garantni rok obuhvata otklanjanje svih grešaka i nepravilnosti koje nijesu nastale nepravilnim korišćenjem.	Garantni rok

Ponuđač je obavezan dostaviti autorizaciju proizvođača ili distributera softvera (MAF) ili njegovog ovlašćenog predstavnika da može da učestvuje u predmetnom postupku nabavke softverskog rješenja.	Drugi uslovi
Podaci o ponuđaču: naziv ponuđača, adresa, grad, broj telefona i fax, poštanski broj, email adresa, PIB, kontakt osoba i internet stranica.	Drugi uslovi
Kao parametar kvaliteta za predmetnu nabavku ponuđač treba da ima minimum jedno lice koje će biti zaduženo za izvršenje ugovora koje posjeduje sertifikat izdat od proizvođača softverskog rješenja koje je predmet nabavke. Ponuđač je radi dokazivanja obavezan da kao dokaz za ovo lice dostavi: dokaz o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i dostavljanjem kopije traženog sertifikata.	Drugi uslovi
Ponuđač čija ponuda bude izabrana kao najpovoljnija je dužan da uz potpisan ugovor o nabavci dostavi naručiocu: - Garanciju za dobro izvršenje ugovora, za slučaj povrede ugovorenih obaveza u iznosu od 10% od vrijednosti ugovora sa rokom važenja 7 dana duže od ponuđenog roka izvršenja ugovora.	Drugi uslovi

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **8.264,46 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		• Otkriva i zaustavlja ne samo tradicionalne viruse i trojance (zasnovane na hash vrijednostima), već i malware i non-malware napade. • Otkriva i zaustavlja tkz. „0-day“ viruse, ransomware napade, kao i scripting i Powershell memory-based napade. • Prepoznaje, otkriva i sprječava „Living-off-the-Land“ (LofL), odnosno fileless napade. • Prepoznaje, otkriva i blokira maliciozne skripte/programe napisane u PowerShell-u, Visual Basic-u, Perl-u, Python-u, Java-i i drugim interpreterima. • Putem web interfejsa pruža uvid u izvor i prirodu samog napada u vidu grafičkog prikaza toka napada i pratećih aktivnosti koje su dio njega, sa ciljem lakšeg otkrivanja malicioznog aktera i utvrđivanja radnji koje želi da izvrši. • Pruža zaštitu od malicioznih dokumenata (poput PDF ili Office fajlova sa ugrađenim makroima). • Pruža mogućnost generisanja „crne liste“ fajlova i aplikacija koje nije moguće pokretati/izvršavati na zaštićenim radnim stanicama. • Posjeduje mogućnost definisanja različitih grupa i primjene različitih bezbjednosnih polisa po grupama u skladu sa potrebama korisnika.	

		• Omogućava kontrolu upotrebe USB uređaja koji se koriste na zaštićenim računarima. • Sama arhitektura rješenja je zasnovana na centralizovanoj web konzoli koja se nalazi u Cloud-u i koja komunicira sa agentima distribuiranim po računarima. • Agent koji se instalira na računarima ima minimalne hardverske zahtjeve i njegov rad ne utiče bitno na performanse sistema na kojem je prisutan (zahtijeva manje od 3% resursa uređaja). • Podržava opciju sprječavanja isključivanja i brisanja agenata od neautorizovanih korisnika. • Agent kontinualno, u realnom vremenu, prati i analizira svaki događaj na sistemu radi detekcije i prevencije malicioznih radnji. • Agent snima svaki događaj lokalno na sistemu i ovako sakupljene podatke šalje ka centralnoj lokaciji gde se vrši njihova agregacija. • Ažuriranje agenata se vrši kroz centralizovanu web konzolu. • Podržava operativne sisteme: Windows 7/8/10/11, macOS 10.12 i noviji, Linux: RHEL 8, CentOS 8, Oracle (UEK 7.6-7.9, 8 i noviji, RHCK), SUSE, Ubuntu, Amazon Linux, Debian (kernel 4.4 i noviji) и Windows Server 2008 R2/2012/2012 R2/2016/2019. Centralizovana konzola za upravljanje mogućnostima rješenja posjeduje sljedeće mogućnosti: • Jasan i pregledan uvid u sve prijetnje koje su identifikovane ili blokirane u sistemu koji se nadzire. • Unificirani pregled statusa i informacija o agentima na svim radnim stanicama koje se štite. • Grafički i tabelarni prikaz broja zaustavljenih poznatih	

1	Antivirusni softver - Obnova licenci	malware-a, potencijalnih malware-a, non-malware-a, potencijalno neželjenih programa (poput adware-a) i sl. • Analiza napada u cilju zaustavljanja malicioznog koda prije njegovog izvršavanja. • Korelacija prikupljenih podataka sa nadgledanih radnih stanica. • Pregled nadgledanih radnih stanica sa centralne konzole i mogućnost brze izolacije zaraženog računara u cilju sprječavanja komunikacije tog računara sa svim drugim računarima u mreži, pri čemu je omogućena komunikacija samo sa konzolom, i to bez instalacije dodatnog software-a na zaraženom računaru u trenutku izolacije. • Direktan udaljeni pristup računaru sa centralne konzole, i kada agent jeste i kada nije mrežno izolovan. Ovo administratoru daje mogućnost izvršavanja osnovnih komandi za: o Pregled pokrenutih procesa, o „Ubijanje“ odgovarajućih procesa na osnovi PID (process kill), o Memory dump, o Brisanje fajlova/direktorijuma, o Upload/download fajlova, o Izvršavanje programa i/li skripti. • Prosljeđivanje fajlova nekom od virus, malware ili URL online servisa u cilju dalje analize. • Mogućnost pretrage prikupljenih događaja po nazivu procesa ili po hash vrijednosti binarne datoteke. • Mogućnost kreiranja SQL upita nad svim prikupljenim podacima kroz centralizovanu konzolu ili API pristup. • Administrator ima mogućnost upload-a sumnjivog fajla na PSC radi dalje analize.	300,00 licenca

		• Administrator ima mogućnost kreiranja korisničkih rola sa različitim nivoima privilegija, počevši od ReadOnly prava. • Mogućnost prikaza informacija o tome da li je radna stanica koja se nadgleda u trenutku napada bila prisutna u kompanijskoj mreži ili ne. • Filtriranje upozorenja po radnim stanicama koje se nadgledaju i po aplikacijama koje su bile uključene u incident. • Prikaz primarnog procesa od kojeg je krenuo napad koji sadrži sljedeće informacije o procesu: o ime izvorne aplikacije, o ko je aplikaciju digitalno potpisao, o ime malware-a, o tip malware-a, o informaciju da li je aplikacija automatski obrisana ili ne, o vektor kroz koji je došao napad. • Podržavanje minimalno sledećeg seta operacija nad aplikacijama za koje se detektuje da su učestvovale u prijavljenom događaju: o Dodavanje aplikacije u kompanijsku „belu“ ili „crnu“ listu, o terminiranje aplikacije, o upload aplikacije radi detaljnije analize, o prosljeđivanje hash vrijednosti date aplikacije na nekom od virus, malware ili URL online servisa, kao i o brisanje same aplikacije sa radne stanice • Na centralnoj konzoli treba da postoje sljedeći podaci o svakom uređaju koji se prati: o njegova javna i privatna IP adresa, o verzija operativnog sistema, o grupa u kojoj se nalazi, o posljednja lokacija uređaja (u kompanijskog mreži ili van nje),	

		o verzija instaliranog agenta, o broj detektovanih malware-a, i o datum i vrijeme kada se radna stanica posljednji put javila centralnoj konzoli. • Na centralnoj konzoli treba da postoje sljedeći podaci o događaju koji je detektovan: o Datum i vrijeme kada se događaj desio, o Ime pokrenute aplikacije i ime korisnika koji je aplikaciju pokrenuo, o ukoliko je aplikacija pokrenuta od strane druge aplikacije navedeno je od koje, o ime i IP adresa uređaja na kojem se detektovani događaj desio, o podatak o tome da li je uređaj na kojem se događaj desio u tom trenutku bio u kompanijskog mreži ili van nje. • Rješenje treba da nudi mogućnost kreiranja polisa koje mogu da terminiraju ili blokiraju procese koji pokušavaju da: o se pokrenu ili su već pokrenuti, o komuniciraju preko mreže, o pristupe memoriji drugog procesa, o ubace kod ili da modifikuju radnu memoriju drugog procesa, o izvrše kod iz memorije, o pokrenu „untrusted“ aplikacije, ili o otvore komandni interpreter. • Mogućnost bypass-a aplikacija na određenim putanjama u okviru fajl sistema. • Mogućnost notifikacije administratora na osnovu značaja, prioriteta, detektovanog upozorenja ili na osnovu primenjene polise. • Rješenje treba da bude je sertifikovani Microsoft antivirus	

		provider za WSC (Windows Security Center), uz mogućnost uključivanja i isključivanje WSC integracije. • Rješenje treba da sadrži i alat za vizuelni prikaz međusobnih veza između raznih entiteta koji čine događaje na konzoli. • Rješenja treba da pruža dinamičan prikaz odnosa između procesa, korisnika, pristupnih web domena, kreiranih fajlova i sl.	