PREGLED POSTUPKA #104127

1 PODACI O NARUČIOCU

Naziv naručioca	UPRAVA ZA STATISTIKU
PIB	02011506
E-mail	contact@monstat.org
Telefon	020/230-811, 020/230-961
Internet adresa	www.monstat.org
Fax	020/230-814, 020/230-961
Adresa	IV Proleterske 2
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Produženje licenci za antivirusni program - 300 korisničkih licenci
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Snežana Obradović
Kontakt	zana.obradovic@monstat.org
Datum objave	25.11.2025. 12:15
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Produženje licenci za antivirusni program ; 300 korisnickih licenci	25.11.2025 12:15	28.11.2025 10:00	28.11.2025 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
2025	**UPRAVA ZA STATISTIKU Produženje licenci za antivirusni program ; 300 korisnickih licenci** 48761000 - Anti-virus softverski paket	16.474,72 EUR	3.459,68 EUR	-	-	-	Otvoreni postupak

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

Opis	Tip uslova / zahtjeva
Ponuđač je dužan u okviru podnijete ponude, a u skladu sa članom 9 stav 10 Pravilnika o načinu sprovođenja jednostavnih nabavki ("Sl. list Crne Gore", broj 016/23, 020/23 , 36/23 , 114/23, 049/24, 114/24), dostaviti Izjavu ponuđača(Obrazac 2) o ispunjenosti uslova utvđenih zahtjevom i nepostojanju sukoba interesa, potpisanu od strane ovlašćenog lica ponuđača, datu na Obrascu 2. Izjava mora biti potpisana elektronskim potpisom.	Obrazac 2
Rok važenja ponude je 60 dana od dana otvaranja ponuda.	Rok važenja ponude
U postupku nabavke može da učestvuje samo privredni subjekat koji posjeduje: MEST EN ISO 9001 (sa obimom sertifikacije: projektovanje, implementacija i održavanje informacionih sistema), MEST EN ISO 20000-1 (sa obimom sertifikacije: projektovanje, implementacija i održavanje informacionih sistema) ili ekvivalentno, MEST EN ISO 27001 (sa obimom sertifikacije: projektovanje, implementacija i održavanje informacionih sistema) i MEST EN ISO 27701 (sa obimom sertifikacije: projektovanje, implementacija i održavanje informacionih sistema) .	Stručna i tehnička sposobnost
Ponuđač je dužan da dostavi ovlašćenje proizvođača, zastupnika, distributera ili predstavnika proizvođača opreme za koju se nabavljaju licence, odnosno mora da ima odgovarajući dokaz proizvođača, zastupnika, distributera ili predstavnika proizvođača (sertifikat ili drugi akt) kojim se potvrđuje da je ovlašćen da vrši prodaju licenci koje su predmet nabavke.	Stručna i tehnička sposobnost
U postupku nabavke može da učestvuje samo privredni subjekat koji ima stalno zaposlena najmanje 2 lica sertifikovana od strane proizvođača za rad sa ponuđenim rješenjima, što se dokazuje dokazom 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 dokaz o stručnoj osposobljenosti (sertifikat, uvjerenje ili drugi akt nadležnog organa ili organizacije).	Stručna i tehnička sposobnost

Ponuđač za softversko rješenje garantuje tehničku podršku naručiocu u trajanju od 12 mjeseci od dana potpisivanja Zapisnika o izvršenoj usluzi..	Garantni rok
Rok isporuke i implementacije ponuđenih softverskih licenci je 2 dana,od dana zaključenja ugovora.	Rok izvršenja ugovora
Mjesto izvršenja ugovora: Uprava za statistiku, Podgorica, Ul IV proleterske br. 2	Mjesto izvršenja ugovora
Plaćanje usluge će se vršiti u roku do 20 dana nakon isporuke licenci, potpisanog zapisnika o izvršenoj usluzi	Rok plaćanja
Način plaćanja: virmanski.	Način plaćanja

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **16.474,72 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		• Rješenje treba da obezbijedi sveobuhvatnu zaštitu od poznatih i zero-day Cyber prijetnji u trajanju od 12 mjeseci. • Mora biti imenovano kao jedno od vodećih rješenja (Leader) u Gartnerovom 'Magic Quadrant for Endpoint Protection Platforms' za 2025. godinu. • Rješenje treba da ima, kao minimum, sljedeće mehanizme zaštite i prevencije: • Antimalver sa detekcijom baziranom na signaturama • Zaštita od ransomware-a • Mašinsko učenje - prije izvršenja i tokom izvršenja • Zaštita od iskorištavanja Veb pretraživača • Praćenje ponašanja • Zaštita skripti • Zaštita od zloupotrebe ranjivosti (anti-exploit) • Prevencija komunikacije sa C&C (Command and Control) serverima • Kontrola aplikacija • Prevencija file-less malvera • Reputacija fajlova i Veb sajtova • Rješenje treba da ponudi kombinaciju zaštite bazirane na signaturama, analizi ponašanja i AI/mašinskom učenju. • Mašinsko učenje mora imati mehanizam za izdvajanje i	

		analizu karakteristika fajla prije samog izvršavanja, kao za i analizu ponašanja fajla/procesa tokom izvršenja radi prepoznavanja prijetnji. • Rješenje mora imati modul za praćenje ponašanja koji konstantno prati štićene sisteme radi neobičnih izmjena operativnog sistema ili instaliranog softvera, pružajući dodatnu zaštitu od programa koji pokazuju zlonamjerno ponašanje. • Rješenje mora imati modul za zaštitu od zloupotrebe ranjivosti, koji prekida programe koji iskazuju abnormalno ponašanje povezano sa zloupotrebom ranjivosti. Sistem mora prepoznavati više tehnika zloupotrebe kao što su korupcija memorije, logičke greške, zlonamjerne injekcije i izvršenja koda. • Rješenje treba da pruža mehanizam zaštite protiv ransomware-a u slučaju kompromitovanja sistema, sa opcijom zaštite dokumenata od neautorizovanog šifrovanja ili izmjena. • Rješenje mora biti sposobno praviti kopije fajlova koje ransomware pokušava da šifruje na štićenom sistemu i mora imati mogućnost vraćanja pogođenih fajlova u njihov prvobitni oblik. • Rješenje mora moći prepoznavati komunikaciju preko HTTP/HTTPS protokola i uobičajenih HTTP portova, kao i otkrivati i sprječavati komunikaciju sa globalnim C&C serverima, uz mogućnost kreiranja korisničkih lista od strane administratora. • Rješenje treba imati mogućnost virtualnog ažuriranja (virtual patching) i pružiti brzu zaštitu od ranjivosti na različitim štićenim sistemima (krajnjim tačkama). • Rješenje mora podržavati host-bazirani firewall sa stateful	

1	Produženje licenci za antivirusni program ; 300 korisnickih licenci	inspekcijom, sa opcijom kreiranja pravila po osnovu Izvora/Odredišta/Porta/Protokola/Aplikacije, radi stateful inspekcije i visokoperformansnog mrežnog skeniranja na viruse. • Rješenje mora imati integrisani modul za kontrolu aplikacija za unapređenje odbrane od malvera i ciljnih napada sprječavanjem izvršenja nepoznatih i neželjenih aplikacija na štićenim krajnjim tačkama, koristeći fleksibilne, dinamičke politike, whitelisting (po defaultu zabrana) i mogućnosti zaključavanja stanja sistema. • Integrisana kontrola aplikacija treba da ima globalnu i lokalnu real-time bazu prijetnji zasnovanu na reputaciji fajlova, povezanu preko globalne mreže. • Kontrola uređaja treba da podržava: mrežne uređaje, USB, mobilne memorijske uređaje, uređaje koji nemaju mogućnost skladištenja podataka, modeme, Bluetooth adaptere, COM/LPT portove, uređaje za skeniranje/slikanje, bežične mrežne kartice, infracrvene uređaje. • Rješenje treba imati integrisanu sposobnost prevencije gubitka podataka (Data Loss Prevention). • Rješenje mora imati funkciju automatskog uklanjanja promjena koje su napravili malveri, uključujući zlonamjerne aplikacije bazirane na mreži i fajlovima, kao i ostatke virusa i crva (trojanci, unosi u registru i zaraženi fajlovi). • Rješenje treba biti u mogućnosti da prikuplja i korelira XDR podatke o aktivnostima za jedan ili više vektora, uključujući, ali ne ograničavajući se na: krajnje tačke, email, servere, cloud servise i mreže. • Rješenje treba da uključuje unaprijed definisane modele detekcije koji kombinuju više pravila i filtera koristeći tehnike kao što su mašinsko učenje i data stacking. Ovi modeli treba	1,00 kom.

		redovno ažurirati radi poboljšanja sposobnosti detekcije prijetnji i smanjenja broja lažno pozitivnih alarma. • Rješenje treba imati mogućnost omogućavanja ili onemogućavanja modela detekcije, kao i dodavanja/konfigurisanja izuzetaka za modele detekcije u skladu sa potrebama organizacije. • Rješenje treba omogućiti kreiranje korisničkih modela detekcije i prilagođenih filtera događaja koji definišu događaje koje model koristi za aktiviranje alarma. • Rješenje treba biti u mogućnosti da analizira i utvrdi da li određeni indikatori signaliziraju aktuelni napad, omogućavajući korisniku da pravovremeno preduzme akcije sprječavanja, istraživanja i sanacije ciljanih napadačkih kampanja. • Rješenje treba imati mogućnost pružanja preporučenih akcija za osnaživanje sistema u cilju zaštite od budućih potencijalnih napada. • Rješenje treba prikazati sve događaje koji su mapirani u MITRE ATT&CK okvir; SOC analitičar može koristiti ove događaje kao početnu tačku za dalje istrage. • Rješenje treba pružiti dodatni kontekst uz mapiranje na MITRE ATT&CK TTPs radi brže detekcije i pouzdanijih alarma. • Rješenje treba imati mogućnost pisanja prilagođenih upita za pretragu, dodavanja sačuvanih upita na listu za nadgledanje i automatskog izvršavanja tih upita nad najnovijim telemetrijskim podacima u regularnim intervalima. U kontekstu odgovora na prijetnje i istrage incidenata, rješenje mora imati sledeće funkcionalnosti: • Rješenje treba da obezbijedi objedinjene mogućnosti za istragu i odgovor širom štićenih radnih stanica, servera,	

		emailova, cloud servisa i mreža. • Rješenje treba da prikaže listu korelisanih upozorenja, koja sadrže sve sigurnosne događaje koji su detektovani i koja pomažu u identifikovanju i ublažavanju potencijalnih sigurnosnih proboja u mrežnom okruženju. • Dodavanje ili uklanjanje indikatora kompromitacije na blok listu, uključujući, ali ne ograničavajući se na: hash fajla, URL, IP adresu i domene. • Automatsko i ručno prikupljanje forenzičkih dokaza sa određenih krajnjih tačaka i slanje forenzičkog paketa nazad u menadžment konzolu radi dalje istrage. • Automatsko i ručno prikupljanje fajlova i objekata sa određenih krajnjih tačaka. • Daljinska konekcija na krajnju tačku radi dump-ovanja memorije procesa. • Daljinska izolacija krajnje tačke uz održavanje komunikacije sa menadžment konzolom. • Mogućnost daljinske konekcije i izvršavanja prilagođenih PowerShell ili Bash skripti. • Mogućnost izvršavanja prilagođenih YARA pravila na određenim krajnjim tačkama. • Mogućnost daljinske shell sesije i izvršavanja udaljenih komandi. • Mogućnost slanja odabranih fajlova ili objekata na automatsku analizu u sandbox. • Mogućnost pregleda i zaustavljanja aktivnih procesa na jednoj ili više krajnjih tačaka. • Rješenje mora prikupljati, organizovati i pružati informacije o aktivnim kampanjama Cyber napada i njihovim akterima (Threat Intelligence). Podaci o kampanjama treba da uključuju	

		izvještaje o TTP-ovima (Tactics, Techniques, and Procedures), alatima, korišćenom zlonamjernom softveru, povezanim CVE-ovima i indikatorima kompromitacije. • Rješenje treba omogućiti izvršavanje skeniranja radi identifikacije indikatora kompromitacije (IoC) i indikatora napada (IoA). • Rješenje treba omogućiti SOC analitičaru da ručno dodaje IoC indikatore kao što su hash-ovi fajlova, IP adrese, domeni i URL-ovi. • Podrška za zaštitu Microsoft Windows (Server i Desktop) i MacOS, 32 i 64-bitne operativne sisteme.	