"Sky Express Montenegro" d.o.o.
Broj 05/26
Podgorica, 22.04. 2026 god.

Broj: 01 - 3822
Podgorica: 15 04 2026

Džona Džeksona bb, 81 000 Podgorica
Telefon:020/412-888, Fax: 020/243-728
www.ijzcg.me
ijzcg@ijzcg.me
PIB:02015340 PDV:30/31-08180-6

Nakon sprovedenog postupka jednostavnih nabavki po zahtjevu za dostavljanje ponuda šifra postupka #108933 od 09.03.2026. godine, **zaključuje se**

UGOVOR O NABAVCI

između:

1. Institut za javno zdravlje Crne Gore sa sjedištem u Podgorici, ulica Džona Džeksona bb, PIB: 02015340,broj računa: 540-11914-02, Naziv banke: Erste banka - Podgorica, koga zastupa dr Ivan Samardžić, v.d. direktora (u daljem tekstu: Naručilac),

i

2. **Sky Express Montenegro d.o.o. iz Podgorice,** ul. Ankarski Bulevar broj 9 , PIB 03301923, Broj računa: 520-45568-44, Naziv banke: Hipotekarna Banka AD, koga zastupa izvršni direktor Jovana Radnić, s druge strane (u daljem tekstu: Izvršilac).

OSNOV UGOVORA:

Zahtjev za dostavljanje ponuda jednostavnih nabavki za nabavku antivirusnog softvera za korisnike, šifra postupka: #108933 od 09.03.2026. godine.
Broj i datum obavještenja o ishodu postupka: 01- 3527 od 07.04.2026. godine;
Ponuda ponuđača Sky Express Montenegro d.o.o. iz Podgorice, dostavljena preko ESJN, šifra ponude 155527od 25.03.2026. godine u 1:44 sati.

Član 1

Predmet ovog ugovora: Antivirusni softver - Obnova licenci (300 licenca)

Data nabavka sadrži sledeće karakteristike:
Antivirusni softver - Obnova licenci:
• 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 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.
• 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.

Član 2

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.

Član 3

Ukupna vrijednost predmetne nabavke iznosi: Bez PDV-a: 8.100,00 EUR, PDV: 1.701,00 EUR.

Član 4

Ugovorne strane su saglasne da će NARUČILAC isplatiti ugovorenu cijenu u roku 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.

Član 5

Rok za izvršenje ugovora definiše se na sljedeći način:
- Izvršilac 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 važenja ugovora je 12 mjeseci od dana zaključenja ugovora potpisanog sa obadvije ugovorne strane.

Član 6

Ugovorne strane su saglasne da do raskida ovog Ugovora može doći ako IZVRŠILAC ne bude izvršavao svoje obaveze u rokovima i na način predvidjen Ugovorom:

- u slučaju kada NARUČILAC ustanovi da kvalitet izvršene usluge koja je predmet ovog ugovora ili način na koje se isporučuje, odstupa od traženog.
- u slučaju da se IZVRŠILAC ne pridržava svojih obaveza i u drugim slučajevima nesavjesnog obavljanja posla.

NARUČILAC je obavezan da u slučaju uočavanja propusta u obavljanju posla pisanim putem pozove IZVRŠIOCA i da putem Zapisnika zajednički konstatuju uzrok i obim uočenih propusta.

Član 7

Ugovor koji je zaključen uz kršenje antikorupcijskog pravila u skladu sa odredbama člana 38 ZJN (Sl.list CG br. 074/19, 003/23, 11/23, 084/24) i Pravilnika o jednostavnim nabavkama ("Službeni list Crne Gore", br. 016/23, 020/23, 036/23 , 114/23, 049 /24, 114/24) ništav je.

Član 8

IZVRŠIOC mora da dostavi garanciju za dobro izvršenje ugovora, za slučaj povrede ugovorenih obaveza u iznosu od 10% od vrijednosti ugovora (sa uračunatim PDV-om), sa rokom važnosti 7 (sedam) dana dužim od roka na koji se zaključuje ugovor o javnoj nabavci. Rok važenja ugovora je godinu dana od dana obostranog zaključivanja ugovora. U slučaju potrebe naručilac ima pravo da traži produženje garancije. Naručilac je ovlašćen da garanciju za dobro izvršenje posla, naplati u cjelosti u slučaju da Isporučilac ne ispuni bilo koju obavezu predviđenu ovim ugovorom i u slučaju jednostranog raskida ugovora. Ako se za vrijeme trajanja ugovora promijene rokovi za izvršenje ugovorne obaveze ili druge okolnosti koje onemogućavaju izvršenje ugovorenih obaveza, važnost garancije se mora produžiti. Troškove produženja bankarske garancije snosi Isporučilac.

Član 9

Za sve što nije predvidjeno ovim ugovorom primjenjuju se odredbe Zakona o obligacionim odnosima i drugih pozitivnih propisa.

Član 10

Ugovorne strane su saglasne da eventualne sporove povodom ovog ugovora rješavaju sporazumom. U protivnom, ugovara se nadležnost suda u Podgorici.

Član 11

Ovaj ugovor je pravno valjano zaključen i potpisan od dolje navedenih ovlašćenih zakonskih zastupnika strana ugovora i sačinjen je u 5 (pet) istovjetnih primjeraka, od kojih 3 (tri) primjerka za NARUČIOCA i 2(dva) za IZVRŠIOCA.

Pripremila:
Dragica Pejanović
Službenik za javne nabavke
D. Pejanović

Odobrio:
Miloš Milutinović, dipl.pravnik

UGOVORNA STRANA

IZVRŠILAC
Sky Express Montenegro d.o.o.

Jovana Radnić, izvršni direktor

UGOVORNA STRANA

NARUČILAC
Institut za javno zdravlje Crne Gore

dr Ivan Samardžić, v.d. direktora