

PREGLED POSTUPKA #123239

1 PODACI O NARUČIOCU

Naziv naručioca	AERODROMI CRNE GORE
PIB	02305623
E-mail	marko.djurovic@apm.co.me
Telefon	020/444-222
Internet adresa	www.montenegroairports.com
Fax	020/444-221
Adresa	Golubovci bb
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Licenca za antivirus
Status	U toku
Vrsta predmeta	Robe
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Marko Đurović
Kontakt	020 444 250
Datum objave	05.10.2026. 10:00
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Licenca za antivirus	05.10.2026 10:00	08.10.2026 10:00	08.10.2026 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	AERODROMI CRNE GORE Licenca za antivirus 48900000 - Razni softverski paketi i kompjuterski sistemi	20.000,00 EUR	4.200,00 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 sedište što se dokazuje dostavljanjem dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlašćenom licu privrednog subjekt.	Uslovi za obavljanje djelatnosti
Uz ponudu se dostavlja i 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 ESJN	Obrazac 2
Privredni subjekat je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora što se dokazuje dokazom o angažovanju radne snage (kopija radne knjižice, prijava za osiguranje ili ugovor o radu) sa odgovarajućim referencama koje su potrebne za izvršenje predmeta nabavke u skladu sa zakonom i to: minimum 1 sertifikovano tehničko lice za rad na endpoint rješenjima, koje posjeduje sertifikat izdat od proizvođača ponuđenog rješenja minimalno nivoa Arhitect ili Expert.	Stručna i tehnička sposobnost
Ponuđač je dužan da dostavi ovlašćenje proizvođača, ovlašćenog distributera, zastupnika ili predstavnika proizvođača navedenih licenci iz tehničke specifikacije, odnosno mora da ima odgovarajući dokaz proizvođača, ovlašćenog distributera, zastupnika ili predstavnika proizvođača kojim se potvrđuje da je ovlašćen da vrši prodaju navedenih licenci u predmetnoj nabavci.	Drugi uslovi
Mjesto izvršenja ugovora: aerodrom Podgorica i aerodrom Tivat.	Mjesto izvršenja ugovora
Rok izvršenja je 30 dana od dana potpisivanja Ugovora.	Rok izvršenja ugovora
Način plaćanja je virmanski, na žiro račun Izabranog ponuđača. Žiro račun: _____ Banka: _____ (Ponuđač je obavezan navesti broj žiro računa i banke).	Način plaćanja
Naručilac će izvršiti plaćanje u roku do 15 (petnaest) kalendarskih dana od dana ispostavljanja fakture	Rok plaćanja

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: 20.000,00 EUR

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		ENDPOINT ANTIVIRUS - isporuka, licenciranje i implementacija cloud-baziranog XDR rješenja za naprednu zaštitu, detekciju, monitoring i odgovor na bezbjednosne incidente na krajnjim uređajima i serverima sa sledećim karakteristikama: • Potrebno je obezbijediti zaštitu za 300 krajnjih uređaja i servera, sa licencama u trajanju od najmanje 12 mjeseci. • Rješenje mora omogućiti cloud-bazirano centralizovano upravljanje i biti skalabilno. • Rješenje mora koristiti jednog agenta po krajnjoj tački za funkcionalnosti endpoint zaštite, detekcije i odgovora na prijetnje. • Rješenje mora omogućiti centralizovanu detekciju, analizu i korelaciju bezbjednosnih događaja sa krajnjih uređaja. • Rješenje mora omogućiti prikupljanje i analizu endpoint telemetrije radi detekcije naprednih prijetnji i sprovođenja threat hunting aktivnosti. • Rješenje mora putem istog endpoint agenta omogućiti centralizovano upravljanje Host Firewall pravilima najmanje na Windows i macOS sistemima, uz centralno evidentiranje događaja i mogućnost automatske primjene različitih skupova firewall pravila u zavisnosti od toga da li se endpoint nalazi	

unutar ili izvan organizacione mreže.

- Rješenje mora biti u stanju da na podržanim Windows, Linux i macOS operativnim sistemima lokalno i tokom izvršavanja detektuje napade zasnovane na tehnikama eksploatacije.
- Rješenje mora na krajnjem uređaju lokalno, tokom izvršavanja, sprječavati poznate i nepoznate tehnike eksploatacije, uključujući najmanje zaštitu od memory-corruption napada, neovlašćenog izvršavanja koda, Return-Oriented Programming (ROP) tehnika i lokalne eskalacije privilegija.
- Rješenje mora omogućiti zaštitu od file-based i fileless prijetnji; eksploitacionih tehnika usmjerenih prema web i lokalnim aplikacijama, kao i operativnom sistemu.
- Rješenje mora omogućiti detekciju i sprečavanje izvršavanja poznatog i nepoznatog malvera korišćenjem više mehanizama detekcije, uključujući metode zasnovane na mašinskom učenju.
- Rješenje mora omogućiti detekciju naprednih prijetnji analizom ponašanja procesa i aktivnosti na krajnjim uređajima,
- Rješenje mora na krajnjem uređaju imati lokalni mehanizam za inspekciju sadržaja mrežnih paketa (Network Packet Inspection/Deep Packet Inspection), koji analizira podatke sadržane u mrežnim paketima, a ne samo metapodatke o mrežnim konekcijama, radi detekcije maliciozne mrežne aktivnosti.
- Rješenje mora omogućiti centralno upravljanje pravilima za dozvoljavanje i blokiranje izvršavanja aplikacija. Rješenje ne smije dozvoliti dodavanje istog elementa na blacklist ukoliko se on već nalazi na whitelist-u, i obrnuto.

- Rješenje mora omogućiti kontrolu korišćenja prenosivih uređaja uređaja na krajnjim tačkama prema definisanim pravilima.
- Rješenje mora omogućiti zaštitu od manipulacije endpoint agentom i neovlašćene deinstalacije na podržanim operativnim sistemima.
- Rješenje mora omogućiti automatsku integraciju sa cloud servisom za analizu sumnjivih fajlova.
- Cloud analitički servis mora koristiti više metoda za analizu i klasifikaciju sumnjivih objekata, uključujući statičku i dinamičku analizu, mašinsko učenje i druge napredne analitičke tehnike.
- Rješenje mora omogućiti prikaz relevantnih threat intelligence informacija i konteksta povezanog sa detektovanim bezbjednosnim događajima i artefaktima.
- Rješenje mora omogućiti integraciju sa eksternim threat intelligence izvorima.
- Endpoint agent mora imati lokalni mehanizam za analizu prethodno nepoznatih fajlova, koji koristi model razvijen primjenom mašinskog učenja i omogućava lokalno utvrđivanje da li je analizirani objekat maliciozan ili benigan, bez oslanjanja isključivo na prethodno postojeće potpise ili cloud analizu.
- Funkcionalnosti lokalne zaštite od malvera zasnovane na mašinskom učenju, zaštite od exploit tehnika, inspekcije mrežnih paketa i behavioral zaštite moraju biti realizovane kroz isti endpoint agent, bez potrebe za instalacijom dodatnih endpoint agenata ili zasebnih lokalnih bezbjednosnih komponenti.
- Rješenje mora kontinuirano prikupljati endpoint telemetriju potrebnu za detekciju i istragu bezbjednosnih događaja.

1	Endpoint Antivirus- produženje licence	• Rješenje mora omogućiti korelaciju događaja i povezivanje međusobno povezanih alarma u bezbjednosne incidente. • Rješenje mora omogućiti pretraživanje prikupljene endpoint telemetrije radi sprovođenja proaktivnih threat hunting aktivnosti. • Rješenje mora omogućiti prikaz procesa i događaja povezanih sa nastankom bezbjednosnog incidenta. • Rješenje mora omogućiti prikaz relevantnih kontekstualnih informacija i metapodataka u okviru bezbjednosnog događaja. • Rješenje mora omogućiti grafički prikaz relevantnih MITRE ATT&CK taktika i tehnika povezanih sa detektovanim prijetnjama. • Rješenje mora omogućiti daljinsku terminalsku sesiju (live shell) prema podržanim krajnjim tačkama radi istrage i odgovora na incidente, uz mogućnost zahtijevanja saglasnosti (consent) krajnjeg korisnika prije uspostavljanja sesije. • Rješenje mora omogućiti selektivno ireverzibilno isključivanje pojedinih zaštitnih modula agenta na nivou pojedinačnog uređaja. • Rješenje mora omogućiti daljinsku mrežnu izolaciju krajnje tačke. • Mora biti moguće zadati izolaciju uređaja koji trenutno nije povezan, pri čemu se zahtijevana akcija izvršava nakon njegovog ponovnog povezivanja sa servisom. • Rješenje mora omogućiti centralno pokretanje response akcija prema jednoj ili više krajnjih tačaka. • Rješenje mora omogućiti preuzimanje relevantnih fajlova sa krajnjih uređaja radi dalje analize, uz mogućnost zaštite preuzetog fajla lozinkom. • Rješenje mora omogućiti izvršavanje skripti ili drugih	300,00 komad
---	--	--	--------------

administratorskih/response akcija na krajnjim uređajima u skladu sa dodijeljenim privilegijama.

- Rješenje mora omogućiti centralni pregled pokrenutih zadataka i status njihovog izvršenja.
- Rješenje mora omogućiti centralizovano upravljanje endpoint agentima.
- Rješenje mora omogućiti pokretanje ažuriranja agenta iz centralnog sistema za upravljanje.
- Rješenje mora omogućiti automatsko ažuriranje endpoint agenta.
- Rješenje mora omogućiti kontrolisanu distribuciju ažuriranja agenata.
- Rješenje mora omogućiti centralno upravljanje allow i deny pravilima za relevantne indikatore i objekte.
- Rješenje mora omogućiti grupisanje krajnjih uređaja prema tehničkim i organizacionim parametrima.
- Rješenje mora omogućiti granularnu primjenu bezbjednosnih politika prema definisanim grupama krajnjih uređaja.
- Instalacioni paket endpoint agenta mora biti kompatibilan sa standardnim sistemima za centralizovanu distribuciju softvera.
- Rješenje mora omogućiti integraciju sa eksternim SIEM i drugim bezbjednosnim sistemima korišćenjem podržanih integracionih mehanizama.
- Rješenje mora evidentirati relevantne administratorske aktivnosti u sistemu.
- Administrativne i bezbjednosno relevantne aktivnosti moraju imati odgovarajući audit trag.
- Rješenje mora omogućiti centralni pregled statusa endpoint sistema, bezbjednosnih događaja, alarma i incidenata.

- Rješenje mora omogućiti generisanje izvještaja o stanju endpoint okruženja i evidentiranim bezbjednosnim događajima.
- Rješenje mora omogućiti definisanje izuzetaka na osnovu identifikovanih bezbjednosnih događaja.
- Rješenje mora podržavati Role-Based Access Control (RBAC).
- Rješenje mora omogućiti višefaktorsku autentifikaciju za pristup upravljačkom sistemu.
- Rješenje mora podržavati Single Sign-On (SSO) korišćenjem standardnih protokola za federaciju identiteta.
- Rješenje mora omogućiti ograničavanje administratorskog pristupa u skladu sa dodijeljenim ulogama i opsegom odgovornosti.
- Rješenje mora imati mogućnost nativne integracije sa Next-Generation Firewall (NGFW) rješenjem istog proizvođača, bez potrebe za korišćenjem posredničkih third-party integracionih platformi, radi razmjene bezbjednosne telemetrije i kontekstualnih informacija o prijetnjama između endpoint i mrežne zaštite, korelacije bezbjednosnih događaja i koordinisanog odgovora na detektovane prijetnje.
- Rješenje mora omogućiti integraciju sa mrežnim i drugim bezbjednosnim sistemima radi razmjene relevantnih informacija o prijetnjama i incidentima.
- Rješenje mora omogućiti korišćenje endpoint telemetrije za centralizovanu analizu, korelaciju i threat hunting.
- Rješenje mora podržavati standardne integracione mehanizme za povezivanje sa drugim bezbjednosnim platformama.
- Ponuđač je dužan izvršiti implementaciju ponuđenog rješenja u informaciono-komunikacionom okruženju

Naručioca.

- Implementacija mora obuhvatiti inicijalnu konfiguraciju platforme, konfiguraciju bezbjednosnih politika, pripremu i distribuciju endpoint agenta, stručnu pomoć u onboardingu krajnjih uređaja i serverskih sistema, konfiguraciju korisničkih i administratorskih privilegija, konfiguraciju logovanja i audita, konfiguraciju potrebnih integracija sa postojećom infrastrukturom,
- Izabrani ponuđač je u obavezi da pruži obuku administratorima platforme u trajanju od minimalno dva dana,
- Implementacija mora biti izvršena na način kojim se minimizira uticaj na raspoloživost postojećih informacionih servisa Naručioca.