PREGLED POSTUPKA #126586

1 PODACI O NARUČIOCU

Naziv naručioca	MINISTARSTVO PRAVDE
PIB	11070094
E-mail	kabinet@mpa.gov.me
Telefon	020/407-501
Internet adresa	mpa.gov.me
Fax	020/407-515
Adresa	ulica Vuka Karadžića 3
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Usluga implementacije, integracije i puštanje u produkcioni rad sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Oliver Bodven
Kontakt	020/407-522
Datum objave	23.11.2026. 16:00

Napomena	Usluga implementacije, integracije i puštanje u produkcioni rad sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu.

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Usluga implementacije, integracije i puštanje u produkcioni rad sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu.	23.11.2026 16:00	27.11.2026 13:00	27.11.2026 13:30	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	**MINISTARSTVO PRAVDE** **Usluga implementacije, integracije i puštanje u produkcioni rad sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu** 48000000 - Softverski paketi i informacioni sistemi 48732000 - Softverski paket za bezbjednost podataka 72200000 - Usluge programiranja programske opreme (softvera) i usluge savjetovanja o programskoj opremi (softveru) 72212732 - Usluge izrade softvera za bezbjednost podataka 72226000 - Savjetodavne usluge u vezi sa testiranjem prihvaćenosti softverskog sistema 72263000 - Usluge implementacije softvera 72265000 - Usluge konfiguracije softvera 72267000 - Usluge održavanja i popravke softvera	20.661,25 EUR	4.338,75 EUR	-	-	-	Otvoreni postupak

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

Opis	Tip uslova / zahtjeva
Način plaćanja je: virmanski	Način plaćanja
Rok važenja ponude je 60 dana od dana otvaranja ponuda.	Rok važenja ponude
Mjesto izvršenja ugovora je Ministarstvo pravde, ulica Vuka Karadžića br. 3.	Mjesto izvršenja ugovora
U postupku nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje što se dokazuje na osnovu uvjerenja ili potvrde organa uprave nadležnog za poslove naplate poreza, odnosno nadležnog organa države u kojoj privredni subjekat ima sjedište	Obavezni uslovi
Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, koja se sačinjava na Obrascu 2 iz Pravilnika o načinu sprovođenja jednostavnih nabavki („Službeni list CG“, broj 016/23, 020/23, 036/23, 114/23, 049/24 i 114/24).	Obrazac 2
U postupku nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja ili potvrde nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište	Obavezni uslovi
Rok za izvršenje ugovora: Ponuđač je obavezan da izvrši implementaciju, integraciju i puštanje u produkcioni rad softverskog rješenja najkasnije u roku od 60 dana od dana potpisivanja ugovora.	Rok izvršenja ugovora

Drugi uslov: Tehnička podrška ponuđača mora trajati 12 mjeseci od dana puštanja u rad. Period podrške obuhvata redovne nadogradnje, otklanjanje kvarova i osiguranje nesmetanog rada.	Drugi uslovi
Rok plaćanja do 30 dana od dana prijema fakture nakon uspješno izvršene usluge implementacije, integracije i puštanja u produkcioni rad softverske platforme, uz potpisan Zapisnik o primopredaji rješenja potpisan od strane ovlašćenog službenika Direktorata za IKT pravosuđa i bezbjednost podataka.	Rok plaćanja
Način utvrđivanja ekvivalentnosti: Ukoliko je u tehničkim specifikacijama predmeta nabavke naveden robni znak, marka, patent, tip ili proizvođač, uz naznaku “ili ekvivalent/no”, privredni subjekat je dužan da u svojoj ponudi u opciji "odgovor" tačno navede koji robni znak, marku, patent, tip ili proizvođača nudi. Ukoliko privredni subjekat u ponudi nudi robni znak, marku, model, patent, tip ili proizvođača koji nije naveden u tehničkoj specifikaciji predmeta nabavke od strane naručioca već nudi tzv ekvivalentan robni znak, marku, patent, tip ili proizvođača, u tom slučaju je dužan u ponudi dostaviti dokaz o ekvivalentnosti. Dokaz o ekvivalentnosti podrazumijeva da se u ponudi dostavi potvrda, stručno mišljenje ili drugi akta kojim se potvrđuje da tzv. ekvivalentan robni znak, marka, patent, tip ili proizvođač koji se nudi ima iste ili bolje karakteristike u odnosu na karakteristike zahtijevane tehničkom specifikacijom predmeta nabavke.	Drugi uslovi

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena
Parametar kvalitet - reference ponuđača. Kvalitet: Minimum dvije reference ponuđača o uspješnom izvršavanju usluga implementacije rješenja za unapređenje bezbjednosti informacionog sistema, u predhodnih pet godina. Naručilac zadržava pravo da kod izdavaoca reference može provjeriti referencu. Broj bodova po osnovu vrednovanja referenci kao mjerila kvaliteta: reference ponuđača = 40 bodova. Ponuđač sa najvećim brojem referenci dobija 40 bodova. Broj bodova za ponuđene reference = broj ponuđenih referenci / najveći broj ponuđenih referenci x 40. Ponuđač koji ne dostavi minimalan broj referenci dobija 0 bodova.

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **20.661,25 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
1	Licenca za centralizovano prikupljanje, analizu i izvještavanje o logovima, sa uslugom podrške proizvođača, na period od 1 (jedne) godine	Nabavka, isporuka, aktivacija, konfiguracija i stavljanje u funkciju FortiAnalyzer-VM (FC1-10-AZVMS-465-01-12) ili ekvivalentne licence na period od 1 (jedne) godine, za kapacitet od 5 GB/dan centralizovanog prikupljanja logova i analitike. FortiCare Premium podrška proizvođača u toku trajanja licence. Servisi IOC (Indicators of Compromise), Security Automation Service i FortiGuard Outbreak Detection Service. Registracija i aktivacija licence na ime naručioca. Konfiguracija sistema: povezivanje mrežne i bezbjednosne opreme naručioca kao izvora logova, podešavanje perioda čuvanja logova (retention) i kreiranje korisničkih naloga sa odgovarajućim pravima pristupa. Podešavanje analitike i izvještavanja: konfiguracija kontrolnih tabli (dashboard), pravila za upozorenja na bezbjednosne događaje i automatskih periodičnih izvještaja prema zahtjevima naručioca.	1,00 komad

2	Licenca za upravljanje ranjivostima i zakrpama na krajnjim radnim stanicama, na period od 1 (jedne) godine za 110 klijenata	Nabavka, isporuka, aktivacija, konfiguracija i stavljanje u funkciju Vulnerability and Patch Management for Check Point Endpoint Security (CP-HAR-EP-PM-1Y) ili ekvivalentne pretplatničke licence na period od 1 (jedne) godine, za 110 (sto deset) klijenata. Podrška proizvođača u toku trajanja licence. Registracija i aktivacija licence na ime naručioca. Konfiguracija sistema: aktiviranje modula na postojećoj Check Point Endpoint Security platformi naručioca, raspoređivanje na 110 krajnjih radnih stanica i definisanje politika skeniranja i instalacije zakrpa. Podešavanje analitike i izvještavanja: pregled identifikovanih ranjivosti (CVE) po nivou rizika, praćenje statusa instaliranih zakrpa i automatski periodični izvještaji prema zahtjevima naručioca.	1,00 komad

3	Usluga rekonfiguracije mrežne i bezbjednosne (security) opreme naručioca	Analiza postojeće konfiguracije mrežne i bezbjednosne opreme (NGFW, svičevi, VPN koncentratori) i izrada prijedloga izmjena u skladu sa zahtjevima naručioca i preporukama dobre prakse. Rekonfiguracija opreme prema zahtjevima naručioca, uključujući izmjene mrežne segmentacije (VLAN), pravila firewall-a, NAT-a i rutiranja, VPN pristupa i politika pristupa. Podešavanje mrežne i bezbjednosne opreme za slanje log poruka i bezbjednosnih događaja ka sistemima za centralizovano prikupljanje i analizu logova i bezbjednosnih događaja iz stavki 1 i 4. Ažuriranje firmvera i softvera opreme na verzije koje preporučuje proizvođač. Izrada rezervnih kopija (backup) konfiguracije opreme prije i nakon svake izmjene, kao i njihova predaja naručiocu. Izmjene konfiguracije se vrše u terminima dogovorenim sa naručiocem, na način koji obezbjeđuje minimalan prekid u radu sistema. Nakon izvršenih izmjena Ponuđač je dužan da naručiocu dostavi ažuriranu tehničku dokumentaciju sa opisom izvršenih izmjena i aktuelnom konfiguracijom opreme.	1,00 komad
		Ponuđač je u obavezi da izvrši usluge implementacije, integracije i puštanja sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu koji posjeduje sljedeće karakteristike: Ponuđeno rješenje treba da bude platforma za centralizovano prikupljanje, normalizaciju, korelaciju i analizu bezbjednosnih događaja (SIEM funkcionalnost sa elementima proširene detekcije i odgovora). Rješenje treba da bude zasnovano na softveru otvorenog	

		koda, licenciranom pod licencom koju priznaje Open Source Initiative, bez naknade za korišćenje samog softvera i bez vremenskog ograničenja upotrebe. Funkcionalnost rješenja ne smije biti uslovljena licencom koja se naplaćuje ili ograničava prema broju nadgledanih uređaja, broju nadgledanih izvora, količini prikupljenih podataka (GB/dan) niti broju događaja u sekundi (EPS). Rješenje mora imati jasno razdvojene funkcionalne slojeve: (a) sloj za prijem i analizu podataka, (b) sloj za indeksiranje i skladištenje podataka, (c) sloj za vizuelizaciju i administraciju putem web interfejsa. Sve komponente moraju da imaju mogućnost instalacije na jednom serveru ili na više servera, u skladu sa tehničkim mogućnostima. Rješenje treba da omogući prijem log poruka sa udaljenih uređaja putem standardnog syslog protokola. Prijem syslog poruka treba biti podržan i preko UDP i preko TCP transporta, sa mogućnošću istovremenog rada oba, kao i sa mogućnošću definisanja proizvoljnog prijemnog porta. Potrebno je da postoji mogućnost ograničavanja prijema podataka na unaprijed definisanu listu dozvoljenih izvornih IP adresa odnosno mrežnih opsega, kako bi se spriječilo neovlašćeno slanje podataka ka sistemu. Rješenje mora obezbjeđivati enkriptovanu komunikaciju između svojih internih komponenti, kao i mogućnost prijema zaštićenog syslog saobraćaja putem TLS-a, neposredno ili posredstvom standardnog syslog posredničkog servisa u okviru iste instalacije. Sistem treba da posjeduje mehanizam za parsiranje (dekodiranje) sirovih log poruka i izdvajanje pojedinačnih polja u strukturirani zapis. Mehanizam mora podržavati definisanje pravila parsiranja pomoću regularnih izraza, u	

4	Usluga implementacije, integracije i puštanja u produkcioni rad sistema za centralizovano prikupljanje, korelaciju i analizu bezbjednosnih događaja u realnom vremenu	tekstualnom formatu čitljivom i izmjenjivom od strane administratora. Rješenje treba u standardnoj isporuci sadržati gotova pravila za prepoznavanje i klasifikaciju događaja sa uređaja vodećih proizvođača mrežne i bezbjednosne opreme (firewall, ruter, svič, IPS/IDS, VPN koncentrator), uz mogućnost naknadnog dodavanja podrške za nove tipove uređaja bez intervencije proizvođača rješenja, kroz konfiguracione datoteke. Sistem mora podržavati definisanje pravila korelacije koja na osnovu jednog ili više povezanih događaja generišu bezbjednosni alarm, sa dodjeljivanjem nivoa ozbiljnosti (severity) i mogućnošću kreiranja pravila po mjeri od strane naručioca. Alarmi moraju biti mapirani na opšteprihvaćene okvire za klasifikaciju napadačkih tehnika (MITRE ATT&CK ili ekvivalentan javno dostupan okvir), sa mogućnošću pretrage i filtriranja događaja po toj klasifikaciji. Rješenje treba da omogući, uz korišćenje posebnog agenta na krajnjim radnim stanicama, evidentiranje instaliranog softvera na nadgledanim sistemima i njegovo poređenje sa javnim bazama poznatih ranjivosti (CVE), uz prikaz identifikovanih ranjivosti i nivoa rizika. Sistem treba da podržava nadzor nad izmjenama kritičnih datoteka i direktorijuma na nadgledanim serverima, sa evidencijom vremena izmjene, tipa izmjene i, gdje je primjenjivo, korisnika koji je izmjenu izvršio, korišćenjem posebnog agenta. Rješenje mora podržavati obogaćivanje alarma podacima iz spoljnih izvora obavještajnih podataka o prijetnjama, putem ugrađenih ili korisnički definisanih integracionih modula, uz mogućnost povezivanja sa javno dostupnim servisima za	1,00 komad

		provjeru reputacije IP adresa, domena i datoteka, kao i čuvanje originalnih (sirovih) log zapisa radi naknadne forenzičke analize. Ponuđač je u obavezi da u okviru implementacije izvrši najmanje sljedeće: Instalacija i konfiguracija agenta na 110 radnih stanica. Prikupljanje Windows Event logova, najmanje za:prijave i odjave korisnika, neuspjele prijave, zaključavanje naloga,izmjene grupa i privilegija, instalaciju servisa. Implementacija Sysmon-a radi detaljnog praćenja procesa i mrežnih konekcija. Inventar hardvera i instaliranog softvera. Detekcija ranjivosti (CVE) po instaliranom softveru. Provjera usklađenosti konfiguracije sa CIS preporukama (SCA). Nadzor izmjena (FIM) kritičnih fajlova i registry ključeva. Provjera sumnjivih fajlova preko servisa VirusTotal ili ekvivalentnog. Automatski odgovor (active response), najmanje blokiranje IP adrese i gašenje procesa. Instalacija i konfiguracija agenta na 20 servera, uz sve funkcionalnosti navedene za radne stanice. Prikupljanje Windows Event logova, najmanje za:prijave i odjave korisnika, neuspjele prijave, zaključavanje naloga,izmjene grupa i privilegija, instalaciju servisa. Implementacija Sysmon-a radi detaljnog praćenja procesa i mrežnih konekcija. Na Linux serverima prikupljanje auditd, SSH i sudo događaja. Detekcija brute-force napada, praćenje izvršenih komandi i nadzor izmjena fajlova sa evidencijom korisnika koji je izmjenu izvršio (whodata). Prijem logova sa FortiAnalyzer-a putem syslog-a.	

		Pravila detekcije najmanje za:IPS događaje, antivirus događaje, web filter događaje, VPN prijave, administratorske prijave, izmjene konfiguracije. Automatsko blokiranje IP adresa na FortiGate-u preko API-ja. Ponuđač izrađuje i isporučuje skriptu za integraciju. Filtriranje logova: šalju se samo odbijeni saobraćaj, UTM događaji i sistemski događaji, bez kompletnih traffic logova. Konfiguracija Check Point Log Exporter-a za izvoz događaja u syslog/CEF formatu, najmanje za: detekcije malvera, blokade, status zakrpa. Izrada vlastitih dekodera i pravila za Check Point endpoint formate koje SIEM rješenje ne podržava u osnovnoj konfiguraciji. Konfiguracija slanja syslog-a sa svičeva. Izrada vlastitih dekodera i pravila najmanje za: podizanje i spuštanje portova, prijave administratora, izmjene konfiguracije, STP promjene, detekciju petlji.	

5	Nadzor, praćenje i izvještavanje u realnom vremenu, konfiguracija security i mrežne opreme.	Ponuđač će u toku trajanja ugovora: Periodično vršiti nadzor i analizu logova i upozorenja generisanih u sistemu: SIEM XDR, FortiAnalyzer, Check Point Endpoint, FortiGate firewalls. Mjesečno dostavljati izvještaj o aktivnostima uočenim tokom praćenja. Mjesečno davati preporuke za implementaciju novih sigurnosnih politika na sistemu. Po potrebi, na zahtjev korisnika, pružiti podršku u rješavanju problema sa security i mrežnom infrastrukturom. Mjesečna podrška, uključujući analizu i izvještavanje, obuhvata trajanje do 10 inženjer sati mjesečno. Obezbijediti telefonsku tehničku podršku radnim danima od 07 do 15 časova. Obezbijediti tehničku podršku putem e-maila radnim danima od 07 do 15 časova.	1,00 komad