Univerzitet Donja Gorica
ERASMUS+ Projekat „CSupMNE“
Broj: 20/25
Podgorica, 23.12.2025

Privatna ustanova Univerzitet Donja Gorica

Vas poziva da uzmete učešće u procesu dostavljanja ponuda za izbor najpovoljnijeg dobavljača za pružanje usluga Unapređenja sajber bezbjednostnih kapaciteta na Univerzitetu Donja Gorica za potrebe realizacije ERASMUS + projekta ERASMUS-EDU-2024-CBHE-STRAND-3/ERASMUS2027/101179688 **„Straightening Up Cybersecurity Posture of Montenegrin Higher Education System“**

I PREDMET NABAVKE:

Predmet nabavke je **Usluga unapređenja Zaštitnih sajber bezbjednostnih kapaciteta Univerziteta Donja Gorica** i **Usluga unapređenja tehničkih kapaciteta za Detekciju sajber bezbjednostnih prijetnji na Univerziteta Donja Gorica** kroz implementacije, nabavke, razvoj i nadogradnja postojećeg integralnog informacionong sistema za potrebe realizacije ERASMUS + projekta ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688 „Straightening Up Cybersecurity Posture of Montenegrin Higher Education System“ prema specifikaciji:

Lot 1. Usluga unapređenja Zaštitnih sajber bezbjednostnih kapaciteta Univerziteta Donja Gorica.

1. Usluga unapređenja sajber bezbjednostnih zaštitnih kapaciteta Univerziteta Donja Gorica			
R. br	**Modul**	**Opis**	**Koli čina**
1.	Nabavka i implementacija cloud-based Web Application Firewall (WAF) i zaštita aplikacija	Predmet nabavke je obezbjeđivanje cloud-baziranog Web Application Firewall (WAF) rješenja, namijenjenog zaštiti web aplikacija i API servisa naručioca od bezbjednosnih prijetnji na aplikativnom sloju. Rješenje treba da obezbijedi zaštitu od najčešćih poznatih ranjivosti, uključujući, ali ne ograničavajući se na napade definisane u okviru OWASP Top 10, kao i mehanizme za detekciju i ublažavanje automatizovanih bot aktivnosti, zloupotreba aplikacija i API servisa.	1

| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

		Traženo rješenje mora biti isporučeno isključivo kao cloud servis, bez potrebe za instalacijom ili održavanjem lokalnog hardvera, softverskih appliance-a ili agentskih komponenti u infrastrukturi naručioca. Rješenje treba da omogući transparentnu integraciju sa postojećim web aplikacijama i API servisima, bez potrebe za izmjenama aplikativnog koda ili značajnim promjenama postojeće infrastrukture. Integracija mora biti realizovana kroz cloud-bazirani zaštitni sloj pozicioniran ispred zaštićenih sistema (npr. putem DNS preusmjeravanja, reverse proxy mehanizama ili ekvivalentnih metoda), tako da cijeli ulazni saobraćaj prema aplikacijama i API servisima prolazi kroz WAF prije dolaska do krajnjih sistema. Rješenje mora podržavati zaštitu aplikacija bez obzira na tehnologiju na kojoj su aplikacije razvijene. Integracija mora omogućiti selektivnu zaštitu pojedinačnih aplikacija ili servisa, primjenu različitih bezbjednosnih politika po aplikaciji ili API-ju, kao i postepeno uključivanje zaštite, u cilju bezbjednog prelaska u produkciono okruženje. WAF rješenje mora da omogući: • automatsku detekciju i blokiranje zlonamjernog saobraćaja; • redovna i automatska ažuriranja bezbjednosnih pravila; • definisanje prilagođenih bezbjednosnih politika i pravila; • zaštitu web aplikacija i API servisa, uključujući REST API-je. U okviru istog cloud rješenja mora biti obezbijeđena i zaštita od DDoS napada na mrežnom, transportnom i aplikativnom sloju, sa mehanizmima za automatsku detekciju anomalija u saobraćaju, efikasno ublažavanje napada i upravljanje bot saobraćajem. Rješenje mora da obezbijedi centralizovani, web-bazirani administratorski interfejs koji omogućava: • praćenje bezbjednosnih događaja u realnom vremenu; • pregled i analizu saobraćaja; • generisanje izvještaja o napadima, blokiranim zahtjevima i bezbjednosnim trendovima. Poželjno je da rješenje omogućava izvoz ili integraciju bezbjednosnih logova prema eksternim sistemima	

		(SIEM/analitika) putem standardnih konektora ili API-ja, ukoliko je dostupno u ponuđenom paketu bez dodatnih uslova. Rješenje mora biti visoko skalabilno i prilagođeno radu sa velikim brojem korisničkih zahtjeva, bez degradacije performansi. Dobavljač mora garantovati minimalnu dostupnost usluge od 99,9% na godišnjem nivou. Dobavljač je dužan da obezbijedi podršku tokom inicijalne konfiguracije, testiranja integracije i validacije ispravnosti rada prije produkcionog korišćenja.	
2.	Nadogradnja postojećeg storage-a za backup (nabavka i ugradnja HPE diskova)	Nabavka, isporuka i ugradnja diskova za proširenje kapaciteta postojećeg storage-a koji se koristi za backup, pri čemu diskovi moraju biti identični/kompatibilni sa postojećim diskovima koji se koriste na produkcionom i backup sistemu. Ponudilac mora isporučiti originalne HPE diskove sljedeće specifikacije (minimum specifikacije): • Requested/Ordered part (P/N): 787648-001 • Opis (SPS): SPS-DRV HD MSA 1.2T 12G 10K 2.5 SAS ENT • Kapacitet: 1,2 TB • Interfejs: SAS 12G • Brzina: 10K • Format: 2,5” • Klasa: Enterprise • Količina za nabavku: 6 (šest) komada • Stanje: novo, originalno, sa garancijom od minimum 12 mjeseci Kompatibilnost: Ponudilac je obavezan da prije isporuke potvrdi kompatibilnost sa postojećim modelom HPE storage. Tačan model storage se dobija upitom na email adresu udg@udg.edu.me Ponuđač mora uključiti sljedeće: • isporuku na lokaciju naručioca, • ugradnju diskova, • provjeru ispravnosti i statusa (controller/storage health), • proširenje RAID/pool kapaciteta u skladu sa postojećom konfiguracijom, Kriterijumi prihvatanja: • isporučeni diskovi odgovaraju P/N 787648-001 i specifikaciji, • diskovi su ugrađeni i storage je proširen bez grešaka, • nema “degraded” stanja i nema aktivnih alarmnih događaja,	1

| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

		• predat je izvještaj o izvedenim radovima + as-built.	
3.	Zahtjevi za EDR/XDR rješenje	Naručilac zahtijeva isporuku, implementaciju i podršku EDR/XDR rješenja, koje obezbjeđuje naprednu zaštitu endpoint uređaja i servera kroz automatizovanu detekciju, odgovor i forenzičku analitiku. Obavezne minimalne funkcionalnosti: Ponuđeno rješenje mora sadržati: 1. EDR zaštita zasnovana na AI/ML. Omogućiti automatsku detekciju i odgovor na prijetnje (malware, exploit, fileless, suspicious behavior) uz minimalnu potrebu za ručnom intervencijom. 2. Prevencija ransomware-a i oporavak (rollback). Spriječiti/zaustaviti ransomware aktivnosti i omogućiti rollback vraćanje kritičnih promjena nastalih tokom napada (gdje je tehnički primjenjivo), uz evidenciju izvršenih radnji. 3. Analiza ponašanja u realnom vremenu (ActiveEDR ili ekvivalent). Detektovati prijetnje kroz korelaciju događaja i ponašanja procesa/korisnika, uz kontekst i uzročno-posljedične veze (process tree, child/parent, command line, network). 4. Kontekstualni prikaz incidenta (Attack Storyline ili ekvivalent). Obezbijediti objedinjeni pregled kompletnog toka napada (“storyline”) radi brže istrage i incident response-a. 5. Brza mitigacija i izolacija. Omogućiti trenutno zaustavljanje zlonamjernih aktivnosti i izolaciju endpointa (network isolation) u roku od nekoliko sekundi/minuta, uz mogućnost selektivnog vraćanja konektivnosti. 6. Centralizovana konzola (XDR). Centralizovano upravljanje, nadzor i izvještavanje kroz jedinstvenu konzolu, sa podrškom za endpoint/server okruženja i integracije (cloud/IoT ili drugi izvori, gdje je primjenjivo). 7. Deception/Decoys (obavezno ili kao opcioni modul – prema ponudi). Podržati “decoys”/deception mehanizme za rano otkrivanje lateralnog kretanja i pokušaja kompromitacije internih resursa. 8. Usklađenost sa MITRE ATT&CK. Obezbijediti mapiranje detekcija/alertova na MITRE ATT&CK tehnike i/ili dokazivu efikasnost kroz javno dostupne evaluacije (gdje je primjenjivo). 9. Forenzički podaci i logovi. Prikupljati i čuvati detaljne telemetrijske i forenzičke podatke (procesi, hash, command line, konekcije, korisničke radnje, promjene na sistemu) radi istrage, izvještavanja i integracije sa SIEM rješenjem.	5

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

		Obavezna isporuka i dokumentacija • Plan implementacije i konfiguracije politika (prevention/detection/response), • Dokumentaciju o integracijama (npr. SIEM), eksportu logova i zadržavanju podataka, • Proceduru incident response-a (izolacija, rollback, cleanup, release from quarantine), • Minimalno osnovnu obuku administratora (operativna upotreba konzole, alarmi, izvještaji).	

Procijenjena vrijednost nabavke je 10.000,00€ bez PDV.

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made

| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

Lot 2. Usluga unapređenja tehničkih kapaciteta za Detekciju sajber bezbjednostnih događaja na Univerzitetu Donja Gorica

2. Usluga unapređenja tehničkih kapaciteta za Detekciju sajber bezbjednostnih događaja na Univerzitetu Donja Gorica			
R. br	**Modul**	**Opis**	**Količina**
1.	Implementacija softverske platforme za detekciju sajber bezbjednostnih događaja	Ponuđač je obavezan da obezbijedi projektovanje, instalaciju, konfiguraciju i puštanje u produkcioni rad softversku platformu namijenjenu za centralizovano prikupljanje, obradu, skladištenje, analizu i vizualizaciju sajber bezbjednosnih događaja, u cilju detekcije i analize bezbjednosnih incidenata, korelacije događaja, nadzora serverskih i krajnjih (endpoint) sistema, kao i izrade standardizovanih i prilagođenih izvještaja. Implementirano rješenje mora da se sastoji od najmanje sljedećih funkcionalnih cjelina: • centralne upravljačke komponente za prijem i obradu događaja, upravljanje agentima i primjenu detekcionih pravila; • komponente za indeksiranje, skladištenje i pretragu događaja i bezbjednosnih alarma; • web-bazirane korisničke konzole za pregled, pretragu, administraciju i upravljanje sistemom. Softverska platforma mora biti instalirana na virtuelnoj infrastrukturi naručioca, kao objedinjena („all-in-one“) instalacija ili kao distribuirana arhitektura na više virtuelnih mašina. Izbor arhitekture mora biti obrazložen i zasnovan na procijenjenom opterećenju sistema (broj događaja u sekundi – EPS), broju agenata, očekivanom rastu sistema i zahtijevanom periodu zadržavanja podataka (retencija). Ponuđač je obavezan da izvrši instalaciju i konfiguraciju svih komponenti sistema, uspostavi bezbjednu i pouzdanu međusobnu komunikaciju između centralnih komponenti, kao i da obezbijedi bezbjedno uključivanje agenata na definisanom broju serverskih i klijentskih sistema. Agenti moraju biti konfigurisani za prikupljanje relevantnih	1

		bezbjednosnih i sistemskih događaja, uključujući, ali ne ograničavajući se na, sistemske dnevnike operativnih sistema, syslog poruke i aplikativne logove, uz primjenu šifrovane komunikacije i kontrolisanog procesa registracije i autorizacije. Rješenje mora omogućiti i prijem syslog poruka sa uređaja i sistema na koje nije moguće ili nije predviđeno instaliranje agenata, uključujući mrežnu i bezbjednosnu infrastrukturu. Ponuđač je dužan da definiše korišćene protokole i portove, listu dozvoljenih izvora, kao i da obezbijedi pravilno parsiranje, indeksiranje i dostupnost prikupljenih događaja za pretragu i analizu putem korisničke konzole. U okviru isporuke, ponuđač je obavezan da: • definiše i dokumentuje politiku retencije i čuvanja podataka; • obezbijedi procedure za backup i restore konfiguracionih podataka i bezbjednosnih zapisa, u skladu sa dogovorenim periodom retencije; • izradi plan redovnog održavanja, nadogradnje i primjene bezbjednosnih zakrpa za sve komponente sistema. Bezbjednosni zahtjevi implementacije moraju obuhvatiti: • zaštitu komunikacije između komponenti sistema korišćenjem odgovarajućih kriptografskih mehanizama; • upravljanje korisnicima i ulogama (RBAC), sa jasno definisanim nivoima pristupa; • primjenu osnovnih mjera hardeninga sistema, uključujući segmentaciju administratorskog pristupa i ograničavanje administrativnih konekcija isključivo na ovlašćene sisteme i korisnike. Kao sastavni dio isporuke, ponuđač je obavezan da dostavi kompletnu tehničku i operativnu dokumentaciju, uključujući: • tehničku dokumentaciju visokog i niskog nivoa (HLD/LLD); • „as-built“ dokumentaciju; • operativni priručnik (runbook) za svakodnevni rad sistema, koji obuhvata procedure nadzora servisa,	

		upravljanje agentima, rješavanje incidenata i postupke oporavka; • test plan i test izvještaj o izvršenim funkcionalnim i bezbjednosnim provjerama. Ponuđač je obavezan da obezbijedi obuku administratora sistema u trajanju od najmanje dva (2) radna dana. Implementacija se smatra uspješno završenom nakon što je potvrđena stabilnost rada svih komponenti sistema, verifikovano pravilno prikupljanje i pretraživost događaja iz definisanih izvora putem korisničke konzole, te potvrđena funkcionalnost minimalnog skupa bezbjednosnih alarma kroz sprovedene kontrolisane testove.	
2.	Uspostavljanje rezervne (backup) lokacije na privatnom cloud-u i proširenje kapaciteta za smještaj backup podataka	Ponuđač je obavezan da izvrši projektovanje, implementaciju i konfiguraciju bezbjedne odredišne backup lokacije na privatnoj cloud infrastrukturi naručioca, namijenjene isključivo za potrebe smještaja i čuvanja backup podataka. Backup lokacija mora biti realizovana kao zasebna, namjenska virtuelna mašina, koja se ne smije koristiti za druge servise ili radna opterećenja. Izvor backup podataka nalazi se u public cloud okruženju. Detaljni tehnički podaci o izvornom okruženju biće dostupni ponuđaču isključivo nakon uspostavljanja formalnog kontakta sa naručiocem i potpisivanja ugovora o povjerljivosti (NDA). Prenos backup podataka između public cloud okruženja i privatnog cloud-a naručioca mora biti realizovan putem bezbjednog VPN tunela, pri čemu se kao prihvatljivo rješenje navodi IPsec ili tehnički ekvivalentna tehnologija. Backup saobraćaj mora biti striktno usmjeren tako da se prenos podataka vrši isključivo kroz uspostavljeni VPN tunel, bez alternativnih ruta. U okviru implementacije, ponuđač je obavezan da kreira i konfiguriše virtuelne mašine zasnovane na Linux open-source operativnom sistemu na lokaciji za oporavak (DR lokacija) u privatnom cloud-u naručioca. Konfiguracija mora obavezno obuhvatiti primjenu mjera sistemskog i bezbjednosnog hardeninga, uključujući, ali ne ograničavajući se na: ograničavanje administratorskog pristupa, segmentaciju mreže, definisanje firewall pravila, instalaciju minimalnog skupa servisa, primjenu	1

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

		bezbjednosnih politika i omogućavanje evidencije i revizije (audit) pristupa i aktivnosti. Virtuelna mašina namijenjena za backup mora biti podešena u skladu sa zahtjevima naručioca, uključujući dodjelu procesorskih, memorijskih i skladišnih resursa, način administrativnog i servisnog pristupa, politike zadržavanja (retencije) podataka, kao i eventualna ograničenja propusnog opsega i definisane vremenske prozore za prenos backup podataka. Ponuđač je obavezan da dokumentuje sve korišćene mrežne portove, tokove saobraćaja i primijenjene bezbjednosne kontrole. Dodatno, ponuđač je obavezan da obezbijedi alternativnu ili komplementarnu implementaciju bezbjednog backup repozitorijuma sa podrškom za nepromjenjivost (immutability), zasnovanu na Linux platformi. Ovakav repozitorijum mora biti realizovan kao namjenska virtuelna mašina, konfigurisana po principu „single-purpose“, sa minimalnim brojem aktivnih servisa. Administrativne privilegije moraju biti striktno definisane u skladu sa principom najmanjih ovlašćenja, uz onemogućavanje interaktivnog administrativnog pristupa gdje je to primjenjivo. Period nepromjenjivosti backup podataka mora biti konfigurisan u skladu sa politikama čuvanja podataka naručioca. Rješenje mora obezbijediti logičku i mrežnu izolaciju backup repozitorijuma, uključujući poseban mrežni segment ili VLAN, ograničen pristup upravljačkim interfejsima, jasno definisana i restriktivna firewall pravila, kao i dozvoljene tokove mrežnog saobraćaja. Ponuđač je obavezan da dokumentuje kompletnu IP i port komunikaciju između backup serverskih komponenti, proxy komponenti i repozitorijuma. Takođe, ponuđač mora obezbijediti mehanizme zaštite od neovlašćenog brisanja ili izmjene backup podataka, evidenciju i audit administratorskih aktivnosti, kao i procedure za kontrolisani i ovlašćeni pristup. Pored backup virtuelne mašine, ponuđač je obavezan da uspostavi i dodatnu virtuelnu mašinu namijenjenu za oporavak sistema u slučaju katastrofe (Disaster Recovery – DR). Na DR virtuelnoj mašini ponuđač mora instalirati i	

		konfigurisati sve neophodne servise i baze podataka, na način koji omogućava spremnost okruženja za pokretanje servisa koji se u redovnom radu izvršavaju u public cloud okruženju. DR okruženje mora biti pripremljeno za sprovođenje procedura oporavka iz backup podataka, uključujući uvoz backup setova, definisane korake oporavka, redosljed pokretanja komponenti sistema, kao i verifikaciju funkcionalnosti nakon oporavka. Ponuđač je obavezan da isporuči detaljno dokumentovan operativni priručnik (runbook) za postupke oporavka u slučaju katastrofe, kako bi se omogućilo brzo i kontrolisano vraćanje sistema u rad u skladu sa unaprijed definisanim ciljevima vremena oporavka (RTO) i tačke oporavka podataka (RPO).	

Procijenjena vrijednost nabavke je 10.000,00€ bez PDV.

II Ponuda treba da sadrži:

1 Opšti dio:

- Tačan naziv i adresu ponuđača, poreski i identifikacioni broj;
- Kontakt ovlašćenog predstavnika;
- Reference ponuđača;
- Garantni rok na isporučenu robu/usluge;
- Ponuđač treba dostaviti ponudu za sve stavke.

2 Komercijalni dio:

- Ponudu dati u jediničnim cijenama, sa i bez PDV-a;
- Ukupna vrijednost ponude izražene u €, sa i bez PDV-a;
- Naznačiti dinamiku i način plaćanja.

III Minimum zahtjeva koje ponuda mora da ispuni:

- Ispunjenje zahtjeva definisanih u tenderskoj dokumentaciji;
- Ponuda mora biti obavezujuća na period od 60 dana. Univerzitet Donja Gorica zadržava pravo na mogućnost produženje ovog roka.
- Ponuđač je u obavezi da pruži kontinuiranu podršku i komunikaciju za Univerzitetom tokom trajanja ugovora.
- Rok za realizaciju svih aktivnosti je 31.05.2026. godine.

U slučaju da izabrani ponuđač odustane od izvršenja ugovora, ili obaveze izvršava suprotno ugovorenom, Univerzitet Donja Gorica se može obratiti drugorangiranom ponuđaču radi zaključivanja ugovora.

IV Kriterijumi vrednovanja ponuda:

Da bi ponuda mogla biti razmatrana mora ispuniti uslove ponude. Ponude koje ne zadovolje gore pomenute uslove neće biti razmatrane.

Vrednovanje ponuda se vrši na osnovu najpovoljnije ekonomske ponude, specifikaciji i referenci ponuđača.

V Dostavljanje ponuda:

Obavezno je opšti i komercijalni dio ponude dostaviti u posebnim i zapečaćenim kovertama sa naznakom na koverti da li se radi o opštem ili komercijalnom dijelu ponude.

Obje koverte dostaviti u trećoj zapečaćenoj koverti na arhivu Univerziteta Donja Gorica Podgorica (ul. Oktoih 1) radnim danima od 09.00-16.00h, sa naznakom:

Za tender nabavku usluga Unapređenja sajber bezbjednostnih kapaciteta na Univerzitetu Donja Gorica za potrebe ERASMUS+ projekta "CSupMNE"– Ne otvarati osim u prisustvu tenderske komisije

Rok za dostavljanje ponuda je 23. 01. 2026. godine do 12.00h.

Kontakt osoba:
Prof.dr Ramo Šendelj
Tel: +382 67 226 333
E-mail: ramo.sendelj@udg.edu.me