

Naša št.: 285-60/4-2026
Datum: 20. 8. 2026

TEHNIČNE SPECIFIKACIJE IN ZAHTEV NAROČNIKA

Varnostne rešitve - programska in strojna oprema, št. 285-60

SKLOP 1: NOZOMI GUARDIAN

SKLOP 2: SANITIZACIJA USB NOSILCEV PODATKOV

SKLOP 3: POVEČANJE LICENČNE KAPACITETE ZA SPLUNK

KAZALO

1	PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA	3
2	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE	4
2.1	SKLOP 1: RAZŠIRITEV NOZOMI GUARDIAN	4
2.1.1	Zahteve za sklop 1	4
2.1.2	Garancija	4
2.1.3	Podpora	5
2.1.4	Rok in kraj dobave	5
2.1.5	Ostale zahteve	5
2.2	SKLOP 2: SANITIZACIJA USB NOSILCEV PODATKOV	6
2.2.1	Zahteve za sklop 2	6
2.2.2	Usposabljanje	9
2.2.3	Inštalacija rešitve in zagon	10
2.2.4	Dokumentacija in testiranje	10
2.2.5	Garancija	10
2.2.6	Podpora	10
2.2.7	Usposobljenost ponudnika	11
2.2.8	Rok in kraj dobave	11
2.2.9	Ostale zahteve	11
2.3	SKLOP 3: POVEČANJE LICENČNE KAPACITETE ZA SPLUNK.....	11
2.3.1	Zahteve za sklop 3	12
2.3.2	Programska podpora za SKLOP 1	12
2.3.3	Rok in kraj dobave	13
2.3.4	Izjava	13

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Naročnik v okviru zagotavljanja visoke ravni kibernetske varnosti, neprekinjenega delovanja kritičnih informacijskih in operativnih sistemov, ter skladnosti z veljavnimi regulativnimi zahtevami (zlasti PART-IS, NIS2 in ISO/IEC 27001) izvaja predmetno javno naročilo za nakup, nadgradnjo in vzdrževanje obstoječih varnostnih rešitev.

Sodobno kibernetsko okolje zaznamujejo hitro razvijajoče se in vse bolj sofisticirane grožnje, ki ciljajo tako informacijske kot operativne sisteme ter dobavne verige. Naročnik že razpolaga z vzpostavljenimi varnostnimi mehanizmi, ki pa jih je zaradi zagotavljanja ustrezne ravni zaščite, razpoložljivosti in skladnosti potrebno redno nadgrajevati, razširjati in vzdrževati.

Predmet javnega naročila tako zajema tri sklope, ki celovito naslavlajo ključna področja kibernetske varnosti:

- detekcije in zaščite operativnih in IoT okolij,
- preprečevanje vnosa zlonamerne kode preko izmenljivih medijev,
- beleženje in ohranjanje revizijskih sledi.
- spremljanje in beleženje dnevniških zapisov in zagotavljanje revizijskih sledi.

Naročilo vključuje nakup nove rešitve za varno uporabo izmenljivih USB nosilcev podatkov, razširitev obstoječe ADS rešitve, kjer trenutne zmogljivosti ne zadoščajo več zahtevam okolja ali zakonskim / regulatornim pričakovanjem, ter nakup dodatnih licenc za obstoječo rešitev za spremljanje, obdelavo in shranjevanje dnevniških zapisov ter revizijskih sledi.

Z izvedbo predmetnega naročila naročnik zasleduje naslednje ključne cilje:

- zgodnje zaznavanje in preprečevanje kibernetskih napadov,
- povečanje odpornosti operativnih sistemov,
- zagotavljanje skladnosti z regulativnimi zahtevami,
- zagotavljanje neprekinjenega in varnega delovanja ključnih storitev.

Posamezni sklopi javnega naročila so medsebojno povezani in tvorijo celovit varnostni ekosistem, ki naročniku omogoča proaktiven, centraliziran in dokazljiv pristop k upravljanju kibernetskih tveganj.

Natančne tehnične specifikacije in zahteve so opisane v nadaljevanju tega dokumenta.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

2.1 Sklop 1: Razširitev Nozomi Guardian

Predmet sklopa 1 je razširitev obstoječe ADS rešitve proizvajalca Nozomi za nadzor in zaznavanje kibernetских groženj v operativnem in IoT okolju - Guardian.

Zaradi uvedbe spremljanja dodatnih prometnih tokov in razširitve nadzorovanega okolja se je bistveno povečal obseg obdelave prometnih tokov, učenja in podatkov, ki presega zmogljivosti obstoječe implementacije. Za zagotavljanje nemotenega in učinkovitega delovanja je zato potrebna nadgradnja v obliki dodatne naprave, ki bo omogočala ustrezno procesiranje in analizo prometa.

Razširitev bo zagotovila ohranjanje visoke ravni vidljivosti nad omrežjem, izboljšala zmožnost zgodnjega zaznavanja varnostnih incidentov ter omogočila nadaljnjo rast nadzorovanega okolja brez vpliva na zmogljivost ali razpoložljivost sistema.

Namen sklopa je zagotoviti zadostne zmogljivosti za obdelavo povečanega obsega podatkov ter s tem ohraniti ustrezno raven zaščite in odpornosti operativnih sistemov.

2.1.1 Zahteve za sklop 1

Postavka	Predmet	Zahteva	Količina
1	Nadgradnja obstoječe ADS rešitve	Nadgradnja obstoječe rešitve z dobavo strojne in programske opreme, model Guardian NS20-1000, proizvajalca Nozomi Networks, vključno s pripadajočo programsko licenco	1 kos
2	Smart Polling licenca - NS20-1000	3 leta	1 kos
3	Asset Intelligence licenca - NS20-1000	3 leta	1 kos
4	Threat Intelligence licenca - NS20-1000	3 leta	1 kos
5	Podpora proizvajalca	3 leta	1 kos

Vsa oprema mora biti dobavljena na lokacijo naročnika (Zg. Brnik 130n, 4210 Brnik – aerodrom) KZPS d.o.o. Dobavljena oprema in licence morajo biti kompatibilne z obstoječo rešitvijo naročnika, ter omogočati njeno nemoteno nadgradnjo brez dodatnih prilagoditev.

Licence morajo vključevati pravico do uporabe, posodobitev in podpore proizvajalca za celotno obdobje trajanja.

2.1.2 Garancija

Zahtevana garancijska doba je 36 mesecev od uspešne primopredaje, t.j. ko naročnik podpiše zapisnik o uspešni primopredaji.

2.1.3 Podpora

Podpora proizvajalca, zahtevana v okviru tega naročila, mora biti zagotovljena za celotno obdobje trajanja garancije oz. licenc, kar se izteče kasneje, ter mora veljati za opremo, nameščeno na lokaciji naročnika.

Podpora proizvajalca mora vključevati najmanj:

- odzivni čas v režimu 8×5 z naslednjim delovnim dnevom (NBD – Next Business Day),
- zamenjavo okvarjene opreme na lokaciji naročnika brez dodatnih stroškov,
- dostop do vseh programskih posodobitev in nadgradenj (vključno s popravki napak, varnostnimi popravki ter minor in major verzijami programske opreme),
- dostop do tehnične dokumentacije in baze znanja proizvajalca (knowledge base),
- dostop do orodij in skript za izvajanje vzdrževalnih opravil (npr. varnostne kopije konfiguracije in drugih sistemskih komponent),
- registracijo podpore proizvajalca neposredno na naročnika.

2.1.4 Rok in kraj dobave

Izvajalec mora dobaviti opremo v roku 30 koledarskih dni po sklenitvi pogodbe.

Pogodbeni stranki ob dobavi opreme in aktivaciji licenc podpišeta prevzemni zapisnik. Z dnem aktivacije licenc začne teči 36-mesečno obdobje za SKLOP 1, pri čemer se 36-mesečno obdobje zagotavljanja licenc in podpore šteje od dneva aktivacije licenc.

2.1.5 Ostale zahteve

Ponudnik mora predložiti izjavo (angl. MAF) odgovorne osebe/proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme/licenc, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj.

..... *konec sklopa 1*

2.2 Sklop 2: Sanitizacija USB nosilcev podatkov

Predmet sklopa 2 je dobava rešitve za varno uporabo izmenljivih USB nosilcev podatkov v informacijskem in operativnem okolju.

Rešitev omogoča preverjanje in sanitizacijo USB naprav pred njihovo uporabo v sistemih naročnika, s čimer se preprečuje vnos zlonamerne programske opreme ter drugih varnostnih tveganj. Uporaba takšne rešitve je ključna predvsem v okoljih, kjer je uporaba izmenljivih medijev nujna zaradi operativnih zahtev.

Namen sklopa je zmanjšati tveganje za kompromitacijo sistemov preko prenosnih medijev ter zagotoviti nadzorovan in varen način prenosa podatkov med različnimi okolji.

Rešitev mora omogočati enostavno in varno uporabo ter delovanje brez vpliva na razpoložljivost in stabilnost obstoječih sistemov.

2.2.1 Zahteve za sklop 2

Postavka	Predmet	Zahteva	Količina
1	Centralna procesna enota (virtualno okolje)	Virtualno okolje za centralno procesiranje in sanitiranje datotek, ki vključuje najmanj 8 AV pogonov različnih proizvajalcev ter CDR (Content Disarm & Reconstruction) funkcionalnost s podporo za obdelavo stisnjenih datotek	1
2	ICAP strežnik	Virtualno okolje za zagotavljanje povezljivosti in dostave datotek v proces sanitiranja preko ICAP protokola	1
3	Centralno upravljanje	Virtualno okolje za centralno upravljanje sistema vključno z licenco, konfiguracijo politik in nadzorom delovanja	1
4	Endpoint programska oprema	Uporabniška programska oprema za omogočanje dostopa do sanitiranih medijev na delovnih postajah	220
5	Terminal za sanitizacijo (kiosk)	Fizična naprava v obliki terminala z zaslonom na dotik za sanitizacijo USB medijev	2
6	Namenska naprava za OT/ICS (Media Firewall)	Fizična naprava za nadzor dostopa do USB medijev na sistemih, kjer namestitev programske opreme ni možna (CNS OT/ICS okolje)	5
7	Podpora proizvajalca	Podpora proizvajalca za celoten sistem (vključno s posodobitvami in nadgradnjami) za obdobje najmanj 24 mesecev in vključenimi 20. inženirskimi urami za pomoč pri implementaciji. Pomoč pri implementaciji obsega; nadgradnja na zadnjo priporočeno različico programske opreme, postavitve opreme na lokaciji naročnika, pomoč pri konfiguraciji opreme, pomoč pri testu delovanja, usposabljanje naročnikovega osebja.	1

Vse programske licence in podpora proizvajalca morajo biti veljavne za obdobje najmanj 24 mesecev.

2.2.1.1 Strojna oprema (HW)

- Ponujena rešitev mora biti na voljo v najmanj dveh različnih velikostih in izvedbah (form factorjih).
- Rešitev mora podpirati več vrst prenosnih medijev, pri čemer podpora ne sme biti omejena zgolj na USB nosilce.
- Rešitev mora temeljiti na strojni platformi, ki vključuje vsaj procesor Intel Core i5-8500 ali zmogljivejši (šest jedrni).
- Rešitev mora vključevati zaslon na dotik (kiosk).

2.2.1.2 Programska oprema (SW)

- Rešitev mora delovati na utrjenem operacijskem sistemu Windows 10 IoT.
- Rešitev mora vključevati mehanizme za sistemsko utrjevanje (hardening).
- Uporabniški vmesnik mora omogočati prilagoditev z logotipom naročnika in izbiro jezika.
- Upravljalvska konzola mora biti dostopna prek naslednjih spletnih brskalnikov:
 - Google Chrome,
 - Mozilla Firefox,
 - Apple Safari,
 - Microsoft Internet Explorer,
 - Microsoft Edge.

2.2.1.3 Varnostne zahteve

- Vsa komunikacija znotraj rešitve mora potekati prek šifriranih komunikacijskih kanalov.
- Spletni dostop do rešitve mora biti omogočen izključno prek protokola HTTPS.
- Rešitev mora omogočati uporabo notranjega (internega) proxy sistema.
- Rešitev mora podpirati upravljanje dostopa na osnovi vlog (RBAC).
- Rešitev mora omogočati integracijo s podatkovnimi diodami (data diode).
- Rešitev mora zagotavljati popolno revizijsko sled vseh pregledanih prenosnih medijev in podatkov, uvoženih v omrežno izolirano okolje in izvoz oziroma prenos v naročnikov SIEM sistem.

2.2.1.4 Omrežne zahteve

- Rešitev mora omogočati delovanje v popolnoma omrežno izoliranih (air-gapped) okoljih.
- Rešitev mora omogočati delovanje kot samostojna naprava brez omrežne povezave.
- Rešitev mora omogočati delovanje v omrežno povezanem načinu.
- Rešitev se sme za potrebe posodobitev povezovati le na en sam vnaprej definiran URL.
- Rešitev mora omogočati ročni uvoz posodobitev, ki so bile predhodno prenesene na sistem z internetno povezavo.
- Mehanizem posodabljanja protivirusnih pogonov in definicij mora podpirati:
 - posodobitve prek interneta,
 - ročne posodobitve,
 - posodobitve prek lokalnih map.
- Rešitev mora omogočati izvoz konfiguracije in izdelavo varnostnih kopij.

2.2.1.5 Upravljanje in administracija

- Rešitev mora zagotavljati centralno upravljanje prek enotnega upravljalvskega vmesnika (»single pane of glass«).

- Rešitev mora omogočati integracijo s sistemi SIEM in standardnim protokolom Syslog.
- Rešitev mora omogočati integracijo z e-poštnimi strežniki za pošiljanje obvestil in opozoril.
- Rešitev mora omogočati samodejno pošiljanje e-poštnih poročil po vsakem opravljenem postopku pregleda.
- Rešitev mora omogočati ustvarjanje uporabniških računov z različnimi administrativnimi in revizijskimi vlogami.
- Rešitev mora podpirati dodeljevanje administrativnih vlog na osnovi skupin Active Directory in LDAP.
- Rešitev mora podpirati več načinov avtentikacije, vključno z avtentikacijo na osnovi RFID.
- Dnevniki delovanja (logi) morajo biti shranjeni lokalno in prenosljivi prek grafičnega uporabniškega vmesnika.
- Rešitev mora omogočati oddaljeno administracijo prek protokolov RDP in HTTPS.
- Rešitev mora vključevati vgrajeno podatkovno bazo.
- Upravljanje vgrajene podatkovne baze mora biti omogočeno neposredno prek uporabniškega vmesnika rešitve.

2.2.1.6 Zaznavanje groženj

- Rešitev mora vključevati več kot 30 različnih protivirusnih pogonov.
- Rešitev mora uporabljati zaznavanje na osnovi:
 - podpisov,
 - hevristike,
 - strojnega učenja.
- Protivirusni pogoni morajo delovati več-nitno (multithreaded).
- Rešitev mora podpirati obdelavo kompleksnih in več nivojskih arhivov.
- Postopek obdelave arhivov mora biti nastavljen.
- Rešitev mora omogočati pregled z geslom zaščitenih arhivov in datotek.
- Rešitev mora omogočati pregled šifriranih USB nosilcev.
- Zaznavanje groženj mora potekati izključno lokalno (on-premise), brez povezave v oblak.
- Licenciranje mora biti enotno za vse uporabljene protivirusne pogone.
- Protivirusni pogoni morajo delovati tudi v omrežno izoliranih (air-gapped) okoljih.
- Frekvenca posodabljanja definicij mora biti nastavljena.
- Vse definicije morajo prihajati iz enotne centralne točke.
- Rešitev mora omogočati zaznavanje znanih ranljivosti v binarnih datotekah.
- Rešitev mora omogočati »in line« integracijo z varnostnimi rešitvami tretjih ponudnikov.
- Rešitev mora omogočati karanteno zaznanih zlonamernih vzorcev za nadaljnjo analizo.
- Rešitev mora omogočati izklop posameznih protivirusnih pogonov.
- Rešitev mora omogočati nastavitve praga lažno pozitivnih zaznav.
- Rešitev mora vključevati tehnologijo za ocenjevanje znanih ranljivosti.
- Rešitev mora zaznavati ranljive namestitvene pakete.
- Rešitev mora zaznavati ranljivosti programske opreme in vdelane programske opreme OT/IoT naprav.
- Rešitev mora vključevati podporo za pravila YARA.

2.2.1.7 Preprečevanje in zaščita podatkov

- Rešitev mora vključevati tehnologijo za razoroževanje in rekonstrukcijo vsebine (CDR / Data Sanitization).
- Tehnologija CDR mora podpirati najmanj 70 različnih vrst datotek.
- Tehnologija CDR mora podpirati obdelavo video datotek.
- Rešitev mora zagotoviti poročilo o odstranjenih objektih v procesu sanitizacije.

- Proces sanitizacije mora biti nastavljen.
- Rešitev mora vključevati modul za preprečevanje izgube podatkov (DLP).
- DLP modul mora podpirati najmanj 30 vrst datotek.
- DLP modul mora podpirati uporabo regularnih izrazov.

2.2.1.8 Funkcionalne zahteve

- Rešitev mora omogočati samodejni prenos preverjenih (čistih) datotek na sekundarni USB nosilec.
- Rešitev mora omogočati samodejni prenos preverjenih datotek v omrežno mapo.
- Rešitev mora omogočati samodejni prenos preverjenih datotek v varno hrambo.
- Varna hramba mora omogočati neprekinjen nadzor in pregled shranjenih datotek.
- Rešitev mora omogočati nadzorovan izvoz podatkov iz varovanega v manj varovano okolje.
- Rešitev mora zagotavljati revizijske dnevnike vseh postopkov.
- Rešitev mora omogočati postopek potrditve s strani nadzornika (four-eyes principle).
- Rešitev mora omogočati obdelavo podatkov iz mobilnih naprav Android in iOS.
- Rešitev mora podpirati procese uvoza in izvoza podatkov.
- Namestitev rešitve mora biti prilagodljiva in omogočati delovanje v različnih okoljih.
- Tok podatkov mora biti nastavljen glede na uporabnike in skupine.
- Rešitev mora omogočati digitalno podpisovanje obdelanih USB nosilcev s certifikatom.
- Rešitev mora omogočati preverjanje podpisanih USB nosilcev na končnih točkah.
- Rešitev mora podpirati obdelavo in razširjanje arhivov naslednjih tipov:
- Zip, 7z, Jar, RAR, RAR5, TAR, ISO, Gzip, CAB, ARJ, LZH, RPM, DEB, LZMA, WIM, SFX, XZ, VDI, VHD, MBR, CPIO, HFS, APK, GZ, MSI, TGZ, TBZ, BZ2.
- Rešitev mora obravnavati dokumente Microsoft Office kot arhive.
- Rešitev mora podpirati samorazširljive arhive narejene s programi: 7-Zip, WinRAR, PKZIP, IExpress.
- Rešitev mora omogočati črne in bele sezname na osnovi hasha, imena datoteke, vrste datoteke ali MIME tipa.
- Karantena mora omogočati integracijo z zunanjimi viri za potrebe obveščevalnih podatkov o grožnjah (threat intelligence).
- Rešitev mora omogočati konfiguracijo različnih delovnih tokov za prilagoditev vrstnega reda in načina obdelave datotek.

2.2.2 Usposabljanje

Zahteva se izvedba osnovnega tehničnega, usposabljanja za osebje naročnika. Usposabljanja se bo udeležilo 4 do največ 6 udeležencev – osebje naročnika. Usposabljanje mora trajati 1 delovni dan v obsegu 4 ur (1 ura je 60 minut), ki je vključeno v 20 inženirskih ur za pomoč pri implementaciji.

2.2.2.1 Obseg usposabljanja

Ponudnik mora zagotoviti usposabljanje za uporabo dobavljene rešitve, ki zajema osnovno in napredno uporabo sistema ter njegovo upravljanje.

Usposabljanje mora vključevati:

- uporabo sistema za sanitizacijo prenosnih medijev (kiosk in programska oprema),
- upravljanje politik in pravil,
- pregled dogodkov, poročanje in revizijske sledi,
- osnovne postopke diagnostike in odpravljanja težav.

Usposabljanje mora biti izvedeno za najmanj:

- skrbnike sistema (administrativni nivo),

- operativne uporabnike (uporaba kioskov in medijev).

Usposabljanje mora biti izvedeno na lokaciji naročnika ali na daljavo, v slovenskem ali angleškem jeziku, ter mora vključevati ustrezna gradiva za nadaljnjo uporabo.

Ponudnik mora zagotoviti tudi prenos osnovnega znanja za samostojno upravljanje sistema po zaključku implementacije.

2.2.3 Inštalacija rešitve in zagon

Ponudnik mora zagotoviti dobavo, namestitev in osnovno konfiguracijo celotne dobavljene rešitve tako, da bo pripravljena za uporabo v okolju naročnika in podporo naročniku v obsegu 20 ur (1 ura = 60 minut).

Inštalacija mora vključevati:

- namestitev vseh programskih komponent v virtualnem okolju naročnika,
- priklop in osnovno konfiguracijo strojne opreme (kiosk terminali in namenske naprave),
- vzpostavitev poveztljivosti med komponentami sistema,
- inicialno konfiguracijo osnovnih politik delovanja,
- preverjanje pravilnega delovanja sistema.

Inštalacija se mora izvesti na način, ki ne vpliva na delovanje obstoječih informacijskih in operativnih sistemov naročnika.

Ponudnik mora naročniku predati tudi osnovno tehnično dokumentacijo za uporabo in upravljanje sistema.

2.2.4 Dokumentacija in testiranje

2.2.4.1 Dokumentacija

Najpozneje ob primopredaji opreme, t.j. po uspešno izvedenem testiranju, je izvajalec dolžan naročniku izročiti ustrezno tehnično dokumentacijo, ki mora obsegati najmanj:

- opis dobavljene strojne in programske opreme,
- navodila za osnovno upravljanje in uporabo sistema,
- navodila za osnovno diagnostiko in odpravo napak,

Dokumentacija mora biti predana v elektronski obliki in mora biti dovolj podrobna, da omogoča samostojno upravljanje sistema s strani naročnika.

2.2.5 Garancija

Zahtevana garancijska doba je 12 mesecev od uspešne primopredaje, t.j. ko naročnik podpiše zapisnik o uspešni primopredaji.

2.2.6 Podpora

Podpora proizvajalca mora biti zagotovljena za celotno obdobje trajanja licenc in mora vključevati:

- podporo preko uradnega portala proizvajalca za prijavo in obravnavo incidentov,
- dostop do tehnične dokumentacije, baze znanja (knowledge base) in drugih podpornih virov proizvajalca,
- zagotavljanje podpore v delovnem času proizvajalca,
- dostop do programskih posodobitev, varnostnih popravkov in novih verzij programske opreme v času trajanja podpore.
- Podpora mora biti registrirana neposredno na naročnika in mora veljati za celotno obdobje trajanja pogodbe.

2.2.7 Usposobljenost ponudnika

Usposobljenost ponudnikovega kadra za instalacijo, konfiguriranje, vzdrževanje, tehnično podporo opreme ponujenega proizvajalca:

- Ponudnik mora zagotoviti najmanj enega (1) strokovnjaka, ki ima veljavno potrdilo/certifikat proizvajalca ponujene opreme/rešitve, da je opravil oz. je usposobljen za upravljanje in konfiguracijo ponujene opreme/rešitve.

2.2.8 Rok in kraj dobave

Izvajalec mora dobaviti opremo v roku 60 koledarskih dni po sklenitvi pogodbe.

Pogodbeni stranki ob dobavi opreme in aktivaciji licenc podpišeta prevzemni zapisnik. Z dnem aktivacije licenc začne teči 24-mesečno obdobje za SKLOP 2, pri čemer se 24-mesečno obdobje zagotavljanja licenc in podpore šteje od dneva aktivacije licenc.

2.2.9 Ostale zahteve

Ponudnik mora predložiti izjavo (angl. MAF) odgovorne osebe/proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme/licenc, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj.

..... *konec sklopa 2*

2.3 Sklop 3: Povečanje licenčne kapacitete za Splunk

Predmet javnega naročila je razširitev licenčne kapacitete obstoječega in že vzpostavljenega sistema Splunk, ki se uporablja za centralizirano zbiranje, obdelavo, analizo in spremljanje dnevnih ter varnostnih dogodkov informacijskih sistemov.

Zaradi širitve obsega sistema, vključevanja dodatnih informacijskih virov ter posledičnega povečanja količine dnevnih podatkov obstoječa licenčna kapaciteta ne zadošča več dejanskim potrebam.

Predmet naročila je zato povečanje obstoječe licenčne kapacitete za dodatnih 30 GB podatkov na dan (30 GB/dan) za obdobje od 1.11.2026 do vključno 31.5.2027.

Pri tem naročilu ne gre za vzpostavitev novega SIEM sistema, temveč za razširitev licenciranja že implementiranega in operativnega okolja Splunk, s čimer se zagotavlja zadostna kapaciteta za nadaljnje vključevanje podatkovnih virov, ter nemoteno izvajanje centraliziranega spremljanja in analize varnostnih dogodkov.

2.3.1 Zahteve za sklop 3

V nadaljevanju so navedene minimalne zahteve naročnika, ki jih mora izpolniti ponudnik za zagotovitev primerne SIEM rešitve.

Postavka	Predmet	Zahteva	Kosov
2.3.1.1	Nakup SIEM licence za obdobje 8 mesecev	Dodatna licenca za hranjenje zapisov za 30 GB/dan za obstoječo SIEM Splunk rešitev	1 KPL
2.3.1.2	Programska podpora	Programska podpora za obdobje 7 mesecev	1 KPL

Licenčna oprema se nabavlja za obdobje 7 mesecev. V času veljavnosti licenc morajo biti za naročnika zagotovljene vse nadgradnje in morebitni popravki programske opreme, ki je predmet tega naročila.

2.3.2 Programska podpora za SKLOP 3

Tehnična podpora in SLA:

- Dostop do podpore preko e-pošte, portala in telefona;
- Popravki in varnostne posodobitve:
 - Ponudnik mora zagotoviti dostop do programske opreme za vzdrževanje celotne rešitve (hotfixi, minor/major verzije jedra in komponent);
 - Ponudnik mora zagotoviti programske popravke za odpravo varnostnih pomanjkljivosti v 15 dneh po objavi;
- Ponudnik mora zagotoviti dostop do baze znanja in dokumentacije:
 - Dokumentacija o nameščenem sistemu;
 - Navodila za obratovanje, diagnostiko in povrnitev, dostop do baze znanja »knowledge base«;
 - Dostop do skript za opravljanje rutinskih opravil (npr. za backup konfiguracije, repozitorijev in filtrov);
 - Izvajalec registrira podporo proizvajalca neposredno na naročnika.

V času veljavnosti licenc, tj. v obdobju 7 mesecev mora biti za naročnika zagotovljena tehnična podpora proizvajalca z odzivnim časom 2 ure v režimu 8 × 5 NBD (Next Business Day).

Za odzivni čas se šteje čas, v katerem proizvajalec potrdi od naročnika prejeto obvestilo o napaki.

2.3.3 Rok in kraj dobave

Izvajalec mora dobaviti licence v roku 10 koledarskih dni po sklenitvi pogodbe.

Pogodbeni stranki ob dobavi licenc podpišeta prevzemni zapisnik. Aktivacija licenc se mora izvesti na dan 1. 11. 2026 in mora trajati do 31. 5. 2027, s tem začne teči 7-mesečno obdobje podpore.

2.3.4 Izjava

Ponudnik mora predložiti izjavo (angl. MAF) odgovorne osebe/proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme/licenc, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj, za blagovno znamko, ki jo ponuja.

..... *konec sklopa 3*

..... *konec dokumenta*

