

Naša št.: 285-52/4-2025
Datum: 6. 11. 2025

TEHNIČNE SPECIFIKACIJE IN ZAHTEVE NAROČNIKA

Programska oprema in SIEM rešitev, št. 285-52

SKLOP 1: SIEM rešitev, licenčnina in podpora

SKLOP 2: Podpora za ArcSight SIEM

KAZALO

1	PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA	3
2	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE - SKLOP 1	3
2.1	SKLOP 1: SIEM rešitev, licenčnina in podpora	3
2.1.1	Specifikacija in tehnične zahteve za SKLOP 1	3
2.1.1.1	Tehnične zahteve za SKLOP 1	3
2.1.1.2	Programska podpora za SKLOP 1	5
2.1.2	Ostale zahteve za SKLOP 1	7
2.1.2.1	Izjava	7
2.1.2.2	Usposobljenost kadra	7
2.1.2.3	Reference ponudnika	7
2.1.2.4	PART-IS	7
3	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE - SKLOP 2	8
3.1	SKLOP 2: Nadgradnja in podpora obstoječega sistema za upravljanje varnostnih dogodkov	8
3.1.1	Specifikacija in tehnične zahteve za SKLOP 2	8
3.1.2	Tehnične zahteve za SKLOP 2	8
3.1.3	Ostale zahteve za SKLOP 2	9
3.1.3.1	Izjava	9

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Predmet tega javnega naročila je izbor usposobljenega izvajalca za vzpostavitev in upravljanje naslednjih gradnikov varnostnega ekosistema KZPS, po posameznih sklopih:

- SKLOP 1: SIEM rešitev, licenčnine in podpora
- SKLOP 2: Podpora za ArcSight SIEM

Licenčna oprema za sklop 1 se nabavlja za obdobje 4 let, oziroma 48 mesecev, šteto od dneva aktivacije licenc oz. od dneva podpisanega primopredajnega zapisnika, podpora sistema za sklop 2 pa se nabavlja za obdobje 1 leta, oziroma 12 mesecev, šteto od dneva aktivacije licenc.

Z vzpostavitvijo teh storitev želi KZPS okrepiti svojo kibernetsko odpornost, izboljšati čas zaznave in odziva na kibernetski incident (MTTD/MTTR), ter zagotoviti trajnostno in prilagodljivo varnostno infrastrukturo, ki je sposobna spremljati hitro razvijajoče se grožnje. Naročnik bo izbral ponudnika, ki skladno z dokumentacijo v zvezi z oddajo javnega naročila in zahtevami tega dokumenta izkaže ustrezne reference, kompetence in certifikate ter ponudi tehnološko napredno SIEM rešitev za proaktivno, varno in zanesljivo zbiranje varnostnih dogodkov iz različnih informacijskih in operativnih virov, ter izvajanje korelacij in analiz.

Natančne tehnične specifikacije za SKLOP 1 in SKLOP 2, ter ostale zahteve so opisane v nadaljevanju tega dokumenta.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE - SKLOP 1

2.1 SKLOP 1: SIEM rešitev, licenčnina in podpora

Predmet sklopa 1 je namenjen izboru SIEM rešitve, ki omogoča centralizirano zbiranje, korelacije in analize varnostnih dogodkov iz različnih informacijskih in operativnih virov.

2.1.1 Specifikacija in tehnične zahteve za SKLOP 1

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

Postavka	Predmet	Zahteva	Kosov
2.1.1.1	Nakup SIEM licence za obdobje 48 mesecev	Licenca za prvo leto za hranjenje zapisov za 50 GB/dan, za drugo in vsako naslednje leto 100 GB/dan skupaj za obdobje 48 mesecev	1 KPL
2.1.1.2	Programska podpora	Programska podpora za obdobje 48 mesecev	1 KPL
2.1.1.3	Storitve inštalacije in integracije sistema	Inštalacija in integracija sistema v naročnikovo okolje	1 KPL

Licenčna oprema se nabavlja za obdobje 4 let. V času veljavnosti licenc morajo biti za naročnika zagotovljene vse nadgradnje in morebitni popravki programske opreme, ki je predmet tega naročila.

2.1.1.1 Tehnične zahteve za SKLOP 1

- Sistem za spremljanje dogodkov mora biti implementiran kot lokalna rešitev (angl. on-premises).
- Rešitev mora zagotoviti zaščito indeksiranih podatkov pred spreminjanjem.

- Sistem za spremljanje dogodkov mora delovati v porazdeljeni arhitekturi (ločeni iskalni in indeksni strežniki), pri čemer mora biti omogočena visoka razpoložljivost z replikacijo podatkov.
- Sistem za spremljanje dogodkov mora zbirati dogodke/dnevnik informacijske infrastrukture in statistiko omrežnega prometa, ter jih hraniti kot revizijsko sled, tudi v primeru izpada komunikacijskih povezav.
- Omogočeno mora biti zbiranje podatkov v običajnih formatih (csv, txt, ...).
- Sistem za spremljanje dogodkov mora podpirati zunanje podatkovne repozitorije za dolgoročno shranjevanje arhivskih podatkov.
- Sistem za spremljanje dogodkov mora omogočati odpornost na izgubo hranjenih podatkov v primeru izpada oz. okvare katere koli komponente sistema.
- Predlagani sistem za spremljanje dogodkov mora biti sposoben zbirati dogodke iz:
 - sistemov (DHCP, DNS, Active Directory),
 - omrežne opreme (usmerjevalniki, stikala, brezžične dostopne točke, delilniki bremen),
 - naprav za omrežno varnost (požarni zidovi, požarni zidovi spletnih aplikacij - WAF, IPS/IDS),
 - operacijskih sistemov (Windows, Unix, Linux),
 - sistemov za upravljanje podatkovnih baz (Oracle, MS SQL, PostgreSQL),
 - delovnih postaj,
 - ostale omrežne in varnostne opreme;
- Predlagani sistem za spremljanje dogodkov mora podpirati standardne protokole za zbiranje dogodkov, kot so: syslog, syslog NG, SNMP, JDBC, OPSEC, API, Windows dnevniški zapisi (varnostni dogodki, AD, revizijski zapisi) in strukturirane besedilne datoteke.
- Sistem za spremljanje dogodkov mora omogočati pošiljanje poročil v HTML ali besedilnem formatu (npr. PDF, XLS) po elektronski pošti.
- Sistem za spremljanje dogodkov mora imeti pred pripravljena poročila (ki jih zagotovi proizvajalec). Omogočeno mora biti tudi ustvarjanje prilagojenih poročil ali uporaba orodij tretjih oseb za poročanje.
- Sistem za spremljanje dogodkov mora omogočati proženje opozoril v realnem času.
- Sistem za spremljanje dogodkov mora omogočati nastavitve samodejnega (po urniku) ali ročnega načina generiranja poročil. Omogočati mora napredno kontrolo pošiljanja alarmov z namenom preprečevanja prekomernega pošiljanja ponavljajočih opozoril.
- Sistem za spremljanje dogodkov mora centralno spremljati procese, ki potekajo v sistemu za spremljanje dogodkov, delovanje dodatnih modulov ali programske opreme ter v primeru okvare o tem obvestiti uporabnike sistema za spremljanje dogodkov.
- Sistem za spremljanje dogodkov mora imeti grafični vmesnik (GUI). Povezava z grafičnim vmesnikom mora potekati preko varnih, šifriranih protokolov (na primer HTTPS). Za uporabo grafičnega vmesnika ni potrebna namestitev dodatne programske opreme z licenco. Grafični vmesnik mora biti podprt na najnovejših različicah Firefox, Safari, Chrome in Microsoft Edge.
- Grafični uporabniški vmesnik sistema za spremljanje dogodkov ne sme uporabljati zastarelih oziroma nepodprtih tehnologij.
- Sistem za spremljanje dogodkov mora imeti orodja za grafični prikaz dogodkov, pripravljena s strani proizvajalca (interaktivni prikazi, histogrami, orodja za ogled poteka dogodkov v realnem času itd.).
- Sistem za spremljanje dogodkov mora imeti funkcionalnost centralizirane avtentikacije uporabnikov. Preden uporabniku omogoči prijavo v grafični vmesnik, mora sistem za spremljanje dogodkov preveriti identiteto uporabnika in mu dodeliti le tista administrativna dovoljenja, ki so mu dodeljena.
- Sistem za spremljanje dogodkov mora omogočati dodeljevanje pravic uporabnikom za dostop samo do naprav in virov podatkov, ki so namenjeni njim (nadzor dostopa na podlagi vlog).
- Sistem za spremljanje dogodkov mora podpirati nadzor dostopa uporabnikov z uporabo podrobnih seznamov za upravljanje dostopnih pravic.
- Sistem za spremljanje dogodkov mora beležiti vsa dejanja, ki jih izvajajo sistemski administratorji (revizijska sled dostopov in sprememb na sistemu).

- Sistem za spremljanje dogodkov mora imeti možnost integracije z zunanjimi direktoriji uporabnikov (na primer: AD, LDAP, SAML,...).
- Število administratorjev in spletnih uporabnikov, ki so istočasno prijavljeni v sistem za spremljanje dogodkov, ne sme vplivati na delovanje sistema.
- Sistem za spremljanje dogodkov mora omogočati ogled dogodkov v realnem času. Podatki, ki jih sistem prejema morajo biti indeksirani v realnem času (manjši od 5 sekund od vnosa do iskanja).
- Sistem za spremljanje dogodkov mora obvestiti, če kateri koli vir podatkov preneha pošiljati dogodke.
- Predlagani sistem za spremljanje dogodkov mora omogočati opisovanje, zbiranje in normalizacijo zapisov standardnega in nestandardnega formata (strukturiranih in nestrukturiranih podatkov) brez potrebe po predhodnem določanju sheme vira. Omogočati mora ti. schema-on-read, da je omogočena takojšnja analiza sporočil brez priprave modela parsanja.
- Sistem za spremljanje dogodkov mora imeti zrelo ekosistemsko okolje, ki omogoča prirojene (angl. native) integracije.
- Sistem za spremljanje dogodkov mora imeti možnost izvajanja strojnega učenja na lastnih podatkih (kot je npr. MLTK).
- Sistem za spremljanje dogodkov mora omogočati t.i. »native« integracijo z orodjem za orkestracijo – SOAR.
- Sistem za spremljanje dogodkov mora omogočati skalabilnost celotne rešitve z dodajanjem novih virtualnih komponent sistema brez omejitve zmogljivosti uvoza oz. pregledovanja.
- Sistem za spremljanje dogodkov mora omogočati razširitev na terabajte dnevnega vnosa podatkov.
- Sistem za spremljanje dogodkov mora podpirati naslednji operacijski sistem: MS Windows, Linux
- Sistem za spremljanje dogodkov mora biti nameščen na lokalni (angl. on-premises) virtualni infrastrukturi naročnika in mora omogočati razporeditev gradnikov med več lokacijami z visoko razpoložljivostjo ter podporo za DR.
- Sistem za spremljanje dogodkov mora biti nameščen kot porazdeljeno (angl. distributed) okolje, kjer morajo biti upravljalni procesi ločeni od zbiralnikov dnevnikov.
- Sistem za spremljanje dogodkov mora podpirati možnost nadgradnje operacijskega sistema s ponovnim zagonom brez izgube podatkov oz. brez prekinitve.
- Načrtovano skupno število nadzorovanih objektov je najmanj 3100 enot (vključno s strežniki, fizičnimi in virtualnimi delovnimi postajami, omrežno opremo, ...).
- Sistem za spremljanje dogodkov mora omogočati vnos (angl. ingest) 100 GB podatkov na dan.
- Rešitev mora omogočati licenciranje na osnovi indeksiranega obsega podatkov (GB/dan) in ne sme biti vezano na število naprav, agentov, uporabnikov ali EPS (events per second). Sistem mora nemoteno delovati tudi v primeru preseganja obsega licence. Omogočati mora metode za natančno določitev in optimizacijo sporočil glede na porabo licence.
- Sistem za spremljanje dogodkov mora omogočati shranjevanje dogodkov za najmanj zadnjih 6 mesecev (dnevniške zapise in statistiko omrežja). Omogočeno mora biti iskanje in pregledovanje dogodkov na podlagi določenih kriterijev.
- Veljavnost licence mora biti min. 4 leta z upoštevanjem rasti naročnika: prvo leto mora sistem omogočati vnos do 50 GB/dan, drugo in vsako naslednje leto do vključenega 4 leta pa 100 GB/dan.

2.1.1.2 Programska podpora za SKLOP 1

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 4 let, 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.

2.1.1.3 Storitve inštalacije in integracije sistema

Implementacija sistema za upravljanje z varnostnimi dogodki je zamišljena v sledečih korakih:

- Analiza zahtev in okolja naročnika;
- Namestitev, konfiguracija in integracija rešitve v virtualno okolje naročnika;
- Integracija posameznih virov iz operative in poslovne informatike;
- Priprava osnovnih varnostnih pogledov, poročil in obveščanja;
- Izvedba izobraževanja za uporabnike;
- Razvoj dodatnih nadzornih pogledov in opozoril;
- Nudenje tehnične podpore in upravljanja do prevzema sistema s strani naročnika.

Posamezni od zgoraj naštetih korakov je v celoti zaključen, ko so izpolnjeni vsi zahtevani pogoji, ki so navedeni v sledeči tabeli:

Opis faze	Dosežen mejnik za zaključek faze	Ocena porabe ur
Analiza zahtev in okolja naročnika	<ul style="list-style-type: none"> ➤ Seznam identificiranih virov dnevnikov - »log sources« ➤ Predlog arhitekture 	25
Namestitev, konfiguracija in integracija rešitve v virtualno okolje naročnika	<ul style="list-style-type: none"> ➤ Sistemska izvedbena dokumentacija ➤ Konfigurirane, nameščene in operative instance končnega sistema 	100
Integracija posameznih virov iz operative in poslovne informatike	<ul style="list-style-type: none"> ➤ Seznam vključenih virov logov ➤ Sistemska izvedbena dokumentacija 	80
Priprava osnovnih varnostnih pogledov, poročil in obveščanja	<ul style="list-style-type: none"> ➤ Zbirka EOI – Events of Interest (varnostnih kontrol ki se spremljajo) ➤ Seznam in dokumentacija aktivnih opozoril (alertov), pogledov in poročil ➤ Sistemska izvedbena dokumentacija 	120
Izvedba izobraževanja za uporabnike	<ul style="list-style-type: none"> ➤ Izvedeno usposabljanje naročnikovega osebja v obliki delavnice 	30
Razvoj dodatnih nadzornih pogledov in opozoril	<ul style="list-style-type: none"> ➤ Dodatni pogledi in napredna poročila ➤ Seznam t.i. »Custom alertov« za specifične scenarije naročnika 	120
Nudenje tehnične podpore in upravljanja do prevzema sistema s strani naročnika	<ul style="list-style-type: none"> ➤ Zaključena sistemska izvedbena dokumentacija ➤ Predaja sistema v upravljanje naročniku 	50
Ocenjeno število ur skupaj:		525

2.1.2 Ostale zahteve za SKLOP 1

2.1.2.1 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.

2.1.2.2 Usposobljenost kadra

Ponudnik mora izkazati, da razpolaga z zadostnim številom strokovno usposobljenih kadrov, ki bodo zagotavljali storitve, ki so predmet tega naročila. Naročnik zahteva usposobljenost s področja instalacije, konfiguriranja, vzdrževanja, tehnične podpore SIEM rešitve.

Ponudnik mora zagotoviti zadostno število strokovno usposobljenih kadrov (najmanj 5), in sicer:

- tri (3) strokovnjake specialiste z inženirskim znanjem (expertni nivo) za upravljanje, in konfiguracijo ponujene SIEM rešitve. Kot ustrezno dokazilo se štejejo priloženi certifikati, proizvajalca ponujene SIEM rešitve;
- dva (2) strokovnjaka s tehničnim znanjem (specialistični nivo) za vzdrževanje ponujene SIEM rešitve. Kot ustrezno dokazilo se šteje priložen certifikat, proizvajalca ponujene SIEM rešitve.

Vsi certifikati morajo biti veljavni na dan oddaje ponudbe. Izbrani ponudnik pa mora zagotoviti, da bodo certifikati veljavni cel čas trajanja/izvajanja pogodbe. Veljavnost certifikatov se izkazuje z izpisom, kjer je tudi razvidno trajanje veljavnosti certifikata. Izbrani ponudnik mora ves čas trajanja predmetnega naročila razpolagati z ustrezno usposobljenimi strokovnjaki z veljavnimi certifikati.

Vsi strokovnjaki morajo aktivno govoriti slovenski jezik (nivo B2 v skladu s CEFR), naročnik pa si pridružuje pravico, da od ponudnika glede tega zahteva ustrezna dokazila.

2.1.2.3 Reference ponudnika

Ponudnik mora imeti vsaj tri (3) reference, ki vključujejo primerljiva dela/storitve s področja predmeta tega javnega naročila (referenčna dela), ki jih je uspešno izvedel v obdobju zadnjih treh letih, šteto od dneva objave te razpisne dokumentacije v zvezi z oddajo javnega naročila.

Ponudnik izkaže izpolnjevanje tega pogoja s predložitvijo:

- dveh (2) referenc o postavitvi, sistema za upravljanje z varnostnimi dogodki v obsegu najmanj 4000 enot nadzorovanih objektov – »log source-ov« (vključno s strežniki, fizičnimi in virtualnimi delovnimi postajami, omrežno opremo, dostopnimi točkami, aplikacijami, ...) za posamezno postavitev, od tega mora biti ena (1) referenca izdana s strani referenčnega naročnika, ki je zavezanec po ZinfV-1;
- eno (1) referenco o postavitvi, sistema za upravljanje z varnostnimi dogodki v obsegu najmanj 4000 enot nadzorovanih objektov – »log source-ov« (vključno s strežniki, fizičnimi in virtualnimi delovnimi postajami, omrežno opremo, dostopnimi točkami, aplikacijami, ...) za posamezno postavitev pri referenčnem naročniku ki imenovan izvajalec bistvenih storitev (letalskega, cestnega, železniškega prometa) in s sedežem v Sloveniji.

2.1.2.4 PART-IS

Izbran ponudnik mora zagotoviti, da bodo vse pogodbeno izvedene dela, ki vključujejo ali vplivajo na informacijske sisteme, podatke ali procese, pomembne za varnost civilnega letalstva, potekala v skladu z zahtevami Izvedbene uredbe (EU) 2023/203 o določitvi pravil

za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu (v nadaljevanju: Uredba). Naročnik zahteva, da izbrani ponudnik oz. izvajalec izvaja/zagotavlja svoje storitve na ustrezni ravni informacijske varnosti in skladnosti z zahtevami omenjene Uredbe, ki vključujejo zahteve iz Priloge II (Part-IS.I.OR).

3 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE - SKLOP 2

3.1 SKLOP 2: Nadgradnja in podpora obstoječega sistema za upravljanje varnostnih dogodkov

3.1.1 Specifikacija in tehnične zahteve za SKLOP 2

Specifikacija in tehnične zahteve so podane spodaj.

Postavka	Predmet	Zahteva	Kosov
3.1.1.1	Podpora obstoječega sistema (ArcSight) za upravljanje varnostnih dogodkov	1 letna podpora	1 KPL

3.1.2 Tehnične zahteve za SKLOP 2

Predmet tega povpraševanja je vzdrževanje in podpora obstoječega sistema za upravljanje varnostnih dogodkov. Rešitev ArcSight je nameščena na enem strežniku. Rešitev je v produkciji in se uporablja za zbiranje, korelacijo in obdelavo varnostnih dogodkov. Izbrani ponudnik bo moral izvajati podporo in storitve v skladu z, v nadaljevanju opredeljenimi, tehničnimi specifikacijami oz. zahtevami naročnika.

Predmet	P/N	Kosov
Podpora za strojno opremo za dobo 12 mesecev	HU4B2AC HPE Tech Care Basic SVC	1 KPL
Podpora za programsko opremo za dobo 12 mesecev	<ul style="list-style-type: none"> ➤ Red Hat support Red Hat Enterprise Linux Server, Standard (Physical or Virtual Nodes) ➤ Arcsight support MF-24-7-SUPP Micro Focus 24x7 	1 KPL

Izbrani ponudnik bo vzdrževal obstoječi naročnikov sistem v smislu posodobitev in nadgradenj z vidika odpravljanja ranljivosti in zagotavljanja funkcionalnosti, brez izgube podatkov ter zagotavljal brezhibno delovanje sistema SIEM za obdobje 12 mesecev.

Izbrani ponudnik mora obstoječo programsko opremo posodobiti/nadgraditi na priporočene programske verzije, ter poskrbeti za vse dejavnike na način, da bo strojna oprema (HP strežnik) in programska oprema (RedHat Enterprise Linux + Microfocus ArcSight SIEM) še naprej delovala brezhibno, skladno z zahtevami proizvajalcev strojne in programske opreme za naslednjih 12 mesecev.

3.1.3 Ostale zahteve za SKLOP 2

3.1.3.1 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.

3.1.3.2 PART-IS

Izbran ponudnik mora zagotoviti, da bodo vse pogodbeno izvedene dela, ki vključujejo ali vplivajo na informacijske sisteme, podatke ali procese, pomembne za varnost civilnega letalstva, potekala v skladu z zahtevami Izvedbene uredbe (EU) 2023/203 o določitvi pravil za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu (v nadaljevanju: Uredba). Naročnik zahteva, da izbrani ponudnik oz. izvajalec izvaja/zagotavlja svoje storitve na ustrezni ravni informacijske varnosti in skladnosti z zahtevami omenjene Uredbe, ki vključujejo zahteve iz Priloge II (Part-IS.I.OR).

.....*konec dokumenta*.....