

Naša št.: 285-53/9-2025
Datum: 9. 10. 2025

TEHNIČNE SPECIFIKACIJE IN ZAHTEV NAROČNIKA

Licenčna programska oprema za XDR rešitev in izvajanje SOC storitev, št. 285-53

KAZALO

1	PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA	3
2	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE.....	3
2.1	XDR rešitev	3
2.1.1	Specifikacija in tehnične zahteve	3
2.1.2	Ostale zahteve.....	6

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Predmet tega javnega naročila je licenčna oprema, podpora proizvajalca in vzdrževanje programske opreme XDR rešitve za delovne postaje in strežnike naročnika.

Izbrani izvajalec bo za naročnika izvedel vzpostavitev in upravljanje gradnika varnostnega ekosistema – varnostno-operativnega centra (SOC), ki bo zagotavljal neprekinjeno spremljanje, analizo in odzivanje na kibernetске grožnje ter incidente v režimu 24/7, z uporabo napredne XDR rešitve za zaščito delovnih postaj in strežnikov. V obseg naročila je vključena tudi dobava licenčne opreme, licenčnin ter proizvajalčeve tehnične podpore, s čimer se naročniku zagotavlja celovito, zanesljivo in vzdrževano delovanje varnostne rešitve.

Licenčna oprema in izvajanje SOC operacije se nabavlja za obdobje 4 let, oziroma 48 mesecev, šteto od dneva podpisanega primopredajnega zapisnika.

Z vzpostavitvijo te storitve želi naročnik okrepiti svojo kibernetско odpornost, izboljšati čas zaznave in odziva na kibernetски incident (MTTD/MTTR), ter zagotoviti trajnostno in prilagodljivo varnostno infrastrukturo, ki je sposobna spremljati hitro razvijajoče se grožnje. Javno naročilo je namenjeno iskanju partnerja, v nadaljevanju ponudnika, ki bo z ustreznimi kompetencami, strokovnimi certifikati ter tehnološko napredno rešitvijo, zagotovil proaktivno, varno in zanesljivo izvajanje storitev na tem področju.

Natančne tehnične specifikacije, ter zahteve so opisane v nadaljevanju tega dokumenta.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

2.1 XDR rešitev

2.1.1 Specifikacija in tehnične zahteve

Specifikacija in tehnične zahteve so podane spodaj.

Postavka	Predmet	Zahteva	Kosov
2.1.1.1	Nakup licence XDR rešitev za 500 naprav	Licenca za skupaj 500 naprav (delovne postaje in strežniki) za obdobje 48 mesecev	1 KPL
2.1.1.2	Vzpostavitev XDR rešitve in programska podpora	Za programsko opremo za obdobje 48 mesecev, navedeno v tabeli v podtočki 2.1.1.1 tega poglavja, se zahteva podpora proizvajalca z odzivnim časom 4 ure v režimu 8 × 5 NBD (Next Business Day). Zahteva se tudi konfiguracijo in integracijo rešitve (»onboarding«)	1 KPL
2.1.1.3	Šolanje	Ponudnik zagotovi osnovno usposabljanje za delo z orodjem, 2 × 4 ure	1 KPL
2.1.1.4	Izvajanje SOC storitve	Izvajanje SOC storitve v režimu 24 × 7 in odzivnimi časi navedenimi pot tehničnimi zahtevami za obdobje 48 mesecev	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

- Rešitev mora omogočati napredno direktno integracijo s Palo Alto požarnimi pregradami, ki jih naročnik že poseduje, brez vmesnih integracijskih sistemov (npr. SOAR, ...)
- Rešitev mora podpirati vsaj sledeče operacijske sisteme:
 - Android 10, 11, 12, 13, 14, 15
 - iOS 15, 16 in kasnejši
 - Mac 11, 12, 13, 14, 15
 - Windows 10, 11
 - Windows server 2012, 2016, 2019, 2022, 2025
 - Linux Oracle, SUSE, Fedora, Debian, Red Hat, ...
- Rešitev mora omogočati SOAR integracijo.
- Rešitev mora omogočati proaktivno analizo z uporabo MITRE ATT&CK okvirja
- Rešitev je protivirusni program naslednje generacije (NGAV):
 - Zaščita brez podpisov z uporabo strojnega učenja in analize vedenja
 - Preprečuje znano in neznano zlonamerno programsko opremo, vključno z izsiljevalsko programsko opremo in zlorabami ničelnega dne (zero-day)
 - Ni odvisnosti od dnevnih posodobitev podpisov
- Zaščita pred vedenjskimi grožnjami:
 - Rešitev mora zaznati in blokirati napade brez datotek, kot so zloraba Power Shell-a ali grožnje, ki temeljijo na WMI
 - Rešitev mora ščititi pred krajo poverilnic in lateralnim premikanjem
 - Rešitev mora uporabljati pravila, ki temeljijo na vedenju s prilagodljivimi kriteriji
- EDR - Zaznavanje in odziv končnih točk mora:
 - Zbirati telemetrijo s končnih točk in jo povezovati/korelirati s podatki omrežja in oblaka
 - Zagotavljati podrobne časovnice incidentov in analizo temeljnih vzrokov
- EDR analitika:
 - Analizirati mora vedenje končnih točk, omrežja in uporabnikov
 - Zaznavati mora anomalije in sumljive dejavnosti z uporabo modelov strojnega učenja
 - Zaznavam mora dodeli stopnje resnosti in ocene zaupanja
- Nadzor naprav:
 - Upravljanje dostopov do USB-jev in perifernih naprav po vrsti ali ID-ju
 - Natančna opredelitev pravic branja/pisanja in omejitve dostopa
- Rešitev mora omogočati odzivne ukrepe:
 - Izolacija končne točke (prekine povezavo ogrožene končne točke z omrežjem, razen povezave z upravljalno konzolo)
 - Omogočati mora terminalski dostop do izolirane naprave iz upravljalne konzole z namenom:
 - Preiskave datotek in procesov
 - Izvajanje skript in ukazov
 - Izpis pomnilnika
 - Zbiranje dnevnih zapisov
 - Uporabe funkcij nalaganja, brisanja, prekinitve itd.
 - Uporaba karantene za sporne datoteke
- Rešitev mora omogočati t.i. »Threat Detection and Response«:
 - Samodejno odkrivanje identitet in privilegiranih računov v Active Directory
 - Detekcija naprednih napadov na identitete
 - Analiza servisnih računov in zaznavanje tveganih konfiguracij (npr. šibka gesla, ...)
 - Odkrivanje lateralnega gibanja in nepooblaščenih dodelitev privilegijev

- Analizo prijav, ki temelji na osnovi naučenega obnašanja – ne-navadni čas, geolokacija, naprava, protokol
- Predlog za remediacijo in samodejni odziv (blokada računa, reset gesla, izolacija naprave)

2.1.1.2 Vzpostavitev XDR rešitve in programska podpora

Vzpostavitev XDR storitve obsega:

- Integracijo varnostne rešitve v naročnikovo okolje, priprava paketov za namestitve XDR agentov na strežnike in delovne postaje, vzorčna namestitve glede na posamezen operacijski sistem
- Zagotovitev dnevniških zapisov - povezava na SIEM (revizijske sledi, kot so spremembe na sistemu, upravljanje sprememb, avtorizacija uporabnikov sistema, ...)
- Ureditev sredstev spremljanja, oznake sistemov, aplikacij, kritičnosti
- Konfiguracija varnostnih pravil
- Konfiguracija in vizualizacija preko dashboardov in poročil (upoštevati je potrebno vloge CISO, sistemska podpora, SOC, ...)
- Izmenjava kontaktnih podatkov
- Zasnova in odobritev poteka izvajanja storitve med strankama v povezavi z možnostmi ukrepanja, kot je poročanje, obveščanje, vprašanja, izvajanje odziva na incident in odobritev blokad, lahko tudi preko namenske mobilne aplikacije
- Vzpostavitev in prilagoditev (»fine-tuning«) naročnikovih primerov uporabe ponudnikovega kataloga zaznave groženj z naročnikovo platformo
- Testiranje zaznav
- Integracija naročnikovih podatkov o podatkovnih virih s ponudnikovo bazo virov podatkov
- Dokumentacija rešitve z vključenimi postopki in osnovnim načrtom odziva na incident

V času veljavnosti licenc, tj. v obdobju 4 let, mora biti za naročnika zagotovljena tehnična podpora proizvajalca z odzivnim časom 4 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 Šolanje

Ponudnik mora zagotoviti usposabljanje za 10 oseb s strani naročnika za uporabo rešitve in uporabo portala v trajanju 2 × 4 ure.

2.1.1.4 Izvajanje SOC storitve

Upravljanje storitev SOC mora zagotavljati naslednje storitve, upravljane zmogljivosti in rezultate:

- Realno-časovno ter stalno (24×7×365) spremljanje okolja in triažo varnostnih dogodkov v naročnikovem okolju s pomočjo dogovorjenih podatkovnih virov, na osnovi primerov uporabe izvajalčevih orodij, ter v okviru dogovorjenih ravni izvajanja storitev (SLA) in z uporabo naprednih avtomatizacijskih in korelacijskih tehnik, s ciljem pridobivanja relevantnih sumljivih dogodkov, ki se podrobno preiščejo.
- Preiskava prejetih alarmov kolikor je mogoče z uporabo dogovorjenih podatkovnih virov. Rezultat je razdelitev aktivnosti med škodljive in neškodljive skupaj s povezanim upravljanjem lažnih pozitivnih zaznav.
- Obveščanje o incidentih vključuje obveščanje dogovorjenih kontaktnih oseb, ko je zaznan varnostni incident v naročnikovem okolju.
- Vzpostavitev in uporaba podatkovne baze o virih naročnika znotraj izvajalčeve platforme, ki vsebuje podatke o naročnikovih virih podatkov z namenom prioritizacije izvajalčevih procesov.

- Integracija in obogatitev naročnikovih podatkov o dogodkih s storitvami obveščanja o grožnjah (threat intelligence - TI) znotraj izvajalčeve platforme, ki zagotavlja informacije o zunanjih akterjih ogrožanja, ranljivostih, zloglasnosti itd.
- Deljenje obveščevalnih podatkov o grožnjah (hitri alarmi, obdobni povzetki, mesečni pregledi).
- V primeru varnostnega incidenta bo izvajalec pripravil sanacijski načrt, ki vključuje zaporedje priporočenih ukrepov za:
 - odpravo tehnične škode, ki jo je povzročil incident,
 - popravilo prizadetih sredstev,
 - ter izvedbo ukrepov za preprečitev ponovitve istega incidenta.
- Na zahtevo in po izrecni odobritvi naročnika bo izvajalec aktivno sodeloval pri implementaciji sanacijskih ukrepov in zagotovil strokovno podporo do stabilizacije prizadetega okolja.
- Nadaljnja obravnava in izboljšave po incidentu - Po izvedbi temeljnih aktivnosti odziva bo izvajalec zagotovil dodatne svetovalne in inženirske storitve za:
 - izvedbo podrobne analize vzrokov incidenta (root cause analysis),
 - pripravo poročil na osnovi pridobljenih izkušenj (lessons learned),
 - načrtovanje in implementacijo izboljšav varnostnih postopkov, arhitekture ali nadzora,
 - ter sodelovanje pri splošnih popravkih naročnikovega okolja, kadar je to potrebno za izboljšanje varnostnega stanja.
 - Izvedba te storitve bo potekala po predhodnem dogovoru z naročnikom.
- SLA: ponudnik mora končati analizo dogodkov in podati poročilo o incidentu najkasneje v roku 60 min po zaznavi kritičnega dogodka, do 140 min po zaznavi visoko resnega dogodka in do 260 min po zaznavi srednje resnega dogodka.
- V sklopu pogodbe mora ponudnik zagotoviti razpoložljivost ekipe za odziv na zahtevne incidente – DFIR («Digital Forensics & Incident response») v roku 60 min od prepoznave kritičnega incidenta. V ponudbi je potrebno navesti urno postavko za rok trajanja pogodbe, naročnik mora naročilo potrditi.
- Storitve odziva na incidente potekajo na daljavo (varen telefon, videokonferenca, itd.) po potrebi oziroma zahtevi naročnika pa na naročnikovi lokaciji.
- Ker se kompleksnost incidentov med sabo lahko bistveno razlikuje, se storitve odziva na incident (razen začetnih hitrih zajezev vključenih v upravljane storitve zaznave) obračunajo glede na porabljen čas in material. Večje angažmaje mora zahtevati in odobriti naročnik.
- Izvajalec mora zagotoviti periodične sestanke 1× mesečno preko MS Teams in izdelavo poročil/priporočil odpornosti 1× mesečno
- V ponudbo naj bo vključenih 50 ur/letno za potrebe strokovnega svetovanja
- V ponudbi naj bo upoštevan t.i. »Purple timing« v okviru 15 ČD/leto
- Ponudnik mora zagotoviti, da bo storitev MDR vzpostavljena in pripravljena za delovanje najkasneje v 60 dneh po podpisu pogodbe.

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.

2.1.2 Ostale zahteve

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 Upravljanje končnih točk in izvajanje SOC operacije

Ponudnik mora v sklopu svojih SOC operacij kumulativno izvajati upravljanje in nadzor najmanj 10.000 končnih točk (kot končno točko se šteje napravo, ki je upravljana s strani upravljalvske konzole). Upravljalvska konzola mora biti od istega proizvajalca, kot ponujena XDR rešitev. Ponudnik priloži lastno izjavo h kateri priloži izpis št. končnih točk iz upravljalvske konzole.

2.1.2.3 Reference

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 petih letih, šteto od dneva objave te razpisne dokumentacije v zvezi z oddajo javnega naročila.

Ponudnik izkaže izpolnjevanje tega pogoja s predložitvijo:

- dveh (2) referenc za zagotavljanje storitve SOC 24/7/365, kjer je v sistem vključenih najmanj 750 nadzorovanih naprav, od tega mora biti en (1) referenca izdana s strani referenčnega naročnika, ki je zavezanec po ZinfV, ZinfV-1 ali NIS2;
- ene (1) reference za zagotavljanje storitve SOC 24/7/365, kjer je v sistem vključenih najmanj 750 nadzorovanih naprav, ki se izvajajo za referenčnega naročnika, ki deluje na področju prometnega sektorja (letalskega, cestnega, železniškega...) in s sedežem v državi članici EU).

2.1.2.4 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 XDR rešitve in izvajanja storitve SOC.

a) Kader za instalacije, konfiguriranja, vzdrževanja in tehnično podporo XDR rešitve

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

- dva (2) usposobljena strokovnjaka s certifikatom Palo Alto: *PCSNE – Palo Alto Network Security Engineer*,
- tri (3) usposobljene strokovnjake s certifikatom za upravljanje in konfiguracijo ponujene XDR rešitve, izdana s strani proizvajalca ponujene opreme. Kot ustrezni se štejejo napredni certifikati, kot na primer za opremo proizvajalca Trend Micro certifikat: Vision One XDR Certified Professional ali opremo proizvajalca Sophos certifikat: XDR Certified Admin.

b) Kader za izvajanja storitve SOC

Ponudnik mora zagotoviti zadostno število strokovno usposobljenih kadrov (najmanj 20), s katerim bo zagotavljal SOC storitve v režimu 365/24/7:

- štiri (4) usposobljene strokovnjake s certifikatom CASP+ (CompTIA Advanced Security Practitioner), oziroma certifikati podobne zahtevnostne stopnje in vsebine;
- tri (3) usposobljene strokovnjake s certifikatom CISSP (Certified Information Systems Security Professional), oziroma certifikati podobne zahtevnostne stopnje in vsebine;
- en (1) usposobljen strokovnjak s certifikatom GRID (GIAC Response and Industrial Defense);

- en (1) usposobljen strokovnjak s certifikatom GRTP (GIAC Red Team Professional), oziroma certifikati podobne zahtevnostne stopnje in vsebine;
- tri (3) usposobljene strokovnjake s certifikatom GCIH (GIAC Certified Incident Handler), oziroma certifikati podobne zahtevnostne stopnje in vsebine;
- en (1) usposobljen strokovnjak s certifikatom OSCP (Offensive Security Certified Professional).

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.

Ponudnik lahko za izpolnjevanje zahtev iz točke a) uporabi kader, ki je predviden za izvajanje storitve SOC iz točke b), v kolikor ti kadri izpolnjujejo tudi vse zahteve glede znanj in certifikatov, določenih v točki a). V tem primeru se šteje, da je zahteva po minimalnem številu strokovno usposobljenih kadrov iz točke a) izpolnjena, če ponudnik izkaže, da ima med kadrom, predvidenim za izvajanje storitve SOC, najmanj:

- dva (2) strokovnjaka s certifikatom Palo Alto PCSNE, ter
- tri (3) strokovnjake s certifikatom za upravljanje in konfiguracijo ponujene XDR rešitve, izdanih s strani proizvajalca ponujene opreme (npr. Trend Micro Vision One XDR Certified Professional, Sophos XDR Certified Admin ali enakovredno).

2.1.2.5 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*.....

