

C) SPECIFIKACIJA ZAHTEV NAROČNIKA

Tehnične zahteve za XDR rešitev:

Ponudnik mora skupaj s sistemskim administratorjem naročnika implementirati celotno rešitev na lokaciji naročnika. Ponudnik mora predati naročniku celovito dokumentacijo o vseh nastavitvah ponujene rešitve.

1. Licenčne zahteve

1.1. Obseg in predmet licenciranja

Predmet naročila je dobava licenčnega paketa za napredno zaščito, zaznavanje in odzivanje na grožnje za skupno **3000 končnih točk**. Licence morajo omogočati namestitev na različne tipe naprav v lasti naročnika, vključno z:

- Delovnimi postajami (npr. Windows 11 64-bit in ARM, macOS)
- Prenosnimi računalniki
- Strežniki (npr. Windows Server 2012 - 2025, Linux)
- Mobilnimi napravami (npr. Android, iOS)

1.2. Trajanje veljavnosti

Ponujene licence morajo imeti zagotovljeno obdobje veljavnosti **12 mesecev (1 leto)**, ki prične teči z dnem uspešne aktivacije storitve.

1.3. Funkcionalna skladnost

Ponujeni licenčni paket, ne glede na njegovo sestavo (npr. enoten SKU, kombinacija osnovnih in dodatnih licenc, "add-on" moduli), mora v končni ponudbeni ceni v celoti pokrivati in omogočati delovanje **vseh funkcionalnosti**, ki so opredeljene v poglavju '*Funkcionalne in tehnične zahteve*' te razpisne dokumentacije.

Ponudnik mora v ponudbi jasno specificirati vse vključene komponente (SKU-je), ki so potrebne za doseganje zahtevane funkcionalnosti. Vsi navedeni SKU-ji morajo biti vključeni v končno ceno ponudbe. Ponudba, ki ne bo v celoti pokrivala vseh tehničnih zahtev, se bo štela za neustrezno.

2. Zahteve glede neodvisnih ocen rešitve (Evaluacijske zahteve)

- Zahteva se izpolnjevanje naslednjih minimalnih pogojev:
 - Učinkovitost zaznav: Rešitev mora v vsaj 70% vseh testiranih korakov (substeps) znotraj vsakega od treh scenarijev (DPRK, CL0P, LockBit) doseči detekcijo na specifičnem nivoju "Tehnike" (Technique).

- Delovanje brez prilagoditev: Zgoraj navedeni rezultati morajo biti doseženi brez sprememb v konfiguraciji (Configuration Change = No) in brez zakasnenih zaznav (Delayed = No).

3. Funkcionalne in tehnične zahteve

3.1. Zahteve za antivirusno zaščito naslednje generacije (NGAV)

- Preprečevanje groženj mora temeljiti na lokalni analizi z uporabo strojnega učenja.
- Zagotovljeno mora biti preprečevanje groženj na podlagi obnašanja za dinamično analizo delujočih procesov.
- Vključeno mora biti preprečevanje izkoriščanja ranljivosti (exploitov) na podlagi tehnik napada.
- Preprečevanje znanih groženj mora temeljiti na obveščanju o grožnjah (npr. zgoščene vrednosti datotek - hashi).
- Zagotovljena mora biti zaščita z "zero-delay" posodobitvami za takojšnje deljenje obveščevalnih podatkov o grožnjah.
- Vključen mora biti mehanizem za pregledovanje omrežnega prometa za zaustavitev omrežnih napadov, ali podobne tehnologije.
- Zagotovljena mora biti zaščita pred "reverse shell" napadi.
- Posodobitve mehanizma za zaznavanje morajo biti transparentne za uporabnika.
- Omogočena mora biti konfiguracija varnostnih profilov in izjem.
- Podprto mora biti ročno in načrtovano skeniranje končnih točk.
- Zagotovljena mora biti zaščita pred zlonamerno programsko opremo, izsiljevalskimi virusi (ransomware) in napadi brez datotek (fileless attacks).
- Za vse funkcionalnosti zaščite, zaznavanja in odzivanja (EPP, EDR) se mora uporabljati en sam, lahek agent.

3.2. Zahteve za zaščito končnih točk (EPP)

- Zagotovljen mora biti centraliziran nadzor nad priklopljivimi napravami za operacijski sistem Windows, ki vključuje:
 - Možnost blokiranja ali dovoljevanja USB naprav glede na tip naprave (npr. diskovni pogoni, CD-ROM).
 - Možnost ustvarjanja podrobnih izjem (seznamov dovoljenih) za USB naprave na podlagi proizvajalca (Vendor ID), produkta (Product ID).
 - Omogočeno mora biti ustvarjanje lastnih pravil za preprečevanje.
- Zagotovljena mora biti združljivost z omrežnim varnostnim odjemalcem za varen oddaljen dostop, preprečevanje groženj in filtriranje URL-jev.

- Zagotovljena mora biti zaščita pred zlonamernimi napadi na MBR (Master Boot Record).
- Modul za zaščito pred izkoriščanjem ranljivosti mora omogočati zaščito kateregakoli procesa v sistemih Windows, Linux ali macOS.
- Omogočeno mora biti ustvarjanje izjem za zaščito pred izkoriščanjem ranljivosti na nivoju posameznih tehnik znotraj določenih procesov (podobno kot MITRE tehnike), brez potrebe po izklopu celotnega modula.
- Rešitev mora preprečevati izkoriščanje ranljivosti (exploits) na osnovi tehnik, specifičnih za Windows (vsaj Anti-Ransomware, Behavioral Threat Protection, Child Process Protection, DLL Hijacking, Data Execution Prevention (DEP), Exploit Kit Fingerprint, Hash Exception, Java Deserialization, JIT Protection, Local Privilege Escalation, MBR Protection, Network Packet Inspection, ROP Mitigation, SEH Protection).
- Rešitev mora preprečevati izkoriščanje ranljivosti (exploits) na osnovi tehnik, specifičnih za **Linux** (Java Deserialization, Privilege Escalation, Reverse Shell, ROP Mitigation, Shellcode Protection, SO Hijacking).
- Rešitev mora preprečevati izkoriščanje ranljivosti na osnovi tehnik, specifičnih za **macOS** (vsaj Anti-Ransomware, Dylib Hijacking, Gatekeeper Enhancement, Privilege Escalation,).
- Vse neznane izvršljive datoteke morajo biti samodejno poslane v analizo v "cloud sandbox".
- Rešitev mora omogočati namestitvev in odstranitvev na končne točke preko centralne konzole ali GroupPolicy

3.3. Zahteve za vidljivost in zaznavanje (XDR)

- Analiza obnašanja mora profilirati in odkrivati anomalije z analizo omrežnega prometa, dogodkov na končnih točkah in dejanj uporabnikov.
- Rešitev mora biti sposobna ustvariti anonimizirane, globalne profile obnašanja na podlagi podatkov več strank za odkrivanje novih zlonamernih dejavnosti.
- Vključene morajo biti zmožnosti nadzorovanega in nenadzorovanega strojnega učenja.
- Na voljo morajo biti vnaprej določena in prilagodljiva pravila za zaznavanje na podlagi obnašanja (BIOC)
- Omogočeno mora biti ustvarjanje lastnih korelacijskih pravil, ki lahko retroaktivno odkrivajo napade v preteklih podatkih.
- Omogočeno mora biti granularno izključevanje alarmov za natančnejše prilagajanje.
- Zagotovljeno mora biti zaznavanje tehnik napada v celotnem življenjskem ciklu napada (odkrivanje, lateralno gibanje, C&C, eksfiltracija).

- Taktike in tehnike morajo biti jasno označene v alarmih, pravilih in incidentih. (podobno kot MITRE ATT&CK)
- Rešitev mora omogočati ustvarjanje dinamičnih oznak za izboljšanje grupiranja in filtriranja informacij od agentov.

3.4. Zahteve za preiskovanje

- Zagotovljena mora biti samodejna analiza temeljnega vzroka (root cause analysis) za katerikoli alarm.
- Omogočena mora biti vizualizacija verige izvajanja (drevesna struktura), ki je vodila do alarma.
- Na voljo mora biti časovni pregled za analizo vseh dejanj in alarmov na časovnici.
- Omogočeno mora biti poizvedovanje po indikatorjih zlorabe (IOC).
- Omogočeno mora biti poizvedovanje po vseh zbranih podatkih (omrežje, končne točke, identiteta, forenzika).
- Omogočeno mora biti enostavno prehajanje med različnimi pogledi preiskave.
- Na voljo mora biti čarovnik, ki omogoča iskanje informacij in zagon odzivnih akcij iz kateregakoli dela konzole.
- Informacije o IP naslovih (vključno z geolokacijo) in zgoščenih vrednostih morajo biti samodejno združene na enem mestu.
- Zagotovljeno mora biti odstranjevanje "šuma" (npr. nepomembnih sistemskih datotek) iz verige izvajanja.

3.5. Zahteve za upravljanje incidentov

- Sorodni alarmi iz različnih virov morajo biti samodejno združeni v enoten incident.
- Zagotovljen mora biti intuitiven pregled incidenta z informacijami o tehnikah in taktikah.
- Točkovanje incidentov mora biti avtomatizirano z uporabo strojnega učenja.
- V pogledu incidenta morajo biti navedeni vsi pomembni artefakti, uporabniki in gostitelji.
- Omogočeno mora biti dodajanje komentarjev k incidentom.
- Podprt mora biti celoten življenjski cikel incidenta (nov, v preiskavi, zaprt, rešen itd.).
- Omogočeno mora biti pošiljanje podatkov o incidentih v zunanje sisteme za upravljanje primerov in izvoz incidentov v datoteko.
- Vsak incident mora imeti preiskovalno središče, ki služi kot revizijska sled vseh samodejnih in ročnih aktivnosti, izvedenih med preiskavo.

- Preiskovalno središče mora omogočati dodajanje opomb (notes) ter komunikacijo med analitiki znotraj samega incidenta.
- Znotraj preiskovalnega vmesnika mora biti na voljo interaktivna ukazna vrstica (CLI), ki omogoča neposreden zagon ukazov, skript brez menjave konzol.
- Prikaz aktivnosti v preiskovalnem središču mora biti mogoče filtrirati po tipu dogodka (npr. ukazi, opombe, sistemska dejanja, klepet) za lažjo preglednost.

3.6. Zahteve za obveščanje o grožnjah (Threat Intelligence)

- Rešitev mora omogočati alarmiranje na podlagi pravil za znane indikatorje zlorabe (IOC).
- Ob dodajanju novih IOC-jev mora sistem samodejno pregledati zgodovinske podatke in sprožiti alarme za nazaj.
- Zagotovljena mora biti vgrajena integracija z vsaj eno storitvijo za obveščanje o grožnjah (npr. VirusTotal) za dodaten kontekst.
- Omogočeno mora biti ustvarjanje IOC-jev preko API-jev ali neposredno v konzoli.
- Podprt mora biti uvoz več IOC-jev hkrati preko API-ja ali iz CSV datoteke ali dodajanje IP naslovov in datotek na blokirno listo preko API klicev.
- Omogočati mora pošiljanje obvestil (e-pošta)

3.7. Zahteve za odzivanje

- Na voljo mora biti oddaljeni terminalski dostop do končnih točk.
- Podprti morajo biti ukazi CMD, PowerShell in Python na sistemih Windows ter Bash in Python na macOS in Linux.
- Na voljo morajo biti vnaprej pripravljene skripte za lažje preiskovanje in odzivanje.
- Omogočena mora biti oddaljena izolacija posamezne ali več končnih točk hkrati, z možnostjo definiranja izjem (procesi, IP naslovi).
- Omogočeno mora biti oddaljeno brisanje datotek na posamezni ali več končnih točkah.
- Na voljo mora biti grafični upravitelj opravil za pregled, zaustavitev ali prenos delujočih procesov.
- Na voljo mora biti grafični brskalnik datotek za pregled.
- Sistem mora ponujati predloge za sanacijo za povrnitev gostiteljev v prvotno stanje.
- Omogočena mora biti funkcija "Išči in uniči" za hitro odstranjevanje groženj po celotnem okolju.
- Zagotovljena mora biti integracija s SOAR in SIEM rešitvami.

- Rešitev mora imeti centraliziran "akcijski center", od koder lahko analitik sproži vse razpoložljive akcije (npr. pridobivanje datotek, zagon skeniranja, izolacija, zagon skript, zbiranje slike pomnilnika).

3.8. Zahteve za zbiranje in integracijo podatkov

- Rešitev mora zbirati podrobne informacije o uporabnikih, napravah, procesih, datotekah, omrežni dejavnosti, registrskih ključih in sistemskih dogodkih za namene analitike.
- 3.9. Zahteve za agenta (sistemska podpora in viri)
- Podprte morajo biti vse novejšie različice sistemov Windows (vključno s Server), macOS, Android, Chrome OS in glavne distribucije Linuxa.
- Posodobitve agenta morajo biti mogoče neposredno iz upravljaljske konzole, z možnostjo samodejnih posodobitev in "peer-to-peer" deljenja med agenti.
- Agent mora biti sposoben hraniti EDR podatke v lokalnem predpomnilniku tudi po ponovnem zagonu sistema.

3.10. Zahteve za implementacijo, upravljanje in varnost platforme

- Rešitev mora temeljiti na enotni, skalabilni arhitekturi, ki je upravljana preko ene same, centralizirane spletne konzole za vse funkcionalnosti (EPP, EDR, XDR, forenzika itd.). Ponudbe, ki za izpolnjevanje zahtev združujejo več ločenih produktov z različnimi upravljaljskimi konzolami, niso sprejemljive.
- Podprta mora biti enotna prijava (SSO) in večfaktorska avtentikacija (MFA) za dostop do upravljanja.
- Agent na končnih točkah mora podpirati in omogočati konfiguracijo za komunikacijo z upravljaljsko konzolo v oblaku preko obstoječega "on-premise" proxy strežnika naročnika.
- Celotna rešitev mora biti varovana v skladu z najboljšimi praksami (šifriranje podatkov, varnostne ocene itd.).
- Podprte morajo biti prilagodljive nadzorne plošče ("dashboardi") z dinamičnim filtriranjem in "drill-down" analizo.
- Omogočeno mora biti ustvarjanje poročil po meri (tudi v PDF formatu) in uporaba vnaprej pripravljenih predlog.

3.11. Zahteve za hrambo podatkov in pokritost

- Zagotovljena mora biti vidljivost v lateralno gibanje po omrežju in drugih delih infrastrukture.

- Standardno mora biti vključena vsaj 30-dnevna hramba vseh zbranih podatkov ("vroča hramba"). Vroča hramba pomeni, da so podatki v tem obdobju takoj dostopni za poizvedovanje in analizo preko poizvedovalnega jezika rešitve.
- Vsi alarmi, primeri (cases) in incidenti morajo biti hranjeni vsaj 365 dni.
- Z dokupom licence mora biti omogočena prilagodljiva hramba podatkov za poljubno dolgo obdobje (z opcijami za vročo in hladno hrambo).
- Omogočeno mora biti posredovanje dogodkov v zunanje sisteme.