DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI
DARS d.d.

POGLAVJE 2

TEHNIČNE SPECIFIKACIJE

in

PONUDBENI PREDRAČUN

za

Vzpostavitev sistema SIEM (Security Information and Event Management)
(int. ev. št. 000285/2023)

V S E B I N A

I. Tehnične zahteve in pogoji vzpostavitve sistema SIEM (Security Information and Event Management)

DARS

Vsebina

I.1. Predmet

Predmet naročila obsega sistem za napredno odkrivanje in obrambo pred kibernetskimi grožnjami – znano kot SIEM (ang. *Security Information and Event Management*).
Predmet naročila je:

- vzpostavitev sistema SIEM (Security Information and Event Management),
- vzdrževanje vzpostavljenega sistema za obdobje šestdeset (60) polnih koledarskih mesecev.
- napredna programska oprema za odkrivanje in obrambo pred kibernetskimi grožnjami,
- vsa potrebna licenčna programska in strojna oprema za vzpostavitev polno delujočega, samostojnega sistema,
- izdelava postopkov neprekinjenega poslovanja vključno z načrtom okrevanja za ponujeno celostno rešitev;
- izobraževanje administratorjev in naprednih uporabnikov naročnika;
- do 800 ur dodatnih storitev do konca vzdrževalnega obdobja (60 mesecev), ki se obračunajo po dejanski porabi.

Ponujena rešitev, sisteme SIEM, mora predstavljati celovito rešitev za upravljanje varnostnih dogodkov in informacij, shranjevanje varnostnih dnevnikov, odkrivanje zlorab in slabih praks, ter upravljanje konfiguracij in ranljivosti. Omogočati mora napredno zaznavanje groženj, enostavno uporabo in nizke skupne stroške lastništva.

Predstavljati mora krovno rešitev za upravljanje varnosti, ki povezuje vse obstoječe in bodoče varnostne sisteme naročnika v logično celoto.
Osnovni način zbiranja varnostnih dogodkov temelji na sledenju aktivnosti v dnevniških zapisih.

I.2. Elementi in funkcije predmeta naročila

Sistem SIEM mora omogočati učinkovit zajem in nadzor podatkov iz strežnikov, delovnih naprav in ostalih mrežnih naprav v obsegu: do 250 strežnikov, do 750 delovnih postaj, mrežne naprave > 100, zajem zapisov Microsoftovih oblačnih storitev.

Zmogljivost sistema mora biti takšna, da omogoča zajem vsaj 8.000 dogodkov na sekundo (EPS). Licenčna kapaciteta za zajem dogodkov iz 200 strežnikov ne sme biti licenčno omejena in mora imeti možnost, da presega 15.000 EPS.
To zagotavlja, da sistem lahko obdela velike količine podatkov in omogoča učinkovito odkrivanje in odzivanje na varnostne incidente.

Sistem mora biti zasnovan tako, da omogoča enostavno upravljanje in konfiguracijo, ter zagotavlja visoko stopnjo varnosti in zanesljivosti. Prav tako mora biti v skladu z veljavnimi standardi in zakonodajo na področju varnosti informacij.

I.2.1. Sistem mora zagotavljati:

- Centralizirano upravljanje in shranjevanje varnostnih dogodkov/dnevnikov, informacij ter ranljivosti (zbiranje, korelacija, normalizacija dogodkov, analiza povezav in odvisnosti);
- zagotavljanje kontinuitete, celovitosti in nespremenljivosti varnostnih dogodkov ter informacij, nezmožnost spreminjanja in brisanja aktivnosti z namenom prikrivanja;

- nadzor in zaščito zaupnih poslovnih ter osebnih podatkov;
- spremljanje revizijske sledi privilegiranih uporabnikov;
- zaščito pred nenamernim ali zlonamernim ravnanjem zaposlenih ali zunanjih sodelavcev;
- pravočasno zaznavo varnostnih tveganj, slabih praks, zlorab;
- hitrejše in učinkovito upravljanje varnostnih dogodkov ter poročanje;
- zmanjševanje števila lažno pozitivnih dogodkov na minimum;
- zagotavljanje skladnosti z zakonodajo in regulativami, kot so ZInfV, ZVOP-2, ISO27001;
- visoko zmogljivo in razširljivo platformo z možnostjo distribuirane arhitekture (npr. ločitev zajema podatkov od obdelave/analize);
- veliko število podprtih pravil (1000+);
- uparjanje pravil z matriko MITRE ATTACK, kar olajša načrtovanje in izvajanje zaznavanja varnostnih incidentov;
- veliko število podprtih naprav za zajem sporočil, kar eliminira razvoj razčlenjevalnikov;
- možnost analize uporabniškega vedenja (»User Behaviour Analytics - UBA«) z uporabo specifičnih pravil in uporabo strojnega učenja ter omogočeno integracijo z AD;
- možnost analize omrežnega prometa (»Network Traffic Analysis – NTA«) in dinamično prilagajanje izhodiščnih vrednosti za zaznavo nenormalnega prometa na osnovi strojnega učenja;
- podporo vidljivosti na uporabniški in omrežni strani;
- možnost analize DNS v kombinaciji z NTA in UBA, ki je podprta s strojnim učenjem z namenom nadzora DNS-a kot enega od pogostih tehnik napadov;
- razvojno pot integracije orodij in procesov skladno s konceptom SOAR (ang. Security, Orchestration, Automation, Response).
- sistem ima grafični urejevalnik za pripravo pravil za razčlenitev in preslikavo zapisov, ki jih sistem še ne zna razčleniti;
- sistem zagotavlja prepoznavo DoS in DDoS napadov;
- sistem ima sposobnost definiranja različnih časov hranjenja dnevniških zapisov glede na definirane kriterije;
- sistem podpira skupno taksonomijo dogodkov (dogodki morajo biti razvrščeni v običajne vrste, kot so npr. authentication, access, malware, system, DoS itd.);
- sistem zagotavlja pred pripravljene politike s strani proizvajalca opreme;
- sistem nudi možnost definiranja politik s strani skrbnikov sistema;
- Rešitev mora zagotoviti neomejeno kapaciteto shranjenih podatkov. To je omejeno zgolj od kapacitete dodeljenega diskovnega prostora in ne od licenc.
- Rešitev mora prepoznati strukturo log zapisov za vse navedene sisteme:
    - Strežnike in delovne postaje, ki temeljijo na Microsoft operacijskem sistemu,
    - Strežnike in delovne postaje, ki temeljijo na Linux/UNIX operacijskem sistemu,
    - Strežnike baz podatkov,
    - Poštne strežnike
    - Spletne strežnike,
    - DNS strežnike,
    - Programsko opremo za e-poštno in spletno zaščito,
    - Požarne pregrade,
    - Komercialne aplikacije,
    - Data Leak Protection (DLP) programsko opremo,
    - Database Activity Monitoring (DAM) programsko opremo,
    - File Integrity/Activity Monitoring (FIM/FAM) programsko opremo
    - Identity and Access Management (IAM) programsko opremo,
    - Intrusion detection/protection systems (IDS/IPS),
    - Anti-malware rešitve,oDirectory (npr. AD, LDAP) strežnike,
    - Network flows (npr. NetFlow, J-Flow, sFlow, IPFIX itd.),

  - Mrežno infrastrukturo (npr. switches, routers, itd.),
  - Infrastrukturo za virtualizacijo (npr. VMware ESX, Hyper-V),
  - Vulnerability scanners,
  - NDR sisteme (npr. Darktrace, Vectra,Checkpoint Horizon,itd.),
  - IOC
  - Ostalih sistemih navedenih v razpisni dokumentaciji
- Rešitev mora omogočati zajem, hranjenje in obdelavo dnevniških datotek, ki so povezani z evidentiranjem dostopa, obdelave ali brisanja v posameznih zbirkah osebnih podatkov.

I.2.2. Alarmiranje in poročanje

- Sistem omogoča dinamično alarmiranje v realnem času glede na prepoznane anomalije ali varnostne dogodke, s prilagodljivimi pragovi in parametri za optimizacijo obveščanja.
- Sistem omogoča prioritizacijo alarmov glede na resnost in kontekst varnostnih groženj iz nadzorovanih naprav, kar omogoča hitrejši odziv na kritične incidente.
- Sistem omogoča avtomatizacijo odziva na alarme, vključno z integracijo z orodji za avtomatizacijo in orkestracijo, za hitrejše in učinkovitejše reševanje incidentov.
- Sistem omogoča analizo in filtriranje lažnih pozitivnih dogodkov z uporabo naprednih analitičnih orodij in algoritmov, kar zmanjšuje število nepotrebnih alarmov.
- Sistem omogoča agregacijo in korelacijo alarmov na podlagi ponavljajočih se dogodkov, kar omogoča boljše razumevanje in analizo varnostnih incidentov
- Sistem omogoča agregacijo in korelacijo alarmov na podlagi ponavljajočih se dogodkov, kar omogoča boljše razumevanje in analizo varnostnih incidentov.
- Sistem omogoča napredno analizo vedenja in generiranje opozoril ob zaznanih nepravilnostih in vedenjskih sprememb v dogodkih, ki so sprejeti preko log zapisov (event) in zapisov tokov (flow). Opazovanje nepravilnosti je mogoče na več načinov:
  - na podlagi pragov (threshold), ko je aktivnost večja ali manjša od definirane;
  - na podlagi vedenjskih sprememb, sprememb količine v primerjavi z običajnimi vzorci, kratkotrajna odstopanja aktivnosti glede na daljši časovni interval;
- Sistem omogoča integracijo z drugimi sistemi in platformami za posredovanje alarmov, vključno z Email, SNMP, Syslog, in drugimi.
- Sistem zagotavlja celovito upravljanje z varnostnimi incidenti, vključno z avtomatiziranim sledenjem, dokumentiranjem in reševanjem incidentov.
- Sistem omogoča prilagodljivo in avtomatizirano poročanje, vključno z izvozom poročil v različnih formatih (PDF, HTML,…) in pošiljanjem poročil na e-poštni naslov.
- Sistem ima podporo za proaktivno preverjanje stanja sistemskih procesov in opozarjanje uporabniku, če obstajajo težave pri njihovem delovanju.
- Sistem omogoča monitoring zbiranja logov in generiranje opozoril sistemskim administratorjem, kadar pride do težav z zbiranjem dnevniških zapisov z izvorne naprave (log source).

I.2.3. Upravljanje revizijske sledi in upravljanje zbirk osebnih podatkov

- Sistem omogoča zajem, hranjenje in obdelavo dnevniških datotek, ki so povezani z evidentiranjem dostopa, obdelave ali brisanja v posameznih zbirkah osebnih podatkov.
- Sistem omogoča napredno iskanje revizijske sledi po uporabniku sistema SIEM, z možnostjo filtriranja in sortiranja rezultatov po različnih kriterijih.
- Sistem omogoča globoko in kontekstualno iskanje revizijske sledi po posameznih uporabnikih v ITK okolju naročnika, z možnostjo analize in vizualizacije povezav med različnimi dogodki in entitetami.

- Sistem omogoča zbiranje revizijske sledi na baznem ali aplikacijskem nivoju, z možnostjo prilagoditve in optimizacije zbiranja glede na specifične potrebe in zahteve organizacije.
- Omogočena je prilagodljiva izdelava poročil glede na revizijske sledi posameznega uporabnika, z možnostjo avtomatizacije in prilagoditve poročil glede na potrebe deležnikov.
- Sistem omogoča dostop do revizijskih sledi v skladu z upravljavskimi pravicami, zagotavljajoč, da so občutljivi podatki zaščiteni pred nepooblaščenim dostopom.
- Sistem omogoča dolgoročno arhiviranje revizijskih sledi, z možnostjo učinkovitega iskanja in pridobivanja arhiviranih zapisov, ko je to potrebno.
- Sistem omogoča avtomatizirano obveščanje in alarmiranje v primeru odkritja potencialno škodljivih ali nenavadnih vzorcev v revizijskih sledih, omogočajoč hitro odzivanje na varnostne incidente.

I.2.4. Arhitekturne zahteve

- Sistem mora zagotavljati delovanje v HA (High Availability) načinu na primarni lokaciji, kar pomeni, da odpoved ene fizične naprave ali aplikativna napaka ne prekine delovanja sistema;
- Po vzpostavitvi dodatne lokacije vzpostavitev sistema na dveh fizično ločenih lokacijah v HA (High Availability) načinu (selitev ene naprave na drugo lokacijo in vzpostavitev delovanja),
- Vzpostavitev virtualnega okolja na obeh host strežnikih ter postavitev vSphere strežnik za uporavljanje;
- Sistem mora zagotavljati varno šifriranje komunikacije med komponentami ponujene rešitve;
- Sistem mora zagotavljati zanesljivo integriteto shranjenih podatkov z uporabo vsaj SHA-2;
- Sistem mora zagotavljati elastično eskaliranje za obvladovanje nenadnih povečanj števila dogodkov, brez zaviranja ali zavračanja dogodkov zaradi licenčnih omejitev.
- Sistem mora zagotavljati Online hrambo dogodkov – za hitro iskanje za obdobje minimalno 12 mesecev;
- sistem mora zagotavljati fleksibilne proste kapacitete za enostavno razširitev kapacitet diskovnega polja na obeh strežnikih.
- Sistem mora zagotoviti integracijo s sistemi za avtentikacijo uporabnikov (MS AD, LDAP), z možnostjo prilagoditve in konfiguracije glede na specifične zahteve organizacije.
- Avtentikacija uporabnikov po principu enotne prijave (Single Sign On);
- Sistem mora shranjevati podatke izključno lokalno, hranjenje ali posredovanje v oblak ni dovoljeno, z zagotovljenim učinkovitim upravljanjem in zaščito lokalno shranjenih podatkov.
- Sistem mora omogočati modularno in kompatibilno nadaljnjo širitev funkcionalnosti z drugimi ali lastnimi rešitvami, z možnostjo enostavne integracije in upravljanja dodatnih modulov in funkcionalnosti.

I.2.5. Infrastrukturne zahteve

Sistema mora biti vzpostavljen na novi virtualni infrastrukturi. Delovanje celotnega sistema SIEM obsega dva (2) po konfiguraciji enaka strežnika z vso pripadajočo strojno in licenčno programsko opremo potrebno za ustrezno vzpostavitev in delovanje končne rešitve.
Povezljivost in ustrezne komunikacijske povezave zagotovi naročnik.

Minimalne zahteve za konfiguracija posameznega strežnika:

- višina v omari 2 RU, možnost vgradnje do 24 x 2,5" vsaj shranjevalnih medijev;
- vgrajena dva (2) procesorja Intel® Xeon® Gold 6430 2.1G, 32C/64T;
- pomnilnik (RAM) kapacitete 256 GB z možnostjo nadgradnje do vsaj 1TB;
- diskovni krmilnik z vgrajenim predpomnilnikom kapacitete 8 GB;
- vgrajene shranjevalne kapacitete:
    - 2 x 480 GB SSD SATA Mix Use 6Gbps 512 2,5in Hot-plug AG Drive, 3 DWPD (za operacijski sistem ESXi in operacijski sistem virtualnih strežnikov)
    - 15x 2,4 TB 7.2k SATA 6Gbps 512 2,5in Hot-plug AG Drive v RAID 6, skupne kapacitete več kot 30 TiB (za podatke sistema SIEM);
    - 2x vmesnik 10Gb RJ45 Ethernet;
    - 2x vmesnik 1Gb RJ45 Ethernet;
    - Strežnik mora biti sestavljen tako, da je mogoče vanj vgraditi skupno vsaj 6 dodatnih kartic (vključno s tistimi, ki so že del ponudbe);
    - priložena vodila za vgradnjo in vodila kablov;
    - priloženi vsi kabli, potrebni za priklop;
    - priložen sistem za organizacijo kablov;
    - nadzor delovanja strežnika in omogočen oddaljen dostop do strežnika preko spletnega vmesnika (ang. out-of-band) s funkcionalnostjo zaslona, tipkovnice, miške in navideznega pogona,
    - strežnik mora imeti zaščito pred izvajanjem kompromitirane firmware kode,
    - strežnik mora imeti možnost obnovitve sistemske mikrokode v primeru aktivacije kompromitirane kode,
    - hot plug redundančni ventilatorji namenjeni dodatnemu hlajenju (High Performance)
    - 2x Hot-Plug redundančni napajalnik vsaj 800W (80 Plus Platinum),
    - vgrajeni varnostni čip TPM 2.0,

- VMware vSphere 8 licence ustreznega nivoja za izpolnitev zahtev;

Sistem mora imeti zagotovljeno tehnično podporo in redne posodobitve, za zagotavljanje nemotenega delovanja in odpravljanje morebitnih varnostnih ranljivosti.

I.3. Vzpostavitev

V okviru implementacije sistema se opravijo najmanj naslednje aktivnosti:

- Dobava in montaža strojne opreme v naročnikovo IKT-okolje, z zagotovljenim testiranjem in optimizacijo delovanja.
- Namestitev potrebne programske opreme z vsemi licencami in funkcionalnostmi, ki so opredeljene v tehničnih zahtevah.
- Konfiguracija omrežja, vključno z IP-naslovov, prehodi, DNS, in drugimi omrežnimi parametri.
- Konfiguracija popravkov in nadgradenj na najnovejšo različico.
- Konfiguracija varnostnega kopiranja podatkov SIEM-okolja, s preizkusom obnovitve.
- Konfiguracija zajema dogodkov s strežnikov (različni OS sistemi), delovnih postaj, požarnih pregrad, omrežnih naprav, in drugih sistemov v naročnikovem okolju.
    - Primer seznama, a ne omejeno zgolj na naštete:
        - konfiguracija zajema dogodkov s strežnikov Linux;
        - konfiguracija zajema zapisov iz MS oblačnih storitev;

        - konfiguracija zajema zapisov Message Tracking in SMTP s poštnih strežnikov Exchange;
        - konfiguracija zajema dogodkov s požarne pregrade;
        - konfiguracija zajema omrežnih tokov (netflow) z omrežnih naprav;
        - SQL, Oracle
        - konfiguracija zajema dogodkov iz sistema protivirusne zaščite;
- Integracija z aktivnim imenikom za avtentikacijo uporabnikov sistema, z možnostjo enotne prijave (Single Sign-On).
- Izdelava skupin z različnimi pravicami in omejitvami pri uporabi sistema, z rednim pregledom in posodobitvami.
- Implementacija privzetih politik za potrebe izvajanja korelacij, skladno z varnostnimi politikami in primeri dobrih praks.
- prilagoditve in podrobne nastavitve privzetih politik korelacij skladno z varnostnimi politikami in primeri dobrih praks;
- Optimizacija sistema, kot so normalizacije, agregacij, alarmiranja, in druge funkcionalnosti, za optimalno delovanje in odzivnost.
- Vzpostavitev sistema alarmiranja glede na prepoznane anomalije ali varnostne dogodke.
- Testiranje alarmiranja pri različnih scenarijih, z dokumentiranimi rezultati in izboljšavami.
    - Nekaterih scenarij, kot so:
        - kreiranje lokalnega uporabnika na strežniku;
        - brisanje dogodkov (Event Log); kreiranje novega opravila s strani nesistemskega uporabnika (Task Scheduler);
        - izvedba sumljive PowerShell-skripte;
        - zaznani večkratni neuspešni poskusi prijave na ciljne sisteme (Brute Force);
        - zaznane spremembe članstva v skupinah prednostnih uporabnikov, skrbniki domene in skrbniki v podjetju; zaznana ponovna nastavitev gesla na skrbniških računih;
- zajem revizijske sledi prednostnih računov iz naslednjih sistemov (audit trail/log): o požarna pregrada, Sistem elektronske pošte, Sistem protivirusne zaščite.
- Generiranje rednih poročil glede na željo naročnika, z možnostjo prilagoditve in izvoza.
- Izobraževanje naročnika za administratorje in napredne uporabnike, z zagotovljenim gradivom in podporo.
- Simulacija izpada primarnega sistema, s preklopom na sekundarni, ter vrnitev na primarni sistem, vključno z dokumentiranimi postopki.

I.4. Lokacija naročnika

Vsa dela se izvajajo na lokaciji naročnika v Ljubljani ali ožji okolici. V dogovoru z naročnikom je možno tudi delo na daljavo. Naročnik izvajalcu ne bo priznal nobenih potnih stroškov.
Kot zagon se šteje opravljene vse storitve iz točke I.3., razen prenosa znanja.

I.5. Zahtevani tehnični pogoji

Zahtevani tehnični pogoji

- SIEM rešitev mora biti uvrščena v Gartnerjev kvadrant vodilnih SIEM rešitev (magic quadrant).
- Izvajalec mora zagotoviti ustrezno podporo in vzdrževanje za ponujeno rešitev.
- Ponujena rešitev mora biti združljiva z obstoječo IT infrastrukturo naročnika.
- Izvajalec mora zagotoviti vse potrebne licence za delovanje ponujene rešitve.

I.6. Usposobljenost tehničnega kadra

Izvajalec zagotavlja, da so vsi strokovnjaki, ki sodelujejo na projektu v celotnem času trajanja pogodbe, ustrezno usposobljeni in certificirani za delo z izbranim sistemom SIEM in pripadajočimi tehnologijami.

Imenovani strokovnjaki morajo biti na voljo za sestanke, razprave in druge komunikacijske potrebe projekta, tako osebno kot virtualno. Strokovnjaki morajo sodelovati z naročnikom in drugimi deležniki projekta, da zagotovijo uspešno izvedbo in vzdrževanje sistema SIEM.

Izvajalec certificiranega strokovnjaka s področja projektnega vodenja imenuje za vodjo projekta pri vzpostavitvi sistema SIEM v predmetnem javnem naročilu.
Vodja projekta mora biti sposoben reševati morebitne težave in izzive, ki se pojavijo med izvedbo projekta, in zagotoviti, da so cilji projekta doseženi.

Vsi referenčni strokovnjaki, s katerimi ponudnik izkazuje svojo strokovno sposobnost, obvezno in ves čas sodelujejo pri vzpostavitvi sistema SIEM, pri vzdrževanju vzpostavljenega sistema SIEM pa vsaj en referenčni strokovnjak posameznega področja, razen usposobljeni vodja projekta.

Izvajalec zagotavlja, da so vsi strokovnjaki, ki sodelujejo na projektu, zavezani k spoštovanju zaupnosti in varovanju informacij naročnika in da so seznanjeni z veljavnimi zakoni, predpisi in standardi, ki se nanašajo na izvedbo in vzdrževanje sistema SIEM.

I.7. Vzdrževanje sistema SIEM

Izvajalec zagotavlja vzdrževanje SIEM sistema ter pripadajoče strojne in programske opreme za obdobje 60 mesecev.

Mesečno vzdrževanje sistema SIEM vključno z vso pripadajočo strojno in programsko opremo vključuje:

- vzdrževanje strojne in programske opreme,
- odpravo napak na strojni in programski opremi,
- redno posodabljanje programskih različic na zadnjo stabilno različico,
- redno posodabljanje in optimizacija politik, pravil, konfiguracij in parametrov sistema SIEM za izboljšanje detekcije in odziva.
- 2 x letno celovit pregled sistema s predlogi za izboljšavo na nivoju varnosti, funkcionalnosti in nadgradenj,

- posodabljanje tehnične dokumentacije in zagotavljanje dostopa do vseh relevantnih informacij, navodil in dokumentov,
- Implementacija in validacija vseh potrebnih varnostnih ukrepov, zaščit, kontrol in rešitev za zagotavljanje integritete, zaupnosti in razpoložljivosti sistema SIEM.
- Odpravo vseh zaznanih kritičnih ranljivosti sistema SIEM ter pripadajoče programske in strojne opreme;
- neomejeno število prijav in odprav napak delovanja sistema.

Storitve, obračunane mesečno po dejansko porabljenem času, so:
- razvoj, implementacija in testiranje integracij, povezav ali vmesnikov z drugimi sistemi, aplikacijami ali storitvami;
- podpora, svetovanje in usposabljanje skrbnikov sistema v okolju naročnika za zagotavljanje samostojnega in učinkovitega upravljanja sistema;
- vključevanje, konfiguracija in validacija novih virov, podatkov, logov ali informacij v sistem SIEM;
- fine nastavitve, kalibracije in optimizacije sistema za zmanjšanje lažno pozitivnih alarmov, opozoril ali detekcij;
- prenos znanja, izkušenj in veščin o upravljanju, konfiguraciji, analizi in odzivu sistema SIEM za izboljšanje kompetenc in zmogljivosti naročnika;

Dodatne zahteve
- Izvajalec mora redno obveščati naročnika o vseh relevantnih vprašanjih, incidentih, spremembah ali tveganjih, ki bi lahko vplivala na kakovost, varnost ali razpoložljivost storitev.
- Izvajalec mora sodelovati z naročnikom pri razvoju in izvajanju izboljšav, optimizacij in inovacij za povečanje učinkovitosti, zmogljivosti in vrednosti storitev.

I.8. Zagotavljanje podpore

Podpora mora biti dosegljiva vsak delavnik **od 8:00 do 16:00 ure**.
V tem času mora biti naročniku zagotovljena učinkovita pomoč pri uporabi rešitve SIEM ali pri odpravi težav pri delovanju programske ali strojne opreme.
Komunikacija je možna preko telefona, elektronske pošte ali namenskega sistema za podporo, ki ga zagotovi izvajalec.

Vsa sporočila, zahteve ali prijave morajo biti evidentirana, dokumentirana in arhivirana s strani izvajalca. Evidenca mora biti dnevno ažurna, pregledna in dostopna naročniku na vpogled. Izvajalec je dolžan mesečno predati skrbniku naročnika podrobno poročilo o vseh opravljenih storitvah, intervencijah in delih v okviru pogodbe za pretekli mesec.

Vse storitve, se opravljajo na lokaciji naročnika v Ljubljani ali ožji okolici, v dogovoru z naročnikom je možno tudi delo na daljavo ter vključujejo vse potne stroške za prevoz. Vzdrževalne ure se zaokrožujejo na 15 minut natančno. Posegi na strežniku se lahko izvajajo na daljavo ob predhodni potrditvi naročnika. V izjemnih primerih, ko je potreben fizičen dostop do strežnika, so vsi potni stroški vključeni v ceno storitve.

Vse napake, ki jih povzroči izvajalec, se odpravijo brez dodatnih stroškov. Odprava napak mora biti hitra, učinkovita in zanesljiva.

Prijava usodnih napak se izvede s telefonskim klicem naročnika, z naknadnim obvestilom preko elektronske pošte ali prijave napake v namenskem sistemu. V primeru splošnih napak se prijava izvede z obvestilom preko elektronske pošte ali prijave napake v namenskem sistemu.

Izvajalec mora zagotavljati visoko raven storitve, ki je v skladu z dogovorjenimi in predvidenimi odzivnimi časi. Prioriteta se določi na podlagi učinka na delovanje sistema in potrebe naročnika.

Prioriteta se določi na podlagi učinka na delovanje sistema.

I.8.1. Odzivni časi

SLA (Service Level Agreement) pogoji in odzivni časi za vzdrževanje sistema, kot je SIEM, so ključnega pomena za zagotavljanje nemotenega delovanja in hitrega odziva na morebitne težave ali incidente.

Prioritete:

prioriteta 1	visoka	Kritična omejitev uporabe; UPORABNIK ne more izvajati nalog zaradi izpada delovanja aplikacije. Izvajanje nalog je prekinjeno.
prioriteta 2	srednja	Srednja omejitev uporabe; UPORABNIKU funkcionalnost ni razpoložljiva ali ne deluje. Izvajanje nalog je moteno.
prioriteta 3	nizka	Majhna omejitev uporabe; UPORABNIKU funkcionalnost ne deluje v skladu z zahtevami. Izvajanje nalog je mogoče, vendar omejeno, gre za manjše težave in za zahteve po spremembah.

Odzivni čas je časovno obdobje, v katerem vzdrževalec sprejme, potrdi in začne z odpravljanjem napake ali nudenjem pomoči po prejemu sporočila.

Odzivni časi:

Napaka	prioriteta 1 (visoka)	prioriteta 2 (srednja)	prioriteta 3 (nizka)
Odzivni čas	**4 h**	**8 h**	**po dogovoru**
Izvedbeni čas	**8 h**	**16 h**	**po dogovoru**

Dodatno

- Izvajalec mora zagotoviti stalno dostopnost in odzivnost v primeru izrednih dogodkov, incidentov ali kriz.
- Vse spremembe, nadgradnje ali posodobitve sistema se izvajajo v sodelovanju in po dogovoru z naročnikom.
- Vse storitve, dela in intervencije se izvajajo v skladu z najvišjimi standardi kakovosti, varnosti in profesionalnosti.

I.9. Politika črpanja ur

Podpora, razvoj, izobraževanje in dodatne zahteve naročnika se izvajajo v okviru kvote ur, ki jih naročnik porablja po potrebi in po vsakokratnem dogovoru z naročnikom in naročilu izvajalcu.

Plačilo zanje se izvede na osnovi potrjenega delovnega naloga. Izvajalec je dolžan naročniku mesečno predložiti izpis vseh posegov, kjer navede:

- datum odpoklica storitve,
- datum posega,
- število porabljenih ur za poseg,
- namen/tip posega,
- oseba naročnika, ki je poseg naročila,
- skupno število porabljenih ur.

Število potrebnih ur za posamezen poseg ter rok izvedbe posameznega obsega je stvar dogovora med naročnikom in izvajalcem.

I.10. Nadzor nad izvajalcem

Upravljanje storitev

- Upravljanje svojih storitev v skladu z Navodilom za uporabo informacijskih sistemov (sklopi: zunanji izvajalci, oddaljen dostop, zaščita pred zlonamerno kodo, politika gesel in politika administratorskih računov). Izvajalec mora upoštevati vse veljavne politike, smernice in postopke naročnika ter zagotoviti varnost, zaupnost in integriteto informacij in sistemov.

II. PONUDBENI PREDRAČUN

Ponudnik: ……

PONUDBENI PREDRAČUN št. ……

Zap. št.	postavka dela	ME	cena/ME	količina	vrednost
1	**STROJNA OPREMA**				
1.1	Strojna oprema (Teh. spec. I.2.5. Inf. zahteve)	kos		2	
1.2	Vmware licenca s 5 letno podporo	kos		1	
1.3	Namestitev opreme z vzpostavitvijo Vmware	kos		1	
2	**SIEM REŠITEV**				
2.1	Programska rešitev z vključeno licenčno podporo za prvo leto	kos		1	
2.2	Podpora za programsko rešitev za štiri leta	kos		1	
2.3	Vzpostavitev sistema SIEM	kos		1	
3	**VZDRŽEVANJE IN PODPORA**				
3.1	Vzdrževanje [SLA]	mesec		60	
3.2	Dodatne storitve na zahtevo naročnika, obračunano po dejanski porabi	ura		800	
3.3	**Nepredvidena dodatna strojna oprema ali licence** (zaradi razvoja tehnologij in zagotavljanja razpoložljivosti, celovitosti in zaupnosti ter nemotenosti delovanja implementirane rešitve)				**80.000,00**

**Vrednost postavke 3.3 je določena in je ponudnik ne sme spreminjati ter jo mora upoštevati v vrednosti Skupaj.*

Skupaj	
DDV 22 %	
Skupaj z DDV	

Strinjamo se, da so razpisane količine na enoto mere in so okvirne ter se prilagajajo konkretnim potrebam ter razpoložljivim finančnim sredstvom naročnika. Naročnik ni zavezan naročiti celotne količine storitev.
Izjavljamo, da smo ponudili in izpolnili vse pozicije iz predračuna. Nobena od postavk ni enaka 0 EUR ali neizpolnjena.
Vse cene in vrednosti so izražene v evrih. Cena ne vsebuje DDV. Cene in vrednosti so obračunane in zaokrožene na dve (2) decimalki. V ponudbeni ceni/ME so zajeti vsi stroški v zvezi s predmetom naročila.

datum: podpis: