# SMLOUVA O DÍLO

# „Dodávka a implementace centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů, serverů, aplikací a zařízení“

uzavřená níže uvedeného dne, měsíce a roku podle § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů a podle zákona č. 121/2000 Sb. (autorský zákon), ve znění pozdějších předpisů

## Smluvní strany

**Město Rýmařov**

se sídlem: **náměstí Míru 230/1, 795 01, Rýmařov**

IČO: **00296317**

DIČ: **CZ 00296317**

zastoupeno: **Ing. Luďkem Šimko**, starostou

bankovní spojení: **Komerční banka, a.s.**

č.ú.: **19-1421771 / 0100**

kontaktní osoba: XXXXX

 email: XXXXX

*(dále jen „objednatel“ nebo „zadavatel“)*

**a**

**Obchodní jméno: HCV group a.s.**

se sídlem / místem podnikání: **Chodská 1203, Rožnov pod Radhoštěm**

IČO: **25395009**

DIČ: **CZ25395009**

zastoupený/jednající: **Ing. Liborem Hutyrou, předsedou představenstva a Ing. Jaroslavem Šimíčkem, členem představenstva**

bankovní spojení: **MONETA Money Bank a.s.**

č.ú.: **157371766/0600**

zapsán v obchodním rejstříku, vedeném **u rejstříkového soudu v Ostravě**, sp. zn. **B 1849**

kontaktní osoba: **IXXXXX**

telefon: **XXXXX**

e-mail: **XXXXX**

*(dále jen „dodavatel“ nebo“ poskytovatel“)*

## Předmět a účel smlouvy

1. Účelem této smlouvy je dodávka centrálního úložiště logů a provedení jeho odborné instalace, spolu se zajištěním jeho servisu a funkčnosti v prostředí objednatele.
2. Předmětem této smlouvy je závazek zhotovitele dodat a nainstalovat funkční centrální úložiště logů, provádět jeho servis, vše dle požadavků objednatele specifikovaných v Příloze č. 1 a 2 této smlouvy (dále jen „dílo“) a za podmínek sjednaných v této smlouvě a objednatel se zavazuje dokončené dílo převzít a zaplatit za něj sjednanou cenu.
3. Pokud v Příloze č. 1 této smlouvy není uvedeno další plnění, které je nezbytné pro řádné provedení díla za podmínek této smlouvy, je zhotovitel povinen bez zbytečného odkladu na tuto skutečnost objednatele písemně upozornit.

## Termín a místo plnění

1. Provádění díla bude zahájeno bez zbytečného odkladu po nabytí účinnosti této smlouvy.
2. Termín dokončení díla
3. Termín dokončení díla: nejpozději do 6 týdnů od účinnosti této smlouvy.
4. Dílo se považuje za dokončené a zhotovitel má právo na zaplacení ceny za dílo, je-li způsobilé sloužit účelu vyplývajícímu z této smlouvy. Předání a převzetí díla se řídí ustanoveními čl. VII. této smlouvy.
5. Servisem díla se rozumí jeho opravy, úpravy a údržba k zajištění funkčnosti díla, a to po dobu: 36 měsíců ode dne předání na HW a 12 měsíců ode dne předání na SW a převzetí díla objednatelem bez výhrad.
6. Místo plnění
7. Místem plnění díla je sídlo objednatele a další budovy objednatele:
* náměstí Míru 230/1, 795 01 Rýmařov

## Práva a povinnosti smluvních stran

1. Zhotovitel se zavazuje za podmínek stanovených touto smlouvou dodat dílo bez právních a faktických vad.
2. Při zhotovování díla se zhotovitel zavazuje počínat si s odbornou péčí tak, aby byl zcela naplněn předmět a účel smlouvy.
3. Zhotovitel je povinen vynaložit maximální úsilí, aby docílil nejlepšího možného výsledku při plnění předmětu této smlouvy prostřednictvím využití svých znalostí a zkušeností.
4. Při provádění díla postupuje zhotovitel samostatně, je však vázán zejména písemnými pokyny objednatele. Zhotovitel je povinen bez zbytečného odkladu písemně upozornit objednatele na nevhodnost jeho pokynů k provedení díla. Pokud nevhodné pokyny brání v řádném provádění díla, je zhotovitel povinen v nezbytně nutném rozsahu přerušit provádění díla do doby změny pokynů objednatele nebo písemného sdělení, že objednatel trvá na provádění díla dle svých pokynů. Zhotovitel nemá nárok na náhradu nákladů spojených s přerušením provádění díla.
5. Objednatel se zavazuje poskytnout zhotoviteli součinnost potřebnou k provedení díla.
6. Zhotovitel se zavazuje, že části díla plněné poddodavatelským plněním, budou příslušným poddodavatelem provedeny v souladu se všemi podmínkami smlouvy. V takovém případě odpovídá zhotovitel za plnění poskytnuté třetí osobou, jako kdyby příslušné plnění poskytl sám, a jeho výlučná odpovědnost za poskytování řádného plnění dle smlouvy tím není jakkoliv dotčena.

## Cena díla

1. Cena za zhotovení díla představuje celkovou cenu díla zahrnující veškeré náklady, včetně licencí, dopravy a servisu, vynaložené zhotovitelem ke splnění účelu této smlouvy.
2. Zhotovitel výslovně prohlašuje, že cena díla obsahuje veškeré práce a dodávky, poplatky a jiné náklady nezbytné pro řádnou a úplnou realizaci sjednaného předmětu plnění a veškeré náklady včetně všech rizik a vlivů souvisejících s plněním předmětu smlouvy.
3. Objednatel a zhotovitel se dohodli, že cena za řádné a včasné provedení celého díla specifikovaného v čl. 2 a Příloze č. 1 a 2 této smlouvy činí celkem částku:

544 366,90 Kč včetně DPH, přičemž

cena bez DPH činí = 449 890,00 Kč

sazba DPH činí 21 %,

výše DPH činí 94 476,90 Kč.

Tato cena je stanovena jako cena konečná a úplná. Zhotovitel přebírá nebezpečí změny okolností.

1. Zhotovitel není oprávněn požadovat po objednateli poskytnutí zálohy.
2. Sjednaná celková cena díla dle této smlouvy je cenou nejvýše přípustnou, kterou je možné překročit pouze v případě zvýšení sazby DPH, a to tak, že zhotovitel ke sjednané ceně bez DPH připočítá DPH v procentní sazbě odpovídající zákonné úpravě účinné k datu uskutečnitelného zdanitelného plnění.

## Platební podmínky

1. Cena díla bude objednatelem uhrazena jednorázovou platbou na základě zhotovitelem vystavené faktury.
2. Fakturu je zhotovitel oprávněn vystavit nejdříve následující den po dni uskutečnění zdanitelného plnění, jímž se pro účely této smlouvy rozumí řádné dodání předmětu díla v souladu s čl. 7 této smlouvy.
3. Podkladem pro vystavení faktury je podepsaný protokol o předání a převzetí předmětu díla za podmínek sjednaných v této smlouvě (dále jen „předávací protokol“), v němž objednatel převzal kompletně provedené dílo bez výhrad.
4. Splatnost faktury činí 21 dnů ode dne jejího prokazatelného doručení na adresu sídla objednatele.
5. Faktura bude mít náležitosti daňového dokladu dle platných právních předpisů (zákona č. 563/1991 Sb., o účetnictví, v platném znění a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění).
6. Faktury musí obsahovat označení smlouvy, číslo účtu zhotovitele a všechny údaje dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
7. Součástí faktury bude specifikace dodaného plnění tak, aby byla v souladu s platnými účetními a daňovými předpisy, a to za účelem řádného vedení evidence majetku objednatele v souladu s těmito právními předpisy. Přílohou faktury musí být předávací protokol o převzetí díla objednatelem bez výhrad podepsaný oběma smluvními stranami. V případě, že objednatel převzal dílo s výhradami, musí být součástí faktury zápis o převzetí díla bez výhrad.
8. V případě, že faktura – daňový doklad nebude obsahovat sjednané náležitosti nebo v něm nebudou správně uvedeny údaje, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury – daňového dokladu.
9. Cena bude zhotoviteli zaplacena bezhotovostní formou převodem na jeho bankovní účet. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch zhotovitele. Objednatel uhradí jen takové plnění, které bylo fakticky zhotovitelem provedeno.

## Předání díla

1. Objednatel prohlašuje, že převezme pouze dokončené dílo bez zjevných vad, nedodělků, tj. dílo, které je způsobilé sloužit svému účelu. V opačném případě si objednatel vyhrazuje právo převzetí díla odmítnout, bez nároku na navýšení ceny díla.
2. Předání a převzetí díla proběhne na základě porovnání skutečných vlastností díla dle specifikace díla uvedené v čl. 2. této smlouvy. Po prohlídce díla smluvní strany sepíší předávací protokol, v němž bude konstatováno, zda je dílo přebíráno s výhradami nebo bez výhrad, zda stav díla vyhovuje stanoveným a sjednaným parametrům a uvedou v něm zjevné nedostatky nebo vady díla, které byly při prohlídce díla zjištěny; dále v předávacím protokole sjednají opatření a lhůty k odstranění zjištěných nedostatků a vad.
3. Pokud objednatel dílo převezme s vadami a nedodělky, které nebrání řádnému užívání díla (převzetí s výhradami), budou tyto vady a nedodělky odstraněny do 5 dnů od převzetí díla objednatelem, nedohodnou-li se strany při předání díla písemně jinak. O odstranění nedodělků a vad ve stanoveném termínu bude sepsán předávací protokol o převzetí díla bez výhrad.
4. Vlastnické právo k dílu přechází na objednatele okamžikem předání díla objednateli. Práva z poskytnuté licence objednatel nabývá okamžikem převzetí díla od zhotovitele.

## Záruka za jakost, odpovědnost za vady

1. Dílo má vady není-li způsobilé sloužit svému účelu nebo neodpovídá požadavkům stanoveným touto smlouvou.
2. Zhotovitelem poskytovaná záruka se vztahuje na kompletní funkčnost díla, jakož i na jeho vlastnosti požadované objednatelem.
3. Zhotovitel poskytuje objednateli záruku za jakost HW v délce 36 měsíců a 12 měsíců na SW, pokud zhotovitel poskytuje ve svých záručních podmínkách delší záruku, než jakou požaduje objednatel, platí tato delší záruka zhotovitele.
4. Záruční doba začíná běžet ode dne převzetí díla objednatelem bez výhrad. Záruční doba se prodlužuje o dobu, po kterou mělo dílo vadu bránící jeho řádnému užívání objednatelem.
5. Veškeré zjištěné vady díla, které se vyskytnou v záruční době, je objednatel povinen bez zbytečného odkladu písemně oznámit zhotoviteli.
6. Zhotovitel je povinen odstranit vadu nejpozději do 5 dnů ode dne jejího vytčení objednatelem, pokud se smluvní strany nedohodnou jinak. Předání a převzetí opraveného díla se řídí přiměřeně ustanoveními čl. 7. Zhotovitel poskytuje záruku za jakost na opravené dílo (jeho část) v délce 12 měsíců ode dne převzetí opraveného díla (jeho části) objednatelem.
7. Objednateli v důsledku vadného plnění vzniká nárok na odstranění vady a není-li odstranění vady možné, nárok na slevu z ceny díla nebo právo od této smlouvy odstoupit, a to dle uvážení a volby objednatele, pokud se smluvní strany nedohodnou jinak.
8. Záruka za jakost se nevztahuje na vady způsobené neodborným zásahem třetích osob nezávisle na vůli zhotovitele.
9. V případě, že zhotovitel písemně oznámí objednateli, že jím vytčenou vadu nepovažuje za záruční vadu, je objednatel oprávněn zajistit posouzení vady znalcem na základě znaleckého posudku.

Jestliže bude znaleckým posudkem zjištěno, že se jedná o záruční vadu, ponese náklady na jeho vyhotovení zhotovitel, který současně nejpozději do tří dnů zahájí odstraňování vady.

Nebude-li se, podle znaleckého posudku, jednat o záruční vadu, ponese náklady na jeho vyhotovení objednatel.

## Licenční ujednání

Pokud zhotovitel v průběhu poskytování plnění dle této smlouvy vytvoří předměty, které jsou způsobilé být předmětem ochrany poskytované právy duševního vlastnictví, zejména právem autorským, právem k patentu, užitnému vzoru, průmyslovému vzoru a dalšími právy průmyslového vlastnictví, a to včetně, nikoliv však výlučně, předmětů vytvořených dle požadavků nebo ve spolupráci s objednatelem (dále jen „chráněná díla“), náleží veškerá autorská práva a další práva průmyslového vlastnictví k takovým chráněným dílům zhotoviteli. Pokud není sjednáno písemně jinak, uděluje zhotovitel objednateli (tedy městu Rýmařov a dále pak pro veškeré městem Rýmařov zřízené příspěvkové organizace, plně či podílově vlastněné obchodní společnosti) dnem úplného zaplacení ceny plnění, v rámci, jehož poskytování bylo příslušné chráněné dílo vytvořeno, objednateli nevýhradní licenci užít takové chráněné dílo v rozsahu území České republiky, bez omezení doby trvání a způsobem potřebným pro zpracování vnitřních transakcí objednatele. Do nabytí licence má objednatel právo užít předané a převzaté chráněné dílo, či jeho jednotlivou část, dočasně. Objednatel má dovoleno vytvářet nezbytné záložní kopie smluvních děl. Záložní kopie musí být označeny jako záložní kopie a nést stejné oznámení o autorských právech jako originál. Cena nevýhradní licence je obsažena v ceně dodaného díla.

## Odpovědnost za škodu

1. Nebezpečí škody na zhotovovaném díle nese zhotovitel v plném rozsahu až do dne převzetí díla (jeho dílčí časti) objednatelem bez výhrad.
2. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
3. Zhotovitel je povinen předem zálohovat všechny IS objednatele (např. Active Directory), budou-li touto smlouvou dotčeny, před zahájením faktického plnění této smlouvy, a to pro případ jejich ztráty nebo poškození v důsledku upgrade nebo jiné nepředvídatelné skutečnosti, např. havárie během implementace.
4. Zhotovitel a jeho poddodavatelé jsou povinni zachovávat mlčenlivost o veškerých skutečnostech a údajích získaných z informačního systému objednatele, včetně údajů z registrů a rejstříků vedených jednotlivými odbory objednatele. Zhotoviteli a jeho poddodavatelům se zakazuje zneužít jakékoliv údaje třetích osob získané z informačních systémů vedených nebo spravovaných objednatelem.
5. Zhotovitel prohlašuje, že má uzavřenou pojistnou smlouvu pro případ pojištění odpovědnosti za škodu způsobenou zhotovitelem třetí osobě ve výši minimálně 0,5 mil. Kč a v této výši se zhotovitel zavazuje udržovat platnost tohoto pojištění po celou dobu účinnosti této smlouvy. Úředně ověřená kopie (bude doplněna při podpisu smlouvy s vybraným dodavatelem; pojistná smlouva se do nabídky nedokládá.) požadované pojistné smlouvy jsou přílohou č. 3 této smlouvy, která tvoří její nedílnou součást. Aktualizovanou či novou pojistnou smlouvu/pojistné smlouvy je zhotovitel povinen předložit objednateli do 5 pracovních dnů ode dne jejího (jejich) uzavření.

## Sankční ujednání

1. Dojde-li k prodlení se zaplacením ceny za dílo, je zhotovitel oprávněn účtovat objednateli úrok z prodlení ve výši 0,05 % z dlužné částky bez DPH za každý započatý den prodlení po termínu splatnosti až do doby zaplacení dlužné částky.
2. V případě, že zhotovitel neprovede dílo v termínu sjednaném touto smlouvou, ve znění jejich případných dodatků, je povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny díla bez DPH za každý i započatý den prodlení.
3. Nesplní-li zhotovitel v dohodnutém termínu svůj závazek odstranit vady a nedodělky vytknuté při převzetí díla nebo v průběhu záruční doby, je objednatel oprávněn požadovat na zhotoviteli zaplacení smluvní pokuty ve výši 0,05 % ze sjednané ceny díla bez DPH za každou vadu a za každý započatý den prodlení až do jejich úplného odstranění.
4. Objednatel je oprávněn požadovat na zhotoviteli smluvní pokutu ve výši 3 000,- Kč za každý den prodlení nebo od této smlouvy odstoupit, pokud zhotovitel není platně pojištěn anebo nepředloží objednateli pojistnou smlouvu podle článku 10. odst. 5 této smlouvy.
5. Zaplacením smluvní pokuty není dotčeno právo poškozené strany na náhradu vzniklé škody. Výši smluvních pokut považují obě smluvní strany za přiměřené.
6. Smluvní pokuty a úroky z prodlení podle tohoto článku jsou splatné do 30 dnů ode dne doručení jejich vyúčtování.
7. V případě, že závazek provést dílo zanikne před řádným ukončením díla, nezaniká nárok na smluvní pokutu, pokud vznikl dřívějším porušením povinnosti. Zánik závazku pozdním splněním neznamená zánik nároku na smluvní pokutu za prodlení s plněním.
8. Smluvní strany se dohodly, že vyúčtovaná smluvní pokuta může být jednostranně započtena vůči ceně díla, kterou je objednatel povinen uhradit.

## Ukončení smlouvy

1. Tuto smlouvu lze ukončit dohodou smluvních stran. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.
2. Od této smlouvy lze odstoupit v případech stanovených (jinde) v této smlouvě a v případě podstatného porušení povinností jednou smluvní stranou, jestliže je takové porušení povinnosti označeno za podstatné touto smlouvou nebo zákonem. Odstoupení od smlouvy je účinné dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
3. Smluvní strany se dohodly, že za podstatné porušení této smlouvy ze strany zhotovitele považují:
4. dodání nebo zhotovení vadného předmětu plnění,
5. prodlení s plněním závazku vyplývajícího z této smlouvy po dobu delší než patnáct (15) dní a nezjednání nápravy ani do deseti (10) dní od doručení oznámení objednatele o prodlení s plněním závazku,
6. prodlení se zaplacením vyfakturované ceny díla delší než třicet (30) kalendářních dnů,
7. nepředání kopie pojistné smlouvy na požadované pojištění dle čl. 10 odst. 5 této smlouvy do 10 dnů ode dne podpisu této smlouvy objednateli,
8. bude-li zjištěno, že zhotovitel je v úpadku nebo s ním bylo zahájeno insolvenční řízení nebo je v likvidaci.
9. Smluvní strany si ujednaly, že odstoupením od smlouvy v případech dle odst. 3 písm. b) a d) tohoto článku se smlouva zrušuje od počátku, pokud nemá částečné plnění samo o sobě pro objednatele význam. V ostatních případech odstoupení od smlouvy smluvní strany sjednávají, že se smlouva zrušuje s účinky do budoucna.
10. Pro případ odstoupení od smlouvy, kdy se smlouva zrušuje od počátku, smluvní strany výslovně ujednaly, že v tomto případě objednatel uhradí zhotoviteli peněžitou částku ve výši odpovídající hodnotě plnění předmětu této smlouvy do odstoupení od smlouvy, tj. to, o co se objednatel obohatil.
11. V případě odstoupení od smlouvy objednatelem objednateli vzniká nárok na úhradu vícenákladů vynaložených na dokončení díla a na náhradu ztrát vzniklých prodloužením termínu provedení díla.

## Závěrečná ustanovení

1. Práva a povinnosti smluvních stran v této smlouvě výslovně neupravené a z ní vyplývající nebo s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
2. Vzhledem k veřejnoprávnímu charakteru objednatele zhotovitel výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů. A to včetně uveřejnění kompletního znění smlouvy na základě zákonné povinnosti objednatele jako veřejnoprávního subjektu.
3. Smlouva nabývá platnosti dnem podpisu druhé smluvní strany a účinnosti dnem jejího zveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Smluvní strany se dohodly, že tuto smlouvu zveřejní objednatel po podpisu smlouvy oběma smluvními stranami.
4. Zhotovitel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě. Práva a povinnosti vyplývající z této smlouvy přecházejí na právní nástupce smluvních stran.
5. Smluvní strany se dohodly, že veškerá komunikace související s plněním předmětu této smlouvy bude probíhat prostřednictvím e-mailu oprávněných osob, přičemž se e-mailová zpráva považuje za doručenou tehdy, potvrdí-li oprávněná osoba druhé smluvní strany její doručení; osobním předáním, prostřednictvím držitele poštovní licence na adresu sídla smluvní strany. Pro případ doručování prostřednictvím pošty si smluvní strany sjednávají, že zásilka je druhé smluvní straně doručena desátým dnem ode dne jejího odeslání první smluvní stranou, pokud se smluvní strany nedohodnou jinak.
6. Smluvní strany shodně prohlašují, že si smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle určitě, vážně a srozumitelně, nikoliv v tísni nebo za nápadně nevýhodných podmínek, a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.
7. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoliv dalších podmínek.
8. Tato smlouva je vyhotovena ve čtyřech (4) stejnopisech, z nichž každý má platnost originálu. Každá ze smluvních stran obdrží po dvou vyhotoveních.
9. Tuto smlouvu je možno platně měnit pouze na základě dohody smluvních stran, formou písemných a vzestupně číslovaných dodatků, podepsaných oběma smluvními stranami.
10. Rada města rozhodla o uzavření této smlouvy o dílo na svém jednání dne 17.06.2019 usnesení č. 17 poř. č. 1017.

### Nedílnou součástí této smlouvy jsou její přílohy:

Příloha č. 1 Podrobná technická specifikace předmětu veřejné zakázky

Příloha č. 2 Řešení SEM/SIEM

Příloha č. 3 Pojistná smlouva

|  |  |  |
| --- | --- | --- |
| V Brně dne 25.06.2019  |  | V Rýmařově dne 18.06.2019 |
| Za dodavatele |  | Za objednatele |
|  |  |  |
| Ing.Libor Hutyra Ing.Jaroslav Šimíčekpředseda a člen představenstva |  | Ing. Luděk Šimkostarosta  |

Příloha 1, Podrobná technická specifikace předmětu veřejné zakázky

# POŽADAVKY NA ROZSAH FUNKCIONALITY

**Obecné funkcionality:**

* Zpracování událostí z různých zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware **- ANO**
* Možnost dopsání parseru pro zařízení aktuálně nepodporované výrobcem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému **- ANO**
* Systém standardizuje přijaté logy do jednotného formátu a logy jsou parserovány (rozdělovány) do příslušných políček dle jejich typu **- ANO**
* Nad takto standardizovanými daty systém automaticky vytváří indexy pro rychlejší vyhledávání pro všechna pole standardizovaného logu **- ANO**
* Všechny rozparsované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem **- ANO**
* Systém nesmí umožnit mazání nebo modifikování již uložených logů **- ANO**
* Konsolidace logů na centrálním místě **- ANO**
* Snadné vyhledávání událostí (ad hoc) bez nutnosti programování **- ANO**
* Grafické znázornění událostí (grafy událostí) **- ANO**
* Grafické znázornění TOP událostí nad všemi daty za určité časové období **- ANO**
* Automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě **- ANO**
* Automatické doplňování reverzních DNS záznamů k IP adresám **- ANO**
* V případě přetížení systému jsou události ukládány do vyrovnávací paměti **- ANO**
* Unifikované vyhledávání napříč všemi typy dat a zařízení **- ANO**
* certifikátem na společnost dodavatele (subdodavatele) nebo společnost výrobce nabízeného systému. Nelze nahradit čestným prohlášením **- ANO**
* Možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování **- ANO**
* Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů **- ANO**
* Předpřipravené pohledy na uložená data **- ANO**
* Aktualizace reportů a pohledů výrobcem **- ANO**
* Konfigurační a Systémové rozhraní a On-line dokumentace v Českém jazyce **- ANO**
* Kapacitní i výkonová škálovatelnost **- ANO**
* Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data musí být minimálně 12TB **- ANO**
* Požadujeme, aby ze systému bylo možné vytáhnout 2 libovolné disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště **- ANO**
* Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog **- ANO**
* Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému **- ANO**
* Uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému **- ANO**
* Možnost ověřovat uživatele systému na externím LDAP serveru **- ANO**

**HW parametry:**

* Jedna hardwarová appliance o velikosti max. 1U **- ANO**
* HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech **- ANO**
* Minimálně 4x 1 Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW **- ANO**
* 2x napájecí zdroje s redundancí napájení 1+1
* Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).

**SW parametry**

* Zařízení funguje formou appliance (všechny části systémů je možné nastavit v centrální webové správcovské konzoli – není nutné editovat žádné konfigurační soubory včetně IP adresace systému) **- ANO**
* Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální webovou správcovskou konzoli **- ANO**
* Průměrný příjem min. 2 tis událostí / s **- ANO**
* Špičkový příjem 4 tis událostí / s, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později **- ANO**
* Licenčně neomezený počet zařízení pro příjem zasílaných událostí **- ANO**
* Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku **- ANO**
* Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy **- ANO**
* Možnost on-line ladění uživatelsky definovaných parserů – při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat **- ANO**
* V centrální webové správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod **- ANO**
* V centrální webové správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.) **- ANO**
* Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem **- ANO**
* Podpora zrcadlení a clusteru - 2 a více zařízení v režimu active / active **- ANO**
* Vícenodový systém se chová jako 1 celek **- ANO**
* V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru **- ANO**
* Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru **- ANO**
* V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody **- ANO**

**Alerty**

* Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert **- ANO**
* Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události **- ANO**
* Předpřipravené sety/vzory alertu výrobcem **- ANO**
* Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku **- ANO**
* V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru) **- ANO**

**Sběr událostí z Microsoft prostředí**

* Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních Windows logů, tak monitoring souborových logů **- ANO**
* Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací **- ANO**
* Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální webové správcovské konzole **- ANO**
* Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální webové správcovské konzole. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku **- ANO**
* Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému **- ANO**
* Správa a aktualizace Windows agenta se neprovádí z Group Policy **- ANO**
* Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.) **- ANO**
* Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů **- ANO**
* Komunikace Windows agenta a centrálního systému musí být šifrovaná **- ANO**
* Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb **- ANO**
* Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému **- ANO**
* Počet instalací Windows agenta nesmí být licenčně omezen **- ANO**
* **ROZSAH PODPORY, SERVISU, DOHLEDU A KONZULTACÍ (MAINTENANCE, ODBORNÉ PODPORY)**
* standardní podpora SW řešení na dobu 12 měsíců – odstraňování chyb řešení, poskytování systémových, bezpečnostních a aplikačních update, držení hotline pro hlášení chyb v pracovní době (po-pá 9-17). Podpora výrobce na aktualizaci systému a parserů na 12 měsíců **- ANO**
* záruka na dodané HW řešení na dobu 36 měsíců – uplatněná u autorizovaného partnera nebo v servisním středisku výrobce - **- ANO**
* Součástí je profylaxe, změny v nastavení pravidel, změny v konfiguraci, konzultace. Forma je telefonická, písemná nebo v místě Zadavatele **- ANO**

Příloha 2, Řešení SEM/SIEM

**Validace s požadavky uvedenými v Zadávací dokumentaci - (Příloha č.7 ) - Řešení SEM/SIEM do 2000 událostí/sec. s minimálně 12TB velikostí databáze**

# OBECNÉ POŽADAVKY NA SYSTÉM PRO CENTRALIZOVANOU SPRÁVU LOGŮ, UDÁLOSTÍ A STROJOVÝCH DAT

|  |  |
| --- | --- |
| Systém pracuje jako appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Alternativně může být systém, včetně kompletní infrastruktury, dodán i jako virtuální appliance, za zachování všech ostatních požadovaných parametrů. | **ANO** |
| Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz seznam podporovaných zařízení) | **ANO** |
| Systém umožňuje dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému – Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce. | **ANO** |
| Parsery a alerty musí umožňovat použití matematických operací. | **ANO** |
| Parsery a alerty musí podporovat dekódování URL. | **ANO** |
| Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožňovat příjem logů i na uživatelsky definovaných UDP a TCP portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.  | **ANO** |
| Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. | **ANO** |
| Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. | **ANO** |
| Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259. | **ANO** |
| Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.  | **ANO** |
| Systém musí umožňovat konfiguraci filtrace nerelevantních událostí. | **ANO** |
| Systém provádí konsolidaci logů na centrálním místě. | **ANO** |
| Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. | **ANO** |
| Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. | **ANO** |
| Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období. | **ANO** |
| Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace. | **ANO** |
| Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám. | **ANO** |
| V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB. | **ANO** |
| Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení. | **ANO** |
| Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením. | **ANO - potvrzení přiloženo níže** |
| Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. | **ANO** |
| Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk. | **ANO** |
| Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. | **ANO** |
| Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem. | **ANO** |
| Konfigurační a Systémové rozhraní a dokumentace musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce. | **ANO** |
| Systém nabízí kapacitní i výkonovou škálovatelnost. | **ANO** |
| Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB. | **ANO** |
| Požadujeme, aby ze systému bylo možné vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště. | **ANO**  |
| Monitoring stavu systému – alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog. | **ANO** |
| Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Požadujeme vzorový návod na integraci s monitorovacím systémem Zabbix. | **ANO** |
| Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“. | **ANO - potvrzení přiloženo níže** |
| Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému. | **ANO** |
| Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. | **ANO** |
| Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes MI protokol neumožňuje monitorovat textové logy.  | **ANO** |
| Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. | **ANO** |

* **Minimální HW parametry požadovaného systému nebo subsystému pro virtualizované řešení**

|  |  |
| --- | --- |
| Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. | **ANO** |
| HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech. V případě virtualizovaného řešení pak i licence pro provoz potřebné virtualizace. | **ANO** |
| 1 procesor, min. 10 jader s podpora HyperThreadingu. | **ANO** |
| RAM Min. 64 GB DDR-4. | **ANO** |
| Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 4GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. | **ANO** |
| Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m. | **ANO** |
| Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. | **ANO** |
| Větráky v systému musí být vyměnitelné za provozu a redundantní. | **ANO** |
| 2x napájecí zdroje s redundancí napájení 1+1. | **ANO** |
| Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. | **ANO** |
| Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). | **ANO** |

* **Výkonnostní a SW parametry systému**

|  |  |
| --- | --- |
| Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli, není nutné editovat žádné konfigurační soubory včetně IP adresace systému). | **ANO** |
| Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli. | **ANO** |
| Systém musí podporovat downgrade, pro případ problémů s novou verzí systému po upgrade. | **ANO** |
| Průměrný trvalý příjem min. 2 tisíce událostí/s. Výkon musí odpovídat pro požadované množství událostí s průměrnou délkou 600Byte. | **ANO** |
| Špičkový příjem minimálně 4 tisíce událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí, než je průměrný trvalý příjem, je systém uloží do bufferu a zpracuje později.  | **ANO** |
| Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 100 GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat. | **ANO** |
| Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | **ANO** |
| Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy. | **ANO** |
| Systém musí podporovat integraci externích informací. | **ANO** |
| Možnost on-line ladění uživatelsky definovaných parserů – při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení. | **ANO** |
| V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. | **ANO** |
| V centrální správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.). | **ANO** |
| Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | **ANO** |
| V případě nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – 2 nody.(Vysokou dostupnost při realizaci sběru logů očekáváme ve spolupráci s aktivními prvky sítě) | **ANO** |
| Dvounodový cluster se chová jako 1 celek. | **ANO** |
| V případě využití dvou nodů v clusteru se zrychluje vyhledávání a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru. | **ANO** |
| V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu (řízenou aktivním prvkem počítačové sítě) a zároveň cluster musí zajišťovat synchronizaci událostí mezi nody. | **ANO** |
| Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. | **ANO** |
| Podpora zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Zálohy musí systém umožnit obnovit a data ze záloh během obnovy znova indexovat tak, aby bylo možné v datech obnovených ze záloh pracovat shodně jako s aktuálním obsahem databáze. | **ANO** |

* **Alerty**

|  |  |
| --- | --- |
| Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert. | **ANO** |
| Text alertu musí být uživatelsky definovatelný s proměnnými z přijaté rozparsované události. | **ANO** |
| Systém musí obsahovat předpřipravené sety/vzory alertů a korelací výrobcem. | **ANO** |
| Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | **ANO** |
| Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. | **ANO** |
| V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha). | **ANO** |
| Systém podporuje základní funkce SIEM – funkce pro korelace událostí a upozornění s hraničními limity. | **ANO** |

* **Sběr událostí z Microsoft prostředí**

|  |  |
| --- | --- |
| Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. | **ANO** |
| Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací. | **ANO** |
| Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. | **ANO** |
| Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | **ANO** |
| Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy. | **ANO** |
| Agent automaticky překládá zástupné kódy status ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network atd.). | **ANO** |
| Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů. | **ANO** |
| Komunikace Windows agenta a centrálního systému musí být šifrovaná. | **ANO** |
| Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. | **ANO** |
| Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. | **ANO** |
| Počet instalací Windows agenta nesmí být licenčně omezen. | **ANO** |

* **Podpora pro sběr událostí z poboček**

|  |  |
| --- | --- |
| Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. | **ANO** |
| Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat. | **ANO** |
| Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.  | **ANO** |
| Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.  | **ANO** |
| Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100 GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem. | **ANO** |
| Řešení pro sběr dat z poboček musí mít výkon minimálně 2 tisíce událostí/s, a to i v trvalé zátěži. | **ANO** |
| Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů. | **ANO** |
| Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V. | **ANO** |
| Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT). | **ANO** |

* **Vysoká dostupnost, SW Podpora a záruka na hardware**

|  |  |
| --- | --- |
| Požadujeme volitelnou podporu pro budoucí nasazení ve vysoké dostupnosti. | **ANO** |
| HW – Požadovaná min. **36 měsíců** servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | **ANO** |
| SW – Podpora výrobce na aktualizaci systému a parserů na **12 měsíců.** Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.  | **ANO** |

* **Minimální seznam podporovaných zdrojů logů:**

Apache httpd, Apache Tomcat, Amavis, Antivir AVG, Antivir Avast, Antivir Eset, Antivir Eset Remote administrator, Brocade FC switches , ArcSight CEF format all sources, Barracuda Email Security Gateway, Cisco ASA, Cisco Firepower, Cisco IOS, Cisco IronPort, Cisco Nexus, Cisco SMB, Cisco WLC, CompuNet GAMA (on request), Dell Force10, Dell iDrac (Server OoB management), Dell PowerConnect, Dell SonicWALL, Dell W-series WiFi, Discard (Special distard rule), Dropbear SSH (mostly Embedded Linux), Extreme NAC, Extreme Networks XOS, FlowMon, FortiAuthenticator, FortiDDoS, Fortigate, FortiGate-Lite (performance optimized), FortiMail, FortiManager, FreeRADIUS, Qradar LEEF format all sources, HAProxy (structured rfc5425 logformat), HPE Aruba Instant AP (WLAN), HPE Aruba Mobility Controller (WLAN), HPE iLo 4 (Server OoB management), HPE IMC, HPE routers, HPE switches Procurve OS, HPE switches Comware OS, HPE Comware WLAN, Huawei USG, CheckPoint LOG Exporter, CheckPoint via OPSEC protocol, ISC BIND, ISC DHCP, ISC DHCPD, JSON format all sources, Juniper SRX, Juniper SRX-Lite (performance optimized), Kaspersky Endpoint Security, Kaspersky Security Center, Kerio Connect, Kerio Control, Kernun Clear Web, Kernun Web filter, Linux Cron, Linux Freeradius, Linux Iptables, Linux Postfix, LOGmanager, Mikrotik, Microsoft Exchange log, Microsoft SharePoint, Microsoft SQL, Microsoft Windows DHCP log, Microsoft Windows DNS debug log, Microsoft Windows Firewall (optimized for performance), Microsoft Windows IIS, MySQL, Nginx, Novell eDirectory, OpenSSH server, Oracle DB, Palo Alto Networks NGFW, PostgreSQL, Ruckuss wireless, SAP, Shorewall, SonicWall, Sophos, SpamAssasin, Squid (Web Proxy), Squid for Windows, RFC5425 format all sources, Symantec Endpoint Protection Manager, Symantec Messaging Gateway (brightmail), Synology NAS DSM, Trapeze, TrendMicro DeepDiscovery, TrendMicro TippingPoint NG-IPS, UBNT Rocket, UBNT UniFI, VMware, Windows - any logs from Event Viewer, Windows - any text log from file