SMLOUVA O DÍLO

(SMLOUVA NA DODÁVKU A IMPLEMENTACI SYSTÉMU CENTRÁLNÍHO LOGOVÁNÍ)

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

Čl. 1. Smluvní strany

1. Plzeňský kraj

se sídlem:	Škroupova 18, 306 13 Plzeň
IČO:	70890366
DIČ:	CZ 70890366
zastoupený:	p. Václavem Šlajsem, hejtmanem Plzeňského kraje
k podpisu smlouvy pověřen:	na základě usnesení Rady Plzeňského kraje č. 2571/14 ze dne 22.9.2014 p. Ivo Grüner, náměstek hejtmana
bankovní spojení:	Raiffeisenbank a.s., pobočka Plzeň
č. ú.:	1083003606/5500
kontaktní osoba:	Ing. Eliška Pečenková, vedoucí odboru informatiky KÚPK telefon: 377195261 e-mail: eliska.pecenkova@plzensky-kraj.cz

(dále jen „objednatel“, „zadavatel“)

a

2. Obchodní jméno: CGI IT Czech Republic s.r.o.

se sídlem: Praha 6, Na Okraji 335/42, PSČ 162 00

IČO: 62412388

DIČ: CZ62412388

zastoupený: Ing. Pavlem Malínkem, jednatelem

bankovní spojení: Citibank a.s.

č. ú.: 2041000305/2600

zapsán v obchodním rejstříku, vedeném Městským soudem v Praze, oddíl C, vl. 34304

kontaktní osoba: Libor Benák, Vice-President

telefon: 737264015, e-mail: libor.benak@cgi.com

(dále jen „zhotovitel“, „uchazeč“)

Tato smlouva se uzavírá v návaznosti na nadlimitní veřejnou zakázku „Centrální logování“, zadávanou objednatelem jakožto zadavatelem v otevřeném zadávacím řízení podle § 27 a násl. zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.

Veřejná zakázka je realizována v rámci projektu Plzeňského kraje s názvem "ICT služby technologického centra Plzeňského kraje – části I., III., IV. a V.“ Výzvy č. 08 na „Rozvoj služeb eGovernementu v krajích“ v rámci Integrovaného operačního programu (IOP). Projekt registrační číslo CZ.1.06/2.1.00/08.07231.

Nabídka zhotovitele coby vítězného uchazeče byla zadavatelem vybrána jako nabídka nejvhodnější usnesením Rady Plzeňského kraje č. 2571/14 ze dne 22.9.2014.

Čl. 2. Předmět smlouvy

1. Touto smlouvou se zhotovitel zavazuje provést řádně a včas pro objednatele dílo spočívající v implementaci jím dodaného softwarového řešení systému centrálního logování - tzv. SIEM (Security Information and Event Management), v souladu s Technickou specifikací objednatele, uvedenou v příloze č. 1 této smlouvy a návrhem technického řešení zhotovitele, uvedeným v příloze č. 2 této smlouvy.
2. Zhotovitel se současně zavazuje dodat objednateli potřebné licence softwarového řešení systému centrálního logování (SIEM) včetně smluvního převedení uživatelských práv k

předmětné licenci a předání případných dokladů nutných k užívání licence. Specifikace licence softwarového řešení je uvedena v příloze č. 3 této smlouvy.

3. Zhotovitel se zavazuje v rámci implementace SIEM řešení do prostředí objednatele provést následující činnosti:
   a) zpracování podrobné implementační analýzy prostředí Plzeňského kraje pro potřeby implementace SIEM;

   b) napojení vybraných informačních systémů na dodané a implementované SIEM řešení.

4. Předmětem plnění smlouvy jsou dále následující činnosti zhotovitele:
   - Proškolení administrátorů. Zpracování školící dokumentace.
   - Zpracování provozní dokumentace (bezpečnostní dokumentace, příručka pro uživatele a administrátory) k implementovanému řešení SIEM, v rozsahu dle přílohy č.1 smlouvy.

Čl. 3. Doba a místo plnění

1. Doba dokončení díla
Práce na díle budou zahájeny ihned po uzavření této smlouvy.

Dodávka a implementace softwarového řešení systému centrálního logování (SIEM) bude zhotovitelem realizována nejpozději do 31.12.2014, dle časového harmonogramu, který je přílohou č. 4 smlouvy.

2. Místo plnění díla
Místem plnění díla je sídlo objednatele – tj. budova sídla Plzeňského kraje a Krajského úřadu Plzeňského kraje na adrese Škroupova 18, Plzeň.

Čl. 4. Práva a povinnosti smluvních stran

1. Zhotovitel se zavazuje za podmínek stanovených touto smlouvou na svůj náklad a na své nebezpečí ve sjednaném termínu splnit celý předmět smlouvy. Zhotovitel se dále zavazuje dodat řádně a včas plnění podle této smlouvy 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 případnými 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. Zhotovitel je povinen v průběhu provádění díla dodržovat obecně závazné předpisy a normy, postupovat s náležitou odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy objednatele.

6. Zhotovitel je povinen v průběhu provádění díla neprodleně informovat objednatele o všech skutečnostech, které mají nebo mohou mít vliv na provedení díla.

7. Pokud objednatel zjistí, že zhotovitel provádí dílo v rozporu se svými povinnostmi, je oprávněn požadovat, aby zhotovitel odstranil v objednatelem stanovené lhůtě vzniklé vady a dílo prováděl řádným způsobem.

8. Objednatel se zavazuje v průběhu provádění díla poskytovat zhotoviteli součinnost v míře nezbytně nutné pro řádné zhotovení díla.

9. Součinnost objednatele bude omezena na nezbytnou míru a bude se vztahovat především na schvalování výstupů zhotovitele v předem definovaných kontrolních dnech a na nezbytnou IT podporu nutnou k nasazení řešení a realizaci vazeb. Rozsah součinnosti bude odsouhlasen při zahájení realizace, včetně termínů jejího poskytování.

10. Objednatel se zavazuje řádně a včas dokončený předmět smlouvy od zhotovitele protokolárně převzít a zaplatit zhotoviteli sjednanou cenu.

11. Zhotovitel se zavazuje udržovat v platnosti po celou dobu plnění závazků ze smlouvy certifikáty a osvědčení stanovené kvalifikační dokumentací, vztahující se ke zhotoviteli a osobám, které se budou podílet na provádění díla.

12. Zhotovitel se zavazuje plnit předmět zakázky prostřednictvím projektového týmu, představeného v nabídce na veřejnou zakázku. Zhotovitel se dále zavazuje zachovávat profesionální složení projektového týmu, uvedeného v nabídce na veřejnou zakázku. Zhotovitel se zavazuje, že členové projektového týmu, jejichž pomocí bylo prokázáno splnění kvalifikačních předpokladů, budou skutečně zapojeni v uvedených rolích do provádění díla. V případě nutné personální změny v projektovém týmu je nutné tuto skutečnost projednat s objednatelem a zhotovitel je povinen předložit splnění srovnatelných kvalifikačních předpokladů pro náhradní osoby, jimiž budou tyto pozice obsazeny, k odsouhlasení objednateli.

Čl. 5. Cena díla

1. Cena za zhotovení díla představuje objednatelem /jakožto zadavatelem/ akceptovanou nabídkovou cenu, předloženou zhotovitelem /jakožto uchazečem/ v nabídce na veřejnou zakázku „Centrální logování", s výjimkou ceny za technickou podporu, která je uvedena v samostatně uzavřené smlouvě o poskytování maintenance. Rozklad ceny díla je uveden v příloze č. 5 této smlouvy.

2. Zhotovitel výslovně prohlašuje, že nabídková cena a 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 činí celkem částku:

   1 936 000,-- Kč včetně DPH, přičemž
   cena bez DPH činí 1 600 000,-- Kč,
   sazba DPH činí 21 %,
   výše DPH činí 336 000,-- Kč.

4. Tato cena je stanovena jako cena konečná a úplná.

5. Zhotovitel není oprávněn požadovat po objednateli poskytnutí zálohy.

6. Zhotovitel na sebe výslovně bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.

7. Daň z přidané hodnoty bude připočtena k ceně díla ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

8. Sjednaná celková cena uvedená v odst. 3. tohoto článku 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.

Čl. 6. Platební podmínky

1. Cena díla bude objednatelem uhrazena vždy 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 dodání předmětu díla definovaného v čl. 2 této smlouvy.

3. Podkladem pro vystavení faktury je podepsaný protokol o předání a převzetí předmětu díla.

4. Splatnost faktur činí 30 dnů ode dne jejich prokazatelného doručení na adresu sídla objednatele.

5. V souladu s § 21 odst. 9 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, sjednávají smluvní strany dílčí plnění.

6. 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).

7. Je dohodnuto, že společně s fakturou zhotovitel poskytne kopii akceptačního protokolu ohledně všech dílčích plnění, jíž se fakturace týká, podepsaného pověřenými zástupci obou smluvních stran.

9. 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.

10. V případě, že faktura – daňový doklad nebude obsahovat stanovené náležitosti nebo v něm nebudou správně uvedené údaje nebo není doložena kopií potvrzeného příslušného akceptačního protokolu/záznamu o činnostech, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury – daňového dokladu.

11. Po vzniku práva fakturovat je zhotovitel povinen vystavit a objednateli předat faktury v trojím vyhotovení.

12. 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.

13. Dojde-li ke dni uskutečnění zdanitelného plnění ke změně sazby DPH, bude zhotovitel fakturovat objednateli cenu s DPH ve výši odpovídající platné právní úpravě ke dni uskutečnění zdanitelného plnění.

14. Každý originální účetní doklad bude obsahovat informaci, že se jedná o projekt IOP a musí být označen číslem projektu.

15. Pokud to bude možné, bude účetnictví vedeno v elektronické formě. V souladu s předpisy ES se účetní záznamy o účetních operacích budou v co největší možné míře uchovávat v elektronické formě, minimálně do 31.12.2021.

16. Zhotovitel souhlasí s tím, aby subjekty oprávněné dle zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze smlouvy s tím, že se zhotovitel podrobí této kontrole, a bude působit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona.

17. Zhotovitel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

18. Zhotovitel se zavazuje řádně uchovávat veškerou dokumentaci související s realizací předmětu smlouvy, včetně účetních dokladů v souladu s článkem 90 Nařízení Rady (ES) č. 1083/2006 minimálně do konce roku 2021, pokud zvláštní právní předpis nestanoví v době trvání tohoto závazku zhotovitele lhůtu delší.

19. Zhotovitel je povinen archivovat originální vyhotovení smlouvy včetně jejích dodatků, originály účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let od zániku této smlouvy, minimálně však do roku 2021. Po tuto dobu je zhotovitel povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s plněním této smlouvy.

20. Zhotovitel je povinen všechny písemné zprávy, písemné výstupy a prezentace opatřit vizuální identitou projektů dle Pravidel pro provádění informačních a propagačních opatření (viz příloha č. 4 Příručky).

21. Zhotovitel prohlašuje, že ke dni nabytí účinnosti této smlouvy je s těmito pravidly seznámen. V případě, že v průběhu plnění této smlouvy dojde ke změně těchto pravidel, je zadavatel povinen o této skutečnosti zhotovitele bezodkladně informovat.

Čl. 7. Předání díla

1. Zhotovitel splní svoji povinnost zhotovit dílo jeho řádným a včasným dokončením v souladu s podmínkami této smlouvy a zadávací dokumentace a předáním hotového díla objednateli.

2. Objednatel prohlašuje, že převezme pouze dokončené dílo, bez zjevných vad a nedodělků, bez podstatných vad bránících funkcionalitě předávaného díla. V opačném případě si objednatel vyhrazuje právo převzetí díla odmítnout, bez nároku na navýšení ceny díla.

3. Předání a převzetí částí díla proběhne na základě akceptace plnění, která zahrnuje porovnání skutečných vlastností díla se specifikací díla uvedenou v čl. II. této smlouvy. Akceptace plnění je potvrzena podpisem akceptačního protokolu Objednatelem. Součástí akceptačního protokolu je jednoznačná identifikace předávaného díla.

4. Podmínkou akceptace plnění na straně objednatele je správný a ověřený provoz řešení včetně správného a úplného vyhodnocování požadovaných logů v SIEM a předání veškeré dokumentace.

5. Zjistí-li objednatel nedostatky, nedodělky, či vady, oznámí to písemnou formou bez zbytečného odkladu zhotoviteli.

6. Místem předání díla je sídlo objednatele na adrese Škroupova 18, 306 13 Plzeň. Za objednatele je oprávněn hotové dílo převzít a akceptační protokol podepsat Ing. Eliška Pečenková, vedoucí odboru informatiky Krajského úřadu Plzeňského kraje.

7. Vlastnické právo k dílu přechází na objednatele okamžikem předání díla objednateli. Práva z poskytnuté licence objednatel nabývá okamžikem převzetí díla od zhotovitele.

Čl. 8. Bezpečnost díla

1. Objednatel upozorňuje zhotovitele, že aby mohl být informační systém (tj. dílo) zařazen do infrastruktury Plzeňského kraje, resp. Krajského úřadu Plzeňského kraje, tak musí splňovat bezpečnostní opatření, která zajistí, že informační systém projde penetračními testy dle metodiky:
http://www.owasp.org/index.php/Category:OWASP_Project

V odkazu jsou všechny techniky napadnutí, proti kterým musí být informační systém zabezpečen.

2. Zda informační systém tato bezpečností opatření splňuje, si objednatel ověří na vlastní náklady. Při zjištění bezpečnostních vad, je zhotovitel povinen tyto vady odstranit. Ještě jeden následný penetrační test po odstranění takových závad hradí objednatel. Pokud bezpečnostní chyby přetrvají, další penetrační testy bude hradit zhotovitel. Bezpečný průchod informačního systému penetračními testy je podmínkou pro akceptaci díla.

Čl. 9. Záruka za dílo

1. Zhotovitel poskytuje objednateli záruku v délce trvání 3 let, že dílo dle této smlouvy bude ke dni předání a převzetí objednatelem způsobilé k řádnému užití a bude mít vlastnosti stanovené touto smlouvou.

2. Zhotovitelem poskytovaná záruka se vztahuje na funkčnosti díla, jakož i na jeho vlastnosti požadované objednatelem.

3. Záruční doba začíná běžet ode dne převzetí díla objednatelem. Záruční doba se prodlužuje o dobu, po kterou mělo dílo vadu bránící jeho řádnému užívání objednatelem, nebo po kterou bylo plnění mimo provoz z důvodu vady, na kterou se vztahuje záruka.

4. Veškeré zjištěné nedostatky, nedodělky a vady díla, které se vyskytnou v záruční době, je zhotovitel povinen bez zbytečného odkladu písemně oznámit objednateli.

5. Vadou díla se pro účely této smlouvy rozumí rozpor mezi sjednanými podmínkami provedení díla a skutečným stavem díla.

6. Objednatel má vůči zhotoviteli tato práva z odpovědnosti za vady:
   - právo na bezplatné odstranění reklamovaných vad, a to bezprostředně po oznámení vady objednatelem, nejpozději ve lhůtě 15 dnů od oznámení vady objednatelem,
   - právo na poskytnutí přiměřené slevy z ceny odpovídající rozsahu reklamovaných vad či nedodělků,
   - právo na odstoupení od smlouvy, kdy vady či nedodělky jsou takového charakteru, že ztěžují či dokonce brání v užívání díla, nebo
   - právo na zaplacení nákladů na odstranění vad v případě, kdy si objednatel vadu či nedodělek odstraní sám nebo použije třetí osoby k jejich odstranění.

7. Uplatněním nároků z odpovědnosti za vady není dotčeno právo na náhradu škody. Zhotovitel odpovídá objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla zhotovitelem ve stanoveném termínu.

Čl. 10. Licenční ujednání

1. Pokud zhotovitel v rámci plnění předmětu této smlouvy vytvoří dílo podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon), poskytuje objednateli licenci - tj. oprávnění k výkonu práva užívat vytvořené autorské dílo.
2. Zhotovitel poskytuje licenci jako:

a) nevýhradní licenci k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně k účelu, ke kterému bylo takové dílo uchazečem vytvořeno v souladu se smlouvou a to v rozsahu minimálně nezbytném pro řádné užívání díla zadavatelem,

b) licenci neomezenou územním či množstevním rozsahem a rovněž tak neomezenou způsobem nebo rozsahem užití;

c) licenci udělenou na dobu určitou, a to po celou dobu trvání majetkových práv k dílu;

d) licenci převoditelnou a postupitelnou, tj. která je udělena s právem udělení bezúplatné podlicence či postoupení licence třetí osobě;

e) licenci, kterou není zadavatel povinen využít.

f) licenci, která umožňuje zadavateli užívání díla všemi známými způsoby pro svou vlastní, výhradně nekomerční potřebu a užívat dílo pro vnitřní potřebu (intranet) bez omezení;

g) zobrazit na internetu dílo nebo jeho vybrané části společně s údajem o autorství zhotovitele; tento údaj bude uveden ve formě © obchodní firma zhotovitele.

3. Z poskytnuté licence vyplývají objednateli následující oprávnění a závazky:

a) užívat dílo všemi známými způsoby pro svou výhradně nekomerční potřebu, k účelům uvedeným v čl. 3. této smlouvy,

b) užívat dílo pro vnitřní potřebu (intranet) bez omezení,

c) zobrazit na internetu vybrané části díla společně s údajem o autorství zhotovitele; tento údaj bude uveden ve formě © obchodní firma zhotovitele,

d) poskytnout dílo jako podklad pro zpracování třetím osobám, které budou na základě smlouvy s objednatelem zpracovávat zakázky pro objednatele,

e) poskytnout dílo nebo jeho část třetím osobám na základě písemné podlicenční smlouvy, objednatel se zavazuje třetí osoby zavázat užíváním díla nebo jeho částí stejným způsobem jako objednatel.

4. Povinnost týkající se licence platí pro zhotovitele i v případě zhotovení části předmětu smlouvy subdodavatelem.

5. Zhotovitel je povinen zajistit, aby výsledkem jeho plnění nebo jakékoliv jeho části nebyla porušena práva třetích osob. Pro případ, že užíváním předmětu plnění nebo jeho dílčí části nebo prostou existencí předmětu plnění nebo jeho dílčí části budou v důsledku porušení povinností zhotovitele dotčena práva třetích osob, nese zhotovitel vedle odpovědnosti za takovéto vady plnění i odpovědnost za veškeré škody, které tím objednateli vzniknou.

8. Zhotovitel je povinen předat objednateli na jeho žádost veškeré zdrojové kódy k dílu (budou-li vzhledem k vybranému technickému řešení existovat), včetně související dokumentace, a to tak, že budou objednateli předány na datovém nosiči CD/DVD. Takové předání proběhne do 10-ti dnů od podání výzvy k předání Objednatelem, nejdříve však předáním díla. Pokud nebude podána výzva k předání kódů k dílu a dokumentaci na CD/DVD, předá je zhotovitel nejpozději k datu ukončení účinnosti této smlouvy.

9. Objednatel a zhotovitel se výslovně dohodli, že odměna za poskytnutí licence je již zahrnuta v ceně za poskytnuté plnění dle této smlouvy o dílo.

10. Při užití autorského díla, software, je zhotovitel povinen respektovat licenční podmínky výrobce nabízené technologie, které jsou přiloženy k této smlouvě jako její příloha č. 6.

11. V případě rozporu mezi definicí licence uvedené v čl. 10. bodě 2. písm. a) až d), na straně jedné, a licenčními podmínkami vykonavatele autorských práv k autorskému dílu (k software), na straně druhé, mají přednost licenční podmínky vykonavatele autorských práv. I v tomto případě však nebude užitím licence dotčeno oprávnění objednatele užívat předmětné software (systém centrálního logování SIEM) v souladu s ustanoveními bodu 10.2. této smlouvy.

Čl. 11. Pojištění

1. Zhotovitel se zavazuje udržovat v platnosti po celou dobu plnění závazků z této smlouvy pojištění odpovědnosti za škodu způsobenou zhotovitelem třetí osobě, přičemž limit pojistného plnění vyplývající z pojistné smlouvy nesmí být nižší než 2 mil. Kč.
2. Kopii pojistné smlouvy o pojištění odpovědnosti za škodu způsobenou zhotovitelem třetí osobě předloží zhotovitel objednateli nejpozději ke dni uzavření této smlouvy.

3. Nesplnění této smluvní povinnosti znamená neposkytnutí řádné součinnosti, potřebné k uzavření smlouvy, a tato smlouva nebude uzavřena.

Čl. 12. Odpovědnost za škodu

1. Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy.

2. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

Čl. 13. Sankční ujednání

1. Dojde-li k prodlení s úhradou daňového dokladu - faktury, je zhotovitel oprávněn účtovat objednateli smluvní pokutu ve výši 0,05 % z dlužné částky za každý započatý den prodlení po termínu splatnosti až do doby zaplacení dlužné částky.

2. Nesplní-li zhotovitel svůj závazek v rozsahu a čase plnění sjednaném touto smlouvou, je oprávněn objednatel požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,2 % ze sjednané ceny plnění dle této smlouvy za každý započatý den prodlení, až do řádného dokončení a předání celého předmětu plnění a zhotovitel je povinen takto požadovanou smluvní pokutu zaplatit.

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 předmětu plnění za každý započatý den prodlení až do jejich úplného odstranění a zhotovitel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

4. Poruší-li zhotovitel povinnost stanovenou v čl. 4 bodu 12. smlouvy, vztahující se k plnění předmětu smlouvy prostřednictvím projektového (realizačního) týmu objednatele, zavazuje se zaplatit objednateli smluvní pokutu 100 000 Kč za každý zjištěný případ porušení této povinnosti.

5. Zaplacením smluvní pokuty není dotčeno právo poškozené strany na náhradu vzniklé škody. Výši smluvních pokut považují obě smluvní strany shodně za přiměřené. Základem pro výpočet smluvní pokuty je cena bez DPH.

6. Smluvní pokuty a úroky z prodlení podle tohoto článku jsou splatné do 30 dnů ode dne doručení jejich vyúčtování.

Čl. 14. Ochrana osobních údajů

Zhotovitel se při plnění předmětu smlouvy zavazuje postupovat v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů. Zejména pak:

1. Souhlas subjektů údajů se zpracováním osobních údajů, jakož i poučení subjektů údajů o zpracování osobních údajů a informační povinnost, jsou-li podle zákona č. 101/2000 Sb. vyžadovány, zajišťuje objednatel.

2. Jestliže zhotovitel zjistí, že objednatel porušuje povinnosti stanovené zákonem č.101/2000 Sb., je povinen jej na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů.

3. Povinnosti stanovené § 5 zákona č. 101/2000 Sb. objednateli jako správci osobních údajů, je zhotovitel povinen obdobně dodržovat. Zhotovitel je zejména povinen:

a) shromažďovat osobní údaje odpovídající pouze účelu stanovenému v této Smlouvě a v rozsahu nezbytném pro naplnění stanového účelu,
b) uchovávat osobní údaje pouze po sjednanou dobu, která je nezbytná k účelu jejich zpracování a za účinnosti této smlouvy,
c) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny,
d) nesdružovat osobní údaje získané k rozdílným účelům,
e) na pokyn správce osobních údajů osobní údaje zlikvidovat, pokud pomine účel jejich zpracování.

4. Zhotovitel je povinen před prvním přístupem k osobním údajům zavázat zaměstnance zhotovitele, kteří při plnění svých pracovních povinností přicházejí do styku s osobními údaji, k zachovávání mlčenlivosti o nich, stejně jako o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

5. Zhotovitel je dále povinen v rozsahu podle předcházejícího odstavce zavázat i fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se zhotovitelem.

6. Objednatel je oprávněn provádět kontrolu dodržování závazků zhotovitele podle této smlouvy v souvislosti se zpracováním osobních údajů zhotovitelem v souladu se zákonem č.101/2000 Sb.

7. Pro provedení kontroly podle předcházejícího odstavce je zhotovitel povinen objednateli poskytnout potřebnou součinnost.

8. Pokud objednatel zjistí při kontrole nebo i jinak, že zhotovitel porušil povinnost stanovenou zhotoviteli zákonem č. 101/2000 Sb., vyzve jej k neprodlenému odstranění závadného stavu. Zhotovitel je povinen závadný stav neprodleně po výzvě odstranit.

9. Zhotovitel je povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů (dále jen „bezpečnostní opatření"). Tato povinnost platí i po ukončení zpracování osobních údajů. Přijatá bezpečnostní opatření je zhotovitel povinen dokumentovat, uplatňovat, kontrolovat a vyhodnocovat jejich dodržování.

10. Zhotovitel je povinen přijmout a uplatňovat komplex bezpečnostních opatření v oblasti personální, fyzické (objektové), administrativní a informační bezpečnosti v dostatečném rozsahu a kvalitě tak, aby nemohlo dojít ke zneužití osobních údajů.

11. Zhotovitel je povinen vymezit zejména:

a) role, oprávnění a odpovědnosti za zpracování osobních údajů v rámci organizační struktury zhotovitele, včetně pravidel přístupu osob k osobním údajům,
b) způsoby a pravidla pro vymáhání odpovědnosti za porušení povinnosti při zpracování osobních údajů,
c) pravidla kontroly dodržování povinností při zpracování osobních údajů, včetně stanovení periodicity kontrol.

12. Zhotovitel je povinen přijímat a uplatňovat bezpečnostní opatření, a to na základě analýzy rizik zneužití osobních údajů, týkající se minimálně:
a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje,
d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

13. Zhotovitel je povinen v rámci bezpečnostních opatření povinen dále minimálně:
a) zajistit, aby systémy pro automatizované zpracování osobních údajů používaly pouze oprávněné osoby,
b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizované zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a zabránit neoprávněnému přístupu k datovým nosičům.

14. Zhotovitel je dále povinen:
a) zajistit, aby aplikace nezpracovávala osobní údaje nad rámec nezbytný k dosažení účelu zpracovávání osobních údajů,
b) zaznamenávat operace s osobními údaji v dostatečném rozsahu nezbytném pro kontrolu a řízení nakládání s osobními údaji,
c) upravit pravidla pro vyřazení a likvidaci dokumentů a záznamových médií obsahujícími osobní údaje.

15. Osobní údaje budou uloženy na samostatném počítači mimo jakoukoliv síťovou dostupnost. Počítač a přenosová média s osobními údaji budou umístěna v uzamčené místnosti.

16. Použije-li zhotovitel ke zpracování osobních údajů podle této smlouvy subdodavatele, je povinen subdodavatele písemně smluvně zavázat k nakládání a ochraně osobních údajů v souladu se zákonem č. 101/2000 Sb. jako zpracovatele osobních údajů, a to nejméně v rozsahu ve kterém je zhotovitel zavázán k nakládání a k ochraně osobních údajů podle této smlouvy.

Čl. 15. 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 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:
   - dodání vadného předmětu plnění,
   - prodlení s plněním závazku vyplývajícího z této smlouvy po dobu delší než třicet (30) dní a nezjednání nápravy ani do patnácti (15) dní od doručení oznámení objednatele o prodlení s plněním závazku.

4. Smluvní strany se dohodly, že za podstatné porušení této smlouvy ze strany objednatele považují:
   - prodlení se zaplacením vyfakturované ceny díla (jeho části) delší než třicet (30) kalendářních dnů.

5. Porušení jakékoliv jiné povinnosti objednatele nebo zhotovitele, vyplývající z této smlouvy, je třeba splnit v dodatečné přiměřené lhůtě k tomu poskytnuté.

6. Odstoupením od této smlouvy nejsou dotčena ustanovení týkající se smluvních pokut a úroků z prodlení a stejně tak práva a povinnosti smluvních stran vzniklá do okamžiku účinnosti odstoupení od smlouvy.

Čl. 16. 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., občanským zákoníkem 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. Pokud jakýkoli závazek dle smlouvy nebo kterékoli ustanovení smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení.

3. Obě smluvní strany berou na vědomí, že tato smlouva včetně případných dodatků bude na základě plnění zákonné povinnosti objednatele uveřejněna na profilu zadavatele Plzeňský kraj, konkrétně na webové adrese https://ezak.cnpk.cz/vz00002536.

4. Tato smlouva je vyhotovena ve čtyřech (4) stejnopisech, z nichž každý má platnost originálu. Každá ze smluvních stran obdrží po dvou vyhotoveních.

5. Tuto smlouvu je možno platně měnit pouze na základě dohody smluvních stran, formou písemných a vzestupně číslovaných dodatků, podepsaných oběma smluvními stranami.

6. Tato smlouva nabývá platnosti i účinnosti dnem jejího podpisu oběma smluvními stranami.

7. Uzavření této smlouvy bylo v souladu s ustanovením § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů, schváleno usnesením Rady Plzeňského kraje č. 2571/14 ze dne 22.9.2014.

8. Nedílnou součástí této smlouvy jsou její přílohy:
   č. 1 – Technická specifikace předmětu díla dle Technické dokumentace objednatele /zadavatele/
   č. 2 - Technické řešení dle nabídky zhotovitele /uchazeče/
   č. 3 – Specifikace licencí softwarového řešení SIEM
   č. 4 - Časový harmonogram plnění předmětu smlouvy
   č. 5 – Rozklad ceny díla
   č. 6 – Licenční podmínky výrobce nabízené technologie

9. Smluvní strany prohlašují, že tuto smlouvu před jejím podpisem přečetly, zcela rozumí jejímu obsahu a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy svých oprávněných zástupců.

V Praze dne 13.11.2014

Za zhotovitele:

PODEPSÁNO

.....

Ing. Pavel Malínek
jednatel

V Plzni dne 23.10.2014

Za objednatele:

PODEPSÁNO

.....

Ivo Grüner
náměstek hejtmana

Příloha č. 1

Technická specifikace předmětu díla dle Technické dokumentace objednatele /zadavatele/

Příloha č. 1 zadávací dokumentace k veřejné zakázce „Centrální logování"

Technická dokumentace

Obsah technické části zadávací dokumentace

1 Předpoklady

Předmětem této veřejné zakázky je dodávka softwarového řešení systému centrálního logování Plzeňského kraje včetně veškerých potřebných licencí, jeho implementace na jeden či více virtuálních serverů zadavatele (formou instalace do doporučeného prostředí, nebo formou dodávky celé virtuální appliance), a následná podpora tohoto řešení.

Poptávané řešení musí zajistit bezpečné, úplné a nezpochybnitelné vyhodnocování a archivaci logů ICT prostředí Plzeňského kraje s důrazem na monitoring komunikace IS KÚPK s ISZR a na naplnění požadavků § 13 zákona č. 101/2000 Sb., v platném znění.

Účelem poptávaného řešení je zajistit (v tomto pořadí sestupně podle důležitosti pro zadavatele):

- garantované bezpečné uložení logů s řízeným přístupem a ochranou proti nedetekovanému podvrhu, modifikaci či smazání i administrátorem,
- centrální zpracování logů, jejich normalizaci, korelaci, grafickou interpretaci a archivaci a to včetně logů generovaných samotným řešením,
- zpětné dohledání událostí v čase přes více parametrů současně,
- snadný a uživatelsky přívětivý přístup k výstupům SIEM dle uživateli přidělených práv a rolí.

Poznámka zadavatele: *Poptávané řešení má zajišťovat komplexní správu logů a správu bezpečnostních informací a událostí. Tato funkcionalita je typicky označována jako SIEM (Security Information and Event Management). V některých případech výrobci oddělují funkcionalitu správy logů a používají odděleně pojmy SIEM a Log Management pro dva různé produkty. Většinou je však správa logů chápána jako podmnožina SIEM a takto pojem SIEM chápe i tento dokument. V tomto textu je proto označení „SIEM" používáno jako zkratka pro celé poptávané řešení, zahrnující veškeré požadované funkcionality.*

2 Popis stávajícího stavu

V současné době jsou auditní záznamy a události v jednotlivých informačních systémech a prvcích ICT infrastruktury Plzeňského kraje zaznamenávány a ukládány převážně odděleně, v nejednotné struktuře, s různou mírou sledovaného detailu a v různých typech úložišť. Tento stav v podstatě znemožňuje včasnou detekci a výrazně komplikuje zpětné dohledání jakékoli nestandardní události, ať už způsobené technickou závadou, chybou uživatele nebo úmyslným jednáním. Negarantované uložení auditních záznamů také snižuje jejich průkaznost. S nárůstem elektronizace procesů v posledních letech a především s příchodem základních registrů začíná být tento stav nevyhovující a je nutné jej urychleně řešit.

Tento stav potvrdila i „Analýza současného stavu systému řízení úřadu a návrhu realizace jeho úprav", kterou Plzeňský kraj zpracoval v r. 2013. Jako řešení bylo doporučeno zavedení jednotného systému centrálního logování a jeho napojení na vybrané významné informační systémy a infrastrukturu kraje tak, aby zajistil jednotnou úroveň a strukturu jednotlivých auditních záznamů, jejich vzájemné logické propojení a jejich bezpečné dlouhodobé uložení.

Vybrané auditní záznamy a události z prvků infrastruktury vnitřní sítě Krajského úřadu Plzeňského kraje se v současné době již sbírají a ukládají. Jedná se vesměs o běžné logy velkých nadnárodních výrobců HW či SW, které jsou v dobře známé standardizované struktuře (Microsoft, Cisco aj.). S významným rozšířením infrastruktury, souvisejícím s budováním Technologického centra kraje a regionální komunikační infrastruktury CamelNET však vzrostl i rozsah požadavků na tento typ logování. Tyto logy jsou aktuálně zabezpečeny pouze na fyzické úrovni jejich uložením na externí server, na který nemá odbor informatiky přístup s úrovní správce, aby byl umožněn nezávislý audit. Pro zpracování je využit nástroj EventLog Analyzer spol. ManageEngine.

Největší potřeba změny v oblasti logování je u aplikačních logů důležitých částí informačního systému Plzeňského kraje. Jde o agendy a aplikace, které byly identifikovány jako kritické pro provoz kraje, kde je prokazatelnost auditní stopy důležitá. Primárně se jedná o logování napojení agend na základní registry, nicméně jsou i další oblasti, kde je nezbytné garantovat prokazatelnost auditní stopy s možností analyzovat události napříč systémy a ukládat je v jednotné struktuře, nezávislé na dodavateli. Typicky se jedná o oběh účetních dokladů a další procesy interního schvalování. Seznam těchto aplikací je uveden dále v tomto dokumentu.

Záměrem Plzeňského kraje je implementovat standardy logování, které do budoucna sjednotí strukturu i obsah aplikačních logů stávajících informačních systémů a budou nutnou podmínkou při pořizování nových. První verze standardu logování byla zpracována v rámci již zmíněného projektu Analýzy. Zadavatel požaduje ověření a případné doplnění či revize standardů logování na základě jejich ověření v praxi.

3 Popis předmětu plnění

Součástí předmětu plnění je:

- zpracování podrobné implementační analýzy prostředí Plzeňského kraje pro potřeby implementace SIEM,
- dodávka licencí SIEM řešení, splňujícího požadavky zadavatele,
- implementace SIEM řešení včetně napojení vybraných informačních systémů,
- zaškolení administrátorů včetně zpracování školící dokumentace,
- zpracování provozní dokumentace (bezpečnostní dokumentace, příručka administrátorská, příručka uživatelská) a plánu obnovy,
- poskytování poimplementační technické podpory a údržby,
- konzultační podpora a Ostatní služby, objednávané ad hoc dle potřeb zadavatele.

3.1 Implementační analýza

Prvním krokem bude zpracování implementační analýzy, která upřesní postup implementace, především konkrétně stanoví typy a počty připojovaných log sources, zapojených do SIEM v rámci implementace, a to u prvků infrastrukturyi u jednotlivých agend a informačních systémů.

Dále implementační analýza stanoví doporučenou strukturu oprávnění a řízení přístupových práv a procesů tak, aby byly naplněny požadavky legislativy, především zákona o ochraně osobních údajů a zákona o základních registrech, a dále požadavek zadavatele na garantovanou neměnnost (nemožnost nedetekované změny) vybraných logů.

Řešení bude napojené jednak na logy prvků infrastruktury, jednak tak i na aplikační logy informačních systémů. V níže uvedených tabulkách je uveden výčet IS/ICT pro potřeby určení vhodného SIEM řešení a stanovení odhadu implementace.

3.1.1 Logování prvků infrastruktury

Pro zpracování logů infrastruktury je v rámci dodávky požadováno připojení níže uvedených zařízení. Součástí implementační analýzy bude stanovení profilu pro každý napojovaný log source, včetně určení vhodné úrovně detailu logování pro dané typy zařízení, relevantní pro jeho roli v infrastruktuře Plzeňského kraje, a včetně potřebných korelací mezi jednotlivými logy (infrastrukturními i aplikačními).

Zadavatel požaduje, aby součástí nabídky byly předpřipravené šablony pro běžně používané typy prvků infrastruktury („základní šablony") minimálně pro produkty Cisco a Microsoft, uvedené v tabulce dále v této kapitole, které na základě znalosti daného prvku určí doporučované log sources a relevantně nastaví typ či závažnost sledovaných událostí (odfiltrování DEBUG událostí, nepodstatných chyb aj.). Základní šablony musí zvládnout minimálně zpracování strukturu logů a filtrování důležitých událostí (zdraví systémů, dostupnost služeb aj.). Základní šablony budou dodavatelem SIEM následně aktualizovány jako součást podpory. *(poznámka zadavatele: Infrastruktura zadavatele je postavena převážně na technologiích Cisco a Microsoft ; s ohledem na ochranu stávajících investic – veřejných prostředků – zadavatele se touto zakázkou navazuje na stávající prostředí, tj. prvky infrastruktury zadavatele)*

Zadavatel předpokládá využití základních šablon při stanovení profilů a odmítá poskytnout součinnost na činnosti, které evidentně vedou k analýze a vytváření základních šablon.

Počty významných zařízení, které zadavatel požaduje implementovat do SIEM jsou uvedeny v následující tabulce. Vždy je uveden výrobce a produkt či rodina produktů, poznámka s upřesněním a dále jednak počty kusů, které zadavatel provozuje celkem (na které musí být SIEM řešení dimenzováno), jednak počty kusů, které zadavatel požaduje napojit v rámci implementace.

Počty jsou nastaveny rámcově pro stanovení pracnosti, přesný počet a typ logů může implementační analýza mírně upřesnit.

Počet zařízení celkem / napojených	Výrobce	Produkt	Poznámka (verze, typy, významné komponenty)
100/50	Cisco	L2/L3 switche, routery, firewally, VPN koncentrátory	Aktuálně řady 12xx, 13xx, 26xx, 29xx, 35xx, 36xx, 45xx, 55xx, 65xx, 76xx
200/50	Microsoft	Windows server	2003 – 2012 V rolích: IIS, file server, print server, terminal server, radius (název dle verze), ftp, sharepoint services
20/15	Microsoft	Active Directory	2008R2, 2012
10/5	Microsoft	Exchange	2003, 2010, 2013
3/3	Symantec	Antivirus - IPS	End Protection Suite
50/20	Microsoft	SQL Server	2000-2012
20/5	GNU/Linux	Debian, CentOS, RedHat	Všechny podstatné logy: syslog, posfix, dns, ntp, ... na jednom stroji ZEN NLB
2/2	Microsoft	ISA, TMG	ISA 2006, TMG 2010
20/12	Microsoft	Certification Authority	2008R2, 2012
4/4	Symantec	BackupExec	2013
4/4	VEEAM	VEEAM Backup	Poslední verze
1000/800	TightVNC	VNC Server	VNC na každé pracovní stanici (logy budou pro zpracování v SIEM centrálně stahovány na jedno místo)
4/2	Microsoft	WSUS	Update services, poslední verze
20/20	VMWare	VSphere ESX	5.x
10/5	Microsoft	DHCP Server	viz MS Windows

Intenzita přibývání logů, generovaný těmito systémy v pracovní době úřadu, je zadavatelem odhadován v řádu tisíců událostí za sekundu, špičkově to může být odhadem až 20.000 událostí za sekundu. Počet „efektivních" událostí, vybraných z toho pro další zpracování, však bude jen malé procento (odhadem do 5% událostí, tj. řádově stovky událostí za sekundu). Navrhované řešení jako celek musí zvládnout takové množství událostí přijmout, provést jejich filtraci na efektivní události a ty následně zpracovávat ON-LINE.

Také počet zdrojových logů (log sources) může být odhadem minimálně 3000 podle toho, jak nabízené řešení definuje jeden zdrojový log (např. v případě, že se počítá jeden log source na každou IP adresu bez ohledu na to, že události byly konsolidovány do jednoho logu). Nabízené řešení jako celek musí opět zvládnout takový počet log sources zpracovat on-line. Zadavatel předpokládá, že v rámci plnění bude první filtrace nastavena už na straně zdroje všude tam, kde je to vhodné a technicky možné (např. Custom Event Log v novějších verzích Microsoft Windows). Požaduje však, aby zůstala zachována kompletní identifikace zdrojového zařízení, tj. kvůli licenčním omezením nesmí při zpracování dojít ke ztrátě informace.

Je na uchazeči, jakým způsobem se s těmito hodnotami událostí a zdrojů vypořádá. Zadavatel bude akceptovat řešení složené z více částí, kdy např. prvotní zpracování logů včetně jejich bezpečného uložení a první filtrace bude zajištěno jiným systémem, než následné zpracování těchto vybraných událostí. Podstatné je, aby u dodaného řešení jako celku byly zajištěny všechny zadavatelem požadované vlastnosti.Logování agend a informačních systémů.

Pro zpracování aplikačních logů je požadováno zpracování logů z minimálně 25 IS/Agend. Tyto logy budou většinově ve standardizovaném formátu, a to buď v textových souborech (1 nebo více souborů na IS/Agendu), nebo v SQL databázích a budou zpracovávány dávkově. V rámci implementace se předpokládá napojení minimálně 50 log sources.

Následující tabulka uvádí předpokládaný seznam logů IS/Agend, jejichž napojení do SIEM uchazeč zahrne do nabídkové ceny, přitom zohlední to, že přesný počet a typ logů může implementační analýza upřesnit v limitech uvedených výše.

Tam, kde je to v poznámce uvedeno, bude struktura logu odpovídat standardizovanému aplikačnímu logu úřadu, míra detailu záznamů se však pro jednotlivé IS/aplikace může i tak lišit.

Priorita zapojení do SIEM	Výrobce	Produkt	Způsob načtení logů	Průměrný počet logů za den	Poznámka
1	Marbes Consulting s.r.o.	Agendio (SaP, ESS)	Soubor	2000	Standardizovaný formát
1	Pilscom s.r.o.	AthenA	Soubor	8000	Standardizovaný formát
3	Foresta SG a.s.	Dotace LH	Soubor	100	Individuální formát
3	Plzeňský kraj	eDotace	Soubor	5000	Individuální formát
1	Marbes Consulting s.r.o.	ePUSA lokální	Soubor	5000	Individuální formát
2	YAMACO Software	Evidence dopravních agend	Soubor	500	Individuální formát
3	Marbes Consulting s.r.o.	Evidence majetku (ENO)	Soubor	2000	Individuální formát
1	Marbes Consulting s.r.o.	Evidence Organizační Struktury (EOS)	Soubor	5000	Standardizovaný formát

Priorita zapojení do SIEM	Výrobce	Produkt	Způsob načtení logů	Průměrný počet logů za den	Poznámka
1	Marbes Consulting s.r.o.	Evidence smluvních partner (ESP)	Soubor	3000	Standardizovaný formát
3	T-Mapy s.r.o.	Evidence vodohospodářskýc h aktivit (EVA)	Soubor	500	Individuální formát
1	Marbes Consulting s.r.o.	Hledáček	Soubor	10000	Standardizovaný formát
1	Marbes Consulting s.r.o.	Kevis	Soubor	3000	Standardizovaný formát
3	MP Orga, spol. s r.o.	MPorga VSP	Soubor	50	Individuální formát
3	Kvasar, s.r.o.	Ovzduší	Soubor	200	Individuální formát
1	SOFTECH s.r.o.	Památky	Soubor	1000	Standardizovaný formát
1	Marbes Consulting s.r.o.	Registr nemovitostí (REN)	Soubor	1000	Standardizovaný formát
3	Pilscom s.r.o.	Virtuos (Galatea)	Soubor	10000	Standardizovaný formát
1	Plzeňský kraj	Helpdesk	Soubor	10000	Standardizovaný formát
1	ICZ a.s.	Dlouhodobé úložiště digitálních dokumentů (ICZ DESA)	Soubor	5000 *)	Individuální formát
1	ICZ a.s.	Pracovní úložiště (ICZ ADU - Alfresco)	Soubor	1000 *)	Individuální formát
1	oXy Online s.r.o.	Portál pro zřizované organizace	Soubor	5000 *)	Standardizovaný formát

*) jedná se o systémy, které se v současné době implementují a v době realizace zakázky budou čerstvě nasazené, počet denních logů je jen odhad po zahájení jejich plného využívání.

Hlavním úkolem zde bude analýza logů jednotlivých aplikací a jejich správná korelace jednak mezi sebou, jednak proti logům z prvků infrastruktury.

3.1.2 Standard logování

Plzeňský kraj připravuje standard logování, který bude požadovat po nových aplikacích a na který chce do budoucna postupně převést i významnější stávající aplikace. Standard je v této chvíli v první pracovní verzi, jeho dopracování bude jedním z výstupů tohoto projektu. Zadavatel zároveň požaduje, aby výstupní logy, které bude SIEM řešení generovat, tento standard již dodržovaly.

3.2 Specifikace předmětu plnění

- Dodávka SIEM řešení, které bude provozováno jako software (program nebo virtuální appliance) ve virtuálním prostředí VMware VSphere; jiná varianta není přípustná
- Zpracování před implementační analýzy, která musí popsat a konkretizovat implementaci řešení. Po odsouhlasení této analýzy zadavatelem bude možno provést vlastní implementaci. Součástí analýzy musí být **zejména**:
    - Integrace s EOS (Evidence organizační struktury, produkt spol. Marbes) pro řízení oprávněných uživatelů; práva a role uživatele budou však již řízena v rámci SIEM
    - Integrace s EOS a SSO (Single sign-on řešení Plzeňského kraje, ověřující uživatele z více IdM systémů) úřadu pro doplňování a aktualizace detailních informací o uživatelích z organizační struktury Plzeňského kraje po každém přihlášení do SIEM
    - Analýza zdrojů logů včetně podpory kódování (Win1250, UTF-8, atd.)
    - Návrhy korelací
    - Návrhy výstupů, přehledů a akcí prováděných na základě pravidel v SIEM
    - Návrh na zajištění prokazatelnosti autenticity logu (jeho pravosti a že nebyl modifikován)
    - Logování aktivit a uživatelských akcí v SIEM (za použití standardizované struktury aplikačního logu úřadu)
    - Zajištění kontroly konzistence aplikačního logu dle pravidel. Nelze vyloučit, že popis aktivity uživatele bude víceřádkový nebo bude obsahovat znaky uvozovek nebo středníku atd. V rámci analýzy je třeba navrhnout postup řešení importu takovéhoto log záznamu.
    - Popis naplnění požadavků zák. č. 101/2000Sb. v aktuálním znění včetně potřebné dokumentace k SIEM.
- Implementace SIEM
- Zpracování dokumentace implementace viz kap. 6 tohoto dokumentu

3.3 Funkční specifikace řešení

Řešení:

- Řešení musí být realizováno formou instalace řešení do virtuálního serveru na platformě VMware VSphere ESX 5.x.
- Musí zahrnovat všechny komponenty pro Log Management, Event management, Korelace, příjem a sběr logů, centrální správu a reporting, a to včetně vlastních logů

- Musí umožňovat výkon pro současné zpracování 20.000 netříděných událostí za sekundu a z toho 1000 efektivních událostí za sekundu ze zrojových logů, uvedených v tabulkách v kap. 3.1 tohoto dokumentu a s dávkovým zpracováním logů (zejména aplikačních). Hodnoty událostí za sekundu jsou zde chápány jako maximální špičkový počet zpracovaných událostí. Efektivní události jsou chápány jako události po provedení jejich prvotní filtrace (viz závěr kap. 3.1.1) .
- V případě, že uchazeč bude nabízené řešení skládat z více částí, případně část řešení hodlá řešit vlastním vývojem, musí toto v nabídce výslovně uvést a výsledek jako celek musí splňovat všechny požadavky zadavatele.
- Musí obsahovat zařízení na centrální zpracování logů, jejich normalizaci, korelaci, grafickou interpretaci a archivaci.
- Musí umožňovat definovat retenční politiku archivovaných logů pro celé řešení i každý log source zvlášť
- Musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky a to včetně uvedení dalších funkcionalit, které jsou součástí dodávané licence.
-
- Zadavatel požaduje, aby dodané licence řešení buď neomezovaly maximální počet log sources (neomezené množství napojených systémů), nebo aby řešení zvládlo licenčně pokrýt všechny log sources, uvedené v kap. 3.1.
- Nesmí dopustit, aby došlo k jakékoli ztrátě logovaných informací. V případě, že při výkonové špičce z jakýchkoli důvodů řešení nebude schopno zpracovat příchozí množství událostí, musí zajistit, aby události byly uloženy do fronty a zpracovány po opadnutí špičky.
- Musí mít kompletní uživatelské rozhraní SIEM dostupné z webového browseru. Musí být jednotné, nevyžadovat více různých podpůrných technologií, pluginů nebo tlustého klienta.
- Musí podporovat načítání log souborů, kde tyto soubory budou mít stanovenu strukturu a význam dat
- Musí podporovat načítání logů z databáze (zejména MS SQL server), kde tyto soubory budou mít stanovenu strukturu a význam dat
- Musí podporovat minimálně protokoly pro příjem a sběr logů
    - syslog
    - snmp
    - scp
    - http
    - ftp
    - sftp
    - nfs
    - cifs
    - netflow
- musí umožňovat definici vlastního atributu (číselného i textového) v událostech, do kterého je automaticky doplňována aktuální hodnota z externího zdroje (např. definice nového atributu, který bude ukládat aktuální reputaci IP adresy z vybrané databáze).
    - Vlastní atribut musí být použitelný pro filtraci, drilldown i definice korelací napříč celým SIEMem

  - Externím zdrojem dat, ze kterého jsou automaticky doplňovány hodnoty, musí být minimálně dostupný následujícími způsoby
    - Strukturovaný soubor dostupný pomocí
      - cifs
      - http
      - ftp
      - nfs
      - scp
      - sftp
    - LDAP
    - Databáze
      - MS SQL
      - MySQL
      - Oracle
- musí poskytovat plně grafické rozhraní pro definici všech typů vlastních dashboardů a reportů. Definice dashboardů a reportů musí být možné exportovat a importovat.
- Dashboardy musí poskytovat stavbu z minimálně následujících typů grafů
  - Počet událostí v závislosti na čase
  - Koláčový graf
  - Tabulkový výpis
  - Sloupcový graf
  - Graf aktivních síťových prvků
  - Geolokační graf
- Grafy v dashboardech musí umožňovat výběr určité své části pro rychlé vymezení oblasti vyhledávaných událostí.
- Musí umožňovat definici vlastních parsovacích pravidel pro nestandardní formáty logů pomocí grafického rozhraní SIEM.
- Řešení bude dodáno jako virtuální appliance (popř. kombinace více virtuálních appliances).
- Musí umět vyhodnocovat i vlastní provozní logy.
- Veškerá konfigurace a definice zdrojů logů musí probíhat z grafického rozhraní SIEM.
- Musí umět pomocí standardizovaných protokolů procházet síťové prvky a mapovat jejich provázanost. Následně musí umět takto získanou mapu provázaností spojit s událostmi.
- Musí umožňovat archivovat originální logy po volně definovanou dobu. Archivované logy budou komprimovány a bude chráněna jejich integrita. Archiv může být uložen na externím diskovém úložišti a zároveň musí být možné s archivy přímo pracovat bez nutnosti dalších mezikroků, jako je např. zpětný import do SIEM.
- Musí umožnit ukládání kontrolních součtů (hash) ukládaných logů odděleně na garantované úložiště pracující na principu WORM tak, aby bylo možné garantovat neměnnost logu od jeho uložení, a to bezodkladně po uložení logu. Zadavatel disponuje zařízením Hitachi HCAP300**, které hodlá pro tento účel využít. Vzhledem k ceně úložné kapacity tohoto zařízení bude použito pouze pro ukládání hash záznamů, vlastní logy budou uloženy jinde. Nestačí však

prosté vygenerování a uložení, řešení musí s takto uloženými hash záznamy umět i nadále aktivně pracovat a kontrolovat proti nim uložené logy.

*** Garantované úložiště Hitachi HCAP300 zadavatel pořídil v rámci nadlimitní VZ s názvem „Dlouhodobé ukládání digitálních dokumentů", ev.č. VZ* ***ve Věstníku veřejných zakázek je 343391.***

- Musí obsahovat funkcionalitu, která umožní přiřazovat (automaticky nebo manuálně) události k řešení jednotlivým osobám a v případě jejich nevyřešení po stanovenou dobu jejich eskalaci na další osobu.
- Na jakoukoliv událost musí být možné navázat automatickou akci. Minimálně musí být k dispozici následující akce
    - Zaslání emailu
    - Vizuální upozornění doplněné zvukem (např. pro dohledové centrum)
    - Založení tiketu do interního case tracking systému
    - Spuštění externího skriptu
- Musí umět zpracovávat výsledky skenu zranitelností minimálně ze systémů pro automatizované ověřování zranitelností aplikací, minimálně ze systému Nessus Vulnerability Scanner od výrobce Tenable Network Security.
- Systém správy uživatelských oprávnění musí být založený na volně definovatelných rolích. Definice role musí umožnit oddělit oprávnění podle libovolného průniku minimálně následujících podmínek
    - SIEM musí být integrován s EOS pro řízení autentizace oprávněných uživatelů
    - Práva pro vykonávání konkrétních akcí a správy různých logických oblastí, minimálně v rozsahu
        - Reportingu
        - Dashboardů
        - Uživatelských oprávnění
        - Case tracking systému
        - Systémového nastavení
        - Zdrojů logů
    - Oprávnění k přístupu k datům z definovaných síťových rozsahů. Roli musí být možné přiřadit viditelnost pouze určité podsítě nebo více podsítí.
    - Oprávnění k přístupu k datům z definovaných zdrojů logů. Roli musí být možné přiřadit viditelnost událostí pouze z vybraných zařízení.
- **Definice korelací** musí umožnovat zahrnovat následující podmínky
    - Posloupnost událostí (striktně musí být definováno, v jakém pořadí musí události dorazit, aby bylo uplatněno korelační pravidlo).
    - Musí být možné navzájem korelovat události vzniklé z logů s událostmi vzniklých z netflow
    - Základní stavební prvky korelace, musí být možné mezi sebou libovolně provazovat
        - Podmínky v rámci jedné události (např. kombinace IP adresy a uživatele z určité skupiny v Active Directory)
        - Doplnění informací o uživatelích z EOS a SSO

- Podmínky mezi více událostmi (např. v definovaném časovém okně nastane událost A a B)
- Limity na počet událostí (definuje po kolika výskytech událostí je podmínka splněna)

- Výsledkem nalezené korelace může být standardní událost v rámci SIEM, která může být použita v dalších korelacích.

Základní porovnatelné údaje o nabízeném řešení vyplní uchazeč do níže uvedené tabulky, která je uvedena v samostatné příloze této zadávací dokumentace. Není povoleno variantní řešení. Uchazeč nahradí text ve <špičatých závorkách>.

V tabulce uchazeči uvedou pouze základní shrnutí plus odkážou na samostatnou kapitolu, ve které stručně a výstižně vysvětlí funkcionalitu a/nebo přístup uchazeče v dané oblasti. Při zpracování této části nabídky budou uchazeči dbát na požadavky zadavatele v zadávací dokumentaci a uvádět odkazy na ně, neměla by obsahovat obecné vlastnosti řešení, není-li to výslovně zadavatelem v některém bodě požadováno.

Oblast	Vyjádření uchazeče k nabídce
Platforma – operační systém	<podporovaný, příp. dodávaný (pokud bude dodána celá virtuální appliance)> <očekávaný rozsah kapitoly: 1 odstavec>
Sběr logů – nativní formát logů	<doplnit> <očekávaný rozsah kapitoly: min 1 odstavec, max 1 strana>
Možnosti rozšiřitelnosti pro sběr dalších nespecifikovaných logů (vlastnosti řešení nad rámec zadání)	<doplnit > <očekávaný rozsah kapitoly: max 1 strana>
Používá agenty: ano/ne	<ano/ne, případně doplnit> <očekávaný rozsah kapitoly: 1 odstavec až 2 strany>
Ochrana logů a jejich integrity	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Uložení logů	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Možnosti filtrování	<doplnit> <očekávaný rozsah kapitoly: 1-4 strany>
Možnosti korelace	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Možnosti reportingu	<doplnit> <očekávaný rozsah kapitoly: 1-4 strany>
Provedení – technické požadavky	<doplnit> <očekávaný rozsah kapitoly: 2-4 strany>
Škálovatelnost	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>

Oblast	Vyjádření uchazeče k nabídce
Možnosti zálohování - offline úložiště logů	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Licencování s ohledem na požadavky zadavatele	<doplnit především s důrazem na licenční omezení – maximální počet instalací/CPU/RAM atd.> <očekávaný rozsah kapitoly: 1-2 strany>
Napojení na reputační systém	<doplnit> <očekávaný rozsah kapitoly: max 1 strana>
Data enrichment	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Řízení přístupových práv až na úroveň jednotlivých zdrojů logů	<doplnit> <očekávaný rozsah kapitoly: 1-2 strany>
Seznam log sources, pro které budou dodány předpřipravené šablony	<uvést rámcový výčet, případně odkaz na přílohu> < rozsah kapitoly není omezen>
Způsob řešení prvotní filtrace efektivních událostí z logů prvků infrastruktury	<zde stručně shrnout, plus podrobněji uvést v samostatné příloze vč. schématu architektury s vyznačenými log sources, toky dat, uložením logů do vysokokapacitního úložiště, hash záznamů do garantovaného úložiště s omezenou kapacitou, přenosových protokolů> <očekávaný rozsah kapitoly: 3-5 stran>

Poznámka zadavatele: V tabulce uvedený očekávaný rozsah vyjádření uchazeče má doporučující charakter a jeho nedodržení není důvodem pro vyřazení nabídky.

3.4 Technická specifikace řešení

Nabízené řešení musí být provozováno jako virtuální server. Zadavatel vlastní prostředí VMware. Konfigurace virtuálního prostředí Plzeňského kraje je uvedena v kapitole **Chyba! Nenalezen zdroj odkazů.**.

Základní definovaná pravidla pro standardizované logy

- Informace budou uloženy v textovém souboru nebo v tabulce databáze SQL serveru. Struktura souboru či tabulky bude jednotná, včetně názvů polí.
- Textové soubory budou uloženy ve sdíleném adresáři s denní periodicitou zpětně. Jednotlivý textový soubor bude pojmenován datem dne, jehož data obsahuje (tedy datem předešlého dne ve struktuře RRRRMMDD) s doplňkem určujícím IS/agendu, např. 20130725_spis.txt.
- Každý jeden záznam bude uložen na samostatném řádku. Před importem je povinností provést kontrolu konzistence.
- Informace, které nejsou v aplikaci vedeny, jsou v exportovaném logu vedeny jako prázdný řetězec, tj. počet polí se nemění.

- Položky typu datum a čas budou uvedeny ve tvaru rok-měsíc-den hod:min:sec.milisec (např. "2013-06-12 04:01:47.125").
- Vybrané údaje budou číselníkové hodnoty, pro následné strojové zpracování.
- Identifikátory, které budou číselníkové, doplní SIEM řešení o jejich lidsky čitelné popisy (data enrichment funkcionalita), které budou platné pro daný okamžik. Typický příklad je indentifikace uživatele (username) a k němu doplněné plné jméno a aktuálně platné zařazení v organizační struktuře Plzeňského kraje. Napojení číselníků bude součástí plnění, přístup k číselníkům bude typicky zajištěn přes definované aplikační rozhraní (WS/SOAP), výjimečně mohou být předány formou statické tabulky, dále udržované v prostředí SIEM.

3.5 Bezpečnostní specifikace řešení

Standardní požadavky na dodávané řešení:

- autentizace přístupu uživatelů z MS AD
- autorizace a řízení přidělování oprávnění na úrovni jednotlivých sestav a log sources
- bezpečně uložený auditní log vybraných akcí uživatelů v systému („logování sebe sama“) bez možnosti tento auditní log nedetekovaně modifikovat nebo smazat – jde např. o logování dočasného omezení filtrovaných událostí podle kap. 3.1.1 nebo jiných akcí, které by umožňovaly administrátorovi zabránit logování vybraných událostí
- naplnění požadavků na řízení přístupu k osobním údajům, které mohou být součástí logů, dle zákona č. 101/2000 Sb., v platném znění
- pro garanci nemodifikovatelnosti a nesmazatelnosti vybraných bezpečnostně kritických logů zadavatel předpokládá využití kombinace garantované úložiště Hitachi HCP300 a využití PKI (důvěryhodné elektronické značky a časová razítka) – nabízené řešení musí být schopno tyto prostředky využít

4 Harmonogram řešení

Uchazeč navrhne etapy a milníky minimálně v následující úrovni detailu (udávat v týdnech od zahájení projektu):

- analýza, zpracování detailního implementačního plánu
- implementace řešení do prostředí KÚPK (včetně případné etapizace)
- školení
- akceptace, předání systému a následný ostrý provoz

5 Požadavky na školení

Školení pro administrátory řešení bude realizovat uchazeč včetně přípravy školících materiálů tohoto školení. Budou proškoleny dvě skupiny administrátorů v maximálním počtu 10 účastníků na jedno školení. Prostory pro školení zajistí zadavatel. Administrátoři musí být na základě informací ze školení schopni spravovat SIEM, včetně napojování nových zdrojů logů ve standardním formátu a mít dostatek podkladů pro proškolení běžných uživatelů k užívání SIEM.

Součástí dodávky bude školicí materiál včetně e-learningového kurzu základů práce se SIEM řešením pro uživatele v českém jazyce, který bude připraven pro potřeby Plzeňského kraje a bude obsahovat specifika této konkrétní implementace (viz školicí materiály v kapitole 6).

6 Požadavky na dokumentaci

Uchazeč po úspěšné implementaci dodá jako součást řešení podrobnou dokumentaci dodávaného řešení včetně kompletního popisu nastavení a konfigurace daného řešení tak, aby jej bylo možné nadále udržovat, zpravovat a rozvíjet pracovníky KÚPK nebo jiným subjektem než je subjekt uchazeče. Nezbytnou podmínkou dodávky je pak manuál popisující krok za krokem uživatelské funkce nabízeného řešení s důrazem na detailní popis práce s dashboardem, parsovací pravidla a způsob jejich nastavení a vizualizace výsledků, pravidla pro přidělování přístupových práv a rolí v SIEM s jednoznačnou definicí jejich pravomocí a omezení z pohledu bezpečnosti, prokazatelnosti a zpětné dohledatelnosti činností dané role.

Zadavatel požaduje dodání dokumentace v následující logické struktuře:

- prováděcí dokumentace (implementační analýza)
- provozní dokumentace
    - bezpečnostní dokumentace (může být součástí administrátorské příručky)
    - administrátorská příručka
    - uživatelská příručka
- plány obnovy
- školicí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro implementaci řešení, bude zpracována v tomto minimálním rozsahu:

- popis procesu nasazení SIEM vč. zpřesněného harmonogramu
- požadavky na součinnost v průběhu implementace a pilotního provozu
- návrh školení administrátorů
- návrh akceptačních testů
- popis údržby

Popis plánů obnovy bude zpracován v míře podrobnosti, použitelné pro zařazení do celkového plánu obnovy (Disaster Recovery Plan) KÚPK. Součástí této dokumentace musí být popis instalace a konfigurace řešení v takovém rozsahu a detailu, který umožní znovu implementovat celé řešení v nově nainstalovaném čistém prostředí bez pomoci dodavatele.

Školicí materiál bude dodán ve formátu MS Office tak, aby umožňoval následnou editaci zadavatelem. E-learningový kurz bude připraven ve struktuře, vhodné pro import do nástroje Moodle. Míra detailu školicích materiálů bude taková, aby zadavatel byl s jejich pomocí do budoucna sám schopen proškolit další osoby.

Školicí materiál a e-learningový kurz musí kromě obecné práce s nástrojem obsahovat i specifické informace o konkrétní implementaci a konfiguraci řešení.

Veškerá dokumentace musí splňovat požadavky na vizuální identitu Integrovaného operačního programu.

7 Podpora provozu řešení

Zhotovitel se smluvně zaváže udržovat a podporovat řešení v dalších letech, zadavatel hodlá uzavřít smlouvu na poskytování podpory na dobu neurčitou. podpora Na údržbu a podporu řešení bude s vybraným uchazečem uzavřena smlouva o technické podpoře na dobu neurčitou. Součástí smlouvy bude dodávka nových verzí produktu, oprava chyb, informační linka a garance úrovně služeb (SLA) při servisním zásahu.

Vybraný uchazeč bude v rámci této smlouvy povinen zajistit, že veškeré funkce řešení, popsané v této zadávací dokumentaci a dodané spolu s dílem a dokumentací díla budou odpovídat obecně platným právním předpisům ČR a platným standardům, které musí podle zákona nebo podle této zadávací dokumentace dodržovat.

Technická podpora a údržba zahrne především:

- právo zákazníka na nové verze produktu a zapracování požadovaných legislativních změn
    - poskytování update a upgrade produktu dle potřeby vzniklé požadavky zadavatele či samostatnou, nevynucenou inovační činností zhotovitele
    - v rámci placené údržby bude dodavatel zajišťovat i aktuálnost dodané dokumentace
- bezplatná služba Hot-line formou telefonické podpory pro zadavatele pro řešení technických problémů, poradenství a konzultace,
- služba Helpdesk pro zadavatele pro hlášení závad jednotlivých kategorií, poradenství a konzultace.

Výše uvedené práce budou zahrnuty v rámci ročního paušálu, který bude zadavatel hradit.

Dále budou součástí další práce, které budou zadavatelem objednávány podle potřeby a hrazeny podle skutečně odebraného množství v maximálním rozsahu 120 člověkohodin ročně:

- instalace a implementace update a upgrade řešení v prostředí zadavatele
    - bude prováděna na základě objednávky zadavatele , odsouhlasených mezi oběma smluvními stranami, nejpozději však k datu, po kterém by byla ohrožena bezpečnost řešení, jeho plná funkcionalita nebo jeho soulad s legislativou
- asistence při přenosu řešení do nového prostředí (operační systém, databázový server)
    - v případě, že výrobce přestane podporovat některou část prostředí, ve kterém je řešení provozováno, dodavatel v rámci podpory provede přenos řešení do nového prostředí, připraveného zadavatelem s respektováním produktové řady komponent prostředí (vyšší verze stejných nebo srovnatelných edicí Microsoft Windows Server a Microsoft SQL Server)
- objednané konzultace při řešení provozních problémů, řešená návštěvou konzultanta dodavatele na místě nebo jeho vzdáleným připojením k řešení

Uchazeč v rámci nabídky stanoví cenu za 1 člověkohodinu těchto služeb, kterou se rozumí 1 člověkohodina odborníka schopného samostatně analyzovat požadavek objednatele a fakticky provést požadovanou službu.

Technická podpora a údržba bude poskytována od převzetí řešení do rutinního provozu a jeho akceptace bez výhrad, a to po celou dobu účinnosti Smlouvy o servisní podpoře. Další informace o rozsahu technické podpory a údržby jsou uvedeny dále.

Pohotovost podpory je poskytována pracovní době, tj. v pracovních dnech od 8:00 do 16:00 (režim 5x8). Provozní doba služby bude v pracovních dnech v této době garantována.

Požadovaná úroveň služeb (SLA)

Priorita	Reakční doba	Doba vyřešení požadavku od převzetí
Vysoká	4 pracovní hodiny	7 pracovních dnů
Střední	8 pracovních hodin	15 pracovních dnů
Nízká	24 pracovních hodin	30 pracovních dnů

Problémem (závadou) se rozumí takový stav systému, který neumožňuje provádět jednotlivé funkce systému, nebo nejsou splněny podmínky stanovené v dokumentaci, nebo je ohrožena bezpečnost uložených dat. Závady jsou klasifikovány dle jejich závažnosti a provozních podmínek na tři kategorie důležitosti:

- Vysoká = závady vylučující užívání software nebo jeho důležité a ucelené části (tj. problémy, zabraňující provozu systému), provoz systému je zastaven.
- Střední = závady způsobující problémy při užívání a provozování informačního systému nebo jeho části, ale umožňující provoz systému. Provoz systému je omezen, ale činnosti mohou pokračovat určitou dobu náhradním způsobem.

- Nízká = provoz systému je závadou ovlivněn, ale může pokračovat jiným způsobem, např. organizačními opatřeními.

Požadavek na servisní zásah může být uplatněn zadavatelem na systému Helpdesk.

Po nahlášení a následném zpětném potvrzení požadavku kontaktuje řešitel případu zadavatele a dohodne podrobnosti a způsob řešení. Závady způsobené chybou aplikace jsou zahrnuty v poplatku za technickou podporu a údržbu.

8 Podmínky akceptace

Podmínkou akceptace je správný a ověřený provoz řešení včetně správného a úplného vyhodnocování požadovaných logů v SIEM a předání veškeré dokumentace. Podrobnosti akceptačního procesu jsou uvedeny v návrhu smlouvy o dílo.

9 Popis prostředí zadavatele

Pro implementaci řešení vítězného uchazeče bude připraveno prostředí v dále definovaném rozsahu. Podrobnosti jsou uvedené v této kapitole.

9.1 Zajištění potřebného hardware

Hardware bude zajišťovat v definovaném rozsahu zadavatel který má . k realizaci řešení připraveno následující prostředí:

1) umístění serverů ve virtuální prostředí datového centra (ESX vSphere 5. x)

   Parametry virtuálního prostředí, přidělené pro řešení, budou podrobněji specifikovány v analytické části dodávky.

   Virtuální servery budou hostovány na společném virtuálním hostu, dimenzovaném pro až 50 virtuálních serverů. Virtuální host má 2 fyzické procesory s výkonem minimálně SPECint_rate2006: 490 bodů, SPECfp_rate2006: 350 bodů

2) umístění systémů a dat ve sdíleném diskovém úložišti NAS datového centra, určeného pro cca 100 serverů.
   Počáteční nastavení pro celé prostředí (součet na všech serverech a podíl na SQL Serverech) vyčleněného v NAS pro realizaci řešení:

   a. 1 TB na poli se výkonem max. 6000 IOPs, minimálně 240 IOPs na diskový oddíl.
   b. 5 TB na poli s výkonem max. 2000 IOPs, minimálně 80 IOPs na diskový oddíl.
   c. 0,5 TB na garantovaném úložišti Hitachi HCP300

   Zadavatel v případě potřeby zajistí potřebnou vyšší kapacitu úložiště.

3) Zajištění bezpečnosti serverů na úrovni síťového provozu (firewall).

V případě nutnosti se do budoucna předpokládá navýšení těchto kapacit po oboustranné dohodě.

9.2 Zajištění potřebného software

9.2.1 Serverová část

Obsahem této poptávky není dodání základního software, který bude zajišťovat v definovaném rozsahu zadavatel.

Zadavatel k realizaci řešení je připraven v současné době zajistit:

1) Operační systém – může být zajištěn potřebný počet virtuálních strojů s operačním systémem Windows 2012 nebo 2008 R2 v edici Data Center
2) Databáze – přístup k jednomu serveru MS SQL 2012 nebo 2008 R2 v edici Standard či Workgroup. Bude poskytnut administrátorský přístup k databázím (vytvoření databáze zajistí zadavatel podle specifikace dodavatele – přímý přístup k operačnímu systému stroje s MS SQL nebude umožněn)
3) Anti-X ochranu, řešenou na úrovni datového centra pro každý server

Na všechen výše uvedený software pod body 1-3 bude zadavatel na své náklady zajišťovat podporu, tj. právo na nové verze a update minimálně z pohledu bezpečnosti po celou dobu provozování řešení. Doba upgrade na vyšší verze bude stanovena po oboustranné dohodě, nejzazší doba upgrade na úrovni operačního systému nebo databáze souvisí s ukončením podpory bezpečnostních update výrobce k dané verzi.

Zadavatel preferuje, aby řešení bylo implementováno do výše popsaného prostředí. V případě, že řešení uchazeče bude vyžadovat pořízení dalšího software kromě vlastního poptávaného řešení a výše uvedeného základního software (např. dodá kompletní připravenou virtuální appliance), zahrne do nabídky pořízení veškerých potřebných licencí, implementaci, důkladné zaškolení všech správců (v rozsahu potřebném pro zajištění provozu) a následnou údržbu ve stejném rozsahu (tj. právo na nové verze a bezpečnostní update) na celé řešení a po celou dobu, po kterou bude poskytována podpora nabízeného řešení. V tom případě uchazeč do nabídky uvede veškerý takový software včetně jeho výrobce a licenční politiky, zahrne pořizovací náklady na pořízení licencí a na následnou údržbu do nabídkové ceny a software zahrne do smlouvy o poskytování technické podpory.

Řešení musí být ošetřeno proti náhlému výpadku serveru. Systém musí být schopen se v takovém případě automaticky vrátit ke konzistentnímu stavu. Software musí přistupovat ke konzistentním datům, sledovat výpadek, vrátit se automaticky v čase (na úrovni záloh i transakcí).

9.2.2 Klientská část

Uživatelské rozhraní dlouhodobého úložiště musí být provozovatelné minimálně na tomto prostředí:

1) Windows 7 a vyšší, podpora alespoň jedné aktivně podporované rozšířené distribuce GNU/Linux
2) Internet Explorer 9 a vyšší, Firefox 20 a vyšší

9.3 Dostupnost infrastruktury pro dodavatele

Zadavatel zajistí celkovou bezpečnost infrastruktury, na níž bude řešení provozováno.

Přístup dodavatele k infrastruktuře bude zajištěn

- fyzicky – běžně v pracovní době, po dohodě lze výjimečně domluvit rozšířený režim (noci, víkendy), pokud to projekt bude vyžadovat
- vzdálený přístup přes VPN na servery, vyhrazené na projekt
- oprávnění
    - přístupová práva k serverům, vyhrazeným pro projekt (v odůvodněných případech na úrovni administrátora)
    - admin přístup k databázi (nikoli k serveru)

9.4 Součinnost dodavatele

Dodavatel musí postavit nabídku bez předpokladu, že přenese některé práce na zadavatele. Zadavatel si vyhrazuje právo limitovat součinnost svých pracovníků jen na úkoly nezbytně nutné, které není možné spravedlivě požadovat po dodavateli.

Příloha č. 2

Technické řešení informačního systému z nabídky uchazeče

1 Funkční požadavky

1.1 Shrnutí funkčních požadavků

Následující kapitola shrnuje rozsah a způsob naplnění požadavků zadavatele specifikovaných v technické dokumentaci kapitole 3.3.

Oblast	Vyjádření uchazeče k nabídce
Platforma – operační systém	Platforma bude dodávaná formou appliance, do virtuálního prostředí VMware ESXi v.5.x ve formátu ovf. Celkem budou dodány 2 appliance – 1 pro collector, 1 pro centrální aplikační server - AlienVault OSSIM.
Sběr logů – nativní formát logů	Sběr logů je realizován prostřednictvím agentů nebo bezagentským přístupem (preferovaný způsob sběru dat). Logy jsou v normalizované podobě uloženy v databázi událostí platformy OSSIM, v surové podobě jsou uloženy na collector serveru. Detailnější popis je uveden v kapitole Architektura řešení.
Možnosti rozšiřitelnosti pro sběr dalších nespecifikovaných logů (vlastnosti řešení nad rámec zadání)	Zpracování dalších logů, které nejsou standardizovány je možné libovolně přidat do stávajícího řešení. Kvantita a specifika zpracování nestandardních logů budou upřesněny v rámci analýzy. V rámci dodávky předpokládáme dodání standardních parserů OSSIM pro standardní systémové aplikace (viz strana 5 technické dokumentace), pro ostatní aplikace bude vytvořeno v rámci dodávky 11 parserů (1 parser pro tzv. standardizovaný formát a 10 dalších parserů pro ostatní zakázkové aplikace – viz strana 6 a 7 technické dokumentace).
Používá agenty: ano/ne	Ano, platforma využívá agenty (primárně OSSEC), ale obecně preferuje bezagentský přístup.
Ochrana logů a jejich integrity	Ochrana logů je realizována prostřednictvím nastavení databáze pro uložení logu, bezpečnost a přístupy jsou standardizovány databázovou specifikací. Dále na úrovni operačního systému. Integrita logů je dále dodatečně zabezpečena pomocí kontrolních součtů.
Uložení logů	Normalizované logy jsou uloženy v EDB - Event database a na úrovni collector jsou surová data uložena ve formě textových logů.
Možnosti filtrování	Filtrování je řešeno na 3 úrovních: 3. Primárně na úrovni zdrojového systému 4. Sekundárně na úrovni collector – předpokládáme, že zde budou ukládána data pro další forenzi (log management). Zároveň zde bude ukládáno až 95% záznamů. Filtrování je řešeno na úrovni standardizovaných šablon. 5. Terciálně budou data uložena a vyhodnocena v jádru SIEM (AlienVault OSSIM). Filtrování logů je realizováno prostřednictvím přednastavených šablon, nebo na míru vyvinutích filtrových modelů.
Možnosti korelace	Pokročilá korelace je plně podporovaná s možností nastavení v kontrolním panelu. Nastavení probíhá prostředky webového rozhraní.

Oblast	Vyjádření uchazeče k nabídce
Možnosti reportingu	Reporting je realizován prostřednictvím integrovaného reportingového modulu, kde lze nastavovat typy reportu, jejích obsah, formát apod. Dále je také možně vytvářet jakékoliv individuální reporty na základě dotazů do DB.
Provedení – technické požadavky	Viz kapitola Architektura řešení.
Škálovatelnost	Systém je škálovatelný primárně na úrovni log collectorů (sekundární úroveň filtrace), na centrální aplikační server je vertikálně škálovatelný. Pro horizontální škálování by bylo nutné licenčně povýšit stávající verzi AlienVault SIEM. S ohledem na předpokládaný počet monitorovaných celků, počet událostí a předpokládanou úroveň filtrace (cca 5% událostí je zpracováno centrálním aplikačním serverem).
Možnosti zálohování - offline úložiště logů	Zálohování je podporováno na několika úrovních: • na úrovni collectorů – surová data jsou ukládána na lokálních discích, respektive DAS. • na úrovní centrální databáze • na úrovni hypervizoru – primárně pro zálohu binárních dat a konfiguračních nastavení.
Licencování s ohledem na požadavky zadavatele	Aplikační server AlienVault OSSIM je licencován podle licence GPLv2. Collector servery obsahují sw, který je licencován pod různými licencemi – primárně Apache nebo LGPL. Součástí dodávky, primárně collectorů jsou výrazné kustomizace.
Napojení na reputační systém	Platforma OSSIM umožnuje připojení reputační systém. Primárně se jedná o tzv. OTX – neboli Open Threat Exchange. Přístup k tomuto zdroj, využití jím poskytovaných dat a jejich prezentace je standardní součástí jádra řešení.
Data enrichment	Data enrichment probíhá na několika úrovních. Primárně na úrovni collector serveru (základní obohacení událostí) sekundárně na úrovni aplikačního serveru, kde dochází k výraznějšímu obohacení a o to i na základě dat z externích zdrojů.
Řízení přístupových práv až na úroveň jednotlivých zdrojů logů	Řízení prav je plně podporováno a integrováno prostřednictvím grafického rozhraní administrace. Práva lze nastavovat nejen na jednotlivé úrovně menu (vymezení funkčních vlastností), ale i na úrovni jednotlivých sledovaných asset/sensorů. Lze tak například vytvořit uživatele s právy auditora (omezení práv k menu), který má oprávnění nahlížet na události z unix celků (omezení na úrovni asset).
Seznam log sources, pro které budou dodány předpřipravené šablony	Předpřipravené šablony vytvořené výrobcem jádra SIEM – AlienVault OSSIM jsou připraveny pro všechny standardní systémy, které jsou uvedeny na straně 5 technické dokumentace ZD.

Oblast	Vyjádření uchazeče k nabídce
Způsob řešení prvotní filtrace efektivních událostí z logů prvků infrastruktury	Filtrace událostí je řešena na třech úrovních. • První úroveň filtrace probíhá přímo na zdrojových celcích buď na úrovni syslog klienta, konfigurace logování na zdrojovém celku, event log apod. Na této úrovni by mělo být nastaveno odesílání událostí, které jsou využitelné pro log management, případně další forenzi. Nicméně předpokládáme, že i zde nebude u několika systémů možné nastavit optimální úroveň filtrace. • Druhotná úroveň filtrace probíhá na úrovni collector serveru (vstupní rozhraní SIEM řešení), zde dochází také k prvotnímu obohacení. Zde dojde k redukci událostí na cca 5% z původního objemu. Zredukovaná data (efektivní data) jsou odeslána do SIEM AlienVault OSSIM. Další vstupní data jsou buď uložena k připojené DAS (využití pro forenzi) nebo jsou zahozena (typicky se týká „nepotřebných" záznamů, které není možné odstranit na úrovni vstupních celků). • Terciální filtrace probíhá přímo na centrálním aplikačním serveru (AlienVault OSSIM).

2 Architektura řešení

2.1 Úvod

Infrastruktura řešení CGI SIEM bude postavena na dodavatelem upravené platformě OSSIM od výrobce AlienVault. Základní platforma OSSIM AlienVault je hodnocena společností Gartner jako „visionaries", a tedy lze s jistotou říct, že se jedná o jedno z nejlepších SIEM řešení pro budoucnost. Řešení je zároveň doplněno o vysoce škálovatelnou komponentu pro sekundární filtraci událostí (collector). Jedná se o v praxi několikrát osvědčenou komponentu, která kombinuje Balabit Syslog-ng (společnost CGI CEE je Silver Partner společnosti Balabit) a vybrané části ElasticSearch stack. Obě součásti (OSSIM a Collector) jsou navíc doplněny o přednastavená pravidla a konfigurační nastavení, která vycházejí ze znalostí společnosti z rozsáhlých SIEM implementací (např. ČS).

2.2 Popis

Integrovaná platforma CGI SIEM tvoří modulární subsystémy, které tvoří celek odpovědný za veškeré zpracování, detekci a prezentaci událostí/logů napříč celou organizací. Jedná se primárně o následující subsystémy:

- Collector – řešení pro sekundární filtraci dat (primární filtrace dat se realizuje na úrovni zdrojového celku). Je tvořeno syslog-ng a elasticsearch logstash, s tím, že pro filtraci syslog zdrojů předpokládáme užití syslog-ng.
- Aplikačním serverem AlienVault OSSIM – je zodpovědný za terciální filtraci, korelaci událostí a prezentaci událost a incident management v rámci webového rozhraní.

2.3 Systémové procesy

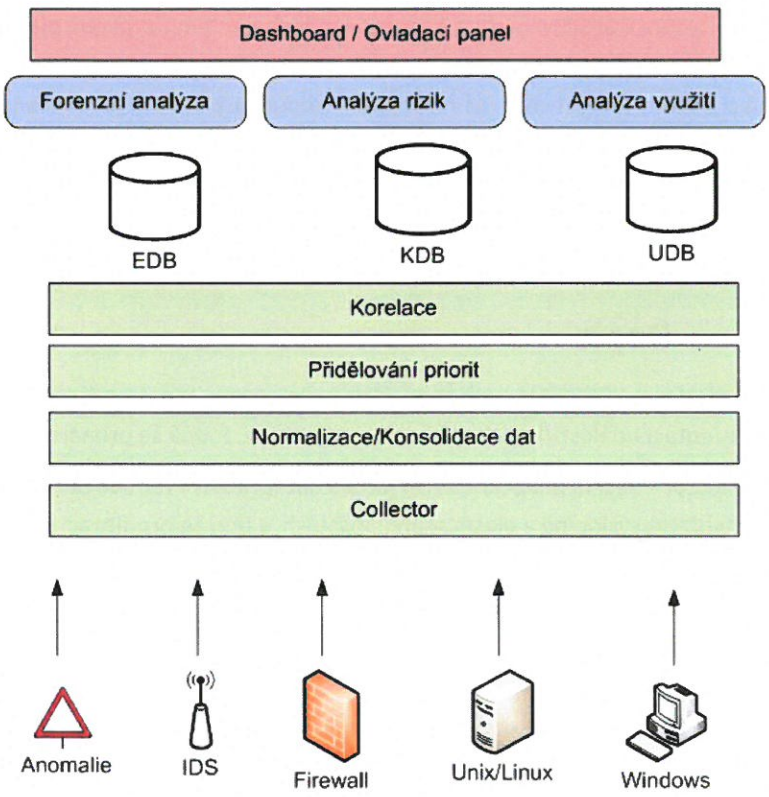
Systémové procesy řešení OSSIM jsou rozděleny do dvou základních úrovní:

- **Preprocesing** – realizovaný na zdrojových systémech (první úroveň filtrace) a na collector serveru (IDS, šablonové detektory, detektory pro anomální chování, Firewally a další).
- **Post-procesing – realizovaný prostřednictvím centralizované konzole** (Korelace, prioritizace, analýza rizik).

2.4 Architektura systému

Následující schéma znázorňuje architekturu systému na základě toku dat:

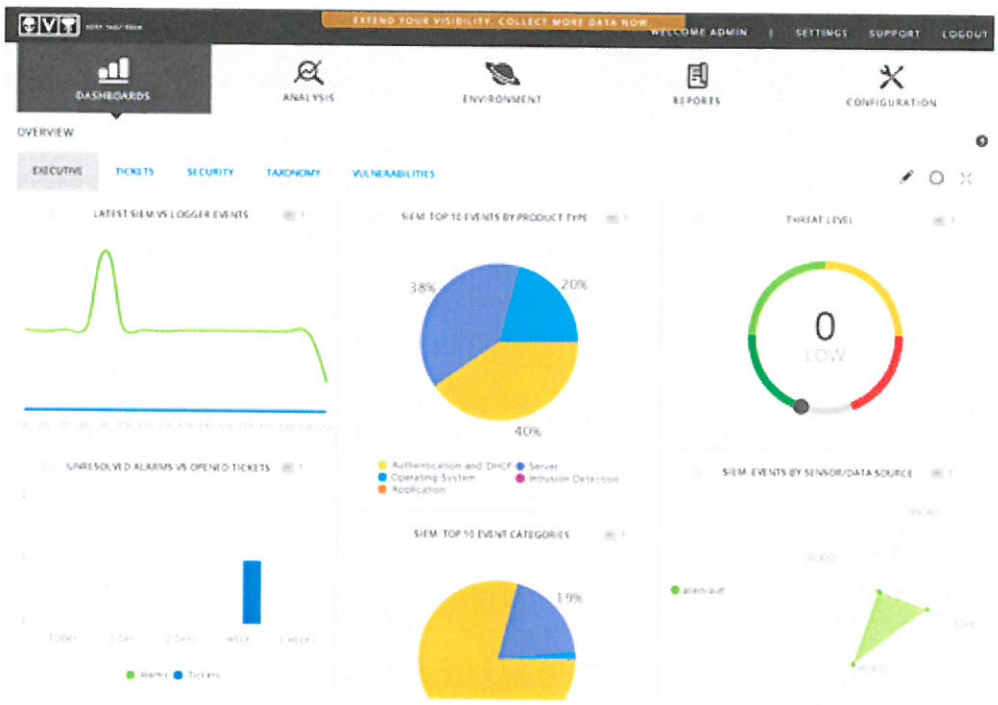
- Události jsou generovány a zpracovány detektory, na základě identifikace anomálie systému, nebo na základě předem nastavené šablony.
- Dále, pomocí collector, (a prostřednictvím široké škály podporovaných protokolů) jsou sbírány a přepracovány jednotlivé události.
- Události jsou následovně zpracovány parserem a ukládány do database událostí. (Event Database). Parser se též stará o priortizaci alarmů na základě předem nastavených bezpečnostních politik a informací uložených v systému. V případě vzniku alarmu dochází k jeho odeslání a upozornění na kontrolním panelu.
- Takto upravené události jsou následovně zpracovány v korelačních vláknech kde je jejich stav průběžně aktualizován a vyhodnocován.
- Následovně jsou všechny takto zpracované události znázorněny v kontrolním panelu, kde uživatel má možnost je dále upravovat, kumulovat, graficky znázorňovat, nebo případně nastavovat další aktivity jako jsou alarmy, notifikace, apod.



Obrázek 1 Logická architektura řešení

Platforma AlienVault OSSIM využívá interní integrované databáze, kde jsou události uloženy do:

- **EDB (event database)** neboli databáze událostí, je největší integrovaná databáze. Obsahuje veškeré raw události které byly sesbíraný detektory.
- **KDB (knowledge or framework database)** obsahuje konfigurační informace všech systémových parametru, nastavení a napojení na externí moduly a definice bezpečnostních politik.
- **UDB (profile database)** ukládá veškerá nastavení profilového monitoru který se stará o dohled a analýzu chování uživatelů napříč systémy. (databáze behaviorálních šablon)



Obrázek 2 AlienVault OSSIM Dashboard

2.4.1 ŘEŠENÍ CGI SIEM

CGI SIEM platforma je postavena na výše představené architektuře, která předpokládá užití dvou subsystémů - aplikačního serveru AlienVault OSSIM a CGI Collectoru.

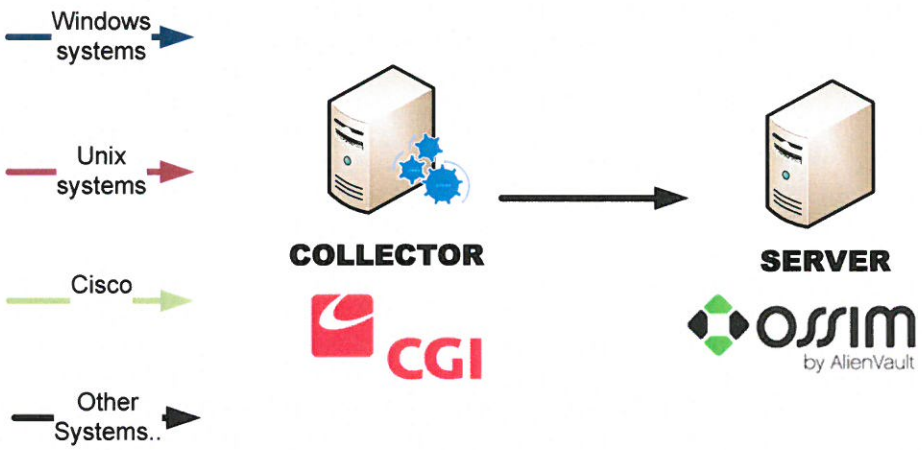
Následující schéma znázorňuje vlastní architekturu dle serverů, pro CGI SIEM. Zahrnuje vstupní systémy, collector server a centrální aplikační server.

- **Vstupní systémy**
  - Předpokládáme, že u monitorovaných systémů dojde k nastavení úrovně logování a to sice tak, aby byly do řešení SIEM odesílány primárně tzv. efektivní události. V případě, že nebude možné upravit úroveň filtrace, předpokládáme další filtraci na úrovni collector. S ohledem na uvedené zdroje a v souvislosti s požadavkem zadavatele na minimalizaci součinnosti předpokládáme bezagentský sběr dat. Vlastní řešení však umožňuje i agentský sběr dat přes agenty OSSEC (není součástí nabídky). Předpokládáme, že na vstupních systémech dojde k výrazné redukci událostí a to cca na úroveň 50%.

- Z pohledu přenosového kanálu předpokládáme následující kanály:
  - syslog, windows eventlog, db komunikaci (jdbc) a souborový přenos (SMB)

- **Collector server**
  - Sekundární komponenta filtrace a obohacení událostí. S ohledem na uvedené systémy (viz technická dokumentace ZD) předpokládáme primárně využití Balabit Syslog-ng OSE, která bude filtrovat, přeposílat a zároveň i ukládat vybrané syslog události. Pro události z windows eventlog, relačních databází a souborových zdrojů předpokládáme užití kustomizované verze ElasticSearch Logstash (CGI rozšíření standardních plugin), která bude zajišťovat obdobnou funkčnost jako syslog-ng. Lokálně uložené, pravidelně rotované logy budou s ohledem na objem uloženy na připojeném DAS, kde budou pro účely prokázání integrity jednotlivé log soubory opatřeny kontrolním součtem (kontrolní součty jsou uloženy v separátním souboru).

- **Centrální aplikační server**
  - Na tomto aplikační serveru jsou instalovány a provozovány komponenty zodpovědné za korelaci událostí, GUI, incident management, centrální databáze SIEM. Tato komponenta by v souladu s požadavky zadavatele měla zpracovávat cca 5% z původních až 20000 událostí za vteřinu. Aplikační server obsahuje moduly moduly: Server, Web Framework, Database, identity Management, Vulnerability Management.



Obrázek 3 Architektura řešení CGI SIEM

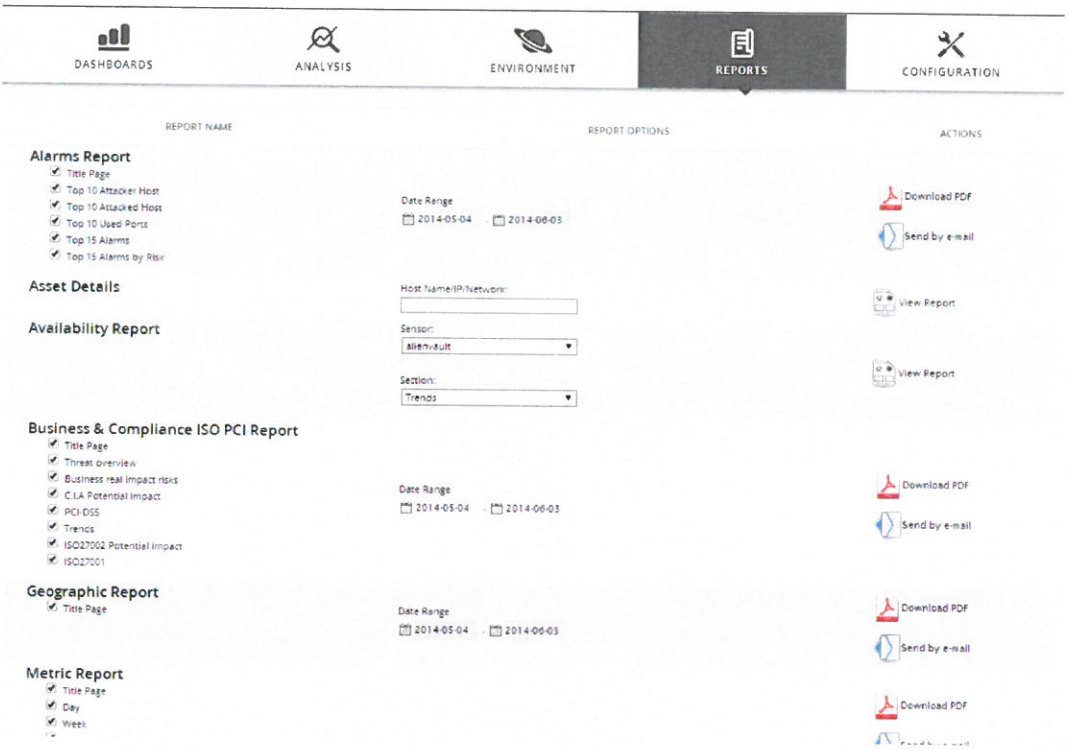
Obě komponenty řešení (collector i aplikační server OSSIM) jsou dodány jako softwarové appliance ve formátu OVF.

2.4.2 REPORTING

Reporting je realizován prostřednictvím integrovaného reporting modulu, kde lze libovolně nastavit typy reportů, jejích formát, velikost, časová razítka apod. Dále je možné určit přístupová práva pro jednotlivé reporty, nebo je možné též v určitém čase reporty posílat na e-mailové adresy.

Základní kustomizaci reportů je možné provádět přímo ve webovém rozhraní SIEM pomocí interaktivního průvodce. Složitější reporty je možné vytvořit např. prostřednictvím JasperReports Server (není součástní nabídky) nad databází OSSIM.

Součástí nabídky je kromě standardně nabízených reportů OSSIM i vytvoření cca 10 základních reportů.



Obrázek 4 AlienVault OSSIM Reporting

2.4.3 ŠKÁLOVATELNOST

Základní komponenty platformy OSSIM budou realizovány jako:

- **Server**
- **Collector**

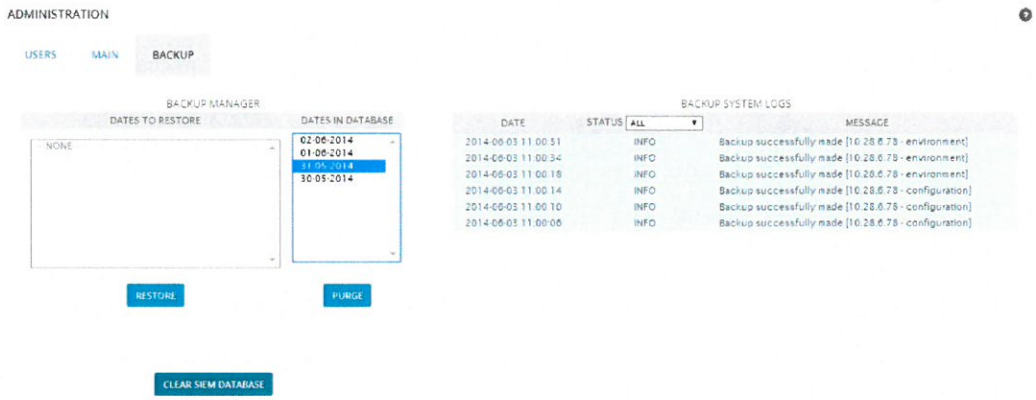
Obě komponenty jsou škálovatelné vertikálně (bez licenčních omezení), komponenta collector je bez licenčních dopadů škálovatelná horizontálně (v rámci implementace a instalace předpokládáme instalace jedné instance). Centrální aplikační server je škálovatelný i horizontálně na úrovni jednotlivých modulů, nicméně pouze v rámci Enterprise verzí AlienVault USM (není součástí nabídky). Případný licenční upgrade na verzi enterprise je možný.

Přesný návrh pro hardware sizing bude vypracován na základě analýzy.

2.4.4 ZÁLOHOVÁNÍ

Zálohování je podporováno na úrovní databáze nebo na úrovni virtuálního operačního systému standardizovanými produkty pro zálohovaní ve VMware.

Další metodu zálohování nabízí samotná centrální konzole, kde lze nastavit jak jednotlivé zálohy, tak i možnost jejích obnovy. Níže uvedený obrázek ilustruje GUI rozhraní pro zálohování.



Obrázek 5 Zálohování

Zároveň předpokládáme zálohování vybraných konfiguračních a binárních souborů, které budou uloženy v definovaných lokalitách (adresáře/svazky).

Konkrétní scénáře záloh budou realizovány na základě analýzy.

2.4.5 PŘÍSTUPOVÁ PRÁVA

Přístupová práva lze ve webovém rozhraní SIEM definovat tzv. per účet. Pro jednotlivé účty lze definovat privilegia na úrovni funkcí (položky menu) a zároveň i per asset/sensor. Díky tomu lze vytvořit např. i účty s omezenými právy pro vybraný monitorovaný celek (např. readonly účet pro Auditory UNIX platforem). Dále lze definovat i superadministrátorské účty. Definice uživatelských účtů probíhá ve webovém rozhraní SIEM.

Kromě interní uživatelské databáze je možné využít i integrace s LDAP (Active Directory).

2.4.6 ŠABLONY PRO STANDARDIZOVANÉ SYSTÉMY

Řešení bude dodáno včetně šablon po standardizované systémy i specializované systémy. Výrobce aplikačního serveru SIEM (AlienVault) standardně podporuje veškeré uvedené systémy s výjimkou Veam Backup a TightVNC. Pro tyto dva systémy budou CGI připraveny šablony zahrnující základní normalizaci dat nutných pro realizaci základní korelačních pravidel (viz kapitola 2.5). Úroveň podpory včetně předpokládaného a v nabídce zahrnutého způsobu čtení logů je uvedena v níže uvedené tabulce. Parsery a jejich šablony jsou vendorem (AlienVault) testovány pro definované verze operačních systémů, databází a systémových aplikací. V případě, že zadavatelem poskytnutá verze systému je v jiné verzi je možné, že může dojít k ovlivnění úrovně parsing. Nepředpokládáme, že by v rámci dodávky mělo dojít k výrazné modifikaci těchto standardních parserů (maximálně v rozsahu minoritních úprav a s výjimkou workshop na kterých dojde k předání informací o možné kustomizaci právě na příkladu standardně dodávaného parseru).

Název systému	Způsob čtení logu	Podpora OSSIM
Cisco L2/L3 switche, routery, firewally, VPN koncentrátory	cisco-acs	Podporováno
Windows server	wmi-security logger-srv2008, wmi-monitor	Podporováno
Active Directory	wmi-securitylogger	Podporováno

Exchange	wmi-monitor	Podporováno
Antivirus – IPS	symantec-epm	Podporováno
SQL Server	wmi-systemlogger	Podporováno
GNU/Linux	syslog-ng	Podporováno
Microsoft ISA, TMG	wmi-monitor	Podporováno
Microsoft Certification Authority	wmi-monitor	Podporováno
Symantec BackupExec	symantec-epm	Podporováno
VEEAM Backup	Soubor	Kustomizace CGI
TightVNC VNC Server	Soubor	Kustomizace CGI
Microsoft WSUS	wmi-monitor	Podporováno
VMWare VSphere ESX	VMWare vandyke-vshell	Podporováno
Microsoft DHCP Server	wmi-monitor	Podporováno

Pro specializované systémy bude vytvořeno 11 specializovaných šablon pro parsing. Těchto jedenáct šablon zahrnuje jednu šablonu pro tzv. standardizovaný formát logů a 10 šablon pro individuální formát logů. S ohledem na popis uvedený v technické dokumentaci tedy předpokládáme, že pro standardizovaný formát bude možné bez dalších změn využít jeden parser

Název systému	Způsob čtení logu	Formát
Agendio (SaP, ESS)	Soubor	Standardizovaný
AthenA	Soubor	Standardizovaný
Dotace LH	Soubor	Individuální
eDotace	Soubor	Individuální
ePUSA lokální	Soubor	Individuální
Evidence dopravních agend	Soubor	Individuální
Evidence majetku	Soubor	Individuální
Evidence Organizační Struktury (EOS)	Soubor	Standardizovaný
Evidence smluvních partnerů (ESP)	Soubor	Standardizovaný
Evidence vodohospodářských aktivit (EVA)	Soubor	Individuální
Hledáček	Soubor	Standardizovaný
Kevis	Soubor	Standardizovaný
MPorga VSP	Soubor	Individuální
Ovzduší	Soubor	Individuální
Památky	Soubor	Standardizovaný
Registr nemovitostí (REN)	Soubor	Standardizovaný

Virtuos (Galatea)	Soubor	Standardizovaný
Helpdesk	Soubor	Standardizovaný
Dlouhodobé úložiště digitálních dokumentů (ICZ DESA)	Soubor	Individuální
Pracovní úložiště (ICZ ADU - Alfresco)	Soubor	Individuální
Portál pro zřizované organizace	Soubor	Standardizovaný

2.5 Korelační pravidla

Součástí dodávky je také vytvoření nebo úprava korelačních pravidel vytvářejících tzv. alarmy (někdy též označované jako alert). Přesná specifikace pravidel bude součástí iniciální analytické fáze, nicméně již dnes na základě našich zkušeností přepokládáme, že dojde k vytvoření do 20 typů korelačních pravidel (tento počet by měl být dle našich zkušeností dostačující).

Ostatní pravidla by měl být schopen zadavatel vytvářet samostatně po absolvování školení a hands-on workshop, které jsou součástí dodávky řešení. Vytvoření dalších pravidel (nad rámec cca 20 uvedených) není součástí dodávky SIEM řešení.

Příloha č. 3

Specifikace licencí softwarového řešení SIEM

Podmínky užívání software CGI SIEM

I.
Definice pojmů:

Autorský zákon: je zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů ve znění pozdějších předpisů.

Licenční smlouva: je tato licenční smlouva uzavřená postupem upraveným v čl. III této licenční smlouvy mezi CGI IT Czech Republic a Registrovaným uživatelem.

CGI IT: je společnost CGI IT Czech Republic s.r..o., se sídlem Praha 6, Na Okraji 335/42, IČ: 624 12 388, společnost zapsána v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka: 34304.

Registrovaný uživatel: Plzeňský kraj

Program: je počítačový program CGI SIEM, který je autorských dílem chráněným autorskými právy, které vykonává společnost Logica podle příslušných ustanovení Autorského zákona.

Uživatel: je osoba, která vyjádřila souhlas s těmito podmínkami užívání software CGI SIEM

II.
Účel Licenční smlouvy

Účelem této Licenční smlouvy je poskytnout Registrovaným uživatelům oprávnění k užití Programu, který byl vytvořen společností CGI IT pro Plzeňský kraj. Souhlas s užitím Programu uděluje touto Licenční smlouvou společnost CGI IT, a to prostřednictvím této smlouvy.

III.
Uzavření Licenční smlouvy

K uzavření této Licenční smlouvy mezi společností CGI IT a Registrovaným uživatelem dochází v souladu s ustanovením § 46 odst. 5 Autorského zákona momentem instalace Programu Registrovaným uživatelem z webových stránek Národní knihovny, a to za podmínek uvedených v této Licenční smlouvě. Registrovaný uživatel instalací Programu souhlasí, že bude touto Licenční smlouvou vázán.

IV.
Licenční oprávnění

CGI IT okamžikem uzavření této Licenční smlouvy dle předcházejícího článku uděluje Registrovanému uživateli nevýhradní licenci k užívání Programu dle následující specifikace:

- Licence je poskytnuta pro území Plzeňského kraje;

- Licence je poskytnutá na dobu trvání majetkových práv k Programu;
- Licence je poskytnuta pouze pro osobní účely Registrovaného uživatele. Užívaní Programu pro účely, které jsou přímo či nepřímo obchodní, není dovoleno;
- Licence je poskytnutá bez množstevního omezení;
- Registrovaný uživatel nemůže oprávnění tvořící součást této licence, a to ani zčásti, poskytnout třetí osobě, bez předcházejícího písemného souhlasu společnosti CGI IT. Registrovaný uživatel je povinen Program odpovídajícím způsobem zajistit proti jakémukoli využití třetí stranou, ke kterému nebyl udělen předcházející písemný souhlas společnosti CGI IT;
- Registrovaný uživatel není bez předcházejícího písemného souhlasu společnosti CGI IT oprávněn rozmnožovat, překládat, zpracovávat, upravovat, spájet s jinými počítačovými programy či jinak upravit nebo měnit Program, dále není oprávněn rozmnožovat kód Programu nebo překládat jeho formu. Ustanovení Autorského zákona týkající se omezení rozsahu práv autora k počítačovému programu, které není možné dohodou smluvních stran vyloučit, nejsou tímto dotčena;
- Licence poskytnutá Registrovanému uživateli na základě této Licenční smlouvy se vztahuje rovněž na aktualizované verze Programu dodané společností CGI IT v rámci upgrade nebo update;
- Registrovaný uživatel není povinen poskytnutou Licenci využít.

V.
Záruky a odpovědnost

V případě porušení ustanovení této Licenční smlouvy Registrovaným uživatelem, si společnost CGI IT vyhrazuje právo požadovat od Registrovaného uživatele odpovídající nápravu, kterou je např. zdržení se jednání, odstranění vzniklého stavu, poskytnutí omluvy, provedení opravy či doplnění, zaplacení náhrady škody, jakož i požadovat jiné nápravy takového stavu vyplývající z platných ustanovení Autorského zákona, zákona č. 513/1991 Sb. Obchodní zákoník, zákona č. 40/1964 Sb. Občanský zákoník, zákona č. 143/2001 Sb. Zákon o ochraně hospodářské soutěže, zákon č. 40/2009 Sb. Trestní zákoník a dalších souvisejících právních norem České republiky.

VI.
Rozhodné právo

Licenční smlouva se řídí právními předpisy České republiky, zejména ustanoveními Autorského zákona a zákona č. 513/1991 Sb. Obchodní zákoník.

VII.
Doba platnosti, ukončení Licenční smlouvy

Licenční smlouva je uzavřena na dobu trvání majetkových práv k Programu. Smrtí nebo zánikem Registrovaného uživatele Licenční smlouva zaniká, práva a povinnosti z této Licenční smlouvy nepřecházejí na právní nástupce.

CGI IT je oprávněna od této Licenční smlouvy odstoupit v případě, dojde-li k jejímu podstatnému porušení, zejména k neoprávněnému užití Programu v rozporu s touto Licenční smlouvou.

Příloha č. 4

Časový harmonogram plnění předmětu smlouvy

ID	Etapa	Trvání v týdnech
E1	Analýza a zpracování implementačního plánu	5 týdnů
E2	Implementace řešení do prostředí KÚPK	E1 + 13 týdnů
E3	Školení	E2 + 1 týden
E4	Akceptace, předání systému a následný ostrý provoz	E3 + 1 týden

Příloha č. 5

Rozklad ceny díla

Plnění	Cena v Kč bez DPH
Platforma OSSIM	0,--
CGI Collector	900.000,--
Implementační práce	700.000,--
CELKEM	**1,600.000,--**