Smlouva o dodávce nástroje SIEM včetně funkcionality pro audit logů

Smluvní strany

KSP Computer & Services, s. r. o.
se sídlem Nad Strání 109/46, 180 00 Praha 8
IČO: 27875849
DIČ: CZ27875849
Bank. spojení:xxxxxxxxxxxxxxx, č. ú.: xxxxxxxxxxxxxxxxxxx

zastoupený Petrem Kašparovským, jednatelem

dále jen „**Dodavatel**“

a

Centrum pro regionální rozvoj České republiky
příspěvková organizace
se sídlem U Nákladového nádraží 3144/4, 130 00 Praha 3
IČO: 04095316
DIČ: CZ04095316
Bank. spojení: xxxxxxxxxxxxxxxx,xxxxxxxxxxxxxxxxxxx

jehož jménem jedná Ing. Zdeněk Vašák, generální ředitel
dále jen „**Objednatel**“

vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto smlouvou vázány se ve smyslu ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**“), dohodly níže uvedeného dne, měsíce a roku na následujícím znění Smlouvy o dodávce nástroje SIEM včetně funkcionality pro audit logů (dále jen „**Smlouva**“):

1. Účel a předmět Smlouvy

1.1. Účelem, pro který je tato Smlouva mezi smluvními stranami uzavírána, je potřeba Objednatele získat nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, vyhovujícího a splňujícího požadavky Objednatele a požadavky platné legislativy, zejména dle vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, v platném znění, zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění, a GDPR (nařízení evropského parlamentu a rady EU).

1.2. Předmětem této Smlouvy je pořízení jednotného řešení SIEM (Security Information and Event Management) a Log Manager, resp. vytvoření systému sběru dat v oblasti počítačové bezpečnosti a vyhodnocování bezpečnostních událostí, a to včetně implementace a včetně podpory s cílem zvýšit zabezpečení Objednatele v oblasti počítačových technologií.

1.2.1. Základními částmi celé architektury bude zejména návrh pokrytí těchto oblastí, v souladu s legislativními požadavky:

- reporting monitoring a analýza síťové aktivity,
- reporting monitoring a analýza logů a událostí,
- korelace událostí,

- kategorizace událostí (závažnost),
- prioritizace událostí (urgentnost),
- oznamování událostí,
- analýza hrozeb,
- zvládání rizik,
- reaktivní opatření na události,
- auditing provozu,
- incident manager,
- reporting,
- ukládání a archivace těchto dat,
- seznam podporovaných systémů, služeb a aplikací, které lze připojit nativně.

1.2.2. Dále bude k dispozici možnost zpracovávat data získaná ze síťových prvků, operačních systémů (případně aplikací) a získávat data z nestandardních (ne nativních) prvků vhodným způsobem, např. pomocí SNMP nebo SYSLOG protokolu. Součástí musí být také zabezpečené datové úložiště, např. diskový prostor, který by byl součástí případného vlastního hardwarového řešení.

1.2.3. Rozsah projektu bude minimálně obsahovat:

ANALYTICKÁ ČÁST

- identifikace zařízení Centra (zejména prvky bezpečnostní infrastruktury, síťové prvky, firewally, IPS, operační systémy, databázové systémy, aplikace (pošta, dhcp,www, dns apod.), které vytváří logy o bezpečnostních událostech - ty budou následně napojeny do SIEM,
- odhad počtu záznamů (EPS),
- případně i denní objem dat, shromažďovaný v SIEM.

NÁVRH ŘEŠENÍ

- návrh technického řešení (popis potřebného hardware a softwarových modulů) vlastního SIEM,
- popis požadovaných úprav v jednotlivých systémech,
- popis (rámcově) i požadované součinnosti se správci dotčených systémů,
- návrh sledování typů jednotlivých logů ze zařízení,
- vytvoření návrhu ohodnocení událostí (incidentů) z hlediska jejich závažnosti,
- návrh umístění sondy (sond) pro sledování provozu na "paketové" úrovni - network-based.

IMPLEMENTACE NÁSTROJE

- implementace schválené podoby nástroje do infrastruktury Objednatele,
- uvedení nástroje do provozu.

PODPORA PROVOZU

- podpora provozu nástroje SW Vmware (aktualizace, úpravy z legislativních a/nebo věcných důvodů, opravy chyb a závad) po dobu 36 měsíců.

1.2.4. Zařízení by tak mělo podporovat minimálně následující funkce:

- reporting monitoring a analýza síťové aktivity (objemy dat dle aplikací apod.),
- reporting monitoring a analýza logů a událostí,
- korelace událostí (spojování událostí z různých zdrojů),
- kategorizace událostí (závažnost),
- přiřazení vlastní úrovně závažnosti,
- prioritizace událostí (urgentnost),
- oznamování událostí,
- analýza hrozeb,

- zvládání rizik,
- reporting,
- ukládání a archivace těchto dat,
- tvorba a úprava pravidel (rules) pro analýzu logovacích dat,
- Možnost upravit a vytvořit vlastní DSM – device support moduly,
- real-time nastavitelné web-based dashboardy,
- threat intelligence feeds – databáze potencionální nebezpečných IP a URL adres (včetně C&C serverů),
- generování reportů v následujících formátech: PDF, HTML, RTF, XML nebo XLS.

1.3. Přesná specifikace technického řešení (popis potřebného hardware a softwarových modulů) vlastního SIEM, plně odpovídající požadavkům Objednatele uvedeným v této Smlouvě a její **Příloze č. 1 - Požadavky na technickou specifikaci a rozsah řešení SIEM** a dále požadavkům obsaženým ve Výzvě včetně zadávací dokumentace na veřejnou zakázku malého rozsahu s názvem „Dodávka nástroje SIEM včetně funkcionality pro audit logů“ a jejích přílohách (dále jen „výběrové řízení“), kterou Dodavatel získal od Objednatele již v rámci výběrového řízení na uvedenou veřejnou zakázku, jehož výsledkem je tato mezi smluvními stranami uzavřená Smlouva, tvoří **Přílohu č. 2 – Popis technického řešení SIEM** a nedílnou součást této Smlouvy.

1.4. Dodavatel se tímto zavazuje, že Objednateli pořídí jednotné řešení SIEM (Security Information and Event Management) a Log Manager, resp. vytvoří systém sběru dat v oblasti počítačové bezpečnosti a vyhodnocování bezpečnostních událostí, a to včetně implementace, podpory a práv Objednatele nutných k užívání řešení Objednatelem, způsobem a v rozsahu stanoveném v této Smlouvě a jejích přílohách, a Objednatel se tímto zavazuje předmět plnění od Dodavatele převzít a zaplatit Dodavateli jeho cenu ve výši a způsobem stanoveným v čl. 4 této Smlouvy.

1.5. Předmět Smlouvy bude financovaný z těchto zdrojů:

SR – státní rozpočet

1.6. Plnění předmětu této Smlouvy bude dále zahrnovat i veškeré související práce a činnosti nezbytné k řádnému poskytnutí plnění dle této Smlouvy; náklady na tyto práce a činnosti jsou již zahrnuty v ceně.

2. Doba plnění předmětu Smlouvy

2.1. Hardware (HW) a příslušný software (SW) ve specifikaci dle čl. 1 a Přílohy č. 2 této Smlouvy bude Dodavatelem dodán nejpozději do 30 dnů ode dne podpisu této Smlouvy.

2.2. Implementace, konfigurace a testovací provoz navrženého technického řešení Dodavatelem bude prováděn po dobu 90 dnů ode dne dodání a instalace HW a příslušného SW dle přechozího odstavce tohoto článku Smlouvy.

2.3. Licence SW SIEM řešení bude poskytována po dobu 12 měsíců ode dne jeho dodání.

2.4. Licence a podpora SW Vmware bude poskytována po dobu 36 měsíců ode dne jeho dodání.

3. Místo plnění předmětu Smlouvy

3.1. Místem plnění předmětu Smlouvy bude sídlo Objednatele na adrese U Nákladového nádraží 3144/4, 130 00 Praha – Strašnice a dále pobočka Objednatele na adrese Vinohradská 46, 120 00 Praha 2.

4. Cena a platební podmínky

4.1. Celková cena za realizaci předmětu plnění dle této Smlouvy byla dohodou smluvních stran stanovena ve výši **1.983.850,00 Kč (slovy: jedenmiliondevětsetosmdesáttřitisícosmsetpadesát bez DPH**, daň z přidané hodnoty ve výši

21% činí 416.608,50 Kč, **celková cena tedy činí 2 400 458,50 Kč (slovy: dvamiliónyčtyřistatisícčtyřistapadesátosmkorunpadesáthaléřů včetně DPH.**

4.2. Ceny jednotlivých položek plnění předmětu této Smlouvy byly dohodou smluvních stran a v souladu s nabídkou Dodavatele podanou do výběrového řízení stanoveny takto:

Položka	Cena v Kč bez DPH	DPH v Kč	Cena v Kč včetně DPH
SW SIEM řešení s licencí na 12 měsíců	1 361 150,00 Kč	285 841,50 Kč	1 646 991,50 Kč
Dodávka a instalace HW pro SIEM	299 000,00 Kč	62 790,00 Kč	361 790,00 Kč
SW Vmware s licencí a podporou po dobu 36 měsíců	73 700,00 Kč	15 477,00 Kč	89 177,00 Kč
Instalace, konfigurace a následné testování celkového řešení	250 000,00 Kč	52 500,00 Kč	302 500,00 Kč
CELKEM	1 983 850,00 Kč	416 608,50 Kč	2 400 458,50 Kč

4.3. Cena dle odst. 4.1. a jakož i ceny za jednotlivé položky předmětu plnění dle odst. 4.2. tohoto článku Smlouvy jsou sjednány jako konečné a nepřekročitelné po celou dobu plnění Smlouvy a zahrnuje veškeré náklady Dodavatele nezbytné pro řádnou a včasnou realizaci předmětu této Smlouvy. Jediným důvodem pro změnu (zvýšení) ceny je změna platné sazby daně z přidané hodnoty v průběhu plnění této Smlouvy. V takovém případě budou ceny upraveny v souladu s platnou právní úpravou.

4.4. Zálohové platby se nesjednávají.

4.5. Úhrada předmětu plnění bude provedena v české měně na základě příslušného daňového dokladu vystaveného Dodavatelem, a to po řádném dodání HW a příslušného SW ve specifikaci dle čl. 1 a Přílohy č. 2 této Smlouvy, osvědčeném podepsaným protokolem o předání a převzetí v souladu s odst. 5.1 této Smlouvy.

4.6. Přílohou faktury vystavené v souladu s odst. 4.5. tohoto článku Smlouvy musí být kopie předávacího protokolu.

4.7. Faktura bude vystavena v souladu se zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a bude obsahovat údaje v souladu s § 435 občanského zákoníku a náležitosti daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

4.8. Splatnost každé faktury je stanovena dohodou smluvních stran na 30 kalendářních dnů od doručení faktury Objednateli. Na faktuře bude vyčíslena platná DPH. Pokud faktura nebude obsahovat všechny zákonem stanovené náležitosti, je Objednatel oprávněn ji do data splatnosti vrátit s tím, že Dodavatel je povinen vystavit novou fakturu s novým termínem splatnosti. V takovém případě není Objednatel v prodlení s úhradou. Nová 30 ti denní lhůta splatnosti počíná běžet dnem doručení opravené nebo nové faktury Objednateli. Za datum úhrady se považuje datum odepsání příslušné finanční částky z účtu Objednatele. Platba bude provedena na účet poskytovatele uvedený na faktuře.

5. Povinnosti a prohlášení Dodavatele

5.1. Dodavatel je povinen poskytovat dodávky a služby sjednané v této Smlouvě řádně, včas, s odbornou péčí, podle svých nejlepších znalostí a schopností a v souladu s obecně závaznými právními předpisy, přičemž je povinen sledovat a chránit oprávněné zájmy Objednatele. Řádné

dodání HW a příslušného SW ve specifikaci dle čl. 1 a Přílohy č. 2 této Smlouvy osvědčí smluvní strany podpisem předávacího protokolu.

5.2. Řádné provedení implementace, konfigurace a testovacího provozu technického řešení SIEM bude osvědčeno zpracováním tzv. charakteristiky provozu Dodavatelem, která bude stvrzena podpisy obou smluvních stran.

5.3. Dodavatel je povinen dodat Objednateli předmět plnění této Smlouvy, jakož i poskytovat licence a podporu a služby v prvotřídní kvalitě, plně odpovídající podmínkám sjednaným v této Smlouvě a jejích přílohách.

5.4. Dodavatel se zavazuje oznámit Objednateli všechny okolnosti, které zjistil v průběhu plnění této Smlouvy a které mohou mít vliv na plnění předmětu této Smlouvy.

5.5. Dodavatel je povinen na požádání informovat Objednatele o průběhu plnění této Smlouvy a akceptovat jeho doplňující pokyny a připomínky k plnění předmětu této Smlouvy.

5.6. Dodavatel 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 povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů, tzn., že je povinen poskytnout požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů (MMR, MF, NKÚ, příslušný FÚ, a další oprávněné orgány státní správy) a vytvořit výše uvedeným orgánům podmínky k provedení kontroly vztahující se k předmětu Smlouvy a poskytnout jim součinnost.

5.7. Dodavatel je povinen archivovat originální vyhotovení smlouvy, její dodatky, originály účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu Smlouvy, a to způsobem obdobným dle zákona č. 499/2004 Sb., o archivnictví a spisové službě, v platném znění, po dobu min. 10 let od zániku závazku vyplývajícího ze smlouvy, minimálně však do konce roku 2032. Po tuto dobu je dodavatel povinen umožnit osobám oprávněným k výkonu kontroly financování předmětu této Smlouvy provést kontrolu dokladů souvisejících s plněním Smlouvy.

5.8. Dodavatel není oprávněn postoupit práva, povinnosti a závazky třetí osobě nebo jiným osobám bez předchozího souhlasu Objednatele.

5.9. Vzhledem k veřejnoprávnímu charakteru Objednatele Dodavatel svým podpisem pod textem této Smlouvy uděluje Objednateli svůj výslovný souhlas se zveřejněním smluvních podmínek obsažených v této Smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů (zejména ust. § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

5.10. Dodavatel se zavazuje během plnění Smlouvy i po ukončení Smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od Objednatele v souvislosti s plněním Smlouvy. Za porušení mlčenlivosti specifikované v této Smlouvě je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 50 000,- Kč, a to za každý jednotlivý případ porušení povinnosti. Povinností mlčenlivosti není dotčena povinnost Dodavatele dle čl. 5 odst. 5.6. této Smlouvy.

5.11. Dodavatel se zavazuje, že pokud v souvislosti s realizací této Smlouvy při plnění svých povinností přijdou jeho pověření pracovníci do styku s osobními/citlivými údaji ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jejich jinému zneužití.

5.12. Dodavatel se zavazuje, že poskytováním plnění dle této Smlouvy nezasáhne neoprávněně do práv k duševnímu vlastnictví, zejména do autorských práv či práv průmyslového vlastnictví, třetí osoby. Odpovědnost za neoprávněný zásah do autorských i jiných práv třetích osob nese výlučně Dodavatel.

5.13.

6. Sankce

6.1. Dojde-li k prodlení Objednatele s dodržením termínu splatnosti fakturované ceny, může Dodavatel uplatnit úrok z prodlení ve výši 0,05 % z nezaplacené ceny za každý následující den prodlení Objednatele. K prodlení Objednatele nedojde, pokud k nezaplacení ceny dojde z důvodů spočívajících na straně Dodavatele.

6.2. Dojde-li k prodlení Dodavatele s dodáním HW a příslušného SW dle čl. 2 odst. 2.1. této Smlouvy, může Objednatel uplatnit vůči Dodavateli smluvní pokutu ve výši 0,2 % z celkové ceny předmětu Smlouvy včetně DPH, a to za každý započatý den prodlení. K prodlení Dodavatele nedojde, pokud k prodlení s plněním předmětu této Smlouvy dojde z důvodů spočívajících na straně Objednatele.

6.3. Pokud Dodavatel neodstraní nedodělky či vady zjištěné při přejímacím řízení předmětu plnění v dohodnutém termínu, je Objednatel oprávněn požadovat po Dodavateli úhradu smluvní pokuty ve výši 500,- Kč za každý nedodělek či vady a za každý den prodlení.

6.4. V případě, že Dodavatel poruší svoji povinnost podle čl. 5 odst. 5.8. a odst. 5.11., čl. 7 odst. 7.10. a čl. 8 odst. 8.5. této Smlouvy, zavazuje se, že uhradí Objednateli smluvní pokutu ve výši 10 000,- Kč za každé jednotlivé porušení povinnosti.

6.5. Zaplacením smluvní pokuty není dotčeno právo smluvních stran na náhradu případné škody. Dodavatel odpovídá Objednateli za své případné poddodavatele jako za plnění své, včetně odpovědnosti za způsobenou škodu.

6.6. Smluvní pokuta a úrok z prodlení budou splatné do 14 kalendářních dnů ode dne jejich vyúčtování smluvní stranou.

7. Další podmínky plnění předmětu Smlouvy

7.1. Objednatel má právo kontroly dodaného předmětu plnění a provedených souvisejících prací. V případě, že Objednatel zjistí vady a nedostatky, je oprávněn na ně Dodavatele upozornit a požadovat jejich bezplatné odstranění.

7.2. Práva z vadného plnění a ze záruky poskytnuté Dodavatelem bude Objednatel uplatňovat postupem sjednaným v této Smlouvě a jejích přílohách a v souladu s platnou legislativou.

7.3. Záruční doby jednotlivých položek předmětu plnění a uplatnění práv z vadného plnění jsou specifikovány v Příloze č. 1 této Smlouvy. Záruční doba počíná běžet ode dne podpisu protokolu o předání a převzetí dle čl. 5 odst. 5.1 této Smlouvy.

7.4. Práva Objednatele z vadného plnění a záruka za jakost se řídí příslušnými ustanoveními občanského zákoníku, není-li v této Smlouvě či jejích přílohách výslovně stanoven postup odlišný.

7.5. Dodavatel se zavazuje, že předmět plnění dle této Smlouvy bude během záruční doby:

a) bez jakýchkoliv vad a způsobilý k užívání pro účel, pro nějž je určen,

b) splňovat všechny požadavky stanovené touto Smlouvou a jejími přílohami a bude mít všechny požadované vlastnosti,

c) splňovat všechny požadavky stanovené platnými zákony a ostatními obecně závaznými právními předpisy a bude odpovídat platným technickým pravidlům, normám a předpisům platným na území České republiky.

7.6. Komunikačním prostředkem pro nahlašování chyb, vad či poruch dodávaného HW či SW, které je Dodavatel povinen odstranit v rámci poskytované záruky, jsou:

Email: xxxxxxxxxxx
Telefon: xxxxxxxxxxxx
Helpdesk: xxxxxxxxxxxx

7.7. Neodstraní-li Dodavatel reklamované vady ve lhůtě a způsobem dle Přílohy č. 1 této Smlouvy, je Objednatel oprávněn podle vlastního uvážení odstranění vad provést sám, pověřit jejich

odstraněním jiný subjekt. Takto vzniklé náklady je Dodavatel povinen Objednateli uhradit na základě jeho písemné výzvy a ve lhůtě určené Objednatelem ve výzvě. V případě, že vady předmětu plnění odstraní Objednatel či jím navržená třetí osoba, nemá tato skutečnost vliv na záruku poskytovanou Dodavatelem dle této Smlouvy.

7.8. Záruční doba neběží po dobu, po kterou nemůže Objednatel předmět plnění řádně užívat pro vady, za které odpovídá Dodavatel.

7.9. Kromě povinností Dodavatele vyplývajících z výše uvedeného je Dodavatel povinen uhradit Objednateli vzniklé prokázané škody, které Objednateli vzniknou v souvislosti s vadným plněním Dodavatele.

7.10. Dodavatel je oprávněn využít k realizaci předmětu této Smlouvy jen ty poddodavatele, které jmenovitě uvedl ve své nabídce. Dodavatel není oprávněn bez předchozího písemného souhlasu Objednatele uzavřít poddodavatelskou smlouvu nebo změnit osobu poddodavatele, a to ani v případě, kdy novým poddodavatelem je osoba zajišťující jinou část plnění dle této Smlouvy. Žádná poddodavatelská smlouva nezakládá smluvní vztahy mezi Objednatelem a poddodavatelem.

7.11. Uzavření jakékoliv poddodavatelské smlouvy nebo uskutečnění jakéhokoliv smluvního plnění poddodavatelem bez předchozího písemného souhlasu Objednatele, případně jakákoliv změna v osobě poddodavatele bez předchozího písemného souhlasu Objednatele, budou považovány za podstatné porušení smlouvy.

8. Odpovědnost za škodu

8.1. Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k přecházení škodám a k minimalizaci vzniklých škod.

8.2. Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. Žádná ze smluvních stran není odpovědna za prodlení způsobené prodlením s plnění závazků druhé smluvní strany.

8.3. Žádná ze smluvních stran není odpovědna za škodu způsobenou prodlením druhé smluvní strany s jejím vlastním plněním.

8.4. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

8.5. Dodavatel je povinen mít po celou dobu trvání Smlouvy uzavřené platné pojištění odpovědnosti za škodu způsobenou třetí osobě v minimální výši pojistného plnění 2 000 000,- Kč. V případě, že pojistný vztah mezi Dodavatelem a pojistitelem skončí, je Dodavatel povinen sjednat nový pojistný vztah ve stejném rozsahu tak, aby byla zachována podmínka existence pojištění v předmětném rozsahu po celou dobu trvání tohoto smluvního vztahu. Existenci pojištění je Dodavatel povinen na žádost Objednatele kdykoliv prokázat.

9. Všeobecná a závěrečná ustanovení

9.1. Tato Smlouva nabývá platnosti a účinnosti dnem podpisu Smlouvy oprávněnými zástupci obou smluvních stran.

9.2. Tato Smlouva se uzavírá na dobu určitou do uplynutí doby poskytování technické podpory či licence sjednané v čl. 2 odst. 2.3. a odst. 2.4. této Smlouvy.

9.3. Tato Smlouva, jakož i práva a povinnosti vzniklé na základě této Smlouvy nebo v souvislosti s ní se řídí občanským zákoníkem.

9.4. Vztahuje-li se důvod neplatnosti jen na některé ustanovení této Smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy nebo obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu Smlouvy.

9.5. Objednatel je oprávněn odstoupit od Smlouvy v případě, že nebude mít zajištěny finanční prostředky na úhradu plnění dle této smlouvy na další kalendářní rok, v takovém případě je oprávněn od Smlouvy odstoupit vždy k 1. 1. příslušného kalendářního roku, kterého se nedostatek finančních prostředků týká.

9.6. Objednatel je dále oprávněn tuto Smlouvu písemně vypovědět i bez udání důvodu, s výpovědní lhůtou v délce 3 měsíců, počínaje prvním dnem měsíce následujícího po měsíci, ve kterém byla výpověď poskytovateli doručena.

9.7. Dodavatel je oprávněn odstoupit od Smlouvy v případě, že je Objednatel v prodlení s plněním peněžitých závazků a toto prodlení trvá po dobu delší než třicet (30) dní po písemném upozornění.

9.8. Odstoupením od Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, úroků z prodlení, ochrany informací, zajištění pohledávky kterékoliv ze smluvních stran, řešení sporů a ustanovení týkající se těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení (zejména jde o povinnost poskytnout peněžitá plnění za plnění poskytnutá před účinností odstoupení

9.9. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných oprávněnými zástupci obou smluvních stran.

9.10. Tato Smlouva je vyhotovena ve čtyřech exemplářích s platností originálu, z nichž dva obdrží Objednatel a dva Dodavatel.

Nedílnou součástí této Smlouvy je:

- Příloha č. 1 – Požadavky na technickou specifikaci a rozsah řešení SIEM
- Příloha č. 2 – Popis technického řešení SIEM

10. Podpisy smluvních stran

10.1. Obě smluvní strany prohlašují, že si tuto Smlouvu před jejím podpisem přečetly, že byla uzavřena po jejím projednání podle jejich pravé a svobodné vůle a nikoli v tísni za jednostranně nevýhodných podmínek.

V Praze dne 17.8. 2017	V Praze dne 17.8.2017
Za Objednatele:	Za Dodavatele:
……..….	…….
Ing. Zdeněk Vašák generální ředitel Centrum pro regionální rozvoj České republiky	Petr Kašparovský jednatel KSP Computer & Services

Příloha č. 1 - Požadavky na technickou specifikaci a rozsah řešení SIEM

Nástroj SIEM musí zabezpečit zejména uvedené činnosti a funkce:

A. Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačních systémů kritické informační infrastruktury (dále jen „KIS“) a z významných informačních systémů (dále jen „VIS“) spravovaných Centrem a z komunikační infrastruktury těchto systémů (dále jen „KI“).

B. Detekci kybernetických bezpečnostních událostí v rámci celé sítě Centra a v případě stanovených nebezpečí okamžité předání této skutečnosti oprávněným osobám stanoveným způsobem.

1. <u>Obecné požadavky na systém SIEM:</u>

1.1. Všechny potřebné komponenty HW i SW musí být součástí dodaného systému SIEM, včetně databáze.

1.2. Všechny komponenty systému SIEM jsou dostupné v českém nebo anglickém jazyce.

1.3. Systém musí být nakonfigurován v takovém režimu dostupnosti, aby nedošlo ke ztrátě sbíraných Log záznamů v lokalitě Vinohrady v případě výpadku lokality Žižkov. Tato funkcionalita musí být zajištěna automaticky.

2. <u>Dodávané zařízení musí být minimálně osazeno takto:</u>

- 1x CPU, min. výkon na jedno CPU dle: Benchmark CPU2006:
- Výsledky veřejně dostupné na www.spec.org
- CINT2006 = 60
- CFP2006 = 112
- CINT2006 Rates = 1050
- CFP2006 Rates = 824

- 28 pozic na hot-plug HDD
- 8x PCIe3.0 slot
- 2x napájecí zdroje max. 450 W každý, účinnost alespoň 94%
- operační paměť min. 256 GB RAM,
- 11 Ks disků SAS 12G 1.2TB 10K 512e HOT PL 2.5
- Raid řadič (podpora RAID 0, 1, 10, 5)
- 2 x SFP+ Module Multi Mode Fiber 10GbE LC
- 2x10Gb SFP
- 4x1Gbit Lan
- záruka 5 roky-oprava na místě (24x 7 oprava do 8 hodin)

Součásti dodávky bude Virtualizační SW, který bude plně hodnotný s VMW vCenter Server FND + VMware vSphere STD. Na dodaném Serveru budou vytvořeny minimálně 3 samostatné stroje dle potřeb zadavatele. Na dodaný SW bude 3letá podpora s možností prodloužení o další období.

2.1. Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“, která je přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím standardního webového prohlížeče (MS IE, Mozilla, Chrome).

2.2. Centrální správa systému SIEM musí podporovat GUI (Grafické uživatelské rozhraní).

2.3. Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů atd.

musí probíhat z grafického rozhraní systému SIEM.

2.4. Přístup uživatelů musí být založen na volně definovaných oddělených rolích s možností granulárního přidělování práv v přístupu do SIEM.

2.5. Systém SIEM musí vyhledávat dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených lozích a v auditních lozích systému

2.6. Systém SIEM musí poskytovat informace při vlastním běhu a vyhodnocování logů.

2.7. Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel.

2.8. Systém musí obsahovat plně integrovaný nástroj pro řízení celého životní cyklu incidentu.

3. <u>Požadavky na výkonnost, škálovatelnost a licenci:</u>

3.1. Systém SIEM musí mít garantovanou licenci pro zpracování min. 500 EPS v denních špičkách.

3.2. Komponenta sbírající logy, musí být schopna trvale zpracovávat 300 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení.

3.3. Licence pro centrální prvek musí být rozšiřitelná na 5000 EPS bez nutnosti upgradu HW, jen pomocí aktivace licence.

3.4. Platnost SIEM licencí budou minimálně s roční podporou.

3.5. Kapacita úložného prostoru:

- systém SIEM musí na každém pracovišti objednavatele umožnit interně uložit log záznamy (RAW formát) po dobu min. 6 měsíců,
- systém SIEM musí umožnit interně uchovat normalizované log záznamy po dobu min. 6 měsíců.

3.6. Systém SIEM musí umožňovat rozšiřování kapacity a výkonu formou distribuce zátěže na více samostatných systémů např. více Log serverů, collectorů, procesorů s jedním centrálním místem pro vyhodnocování (event management).

3.7. Systém SIEM musí podporovat současnou práci min. 2 uživatelů.

3.8. Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů a vlastních custom logů.

4. <u>Požadavky na sběr dat</u>

Vrstva sběru logů musí splňovat:

- musí podporovat (sbírat, zpracovat a interpretovat) následující typy logů a protokolů: Syslog, SNMP Trap, textové logy (včetně "custom logs "), Windows Event Logs, Netflow, JUNIPER firewally SRX3600, SRX550, SRX220H2, SRX100H2, Symantec Endpoint protection Manager,

- musí podporovat sběr událostí z aktivních síťových zařízení.

5. <u>Požadavky na zpracování událostí</u>

- normalizaci bezpečnostních událostí v systému SIEM do jednotného formátu,

- kategorizaci logů, kterou poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti znalosti konkrétního logu,
- vyhodnocovat i vlastní provozní logy,
- zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem,
- export a import pravidel i log parserů,
- definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů,
- real-time korelaci a korelaci v časovém okně mezi událostmi z různých zdrojů,
- automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací,
- vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat,
- agregace událostí v systému SIEM do jedné události po definovaném čase,
- ukládání logů v systému SIEM ve tvaru, ve kterém je možné jejich prohledávání tj. minimálně musí poskytovat vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov,
- na jakoukoliv událost musí být možné navázat automatickou akci,
- notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod.,
- musí poskytovat zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, min 1x měsíčně. Musí obsahovat minimálně:
    - Generické politiky
    - Generické korelační pravidla
    - Generické předdefinované reporty, pokud budou k dispozici
- musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí,
- musí obsahovat reporting a monitoring a analýzu síťové aktivity (objemy dat dle aplikací apod.),
- musí obsahovat reporting a monitoring a analýza logů a událostí,
- musí obsahovat korelaci událostí (spojování událostí z různých zdrojů),
- musí obsahovat kategorizaci událostí (závažnost),
- musí obsahovat možnost přiřazení vlastní úrovně závažnosti,
- musí obsahovat možnost prioritizaci událostí (urgentnost),
- musí obsahovat oznamování definovaných událostí určeným způsobem (emailem),
- musí obsahovat možnost tvorby a úpravy pravidel (rules) pro analýzu logovaných dat,
- musí obsahovat možnost upravit a vytvořit vlastní DSM – device support moduly,
- musí obsahovat real-time nastavitelné web-based dashboardy,
- musí obsahovat threat intelligence feeds – databáze potencionálně nebezpečných IP a URL adres (včetně C&C serverů),
- musí obsahovat generování reportů v následujících formátech: PDF, HTML, RTF, XML nebo XLS,
- celé řešení musí plně splňovat licenčně tyto minimální parametry (500 EPS, 15000 Flows, 750 napojených zdrojů).

6. Požadavky na archivaci a ukládání

Systém SIEM musí umožňovat:

- interně uchovat data bez ztráty informací, tzv. RAW logy (bez filtrace, normalizace, redukce) po dobu minimálně 6 měsíců,

- interně uchovat normalizované log záznamy po dobu min. 6 měsíců,
- automaticky archivovat a zálohovat logy podle nastavených požadavků,
- systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu.

7. Požadavky na reporting a interpretaci dat

- předdefinované reporty systému SIEM a musí být modifikovatelné,
- systém SIEM musí poskytovat reporty i ve formě grafů a tabulek,
- systém SIEM vytváří reporty ve formátech PDF, HTML a CSV, popř. dalších,
- systém SIEM musí umožňovat export dat ve formátu XML nebo CSV,
- systém SIEM musí obsahovat analytické nástroje umožňující např. reportování, statistické reporty nad aktuálními i historickými daty,
- systém musí poskytovat report o aktivitách vybraných uživatelů resp. skupiny uživatelů,
- systém musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzv. raw-message,
- systém SIEM musí poskytovat pro každého uživatele vlastní personalizovaný dashboard,
- Drill-down analýza v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným OS a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / logách / zdrojích na daném hostu apod.),
- systém musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.

8. Požadavky na integraci

8.1. Zadavatel požaduje v rámci implementace integrovat a podrobně zdokumentovat následující typy zdrojů logů a událostí do systému SIEM. Nativní nebo v rámci dodávky integrovaná podpora aplikací (sběr dat, parsování a jejich normalizace) musí být poskytovatelem poskytnuta na klíč.

8.2. Požadované zdroje:

1. Systém SIEM musí podporovat a integrovat NetFlow.

2. Součástí instalace bude obsahovat:
   - připojení k 20 prvkům současné bezpečnostní infrastruktury,
   - připojení 30 serverům Windows,
   - nastavení vlastních pravidel chování a konfigurace vestavěných zařízení,
   - připojení Flow sond, které budou připojené do vybraných míst v síti,
   - nastavení collectorů,
   - nastavení procesorů pro vyhodnocování,
   - vytvoření seznamu úrovní logování z jednotlivých systémů, tak, aby plně vyhovělo zákonům 181/2014 a 365.

3. Systém SIEM musí podporovat integraci následujících operačních systémů a služeb:
   a. Microsoft Windows Server 2008 a vyšší,
   b. Microsoft Windows 7 a vyšší,
   c. Hyper-V,
   d. Služby Active Directory,
   e. Služby sdílení souborů MS Windows,
   f. IIS Web Server,
   g. DNS na platformě Microsoft,
   h. DHCP na platformě Microsoft.

4. Systém SIEM musí podporovat integraci následujících aplikací a informačních systému:
    a. MS SQL 2005 a vyšší,
    b. MS WSUS,
    c. MS Exchange í,
    d. AV Symantec 12.1,
    e. Firewall(Junos),
    f. Síťové prvky HP.

Příloha č. 2 - Popis technického řešení SIEM

Příloha č. 2 - Popis technického řešení SIEM

Naše společnost by Vám ráda nabídla produkt „***Virtual JSA Threat Management All-In-One***“ pro pracoviště U Nákladového nádraží a „***Virtual JSA Threat Management Event Collectors*** „ pro pracoviště Vinohradská. Oba tyto produkty mají roční podporou.
Toto řešení plně splňuje požadované řešení na sběr a vyhodnocování dat, které jsou uvedené v ZD.

Analytická část

Bude provedena na základě poskytnutých podkladů o zařízení Zadavatelem v místě instalace. Na základě informací bude vytvořen plán a nasazení kritických zařízení do systému SIEM.
Po 14 dnech bude vyhodnocené data SIEM řešení a dojde k postupnému zadání dalších potřebným zařízení, které se budou moci připojit k systému SIEM, které jsou popsané v Technické specifikaci Zadavatele. Vše bude řádně protokolováno a obě strany tento postup předem odsouhlasí.

Při předání finálního stavu systému SIEM bude vše řádně technicky zdokumentované a předané Zadavateli.

Návrh řešení

Server pro SIEM na pracovišti U Nákladového nádraží 3144/4 a Vinohradská 46
Dále Vám nabízíme Server Fujitsu PY RX2540 M2, který bude osazen takto:

Intel Xeon E5-2650v4 12C/24T 2.20 GHz	1
Performance Mode Installation	1
32GB (1x32GB) 2Rx4 DDR4-2400 R ECC	4
DVD-RW supermulti ultraslim SATA	1
Config 5: 16x 2.5" HDD	1
HD SAS 12G 1.2TB 10K 512e HOT PL 2.5' EP	11
PRAID EP400i	1
RAID Ctrl FBU option with 25cm cable	1
TFM module for FBU on PRAID EP400i	1
SFP+ Module Multi Mode Fiber 10GbE LC	2
PLAN EM 2x10Gb SFP OCl14000-LOM interfac	1
PLAN CP 4x1Gbit Cu Intel I350-T4 LP	2
Rack Mount Kit F1 CMA QRL LV	1
Mounting of RMK in symmetrical racks	1
Rack Cable Arm 2U	1
Made in Germany sticker	1
region kit APAC/EMEA/India	1
eLCM Activation License	1
iRMC advanced pack	1
Modular PSU 450W platinum hp	2
Cable powercord rack, 1.8m, black	2
SP 5y OS,24x7	1

Záruka na tento server je 5 let, oprava na místě u Zákazníka do 8 hodin.

K serveru bude dodán SW VMW vCenter Server FND w/o a VMware vCenter Server Foundation for 1 Instance of VC (Max 3 ESXi Nodes) s 3 letou licencí a podporou. SW bude plně využit pro Virtuální prostředí daného řešení.

Zadavatel pro záložní pracoviště poskytne HW prostředky na, které bude naistalován SW „Virtual JSA Threat Management Event Collectors „. Tento Sw bude zastávat funkci (sběr logů v lokalitě Vinohradská) a to pouze v případě výpadku nebo nedostupnosti lokality U Nákladového nádraží.

Implementace nástroje

Na lokalitu U Nákladového nádraží bude dodán Server Fujitsu, SIEM a VMware SW. Po odsouhlasení dodávky započne instalace Serveru Fujitsu do rekové infrastruktury. Zadavatel poskytne IP rozsah pro daný server (managment) a poté i IP rozsah pro SW SIEM. Proběhne test funkčnosti serveru. Další kroky budou následovat takto:

- vytvořen oddíl pro systém a oddíl pro sběr logů
- instalace SW VMware
- instalace SW SIEM v lokalitě U Nákladového nádraží a v Vinohradská
- připojení požadovaných systémů Zadavatele k SIEM řešení
- ladění a detekce rizikového provozu v prostředí SW SIEM dle požadavků Zadavatele

- úprava raportů dle požadavku Zadavatele
- předání dokumentace provozu a zaškolení obsluhy Zadavateli

Celé řešení bude plně splňovat požadavky Zadavatele, které jsou součástí smlouvy Příloha č.1 „Smlouva dodávce nástroje SIEM včetně funkcionality pro audit logů“

Podpora provozu

Podpora provozu nástroje SW Vmware (aktualizace, úpravy z legislativních a/nebo věcných důvodů, opravy chyb a závad) po dobu 36 měsíců. Dodané Licence a SW jejich počty a záruky:

Popis produktu	Počet
Virtual JSA Threat Management All-In-One SW License100 EPS, 15k Flows and 750 log sources included	1
Virtual JSA Threat Management Event Collector SW License	1
JSA Threat Management EPS Increase 100 SW License	4
Juniper Care Software Advantage Support for VJSA-TMAIO	1
Juniper Care Software Advantage Support for VJSA-TMEC	1
Juniper Care Software Advantage Support for JSA-TMAD100EPS	4

Popis produktu	Počet
VMware vSphere STD for 1 CPU w/o SP-3yr	**3**
VMware vSphere Standard for 1 CPU - Mandatory 3 year Support Pack needed!	**3**

Navrhované zařízení podporuje následující funkce:

- ✓ reporting monitoring a analýza síťové aktivity (objemy dat dle aplikací apod.),
- ✓ reporting monitoring a analýza logů a událostí,
- ✓ korelace událostí (spojování událostí z různých zdrojů),
- ✓ kategorizace událostí (závažnost),
- ✓ přiřazení vlastní úrovně závažnosti,
- ✓ prioritizace událostí (urgentnost),
- ✓ oznamování událostí,
- ✓ analýza hrozeb,

- ✓ zvládání rizik,
- ✓ reporting,
- ✓ ukládání a archivace těchto dat,
- ✓ tvorba a úprava pravidel (rules) pro analýzu logovacích dat,
- ✓ Možnost upravit a vytvořit vlastní DSM – device support moduly,
- ✓ real-time nastavitelné web-based dashboardy,
- ✓ threat intelligence feeds – databáze potencionální nebezpečných IP a URL adres (včetně C&C serverů),
- ✓ generování reportů v následujících formátech: PDF, HTML, RTF, XML nebo XLS.

Navrhovaný nástroj SIEM zabezpečuje uvedené činnosti a funkce:

C. Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačních systémů kritické informační infrastruktury (dále jen „KIS“) a z významných informačních systémů (dále jen „VIS“) spravovaných Centrem a z komunikační infrastruktury těchto systémů (dále jen „KI“).

D. Detekci kybernetických bezpečnostních událostí v rámci celé sítě Centra a v případě stanovených nebezpečí okamžité předání této skutečnosti oprávněným osobám stanoveným způsobem.

Obecné vlastnosti navrhovaného systému SIEM:

i. Všechny potřebné komponenty HW i SW jsou součástí dodaného systému SIEM, včetně databáze.

ii. Všechny komponenty systému SIEM jsou dostupné v českém nebo anglickém jazyce.

iii. Systém je nakonfigurován v takovém režimu dostupnosti, aby nedošlo ke ztrátě sbíraných Log záznamů v lokalitě Vinohrady v případě výpadku lokality Žižkov. Tato funkcionalita musí být zajištěna automaticky.

iv. Součásti dodávky je Virtualizační SW, který bude plně hodnotný s VMW vCenter Server FND + VMware vSphere STD. Na dodaném Serveru budou vytvořeny minimálně 3 samostatné stroje dle potřeb zadavatele. Na dodaný SW bude 3letá podpora s možností prodloužení o další období.

v. Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“, která je přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím standardního webového prohlížeče (MS IE, Mozilla, Chrome).

vi. Centrální správa systému SIEM musí podporovat GUI (Grafické uživatelské rozhraní).

vii. Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů atd. musí probíhat z grafického rozhraní systému SIEM.

viii. Přístup uživatelů je založen na volně definovaných oddělených rolích s možností granulárního přidělování práv v přístupu do SIEM.

ix. Systém SIEM vyhledávádle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených lozích a v auditních lozích systému

x. Systém SIEM poskytuje informace při vlastním běhu a vyhodnocování logů.

xi. Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel.

xii. Systém obsahuje plně integrovaný nástroj pro řízení celého životní cyklu incidentu.

Výkonnost, škálovatelnost a licence:

i. Systém SIEM má garantovanou licenci pro zpracování min. 500 EPS v denních špičkách.

ii. Komponenta sbírající logy, je schopna trvale zpracovávat 300 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení.

iii. Licence pro centrální prvek je rozšiřitelná na 5000 EPS bez nutnosti upgradu HW, jen pomocí aktivace licence.

iv. Platnost SIEM licencí je s roční podporou.

v. Kapacita úložného prostoru:
- systém SIEM na každém pracovišti objednavatele umožňuje interně uložit log záznamy (RAW formát) po dobu min. 6 měsíců,
- systém SIEM umožňuje interně uchovat normalizované log záznamy po dobu min. 6 měsíců.

vi. Systém SIEM umožňuje rozšiřování kapacity a výkonu formou distribuce zátěže na více samostatných systémů např. více Log serverů, collectorů, procesorů s jedním centrálním místem pro vyhodnocování (event management).

vii. Systém SIEM podporuje současnou práci min. 2 uživatelů.

viii. Licence obsahuje možnost sbírat všechny typy výrobcem podporovaných zdrojů a vlastních custom logů.

Sběr dat - vrstva sběru logů splňuje:

i. podporuje (sbírat, zpracovat a interpretovat) následující typy logů a protokolů: Syslog, SNMP Trap, textové logy (včetně "custom logs "), Windows Event Logs, Netflow, JUNIPER firewally SRX3600, SRX550, SRX220H2, SRX100H2, Symantec Endpoint protection Manager,

ii. podporuje sběr událostí z aktivních síťových zařízení.

Zpracování událostí:

i. normalizaci bezpečnostních událostí v systému SIEM do jednotného formátu,

ii. kategorizaci logů, kterou poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti znalosti konkrétního logu,

iii. vyhodnocovat i vlastní provozní logy,

iv. zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem,

v. export a import pravidel i log parserů,

vi. definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů,

vii. real-time korelaci a korelaci v časovém okně mezi událostmi z různých zdrojů,

viii. automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací,

ix. vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat,

x. agregace událostí v systému SIEM do jedné události po definovaném čase,

xi. ukládání logů v systému SIEM ve tvaru, ve kterém je možné jejich prohledávání tj. minimálně musí poskytovat vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov,

xii. na jakoukoliv událost je možné navázat automatickou akci,

xiii. notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod.,

xiv. poskytuje zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, min 1x měsíčně. Musí obsahovat minimálně:
- Generické politiky
- Generické korelační pravidla
- Generické předdefinované reporty, pokud budou k dispozici

xv. obsahuje komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí,

xvi. obsahuje reporting a monitoring a analýzu síťové aktivity (objemy dat dle aplikací apod.),

xvii. obsahuje reporting a monitoring a analýza logů a událostí,
xviii. obsahuje korelaci událostí (spojování událostí z různých zdrojů),
xix. obsahuje kategorizaci událostí (závažnost),
xx. obsahuje možnost přiřazení vlastní úrovně závažnosti,
xxi. obsahuje možnost prioritizaci událostí (urgentnost),
xxii. obsahuje oznamování definovaných událostí určeným způsobem (emailem),
xxiii. obsahuje možnost tvorby a úpravy pravidel (rules) pro analýzu logovaných dat,
xxiv. obsahuje možnost upravit a vytvořit vlastní DSM – device support moduly,
xxv. obsahuje real-time nastavitelné web-based dashboardy,
xxvi. obsahuje threat intelligence feeds – databáze potencionálně nebezpečných IP a URL adres (včetně C&C serverů),
xxvii. obsahuje generování reportů v následujících formátech: PDF, HTML, RTF, XML nebo XLS,
xxviii. celé řešení splňuje licenčně tyto minimální parametry (500 EPS, 15000 Flows, 750 napojených zdrojů).

Archivace a ukládání - systém SIEM umožňuje:

i. interně uchovat data bez ztráty informací, tzv. RAW logy (bez filtrace, normalizace, redukce) po dobu minimálně 6 měsíců,
ii. interně uchovat normalizované log záznamy po dobu min. 6 měsíců,
iii. automaticky archivovat a zálohovat logy podle nastavených požadavků,
iv. systém umožňujet snadnou obnovu historických dat z archivů pro zpětnou analýzu.

Reporting a interpretace dat

i. předdefinované reporty systému SIEM a musí být modifikovatelné,
ii. systém SIEM poskytuje reporty i ve formě grafů a tabulek,
iii. systém SIEM vytváří reporty ve formátech PDF, HTML a CSV, popř. dalších,
iv. systém SIEM umožňuje export dat ve formátu XML nebo CSV,
v. systém SIEM obsahuje analytické nástroje umožňující např. reportování, statistické reporty nad aktuálními i historickými daty,
vi. systém poskytuje report o aktivitách vybraných uživatelů resp. skupiny uživatelů,
vii. systém podporuje možnost zobrazit Log záznam v původní formě, jak byl přijat, tzv. raw-message,
viii. systém SIEM poskytuje pro každého uživatele vlastní personalizovaný dashboard,
ix. Drill-down analýza v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným OS a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / logách / zdrojích na daném hostu apod.),
x. systém podporuje automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.

Integrace:

i. Zadavatel požaduje v rámci implementace integrovat a podrobně zdokumentovat následující typy zdrojů logů a událostí do systému SIEM. Nativní nebo v rámci dodávky integrovaná podpora aplikací (sběr dat, parsování a jejich normalizace) musí být poskytovatelem poskytnuta na klíč.
ii. Požadované zdroje:
    5. Systém SIEM podporuje a integruje NetFlow.
    6. Instalace obsahuje:
        - připojení k 20 prvkům současné bezpečnostní infrastruktury,

- připojení 30 serverům Windows,
- nastavení vlastních pravidel chování a konfigurace vestavěných zařízení,
- připojení Flow sond, které budou připojené do vybraných míst v síti,
- nastavení collectorů,
- nastavení procesorů pro vyhodnocování,
- vytvoření seznamu úrovní logování z jednotlivých systémů, tak, aby plně vyhovělo zákonům 181/2014 a 365.

7. Systém SIEM podporuje integraci následujících operačních systémů a služeb:
   - Microsoft Windows Server 2008 a vyšší, Microsoft Windows 7 a vyšší, Hyper-V,Služby Active Directory, Služby sdílení souborů MS Windows, IIS Web Server, DNS na platformě Microsoft, DHCP na platformě Microsoft.
8. Systém SIEM podporuje integraci následujících aplikací a informačních systému:
   - MS SQL 2005 a vyšší, MS WSUS, MS Exchange, AV Symantec 12.1, Firewall(Junos), Síťové prvky HP.