Smlouva
o dodávce komplexního systému SIEM

uzavřená podle § 1746 odst.2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a zákona č.120/2001 Sb., autorský zákon, ve znění pozdějších předpisů, mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo také „ČNB")

a

S&T CZ s.r.o.
Na Strži 1702/65, 140 00 Praha 4
zapsanou v obchodním rejstříku vedeném u Městského soudu v Praze oddíl C, vložka 6033
zastoupenou: Miroslavem Bečkou, jednatelem
a
Ing. Kamilem Krusem, jednatelem
IČO: 44846029
DIČ: CZ44846029
Československá obchodní banka, a. s., Radlická 333/150, 150 57 Praha 5
Číslo účtu: 117422733 / 0300)

(dále jen „zhotovitel")

Článek I
Předmět smlouvy a místo plnění

1. Poskytovatel se zavazuje dodat, nainstalovat a implementovat technické a programové prostředky (dále též „HW a SW") managementu bezpečnostních informací a událostí (dále jen "SIEM řešení" nebo jen „SIEM"). SIEM řešení musí splňovat požadavky objednatele uvedené v příloze č. 1 a splňovat specifikaci z nabídky poskytovatele, která tvoří přílohu č.2 smlouvy.
2. Součástí plnění je dále zaškolení zaměstnanců objednatele, poskytnutí spoluúčasti poskytovatele při akceptačních testech a dodání dokumentace podle čl. II odst. 1 písm. b).
3. Poskytovatel se zavazuje v rámci plnění podle této smlouvy nainstalovat nejnovější verzi programových prostředků, která bude výrobcem v době plnění uvedena na trh.
4. Předmětem této smlouvy je dále závazek poskytovatele poskytovat objednateli podporu podle článku VI, a to ode dne podpisu závěrečného akceptačního protokolu.

5. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1 a Strojírenská 175, Praha 5;

6. Předmětem této smlouvy je závazek objednatele poskytnout potřebnou součinnost a zaplatit za poskytnutá plnění ceny dle čl. V.

7. Poskytovatel bere na vědomí, že mu nebude umožněn vzdálený přístup k serverům objednatele.

Článek II
Průběh plnění

1. Plnění podle čl. I odst. 1 a 2 bude realizováno ve třech etapách takto:

   a) První etapa – **ANALÝZA, vypracování detailního technického popisu cílového stavu a vypracování implementačního postupu**:

   - poskytovatel se zavazuje na základě analýzy systémového prostředí ČNB vypracovat **implementační postup a detailní popis cílového stavu**, který bude minimálně obsahovat:
     - klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu)
     - doporučení pro zlepšení nastavení logování pro jednotlivé zdroje. Seznam zdrojů je uveden v článku II. technických požadavků objednatele
     - detailní architekturu systému SIEM
     - výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů
     - návrh postupu řešení importu aplikačního log záznamu, kde popis aktivity uživatele bude víceřádkový nebo bude obsahovat znaky uvozovek nebo středníku atd.
     - metody a pravidla identifikace, zpracování a vyhodnocování událostí
     - pravidla pro vznik varováni, alertů, incidentů a notifikací, včetně priority
     - návrh na zajištění prokazatelnosti autenticity logu (jeho pravosti, a že nebyl modifikován)
     - návrh organizačního zabezpečení
     - návrh plánu zálohování
     - způsob autentizace k systému SIEM dle jedné z variant uvedených v článku I odst. 1.10 přílohy č. 1 - Technické požadavky objednatele
     - proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, alertu, incidentu a notifikace
     - definici pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.)
     - návrh testovacích scénářů na základě technických požadavků objednatele, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Testy musí obsahovat simulace minimálně několika typů útoků (např. test detekce útoku na hesla "hrubou silou", test detekce postupného útoku na různé systémy tj. neúspěšné pokusy o přihlášení se jedním uživatelským účtem postupně na více systémů apod.).
     - harmonogram implementace SIEM v prostředí ČNB, v souladu s čl. III odst. 1 a 2 této smlouvy
     - nároky na součinnosti objednatele.

b) Druhá etapa – **IMPLEMENTACE**:

tato fáze zahrnuje především:

- kompletní dodávku HW a SW, jeho instalaci a konfiguraci v systémovém prostředí ČNB
  - poskytovatel dodá a zajistí montáž a instalaci všech HW komponent do technologických stojanů na http a ZTP dle článku I odst. 1.5 technických požadavků objednatele včetně označení kabelů
  - poskytovatel zajistí instalaci softwarového vybavení a agentů a konfiguraci SIEM systému v prostředí ČNB
  - poskytovatel zajistí integraci s Active directory objednatele pro řízení oprávněných uživatelů dle jedné z variant uvedených v článku I odst. 1.10. přílohy č. 1 smlouvy, práva a role uživatele budou však již řízena v rámci SIEM
  - poskytovatel zajistí v systému SIEM integraci dle čl. II přílohy č. 1 smlouvy
  - poskytovatel zajistí konfiguraci pravidelné automatické archivace logů (např. denně, týdně a pod.)
  - poskytovatel zajistí konfiguraci automatického zálohování systému SIEM (konfigurace a dat)
  - poskytovatel zajistí konfiguraci zpracování dat (od sběru, normalizace, pokročilé korelace až po vyhodnocování incidentů)
  - poskytovatel zajistí konfiguraci notifikací o bezpečnostních incidentech
  - poskytovatel zajistí konfiguraci min. 10 ks custom reportů, včetně automatického generování a zasílání definovaných reportů e-mailem přímo ze systému
  - poskytovatel zajistí konfiguraci zabezpečení celého řešení, včetně nastavení politik přístupů, hesel a pod., pro 10 uživatelů ČNB
  - poskytovatel zajistí konfiguraci monitoringu dostupnosti dodaného řešení a přeposílání provozně významných událostí do centrálního monitorovacího systému MS System Center Operations Manager (syslog)
  - poskytovatel v rámci řešení navrhne a zrealizuje automatický sběr a evidenci vztahů mezi:
    - časový interval -> IP adresa -> jméno PC / MAC adresa
    - časový interval -> jméno PC -> Online uživatelský účet
    - přiřazení uživatelských účtů k uživatelům

    Uvedené vztahy bude možné využívat v reportech nebo při přiřazování aktivit k uživatelům.
- provedení funkčních testů SIEM v prostředí ČNB, spočívající především v ověření:
  - autentizace uživatele do systému SIEM
  - sběru logů ze všech zdrojů uvedených v čl. II technických požadavků objednatele
  - normalizace a korelace logů
  - vytváření a automatické zasílání reportů e-mailem
  - automatické odesílání notifikací e-mailem
  - automatické zálohování konfigurace a logů
- vypracování a předání podrobné technické a provozní dokumentace SIEM v českém nebo anglickém jazyce, zahrnující minimálně:

- popis funkčního schématu řešení
- popis zapojení dodaných zařízení
- popis konfigurace jednotlivých zařízení
- popis bezpečnostních rysů a jejich konfigurace
- popis provedených nativních i custom integrací se systémy ČNB, jejich nastavení a konfiguraci, včetně dodání kompletních zdrojových kódů s popisem kódu a použitých vývojových prostředí
- popis zálohování, archivace a obnovy logů a dat pro analýzu a vyhledávání v historických údajích
- postup implementace dodaného systému
- postupy integrace logů / událostí z nových zařízení tj. tvorbu pravidel pro parsování, normalizaci logů a jejich následné zpracování (např. pokročilou korelaci)
- postupy pravidelné údržby dodaného systému
- postupy diagnostiky a monitorování provozu dodaného systémů
- postupy řešení havarijních stavů dodaného systému
- postupy zálohování, archivace a obnovy konfigurace dodaného systému a dat

- zajištění školení pro dodaný systém pro minimálně 10 zaměstnanců ČNB v rozsahu umožňujícím provádět:
  - běžný rutinní provoz a údržbu dodávaného řešení, včetně provedení příslušných konfiguračních změn
  - řešení obvyklých problémů
  - správu uživatelských oprávnění
  - monitoring stavu zařízení
  - zálohování a obnovu konfigurace a dat
  - obnovu logů a dat pro dodatečnou analýzu zaznamenaných údajů
  - tvorbu pohledů a reportů
  - tvorbu korelačních pravidel
  - správu zdrojů a jejich přidávání, včetně přidávání custom zdrojů
  - činnosti při detekci a analýze incidentů a vyhledávání informací
  - zpracování a vyhodnocování vlastních custom logů
- předání médií (CD, DVD, disk), na kterých je uložena veškerá dokumentace ve formátech MS Office 2003 (2010).

c) Třetí etapa – **AKCEPTAČNÍ TESTY**:

- Objednatel provede akceptační testy SIEM řešení jako celku ve lhůtě do deseti pracovních dnů po dokončení druhé etapy. Poskytovatel souhlasí s tím, že akceptační testování bude provádět objednatel.
- Objednatel rovněž ověří, zda dodané SIEM řešení splňuje veškeré požadavky objednatele uvedené v příloze 1.
- Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného SIEM řešení nebo jeho části. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podstatné vady jsou vady, které způsobují tak závažné problémy, že objednatel nemůže produkt nebo jeho klíčovou část používat, ovládat nebo není funkční sběr logů z integrovaných zdrojů.

2. Objednatel převezme SIEM řešení podpisem závěrečného akceptačního protokolu dle čl. IV.
3. Objednatel umožní poskytovateli vykládku technických prostředků v prostorách objednatele v termínu, o kterém byl poskytovatelem zpraven nejméně tři pracovní dny předem. Objednatel převezme technické prostředky do úschovy a zajistí jejich bezpečné uskladnění do doby zahájení jejich instalace. Při předání a převzetí prostředků do úschovy bude pověřenými osobami obou smluvních stran podepsán dodací list.

Článek III
Lhůty plnění

1. Poskytovatel předá objednateli plnění dle článku I odst. 1 a 2 do 24 týdnů ode dne podpisu smlouvy.
2. Poskytovatel se zavazuje dokončit a uzavřít jednotlivé etapy v následujících lhůtách:
    1. etapu do 6 týdnů od podpisu smlouvy,
    2. etapu do 20 týdnů od podpisu smlouvy.
3. Pověřenými osobami jsou:

    a) za objednatele:

    Luboš Minár, tel. č.: +420 22441 2606, e-mail:lubos.minar@cnb.cz

    Petr Puchmeltr, tel. č.: +420 22441 2883, e-mail: petr.puchmeltr@cnb.cz

    b) za poskytovatele:

    Martin Frühauf tel. č. +420 724 116 649, e-mail: martin.fruhauf@sntcz.cz

    Pavel Urban, tel. č. +420 602 178 533, e-mail: pavel.urban@sntcz.cz

4. Smluvní strany se zavazují ohlástit změnu pověřených osob nebo kontaktních údajů podle tohoto článku nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob.

Článek IV
Akceptace předmětu plnění smlouvy

1. Po ukončení první a druhé etapy předloží poskytovatel výsledek jím provedených prací objednateli k posouzení a odsouhlasení v akceptačním řízení. O výsledku akceptačního řízení bude sepsán akceptační protokol zhotovený objednatelem. Každá etapa bude považována za úspěšně ukončenou pouze, pokud bude výsledek prací prostý vad, nerozhodne-li objednatel jinak.
2. K akceptačnímu protokolu vyhotovenému objednatelem vyjádří poskytovatel své stanovisko vždy nejpozději do 5 pracovních dnů od jeho obdržení. Pokud tak neučiní, má se za to, že s uvedeným závěrem souhlasí.

3. Pokud objednatel pro vady neodsouhlasí předmět prací provedený v dané etapě, sdělí poskytovateli připomínky do 5 pracovních dnů od převzetí výsledků provedených prací. Poskytovatel není oprávněn pokračovat v navazující etapě, dokud nebudou vady odstraněny a objednatel předmět prací neodsouhlasí bez výhrad a nebo pokud se objednatel nerozhodne odsouhlasit předmět prací s výhradami. V takovém případě budou jednotlivé výhrady zaznamenány v akceptačním protokolu a poskytovatel je oprávněn pokračovat v navazující etapě.
4. Objednatel převezme SIEM řešení jako celek pouze tehdy, pokud:
   - byly odsouhlaseny všechny dílčí etapy a případné vady byly odstraněny
   - poskytovatel dodal kompletní SIEM řešení prosté vad a včetně požadované dokumentace,
   - poskytovatel poskytl veškeré potřebné licence pro provoz SIEM řešení,
   - poskytovatel předal v elektronické podobě na sjednaném datovém médiu (např. CD, DVD) veškeré podklady a dokumenty potřebné ke správě, údržbě.
5. Převzetí SIEM řešení bude uskutečněno podpisem závěrečného akceptačního protokolu. Tím je plnění předáno objednateli k běžnému provoznímu využití.

Článek V
Ceny plnění, množství a platební podmínky

1. Cena za plnění dle článku I odst. 1 a 2 byla stanovena dohodou smluvních stran a činí celkem **2 952 000 Kč bez DPH.** Z toho činí cena školení částku ve výši **38 400 Kč bez DPH**. Bližší specifikace ceny je uvedena v příloze č. 4 (cenová tabulka).
2. Cena za podporu dle čl. VI odst. 2 písm. a) až d) činí **372 000 Kč bez DPH ročně.** Z toho činí cena podpory technických prostředků částku ve výši **111 600 Kč bez DPH** a cena podpory progamových prostředků částku ve výši **260 400 Kč bez DPH.**
3. Cena za podporu na místě bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí **2 000 Kč bez DPH**. K ceně prací je poskytovatel oprávněn účtovat kilometrovné ve výši 8 Kč/km.
4. K cenám uvedeným v odst. 1, 2 a 3 bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny uvedené v odst. 1, 2 a 3 zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy (včetně nákladů na náhradní díly technických prostředků dodávaných v rámci podpory).
5. Úhrada ceny dle odst. 1 bude provedena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu.
6. Úhrada ceny dle odst. 2 bude prováděna vždy ročně předem, a to na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve první den období, na které se platí.
7. Úhrada ceny dle odst. 3 bude prováděna na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, ve kterém bylo plněno.
8. Daňový doklad bude vedle náležitostí stanovených zákonem o DPH a údajů dle § 435 občanského zákoníku obsahovat i evidenční číslo smlouvy objednatele. V případě, že daňový doklad bude postrádat některou z těchto náležitostí nebo bude obsahovat

chybné údaje, je objednatel oprávněn vrátit vadný daňový doklad poskytovateli. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného daňového dokladu. Daňový doklad zašle poskytovatel na adresu:

Česká národní banka
sekce rozpočtu a účetnictví
odbor centrální účtárna
Na Příkopě 28
115 03 Praha 1
nebo elektronicky na adresu: faktury@cnb.cz.

9. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

10. V případě, že podpora dle čl. VI odst. 2 písm.a) až d) bude poskytovatelem pořizována mimo území České republiky, je kterákoliv smluvní strana oprávněna navrhnout úpravu ceny předplacené podpory uvedené v odst. 2 tohoto článku, jestliže se změní průměrný měsíční kurz CZK k zahraniční měně, za kterou poskytovatel podporu pořizuje, o více než 5 %. Při první změně ceny se bude vycházet z měsíčního průměru devizového kurzu vyhlášeného ČNB za kalendářní měsíc, v němž uplyne lhůta pro podání nabídky, tj **27,394 Kč/ EUR**. Při dalších změnách ceny se bude vycházet z kurzu poslední úpravy cen; upravena bude ta část ceny, které se změna uvedeného kurzu dotýká.

11. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

12. Ke konci kalendářního roku, nejpozději však do 31.12. je poskytovatel povinen písemně sdělit objednateli, jakou část z uhrazené roční ceny podpory tvoří cena nových verzí představujících technické zhodnocení programových prostředků.

Článek VI
Podpora

1. Poskytovatel ručí za to, že SIEM řešení bude funkční a schopné použití v prostředí objednatele a bude odpovídat požadavkům objednatele uvedeným v příloze č. 1 a vlastnostem a parametrům deklarovaným v příloze č. 2 a v dokumentaci.

2. Podpora SIEM řešení (technických a programových prostředků) zahrnuje:

   a) odstraňování vad technických a programových prostředků;

   b) poskytování aktualizací programových prostředků (nové verze, opravné verze,bezpečnostní záplaty),

   c) pravidelné aktualizace databáze SIEM, které musí obsahovat minimálně:

   - generické politiky
   - generická korelační pravidla
   - generické předdefinované reporty, pokud budou k dispozici
   - předdefinované analytické nástroje a akce pro identifikaci hrozeb a obranu vůči nim.

   d) pomoc při řešení provozních problémů,

e) podpora na místě při implementaci aktualizací programových prostředků, a to na základě výzvy objednatele.

3. Podpora bude poskytována v pracovní dny v pracovní době objednatele od 7:45 do 16:15 hod.
4. Odstraňování vad technických prostředků bude poskytovatelem prováděno výměnným způsobem bez nutnosti odborného servisního zásahu poskytovatele na místě s tím, že náhradní díl nebo zařízení musí být nové a bezvadné a musí být doručeny do sídla objednatele nejpozději do 2 pracovních dnů ode dne ohlášení vady.
5. Poskytovatel poskytne objednateli aktualizace programových prostředků bez zbytečného odkladu, nejpozději však do 14 dnů od uvedení SW výrobcem na trh. Pravidelné aktualizace databáze SIEM je poskytovatel povinen provádět minimálně 1x za měsíc.
6. Poskytovatel zahájí řešení odstranění vady programových prostředků do 1 pracovního dne ode dne jejího ohlášení. Dodavatel dodá opravnou verzi programových prostředků bez zbytečného odkladu po jejím vydání výrobcem.
7. Potřebu podpory ohlašuje objednatel poskytovateli telefonicky na telefonní číslo poskytovatele **+420 281 006 281** v době od 7:45 do 16:15 hod. s následným písemným potvrzením e-mailem na e-mailovou adresu **CZ.servisdesk@sntcz.cz** nebo potřebu podpory objednatel nahlašuje e-mailem na mailovou adresu poskytovatele uvedenou v tomto odstavci. Oznámení učiněná po uvedené době se považují za oznámené následující pracovní den, v hodině odpovídající začátku uvedené doby.
8. Poskytovatel je povinen potvrdit přijetí oznámení učiněné v pracovní dny v době uvedené v odst.7 do 4 pracovních hodin od doručení. Služby poskytované poskytovatelem musí vyhovovat technickým specifikacím a požadavkům výrobce.

Článek VII
Přechod vlastnictví a nebezpečí škody, licenční ujednání

1. Vlastnické právo k technickým prostředkům dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu. Programové prostředky poskytnuté podle této smlouvy je objednatel oprávněn užívat od okamžiku instalace/implementace.
2. Poskytovatel poskytuje objednateli nevýhradní, nepřevoditelnou, nedělitelnou, časově a územně neomezenou multilicenci umožňující užívat poskytnuté programové prostředky pouze pro vnitřní potřebu objednatele.
3. Objednatel není povinen licenci využít.
4. Součástí licence je příslušná dokumentace v elektronické podobě.
5. Poskytovatel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.
6. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

Článek VIII
Mlčenlivost, bezpečnostní požadavky objednatele, ochrana osobních údajů

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí, a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.
2. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 3 této smlouvy.
3. Dle § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOU"), strany sjednaly:

   3.1 zpracování veškerých osobních údajů objednatelem, který je ve smyslu ZOOU zpracovatelem, probíhá podle ZOOU, zejména je zpracovatel povinen ve smyslu § 7 ZOOU splnit obdobně všechny povinnosti stanovené v § 5 ZOOU pro správce osobních údajů.

   3.2 Toto ujednání o zpracování osobních údajů se uzavírá za účelem zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB způsobem, v rozsahu a postupem dle smlouvy, jejímž je toto ujednání dle § 6 ZOOU součástí. Rozsah zpracování osobních údajů bude odpovídat účelu zpracování, tedy bude obsahovat identifikační osobní údaje (jméno, příjmení a číslo průkazu totožnosti zaměstnanců poskytovatele). Zpracování osobních údajů podle tohoto ujednání se sjednává na dobu existence závazkového vztahu vzniklého ze smlouvy, jejíž součástí je toto ujednání, nejpozději do likvidace posledního osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOU.

   3.3 Objednatel poskytuje poskytovateli následující záruky technického a organizačního zabezpečení ochrany osobních údajů:
   - veškeré materiály s osobními údaji jsou zajištěny v uzamykatelném nábytku v uzamčených prostorách v sídle objednatele,
   - všechny osobní údaje jsou následně zpracovávány na PC, která jsou zabezpečena heslem, a jsou přístupné pouze vybraným zaměstnancům objednatele,
   - organizace a povinnosti zaměstnanců objednatele ohledně ochrany osobních údajů, jsou stanoveny ve vnitřním předpisu objednatele.

Článek IX
Uveřejnění smlouvy, výše skutečně uhrazené ceny a seznamu subdodavatelů

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků, výši skutečně uhrazené ceny za plnění této smlouvy a seznam subdodavatelů, kterým poskytovatel za plnění subdodávky uhradil více než 10 % z ceny za plnění dle této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ") uveřejňuje informace a dokumenty ke svým

veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je.

3. Poskytovatel je povinen dle § 147a odst. 4 ZVZ předložit objednateli vždy nejpozději do 28. února následujícího kalendářního roku seznam subdodavatelů, jímž za plnění subdodávky uhradil více než 10 % z části ceny uhrazené objednatelem poskytovateli za plnění dle této smlouvy v předchozím kalendářním roce či prohlášení, že nemá subdodavatele, jímž by za plnění subdodávky uhradil více než 10 % z části ceny uhrazené objednatelem poskytovateli za plnění dle této smlouvy v předchozím kalendářním roce. Má-li subdodavatel formu akciové společnosti, tvoří přílohu seznamu i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu. Seznam vlastníků akcií musí být vyhotoven ve lhůtě 90 dnů před dnem předložení seznamu subdodavatel. Poskytovatel zašle seznam objednateli na adresu:

   Česká národní banka
   sekce správní
   odbor obchodní
   Na Příkopě 28
   115 03 Praha 1.

4. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 147a ZVZ a uveřejňování bude prováděno dle ZVZ a příslušného prováděcího předpisu ZVZ.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě, že poskytovatel nedodrží závaznou lhůtu pro předání plnění dle čl. III odst. 1 nebo lhůtu pro úspěšné ukončení 1. nebo 2. etapy dle čl. III odst. 2, uhradí objednateli smluvní pokutu ve výši 1 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele.
2. V případě, že se v průběhu plnění podle článku II prokáže, že nebyl poskytovatelem splněn jakýkoliv požadavek objednatele uvedený v příloze č. 1 má objednatel právo požadovat smluvní pokutu ve výši 1 000 Kč za každý případ nedodržení požadavku.
3. V případě prodlení poskytovatele ve lhůtě pro dodání náhradního zařízení nebo náhradního dílu podle článku VI odst. 4 je objednatel oprávněn požadovat smluvní pokutu ve výši 3 000 Kč za každý pracovní den prodlení.
4. V případě prodlení poskytovatele ve lhůtě pro potvrzení ohlášení podle čl. VI odst. 8 je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každou pracovní hodinu prodlení.
5. V případě prodlení objednatele s úhradou daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
6. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
7. Ujednáním o smluvní pokutě není dotčeno právo na náhradu škody ve výši, v jaké převyšuje smluvní pokutu.

Článek XI
Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části poskytování podpory uzavírá na dobu neurčitou.
2. Smlouvu lze v části podpory ukončit písemnou výpovědí bez uvedení důvodu, která musí být doručena druhé smluvní straně nejpozději 3 měsíce přede dnem uplynutím předplacené doby podpory.
3. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele vypovědět tuto smlouvu v části týkající se poskytování podpory, a to ve 14 denní výpověďní lhůtě, která počíná běžet dnem následujícím po doručení písemné výpovědi poskytovateli.
4. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí poskytovatel objednateli alikvotní část předplacené ceny podpory.
5. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to písemným oznámením o odstoupení. Odstoupení je účinné dnem doručení oznámení o odstoupení druhé smluvní straně. V případě podstatného porušení smlouvy poskytovatelem může objednatel odstoupit od smlouvy do 30 dnů ode dne porušení.
6. Za podstatné porušení smlouvy strany považují zejména tyto případy:
   a) objednatel neuhradí poskytovateli cenu ve lhůtě 30 dnů po dni její splatnosti ani po písemném oznámení poskytovatele,
   b) dodané SIEM řešení, nebo některá jeho komponenta, nebude splňovat veškeré požadavky dle této smlouvy,
   c) systém není způsobilý pracovat v rámci systémového prostředí ČNB - např. není plně kompatibilní s operačními systémy (jejich verzemi), databázemi (jejich verzemi) a aplikacemi (jejich verzemi),
   d) poskytovatel bude v prodlení s předáním plnění nebo kterékoliv etapy plnění delším než 30 dnů.
7. V případě odstoupení od smlouvy objednatelem se poskytovatel zavazuje zajistit na své náklady odvoz technických a programových prostředků, a to nejpozději do 30 dnů ode dne doručení oznámení o odstoupení od smlouvy.
8. Smluvní strany si sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 50 000 Kč na účet zhotovitele, a to kdykoli do akceptace 1. etapy. Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet zhotovitele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti zhotovitele.

Článek XII
Ostatní ujednání

1. Poskytovatel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění pro případ vzniku odpovědnosti za škodu způsobenou v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 10 000 000 Kč (slovy: deset milionů korun českých) a jeho spoluúčast nepřevyšuje 5 %.
2. Poskytovatel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, a do 5 pracovních dnů od výzvy objednatele je poskytovatel povinen toto objednateli prokázat.

3. Použije-li poskytovatel při své činnosti subdodavatele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
4. Poskytovatel je povinen:
   4.1 poskytovat plnění v objektech a prostorách vymezených objednatelem, a to pouze pracovníky schválenými objednatelem,
   4.2 mít po celou dobu účinnosti této smlouvy platnou autorizaci, kterou objednatel požadoval v kvalifikačních požadavcích zadávacího řízení na předmět této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na požádání objednateli tuto skutečnost doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele,
   4.3 zajistit, aby jeho pracovníci, kteří se budou podílet na plnění této smlouvy, splňovali kvalifikační kritéria, která objednatel požadoval v kvalifikačních požadavcích zadávacího řízení na předmět této smlouvy. Poskytovatel je po dobu účinnosti této smlouvy povinen na požádání kvalifikaci jednotlivých osob objednateli doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele,
   4.4 v případě poskytování služeb prostřednictvím subdodavatele platí všechna ustanovení tohoto článku také pro subdodavatele a jeho pracovníky, kteří se budou na plnění smlouvy podílet. V případě, že poskytovatel splnil některý z požadavků stanovených objednavatelem v zadávací dokumentaci zadávacího řízení na předmět této smlouvy prostřednictvím subdodavatele, je povinen v případě změny tohoto subdodavatele na požádání objednatele prokázat, že nový subdodavatel tento požadavek splňuje, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

Objednatel si vyhrazuje právo ověřit si skutečnosti dle odst. 4.2 až 4.4 u výrobce. Nesplnění kteréhokoliv požadavku objednatele uvedeného odst. 4.2 až 4.4 je považováno za podstatné porušení smlouvy.

Článek XIII
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována výměna e-mailových či jiných elektronických zpráv. Výjimkami jsou změny pověřených osob nebo jejich kontaktních údajů dle čl.III odst. 3.
3. Práva a povinnosti vzniklé z této smlouvy mohou být postoupena pouze po předchozím písemném souhlasu druhé smluvní strany. Za písemnou formu se nepovažuje e-mail či jiné elektronické zprávy.
4. Odpověď strany této smlouvy podle § 1740 odst.3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
5. Závazkový vztah založený touto smlouvou se řídí zákonem č. 89/2012 Sb., občanský zákoník a zákonem č. 121/2000 Sb., autorský zákon,ve znění pozdějších předpisů.
6. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.

7. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak
8. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
9. Smlouva je vyhotovena ve čtyřech vyhotoveních s platností originálu, z nichž objednatel obdrží tři a poskytovatel jedno vyhotovení.

Přílohy: č. 1 – Technické požadavky objednatele
č. 2 - Technická specifikace SIEM
č. 3 - Bezpečnostní požadavky objednatele
č. 4 - Cenová tabulka

V Praze dne: 3. 6. 2014

Za objednatele:

[redacted]

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Xxrius
ředitel sekce správní

[redacted]

V Praze dne: 30. 5. 2014

Za poskytovatele:

[redacted]

Ing. Kamil Krus
jednatel

[redacted]

Miroslav Bečka
jednatel

[redacted] NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1

S&T CZ s.r.o.
Na Strži 1702/65
140 00 Praha 4
IČ: 44846029

Příloha č.1

TECHNICKÉ POŽADAVKY OBJEDNATELE

Technická kritéria požadovaná po nabízeném řešení

Preambule

Zadavatel požaduje dodávku komplexního systému, zajišťující monitoring, sběr, centrální ukládání a vyhodnocování bezpečnostních událostí ze sítě, serverů, databází, aplikací a dalších zdrojů v prostředí ČNB (dále jen „SIEM")

Popis systémového prostředí ČNB pro potřeby nasazení systému SIEM

Prostředí ČNB se skládá z fyzických serverů a virtuálních serverů na platformě VMware a Oracle VM, z fyzických a virtuálních pracovních stanic, síťových prvků HP a Cisco a dalších zařízení.

Virtuální pracovní stanice

Virtuální pracovní stanice zadavatel provozuje jako terminálové servery s operačním systémem Windows 2008 R2 a Citrix XenApp 6.5. Proces sestavení jednotlivých serverů je řízen Provisioning Services – jednotlivý terminálový server je každý den vytvářen z master (golden) image.

Autentizace

U informačních systémů ČNB je realizována funkce Single Sign-On s využitím služby Microsoft Active Directory (autentizační protokol Kerberos). Uživatel se autentizuje pouze do domény CNB, pomocí certifikátu uloženého na čipové kartě.

SW čipové karty SAC a čipové karty typu 330u, 400 a 4100 dodává firma SafeNet

Při vyvolání libovolné aplikace již pak není zadávání jména/hesla nutné, ani žádná další autentizace uživatele není požadována.

SAN
Základ SAN tvoří Fibre Channel Directory/Switche Cisco MDS 9509

Použité zkratky a vysvětlení pojmů:

- **HTP** - hlavní technologické pracoviště (**Na Příkopě 28, Praha 1**)
- **ZTP** - záložní technologické pracoviště (**Strojírenská 175, Praha 5**)
- **SIEM** – kompletní systém, zajišťující sběr, centrální ukládání a vyhodnocování bezpečnostních událostí ze sítě, serverů a dalších zdrojů. Zahrnuje všechny komponenty pro Log Management, Event management, pokročilá korelace (korelace z více zdrojů), příjem a sběr logů, centrální správu a reporting, a to včetně vlastních logů
- **Log záznam** - řádek v logu resp. jeden záznam před zpracováním (RAW formát)
- **Zdroje** – jsou jednotlivá zařízení, která posílají bezpečnostní logy do systému SIEM (servery, Databáze, aplikace, atd.)
- **Auditní log systému** – je vlastní auditní log systému SIEM
- **EPS** – počet záznamů/sec

- **Parsování** –proces, při kterém je zpracován log záznam. Jsou z něj vybírány údaje a ukládány v jednotném formátu do Databáze. Tyto údaje jsou doplněny o další známé skutečnosti
- **AD** – Active directory

Čl. I. Požadavky na dodaný systém (dále jen systém SIEM)

1. Obecné požadavky na systém SIEM:

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 režimu vysoké dostupnosti tak, aby nedošlo ke ztrátě sbíraných Log záznamů v případě výpadku některé komponenty. Tato funkcionalita musí být zajištěna automaticky.

1.4. Systém umožňuje zasílání log záznamů do více lokalit najednou (HTP, ZTP) zároveň musí poskytovat možnost automatického zasílání logů do sekundárního umístění, pokud je primární lokalita nedostupná. Obě lokality musí být okamžitě v reálném čase přístupné při zachování plné funkcionality.

1.5. Každé dodávané zařízení musí:
- obsahovat min. 2 redundantní napájecí zdroje
- být montovatelné do standardního 19" technologického stojanu 800x1000mm (1U či 2U velikost)
- obsahovat montážní sadu pro instalaci do technologického stojanu, tak aby byla zajištěna snadná manipulace bez použití dodatečných nástrojů
- mít připojení ke dvěma samostatným zdrojům napájení 230V, délka kabelů min. 2m
- obsahovat min. 2x LAN port, každý alespoň 1Gbit / s
- mít synchronizovaný čas z NTP

1.6. Součástí dodávky systému SIEM musí být připojení na externí SAN úložiště s rychlostí alespoň 4Gbit/s. Připojení bude sloužit jako externí a archivační storage pro logy a data.

1.7. 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 Internet exploreru 8.0 a novějších.

1.8. Centrální správa systému SIEM musí podporovat GUI (Grafické uživatelské rozhraní), a skriptovací nástroje

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

1.10. Správa uživatelů systému SIEM musí být integrovatelná s MS Active Directory, tj.
a) systém k přihlášení využívá doménové účty s využitím SSO (web SSO), pro uživatele autentizované čipovou kartou (autentizační protokol Kerberos). nebo
b) přihlášení pomocí certifátu uloženého na čipové kartě ČNB.

1.11. Systém SIEM musí rovněž umožňovat přihlašování pomocí lokálních účtů

1.12. Přístup uživatelů musí být založen na volně definovaných oddělených rolí s možností granulárního přidělování práv v rámci role podle zdrojů logů, skupinu zařízení, jednotlivých serverů, typu logu a pod.

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

1.14. Systém SIEM musí zaznamenávat vlastní auditní logy po nastavitelnou dobu a musí být chráněny proti modifikaci.
1.15. Systém SIEM musí poskytovat informace při vlastním běhu a vyhodnocování logů
1.16. Systém SIEM podporuje monitorování vlastní dostupnosti a jeho jednotlivých částí (zařízení) prostřednictvím SNMP v2/v3 nebo logováním na vzdálený syslog server
1.17. Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel
1.18. Systém musí obsahovat plně integrovaný nástroj pro řízení celého životní cyklu incidentu, který podporuje nezávislé fronty.

2. Požadavky na výkonnost, škálovatelnost a licenci:

2.1. Systém SIEM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat
2.2. Systém SIEM musí mít garantovanou licenci pro zpracování min. 1000 EPS v denních špičkách
2.3. Komponenta sbírající logy, musí být schopna trvale zpracovávat 3000 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení
2.4. Systém SIEM musí být schopný nárazově (minimálně po dobu 72h) zpracovat 7 000 EPS, bez jakýchkoliv výkonnostních nebo licenčních omezení, včetně zachování plné funkcionality u všech komponent
2.5. Licence pro centrální prvek musí být rozšiřitelná na 3000 EPS v průměru (sustained EPS) bez nutnosti upgradu HW, jen pomocí aktivace licence
2.6. Systém SIEM nesmí technicky limitovat počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, tak aby nedošlo k jejich zahození
2.7. Kapacita úložného prostoru:
- Systém SIEM musí na každém pracovišti objednavatele umožnit interně uložit log záznamy (RAW formát) po dobu min. 13 měsíců
- Systém SIEM musí umožnit interně uchovat normalyzované log záznamy po dobu min. 13 měsíců

2.8. Systém SIEM musí umožňovat rozšiřování kapacity a výkonu formou distribuce zátěže na více samostatných systémů např. více Logserverů s jedním centrálním místem pro vyhodnocování (event management).
2.9. Systém SIEM musí podporovat současnou práci min. 10 uživatelů
2.10. Licence musí obsahovat možnost minimálně 1700 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje,atd)
2.11. Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů a vlastních custom logů

3. Požadavky na sběr dat

Vrstva sběru logů musí splňovat:
3.1. Musí být funkčně i technicky oddělena od ostatních částí systému SIEM
3.2. Musí být funkční samostatně bez centrálního prvku
3.3. Nesmí nijak zasahovat do sbíraných systémů a sběr logů musí probíhat vzdáleně pro všechny zdroje (bezagentní sběr)
3.4. Musí podporovat (sbírat, zpracovat a interpretovat) následující typy logů a protokolů: Syslog, SNMP Trap v2/v3, jedno a víceřádkové textové logy (včetně "custom logs "),

Windows Event Logs (včetně" custom Event logs "), agentless Windows, ODBC (logy v DB tabulkách), sdee, CheckPoint LEA, ftp, ssh, scp, http, sftp, nfs, cifs, Time Based DB, file, xml, cef, netflow V5 a V9

3.5. Musí podporovat sběr událostí ze síťových zařízení a jejich parsování za účelem identifikace útoků na L3 a L2 vrstvu (minimálně Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard)

3.6. Musí podporovat načítání log souborů, kde tyto soubory budou mít stanovenu strukturu a význam dat

3.7. Musí podporovat načítání logů z databáze (zejména MS SQL a Oracle), kde tyto logy budou mít stanovenu strukturu a význam dat

3.8. Musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů

3.9. Navržené technologie nesmějí být limitujícím faktorem při detekci neúspěšných nebo chybějících přenosů logů do systému SIEM ani stavu, když neznámé zařízení začne posílat logy (podvrhy), tj. v případě použití agentů navrženého systému toto musí být detekovatelné a pod.

3.10. Komponenta sbírající logy je posílá dále zašifrované a komprimované a umožňuje regulovat šířku užívaného pásma.

4. Požadavky na zpracování událostí

Systém SIEM musí umožňovat:

4.1. používání regulárních výrazů na straně agentů (pokud budou využity) i serveru systému SIEM

4.2. normalizaci bezpečnostních událostí v systému SIEM do jednotného formátu (centrální logy musí mít stejný formát ze všech zdrojů) a doplnění o další detailní informace (např. doplnění jména uživatele na základě uživatelského účtu apod.).

4.3. 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

4.4. Vyhodnocovat i vlastní provozní logy

4.5. Zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem.

4.6. Export a import pravidel i log parserů.

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

4.8. Real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému)

4.9. Korelaci událostí dávkově importovaných do systému SIEM tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů.

4.10. Automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací

4.11. Vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době a pod.) nebo datových tocích (např. neobvyklé toky dat)

4.12. Zpracovávat výsledky skenu zranitelností minimálně ze systému Qualys Guard, kdy si systém SIEM automaticky v nastaveném intervalu stáhne výsledky skenu zranitelností prostřednictvím Qualys API
4.13. Agregace událostí v systému SIEM do jedné události po definovaném čase
4.14. 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
4.15. Na jakoukoliv událost musí být možné navázat automatickou akci
- notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje a pod.
- spuštění externího skriptu

4.16. 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
- Předdefinované analytické nástroje a akce pro identifikaci hrozeb a obranu vůči nim

4.17. Musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí:
- Útoky robotů, červů a virů (chyby antivirů)
- Monitorování databází (Chyby a varování, přístupy do DB, konfigurace)
- Neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace)
- Chyby a změny v sítích (chyby a stavy síťových zařízení)
- Monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma)
- VPN útoky (chyby při ověřování, změny konfigurace, aktivita připojování)
- Compliance Reporting pro různé stupně regulací
- Uchvácení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace

5. Požadavky na archivaci a ukládání

Systém SIEM musí umožňovat:
5.1. připojení na dedikované externí úložiště bezpečnostních událostí prostřednictvím SAN
5.2. interně uchovat data bez ztráty informací, tzv. RAW logy (bez filtrace, normalizace, redukce) po dobu minimálně 13 měsíců
5.3. interně uchovat normalizované log záznamy po dobu min. 13 měsíců
5.4. ukládání dat v komprimované podobě pro úsporu diskové kapacity
5.5. automaticky archivovat a zálohovat RAW logy podle nastavených požadavků
5.6. Systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu
5.7. Systém musí umožňovat rychlou obnovu uložených logů pro případ obnovy systému po eventuální havárii
5.8. Systém musí poskytovat mechanismus detekce neautorizovaných změn dat v souborech systému SIEM

5.9. Zajištění autenticity a integrity archivačních souborů (např. digitálním podpisem a pod.)
5.10. Systém SIEM musí splňovat některou z mezinárodních certifikací, které garantují bezpečné a nezpochybnitelné ukládání logů
5.11. Filtrování událostí před archivací
5.12. Systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště resp. archivu podle definovaných pravidel

6. Požadavky na reporting a interpretaci dat

6.1. Předdefinované reporty systému SIEM a musí být modifikovatelné
6.2. Systém SIEM musí poskytovat reporty i ve formě grafů a tabulek
6.3. Systém SIEM vytváří reporty ve formátech PDF, HTML a CSV, popř. dalších
6.4. Systém SIEM musí umožňovat export dat ve formátu XML nebo CSV
6.5. Systém SIEM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.
6.6. Systém musí poskytovat report o aktivitách vybraných uživatelů resp. skupiny uživatelů
6.7. Systém musí mít optimalizovanou databázi logů pro rychlé prohledávání a reportování (indexace).
6.8. Systém musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzv.. raw-message
6.9. Systém SIEM musí poskytovat pro každého uživatele vlastní personalizovaný dashboard
6.10. 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 / lozích / zdrojů na daném hostu apod.).
6.11. 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
6.12. Systém SIEM musí podporovat grafickou interpretaci vzorků standardního a nestandardního chování (včetně real-time režimu).

Čl. II. Požadavky na integraci

Objednatel 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. Pro všechny uvedené systémy musí fungovat všechny definované vlastnosti, které SIEM nabízí. Výsledný formát logů (i korelovaných událostí) musí být jednotný a musí být možné tyto logy přečíst mimo SIEM .

Požadované zdroje:

1. Systém SIEM musí plnohodnotně podporovat a integrovat NetFlow (V5, V9), např. NetFlow analyzer exportuje alerty do systému SIEM, který tyto podporuje a následně dále zpracovává
2. Systém SIEM musí podporovat integraci následujících operačních systémů a služeb:
    a. Microsoft Windows Server 2003 a vyšší
    b. Microsoft Windows XP a vyšší
    c. Linux (Red Hat Enterprise Linux 5.8 a vyšší)
    d. VMware ESX 4.0 a vyšší
    e. Oracle VM 3.2 a vyšší
    f. HP-UX B 11.23 a vyšší
    g. IBM AIX 6 a vyšší
    h. Služby Active Directory
    i. Služby sdílení souborů MS Windows
    j. Služby MS PKI 2008
    k. IIS Web Server
    l. DNS na platformě Microsoft
    m. DNS (bind 9.x a vyšší)
    n. DHCP na platformě Microsoft
    o. DHCP (Internet Systems Consortium)(Linux)
3. Systém SIEM musí podporovat integraci následujících aplikací a informačních sytémů:
    a. Oracle 10 a vyšší
    b. MS SQL 2005 a vyšší
    c. MS WSUS
    d. MS Exchange 2010
    e. Mail Marshal SMTP 7.1.1
    f. Apache 2.2 a vyšší
    g. VMware vCenter Server version 4.1 a vyšší
    h. MS System Center Configuration Manager
    i. SWIFT (SW pro mezibankovní komunikaci)
    j. BlackBerry Enterprise Server 4.1 a vyšší
    k. AV Symantec 12.1
    l. VPN CAG 9.3 (Citrix access gateway)
    m. Citrix NetScaler 10 a vyšší
    n. ISA 2006 a vyšší
    o. Cyber-Ark PIM/PSM 7.2 a vyšší
    p. CMS MYiD 8.0 a vyšší
    q. Qualys guard VM 7.10 / WAS 3.0 a vyšší (vulnerability management/Web application scaning
    r. Citrix Provisioning server 6.1 a vyšší
    s. Citrix Web interface 5.4 a vyšší
    t. Xen App 6.5 a vyšší
    u. Appsense management 8 a vyšší (application manager, performence manager)
    v. Oracle IRM
    w. Oracle Weblogic 10 a vyšší
    x. Oracle Business Intelligence 10 a vyšší
    y. Oracle Application Server 10 a vyšší
    z. HSM modul *
    aa. Invea FlowMon ADS Business *
    bb. HP Data protector

cc. Storage Hitachi ASM 2100, Hitachi USP-V, Dell MD-1220, IBM DS-3524
dd. Firewall Checkpoint R75.40/ R75.45 a vyšší (včetně IPS)
ee. Síťové prvky Cisco VSS 1440

*- zdroj bude pravděpodobně pořízen v průběhu roku 2014

Příloha č. 2

Technická specifikace SIEM řešení

Navrhované technické řešení splňuje všechny požadované vlastnosti v příloze č.1

Technická specifikace SIEM řešení

1. Seznam dodávaného hardware

1.1. HP ArcSight Express server AE-7511

a. HP ProLiant DL380P G8 Server
b. Red Hat Enterprise Linux 6 64-bit
c. 2x Intel Xeon ES-2650 2.0 GHz 8-core
d. RAM 64 GB, 1 600 MHz RAM
e. 6x 600 GB 6G SAS 15K rpm (1.8 TB RAID 10)
f. Rack mount 2U
g. 2x 750W CS platinum power supply
h. 29.5" x 17.54" x 3.44"
i. iLO 4 advanced remote management

1.2. HP ArcSight Logger L3500

a. HP ProLiant DL380P G8 Server
b. Red Hat Enterprise Linux 6 64-bit
c. 1x Intel Xeon ES-2620 2.0 GHz 6-core
a. RAM 32 GB, 1 600 MHz RAM
b. 4x 500 GB 6G SATA 7.2K rpm (1.5 TB RAID 5)
c. Rack mount 1U
d. 2 x 460 W CS platinum power supply
e. 27.5" x 17.1" x 1.7"
f. iLO 4 advanced remote management

2. Seznam dodávaných licencí

2.1. HP ArcSight Express server AE-7511

a. 1000 peak EPS (licenčně rozšiřitelné na 15000 peak EPS, bez změny hardware)
b. 26 uživatelských licencí na konzole
c. 50 Identity view pro administrátory
a. iLO 4 advanced remote management

2.2. HP ArcSight Logger L3500

a. 2000 EPS
b. Neomezený počet uživatelských licencí na konzole
c. iLO 4 advanced remote management

2.3. Software konektory pro sběr logů

d. Neomezený počet typů připojených zdrojů
e. Všechny typy standardně podporovaných zdrojů bez omezení
f. Neomezený počet softwarových konektorů
g. FlexKit - neomezený počet připojených vlastních aplikací z zdrojů logů

Příloha č. 3

Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB") budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu, schváleném ČNB (dále jen „seznam"). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději v den podpisu smlouvy.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti pracovníků poskytovatele. Součástí seznamu je,, Prohlášení o získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů". Poskytovatel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu vydali souhlas se zpracováním osobních údajů Českou národní bankou v rozsahu: jméno, příjmení a číslo průkazu totožnosti. Důvodem předání těchto osobních údajů je zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB.
3. Požadavky na případné doplňky a změny schváleného seznamu pracovníků poskytovatele je nutno neprodleně oznámit ČNB. Případné doplňky a změny podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
4. Při příchodu do objektů ČNB pracovníci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny na seznamu, nebudou do objektu ČNB vpuštěny.
5. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostorů ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.
6. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem.
7. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
8. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
9. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
10. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací, dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či zcizení majetku ČNB, a dále zdržet se nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
11. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifikami daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární

ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka poskytovatele uvedeného na seznamu z dodržování těchto předpisů a ustanovení.

Příloha č.4

CENOVÁ TABULKA

Dodávka komplexního systému SIEM

Komponenta	Název komponenty	Počet ks	Jednotková cena v Kč bez DPH	Celková cena v Kč bez DPH
Dodávka technických prostředků SIEM (dle čl. I odst.1 smlouvy)				
HW 1	HP ArcSight L3500 Server	1,00	123 800,00	123 800,00
HW 2	HP ArcSight Express Server	1,00	447 000,00	447 000,00
Dodávka programových prostředků SIEM včetně licencí (dle čl. I odst.1 smlouvy)				
SW 1	HP ArcSight L3500 Licence	1,00	279 300,00	279 300,00
SW 2	HP ArcSight AE-7511 Licence	1,00	996 800,00	996 800,00
SW 3	HP ArcSight FlexConnect Kit SW	1,00	119 700,00	119 700,00
Analýza a implementace SIEM (dle čl. II odst.1a a 1b smlouvy)		1		895 000,00
Dodávka dokumentace (dle čl. II odst.1b smlouvy)		1		52 000,00