Příloha č. 1 smlouvy

Kupní smlouva č. CTU/2019_021

uzavřená ve smyslu ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

I. Smluvní strany

Kupující:	**Česká republika – Český telekomunikační úřad**
Se sídlem:	Sokolovská 58/219, Praha 9 - Vysočany
Doručovací adresa:	poštovní přihrádka 02, 225 02 Praha 025
IČO:	701 06 975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
Bankovní spojení	xxxxxxxxxxxxxxxxxxxx
Číslo účtu:	xxxxxxxxxxxxxxxxxxxx

Jejímž jménem jedná: Ing. Mgr. Jaromír Novák, předseda Rady ČTÚ

(dále jen **„kupující“**)

a

Prodávající:	**IXPERTA s.r.o.**
Se sídlem:	Lihovarská 1060/12, Libeň, 190 00 Praha 9
IČO:	275 99 523
DIČ:	CZ27599523
Zastoupena:	Pavlem Šiprem, jednatelem společnosti
Bankovní spojení:	xxxxxxxxxxxxxxxxxxxxxx
Číslo účtu:	xxxxxxxxxxxxxxxxxxxxxx

Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka C117991

(dále jen **„prodávající“**)

II. Úvodní ustanovení

Smluvní strany uzavírají tuto kupní smlouvu (dále jen „smlouva“) na základě výsledků zadávacího řízení v rámci veřejné zakázky na dodávky s názvem „Management bezpečnostních informací a událostí, server a přepínače “.

III. Účel a předmět smlouvy, závazky smluvních stran

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě dojde k realizaci dodávky systému SIEM (Security Information and Event Management), serveru a přístupových přepínačů (switchů), implementaci SIEMu a dalších služeb včetně garance dostupnosti náhradních dílů po dobu účinnosti této smlouvy. Plnění této smlouvy bude součástí informačního systému MSEK (Měřicí systém elektronických komunikací), jakožto významného informačního systému kupujícího, podléhajícího zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
2. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu do místa plnění podle čl. V odst. 1 této smlouvy systém SIEM, 1 ks serveru a 2 ks přístupových přepínačů (switche), vše nové, tj. nepoužité, nepoškozené, nerepasované a zkompletované) a v souladu s technickou specifikací uvedenou v příloze č. 1 této smlouvy, poskytnout kupujícímu související plnění podle této smlouvy a převést na kupujícího vlastnické právo

k systému SIEM, serveru a přístupovým přepínačům (switchům), na druhé straně závazek kupujícího za řádně a včas dodaný systém SIEM, server a přístupové přepínače (switche) zaplatit prodávajícímu sjednanou kupní cenu. Součástí plnění musí být také veškeré potřebné licence k provozu HW a SW prvků podle parametrů uvedených v technické specifikaci (příloha č. 1 této smlouvy), kdy žádný parametr uvedený v technické specifikaci nebude licenčně omezen a pokud případně ano, musí být licence opravňující kupujícího užívat plnění bez omezení součástí plnění této smlouvy, a to v souladu s čl. IX, resp. čl. XI odst. 10 a 11 této smlouvy.

IV. Cena a platební podmínky

1. Prodávající se zavazuje poskytnout kupujícímu plnění podle této smlouvy za cenu ve výši 2.488.062,08 Kč bez DPH (dále jen „kupní cena“).
2. Ke kupní ceně bude připočtena DPH ve výši platné ke dni uskutečnění zdanitelného plnění. Celková kupní cena uvedená v této smlouvě je sjednána dohodou smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a je stanovena jako konečná, pevná a nepřekročitelná. Kupní cena může být změněna pouze v případě změn sazby daně z přidané hodnoty.
3. Kupní cena zahrnuje veškeré náklady související s plněním této smlouvy.
4. Kupní cena bude uhrazena bezhotovostním převodem na bankovní účet prodávajícího uvedený v záhlaví této smlouvy, a to na základě daňového dokladu – faktury (dále jen „faktura“) vystaveným prodávajícím po převzetí systému SIEM, serveru a přístupových přepínačů (switchů) kupujícím a provedení veškerých souvisejících požadovaných činností (tj. instalace, implementace, předání dokumentace, zaškolení a dalších činností dle technické dokumentace) prodávajícím, výjimkou jsou činnosti související s následným provozem (bezpečnostní audit a dodatečné změny nastavení).
5. Prodávající vystaví fakturu ke dni uskutečnění zdanitelného plnění, kterým je den protokolárního předání a převzetí plnění v podobě dodání systému SIEM, serveru, přepínačů a poskytnutí souvisejících plnění podle této smlouvy. Splatnost faktury je 30 dnů ode dne jejího doručení kupujícímu. Faktura musí být doložena kopiemi zástupcem kupujícího podepsaných dodacích listů k systému SIEM, serveru a přístupovým přepínačům (switchům) a akceptačního protokolu podle čl. VI odst. 7 této smlouvy.
6. Faktura musí obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, § 435 občanského zákoníku a současně číslo této smlouvy, včetně uvedení označení „MSEK“.
7. V případě, že faktura nebude obsahovat náležitosti podle platných právních předpisů, popř. bude obsahovat jiné chyby či nedostatky, je kupující oprávněn fakturu vrátit, přičemž nová lhůta splatnosti počíná běžet dnem doručení opravené faktury kupujícímu.

V. Místo a čas plnění, způsob plnění, kontaktní osoba

1. Místem plnění je Datové centrum DC TOWER – České Radiokomunikace, Mahlerovy sady 2699/1, 130 00 Praha 3 – Žižkov.
2. Kontaktní osobou pro převzetí systému SIEM, serveru a přístupových přepínačů (switchů) na straně kupujícího v místě plnění je Ing. xxxxx xxxxx, tel.: xxx xxx xxx, e-mail: xxxxxxxx@ctu.cz.
3. Prodávající se zavazuje, že dodá systém SIEM, 1 ks serveru a 2 ks přístupového přepínače (switche), včetně potřebných licencí na software (SW), provede instalaci hardware (HW) prvků v datovém centru, provede konfiguraci přepínačů, tak aby mohly být

ihned začleněny do již existující síťové struktury a instalaci SW appliance (SIEM) v prostředí VMware, nejpozději do 45 dnů ode dne účinnosti této smlouvy.

4. Od data převzetí plnění dle odstavce 3 tohoto článku smlouvy má dodavatel maximálně 45 dnů na provedení dalších činností podle technické dokumentace (implementace zdrojů logů, dokumentace všech dodaných prvků, zaškolení). Po ukončení souvisejících činností má kupující lhůtu 15 pracovních dnů na dotazy a připomínky ohledně implementace, dokumentace a funkčnosti systému. Prodávající je povinen se připomínkami a dotazy kupujícího zabývat a řešit.
5. SIEM, server a přístupové přepínače (switche) budou prodávajícím instalovány v místě plnění v prostorech Datového centra. Místo plnění je pak i místem plnění ve vztahu ke sjednané záruce (NBD).

VI. Dodací podmínky

1. Prodávající se zavazuje nejméně tři pracovní dny předem písemně, nebo elektronicky uvědomit kontaktní osobu kupujícího o předpokládaném termínu dodání systému SIEM, serveru a přístupových přepínačů (switchů) podle čl. V odst. 3 této smlouvy. Kupující pak zajistí přístup do místa instalace.
2. Řádné dodání systému SIEM, serveru a přístupových přepínačů (switchů), včetně potřebných licencí a jejich následné instalace podle čl. V odst. 3 této smlouvy potvrdí prodávajícímu formou podpisu předávacího protokolu kontaktní osoba kupujícího.
3. Kupující není povinen převzít systém SIEM, server a přístupové přepínače (switche) zejména v případech, kdy komponenty, případně jejich obal, vykazuje známky poškození, resp. systém SIEM, server a přístupové přepínače (switche) vykazují vady, které brání jejich řádnému užívání.
4. Prodávající je povinen společně se systémem SIEM, serverem a přístupovými přepínači (switchi) předat kupujícímu doklady, jež jsou nutné k převzetí a užívání systému SIEM, serveru a přístupových přepínačů (switchů) podle občanského zákoníku a předpisů souvisejících, v českém jazyce. Současně je prodávající povinen předat kupujícímu i podrobný původní uživatelský manuál v českém, nebo anglickém jazyce.
5. Veškerá požadovaná dokumentace a manuály související s plněním této smlouvy a technickou specifikací bude předána v elektronické podobě na USB flash disku, výjimkou mohou být dokumenty u kterých je předání v elektronické podobě nemožné, nebo komplikované, jako jsou například některé licence. Takové dokumenty mohou být předány i v listinné podobě.
6. Kupující je povinen převzít plnění, které je poskytnuto řádně, tj. systém SIEM, server a přístupové přepínače (switche) zejména vykazují všechny vlastnosti a vyhovují všem podmínkám uvedeným v této smlouvě či stanoveným kupujícím nebo právními předpisy a technickými normami, a včas.
7. Řádné provedení implementace systému SIEM, zaškolení správců, předání dokumentace serveru a přístupových přepínačů (switchů), včetně poskytnutí všech souvisejících plnění podle této smlouvy podle čl. V odst. 4 bude potvrzeno prodávajícímu formou podpisu akceptačního protokolu kontaktní osobou kupujícího.

VII. Zajištění závazků

1. Pro případ prodlení kupujícího s uhrazením ceny ve smyslu čl. IV odst. 5 této smlouvy má prodávající právo požadovat úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení.
2. V případě prodlení prodávajícího s řádným plněním (dodání, instalace a implementace systému SIEM, serveru a přístupových přepínačů (switchů) včetně potřebných licencí,

a poskytnutí všech souvisejících plnění podle této smlouvy) je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny včetně DPH za každý i započatý den prodlení.

3. V případě nesplnění závazku prodávajícího týkajícího se garance možnosti časového prodloužení licencí podle čl. IX odst. 2 této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 100.000 Kč za každý jednotlivý případ.
4. V případě prodlení prodávajícího s odstraněním ohlášené vady systému SIEM, serveru a/nebo přístupových přepínačů (switchů) podle čl. X této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,1 % z kupní ceny včetně DPH za každý i započatý den prodlení.
5. V případě nesplnění závazku prodávajícího týkajícího se garance dostupnosti náhradních dílů podle čl. X odst. 5 této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ.
6. V případě, že prodávající řádně a včas neprovede bezpečnostní audit nebo následné konzultace auditu podle čl. XI odst. 2 této smlouvy, nebo bezpečnostní audit nebude výsledkem práce bezpečnostního specialisty, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 15.000 Kč za každý jednotlivý případ.
7. V případě, že prodávající řádně a včas nezajistí splnění povinnosti podle čl. XI odst. 3 této smlouvy, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 15.000 Kč za každý neposkytnutý člověkoden.
8. V případě nesplnění závazku prodávajícího podle čl. XI odst. 4, 5, 6 nebo 7 této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ.
9. V případě nesplnění závazku prodávajícího týkajícího se garance aktualizace SW podle čl. XI odst. 10 nebo 11 této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ.
10. V případě porušení jiné povinnosti prodávajícího zakotvené touto smlouvou je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 500 Kč za každý jednotlivý případ.
11. Smluvní pokuta je splatná ve lhůtě 5 dnů ode dne doručení písemné výzvy k její úhradě.
12. Zaplacením smluvní pokuty podle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci. Uplatněním nároku na smluvní pokutu ani jejím skutečným uhrazením nezaniká povinnost zavázané strany splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

VIII. Nebezpečí škody a nabytí vlastnického práva

Nebezpečí škody a vlastnické právo k systému SIEM, serveru a přístupovým přepínačům (switchům) přechází z prodávajícího na kupujícího okamžikem, kdy kupující převezme systém SIEM, server a přístupové přepínače (switche) a potvrdí převzetí systému SIEM, serveru a přístupových přepínačů (switchů) způsobem uvedeným v čl. VI odst. 7 této smlouvy.

IX. Práva k duševnímu vlastnictví

1. Prodávající poskytuje kupujícímu nevýhradní licenci či licence k užití plnění v souladu s touto smlouvy, případně s obvyklému účelu, časově omezenou v souladu s čl. XI odst. 10, resp. 11 smlouvy, územně určenou min. pro území České republiky.
2. Prodávající garantuje kupujícímu, že pro dodaný SW SIEM bude možné prodloužení všech licencí o minimálně dalších 5 let nad časové omezení podle čl. XI odst. 10 smlouvy, přičemž prodávající nijak neomezuje možnost prodloužení licence (licencí)

prostřednictvím jiného subjektu, například u výrobce, nebo jiného partnera výrobce dodaného SW SIEM.

X. Záruka a odpovědnost za vady

1. Prodávající odpovídá za vady a chybnou konfiguraci dodaného systému SIEM, serveru a přístupových přepínačů (switchů).
2. Na veškeré dodávané HW komponenty (server a přístupové přepínače) poskytuje prodávající kupujícímu záruku za jakost v délce 60 měsíců. Záruční doba počíná běžet dnem převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy. Záruční doba se prodlouží o dobu, po kterou nebude moci kupující užívat některý z dodaných prvků z důvodu vad, za něž odpovídá prodávající, a to ode dne oznámení kupujícího o vadě prodávajícímu do dne ukončení servisního zásahu podle odstavce 7 tohoto článku smlouvy.
3. Na dodávaný systém SIEM poskytuje prodávající kupujícímu záruku za jakost v délce 36 měsíců. Záruční doba počíná běžet dnem převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy. Záruční doba se prodlouží o dobu, po kterou nebude moci kupující užívat některý z dodaných prvků z důvodu vad, za něž odpovídá prodávající, a to ode dne oznámení kupujícího o vadě prodávajícímu do dne ukončení servisního zásahu.
4. Záruka se vztahuje na výrobní vady a na vady vzniklé při běžném používání systému SIEM, serveru a přístupových přepínačů (switchů).
5. Prodávající poskytuje kupujícímu garanci dostupnosti veškerých náhradních dílů minimálně po dobu 3 let po ukončení záruky.
6. Záruka se nevztahuje na vady vzniklé v důsledku živelné události, zásahu vyšší moci, zásahu nepovolané osoby, na závady vzniklé úmyslným poškozením, neodbornou manipulací nebo nedodržením návodu k obsluze.
7. Prodávající poskytuje kupujícímu na veškeré dodávané HW komponenty výrobcem garantovaný záruční servis s garancí ukončení servisního zásahu nejpozději následující pracovní den po nahlášení vady v místě instalace (NBD). Záruční servis zahrnuje náklady na náhradní díly, dopravu, čas a práci technika.
8. Vady budou hlášeny pověřenými zaměstnanci kupujícího prodávajícímu telefonicky na linku „xxx xxx xxx – Hot-line“ nebo písemně na e-mail xxx@xxx.xx. Prodávající se zavazuje, že v případě změny telefonního čísla nebo e-mailové adresy bude kupujícího řádně, včas a prokazatelným způsobem informovat o této změně.
9. Prodávající se zavazuje, že ke dni převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy poskytne kupujícímu možnost sledování servisních reportů prostřednictvím internetu.
10. Kupující se zavazuje, že zajistí servisnímu technikovi podmínky pro provádění servisu (přístup do místa instalace plnění).

XI. Další práva a povinnosti smluvních stran, součinnost

1. Prodávající se zavazuje, že kupujícímu poskytne ke dni převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy možnost prostřednictvím Internetu bezplatně stahovat ovladače a manuály pro dodaný systém SIEM, server a přístupové přepínače (switche).
2. Prodávající se zavazuje k poskytnutí služby bezpečnostních auditů po dobu 24 měsíců ode dne převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy. V rámci této služby musí dodavatel jednou za dva měsíce poskytnout kupujícímu bezpečnostní report z platforem SIEM a Check Point Smart Event a Smart Log ve vlastnictví kupujícího. První bezpečnostní audit, bude proveden 2 měsíce po předání řešení do vlastnictví kupujícího.

Celkově se bude jednat o 12 bezpečnostních auditů. Bezpečnostní report musí obsahovat informace uvedené v technické specifikaci. Bezpečnostní report je produktem pracovní aktivity bezpečnostního specialisty a nejedná se pouze o export dat ze SIEMu či jiné technické platformy. Prodávající je povinen každý takový report s kupujícím projít a navrhnout kupujícímu bezpečnostní opatření k zajištění nápravy zjištěných událostí. Prodávající se zavazuje, že nejpozději 14 dní před vyhotovením prvního auditu, předloží kupujícímu vzorový anonymizovaný audit, a projedná se zástupcem kupujícího případné připomínky k navrženému rozsahu a způsobu provedení bezpečnostního auditu.

3. Součástí plnění této smlouvy jsou také dodatečné práce techniků v rozsahu 12 člověkodnů („Man-day“), které kupující bude moci čerpat na dodatečné práce na systému SIEM (změny nastavení, zavádění nových logů). Na vyčerpání těchto 12 člověkodnů má kupující 24 měsíců ode dne převzetí plnění kupujícím podle čl. VI odst. 7 této smlouvy. Kupující, bude prodávajícího informovat předem o požadavcích na práci technika. Prodávající pak musí ve lhůtě 5 pracovních dnů zajistit technika na požadovanou činnost na systému SIEM. Prodávající také musí informovat kupujícího o každém již vyčerpaném člověkodni. Jeden člověkoden odpovídá 8 hodinám práce technika.

4. Kupující umožní prodávajícímu nezbytný přístup do systému MSEK pro potřeby implementace a vytváření bezpečnostního auditu. Tento přístup bude poskytnut jen konkrétním osobám určeným prodávajícím, které budou v pracovněprávním poměru s prodávajícím. Prodávající bude prokazatelným způsobem informovat kupujícího o jménech a pracovní pozici těchto osob. Prodávající odpovídá za to, že jím určené osoby neposkytnou svůj přístup do systému MSEK jiným osobám (včetně ostatních zaměstnanců prodávajícího). Prodávající je povinen neprodleně informovat kupujícího, pokud dojde k podezření o odcizení, či zneužití přístupových oprávnění, případně informovat kupujícího o ukončení pracovně pracovního poměru s osobami, kterým byl poskytnut přístup do systému MSEK.

5. Prodávající se zavazuje, že neposkytne bez souhlasu prodávajícího žádné informace třetím stranám ohledně plnění této smlouvy, včetně informací vyplývající z bezpečnostních reportů, konfigurace, zapojení a také informací ohledně systému MSEK, které mohl zjistit při instalaci a konfiguraci ohledně jiných prvků, které nejsou součástí plnění této smlouvy. Zároveň se prodávající zavazuje, že bude uchovávat citlivé informace ohledně plnění této smlouvy, jako jsou logy, konfigurace, topologie, bezpečnostní audity, jen po nezbytně nutnou dobu, potřebnou pro řádné a efektivní plnění této smlouvy, nebo pro potřeby zlepšení kvality bezpečnostních reportů. Veškeré takové informace je také prodávající povinen chránit proti odcizení, či zneužití. Bezpečnostní audit sestavený prodávajícím a veškeré logy jsou majetkem kupujícího.

6. Kupující má právo jednou za kalendářní rok, po dobu plnění podle odstavce 2 a 3 tohoto článku smlouvy, provést zákaznický audit u prodávajícího; předmětem takového zákaznického auditu bude kontrola, jakým způsobem vzniká bezpečnostní audit, jakým způsobem pracují technici a jestli jsou dodržována bezpečnostní pravidla pro přístup do systému kupujícího. Kupující upozorní prodávajícího nejméně 5 pracovních dnů dopředu o záměru provést zákaznický audit. Při zákaznickém auditu musí být přítomni alespoň někteří technici sestavující bezpečnostní audit a alespoň někteří technici pracující na konfiguraci a změnách nastavení dodaného řešení SIEM.

7. Prodávající je povinen informovat kupujícího o případném bezpečnostním incidentu souvisejícím s plněním této smlouvy. V případě závažného bezpečnostního incidentu, jehož povaha může mít další vliv na bezpečnost systému, či integritu dat musí prodávající informovat kupujícího neprodleně telefonicky na kupujícím určenou osobu. O každém bezpečnostním incidentu souvisejícím s plněním této smlouvy je prodávající také povinen informovat kupujícího elektronicky e-mailem, a to nejpozději do 24 hodin. Kontaktní osobou pro hlášení bezpečnostních incidentů je xxxx xxxxxxx (tel.: xxx xxx xxx, e-mail:

xxxxxxxxx@ctu.cz). V případě změny kontaktní osoby pro hlášení bezpečnostních incidentů, bude kupující předem písemně (elektronicky) informovat kontaktní osobu prodávajícího xxxxxxx xxxxxxx (tel.: xxx xxx xxx, e-mail: xxxxxxxxx@xxxxxxxxxx).

8. Prodávající je povinen informovat kupujícího, jakým způsobem řídí rizika a jaká jsou zbytková rizika v souvislosti s plněním této smlouvy. Tyhle informace je dodavatel povinen dodat kupujícímu nejpozději při převzetí plnění dle čl. VI odst. 7 této smlouvy v elektronické podobě na USB flash disku, nebo zaslat e-mailem kontaktní osobě kupujícího uvedené v čl. V odst. 2 této smlouvy.
9. Prodávající, je povinen informovat kupujícího o významné změně ovládání prodávajícího. Ovládáním se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení.
10. Na SW SIEM musí být součástí plnění smlouvy poskytnutí všech požadovaných licencí na dobu 3 let, přičemž požadované licence jsou veškeré licence, které jsou potřebné k využívání veškerých definovaných parametrů a funkcí uvedených v příloze č. 1 této smlouvy. Zároveň musí být jako součást plnění smlouvy prodávajícím garantovány veškeré aktualizace dodaného SW, a to po dobu min. 3 let. Prodávající je povinen dodat vždy nejnovější dostupnou verzi příslušného SW.
11. V případě HW komponent musí být součástí plnění smlouvy poskytnutí všech případných licencí na dobu min. 5 let s tím, že prodávajícím musí být po tuto dobu jako součást plnění smlouvy garantovány veškeré aktualizace. Prodávající je povinen dodat vždy nejnovější dostupnou verzi příslušného SW.

XII. Ukončení smlouvy

1. Tato smlouva může být ukončena splněním, písemnou dohodou obou smluvních stran nebo odstoupením od smlouvy.
2. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným způsobem své povinnosti vyplývající z této smlouvy.
3. Za podstatné porušení smluvních povinností kupujícím se bude podle této smlouvy považovat prodlení kupujícího s uhrazením kupní ceny o více než 30 dnů.
4. Za podstatné porušení smlouvy prodávajícím se považuje:
   a) nedodržení stanoveného termínu dodání,
   b) neodstranění vady ve sjednané lhůtě,
   c) existence vady bránící naplnění účelu smlouvy a neposkytnutí součinnosti,
   d) uvedení nepravdivých údajů v nabídce ze strany prodávajícího,
   e) porušení bezpečnostních pravidel kupujícího podle čl. XI odst. 4 a 5 této smlouvy,
   f) zamlčení bezpečnostního incidentu, vzniklého v souvislosti s plněním této smlouvy.
5. Stanoví-li oprávněná smluvní strana druhé smluvní straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá smluvní strana v průběhu této lhůty prohlásí, že svůj závazek nesplní.
6. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají dnem doručení odstoupení od smlouvy druhé smluvní straně.
7. V případě, že tato smlouva zanikne odstoupením z důvodů na straně prodávajícího podle odstavce 2 tohoto článku, nemá prodávající nárok na náhradu vynaložených nákladů.
8. Kupující je oprávněn odstoupit od smlouvy, pokud dojde v době plnění smlouvy k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv,

ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení. Pokud by k významné změně kontroly nad dodavatelem došlo až po převzetí plnění, bude předmětem případného vyrovnání po odstoupení smlouvy jen část týkající se provozních služeb, jako jsou bezpečnostní audity, nebo úprava nastavení.

XIII. Salvatorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

XIV. Závěrečná ustanovení

1. Smluvní strany jsou vázány obsahem této smlouvy.
2. Veškeré změny či doplňky této smlouvy mohou být provedeny pouze písemně, a to formou písemných, vzestupně číslovaných dodatků k této smlouvě potvrzenými oběma smluvními stranami, a to osobami oprávněnými jednat za smluvní strany ve věcech smluvních.
3. Tato smlouva a práva a povinnosti z ní vyplývající se řídí českým právem. Práva a povinnosti smluvních stran, pokud nejsou upraveny touto smlouvou, se řídí občanským zákoníkem a předpisy souvisejícími.
4. Smluvní strany bezvýhradně souhlasí s uveřejněním této smlouvy, případných dodatků uzavřených k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění zajistí kupující.
5. Smluvní strany prohlašují, že smlouvu před jejím podepsáním přečetly, jejímu obsahu rozumí a s jejím obsahem souhlasí. Na důkaz svého souhlasu připojují obě smluvní strany své podpisy.
6. Smlouva byla sepsána ve třech stejnopisech, z nichž prodávající obdrží jeden a kupující dva stejnopisy. Nedílnou součást této smlouvy tvoří příloha č. 1 – Technická specifikace.
7. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění smlouvy podle zákona o registru smluv.

V Praze dne 27. 6. 2019

za kupujícího:

……
Ing. Mgr. Jaromír Novák
předseda Rady
Českého telekomunikačního úřadu

V Praze dne 17. 6. 2019

za prodávajícího:

……..
Pavel Šipr
jednatel

Příloha č. 1 smlouvy

TECHNICKÁ SPECIFIKACE

Seznam zkratek

ACL	Access Control Lists
AD	Active Directory
API	Application Programming Interface
ARP	Address Resolution Protocol
AVDS	Automated Vulnerability Detection Systém
CCSA	Check Point Certified Admin
CERT	Computer Emergency Response Team
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
CSV	Comma-separated values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Systém
DB	Database
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DNS	Domain Name System
ECC	Error Correction Code
EPS	Event per secund
FPM	Flows per minute
GB	Gigabyte
GbE	Gigabit Ethernet
Gbps	Gigabit per second
GUI	Graphical User Interface
HBA	Host Bus Adapter
HLD	High-level design
HMAC	Keyed-hash Message Authentication Code
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systém
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention Systém
ISO	International Organization for Standardization
ISSU	In-Service Software Upgrade
JDBC	Java Database Connectivity
KVM	Kernel Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLD	Low-level design
LRDIMM	Load-Reduced DIMM
MAC	Media Access Control
MD	Man Day
Mpps	Mega Packet Per Second
MS	Microsoft
MSRPC	Microsoft Remote Procedure Call
MT	Megatransfers
NBD	Next Business Day
NSEL	NetFlow Secure Event Logging
ODBC	Open Database Connectivity
OOB	Out-Of-Band
OPSEC LEA	Operations Security Log Export API
OS	Operating Systém
OSI	Open Systems Interconnection
PCIe	Peripheral Component Interconnect Express
PDF	Portable Document Format
POP	Post Office Protokol
PSU	Power Supply Unit
QSFP	Quad Small Form-factor Pluggable
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDIMM	Registred dual in-line memory module
RFC	Request For Comments
RJ	Registered jack
RU	Rack Unit
SAS	Serial Attached SCSI
SCP	Secure copy protocol
SCSI	Small Computer System Interface
SD	Secure Digital
SDEE	Security Device Event Exchange
SFF	Small Form Factor (2,5“)
SFP	small form-factor pluggable
SFP+	enhanced small form-factor pluggable
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSO	Single Sign-On
SW	Software
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TSL	Transport Layer Security
UBA	User Behavior Analytics
UDIMM	UnRegistred DIMM
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual LAN
XML	eXtensible Markup Language

Příloha č. 1 smlouvy

PARAMETRY SIEMU, SERVERU A PŘEPÍNAČŮ

Povinné parametry

Povinné parametry jsou minimální požadavky na technické vybavení, které kupující vyžaduje.

1. Server (1 ks)

- 1.1 Provedení
  - 1.1.1 Konfigurovatelný server (modulárně vyměnitelné provedení)
  - 1.1.2 Umístitelný do racku 19" (RACK MOUNT) max. 1 RU
  - 1.1.3 Počet slotů pro CPU – minimálně 2
  - 1.1.4 Počet slotů pro PSU – minimálně 2
  - 1.1.5 24 DIMM slotů pro instalaci RDIMM a LRDIMM DDR4 pamětí, 2666 MT za vteřinu
  - 1.1.6 2 ks SAS HBA – každý s 2 x SAS 12 Gbps, 8 externích linek SAS, včetně dvou SAS 12 Gbps kabelů pro redundantní připojení k diskovému poli o délce min. 2,5 m
  - 1.1.7 2x vnitřních dual SD Enterprise (min. 8 GB) pro instalaci VMware ESX, vzájemné zálohování – synchronní zrcadlo (RAID 1) s předinstalovaným hypervisorem ESXi 6.5 (licence bude aktivována kupujícím)
  - 1.1.8 Server musí být možné osadit min. 8x SFF (2,5") pevnými disky, v libovolné kombinaci disků SAS, Near Line SAS i SSD zároveň – veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájení apod.) musí být již osazeny tak, aby server bylo možné funkčně osadit plným počtem disků pouhým vložením disků
  - 1.1.9 grafický adaptér (integrovaný)
  - 1.1.10 Min. 6x hot-plug větráky (redundantní)
  - 1.1.11 Min. 2 x PCIe 3.0 z toho alespoň jeden slot full height
  - 1.1.12 Min. 2 x USB port
- 1.2 Procesory
  - 1.2.1 Dva procesory, 12 core každý, min. 24 MB cache, nominální frekvence min. 3 GHz. Average CPU Mark minimálně 20000 bodů pro jedno CPU a obě CPU musí dohromady (Dual CPU) splnit minimálně 28000 bodů (http://www.cpubenchmark.net)
- 1.3 Paměť
  - 1.3.1 12x16 GB DDR4-2666 ECC registred
    (Veškerá RAM dodaná jako součást musí být certifikována výrobcem serveru pro použití v dodaném typu serveru)
- 1.4 Porty/rozhraní pro síťové zapojení
  - 1.4.1 10 Gbps Ethernet (SFP+) minimálně 2 porty (postaveno chipsetech s podporou SR-IOV, PXE, IEEE 1588, automatickou negociací 1/10 Gbps)
  - 1.4.2 10 Gbps Ethernet (RJ45) minimálně 2 porty (nutná podpora SR-IOV)
  - 1.4.3 4 x 1 Gbit Ethernet (RJ45)
- 1.5 Vzdálená správa
  - 1.5.1 Součástí serveru musí být integrovaná HW (s vlastním procesorem, nezávislým na stavu CPU) vzdálená správa s funkcí vzdálené konzole a připojování médií bez nutnosti běžícího OS
  - 1.5.2 Pomocí vzdálené správy musí být možné následující (součástí nabídky musí být i licence)
    - 1.5.2.1 Aktualizace BIOS a firmware komponent serveru
    - 1.5.2.2 KVM over IP
    - 1.5.2.3 Remote media over IP
    - 1.5.2.4 Remote boot
    - 1.5.2.5 Vlastní management, integrované GUI po HTTPS
- 1.6 RAIL Kit
  - 1.6.1 1x kolejnice pro instalaci do racku
- 1.7 Napájecí zdroje
  - 1.7.1 2x minimálně 800 W hot-plug redundantní zdroje s certifikací 80 PLUS Platinum

1.7.2 2x 1,8 m napájecí kabel (IEC320-C14/IEC320-C13)

2. Přepínače (2 ks)

2.1 Provedení

2.1.1 Rack-mount (max. 2U), včetně Rack-mount kitu, (modulární, nebo fixed port)

2.1.2 2 ks redundantní a za chodu vyměnitelné napájecí zdroje o maximálním spotřebě 700W, klidová spotřeba při mírném zatížení přepínače nesmí překročit 200W

2.1.3 2 ks redundantní a za chodu vyměnitelné ventilátory s nasáváním vepředu anebo po stranách a výduchem v zadní části

2.1.4 Přepínač musí být určen pro nasazení v datových centrech jako „Top of Rack“ prvky, přepínače musí být identického modelu (part number)

2.1.5 Přepínač musí být osazen nejméně: 2 x 40 GbE QSFP porty, 8 x 10 GbE SFP+ porty a 30 x 10 GbE (RJ45) porty, metalické porty musí podporovat protokoly jak 1G, tak i 10G Base T. 10 GbE (RJ45) porty mohou být řešeny prostřednictvím originálních SFP+ transceiverů (RJ45) zasunutých v optických portech.

2.1.6 Přepínač musí mít nezávislý port pro management (RJ45) a konzolový port (RJ45)

2.2 Vlastnosti přepínače

2.2.1 Přepínač musí podporovat neblokující architekturu, a tedy musí zvládnout přenést nejméně 920 Gbps

2.2.2 Přepínač musí mít prostupnost minimálně 684 Mpps

2.2.3 Tabulka MAC adres přepínače musí zaznamenat alespoň 128 tisíc záznamů

2.2.4 Přepínač musí podporovat následující protokoly a standardy:

2.2.4.1 RFC 1305 NTPv3

2.2.4.2 RFC 1591 DNS (klient)

2.2.4.3 RFC 2573 (SNMPv3)

2.2.4.4 SSHv1/SSHv2

2.2.4.5 TACACS/TACACS+

2.2.4.6 IEEE 802.1ad Q-in-Q

2.2.4.7 IEEE 802.1ag Service Layer OAM

2.2.4.8 IEEE 802.1D MAC Bridges

2.2.4.9 IEEE 802.1D Spanning Tree Protocol

2.2.4.10 IEEE 802.1p Priority IEEE 802.1Q VLANs

2.2.4.11 IEEE 802.1s Multiple Spanning Trees

2.2.4.12 IEEE 802.3 Type 10BASE-T

2.2.4.13 IEEE 802.3ab 1000BASE-T (10/100/1000 módy)

2.2.4.14 IEEE 802.3ad Link Aggregation Control Protocol (LACP)

2.2.4.15 IEEE 802.3ae 10-Gigabit Ethernet

2.2.4.16 IEEE 802.3ag Ethernet OAM

2.2.4.17 IEEE 802.3x Flow Control

2.2.4.18 RFC 768 UDP

2.2.4.19 RFC 783 TFTP

2.2.4.20 RFC 791 IP

2.2.4.21 RFC 792 ICMP

2.2.4.22 RFC 793 TCP

2.2.4.23 RFC 826 ARP

2.2.4.24 ACL –Access Control Lists tabulky s nejméně 250 záznamy

2.2.4.25 IEEE 802.1p (CoS)

2.2.4.26 RFC 2475 DiffServ Architecture

2.2.4.27 RFC 2597 DiffServ Assured Forwarding (AF)

2.2.4.28 Stohování do větších celků pomocí 40GbE, nebo 100GbE portů, nejméně pro čtyři přepínače ve stohu. Cílem je vytvořit moderní leaf-spine topologii.

2.2.4.29 ISSU – možnost upgradovat firmware přepínače za chodu

2.2.4.30 Podpora protokolů TRILL, VEPA a DCB

2.2.4.31 Podpora statického směrování a alespoň jednoho směrovacího protokolu

2.2.4.32 Podpora NetFlow nebo sFlow

2.2.4.33 Konfigurace všech funkcí pomocí CLI dostupného přes SSH a webového rozhraní dostupného pomocí HTTPS. Pomocí této technologie musí být možné oba přepínače spravovat z jednoho místa jako jeden celek.

2.2.4.34 Podpora Jumbo Frames do velikosti 10 tisíc bajtů

3. SIEM

3.1 Požadované řešení SIEM je vše v jednom (all-in-one)

3.2 Řešení musí kombinovat HW a SW, musí být použita virtualizační vrstva, která zajistí vyšší automatizaci, vizualizaci provozu a komfort obsluhy, proto SIEM musí být ve formě virtuální appliance (vč. software, licencí apod.), požadovaná virtualizační platforma je VMware ESXi/vCenter V5 a vyšší (instalace virtuální appliance prostřednictvím OVA/ISO souboru)

3.3 Minimální požadovaný garantovaný výkon SIEM při současném zpracování logů musí být 600 událostí za sekundu (events per second / EPS)

3.4 Minimální požadovaný garantovaný výkon při současném zpracování datových toků musí být 15 000 toků za minutu (flows per minute / FPM)

3.5 Řešení musí být dobře škálovatelné, aby mohlo růst s počtem nově začleňovaných zdrojů.

3.6 Rozšiřování počtu garantovaných EPS musí být umožněno dokupováním licenčních balíků, přičemž maximální velikost nejmenšího balíku, který lze koupit je 100 EPS

3.7 Řešení musí být výkonově rozšiřitelné do garantované minimální hodnoty 5000 EPS na základě pouhého dokoupení licenčních balíků bez jakéhokoliv dodatečného SW

3.8 Řešení musí být výkonově rozšiřitelné do garantované minimální hodnoty 100 000 FPM na základě pouhého dokoupení licenčních balíků bez jakéhokoliv dodatečného SW

3.9 Garance sběru logů z minimálně níže uvedených produktů:

- 3.9.1 Microsoft Windows Server 2003, 2008, 2012 a 2016
- 3.9.2 Microsoft Windows 7, 8 a 10
- 3.9.3 Linux všechny běžné edice

3.10 Řešení SIEM musí být bezpečné, výrobce SIEM musí aplikovat globální bezpečnostní standardy a best-practices, bezpečnost SIEM musí vycházet z ISO/IEC 15408, kdy samotný produkt SIEM musí mít platný certifikát Common Criteria vydaný patřičným certifikačním úřadem

3.11 Výrobce SIEM musí provozovat vlastní CERT/CSIRT, kdy v případě zjištění bezpečnostních zranitelností v produktu SIEM automaticky elektronicky notifikuje uživatele, oznámí jejich označení a závažnost prostřednictvím CVE a CVSS, poskytne postupy k dočasnému a finálnímu odstranění těchto zranitelností

3.12 Řešení musí obsahovat výrobcem předefinovaná pravidla pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně z:

- 3.12.1 Microsoft AD, print, file, DNS, DHCP a WINS služby
- 3.12.2 Microsoft Exchange 2013 a 2016
- 3.12.3 Microsoft SharePoint
- 3.12.4 Microsoft IIS 6, 7 a 8
- 3.12.5 Microsoft System Center
- 3.12.6 Microsoft Hyper-V
- 3.12.7 Apache Web server
- 3.12.8 Apache TomCat server
- 3.12.9 Nginx web server
- 3.12.10 Linux DNS, DHCP
- 3.12.11 Logování z interní aplikace, kterou kupující provozuje na DB Postgres a frameworku .NET Framework 4.6.1, která loguje pomocí protokolu windows log a syslog

3.13 Řešení musí obsahovat výrobcem předefinovaná pravidla pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně z:

- 3.13.1 Aktivní prvky HPE (switche, routery, wireless zařízení)
- 3.13.2 Aktivní prvky Nokia (switche, routery, wireless zařízení)
- 3.13.3 Aktivní prvky Cisco (switche, routery, wireless zařízení)
- 3.13.4 VMware ESXi V5 a vyšší
- 3.13.5 VMware vSphere V5 a vyšší

3.13.6 VMware vCenter V5 a vyšší
3.13.7 VMware vShield
3.13.8 HPE diskové úložiště
3.13.9 HPE a DELL server management

3.14 Řešení musí obsahovat výrobcem předefinovaná pravidla pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně z:
3.14.1 Microsoft SQL 2012 a 2014
3.14.2 Oracle
3.14.3 MySQL
3.14.4 Informix 11
3.14.5 PostgreSQL

3.15 Řešení musí obsahovat výrobcem předefinovaná pravidla pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně z:
3.15.1 Check Point NG Firewall, IPS, Antivirus, Antibot, URL filtering pomocí nativní podpory API OPSEC.
3.15.2 Microsoft firewall
3.15.3 Linux IP tables
3.15.4 Microsoft Security Event Log
3.15.5 Microsoft IAS
3.15.6 Microsoft CA
3.15.7 Antivir (Endpoint Protection V11, V12, a V14 pomocí protokolu syslog)

3.16 Řešení musí podporovat příjem/stahování logů z požadovaných zdrojů logů, minimálně je požadována podpora následujících protokolů:
3.16.1 Syslog
3.16.2 Forwarded syslog
3.16.3 TCP/UDP multiline syslog
3.16.4 TLS syslog
3.16.5 JDBC
3.16.6 ODBC
3.16.7 OPSEC LEA
3.16.8 HTTP Receiver
3.16.9 Cisco NSEL
3.16.10 EMC VMware
3.16.11 Oracle DB Listener
3.16.12 SDEE
3.16.13 SMB Tail
3.16.14 Log File
3.16.15 SNMP v1, v2, v3
3.16.16 Microsoft Event Log over MSRPC

3.17 Řešení musí podporovat Flow protokoly:
3.17.1 Netflow v1, v3, v7 a v9
3.17.2 Jflow
3.17.3 Sflow v2, v4 a v5
3.17.4 IPFIX
3.17.5 Flowlog file
3.17.6 Qflow

3.18 Řešení musí podporovat import dat ze skenerů zranitelností následujících předních výrobců:
3.18.1 Nessus Scanner
3.18.2 Qualys
3.18.3 Axis Scanner
3.18.4 Tenable Security Scanner
3.18.5 Outpost24 Scanner
3.18.6 McAfee Vulnerability Scanner
3.18.7 Beyond Security AVDS Scanner
3.18.8 Saint Scanner
3.18.9 Rapid7 Nexpose Scanner

3.18.10 SecureScout Scanner
3.18.11 Positive Technologies Scanner

3.19 Je požadována podpora vyčítání vzdálených souborů s logy (Log Files), minimálně prostřednictvím bezpečných protokolů SCP a SFTP

3.20 Příjem toků ze zrcadlených zdrojů toků, minimálně podpora:
3.20.1 Zrcadleného provozu (toků) z prvků LAN sítě (funkce Port Monitoring)
3.20.2 Monitoring min. 2x 10 GE fyzických rozhraní z centrálního prvku kupujícího

3.21 Kupující má následující požadavky na sběr logů:
3.21.1 Je požadováno automatické rozpoznání zdrojů logů (vč. typu zařízení a výrobce) u globálně rozšířených produktů
3.21.2 Je požadováno začlenění i specifických zdrojů logů (např. aplikací vytvořených „na míru“) prostřednictvím univerzálního profilu, který umožní pojmenování a dodatečnou konfiguraci těchto zdrojů logů
3.21.3 Naučení specifických zdrojů logů musí být prováděno jen prostřednictvím jednotného GUI SIEM
3.21.4 Je požadováno vyhodnocení datových toků na aplikační úrovni, uživateli musí být umožněn náhled do aplikačního obsahu datové komunikace (ISO OSI L7 analýza)
3.21.5 Díky ISO OSI L7 analýze musí být z obsahu jasné, jaké řídící příkazy aplikační protokol používá, minimálně: FTP, POP3, Telnet, SMTP, HTTP, SIP
3.21.6 Zobrazení aplikačního obsahu z analýzy toků musí být dostupné prostřednictvím jednotného GUI SIEM
3.21.7 Je požadováno vyhodnocení logů a toků společně se zjištěnými technickými zranitelnostmi
3.21.8 Je požadována podpora importovaných hodnocení zranitelností na základě obecného standardu Common Vulnerability Scoring System (CVSS)
3.21.9 Je požadováno doplňování informací o uživatelích a počítačích ze systému identit (minimálně jméno účtu uživatele, jméno a příjmení uživatele a jméno počítače)
3.21.10 Řešení musí poskytovat sběr logů ze všech požadovaných zdrojů i bez jakýchkoliv instalovaných agentů ve zdrojích logů (bezagentský sběr)
3.21.11 Je požadována podpora zpracování více řádkového logu (Multi-line Syslog)
3.21.12 Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při komunikaci se zdroji dat, tak i při normalizaci vstupních dat
3.21.13 Systém SIEM nesmí být licenčně omezen na počet zařízení generujících logy (zdrojů logů), na počtu evidovaných aktiv a na počtu uživatelů/konzolí
3.21.14 Systém SIEM nesmí technicky limitovat počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, aby nedošlo k jejich zahození.

3.22 Kupující má následující požadavky na zpracování logů a toků:
3.22.1 Řešení musí obsahovat přednastavená korelační pravidla, která řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z následujících oblastí:
3.22.1.1 Útoky červů, virů a robotů
3.22.1.2 Neoprávněný přístup vč. ověřování, změny konfigurace
3.22.1.3 Chyby a změny v sítích vč. chyb a stavů síťových zařízení
3.22.1.4 Monitorování aktiv vč. aktivit privilegovaných uživatelů, přístupů a změn konfigurací, odmítnutých připojení, úspěšných a chybných přihlášení a hlášení systémů IPS/IDS)
3.22.1.5 Překročení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla a změny konfigurace)
3.22.1.6 Detekované masivní šifrování dat (crypto-ransomware)
3.22.2 Řešení musí korelovat minimálně položky: zdrojová IP, cílová IP, zdrojový port, cílový port, uživatelské jméno, jméno účtu, jméno počítače, jméno události, kategorie události, čas přijetí, čas vygenerování, MAC, surová data
3.22.3 Řešení musí podporovat doplnění údajů do korelovaných výstupů z připravených číselníků
3.22.4 Řešení musí umožňovat definici vlastního (custom) atributu (číselného a textového) v událostech, do kterého je automaticky doplňována hodnota z externího zdroje

3.22.5 Výsledkem korelace je standardní událost v rámci SIEM, která může být dále použita i jako základ pro další korelace a vznik kumulovaných událostí
3.22.6 Součástí korelace musí být i informace z integrovaných globálních reputačních služeb výrobce
3.22.7 Řešení musí korelovat dohromady události z logů a toků (vč. zrcadleného toku a NetFlow/IPFIX)
3.22.8 Řešení musí umožnit definovat vlastní (custom) pravidla pro vyhodnocování anomálií i v síťovém provozu
3.22.9 Vlastní (custom) atribut musí být použitelný pro filtraci, drill-down i definice korelací napříč celým SIEM
3.22.10 Výsledky scanneru zranitelností se automaticky korelují do korelovaných událostí.
3.22.11 V případě zaznamenání útoku, musí dojít ke korelaci informací ze scanneru ohledně zjištěných zranitelností v interních aktivech, SIEM pak musí určit, zdali byl útok na dané aktivum úspěšný či nikoliv
3.22.12 Je požadována integrovaná analýza chování uživatelů a strojových identit (tzv. UEBA/UBA), tyto události a anomálie musí být vyjádřené graficky prostřednictvím prioritizovaných přehledů a grafů

3.23 Řešení musí provádět evidenci aktiv v SIEMu s informací o jejich geografickém umístění a zobrazení na mapě, to platí i o vizualizaci vzniklých (korelovaných) událostí na geolokační mapě
3.23.1 Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup)
3.23.2 Je požadováno intuitivní prostředí (průvodce) k přidávání a změně log parserů prostřednictvím jednotného GUI SIEM, bez nutnosti spolupráce s prodávajícím, nebo výrobcem
3.23.3 Konfigurace integrovaného parsovacího nástroje k naučení specifických zdrojů logů musí být prováděna pouze prostřednictvím jednotného GUI SIEM.
3.23.4 Je požadováno intuitivní prostředí (průvodce) k přidávání a změně vlastních korelačních pravidel prostřednictvím jednotného GUI SIEM bez nutnosti spolupráce s prodávajícím nebo výrobcem

3.24 Kupující má následující požadavky na pohledy na data:
3.24.1 Řešení musí poskytovat grafický dashboard (grafickou pracovní plochu) libovolně konfigurovatelný pro každého uživatele SIEM zvlášť dle náplně práce a geografického uspořádání ICT.
3.24.2 Dashboardy musí umožňovat jejich stavbu z minimálně následujících typů grafů:
3.24.2.1 Graf v závislosti na čase
3.24.2.2 Koláčový graf
3.24.2.3 Tabulkový výpis
3.24.2.4 Sloupcový graf
3.24.3 Grafy v dashboardech musí umožňovat výběr určité své části pro rychlé vymezení oblasti vyhledávaných událostí.
3.24.4 Je požadována analýza dat v reálném čase a jejich zobrazení pomocí GUI prohlížeče.
3.24.5 Jsou vyžadovány minimálně následující pohledy:
3.24.5.1 Bezpečnost = stav bezpečnosti a detekované incidenty
3.24.5.2 Autentizace = kdo, kdy, kde se přihlásil
3.24.5.3 Uživatelská aktivita = co dělal vybraný uživatel
3.24.5.4 Využívání sítě
3.24.5.5 Využívání aplikací
3.24.5.6 Shoda s pravidly = který počítač porušuje pravidla = využívá závadný obsah, provozuje nepovolené programy, služby a aplikace, komunikuje nepovolenými protokoly, komunikuje se zakázanými cíli apod.
3.24.5.7 Audit = kdo, kdy a jak změnil nastavení systému
3.24.6 Řešení musí umožnit pohled na korelované události v reálném čase včetně nastavení vlastních vyhledávání a filtrů

3.24.7 Řešení musí umožnit pohled na korelované historické události včetně nastavení vlastních vyhledávání a filtrů
3.24.8 Řešení musí obsahovat v dashboardu pohled na časově nejbližší korelované událostí
3.24.9 Řešení musí obsahovat v dashboardu pohled na nejvýznamnější korelované události
3.24.10 Řešení musí umožnit pohledy na sběr logů a toků podle typu aktiv, typu události, libovolného časového období a míry detailu/abstrakce
3.24.11 Každý uživatel musí být schopen si vytvářet vlastní dashboardy podle jemu svěřené agendy
3.24.12 Řešení musí podporovat vyhledávání logů/eventů na základě „full-text“ indexace
3.24.13 Řešení musí podporovat vyhledávání a filtrování prostřednictvím jednotného GUI SIEM

3.25 Kupující má následující požadavky na reakce systému:
3.25.1 Podpora varování (alerting) na zjištěné bezpečnostní události:
3.25.1.1 Přímo v GUI SIEM
3.25.1.2 E-mailem uživateli
3.25.1.3 SNMP trap / inform do dalších zařízení (bezpečnostní prvky a management nástroje)
3.25.1.4 Skriptem ke spuštění operací v externích zařízeních a aplikacích
3.25.2 Řešení musí v sobě obsahovat interní skriptovací jazyk k vytvoření reakce na na-míru při události, minimálně podpora Bash, Python a Perl
3.25.3 Řešení musí obsahovat funkcionalitu ticketovcího systému, která umožní přiřazovat události k řešení jednotlivým uživatelům (řešitelům), v jednotném GUI SIEM je viditelný stav jejich řešení

3.26 Kupující má následující požadavky na ověřování:
3.26.1 Je požadováno ověřování uživatelů proti interní databázi
3.26.2 Je požadováno proti externímu ověřovacímu serveru na základě metod LDAP/Microsoft AD, RADIUS a pomocí prostředků více faktorového ověřování

3.27 Kupující má následující požadavky na Reporting:
3.27.1 Řešení musí obsahovat předdefinované a upravitelné reporty
3.27.2 Řešení musí umožnit definici vlastních reportů typu denní, týdenní, měsíční
3.27.3 Součástí řešení musí být průvodce k vytváření vlastních (custom) reportů „na míru“, který je součástí jednotného GUI SIEM
3.27.4 Reporty musí podporovat popisy českým jazykem s diakritikou
3.27.5 Reporty musí být k dispozici v jednotném GUI SIEM a musí být možné je zasílat uživateli e-mailem
3.27.6 Řešení musí být schopno generovat reporty obsahující kterékoliv hodnoty z korelovaných položek
3.27.7 V řešení jsou vyžadovány minimálně následující denní reporty:
3.27.7.1 Autentizace = kdo, kdy, kde a jak se přihlásil
3.27.7.2 Uživatelská aktivita = co dělal vybraný uživatel
3.27.7.3 Shoda s pravidly = který počítač porušuje pravidla = např. využívá mravně závadný obsah či nepovolené aplikace
3.27.7.4 Audit = kdo a kdy změnil nastavení systému
3.27.7.5 Bezpečnost = detekované incidenty dle závažnosti, důvěryhodnosti, relevance
3.27.7.6 Využití sítě
3.27.7.7 Využití aplikací
3.27.8 Systém vytváří reporty ve formátech PDF, HTML a CSV, popř. dalších
3.27.9 Systém musí umožňovat export dat ve formátu XML nebo CSV

3.28 Kupující má následující požadavky na webové GUI SIEM:
- 3.28.1 Produkt musí mít kompletní centrální grafické uživatelské rozhraní (GUI) vzdáleně přístupné prostřednictvím běžného webového klientského prohlížeče (např. Firefox, Google Chrome, Internet Explorer)
- 3.28.2 GUI musí být jednotné, nesmí vyžadovat doplnění dodatečných technologií, instalaci pluginů nebo instalaci tlustého klienta
- 3.28.3 Je požadována podpora přístupu uživatelů do GUI systému dle rolí (RBAC), minimálně administrátor (může vše), operátor (může ladit), prohlížeč (nemůže nic měnit)
- 3.28.4 Jakmile se uživatel přihlásí do GUI, musí být ověřen a autorizován pro práci s ním. GUI a jeho všechna webová okna využívají úvodní přihlášení bez nutnosti jakékoliv dodatečné autentizace při práce s více okny v SIEM (SSO)
- 3.28.5 Podpora autorizace a řízení přidělování oprávnění na úrovni jednotlivých pohledů, reportů, zdrojů a IP sítí
- 3.28.6 GUI musí být jednotné jak pro vyhodnocení logů a toků, přehled korelovaných událostí, tak konfiguraci samotného SIEM
- 3.28.7 V GUI musí být grafický okamžitý a dlouhodobý přehled o výkonu systému z pohledu hodnot EPS a FPM
- 3.28.8 Řešení musí podporovat úpravu přihlašovací stránky GUI vč. vlastního přihlašovacího informačního banneru a vlastního loga

3.29 Kupující má následující požadavky na Dostupnost systému, zálohování a archivace:
- 3.29.1 Řešení musí poskytovat plánované automatizované i manuální zálohy dat a konfigurace, nastavení funkcí zálohování musí být prováděno jen prostřednictvím jednotného GUI SIEM
- 3.29.2 Je požadována podpora flexibilní retenční politiky k nastavení archivace logů na základě různých typů zdrojů logů a jejich důležitosti
- 3.29.3 Je požadována podpora funkce k zajištění integrity uložených logů a toků (hashování), možnost aktivace algoritmu SHA-512 nebo vyššího/bezpečnějšího prostřednictví jednotného GUI SIEM
- 3.29.4 Nativní podpora funkce k zajištění důvěrnosti uložených logů a toků v SIEM (šifrování), možnost aktivace algoritmu HMAC SHA-512 nebo vyššího/bezpečnějšího prostřednictví jednotného GUI
- 3.29.5 Řešení musí umožňovat archivovat originální (neagregované) logy po volně definovanou dobu
- 3.29.6 Je požadována podpora uložení archivu na externím diskové úložiště a zpětné načtení archivu do SIEM

3.30 Kupující má následující požadavky na aktualizace:
- 3.30.1 Výrobce řešení musí poskytovat automatické aktualizace systému, které musí minimálně obsahovat:
  - 3.30.1.1 Nové metody detekce porušení bezpečnosti (threat-inteligence)
  - 3.30.1.2 Podporu nově uvolňovaných zařízení 3tích stran jakožto zdrojů logů
  - 3.30.1.3 Nové verze, nová funkcionalita
  - 3.30.1.4 Opravy chyb
- 3.30.2 Produkt musí podporovat nastavení periody dotazování aktualizací, které typy aktualizací mohou být prováděny bezobslužně

4. Servisní služby včetně garance dostupnosti náhradních dílů (server, přepínače i SIEM)

4.1 Na veškeré hardware komponenty musí být výrobcem garantovaná záruka min. na 5 let v režimu NBD On-Site. Ukončený servisní zásah nejpozději následující pracovní den po nahlášení vady v místě instalace

4.2 Pozáruční servis. Garance dostupnosti veškerých náhradních dílů minimálně po dobu 36 měsíců po ukončení záruky

4.3 Help desk prodávajícího dostupný v režimu non stop 24 x 7 hovořící v českém jazyce, který je možné kontaktovat pomocí webového formuláře, emailem či telefonicky. Podpora musí být garantovaná výrobcem zařízení. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů z internetu

4.4 Na SW SIEM musí být součástí nabídky veškeré požadované licence a aktualizace garantovány prodávajícím po dobu min. 3 let. Kupující požaduje, aby prodávající dodal vždy nejnovější dostupnou verzi SW

4.5 Na HW komponenty musí být součástí nabídky veškeré požadované licence a aktualizace garantovány prodávajícím po dobu min. 5 let. Kupující požaduje, aby prodávající dodal vždy nejnovější dostupnou verzi SW

4.6 Požadované licence (podle bodu 4.4 a 4.5) jsou také veškeré licence, které jsou potřebné k využívání veškerých definovaných parametrů v této technické specifikaci. V případě, že by bylo splnění jakéhokoliv parametru této technické specifikace vázané na licenci, musí být taková licence součástí nabídky minimálně v rozsahu definovaného parametru a na dobu podle bodu 4.4 a 4.5 této technické specifikace

5. Požadavky na řešení

5.1 Součástí dodávky musí být veškeré potřebné komponenty (kabely atd.) pro propojení stávajícího diskového pole (MSA 2052) a nového serveru, prostřednictvím SAS 12Gb.

5.2 Kupující požaduje po prodávajícím realizaci následujících propojení. Kupující nechává na prodávajícím, zda použije direct attach-twinax kabely, nebo kombinaci SFP+/QSFP-optický patchcord- SFP+/QSFP. Všechny propoje budou o délce 5 metrů. Propoje budou následující:

5.2.1 Mezi dvěma přepínači dva propoje realizované pomocí 40GbE QSFP

5.2.2 Mezi přepínači a již zakoupenými 2ks serverů (HPE DL360 Gen 10) celkem čtyři propoje (8 kusů 10 GbE SFP+)

5.2.3 Mezi přepínači a nově zakoupeným serverem, celkem dva propoje (4 kusy 10 GbE SFP+)

5.3 Kupující požaduje dodání sestaveného a zkompletovaného serveru a přepínačů, nikoliv dodaní jednotlivých komponentů, resp. částí (procesor, karty atd.)

5.4 Dodané HW komponenty musí být kompatibilní s MS Windows server pro aktuálně na trhu dostupnou nejnovější verzi OS

5.5 Server musí být na „hardware compatibility listu" společnosti VMware pro aktuálně na trhu dostupnou nejnovější verzi vSphere

5.6 Přepínače a server musí být nové a nepoužité. Kupující si vyhrazuje právo vrátit nejenom produkty, které budou vykazovat stopy používání či poškození, a odstoupit okamžitě od části či celé smlouvy, pokud mu budou dodány použité či opravované produkty

6. Implementace

6.1 Kupující požaduje od prodávajícího činnosti, které odhadl níže (pozn.: kupujícím uváděný odhad je minimální a je doporučováno prodávajícímu věnovat pozornost při cenotvorbě všem vlastnostem příslušné zadávací dokumentace). Kupující odhadl činnosti takto:

6.1.1 Projektové řízení – pomocí certifikovaného vedoucího projektu (nejméně 5 člověkodnů)

6.1.2 Příprava realizace (před realizační dokumentace, postup, harmonogram, součinnost, integrační plán, nejméně 4 člověkodny)

6.1.3 Provedení instalace a konfigurace SW a HW (nejméně 3 člověkodny)

6.1.3.1 Instalace HW v datovém centru

6.1.3.2 Instalace SW appliance (SIEM) v prostředí VMware

6.1.3.3 Nastavení vzdáleného přístupu (OOB) na dodaný server

6.1.3.4 Konfigurace přepínačů a jejich začlenění do již existující struktury systému MSEK

6.1.3.4.1 Nastavení přístupu

6.1.3.4.2 Nastavení portů (přiřazení VLAN ID portům) a nastavení agregace portů

6.1.3.4.3 Nastavení přepínačů do stohu

6.1.3.4.4 Natavení přepínačů podle „Best practice“ výrobce

6.1.4 Zavedení zdrojů logů a toků, nastavení pohledů a reportů, zavedení správců (nejméně 15 člověkodnů)

6.1.4.1 Syslog pro standardizované zdroje

6.1.4.2 Wincollect agent pro MS OS

6.1.4.3 JDBC pro připojení logů databáze

6.1.4.4 OPSEC pro připojení logů z firewallů

6.1.4.5 VMWare log protocol

6.1.4.6 Rest API pro vlastní webové aplikace

6.1.5 Provedení akceptačních testů k ukončení implementační fáze (nejméně 2 člověkodny)

6.1.6 Zaškolení správců systému (maximálně 5 osob), s délkou školení 2 dny. Školení bude provedeno po implementaci řešení a zavedení logů se zaměřením na dodané řešení SIEM

6.1.7 HLD a LLD dokumentace skutečného provedení (nejméně 2 člověkodny)

6.1.7.1 V HLD dokumentaci musí být popsána architektura řešení, podrobný popis bezpečnostních funkcí, které využívá správce systému a návod na použití těchto funkcí. Dále pak parametry SIEMu a přepínačů

6.1.7.2 V LLD dokumentaci bude uveden popis všech funkcí včetně bezpečnostních společně s návodem. Rozepsané nastavení SIEMu, popsány způsoby a typy aktualizací, popsány zavedené logy a reporty

6.2 Prodávající je povinen dodat a nainstalovat HW komponenty, nejpozději do 45 dnů ode dne účinnosti smlouvy, následně pak do 45 dnů provést veškeré další činnosti vyplívající z technické přílohy (implementace, dokumentace, zaškolení správců), následně pak bude běžet lhůta 14 dnů, která bude složit již zaškoleným správcům jako testovací období, ve kterém budou moci konzultovat nastavení, vyžadovat dodatečnou konfiguraci a změny v dokumentaci

7. Provoz

7.1 Kupující vyžaduje, aby součástí plnění byly také následující služby provozu SIEMu po dobu 24 měsíců, které budou zahrnovat nejméně následující činnosti:

7.1.1 Bezpečnostní report (celkem 12 bezpečnostních reportů)

7.1.1.1 Prodávající se zavazuje k poskytování služby bezpečnostního reportu v rámci které jednou za 2 měsíce kupujícímu musí poskytnout bezpečnostní report. Kupující požaduje, aby tento report zohlednil vstupy z platforem:

7.1.1.1.1 SIEM

7.1.1.1.2 Check Point Smart Event a Smart Log ve vlastnictví kupujícího

7.1.1.2 Bezpečnostní report musí obsahovat tyto části:

7.1.1.2.1 Manažerské shrnutí

7.1.1.2.2 Doporučení změn

7.1.1.2.3 Popis bezpečnostních incidentů (číslo CVE pokud je k dispozici, obsah incidentu, dopad incidentu, adresní a uživatelské informace), kategorizaci incidentů na kritické a ostatní.

7.1.1.2.4 Seznam infikovaných platforem, hostů (IP, Domain name)

7.1.1.2.5 Statistiky incidentů vyjádřené na časové ose

7.1.1.3 Kupující požaduje, aby každé 2 měsíce prodávající s kupujícím report prošel a navrhnul bezpečnostní opatření k zajištění nápravy jednotlivých zjištěných událostí

7.1.1.4 Bezpečnostní report je produktem pracovní aktivity bezpečnostního specialisty a nejedná se pouze o export ze SIEMu či jiné technické platformy. V týmu který bude sestavovat bezpečnostní report musí být bezpečnostní specialista certifikován certifikací minimálně CCSA pro verzi R80 a certifikací na dodávané řešení SIEM a Log Manager

7.1.2 Dodatečná nastavení – součástí plnění musí být také 12 MD (man-day), které bude možné vyčerpat pro zavádění dalších zdrojů logů, či změně nastavení SIEMu