SMLOUVA O DODÁVCE A IMPLEMENTACI SIEM A POSKYTOVÁNÍ SLUŽEB V RÁMCI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

uzavřená dle zákona č. 89/2012 Sb., občanského zákoníku

mezi:

Odběratelem				
Název:	**Fakultní nemocnice Ostrava**			
Sídlo:	17. listopadu 1790, 708 52 Ostrava-Poruba			
IČ:	00843989	**DIČ:**	CZ00843989	je plátcem DPH
Zřizovací listina MZ ČR ze dne 25. listopadu 1990 č. j. OP-054-25.11.90				
Zastoupena:	MUDr. Jiřím Havrlantem, MHA, ředitelem			
Bankovní spojení:	Česká národní banka, č. ú. 43 - 65137761/0710			

a

Dodavatelem				
Obchodní firma:	**TOTAL SERVICE a.s.**			
Sídlo:	U Uranie 954/18, Holešovice, 170 00 Praha 7			
IČ:	256 18 067	**DIČ:**	CZ25618067	je* - ~~není~~* plátcem DPH
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze oddíl B vložka 23580				
Jednající:	Jiří Chovanec, člen představenstva			
Bankovní spojení:	ČSOB a.s., č. ú. 579 579 583/0300			

Odběratel a Dodavatel jsou dále souhrnně označeni jako „**Smluvní strany**" nebo jednotlivě „**Smluvní strana**"

I.
Základní ustanovení

1. Odběratel a dodavatel uzavírají tuto Smlouvu o dodávce a implementaci SIEM a poskytování služeb v rámci kybernetické a informační bezpečnosti (dále také jen „**Smlouva**") na základě výsledku výběru nejvhodnější nabídky veřejné zakázky **„Dodávka a implementace SIEM a služby v rámci kybernetické a informační bezpečnosti"** (dále také jen „**Veřejná zakázka**"), na základě které má Dodavatel provést dodávku a implementaci SIEM (dále také jen **„SIEM"** nebo **„technologie SIEM"** nebo „**Řešení**") a poskytování služeb v rámci kybernetické a informační bezpečnosti (dále také jen „**SŘBI**") dle zadávací dokumentace Veřejné zakázky (dále také jen „**Zadávací dokumentace**"), jejíž součástí je mimo jiné technická specifikace „Dodávka a implementace SIEM a služby v rámci kybernetické a informační bezpečnosti", která tvoří rovněž přílohu č. 1 této Smlouvy (dále také jen „**Technická specifikace**").

2. Veřejná zakázka **„Dodávka a implementace SIEM a služby v rámci kybernetické a informační bezpečnosti"** byla vyhlášena podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek, ve znění platném ke dni vyhlášení veřejné zakázky.

3. Dodávka a implementace SIEM a služby podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZ ČR, které jsou předmětem této Smlouvy, jsou spolufinancovány v rámci Integrovaného regionálního operačního programu, specifického cíle 3.2 – Zvyšování efektivity a

[redacted]

transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT, 10. výzva „Kybernetická bezpečnost" a v souladu s projektem Odběratele *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"* (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023). Poskytování pravidelných služeb kontroly rizik a dodržování předpisů nad platformou SIEM po dobu 5-ti let a zajištění technické podpory dodané technologie SIEM po uplynutí prvních dvou let jejího trvání, a to na dobu následujících 3 let je hrazeno z vlastních zdrojů Odběratele, nikoliv s poskytnutých prostředků Integrovaného regionálního operačního programu.

4. Součástí plnění Smlouvy je krom dodání technických zařízení, vybavení a jejich příslušenství (dále také jen „**Hardware**" nebo „**Technická zařízení**") a převodu vlastnického práva k tomuto vybavení na Odběratele, také mimo jiné dodání všech potřebných licencí a subskripcí (dále také jen „**Licence**") pro počítačové programy (včetně operačních systémů) potřebné pro řádný chod SIEM (dále také jen „**Software**"), instalace, nastavení a zprovoznění SIEM dle Zadávací dokumentace a požadavků Odběratele včetně spuštění do ostrého provozu (dále také jen „**Implementace**") v rámci počítačového prostředí – IT infrastruktury Odběratele (dále také jen „**IT Infrastruktura**"), provedení školení personálu Odběratele (dále také jen „**Školení**") a poskytování technické podpory pro zajištění náležitého chodu SIEM po jeho uvedení do ostrého provozu (dále také jen „**Technická podpora**"). Technická podpora bude poskytována v délce 2 (slovy: dvou) let s možností rozšíření o další 3 (slovy: tři) roky na celkovou dobu 5 (slovy: pět) let.

5. Součástí plnění Smlouvy je dále poskytování služeb podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZ ČR, který byl zveřejněn ve Věstníku č. 7/2019 a poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad dodanou technologií SIEM.

II.
Předmět smlouvy

1. Dodavatele se zavazuje poskytnout a provést Odběrateli následující plnění dle Zadávací dokumentace, které zahrnuje:
   a) dodávku Hardware (včetně převodu vlastnického práva k Hardware na Odběratele);
   b) dodávku a poskytnutí všech potřebných Licencí pro řádný chod SIEM;
   c) provedení Implementace včetně uvedení SIEM do ostrého provozu;
   d) provedení Školení;
   e) poskytování Technické podpory;
   f) poskytování Služeb podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZ ČR, který byl zveřejněn ve Věstníku č. 7/2019;
   g) poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad technologií SIEM a
   h) další plnění dle Zadávací dokumentace;

   (dále souhrnně také jen „**Předmět plnění**"), přičemž detaily a rozsah jsou vymezeny v Technické specifikaci, která je přílohou č. 1 této Smlouvy a v příloze č. 2 této Smlouvy – Položkový rozpočet předmětu plnění (dále také jen „**Rozpočet**").

2. V rámci Předmětu plnění bude Odběrateli dodán Hardware, který je originální, nový a nepoužitý. V databázi výrobce Hardware a Licencí bude Odběratel veden jako první uživatel dodaného Hardware/Licence. Dodavatel je povinen doložit do 7 (slovy: sedmi) pracovních dnů od doručení žádosti Odběratele potvrzení výrobce o určení dodávaného Hardware pro evropský trh, včetně sériových čísel dodávaného Hardware, případně jiný doklad výrobce prokazující pro dodaná Technická zařízení provozovaná na území ČR poskytnutí plné podpory výrobce při řešení technických problémů (požadavek uvedený v Technické

specifikaci). Před převzetím Hardware si Odběratel vyhrazuje právo kontroly dle sériových čísel (pokud jsou přidělena) u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Odběratel (a to historicky), bude se jednat o podstatné porušení této Smlouvy.

3. Veškeré potřebné Licence budou Dodavatelem dodány v rozsahu potřebném pro řádné užívání SIEM, včetně možnosti jeho správy, konfigurace a provádění obnovy dat. Časový rozsah těchto Licencí bude na celou dobu trvání majetkových autorských práv k dodanému Software.

4. Předmět plnění zahrnuje rovněž vyhotovení a dodání instalační, administrační a provozní dokumentace SIEM (dokumentace bude zpracována nejméně v rozsahu potřebném pro zajištění užívání, správy a údržby SIEM Odběratelem a dále bude obsahovat popis skutečného provedení SIEM včetně jeho vazeb na další části IT Infrastruktury).

III.
Místo a způsob poskytnutí Předmětu plnění

1. Místem dodání Předmětu plnění je v sídle Odběratele - Fakultní nemocnice Ostrava – prostory ve správě Útvaru náměstka ředitele pro informační technologie (dále také jen „**Místo plnění**").
2. Náklady na dodání Předmětu plnění a jeho částí do místa dodání hradí Dodavatel.
3. Dodání technologie SIEM včetně veškerého Hardware, Licencí a provedení Implementace a uvedení SIEM do ostrého provozu bude provedeno nejpozději do 160 (slovy: stošedesáti) kalendářních dnů ode dne podpisu této Smlouvy oběma Smluvními stranami (dále také jen „**Termín plnění**"), a to dle vzájemně odsouhlaseného harmonogramu (dále také jen „**Harmonogram**").
4. Služby podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZ ČR budou poskytnuty nejpozději do 180 (slovy: stoosmdesáti) kalendářních dnů ode dne podpisu této Smlouvy oběma Smluvními stranami (dále také jen „**Termín plnění pro naplnění metodického pokynu**"), a to dle vzájemně odsouhlaseného Harmonogramu.
5. Poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad platformou SIEM bude realizováno průběžně po celou dobu 5 (slovy: pěti) let ode dne podpisu Akceptačního protokolu ve smyslu odst. 8 tohoto článku níže oběma Smluvními stranami.
6. Termín plnění a termín plnění pro naplnění metodického pokynu můžou být posunuty pouze o délku případného prodlení zaviněného na straně Odběratele, a to formou písemného dodatku k této Smlouvě.
7. Smluvní strany se dohodly, že po instalaci a uvedení SIEM do provozu, budou Dodavatelem v místě plnění provedeny zkoušky provozu, činnosti a veškerých funkcí SIEM (dále také jen „**Akceptační testy**"). Odběratel je oprávněn se Akceptačních testů zúčastnit. Termín provádění Akceptačních testů je povinen Dodavatel sdělit Odběrateli nejméně 2 (slovy: dva) pracovní dny před plánovaným dnem jejich provádění; v případě, že by takto navržený termín Odběrateli z relevantních důvodů nevyhovoval, je oprávněn požadovat odložení Akceptačních testů o nejvýše 4 (slovy: čtyři) pracovní dny. V případě, že SIEM nebo jeho příslušenství bude vykazovat vady, není SIEM způsobilý předání a Odběratel nemá povinnost jej převzít. Po provedení Akceptačních testů, dle kterých bude SIEM bez vad, bude spuštěn do ostrého provozu (dále také jen „**Ostrý provoz**").
8. Předmět plnění je způsobilý předání Odběrateli, pokud budou provedeny všechny plnění, které jsou jeho součástí, tj. zejména dodání Hardware a jeho příslušenství, dodání a poskytnutí Licencí (včetně dodání dokumentů ohledně oprávnění Odběratele k užívání Software na základě Licencí), dodání veškeré dokumentace, instalace a uvedení SIEM do Ostrého provozu (Implementace) v Místě plnění a v rámci Akceptačních testů nebude SIEM vykazovat jakékoliv vady nebo nedostatky. Předmět plnění se považuje za řádně dodaný podpisem akceptačního protokolu Odběratelem (dále také jen „**Akceptační protokol**") po

uvedení SIEM do Ostrého provozu. Nárok na úhradu ceny za Předmět plnění sjednané v čl. IV. odst. 3 písm. A/ této Smlouvy vzniká Dodavateli podpisem Akceptačního protokolu Odběratelem.

9. Přechod nebezpečí škody a vlastnického práva

9.1. Nebezpečí škody na dílčích částech Předmětu plnění (typicky jednotlivého Hardware) přechází na Odběratele převzetím jednotlivých dílčích částí Předmětu plnění Odběratelem a podpisem protokolu o takovém převzetí k tomu oprávněným zástupcem Odběratele (dále také jen „**Protokol o dodání dílčí části**"). Protokol o dodání dílčí části slouží pouze pro evidenční účely, že došlo k dovozu/provedení dílčí části Předmětu plnění, neboť není fakticky možné, aby byl celý Předmět plnění dodán najednou.

9.2. Převzetí dílčích částí Předmětu plnění dle odst. 9.1 tohoto článku výše, ani podepsání Protokolu o dodání dílčí části, nelze považovat za částečné plnění předmětu této Smlouvy Dodavatelem. Dodavatel v této souvislosti bere na vědomí, že Odběratel požaduje dodání Předmětu plnění jako celku, když očekává plně funkční SIEM a dílčí plnění pro něj nemají žádný význam ani užitek.

9.3. Vlastnické právo k movitým věcem dodaným Odběrateli na základě této Smlouvy přechází na Odběratele podpisem Akceptačního protokolu.

10. Realizační tým

10.1. Dodavatel bude Předmět plnění realizovat majoritně za účasti (prostřednictvím) osob, které jsou uvedeny v příloze č. 3 této Smlouvy – Realizační tým dodavatele. V případě, že dojde ke změně těchto osob je Dodavatel povinen tuto skutečnost oznámit Odběrateli nejpozději do 5 (slovy: pěti) pracovních dnů od vzniku této skutečnosti. Nová osoba, která bude součástí realizačního týmu, musí splňovat podmínky, které Odběratel stanovil v Zadávací dokumentaci. Zároveň s oznámením o změně osoby tak budou doručeny doklady, které budou prokazovat osvědčení o vzdělání a odborné kvalifikaci této nové osoby. O této změně bude vyhotoven písemný dodatek k této Smlouvě.

11. Dodavatel je povinen realizovat Předmět plnění tak, aby se vyhnul jednání, které způsobí nebo by mohlo způsobit narušení, ohrožení či přerušení IT infrastruktury Odběratele nebo narušení integrity či kvality služeb poskytovaných IT infrastrukturou Odběratele.

IV.
Cena a platební podmínky

1. Cena Předmětu plnění (dále také jen „**Cena**") je stanovena jako nejvýše přípustná a nepřekročitelná a zahrnuje veškeré náklady, rizika, zisk a finanční vlivy (např. inflace nebo vývoj kurzu české měny vůči zahraničním měnám), a to po celou dobu realizace zakázky v souladu s podmínkami uvedenými v Zadávací dokumentaci. Ceny jsou závazné a nejvýše přípustné.

2. Cena zahrnuje veškeré náklady spojené s realizací Předmětu plnění dle čl. II. této Smlouvy včetně dodání/poskytnutí Licencí a řádném poskytování SŘBI.

3. V souladu se zněním zákona č. 526/1990 Sb., o cenách se Smluvní strany dohodly na celkové Ceně za Předmět plnění ve výši:

   A/ z projektu Odběratele *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"* (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023 bude uhrazena částka za pořízení jednotlivých položek Předmětu plnění vč. potřebných Licencí, jejich instalace, Implementace, záruční technické podpory SIEM a poskytování Služeb podpory při zajištění organizačních bezpečnostní opatření dle Metodického pokynu MZ ČR, který byl zveřejněn ve Věstníku č. 7/2019 ve výši

Nabídková cena bez DPH	11 772 160,00 Kč
DPH 21 %	2 472 153,60 Kč
Nabídková cena celkem vč. DPH	14 244 313,60 Kč

   Podrobný položkový Rozpočet Předmětu plnění je uveden v příloze č. 2 této Smlouvy.

B/ Z vlastních zdrojů Odběratele bude uhrazena částka za zajištění Technické podpory nad rámec prvních 2 (slovy: dvou let), přičemž cena za zajištění Technické podpory po dobu následujících 3 (slovy: tří) let od uplynutí prvních dvou let doby poskytování Technické podpory činí ročně:

Nabídková cena bez DPH za rok	324 000,00 Kč
DPH 21 %	68 040,00 Kč
Nabídková cena za rok celkem vč. DPH	392 040,00 Kč

a tato cena bude hrazena po částech, vždy na 1 (slovy: jeden) rok trvání Technické podpory nad rámec prvních dvou let trvání Technické podpory, tj. od 3 (slovy: třetího) roku.

C/ Z vlastních zdrojů Odběratele bude uhrazena částka za poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad platformou SIEM, kdy hodinová sazba za poskytování těchto služeb činí:

Cena za 1 (slovy: jednu) hodinu poskytování služeb bez DPH	1 350,00 Kč
DPH 21 %	283,50 Kč
Cena za 1 (slovy: jednu) hodinu poskytování služeb vč. DPH	1 633,50 Kč

a tato cena bude hrazena na základě Odběratelem a Dodavatelem odsouhlaseného výkazu plnění Služeb (dále také jen „**Měsíční výkaz**"), který bude e-mailem zasílán Dodavatelem Odběrateli měsíčně, vždy do 5. (slovy: pátého) pracovního dne měsíce, který následuje po měsíci, za který je Měsíční výkaz.

4. Zálohy nebudou poskytovány.

5. Dodavatel vyúčtuje Cenu nebo její část v souladu se Smlouvou, daňovým dokladem – fakturou (dále také jen „**Faktura**"), která bude vystavena na základě Akceptačního protokolu podepsaného odpovědnými zástupci obou Smluvních stran nebo na základě Měsíčního výkazu podepsaného odpovědnými zástupci obou Smluvních stran.

6. Dodavatel výslovně prohlašuje, že je ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, plátcem DPH, resp. pro oblast přijatého plnění osobou povinnou k dani. Dodavatel se zavazuje při účtování dodávky uvést na faktuře odpovídající kód nomenklatury celního sazebníku. V případě, že se na dodávku Předmětu plnění vztahuje přenesená daňová povinnost, uvede Dodavatel na faktuře pouze platnou sazbu DPH a sdělení, že výši daně je povinen vypočítat, doplnit a přiznat Odběratel, pro kterého je plnění uskutečněno (§92f)".

7. Splatnost Faktury se sjednává do **60** (slovy: šedesát) kalendářních dnů od doručení Faktury Odběrateli.

8. Faktura musí splňovat mimo náležitostí podle ust. § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, dále níže uvedené náležitosti:

   a. předmět plnění je spolufinancován z prostředků Integrovaného regionálního operačního programu. Na Faktuře musí být vždy uveden:

      - název projektu: *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"*;
      - registrační číslo projektu: *CZ.06.3.05/0.0/0.0/15_011/0007023*;
      - věta *„Projekt je spolufinancován v rámci Integrovaného regionálního operačního programu"*,

   b. dále bude Faktura obsahovat:

      - IČ;
      - den splatnosti;
      - označení peněžního ústavu a číslo účtu, ve prospěch kterého má být provedena platba, konstantní a variabilní symbol;
      - odvolávka na smlouvu, číslo smlouvy, Dodavatele a Odběratele;
      - razítko a podpis osoby oprávněné k vystavení účetního dokladu;
      - přílohou Faktury bude kopie potvrzeného Akceptačního protokolu.

Smluvní strany se v souladu s ust. § 26, odst. 3, zákona č. 235/2004 Sb., o dani z přidané hodnoty, dohodly, že Dodavatel bude zasílat Fakturu, včetně příloh výhradně e-mailem na adresu: efakturace-inv@fno.cz.

Dodavatel se zavazuje při této komunikaci dodržovat následující pravidla:

- v jednom e-mailu budou jako přílohy zaslány dokumenty vztahující se pouze k jedné Faktuře, platí tedy pravidlo "jeden e-mail = jedna faktura a související dokumenty";
- všechny přiložené dokumenty budou výhradně ve formátu PDF a v pořadí dokladů: faktura, ostatní související dokumenty;
- Odběratel se zavazuje akceptovat takto zasílané dokumenty, pokud splňují ostatní náležitosti dané zákonem.

Pouze výjimečně je možné zasílat Fakturu v papírové podobě.

9. Za okamžik uhrazení Faktury se považuje datum, kdy byla předmětná částka odepsána z účtu Odběratele.

10. V případě, že Faktura nebude obsahovat výše uvedené náležitosti, je Odběratel oprávněn Fakturu vrátit do doby její splatnosti způsobem, který prokazuje, že do tohoto data Dodavatel vrácený daňový doklad od Odběratele převzal. V takovém případě je Dodavatel povinen Fakturu opravit a v případě, že by oprava činila Fakturu nepřehlednou, vystavit Fakturu nový. Opravená nebo nová Faktura musí být znovu zaslán Odběrateli a začíná běžet nová lhůta splatnosti.

V.
Technická podpora

1. Dodavatel zajistí Technickou podporu po dobu prvních dvou (slovy: dvou) let trvání Záruční doby ve smyslu čl. VI. odst. 4.1 této Smlouvy a případného rozšíření doby Technické podpory až o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let) a to za cenu sjednanou v čl. IV. odst. 3 písm. B/ této Smlouvy. Odběratel si vyhrazuje právo nevyužít případné rozšíření doby Technické podpory o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let). V tomto případě odešle Odběratel v době trvání Záruční doby sdělení Dodavateli, že o rozšířenou dobu Technické podpory již nemá zájem.

2. Technická podpora bude poskytnuta v režimu servis v místě instalace (tzv. on-site service).

3. Technická podpora bude poskytována v režimu:

   a) 7 x 24 (7 dnů v týdnu a 24 hodin každého dne) na dodaný Hardware a

   b) 5 x 9 (5 pracovních dnů v týdnu a 9 hodin denně od 8:00 hod do 17:00 hod, hlášené požadavky mimo tuto dobu budou považovány za nahlášené bezprostředně následující pracovní den) na platformu SIEM pokud se nejedná o Hardware.

4. Odběratel bude hlásit požadavky na poskytnutí Technické podpory (dále také jen „**Požadavky**") přes helpdesk systém Dodavatele (dále také jen „**Helpdesk**") dostupný na internetové adrese [redacted] nebo telefonicky na telefonní číslo servisního střediska Dodavatele [redacted]. Dodavatel bude veškeré Požadavky evidovat v Helpdesku a Odběratel bude mít k evidenci Požadavků přístup.

5. Dodavatel je povinen reagovat na jednotlivé Požadavky dle odst. 3.b) tohoto článku do 8 (slovy: osmi) hodin od jejich nahlášení Dodavateli postupem dle odst. 4 tohoto článku výše (dále také jen „**Reakční doba**"). V rámci Reakční doby je Dodavatel povinen (i) potvrdit přijetí Požadavku, (ii) dostavit se na místo, kde se nachází SIEM a (iii) začít s řešením Požadavku.

6. Dodavatel se zavazuje vyřešit Požadavek v následujících lhůtách:

a) v případě Technické podpory dle odst. 3 písm. a) tohoto článku, tzn., že Požadavek je zapříčiněn poruchou či závadou Hardware, zavazuje se Dodavatel k vyřešení Požadavků včetně odstranění případné závady (oprava) do 24 (slovy: dvaceti čtyřech) hodin od nahlášení Požadavku;

b) v případě Technické podpory dle odst. 3 písm. b) tohoto článku, tzn., že Požadavek je zapříčiněn jiným důvodem, než dle bodu a) výše a týká se platformy SIEM, pokud se Smluvní strany nedohodnou jinak, bude Požadavek vyřešen do 14 (slovy: čtrnácti) kalendářních dnů ode dne jeho nahlášení, to vše pokud není v této Smlouvě stanoveno jinak.

7. Požadavek se považuje za vyřešený akceptací jeho řešení Odběratelem.

8. V případě, že Požadavek nebude vyřešen ve lhůtách sjednaných v tomto článku Smlouvy, je Odběratel oprávněn uplatnit požadavek na odstranění závady SIEM přímo u jeho výrobce.

VI.
Vady Předmětu plnění, jejich uplatnění a záruka

1. Vady Předmětu plnění

1.1. Předmět plnění vykazuje vady, nemá-li vlastnosti sjednané v této Smlouvě včetně jejich příloh, tj. zejména neodpovídá-li Technické specifikaci.

2. Právní vady

2.1. Dodavatel odpovídá za to, že jím poskytnutá plnění dle této Smlouvy nebudou zatíženy právem třetí osoby.

2.2. V případě, že k plněním poskytnutým Odběrateli na základě této Smlouvy uplatní právo jakákoliv třetí osoba, zavazuje se Dodavatel nahradit Odběrateli veškerou újmu takto způsobenou, jakož i náklady vynaložené na obranu práv Odběratele. Dodavatel se v takovém případě dále zavazuje na svůj náklad poskytnout Odběrateli veškerou možnou součinnost k ochraně jeho práv. Dodavatel je povinen na své náklady vypořádat veškeré nároky třetích osob uplatněné vůči Odběrateli z titulu právních vad plnění dodaného na základě této Smlouvy. V případě soudního sporu je Dodavatel povinen zajistit řádné a svědomité vedení takového sporu a činit veškeré potřebné úkony tak, aby práva Odběratele nebyla zpochybněna z důvodu nedostatečné procesní obrany; Odběratel se zavazuje poskytnout Dodavateli potřebnou součinnost při vedení takového sporu.

3. Reklamace vad

3.1. Jakákoliv reklamace vad Předmětu plnění musí být Odběratelem provedena bez zbytečného odkladu, nejpozději do 5 (slovy: pěti) pracovních dnů, co se Odběratel o vadě dozvěděl. Uplynutím této lhůty nedochází ke ztrátě nároků Odběratele z vad Předmětu plnění.

3.2. Reklamace bude prováděna písemně. Za písemnou formu pro účely reklamace vad Předmětu plnění považují Smluvní strany rovněž e-mailovou komunikaci.

3.3. V rámci písemné reklamace musí Odběratel sdělit popis reklamované vady včetně doložení případných fotografií, pokud je má Odběratel k dispozici.

4. Záruka za jakost a možnost rozšíření její doby

4.1. Záruka za jakost na SIEM a jeho dílčí části (dále také jen „**Záruka**") je 2 (slovy: dva) roky (dále také jen „**Záruční doba**") a začíná plynout ode dne převzetí SIEM na základě podepsání Akceptačního protokolu Odběratelem.

4.2. Dodavatel se zavazuje, že po dobu Záruky bude mít SIEM vlastnosti požadované Odběratelem v rámci Technické specifikace a vlastnosti obvyklé.

4.3. Případné náklady související s odstraněním vad SIEM včetně dílů a materiálu pro jejich odstranění, jsou v případě odstranění vad v rámci Záruky, neseny Dodavatelem.

VII.
Sankční ustanovení

1. V případě, že Dodavatel nesplní povinnost dle čl. II. odst. 2 této Smlouvy, vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

2. V případě, že v průběhu trvání Záruky Odběratel zjistí, že vlastnosti (zejména technické parametry) Hardware nebo Software jsou prokazatelně v rozporu s touto Smlouvou (zejména nesplňují minimální požadované parametry uvedené v Technické specifikaci uvedené v příloze č. 1 této Smlouvy), vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

3. V případě prodlení Dodavatele s poskytnutím Technické podpory, tj. se splněním Reakční doby a/nebo splnění lhůty pro vyřešení Požadavku, delším než 2 (slovy: dva) pracovní dny, vzniká Odběrateli nárok na smluvní pokutu vůči Dodavateli ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každý den prodlení s poskytnutím Technické podpory.

4. Odběratel se zavazuje při prodlení se zaplacením ceny Předmětu plnění zaplatit Dodavateli úrok z prodlení ve výši stanovené zákonem č. 89/2012 Sb., občanským zákoníkem.

5. V případě prodlení Dodavatele s plněním Termínu plnění vzniká Odběrateli vůči Dodavateli nárok na smluvní pokutu ve výši 0,5% (slovy: pět desetin procenta) z ceny Předmětu plnění za každý započatý den prodlení. Úhradou smluvní pokuty není dotčeno právo na náhradu škody.

6. Smluvní pokuty dle tohoto článku Smlouvy jsou splatné 3. (slovy: třetí) den od doručení výzvy k jejich úhradě druhé Smluvní straně.

VIII.
Ochrana osobních údajů a důvěrných informací

1. Smluvní strany se zavazují při zpracování osobních údajů dodržovat nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „**GDPR**"). Smluvní strany berou na vědomí, že cílem této Smlouvy není zpracování osobních údajů třetích osob (ve smyslu tohoto odstavce jsou třetími osobami chápáni i zaměstnanci smluvních stran). Za předpokladu, že se i přes tuto skutečnost dostane Dodavatel do kontaktu s osobními údaji třetích osob, zavazuje se tyto zpracovávat v minimálním možném rozsahu a v souladu se smlouvou o zpracování osobních údajů uzavřenou mezi Smluvními stranami.

2. Smluvní strany se vzájemně zavazují zachovávat mlčenlivost o všech podstatných skutečnostech získaných při své činnosti vyplývající z této Smlouvy (dále jen „**Povinnost mlčenlivosti**"), a to zejména o skutečnostech, které tvoří jejich obchodní tajemství ve smyslu ust. § 504 Občanského zákoníku a důvěrné informace (dále také jen „**Důvěrné informace**").

3. Za Důvěrné informace Odběratele Smluvní strany považují zejména (nikoliv výlučně):

   a) strukturu počítačových systémů a programů Odběratele;

b) popis procesů Odběratele;

c) přístupové údaje k počítačovým systémům a programů Odběratele;

d) data Odběratele;

e) informace o plánovaném rozvoji struktury počítačových systémů a programů Odběratele.

4. Za Důvěrné informace Dodavatele Smluvní strany považují detailní funkční specifikaci Software.

5. Za Důvěrné informace kterékoliv Smluvní strany se dále považují informace a údaje, které poskytující Smluvní strana výslovně a zřetelně označí jako „důvěrné".

6. Za porušení Povinnosti mlčenlivosti je kvalifikováno jednání, jímž jedna smluvní strana jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství či Důvěrné informace získané při své činnosti od jiné Smluvní strany, pokud je to v rozporu se zájmy jiné Smluvní strany, a učiní tak bez jejího souhlasu.

7. Porušením závazku mlčenlivosti není:

a) poskytnutí obchodního tajemství a/nebo Důvěrných informací v nezbytném rozsahu orgánům nebo osobám majícím ze zákona právo na tyto informace a kontrolu činnosti Smluvních stran;

b) poskytnutí obchodního tajemství a/nebo Důvěrných informací osobám, které mají ze zákona uloženou povinnost mlčenlivosti (notář, advokát, daňový poradce);

c) poskytnutí obchodního tajemství a/nebo Důvěrných informací Smluvní strany či umožnění přístupu k němu třetím osobám v souvislosti s plněním této Smlouvy, pouze však v nezbytném rozsahu, přičemž příslušná Smluvní strana je povinna poučit tyto třetí osoby o tom, že jde o obchodní tajemství a/nebo Důvěrné informace jiné Smluvní strany a zavázat takové třetí osoby k mlčenlivosti nejméně ve stejné rozsahu v jakém je k mlčenlivosti vázána dle této Smlouvy Smluvní strana, třetí osobě takové informace sdělující;

d) použití obchodního tajemství a/nebo Důvěrných informací v souladu s touto Smlouvou nebo na základě výslovného souhlasu příslušné Smluvní strany, popř. jiné použití důvěrných informací, které se staly veřejně dostupnými nikoliv v důsledku porušení závazku mlčenlivosti povinnou Smluvní stranou;

e) použití a/nebo sdělení obchodního tajemství a/nebo Důvěrných informací Odběratelem třetí osobě za účelem správy, údržby, rozšíření, úprav, změn, oprav a dalšího nakládání se Software prováděného pro Odběratele takovou třetí osobou.

8. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace.

9. Povinnosti mlčenlivosti jsou Smluvní strany vázány po dobu trvání skutečností zakládajících tuto Povinnost mlčenlivosti, pokud nebudou mlčenlivosti zproštěny nebo se nestanou dané informace veřejně dostupnými jinak než porušením Povinnosti mlčenlivosti některou ze Smluvních stran.

10. V případě porušení Povinnosti mlčenlivosti Dodavatelem, vzniká Odběrateli nárok na smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc korun českých) za každé jednotlivé porušení Povinnosti mlčenlivosti. Tato smluvní pokuta je splatná do 10 (slovy: deseti) kalendářních dnů od doručení výzvy k její úhradě. Úhradou této smluvní pokuty není dotčen nárok Odběratele na náhradu škody ani nárok na případné sankce ze závislých smluv na této Smlouvě.

IX.
Ukončení Smlouvy

1. Odběratel je oprávněn od této Smlouvy odstoupit kromě podmínek daných zákonem č. 89/2012 Sb., občanským zákoníkem a případů sjednaných v této Smlouvě, rovněž v následujících případech, které se považují za podstatné porušení této Smlouvy:

[redacted]

a) prodlení Dodavatele s dodáním Hardware, Licencí nebo jiných plnění dle této Smlouvy, které je delší než 60 (slovy: šedesát) kalendářních dnů;

b) prodlení s Technickou podporou o více než 7 (slovy: sedm) kalendářních dnů.

2. V případě odstoupení od Smlouvy jsou si Smluvní strany povinny vrátit vše, co si v souvislosti s touto Smlouvou plnily, přičemž Smluvní strany se dohodly, že dojde-li k odstoupení v druhém nebo dalším roce trvání platnosti této Smlouvy, není Dodavatel povinen vracet tu část uhrazené Ceny, po jaký počet měsíců trvala tato Smlouva.

3. Zánikem Smlouvy z důvodu odstoupení od Smlouvy nezanikají nároky na smluvní pokuty sjednané v čl. VII. této Smlouvy, stejně jako nezaniká právo na náhradu škody.

X.
Závěrečná ustanovení

1. Pohledávky vyplývající z této Smlouvy nemohou být postoupeny třetí osobě bez předchozího písemného souhlasu druhé Smluvní strany.

2. V souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, je Dodavatel osobou povinnou spolupůsobit při výkonu finanční kontroly. Tato povinnost se vztahuje na právnickou nebo fyzickou osobu, podílející se na dodávkách zboží nebo služeb hrazených z veřejných rozpočtů nebo z veřejné finanční podpory.

3. Dodavatel je povinen archivovat veškerou dokumentaci související s realizací Předmětu plnění, zejména originální vyhotovení Smlouvy, její dodatky, originály účetních dokladů a dalších dokladů vztahujících se k realizaci Předmětu plnění této Smlouvy po dobu 10 (slovy: deseti) let od zániku závazku vyplývajícího ze Smlouvy a po tuto dobu je Dodavatel rovněž povinen umožnit kontrolu těchto dokladů osobám oprávněným k výkonu kontroly Předmětu plnění a vytvořit těmto osobám podmínky k provedení kontroly vztahující se k realizaci Předmětu plnění a poskytnout jim při provádění kontroly součinnost.

4. Smluvní strany se dohodly, že 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), tuto Smlouvu, včetně případných dodatků, v Registru smluv uveřejní Odběratel.

5. Veškeré změny a doplňky této Smlouvy je možné činit písemně, a to formou číslovaných dodatků.

6. Tato Smlouva je sepsána ve 2 (slovy: dvou) vyhotoveních s platností originálu, z nichž každá Smluvní strana obdrží po jednom.

7. Veškeré právní vztahy touto Smlouvou neupravené se řídí obecně závaznými právními předpisy České republiky, zejména zákona č. 89/2012 Sb., občanským zákoníkem.

8. Tato Smlouva nabývá platnosti podpisem obou Smluvních stran a účinnosti od data zveřejnění v Registru smluv.

9. Jestliže jednotlivá ustanovení této Smlouvy jsou nebo se stanou zcela nebo částečně neplatnými nebo jestliže v této Smlouvě nějaké ustanovení zcela chybí, není tím dotčena platnost ostatních ustanovení. Namísto neplatného či chybějícího ustanovení dohodnou Smluvní strany takové platné ustanovení, které nejvíce odpovídá smyslu a účelu neplatného či chybějícího ustanovení.

Přílohy:

Příloha č. 1 - Technická specifikace Předmětu plnění;
Příloha č. 2 – Položkový rozpočet Předmětu plnění
Příloha č. 3 – Realizační tým Dodavatele

V Ostravě, dne ----------

MUDr. Jiří Havrlant
Digitálně podepsal MUDr. Jiří Havrlant
Datum: 2020.10.08 10:57:37 +02'00'

Fakultní nemocnice Ostrava
MUDr. Jiří Havrlant, MHA
ředitel

V Praze ---------- , dne ----------

Jiří Chovanec
Digitálně podepsal Jiří Chovanec
Datum: 2020.10.05 13:36:15 +02'00'

TOTAL SERVICE a.s.
Jiří Chovanec
člen představenstva

Příloha č. 1

Technická specifikace předmětu plnění

Dodávka a implementace SIEM a služby v rámci kybernetické a informační bezpečnosti – technická specifikace.

Předmět

1. Předmětem této veřejné zakázky je dodávka a implementace systému pro řízení bezpečnostních informací a událostí – SIEM. Součástí předmětu veřejné zakázky je dodávka potřebného hardware, software resp. licencí programového vybavení a poskytnutí souvisejících služeb v rámci kybernetické a informační bezpečnosti - organizačních opatření po dobu 5 let, přičemž požadované řešení tvoří součást opatření k zajištění standardů kybernetické bezpečnosti podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění. Řešení musí být navrženo pro sběr dat, jejich korelaci a dostupnost ze dvou datových center zadavatele.

2. Součástí předmětu plnění je zejména:

   a) Dodávka technologie SIEM a její implementace

   - Zpracování návrhu implementace před dodáním vlastního řešení.

     Výstupem bude návrh implementace řešení SIEM, ve kterém dodavatel popíše implementaci dle požadavku zadání (které zdroje bezpečnostních logů a síťových flows a v jakém režimu bude sledovat) a mimo jiné bude obsahovat:

     - způsob zasílání logů do řešení SIEM minimálně z následujících typů zdrojů: síťové přepínače Cisco, servery OS Windows, servery OS Linux, databáze Oracle a MS SQL, poštovní systém MS Exchange, Antispam Barracuda, Antivirus ESET, aplikační firewall Cisco ASA Sourcefire, VPN koncentrátory Cisco ASA, Disková pole Netapp a MSA, HW servery, Cisco ISE server, Virtualizační platforma VMware Vsphere, MDM VMware AirWatch, MS Active Directory, ISC DHCP server, Tacacs+ server tac-plus, Radius server freeradius, aplikace NIS IKIS;
     - způsob iniciálního nastavení alarmů, reportů, rolí a uživatelů;
     - způsob nasazení modulu testování zranitelností
     - způsob nasazení modulu ochrany databázového prostředí
     - doporučení činností k provozování a údržbě řešení SIEM Zadavatelem

   - Dodávka HW platformy pro SIEM a příslušných licencí
     - licence SIEM, včetně modulu testování zranitelností a modulu ochrany databázového prostředí
     - HW platforma (servery) včetně jejich instalace a implementace určené pro provoz SIEM řešení
     - HW platforma i licence budou se standardní zárukou (podporou) 2 roky, a s rozšířením této podpory na celkové období 5 let včetně nároku na aktuální verze SW

   - Instalace, konfigurace a nastavení SIEM pro integraci bezpečnostních událostí a jejich centrálního vyhodnocování musí vycházet z návrhu implementace řešení SIEM a musí zahrnovat následující kroky:
     - instalace hardware v prostředí zadavatele
     - instalace platformy SIEM, funkce testování zranitelností a funkce ochrany databázového prostředí
     - instalace agentů, pokud jsou pro daný systém potřeba a zajištění sběru logů z monitorovaných zařízení do řešení SIEM
     - nastavení logovacích politik dle požadavků zadavatele
     - konfigurace zálohování a archivace SIEM

- nastavení síťových prvků pro sledování (konfigurace syslog a flows)
- nastavení serverů pro sledování
- nastavení výstražného systému, včetně nastavení email notifikace
- zapojení všech požadovaných zdrojů bezpečnostních logů a konfiguraci nabízeného systému SIEM
- integraci SIEM na helpdeskový systém Zadavatele (Alvao Service Desk) u vybraných kategorií incidentů. Integraci je možné zajistit odesíláním emailů v požadovaném formátu na určenou adresu.
- vytvoření parserů pro následující informační systémy (software):
    - NIS, RIS – Medical Systems
    - LIS – Stapro
    - PACS – ORCZ
    - IntelliPAT – SW Services (Roman Stejskal)
    - Transfúzní IS – TIS Brno
    - Personální systém (VEMA) – VEMA
    - Lékárenský systém (MEDIOX) – Apatyka
    - Vyvolávací systém (MedOrganizer) – Artiis Brno
- integrace monitorovaných technologií v rozsahu minimálně:
    - 100x Windows Server (2008-2016)
    - 80x Linux Server (Debian 8+, Centos 6+, RedHat)
    - 100x Přepínače LAN (Cisco 2960X, 3750X, 9x00)
    - 50x DB server (MS SQL, MySQL, MariaDB, PostgreSQL, Informix, Oracle)
    - 1x Ochrana databáze aplikace NIS (Oracle cluster v režimu Active-Active)
    - 7x Firewall (ASA 5506X, 5525X, 5585X)
    - 2x Wireless controller (Cisco 5520 WLC)
    - 2x Exchange server (2010)
    - 1x Cisco Prime (3.6)
    - 2x Cisco ISE server (2.0.x)
    - 1x Cisco Firepower Management Center (6.0.x)
    - 1x MDM VMware Workspace ONE
    - 1x TACACS+ server tac-plus (Debian)
    - 1x ESET Management Console
    - 3x DNS server (bind)
    - 3x DHCP server (ISC DHCP server, Debian)
    - 3x Radius/LDAP (freeradius, Debian)
    - 2x Email Content/Spam Filtering (Barracuda Spam & Virus Firewall 400)
- u těchto technologií bude provedeno:
    - nastavení sběru a zpracování událostí z monitorovaných technologií;
    - zajištění sběru dat, jejich uložení a korelaci i v případě výpadku jednoho ze dvou datových center;
    - vytvoření logických skupin monitorovaných zařízení podle typu;
    - nastavení korelačních pravidel nad jednotlivými zdroji událostí
    - konfigurace a nastavení rolí/skupin a oprávnění k monitorovaným zdrojům dle kompetencí;
    - začlenění do modulu testování zranitelností v minimálním počtu 500 zařízení;
- testování a ověření funkčnosti
- nastavení reportování
- dokumentace skutečného stavu v rozsahu:
    - popis řešení a jeho jednotlivých komponent,
    - výčet použitých HW komponent včetně výrobních čísel,

- výčet použitých SW licencí,
- příručka pro práci uživatelů s jednotlivými částmi systému, provozní dokumentace včetně postupů řešení běžných provozních situací

○ zaškolení pracovníků FNO v rozsahu nutném pro zvládnutí každodenní správy systému SIEM, modulu pro testování zranitelností a modulu pro ochranu databázového prostředí v minimálním rozsahu 40 hodin pro 6 lidí. Školení bude probíhat v prostorách FNO a v termínech stanovených ÚNIT FNO

b) Služby podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZČR, který byl zveřejněn ve Věstníku č. 7/2019 (http://www.mzcr.cz/Legislativa/dokumenty/vestnik-c7/2019_17620_3977_11.html) v následujících oblastech:

- systém řízení bezpečnosti informací, řízení rizik
- bezpečnostní politika, návrh a dokumentace procesů SŘBI
- bezpečnostní postupy a dokumentace
- návrh projektů na zavedení technických opatření s důrazem na nástroje
- organizační bezpečnost
- stanovení bezpečnostních požadavků pro dodavatele
- řízení aktiv
- bezpečnost lidských zdrojů
- řízení provozu a komunikací
- řízení přístupu osob
- akvizice, vývoj a údržba
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- kontrola a audit

c) Záruční technická podpora platformy SIEM:

- Služby správy a údržby platformy SIEM při řešení provozních problémů a vyhodnocování událostí v rozsahu ladění a konfigurace stávajících i nových zdrojů logů, dashboardů, reportů a připojování nových zařízení do SIEM, vlastní obsluha zařízení SIEM, generování výstupů pro reporty, sestavování dotazů a korelačních pravidel;
- Garance zahájení prací následující pracovní den po nahlášení požadavku; hlášení požadavků v režimu 9x5 (9 hodin denně a 5 dnů v týdnu, v pracovní době od 8:00 do 17:00 hod), hlášené požadavky mimo uvedenou pracovní dobu budou považovány za nahlášené bezprostředně následující pracovní den; na dodaný HW je úroveň podpory 7x24 s reakční dobou 8 hodin a garantovanou opravou do 24 hodin od nahlášení.
- Požadovaný rozsah prací 40 hodin za 1 měsíc po celou záruční dobu 24 měsíců

d) Rozšířená podpora provozu platformy SIEM:

- Služby kybernetické bezpečnosti na platformě SIEM, podpora při vyhodnocování událostí a rizik, bezpečnostní monitoring z pohledu kybernetické bezpečnosti, obsluha platformy SIEM, nastavování zdrojů logů, generování výstupů pro reporty, sestavování dotazů a korelačních pravidel;
- Pravidelná týdenní konzultace týkající se vyhodnocování funkčnosti systému a případných úprav konfigurace SIEM řešení
- Garance zahájení prací následující pracovní den po nahlášení požadavku; hlášení požadavků v režimu 9x5 (9 hodin denně a 5 dnů v týdnu, v pracovní době od 8:00 do 17:00 hod), hlášené požadavky mimo uvedenou pracovní dobu budou považovány za nahlášené bezprostředně následující pracovní den; na dodaný HW je úroveň podpory 7x24 s reakční dobou 8 hodin a garantovanou opravou do 24 hodin od nahlášení.

- Požadovaný rozsah prací 20 hodin za 1 měsíc po dobu následujících 36 měsíců

e) Poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad platformou SIEM formou služby v předpokládaném rozsahu 52 hodin za měsíc:
   - hodnocení bezpečnostních událostí:
     - analýza trendu závažnosti zjištěných událostí v závislosti na typu a hodnotě sledovaných informačních aktiv
     - hodnocení událostí v závislosti na přijatých organizačních a technických opatření. Analýza trendu v hodnocení těchto událostí a účinnosti přijatých opatření.
     - informace o počtu a závažnosti zjištěných událostí a evidovaných zranitelnostech.
     - informace o stavu zranitelností z provedených testů zranitelností v metrice odpovídající metrice hodnocení událostí. Analýza trendu výskytu zranitelností.
     - roční vyhodnocování účinnosti systému řízení bezpečnosti informací formou služby.
     - hodnocení událostí a klasifikace incidentů v závislosti na hodnotách dotčených informačních aktiv.

   - průběžná správa rizik:
     - zpracování vstupních dat o úrovni rizik z registrů rizik vedených v databázích nebo samostatných dokumentech.
     - informace o úrovni rizik ve vazbě na sledovaná informační aktiva a identifikované události. Analýza trendu vývoje úrovně rizik.
     - informace o stavu a trendu plnění bezpečnostních cílů a opatření v systému řízení bezpečnosti informací.

   - roční hodnocení aktiv a rizik:
     - provedení případné aktualizace metodiky hodnocení aktiv a rizik FNO
     - provedení aktualizace aktiv a jejich hodnoty včetně úpravy pravidel pro manipulaci a likvidaci informací
     - provedení ročního hodnocení rizik včetně:
       - zpracování zprávy o hodnocení rizik
       - aktualizace Prohlášení o aplikovatelnosti
       - aktualizace Plánu zvládání rizik.

   - hodnocení shody formou služby:
     - informace o stavu vypořádávání neshod systému řízení bezpečnosti informací. Analýza trendu vypořádávání neshod.
     - hodnocení neshod systému řízení bezpečnosti informací v závislosti na zjištěné události a evidované zranitelnosti.

   - roční vyhodnocování účinnosti systému řízení bezpečnosti informací formou služby
     - shromáždění podkladů pro hodnocení:
       - stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik
       - posouzení výsledků provedených auditů kybernetické bezpečnosti a

dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací

- podpora při zpracování roční zprávy k vyhodnocování účinnosti systému řízení bezpečnosti informací

- reporting
  - zpřístupnění reportů z hodnocení bezpečnostních událostí a průběžné správy rizik jednotlivým rolím (IT manažer a bezpečnostní manažer s možností konfigurace dalších rolí) skrze on-line rozhraní s okamžitou aktualizací dle aktuálních dat

Harmonogram projektu

Služby budou provedeny v následujících etapách, odhadovaném rozsahu a požadovaných termínech:

Etapy zavedení SŘBI	Činnosti	Výstupy	Počet MD	Termín realizace od podpisu smlouvy
Etapa 1: Bezpečnostní politika, návrh a dokumentace procesů SŘBI	Obsahem fáze bude navržení vrcholových dokumentů obsahujících popis procesů - Návrh, projednání a popis postupů pro organizaci systému informační a kybernetické bezpečnosti a naplnění bezpečnostních a regulatorních požadavků. - Návrh vrcholové Bezpečnostní politiky v oblasti SŘBI	• Zavedení a formalizace **procesu systému řízení bezpečnosti informací** a řízení rizik informací – procesní dokument **Směrnice řízení bezpečnosti informací ve FNO** • **Bezpečnostní politika v oblasti SŘBI** – dokument obsahující hlavní zásady, cíle, potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací FNO,	15	T+20
Etapa 2: Bezpečnostní postupy a dokumentace	Návrh zásad a postupů v oblastech: • Řízení aktiv • Řízení rizik • Řízení dodavatelů • Bezpečnost lidských zdrojů • Řízení provozu a komunikací • Řízení změn • Řízení přístupu • Akvizice, vývoj a údržba • Správa kybernetických bezpečnostních událostí	Výstupy budou zahrnovat dvojí způsob zpracování: 1. **Doplnění a úprava stávajících dokumentů**, a to zejména v oblastech: a. IT b. Personální práce c. Fyzické bezpečnosti d. Řízení projektů (dodavatelů) e. Auditu 2. **Vytvoření nových dokumentů** – zejména: a. směrnice s důrazem na	20	T+60

Etapy zavedení SŘBI	Činnosti	Výstupy	Počet MD	Termín realizace od podpisu smlouvy
	a incidentů • Řízení kontinuity činností • Audit kybernetické bezpečnosti • Fyzická bezpečnost	• Uživatelská bezpečnost • IT bezpečnost b. Bezpečnostní požadavky do smluv s dodavateli FNO		
Etapa 3 A: Návrh projektů na zavedení technických opatření s důrazem na nástroje	Návrh způsobu zavedení nástrojů k zajištění kybernetické bezpečnosti v oblastech: • Bezpečnost komunikačních sítí • Správa a ověřování identit • Sběr a vyhodnocování kybernetických bezpečnostních událostí • Aplikační bezpečnost	Výstupem bude provedení analytických činností (studie proveditelnosti) s cílem vytvořit zadání pro zpracování návrhu implementace: • **802.1x** pro přihlášení při fyzickém připojení k počítačové síti (ethernet a wifi) s ohledem na typ a kategorii připojovaného zařízení (počítač, zdravotnická technika, MaR, zařízení IT infrastruktury, mobilní zařízení s OS Windows, Android a IOS apod.) • **Více-faktorová autentizace** pro přihlašování k operačním a informačním systémům • Systém řízení rizik a shody Vytvoření dlouhodobého **plánu bezpečnostních testů** jednotlivých informačních systémů	20	T+90
Etapa 3 B: Implementace technických opatření SIEM	Dodávka a Implementace nástroje k zajištění kybernetické bezpečnosti v oblastech: • Sběr a vyhodnocování kybernetických bezpečnostních událostí • Test zranitelností • Zabezpečení databázového prostředí aplikace NIS	Výstupy jsou následující: • **Implementace systému SIEM** pro sběr a vyhodnocování kybernetických bezpečnostních událostí, včetně modulu testování zranitelností a modulu ochrany databázového prostředí, dle oboustranně odsouhlaseného návrhu implementace řešení SIEM • Vytvoření dokumentace skutečného stavu	60	T+160
Etapa 4: Plán bezpečnostního	Nejprve je potřebné navrhnout koncepci tvorby a budování bezpečnostního povědomí zaměstnanců FNO včetně způsobu	**Plán rozvoje bezpečnostního povědomí**	10	T+120

Etapy zavedení SŘBI	Činnosti	Výstupy	Počet MD	Termín realizace od podpisu smlouvy
povědomí zaměstnanců (školení, informovanost, odborná způsobilost)	bezpečnostního vzdělávání (zaměstnanci zastávající bezpečnostní role) a školení (všichni uživatelé informací). Poté je nutné upřesnit: • formu, četnost a bodový obsah školení a vzdělávání • Návrh druhů školení (poučení nových zaměstnanců, při zavedení nových postupů a aplikací, po vyhodnocení incidentu/události) • Návrh způsobu ověření rozvoje bezpečnostního povědomí a toto uvést do **Plánu rozvoje bezpečnostního povědomí**			
Etapa 5: Interní audity a přezkoumání SŘBI	**Zavést činnosti spojené s plánováním interních auditů SŘBI**, tyto činnosti budou v základu popsány ve směrnici řízení bezpečnosti informací ve FNO. Vlastní auditorské postupy se zapracují do stávající auditní dokumentace. Dále budou zpracovány: **Program interního auditu SŘBI** – dokument popisující auditované oblasti SŘBI, zdroje, požadavky na součinnost a perioda provedení interních auditů SŘBI. **Plán interního auditu SŘBI** – dokument upřesňující provedení konkrétního	**Program interního auditu SŘBI** **Plán interního auditu SŘBI** **Metodika řízení interních auditů SŘBI** **Metodika přezkoumání SŘBI** **Zpráva z interního auditu SŘBI** **Specifikace vstupů** pro pravidelné vyhodnocení účinnosti SŘBI **Struktura pravidelného vyhodnocení účinnosti SŘBI** **Podpora při vyhodnocení účinnosti SŘBI**	25	T+160

Etapy zavedení SŘBI	Činnosti	Výstupy	Počet MD	Termín realizace od podpisu smlouvy
	interního auditu SŘBI. **Metodika řízení interních auditů SŘBI** – dokument popisující způsob provádění, kritéria a způsob hodnocení interních auditů SŘBI. **Po zpracování metodik bude proveden vzorový interní audit** s cílem zaškolit interní auditory SŘBI ve FNO. Z auditu bude zpracována Zpráva z interního auditu SŘBI, která bude mimo podmínek auditu uvádět kritéria auditu, stav SŘBI FNO a zjištěné neshody s požadovaným stavem. Následně budou navrženy a zdokumentovány postupy pro provádění pravidelného hodnocení stavu – přezkoumání SŘBI ve FNO. Na závěr etapy bude **poskytnuta podpora při provedení pravidelného vyhodnocení účinnosti SŘBI**, která bude zejména obsahovat hodnocení stavu SŘBI, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na SŘBI.			
Etapa 6: Harmonizace a podpora přípravy	Na závěr implementace postupů bude zpracována zpráva, která bude obsahovat vyhodnocení projektu a doporučení, která budou nezbytná pro další	**Zpráva o stavu implementace a dalším postupu při provozu SŘBI** – dokument hodnotící stav SŘBI s návrhem dalšího postupu.	10	T+180

Etapy zavedení SŘBI	Činnosti	Výstupy	Počet MD	Termín realizace od podpisu smlouvy
organizace v dalších činnostech	rozvoj SŘBI. Zpráva bude projednána se zástupci FNO. Na samotný závěr projektu bude aktualizován Plán zvládání rizik FNO.	**Aktualizovaný Plán zvládání rizik** – se zapracování změn na základě provedení interního auditu SŘBI a provedeného pravidelného vyhodnocení účinnosti SŘBI		
	Celkem za implementaci		160	T+180

Minimální technické parametry platformy SIEM.

SIEM bude automaticky sbírat, archivovat a analyzovat data, zahrnující logy bezpečnostní povahy napříč celou infrastrukturou od síťových prvků přes různé operační systémy až po specifické IS FNO. Nad těmito daty bude probíhat analýza a notifikace vyhodnocených bezpečnostních událostí a dalších fenoménů. Díky SIEM budou mít správci aktuální přehled o potencionálních i skutečných anomáliích, hrozbách a bezpečnostních incidentech monitorovaného prostředí. Řešení SIEM musí podporovat centrální sběr a zpracování logů, jejich normalizaci, grafickou interpretaci a archivaci, centrální správu a reporting, a to včetně vyhodnocení svých vlastních logů.

Součástí nabídky řešení dodavatele bude podrobný popis použitých prvků řešení, se zdůrazněním toho jak plní požadované technické parametry.

Dodavatel zprovozní celé řešení (hardware i software) v místě zadavatele.

Řešení bude nasazeno formou distribuované HW appliance, skládající se z jednotlivých HW/SW modulů. SW řešení pak musí být dodáno jako ucelené tj. od jednoho výrobce, včetně společné a jednotné management konzole;

Všechny v zadání zmíněné parametry jsou definovány jako minimální, není-li uvedeno jinak.
Celkové dodávané řešení musí splňovat následující základní technické požadavky.

Shrnutí základních vlastností poptávaného SIEM řešení:

- licence pro trvalé zpracování 2 500 EPS (Events Per Second) a 150 000 FPM (Flows per Second)
- licence pro modul testování zranitelností pro minimálně 500 IP adres, který je přímo součástí rozhraní pro správu SIEM
- licence pro modul ochrany databáze aplikace NIS (Oracle cluster v režimu Active-Active)
- úložná kapacita pro logy a flow za období minimálně 18 měsíců o předpokládané celkové velikosti nejméně 22TB;
- komplexní zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase
- pokročilé techniky detekce hrozeb APT a „Zero-Day" útoků, včetně behaviorální analýzy
- monitorování chování v síti, tvorba přehledných reportů
- identifikace a kategorizace zranitelností. Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení pro její odstranění.
- možnost filtrováni nalezených zranitelností a jejich prioritizace. Možnost tvorby pravidel pro korelaci nad filtry zranitelností

- podpora operačních systémů Windows/Linux, síťových zařízení (swtiche, routery, firewally), databází, webových serverů, mail serverů, DNS serverů a koncových zařízení.
- snížení rizik provozovaných aplikací a možnosti jejich kompromitace. Detekce kybernetických bezpečnostních událostí a zajištění reakce na incidenty a to zejména analýzou prostředí v reálném čase a zajištění včasné reakce na vzniklé události a porušení dat.
- možnost forenzního šetření a analýzy nad událostmi z mnoha typů zdrojů a zařízení. Automatizovaná korelace událostí a následná reakce na identifikované problémy. Minimalizace rizik včasnou identifikací skutečných útoků.
- zajištění souladu s regulatorními a legislativními požadavky regulatorních orgánů jestli jsou ve shodě s požadovanými pravidly (nebo vlastními) pro konfiguraci systémů nebo zařízení a vyhodnocování událostí z těchto systémů. Zajištění požadavků Zákona o kybernetické bezpečnosti.

Pravidla pro vyplňování technických parametrů řešení

V níže uvedené tabulce (sloupci 1) jsou uvedeny veškeré povinné minimální parametry kladené na celý systém SIEM a včetně dodávaných serverů. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.
Sloupec „Způsob splnění požadovaného parametru" bude obsahovat krátký popis, jak dodavatel požadavek naplní a pokud je požadován, i „Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru".
Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky.

POVINNÉ PARAMETRY SIEM řešení

Dodavatel musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena

Parametr	Popis technických parametrů	Způsob splnění požadovaného parametru a pokud je požadován, i „Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru".
1.	Podpora logů protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, SFTP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file (plain text).	Ano splňuje. Nabízené řešení podporuje nejen všechny požadované typy protokolů pro sběr událostí, ale i další.
2.	Sběr logů bez nutnosti instalovat agenta na zdrojový systém.	Ano splňuje. Nabízené řešení umožnuje bez-agentní sběr u protokolů, kde je to možné. Nabízené řešení umožňuje mimo bez-agentního sběru také sběr dat pomocí agentů či aktivního čtení cílových souborů nebo databází. Takto načtené události jsou normalizovány a je s nimi pracováno jako s ostatními nasbíranými událostmi (logy).
3.	Sběr logů také lokálním kolektorem s přeposíláním do SIEMu.	Ano splňuje. Navrhované řešení podporuje využití lokálního kolektoru událostí s přeposíláním do SIEMu. Sběr logů je oddělen od centrálního prvku a funguje plně samostatně, tedy i v případě výpadku centrálního prvku nedochází k výpadku sběru logů. Nabízené řešení je připraveno na rozšíření o další prvky pro sběr nebo vyhodnocování dle potřeby. Další prvky zle přidávat pro účely rozložení zátěže, rozšíření sběru událostí do nových segmentů či vzdálených poboček. Stávající i nově přidané prvky lze stále řídit z jedné centrální konzole.
4.	Podpora šifrované komunikace mezi zdroji logů a SIEM.	Ano splňuje. Nabízené řešení podporuje komunikaci a zasílání logů šifrovanou komunikací. Nabízené řešení taktéž podporuje schopnost šifrovat připojení mezi jednotlivými komponentami SIEMu, aby byla zajištěna bezpečnost dat v síti.
5.	Licence pro trvalé zpracování 2 500 EPS a 150 000 FPM s možností rozšíření až na 15 000 EPS bez nutnosti upgrade nebo doplnění HW.	Ano splňuje. Nabízené řešení je schopno výkonově i licenčně trvale zpracovávat 2 500 EPS a 150 000

<table>
<tr><td></td><td></td><td>FPM bez jakýchkoliv dalších omezení. Nabízené řešení je možno v budoucnu licenčně rozšířit až na zpracování 15 000 EPS bez nutnosti upgrade nebo doplnění HW.</td></tr>
<tr><td>6.</td><td>Řešení nebude licenčně omezeno úložnou kapacitou ani počtem zdrojů událostí.</td><td>Ano splňuje. Nabízené řešení není licenčně omezeno počtem zdrojů událostí. Ať se jedná o logy podporované přímo výrobcem, či vlastní logy. Nabízené řešení taktéž není licenčně omezeno velikostí příchozích logů, délkou jejich uložení nebo úložnou kapacitou.</td></tr>
<tr><td>7.</td><td>Uchování nasbíraných dat nejméně po dobu 18 měsíců, bez nutnosti použití externích paměťových zařízení.</td><td>Ano splňuje. Nabízené řešení obsahuje interní kapacitu úložného prostoru podle požadavků, tedy dostatečnou kapacitu pro uložení logů (včetně RAW logů) a síťových toků po dobu 18 měsíců.</td></tr>
<tr><td>8.</td><td>Řešení musí mít schopnost uchovat nejméně 22TB dat (v normalizovaném i RAW formátu), aniž by vyžadovalo použití externích paměťových zařízení.</td><td>Ano splňuje. Nabízené řešení obsahuje interní úložnou kapacitu vyšší než 22 TB, tedy dostatečnou kapacitu pro uložení 18 měsíců logů v normalizovaném a RAW formátu plus síťových toků.</td></tr>
<tr><td>9.</td><td>Podpora výrobce na 5 let včetně SW upgrade.</td><td>Ano splňuje. Nabízené řešení obsahuje podporu výrobce na 5 let včetně možnosti SW upgrade a pravidelných aplikací.</td></tr>
<tr><td>10.</td><td>Řešení musí integrovat sběr událostí ze KII/ISZS/IS/KS, jejichž výčet je uveden dále s tím, že IT FNO zajistí u dodavatelů jednotlivých IS podporu protokolů syslog nebo Windows Events Collection v uvedených systémech:
<table>
<tr><th>Název</th><th>Popis</th><th>Typ</th></tr>
<tr><td>NIS</td><td>Nemocniční informační systém (Medical Systems)</td><td>ISZS</td></tr>
<tr><td>LIS</td><td>Laboratorní informační systém (Stapro)</td><td>ISZS</td></tr>
<tr><td>RIS</td><td>Radiologický informační systém (Medical Systems</td><td>ISZS</td></tr>
<tr><td>PACS</td><td>Systém pro správu zdravotní obrazové dokumentace (ORCZ)</td><td>IS</td></tr>
<tr><td>LékIS</td><td>Lékárenský informační systém (Mediox - Apatyka)</td><td>IS</td></tr>
<tr><td>IntelliPAT</td><td>Informační systém pro evidenci histologických, cytologických, toxikologických a pitevních vyšetření</td><td>ISZS</td></tr>
</table></td><td>Ano splňuje. Nabízené řešení umožňuje sběr událostí protokoly syslog a Windows Events Collection, které IT FNO zajistí. Nabízené řešení tedy umožňuje sběr a integraci událostí z vyjmenovaných systémů.</td></tr>
</table>

		(SW Services – Roman Stejskal)		
	Transfúzní IS	**Informační systém transfúzní stanice** (TIS Brno)	**ISZS**	
	Vyvolávací systém	Objednávání a plánování vyšetření pacientů (MediOrganizer – ARTIIS GROUP)	IS	
	Personalistika	Personální informační systém (Vema)	IS	
	Intranet	Systém informací a aplikací podporující provoz FNO (MS Sharepoint)	IS	
	e-mail	Elektronická poštovní služba (MS Exchange)	KS	
	Campus infrastruktura	Páteřní a distribuční komunikační infrastruktura FNO (Cisco)	KS	
	LAN infrastruktura - Access	Pevná a bezdrátová přístupová komunikační infrastruktura FNO (Cisco)	KS	
	VPN infrastruktura	Infrastruktura pro bezpečné připojení externích dodavatelů a servisních pracovníků do Infrastruktury FNO (Cisco)	KS	
	Infrastruktura připojení k síti Internet a externím sítím	Infrastruktura připojení k mezinárodní síti Internet a dalším externím sítím (Cisco)	KS	
11.	Řešení musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z následujících oblastí: • útoky robotů, červů a virů; • neoprávněný přístup k aplikacím; • chyby a změny v sítích (chyby a stavy síťových zařízení); • monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, varování systémů IPS/IDS, využívání šíře pásma; • porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace); • masivní šifrování dat (ransomware); • vědomá snaha nebo neuvědomělá činnost vedoucí k odcizení nebo znehodnocení důvěrných dat (porušení logů LM a SIEM, porušení časových razítek apod.)			Ano splňuje. Nabízené řešení obsahuje více než 400 korelačních pravidel, které implementují nejběžnější Use cases, které pokrývají vyjmenované oblasti. Další korelační pravidla si lze volně stáhnout z IBM portálu případně zcela volně vytvářet vlastní pravidla.
12.	Podpora záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku).			Ano splňuje. Nabízené řešení podporuje nastavení automatických záloh nejen konfigurace ale i

		auditních dat (logy událostí a síťové toky). Tyto zálohy lze ukládat na připojené externí uložiště.
13.	Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní. Nabízené řešení nesmí být založeno na technologiích Java, Flash nebo na bázi tlustého klienta.	Ano splňuje. Nabízené řešení je řízeno z centrální konzole umožňující kompletní práci se systémem a jeho administraci. Grafické prostředí je přístupné pomocí nejrozšířenějších prohlížečů a využívá bezpečný HTTPS protokol. Pro práci s administrační konzolí není třeba instalace doplňků Java či Flash.
14.	Podpora přístupu více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení či síťovým segmentům a serverům, typu vstupních dat, apod.	Ano splňuje. Nabízené řešení přístup vícero uživatelů současně a umožňuje definovat přístup uživatelům k datům v SIEMu na úrovni definovaných síťových segmentů, zdrojů logů či skupin zdrojů.
15.	Integrace s adresářovým systémem (LDAP, Active Directory a RADIUS) pro potřeby autentizace uživatelů. Systém ale musí rovněž umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti externích autentizačních mechanismů).	Ano splňuje. Nabízené řešení umožnuje autorizaci uživatelů pomocí integrace s adresářovým systémem a možností mapovat skupiny uživatelů na uživatelské role v rámci SIEMu. Dále nabízené řešení umožňuje také přihlašování pomocí lokálních účtů.
16.	Automatická identifikace systémů – zdrojů logů	Ano splňuje. Nabízené řešení automaticky identifikuje zdroje událostí a pokud rozpozná zdrojový systém automaticky zaregistruje nový zdroj událostí s přidělením příslušného parseru pro správnou normalizaci událostí.
17.	Log Management s minimální postimplementační administrací (agregace událostí dle typů, analýza, vyhodnocování) pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí	Ano splňuje. Nabízené řešení nabízí díky automatickému rozpoznávání zdrojů událostí, jejich normalizaci, zařazení do skupin a mnoha korelačních pravidel obsažených v základu, poskytuje minimální postimplementační administraci.
18.	Minimální administrace (výběr zařízení ze seznamu od výrobce) pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, síťové prvky)	Ano splňuje. Nabízené řešení nabízí široký seznam podporovaných zdrojových systémů a při jejich integraci je možno jednoduše vybrat připojovaný systém ze seznamu a tím zajistit zařazení do správné skupiny a bezproblémové normalizace.

19.	Automatické připojení a samoučící rozpoznání připojených zařízení.	Ano splňuje. Nabízené řešení automaticky identifikuje zdroje událostí a pokud rozpozná zdrojový systém automaticky zaregistruje nový zdroj událostí s přidělením příslušného parseru pro správnou normalizaci událostí.
20.	Podpora sběru síťových toků a automatická identifikace (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, NetFlow sondy).	Ano splňuje. Nabízené řešení umožňuje sběr a normalizaci síťových toků přímo z vlastních síťových karet, případně umožňuje přijímat toky ze síťových zařízení známých výrobců včetně speciálních formátů síťových toků.
21.	Řešení musí umožňovat automatické aktualizace	Ano splňuje. Nabízené řešení umožňuje nastavení stahování a automatické instalace aktualizací řešení, parserů, pravidel a dashboardů.
22.	Dashboard pro operátory v českém nebo anglickém jazyce.	Ano splňuje. Nabízené řešení nabízí webové grafické rozhraní v anglickém jazyce.
23.	Tvorba reportů ve formátech PDF, HTML a CSV, popř. dalších.	Ano splňuje. Nabízené řešení obsahuje stovky reportů, které lze jednoduše upravit nebo vytvořit nové. Řešení umožňuje vytvořené reporty exportovat v různých formátech, například PDF, HTML nebo CSV.
24.	Automatický backup proces tak, že každou půlnoc jsou automaticky zálohovány veškeré konfigurační soubory SIEM řešení, datové soubory SIEM řešení (log, events, flows, reporty, indexy).	Ano splňuje. Nabízené řešení podporuje nastavení automatických záloh, prováděných každý den ve stanovený čas, nejen konfigurace ale i auditních dat.
25.	Interní kontrola stavu zařízení (healthcheck) a upozornění uživatele v případě problému.	Ano splňuje. Nabízené řešení má vlastní robustní systém na logování vlastního stavu a upozorňuje uživatele na případné problémy a zobrazuje varování při nestandardním chování.
26.	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box).	Ano splňuje. Nabízené řešení obsahuje více než 400 korelačních pravidel, které implementují nejběžnější Use cases. Další korelační pravidla si lze volně stáhnout z IBM portálu případně zcela volně vytvářet vlastní pravidla.
27.	Možnost rozšíření výběrů o uživatelské položky z obsahu logů.	Ano splňuje. Nabízené řešení umožňuje definici

		vlastních položek, které budou vyčítány z obsahu logů a zobrazeny v souhrnu událostí, případně je možno dle těchto položek vyhledávat filtrovat a používat je v korelačních pravidlech.
28.	Možnost hromadného importu zdrojů logů.	Ano splňuje. Nabízené řešení poskytuje robustní a uživatelsky přívětivý systém přidávání nových zdrojů událostí, včetně možnosti hromadného přidání či importu zdrojů logů.
29.	Možnost nastavení více filtrů retenčních politik pro různé zdroje dat.	Ano splňuje. Nabízené řešení umožňuje nastavení retenční politiky s rozdílnými parametry pro rozdílné zdroje událostí. Na základě těchto pravidel lze definovat délku uložení logů z různých zdrojů událostí.
30.	Analýza dlouhodobých trendů událostí.	Ano splňuje. Řešení nabízí analýzu dlouhodobých trendů, kterou pomocí strojového učení a korelačních pravidel využívá k detekci neobvyklých událostí.
31.	Rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd.	Ano splňuje. Grafické prostředí nabízeného řešení umožňuje podrobnější analyzování zobrazených výsledků pomocí postupného „proklikávání" na jednotlivé detaily.
32.	Kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně.	Ano splňuje. Nabízené řešení podporuje tvorbu komplexních vyhledávacích dotazů s podmínkami, regulárními výrazy, fulltextovým vyhledáváním v indexovaných i neindexovaných datech a aritmetickými operacemi.
33.	Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy.	Ano splňuje. Nabízené řešení podporuje tvorbu komplexních vyhledávacích dotazů s podmínkami, regulárními výrazy, fulltextovým vyhledáváním v indexovaných i neindexovaných datech a aritmetickými operacemi. Případně vyhledávání pomocí Booleovy logiky.
34.	Požadujeme, aby pro vybrané položky z databáze SIEM, bylo možné pseudoanonymizovat či zamaskovat při zobrazení, pro potlačení zobrazení citlivých nebo osobních dat.	Ano splňuje. Nabízené řešení umožňuje zamaskovat konkrétní data pro určené uživatele či reporty na

		základě nastavených pravidel.
35.	Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí.	Ano splňuje. Nabízené řešení vytváří upozornění na bezpečnostní hrozby založené na korelačních pravidlech nad událostmi a síťovými toky. Alert je vytvořen i v případě detekování neobvyklého chování systémů na základě událostí nebo síťových toků. Alert může mít formu upozornění v uživatelské konzoli, emailu nebo napojení na software třetích stran.
36.	Systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives.	Ano splňuje. Nabízené řešení koreluje aktivitu ze síťových toků s událostmi ze sledovaných systémů a při vytvoření bezpečnostního incidentu obsahuje souhrn o incidentu seznam veškerých síťových toků a událostí souvisejících s incidentem.
37.	Alerting vycházející z detekovaných bezpečnostních hrozeb monitorovaných zařízení.	Ano splňuje. Nabízené řešení vytváří na základě nalezených bezpečnostních hrozeb incidenty tzv. „offense" Jako reakce na vytvoření offense může být definováno zaslání alertu.
38.	Řešení musí nabízet bezpečnostní informace jako je IP Reputation feed, botnety, zdroje malwaru apod., které jsou pravidelně online aktualizované výrobcem SIEM a jsou korelované v reálném čase se všemi událostmi.	Ano splňuje. Řešení nabízí napojení na reputační databázi výrobce, případně možnost jednoduše připojit další reputační databáze a feedy. Řešení automaticky koreluje informace z těchto databází a feedů s informacemi ze sledovaných systémů.
39.	Řešení musí umět aktivně skenovat zařízení v sítí na zranitelnosti. Minimálně pak musí nabízet tyto typy scanerů: discovery scan, patch scan, webový scan, databázový scan.	Ano splňuje. Nabízené řešení obsahuje integrovaný správce a skener zranitelností. Tento skener umožňuje aktivně skenovat zařízení v síti těmito typy skenů: discovery scan, patch scan, webový scan, databázový scan.
40.	Řešení musí zřetězit události do jednoho záznamu o incidentu, takže pokud korelační testy označí, že více činností souvisí s jedním útokem, vygeneruje řešení pouze jeden incident, aby nedošlo k přetížení bezpečnostního operačního týmu.	Ano splňuje. Nabízené řešení koreluje aktivitu ze síťových toků s událostmi ze sledovaných systémů. Řešení vytváří na základě nalezených bezpečnostních hrozeb incidenty tzv. „offense" Tyto offense obsahují souhrn o incidentu a seznam veškerých síťových toků a událostí souvisejících

		s incidentem. Tyto offense jsou sdružovány v případě rozsáhlejšího útoku a popisují tak kompletní postup útoku v rámci jedné offense.
41.	Behaviorální analýza síťového provozu včetně upozornění na anomálie a změny chování v síťové vrstvě.	Ano splňuje. Řešení nabízí analýzu dlouhodobých trendů, kterou pomocí strojového učení a korelačních pravidel využívá k detekci neobvyklých událostí, včetně upozornění na anomálie a změny chování v síťové vrstvě.
42.	Behaviorální analýza chování uživatelů včetně záznamu jejich chování v čase.	Ano splňuje. Nabízené řešení nabízí modul behaviorální analýzy chování uživatelů, která analyzuje chování uživatelů v čase a umožňuje odhalit odchylky v chování.
43.	Přístup k datům skrze otevřené REST API pro integraci s dalšími systémy.	Ano splňuje. Nabízené řešení poskytuje otevřené RestAPI rozhraní pro administraci systému SIEM a pro integraci se systémy třetích stran.
44.	Podpora vykonávání akcí v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript	Ano splňuje. Nabízené řešení umožňuje uživatelům nastavit spuštění konkrétní reakce v důsledku alertu, například: • vytvořit incident • spustit SNMP trap • odeslat email • odeslat zprávu Syslog • spustit vlastní skript
45.	Možnost rozšíření o schopnost pracovat s IP geolokacemi (botnet kanály atp.)	Ano splňuje. Nabízené řešení umožňuje napojení na geolokační služby a automatické zobrazování informací o geolokaci u IP adres.
46.	Generování alertů při výpadku logů z konkrétního zařízení.	Ano splňuje. Nabízené řešení poskytuje automatické upozornění v případě výpadků příchozích logů z konkrétních zařízení. Tyto upozornění zobrazuje řešení v sekci notifikací pro administrátora a zároveň umožňuje nastavení zasílání emailového upozornění.
47.	Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server)	Ano splňuje. Nabízené řešení automaticky identifikuje zdroje událostí a pokud rozpozná

		zdrojový systém automaticky zaregistruje nový zdroj událostí s přidělením příslušného parseru pro správnou normalizaci událostí. Taktéž jej zařadí do skupiny dle typu zdrojového zařízení.
48.	Monitorování historie útoků (typů událostí) na kritické komponenty a historie útoků jednotlivých uživatelů	Ano splňuje. Nabízené řešení poskytuje historické informace o již proběhlých incidentech v případě vytvořené nové incidentu pro stejné zdrojové zařízení nebo uživatele. V souhrnu incidentu je tak možné zobrazit i předchozí útoky.
49.	Korelace události DHCP, VPN a Active Directory a sledování průběhu uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele)	Ano splňuje. Nabízené řešení umožňuje korelaci informací o uživatelích z vícero zdrojů událostí a jejich slučování do jednoho incidentu v případě postupného postupu přes několik systémů.
50.	Rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy	Ano splňuje. Nabízené řešení umožňuje vytvářet reporty pomocí průvodce kde je možné vybraná data prezentovat formou přehledných grafů nebo tabulek. Dotazy pro reporty je možno tvořit pomocí filtrů v grafickém rozhraní a není třeba dotazy vytvářet pomocí SQL dotazů.
51.	Řešení musí podporovat nezměněnou funkcionalitu reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS	Ano splňuje. Nabízené řešení umožňuje vytvoření reportů pomocí skupin zdrojů událostí, kdy nezáleží na konkrétním typu nebo názvu zdroje událostí a report je tak zachován i při změně technologie nebo názvu zdroje událostí.
52.	Řešení musí být rozšiřitelné o podporu sběru a analýzy sledovaného síťového provozu až na aplikační vrstvu ISO/OSI modelu, pomocí rozšíření licence	Ano splňuje. Nabízené řešení umožňuje rozšíření o sondu pro sběr a analýzy sledovaného síťového provozu až na aplikační vrstvu ISO/OSI modelu.
53.	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.	Ano splňuje. Architektura nabízeného řešení umožňuje nasadit veškeré prvky v režimu vysoké dostupnosti, která zajišťuje automatické přepínání mezi jednotlivými prvky, pro zajištění kontinuálního sběru logů. Dodávané řešení je navrženo tak aby nedošlo k výpadku sběru nebo zpracování logů. Nasazení v režimu vysoké dostupnosti nevyžaduje

		komponenty/software třetích stran.
54.	Komponenty určené pro ukládání a korelaci, musejí být nasazeny v režimu HA. Další komponenty musí být možné připojit do režimu HA v jakékoliv fázi, bez nutnosti reinstalace celého řešení.	Ano splňuje. Architektura nabízeného řešení počítá s nasazením komponenty určené pro ukládání a korelaci v režimu HA. Další komponenty je možné připojit do režimu HA v jakékoliv fázi, bez nutnosti reinstalace celého řešení.
55.	Některá zařízení v síti často mění svou IP adresu. Nabízené řešení musí být schopno udržet databázi zařízení konzistentní i v těchto případech.	Ano splňuje. Nabízené řešení umožňuje sledování změn IP adres pro jednotlivé zařízení v síti a udržuje si aktuální informace o IP a MAC adresách.
56.	Nabízené řešení musí poskytovat webové uživatelské rozhraní pro správu, analýzy, reportovaní a podobně. Rozhraní nesmí obsahovat pluginy nebo být založeno na technologiích Java, Flash nebo na bázi tlustého klienta.	Ano splňuje. Nabízené řešení je řízeno z centrální konzole umožňující kompletní práci se systémem a jeho administraci. Grafické prostředí je přístupné pomocí nejrozšířenějších prohlížečů a využívá bezpečný HTTPS protokol. Pro práci s administrační konzolí není třeba instalace doplňků Java či Flash.
57.	Řešení musí být schopno agregovat záznamy o síťovém provozu z obou stran datového toku do jednoho záznamu popisujícího obousměrnou komunikaci.	Ano splňuje. Nabízené řešení umožňuje spojování (agregaci) záznamů o síťovém provozu z obou stran datového toku a poskytuje tak komplexní informaci o proběhlé komunikaci.
58.	Řešení musí uchovávat logy jak v normalizovaném formátu, tak i v „raw" formátu.	Ano splňuje. Nabízené řešení události ze zdrojových systémů ukládá jak v RAW formátu, tak i v normalizovaném formátu s možností definice uživatelských atributů. Tato data jsou ukládána v komprimovaném formátu pro úsporu diskové kapacity.
59.	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.	Ano splňuje. Nabízené řešení není licenčně omezeno počtem používaných korelačních pravidel. Ať se jedná o korelační pravidla podporovaná přímo výrobcem, či vlastní korelační pravidla.
60.	Řešení nebude licenčně omezeno počtem generovaných reportů.	Ano splňuje. Nabízené řešení není licenčně omezeno počtem používaných reportů. Ať se jedná o reporty podporované přímo výrobcem, či vlastní generované reporty.

61.	Řešení musí umět sledovat síťovou komunikaci v rámci virtualizovaného prostředí VMware ESX.	Ano splňuje. Nabízené řešení umožňuje sledovat síťovou komunikaci v rámci virtualizovaného prostředí VMware ESX.

POVINNÉ PARAMETRY funkce pro testování zranitelnosti

Dodavatel musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena

Parametr	Popis technických parametrů	Způsob splnění požadovaného parametru a pokud je požadován, i „Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru".
1.	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.	Ano splňuje. Nabízené řešení umožňuje konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů. Nabízené řešení umožňuje integraci se skenery třetích stran, jako jsou například: Nessus, Rapid 7, Nmap, nCircle.
2.	Řešení musí umět aktivně skenovat zařízení v síti na zranitelnosti. Minimálně pak musí nabízet tyto typy scanerů: discovery scan, patch scan, webový scan, databázový scan.	Ano splňuje. Nabízené řešení obsahuje integrovaný správce a skener zranitelností. Tento skener umožňuje aktivně skenovat zařízení v síti těmito typy skenů: discovery scan, patch scan, webový scan, databázový scan.
3.	Kontrola zranitelností musí reagovat na pravidly definované události a v případě naplnění podmínek (například nové neznámé zařízení) musí spustit automatizovaný scan zranitelností.	Ano splňuje. Nabízené řešení umožňuje nastavení automatizovaných skenování například nově rozpoznaných zařízení.
4.	Řešení musí prioritizovat výsledky scanu zranitelností na základě dostupných informací o síťové konfiguraci. Například zda konfigurace síťové infrastruktury umožňuje takovýto typ útoku.	Ano splňuje. Výsledky skenu zranitelností jsou v rámci nabízeného řešení seskupeny a prioritizovány na základě kritičnosti a aktuálním stavu síťové infrastruktury.
5.	Řešení musí umožňovat definici výjimek pro jednotlivé zranitelnosti dle různých kritérií tak, aby se nalezené zranitelnosti nepropagovaly v korelacích nebo v reportech.	Ano splňuje. Nabízené řešení umožňuje vytvoření výjimek pro jednotlivé zranitelnosti dle různých kritérií tak, aby se nalezené zranitelnosti nepropagovaly v korelacích nebo v reportech.
6.	Řešení musí být schopno na základě historického výsledku scanu a informacích o nových zranitelnostech identifikovat zařízení, který mohou být ohrožena.	Ano splňuje. Správa zranitelností nabízeného řešení umožňuje upozornit na zařízení, která mohou být ohrožena nově objevenými zranitelnostmi v rámci aktualizované databáze definic zranitelností.

7.	Řešení musí zajišťovat automatickou a pravidelnou aktualizaci databází zranitelností.	Ano splňuje. Databáze definic zranitelností je v rámci nabízeného řešení pravidelně aktualizována v rámci automatických aktualizací.

POVINNÉ PARAMETRY Ochrany databází

Dodavatel musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena

Parametr	Popis technických parametrů	Způsob splnění požadovaného parametru a pokud je požadován, i „Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru".
1.	Řešení podporuje monitoring veškerých session (vzdálená nebo lokální).	Ano splňuje. Nabízené řešení umožňuje monitorovat většinu komerčně používaných databází. Řešení umožňuje monitorovat vzdálená sezení i akce lokálně přihlášených uživatelů včetně těch privilegovaných.
2.	Podporované databáze: Oracle, Microsoft SQL Server, mySQL, IBM Informix, PostgreSQL.	Ano splňuje. Nabízené řešení podporuje monitoring databázových serverů s databázemi typu: Oracle, Microsoft SQL Server, mySQL, IBM Informix, PostgreSQL. Nabízené řešení umožňuje monitorovat většinu komerčně používaných databází.
3.	Podpora platforem: Windows, UNIX, Linux.	Ano splňuje. Nabízené řešení umožňuje monitorovat databázovou aktivitu využitím lokáních agentů na databázových serverech. Lokální agenti podporují instalaci na nejpoužívanější operační systémy. Agenti řešení podporují platformy Windows, UNIX, Linux
4.	Řešení identifikuje: časovou značku každé operace, celý příkaz operace, uživatelské jméno, odkazovaný objekt.	Ano splňuje. Nabízené řešení identifikuje množství detailů o každé operaci, například časovou značku, SQL příkaz, uživatelské jméno uživatele databáze a název objektu. Je možné zaznamenat i například uživatele OS, aplikaci, IP adresy zdroje i cíle, a mnoho dalšího.
5.	Řešení poskytuje nepřetržitý monitoring používání a toku dat.	Ano splňuje. Nabízené řešení umožňuje nejen sledovat aktivitu na konkrétních databázích a tabulkách, ve kterých jsou obsažena citlivá data, ale zároveň umožňuje nastavit sledování výsledků dotazů, ve

		kterých vyhledává například rodná čísla či jiné citlivé údaje. Na základě nalezených dat a bezpečnostních politik je možné nastavit příslušnou reakci systému jako je blokování či notifikace.
6.	Řešení musí podporovat monitoring šifrovaných spojení na Oracle a MSSQL.	Ano splňuje. Nabízené řešení umožňuje monitorovat i šifrovanou komunikaci s databázovými servery Qracle a Microsoft SQL.
7.	Řešení musí analyzovat data v reálném čase.	Ano splňuje. Nabízené řešení monitoruje databázovou aktivitu v reálném čase. V reálném čase taktéž řešení vyhodnocuje bezpečnostní politiky, které umožňují například zablokovat nebezpečnou aktivitu.
8.	Řešení umožňuje aktivní blokování dle: ip adresy zdroje a cíle, uživatelského jména, databáze, tabulky, sloupce nebo názvu souboru, typ database.	Ano splňuje. Nabízené řešení analyzuje veškeré dotazy směřující na databázové servery. Aktivita se porovnává s bezpečnostními politikami a pokud aktivita odpovídá podmínkám pro blokaci, je dotaz zablokován ještě před tím, než dorazí do databázového enginu a není tak proveden. Bezpečnostní politiky lze nastavit v nejmenším detailu a aktivní blokování lze nastavit například pomocí IP adresy, uživatelského jména, názvu databáze, tabulky, sloupce či typu databáze.
9.	Řešení musí korelovat události dle nastavených prahů.	Ano splňuje. Nabízené řešení umožňuje definovat manuálně, nebo samoučením prahy určitých hodnot a ty poté sledovat. V případě překročení prahové hodnoty je vytvořen alert a upozorněn administrátor řešení pomocí notifikace ve webovém rozhraní nebo pomocí emailové zprávy.
10.	Řešení se musí učit odhalovat anomálie, aby identifikovalo: neobvyklé nebo nové aktivity, neobvyklé nebo nové chyby, nové uživatele, nové typy objektů žádaných uživatelem, změnu chování v SQL struktuře, změnu chování v přístupovém čase.	Ano splňuje. Nabízené řešení umožňuje díky integrované analytické funkcionalitě a behaviorálnímu enginu sledovat změny dlouhodobě a odhalit tak i neobvyklé aktivity jako změnu chování v SQL struktuře, dříve neprováděné aktivity, chyby, uživatele a mnoho dalšího. Reakcí na tyto anomálie může být změna politiky či zaslání notifikace.

11.	Řešení musí umožňovat zasílat poplachy, událostí, které identifikuje, pomocí: emailu, syslog události (konfigurovatelné pro integraci se SIEM systémy), programovatelného API rozhraní.	Ano splňuje. Nabízené řešení umožňuje oznámení o identifikovaných událostech zasílat pomocí emailu přímo administrátorům, SYSLOG zprávou pro například SIEM systém, který může následně reagovat a omezit útočníka v celé organizaci. Řešení podporuje standard RestAPI a je možné na událost reagovat i API voláním.
12.	Řešení musí přístup ke kontrolovaným datům kontrolovat RBAC a to na dvou vrstvách: přístup k systémovým funkcionalitám, přístup k uloženým datům.	Ano splňuje. Nabízené řešení podporuje funkcionalitu nastavení bezpečnostních rolí. Na základě těchto rolí je poté řízen přístup uživatelů jak k jednotlivým funkcionalitám řešení, tak i přístup k auditním datům. Je tak možné plně oddělit přístup uživatelů k funkcím a datům na základě požadavků interních bezpečnostních norem. Možností je i integrace na LDAP s možností aktualizace rolí a bezpečnostního ověřování při přihlašování uživatelů řešení.
13.	Analýza SQL proudu by měla pokrývat příchozí a odchozí provoz a generované chyby.	Ano splňuje. Nabízené řešení sleduje veškerý provoz nad databázemi (příchozí i odchozí), tedy včetně sledování chyb.
14.	Řešení musí umět klasifikovat data pro identifikaci citlivých informací v databázích.	Ano splňuje. Nabízené řešení umožňuje detekovat a klasifikovat citlivá data v databázích. Cíle s citlivými daty lze přidat do skupin, na které lze vázat přísnější politiky pro ochranu či sledování. Pravidla pro klasifikaci jsou předdefinována, ale je velice jednoduché tyto pravidla upravit případně doplnit o vlastní. Samotné vyhledávání je možné naplánovat, a tak automatizovat proces vyhledávání citlivých údajů.
15.	Řešení musí podporovat sady pravidel pro požadavky PCI-DSS, SOX a GDPR.	Ano splňuje. Nabízené řešení je připraveno na mezinárodní normy a nařízení pomocí předpřipravených pravidel, politik a reportů pro GDPR, BASE II, HIPAA, PCI a SOX. Tyto pravidla, politiky a reporty lze volně upravovat, kopírovat či doplňovat o vlastní pravidla, politiky a reporty.
16.	Řešení musí umožňovat vytváření vlastních klasifikačních pravidel dle: regulárních	Ano splňuje. Nabízené řešení již obsahuje

	výrazů, porovnání se slovníkem, programovatelného API rozhraní.	předpřipravená pravidla pro klasifikaci citlivých dat. Navíc ale umožňuje tyto pravidla doplnit, upravit nebo vytvořit zcela nová. V rámci řešení lze vytvářet vlastní klasifikační pravidla pomocí regulárních výrazů, porovnání se slovníkem, programovatelného API rozhraní.
17.	Řešení musí umožňovat tvorbu reportů v tabulkové a grafické formě.	Ano splňuje. Nabízené řešení obsahuje desítky předdefinovaných reportů a dashboardů, ty je možné editovat a případně vytvářet i zcela vlastní. U interpretace dat si lze zvolit formu jak tabulkovou, tak i formu grafickou.
18.	Řešení musí umožňovat vytváření automatizovaných reportů dle naplánovaného rozsahu.	Ano splňuje. Nabízené řešení umožňuje naplánovat tvorbu pravidelných reportů, které se v naplánovaný čas sestaví z dostupných dat a je možné u nich nastavit i automatické zaslání upozornění uživateli o jejich dostupnosti nebo jej přímo zaslat pomocí emailu.
19.	Systém musí umožnit definovat postup vytváření a distribuce automatických výstrah a zpráv.	Ano splňuje. Nabízené řešení umožňuje definovat vlastní aletry a notifikace, které se budou zasílat uživatelům a administrátorům řešení, ale i třeba manažerům a dalším bezpečnostním řešením jako jsou systémy SIEM. Upozornění mohou být zasílána pomocí emailu, Syslogu, SMTP či API.
20.	Řešení musí archivovaná data ukládat v šifrované podobě.	Ano splňuje. Nabízené řešení umožňuje provádět automaticky i manuálně archivaci auditních dat na externí uložiště. Tato archivovaná data jsou při procesu archivace zašifrována a nelze je otevřít ani pozměnit. Archivovaná data zle obnovit zpět do prostředí řešení pro potřeby například historického vyšetřování.
21.	Řešení musí být schopno monitorovat konfigurační nastavení a identifikovat změny na: databázové úrovni (SQL, skripty), na úrovni operačního systému (skripty, proměnné prostředí, registry).	Ano splňuje. Nabízené řešení umožňuje monitorovat a identifikovat změny konfiguračního nastavení (SQL, skripty), na úrovni operačního systému (skripty, proměnné prostředí, registry).

22.	Je požadována licence pro pokrytí databáze aplikace NIS (Oracle cluster v režimu Active-Active)	Ano splňuje. Architektura nabízeného řešení licenčně i výkonově pokrývá použití pro ochranu databáze aplikace NIS (Oracle cluster v režimu Active-Active).

Obecné požadavky

- Veškeré dodávané HW a SW produkty byly získány legálně a umožňují využití těchto produktů Zadavatelem jako koncovým zákazníkem v souladu s distribučními a licenčními podmínkami výrobce zařízení,
- V případě dodání HW a SW produktů Zadavateli jako koncovému zákazníkovi nebude Zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje. Uvedené musí zahrnovat i nárok Zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání podpory výrobce,
- Musí být umožněn přímý přístup Zadavatele k dokumentaci výrobce HW/SW a znalostní bázi, kterou výrobce v rámci své podpory poskytuje,
- Zadavatel musí mít možnost eskalovat závady přímo k technické podpoře výrobce HW/SW včetně možnosti si sám a přímo otevřít požadavek na technickou podporu, provádět změny priority požadavků a případné eskalace pracovníky Zadavatele. A to po celou dobu požadované podpory.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží a licencí/subscripcí/operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh. Před převzetím zboží si Zadavatel vyhrazuje právo kontroly dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Zadavatel, bude se jednat o porušení podmínky originálního a nového zařízení.
- Dodavatel garantuje, že v případě dodání zboží Zadavateli jako koncovému zákazníkovi Dodavatelem bude poskytnuta k dodávanému zařízení záruka výrobce a produktová podpora v plném, výrobcem poskytovaném rozsahu.
- Servisní pracovníci Dodavatele musí disponovat technickou certifikací výrobce HW/SW na dodávané komponenty řešení, která je opravňuje k jejich instalaci a konfiguraci. Osvědčení o certifikaci nebo jiný odpovídající doklad výrobce dodávané technologie musí být předložen v českém, slovenském nebo anglickém jazyce – viz zadávací dokumentace bod 9.1.e).

Akceptační testy

Po nasazení a implementaci dodávaného řešení na všechna Zadavatelem specifikovaná zařízení a IS budou vyžadovány níže uvedené, dodavatelem provedené, akceptační testy:

- Testování sběru událostí ze všech monitorovaných zařízení, testování správné funkce korelačních pravidel, testování správného generování a obsahu alertů a reportů, testování oprávnění.
- Testování sběru událostí v případě výpadku jedné lokality.
- Detailní parsování logů zařízení a systémů uvedených v rámci zadávací dokumentace.
- Test příjmu alespoň 2 500 událostí za sekundu a 150 000 flows za minutu, v 10 minutovém intervalu s pomocí generátoru událostí a flows.
- Test příjmu alespoň 4 000 událostí za sekundu a 200 000 flows za minutu k ověření chování v situaci maximální zátěže, v 10 minutovém intervalu s pomocí generátoru událostí a flows. Systém musí události udržet v rámci vyrovnávací paměti.
- Vytvoření ukázkových reportů dokumentujících různé výstrahy jdoucí z podporovaných aplikací a reportů dopadů zjištěných zranitelností s ohledem na hodnoty rizik.
- Ukázka vytvoření vlastního dashboardu.
- Test příjmu výstrah na definovaný email.
- Test integrace na Helpdeskový systém zadavatele.

Příloha č. 2

Položkový rozpočet předmětu plnění

Položka č.	Plnění	Měrná jednotka (m.j.)	Jednotková cena v Kč bez DPH	Zadavatelem požadovaný / předpokládaný počet m.j.	Nabídková cena v Kč bez DPH za období 60 měsíců	DPH v %	DPH v Kč	Nabídková cena v Kč vč. DPH za období 60 měsíců
1	Dodávka technologie SIEM a její implementace včetně požadovaného školení obsluhy:							
	· HW část platformy SIEM	x	x	x	1 994 400,00 Kč	21,00%	418 824,00 Kč	2 413 224,00 Kč
	· Licence SIEM	x	x	x	4 496 800,00 Kč	21,00%	944 328,00 Kč	5 441 128,00 Kč
	· Licence modulu testování zranitelnost	x	x	x	419 020,00 Kč	21,00%	87 994,20 Kč	507 014,20 Kč
	· Licence modulu ochrany databázového prostředí	x	x	x	737 940,00 Kč	21,00%	154 967,40 Kč	892 907,40 Kč
	· Instalace, konfigurace a nastavení SIEM včetně školení obsluhy	x	x	x	900 000,00 Kč	21,00%	189 000,00 Kč	1 089 000,00 Kč
2	Služby podpory při zajištění organizačních bezpečnostních opatření dle Metodického pokynu MZČR	x	x	x	1 400 000,00 Kč	21,00%	294 000,00 Kč	1 694 000,00 Kč
3	Záruční technická podpora platformy SIEM v předpokládaném rozsahu prací 40 hodin za 1 měsíc po dobu 24 měsíců (dodavatel uvede roční sazbu, která bude zadavateli účtována)	rok	912 000,00 Kč	2	1 824 000,00 Kč	21,00%	383 040,00 Kč	2 207 040,00 Kč
4	Rozšířená podpora provozu platformy SIEM v předpokládaném rozsahu prací 20 hodin za 1 měsíc po dobu následujících 36 měsíců (dodavatel uvede roční sazbu, která bude zadavateli účtována)	rok	324 000,00 Kč	3	972 000,00 Kč	21,00%	204 120,00 Kč	1 176 120,00 Kč

5	Poskytování pravidelných služeb kontroly rizik a dodržování předpisů (včetně SŘBI) nad platformou SIEM v předpokládaném rozsahu 52 hodin za měsíc po dobu 5-ti let od implementace SIEM (dodavatel uvede i hodinovou sazbu, která bude zadavateli účtována)	člověkohodina	1 350,00 Kč	3120	4 212 000,00 Kč	21,00%	884 520,00 Kč	5 096 520,00 Kč
Celková nabídková cena za 60 měsíců v Kč bez DPH, tzn. celková nabídková cena za realizaci předmětu plnění veřejné zakázky					**16 956 160,00 Kč**	x	3 560 793,60 Kč	20 516 953,60 Kč

Příloha č. 3

Realizační tým Dodavatele

Označení role	Jméno a příjmení	Kontaktní údaje (telefon, e-mail)
Hlavní projektový manažer	[redacted]	
Specialista architekt řešení		
Vedoucí projektu – specialista SŘBI		
IT specialista na bezpečnostní technologie SIEM		
IT specialista na bezpečnostní technologie SIEM		
IT specialista na penetrační tetování a zranitelnosti		
IT specialista na zabezpečení databázových systémů		
IT specialista pro systémy LAN		
IT specialista pro serverovou infrastrukturu – hardware		