PŘÍLOHA Č. 3

SPECIFIKACE POSKYTOVANÝCH SLUŽEB

1. ZPŮSOB A ROZSAH POSKYTOVÁNÍ SLUŽEB ÚDRŽBY (MAINTENANCE) PODLE ČL. 2.1.1.1. SMLOUVY

1.1 Poskytování nových verzí SIEM a opravných patchů zahrnuje následující činnosti:

(i) poskytování aktualizací a nových verzí SIEM;

(ii) poskytování opravných patchů nutných pro bezchybný chod SIEM.

1.2 Objednatel má nárok na veškerá zlepšení a dodatky k SIEM (upgrade nebo update SIEM) vydané během účinnosti Smlouvy. Součástí poskytnutí těchto upgrade a update je též jejich testování a implementace u Objednatele a rozdílové školení v rozsahu školení dle čl. 1.3 přílohy č. 1 zadávací dokumentace, pokud bude potřeba s ohledem na rozsah upgrade či update.

1.3 Update se rozumí aktualizace SIEM formou opravných patchů, zohledňující většinou chyby nebo bezpečnostní mezery, které u předcházející verze nebyly známé včetně veškerých dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technická dokumentace zahrnující i případné bezpečnostní pokyny související s opravným balíčkem k SIEM).

1.4 Upgrade se rozumí vylepšení dosavadního SIEM na vyšší výkonnost a nové funkce včetně veškerých dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, instalačního manuálu a doporučení pro implementaci, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technická dokumentace zahrnující i případné bezpečnostní pokyny související s aktualizací komponent SIEM).

1.5 Součástí předmětu plnění dle čl. 2.1.1.1. Smlouvy není nárok na poskytování nových verzí SIEM vytvořených na základě individuální objednávky Objednatele, ani dokumentace k takto vytvořeným novým verzím SIEM.

1.6 Poskytovatel do 5 pracovních dnů ode dne vydání update či upgrade oznámí oprávněné osobě Objednatele podle čl. 12.1. Smlouvy uvolnění každého update i upgrade a důvod, proč k update či upgrade dochází.

1.7 Poskytovatel je povinen do 5 pracovních dnů ode dne vydání update či upgrade zajistit jejich neomezenou dostupnost tak, aby takový update a/nebo upgrade byl pro Objednatele kdykoliv přístupný.

1.8 O poskytnutí Služeb podle tohoto článku bude vždy vyhotoven písemný zápis, jehož součástí musí být i veškerá dokumentace podle výše uvedených ustanovení 1.1 až 1.6 této přílohy k update i upgrade.

1.9 Cena za poskytování Služeb dle tohoto článku 1. je v plném rozsahu zahrnuta v ceně za Služby dle čl. 4.1. Smlouvy.

2 ZPŮSOB A ROZSAH POSKYTOVÁNÍ SLUŽEB PODLE ČL. 2.1.1.2. A ČL.2.1.1.3.

SMLOUVY

2.1 Služba certifikovaného bezpečnostního konzultanta zahrnuje odbornou pomoc oprávněným osobám Objednatele v oblasti konzultací souvisejících s problematikou kybernetické ochrany, a to nejen v přímé souvislosti s řešením SIEM, ale i poradenství ve vztahu legislativním změnám, a to v rozsahu 16 člověkohodin měsíčně. Jednou člověkohodinou se rozumí práce vykonaná jedním pracovníkem Poskytovatele za dobu jedné (1) hodiny (dále jen „**člověkohodina**").

2.2 Legislativní úpravou se rozumí úprava stávající funkčnosti stávajícího SIEM, kterou je nutné provést, protože stávající funkcionalita by nutila Objednatele postupovat v rozporu s novou legislativní úpravou (např. zákona o kybernetické bezpečnosti). Legislativní úpravou v žádném případě není doplnění funkcionality (řešené oblasti), kterou stávající SIEM disponuje. Služba dle článku 2.1.1.2. Smlouvy zahrnuje např. i návrh dočasného fungování SIEM v případě, že nebude objektivně možné legislativní změnu zapracovat ke dni účinnosti legislativní změny

2.3 V případě, že Objednatel kontaktoval Poskytovatele za účelem bezpečnostní konzultace od certifikovaného bezpečnostního konzultanta, prostřednictvím HotLine, je Poskytovatel povinen řádně odeslat Objednateli odpověď nejpozději do 48 hodin po obdržení předmětného požadavku

2.4 Poskytování služeb monitoringu a dohledových služeb nad platformou SIEM, tj. zaručený provoz, v režimu 24/7/365, monitoringu nad dodaným HW/SW řešením, se rozumí dodávka takové služby, která splňuje následující kritéria:

(i) Dohled nad HW infrastrukturou SIEM je realizován nástrojem, s webovým rozhraním a s možností definice práv na úrovni rolí nebo jednotlivých řešitelů. Výchozí jazyk monitorovacího nástroje může být angličtina, s variantní podporou českého jazyka.

(ii) Komunikace mezi centrálním dohledovým serverem Poskytovatele a lokálními SIEM servery v prostředí Objednatele, i jednotlivými agenty, musí probíhat šifrovaně a využívá crypto knihovny. Přístup řešitelů musí být realizován přes zabezpečený protokol HTTPS. Nástroj musí umožňovat kontrolu výkonnosti a performance monitoring sledovaných technologií, dále kontrolu dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců, případně nových verzí opravující vážné bezpečnostní chyby podkladové vrstvy řešení SIEM.

(iii) Incidentní stavy jsou automaticky zakládány formou zápisu typu Incident v ticketovacím systému Helpdesk. Je možné nastavit vlastní eskalační postupy i v závislosti jednotlivých sledovaných prvků (např. ISP > core switch > ESXi > VM).

(iv) Monitoring sleduje fyzické i virtuální prvky SIEM, společně s funkcí autodiscovery zabezpečuje aktuální monitoring pro velikost a alokaci logických disků, CPU, SNMP discovery, windows services, možnost automatického sběru a vyhodnocení ODBC dotazů. Nástroj umožnuje tvorbu individuálních skriptů nebo exportu/importu XML souborů. Podporuje sledování pro technologie s protokolem SNMP v1 – v3 (SNMP traps, síťová zařízení)

(v) Reporting – nástroj umožnuje ad hoc nebo individuální grafické reporty z nasbíraných hodnot, zobrazené v prostředí řešitele. Výstupy z monitoringu dostupnosti SIEM infrastruktury budou součástí pravidelných měsíčních reportů vůči Objednateli. Historie dat: min. 90 dní zpět

2.5 Cena za poskytování Služeb dle tohoto článku 2 je v plném rozsahu zahrnuta v ceně za Služby dle čl. 4.1. Smlouvy.

3 ZPŮSOB PŘEDÁVÁNÍ DOKUMENTACÍ V SOUVISLOSTI S ČL. 2.1.1.1. A ČL. 2.1.1.2.

3.1 Poskytovatel je povinen poskytnout Objednateli dokumentaci, a to jejím vložením do Objednatelem určeného datového úložiště. Poskytovatel je povinen tuto dokumentaci v případě změny SIEM průběžně aktualizovat a po každé provedené aktualizaci ji poskytovat Objednateli vč. dokumentace provedených změn týmž způsobem. Poskytovatel je povinen předat Objednateli poslední verzi dokumentace ke dni ukončení Smlouvy nejpozději do tří (3) dnů ode dne ukončení této Smlouvy.

4 ZPŮSOB A ROZSAH POSKYTOVÁNÍ SLUŽEB PODLE ČL. 2.1.2.1 SMLOUVY

4.1 Služba Helpdesk a HotLine

Pro účely Smlouvy je pro vyžádání Služeb poskytovaných Poskytovatelem a podchycení komunikace oprávněných osob Poskytovatele a Objednatele zřízeno komunikační centrum Helpdesk a v jeho rámci komunikační centrum HotLine s garantovanou reakcí ze strany Poskytovatele. Služby Helpdesk a HotLine zahrnují zejména přijímání dotazů či požadavků ze strany Objednatele týkající se aplikační části SIEM a prostředí, ve kterém je provozován, jejich vyhodnocení a zajištění jejich vyřešení v souladu se Smlouvou.

Komunikační centrum Helpdesk a v jeho rámci komunikační centrum HotLine jsou realizována pomocí určené telefonní linky, e-mailové adresy a webového rozhraní systému Helpdesk poskytovatele. Technické vybavení a prostory komunikačního centra Helpdesk musí splňovat standartní bezpečnostní požadavky dle normy ISO 27001 a být řízeny dle obecně akceptovaného standartu (např. ITIL). Přístup k Helpdesk a k HotLine bude zřízen neprodleně po podpisu Smlouvy spolu s nadefinováním přístupových práv oprávněných osob uvedených v čl. 12.1. Smlouvy.

Webový Helpdesk nástroj pro zajištění a evidence všech požadavků (telefonních, emailových, i vygenerovaných monitoringem), musí mít nadřazený dispečink s pracovníky vykonávajícími dohled nad řešením otevřených požadavků, událostmi a logistikou pracovníků, včetně evidence servisních zásahů, obsahujících informaci o místě, čase a typu výkonu pracovníka Poskytovatele.

HelpDesk nástroj bude splňovat následující parametry:

a) HelpDeskový nástroj zabezpečený protokolem HTTPS

b) Zajišťuje automatické potvrzení o přijetí požadavku

c) Zajišťuje automatické zaslání zpětné vazby zadavateli po uzavření požadavku

d) Je nastaven pro příjem automatizovaných notifikací o incidentech z monitorovacího nástroje

e) Reporting – zajištění individuálních reportů z databáze požadavků a událostí

f) Přístup skrze mobilní aplikaci. Přístup do Helpdek nástroje musí být umožněn skrze klienta pro mobilní platformu (alespoň jednu) Android, IOS (Apple) či Windows Mobile. Mobilní aplikace musí být dostupná ke stažení zdarma skrze certifikované tržiště mobilních aplikací (Appstore, Google Play, atp.). Komunikace mezi Helpdesk nástrojem a aplikací musí probíhat po zabezpečeném protokolu.

Kontaktní údaje Helpdesk a HotLine

www stránky: [redacted]

E-mail pro automatizované zpracování požadavku: [redacted]

Tel: V případě potřeby telefonické komunikace se použijí telefonní čísla oprávněných osob Poskytovatele uvedená v čl. 12.1. Smlouvy.

Pozn. Objednatel výhledově počítá s vybudováním vlastního Helpdesku/Servicedesku. Po jeho vybudování bude zapotřebí zajistit integraci mezi Helpdesky objednatele a poskytovatele tak, aby požadavky zadávané v Helpdesku objednatele byly automaticky přeneseny do Helpdesku Poskytovatele.

4.2 Dostupnost služby Helpdesk a HotLine

(i) Poskytovatel je povinen reagovat na požadavky Objednatele pouze v pracovní dny v době od 8.00 do 18.00 hodin (dále jen „**Pracovní doba**"). Pracovním dnem se rozumí pondělí až pátek (dále jen „**Pracovní den**"), Pracovními dny nejsou soboty, neděle, státní svátky a ostatní svátky dle zákona č. 245/2000 Sb., o státních svátcích, o ostatních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších předpisů.

(ii) Komunikační centrum Helpdesk a HotLine je pro Objednatele telefonicky dostupná v Pracovní době, elektronicky lze předkládat požadavky 7 dní v týdnu, 24 hodin denně.

4.3 Reakce Poskytovatele

Poskytovatel je povinen potvrdit přijetí požadavku Objednatele ve lhůtě dle čl. 4.5.9 této Přílohy, v případě tímto článkem neupraveným, do 3 dnů. Je-li požadavek zapsán mimo Pracovní dobu, lhůta pro potvrzení začíná běžet okamžikem, kdy začne nejbližší Pracovní doba Poskytovatele po obdržení požadavku Objednatele.

4.4 Zásady komunikace na Helpdesk a HotLine

(i) Za Objednatele je oprávněna požadavek na poskytnutí Služby ohlásit oprávněná osoba dle čl. 12.1. Smlouvy:

- Zápisem na www stránky (webové rozhraní systému Helpdesk Poskytovatele) uvedené v čl. 4.1 této přílohy.
- Zápisem na email uvedeným v čl. 4.1 této přílohy, který je automaticky konvertován do nově založeného požadavku v nástroji Helpdesk.

V případě, že nejde použít výše uvedený způsob:

- Telefonicky na linku dle čl. 4.1 této přílohy

Jen ve výjimečných případech:

- osobním předáním požadavku oprávněné osobě Poskytovatele, při kterém oprávněná osoba Poskytovatele písemně potvrdí datum a čas předání.

V případě, že dojde k ohlášení požadavku jiným způsobem než s pomocí www stránek Helpdesk či emailu, je Objednatel, příp. po vzájemné dohodě Smluvních stran Poskytovatel, povinen učinit zápis na www stránky či emailem neprodleně, jakmile je to možné.

(ii) V případě, že Objednatel ohlásí požadavek mimo výše uvedená kontaktní místa služby HotLine, nebude na něj Poskytovatel brát zřetel.

4.4.3 Jestliže požadavek ohlásí jiná osoba, než je oprávněná osoba uvedená v čl. 12.1. Smlouvy, je Poskytovatel povinen neprodleně kontaktovat oprávněnou osobu s žádostí o potvrzení požadavku. Poskytovatel je povinen reagovat na všechny oprávněnou osobou Objednatele vznesené a potvrzené požadavky podle Smlouvy. Reakcí se rozumí potvrzení přijetí požadavku pomocí příslušných nástrojů systému Helpdesk, nebo v případě komunikace o požadavku mimo systém Helpdesk, písemně nebo e-mailem na adresu oprávněné osoby Objednatele uvedené v čl. 12.1. Smlouvy. Součástí přijetí požadavku ze strany Poskytovatele je předběžná klasifikace vady, resp. upozornění, že se o vadu dle Smlouvy nejedná, a stanovení požadavků na součinnost Objednatele.

4.5 Pohotovost a garance termínů řešení vad a požadavků

4.5.1 Poskytovatel je povinen po dobu platnosti Smlouvy (bez ohledu na trvání záruční doby) odstraňovat v termínech uvedených níže vady SIEM a řešit požadavky Objednatele.

4.5.2 Vadou se rozumí stav, kdy funkčnost SIEM není v souladu s podmínkami specifikovanými v dokumentaci k SIEM (detailní návrh řešení, akceptační protokol, apod.) nebo neodpovídá stavu při akceptaci SIEM, a to za podmínek, že IPM je využíván v souladu s příslušnými licenčními podmínkami, uživatelskou příručkou, a jinou dokumentací a je provozován na odborně provozované počítačové síti Objednatele. Nárok na odstranění vady v rámci ceny dle čl. 4.1. Smlouvy se nevztahuje zejména na případy, kdy vady SIEM byly způsobeny:

(i) chybami HW (mimo HW na kterém je SIEM provozován a byl součástí dodávky SIEM) tj. vadou počítače a síťových prostředků, např. výpadky sítě bez záložního zdroje, vady médií pro ukládání souvisejících dat, apod.;

(ii) nevhodným nebo neautorizovaným používáním SIEM v rozporu s příslušnými licenčními podmínkami, uživatelskou příručkou, a jinou dokumentací, která byla ze strany Poskytovatele předána Objednateli;

(i) neodborným zásahem Objednatele do instalace či nastavení parametrů SIEM vč. chybného konfigurování přístupových práv ze strany Objednatele;

(ii) chybným nakonfigurováním operačního systému či databáze či porušením jeho funkčnosti ze strany Objednatele;

(iii) naplněním databáze chybnými údaji, které odporují zabudovaným kontrolám v SIEM, ze strany Objednatele.

4.5.3 Kategorie vad:

Pro účely Smlouvy jsou vady kategorizovány takto:

Vady kategorie A: kritická vada, je Vada, která znemožňuje provádění stěžejních operací SIEM - jedná se o stav, kdy je ohrožena přímo funkce SIEM jako programu, je ohrožena bezpečnosti informačních systémů, nebo je nutné přikročit ke komplikovaným a nákladným řešením mimo SIEM.

Vady kategorie B: závažná vada, je Vada, která znemožňuje řádné fungování určité podstatné funkce SIEM u některého z informačního systému tak, že ohrožuje splnění závazků Objednatele, nebo SIEM vykazuje nepřiměřeně dlouhé odezvy, a tyto vadné funkce nelze nahradit jinou funkcionalitou či

náhradním postupem bez podstatně zvýšené pracnosti nebo nákladů Objednatele.

Vady kategorie C: středně závažná vada, která komplikuje nebo znemožňuje řádné fungování určité funkce SIEM, nebo SIEM nekomunikuje s některou částí informačního systému, avšak jeho činnost lze dle pokynů Poskytovatele nahradit jinou funkcionalitou, byť za cenu vyšší pracnosti na straně Objednatele.

Vady kategorie D: nezávažný nedostatek, kdy některá z funkcionalit SIEM není plně činná nebo ztěžuje užívání u některého uživatele, avšak tento stav nemá žádné, nebo jen zanedbatelné dopady na provoz u Objednatele.

4.5.4 Objednatel oznámí (ohlásí) vadu Poskytovateli prostřednictvím oprávněné osoby službou HelpDesk nebo HotLine s označením kategorie vady. Jestliže Objednatel neoznačí kategorii vady, má se za to, že se jedná o vadu kategorie C.

4.5.5 Poskytovatel reaguje na oznámení vady či požadavku pomocí příslušných nástrojů systému Helpdesk. V případě nedostupnosti systému Helpdesk, nebo v případě komunikace o požadavku mimo systém HelpDesk, písemně na Hotline nebo e-mailem na adresu oprávněné osoby Objednatele. Reakcí se v tomto případě rozumí potvrzení přijetí oznámení o vadě či požadavku včetně klasifikace vady a poskytnutí informace Objednateli, zda se jedná či nejedná o vadu či požadavek dle Smlouvy, jakým způsobem bude Poskytovatel vadu či požadavek řešit a předpokládanou dobou potřebnou na odstranění vady či vyřešení požadavku, případně požadavky na součinnost. Není-li Poskytovatel tyto informace schopen poskytnout, stanoví termín, kdy tyto informace Objednateli poskytne.

4.5.6 Postup při řešení vad či požadavků:

4.5.7 Poskytovatel zahájí v termínu uvedeném v čl. 4.5.9 této přílohy řešení vady či požadavku, v souladu s čl. 4.5.5 této přílohy vyhodnotí ohlášený požadavek a podle výsledku postupuje následovně:

(a) Objednatel požaduje odstranění vady a Poskytovatel vyhodnotil situaci tak, že se jedná o vadu:

- Poskytovatel pokračuje v řešení vady;
- Poskytovatel průběžně informuje Objednatele o tom, jakým způsobem vadu řeší, o předpokládané době potřebné na vyřešení vady, případně o požadavcích na součinnost Objednatele či třetích stran;
- vada bude odstraněna bez dalších nákladů pro Objednatele v rámci ceny dle čl. 4.1. Smlouvy;
- po vyřešení vady potvrdí Objednatel na Helpdesk nebo Hotline převzetí opravy vady a potvrdí protokol o zásahu vypracovaný poskytovatelem

4.5.8 Jestliže bude Poskytovatelem kdykoliv v průběhu řešení vady vyhodnoceno, že se nejedná o vadu dle Smlouvy nebo se jedná o vadu jiné kategorie, postupuje Poskytovatel dále dle následujícího článku (b).

(b) Objednatel požaduje odstranění vady a Poskytovatel vyhodnotil situaci tak, že se nejedná o vadu:

- Poskytovatel sdělí Objednateli, že situaci nepovažuje za vadu SIEM nebo považuje za vadu jiné kategorie a s odůvodněním zastaví práce na řešení požadavku;
- Objednatel na základě reakce Poskytovatele rozhodne, zda požadavek ukončí, nebo dá pokyn k pokračování řešení požadavku;
- Poskytovatel je oprávněn a současně povinen pokračovat v řešení požadavku jen pokud k tomu dostane od Objednatele pokyn;
- jestliže Objednatel dá Poskytovateli pokyn pokračovat v řešení požadavku, je Poskytovatel povinen tento požadavek vyřídit jako vadu dle tohoto článku 4 ve sjednaných termínech, a to v režimu dle klasifikace vady provedené Objednatelem. V takovém případě je Poskytovatel oprávněn postupovat dle čl. 13.4 Smlouvy.
- Po vyřešení požadavku Poskytovatelem potvrdí Objednatel na Helpdesk nebo Hotline převzetí opravy vady a potvrdí protokol o zásahu vypracovaný Poskytovatelem.

(c) Objednatel požaduje jiné Služby, než odstranění vady:

- Poskytovatel informuje Objednatele o přijetí požadavku a o tom, dle kterého ustanovení Smlouvy budou Služby řešeny;
- v případě, že Objednatel kontaktoval Poskytovatele za účelem konzultace prostřednictvím e-mailu, je Poskytovatel povinen řádně odeslat Objednateli svou odpověď nejpozději do dvou (2) Pracovních dnů po obdržení požadavku, není-li ve Smlouvě stanoveno jinak. Objednatel i Poskytovatel se musí shodnout na tom, o jaký problém se jedná (čeho se týká), jakož i na parametrech přijatelného řešení a jaké úsilí bude potřebné k jeho vyřešení;
- Poskytovatel průběžně informuje Objednatele o tom, jakým způsobem požadavek řeší, o předpokládané době potřebné na vyřešení požadavku, případně o požadavcích na součinnost Objednatele či třetích stran;
- Konzultační požadavek může ke svému konečnému zodpovězení vyžadovat i několik telefonických hovorů a/nebo průzkum ve znalostních databázích;
- po vyřešení požadavku potvrdí Objednatel (zprávou na HotLine) převzetí požadavku a potvrdí zápis o zásahu vypracovaný Poskytovatelem.

4.5.9 Lhůty na odstranění vad:

Poskytovatel se zavazuje poskytovat služby dle Smlouvy v následujících termínech:

Garance	**Vada kategorie A**	**Vada kategorie B**	**Vada kategorie C**	**Vada kategorie D**
Zahájení řešení vady a reakce vč. poskytnutí informace	Do 2 pracovních hodin od okamžiku	Do 4 pracovních hodin od okamžiku	Do 1 pracovního dne od okamžiku	Do 2 pracovních dnů od okamžiku

Objednateli, jakým způsobem bude Poskytovatel vadu řešit.	nahlášení vady.	nahlášení vady.	nahlášení vady.	nahlášení vady.
Zprovoznění SIEM alespoň náhradním způsobem pro zajištění jeho základních funkcí (tj. prozatímní, ne úplné odstranění vady).	Do 5 pracovních hodin od okamžiku nahlášení vady.	Do 8 pracovních hodin od okamžiku nahlášení vady.	Do 2 pracovních dnů od okamžiku nahlášení vady.	Do 5 pracovních dnů od okamžiku nahlášení vady.
Úplné odstranění vady (tj. dosažení stavu, který je popsán v dokumentaci k SIEM nebo odpovídá stavu při akceptaci SIEM).	Do 24 pracovních hodin od okamžiku nahlášení vady	Do 48 pracovních hodin od okamžiku nahlášení vady.	Do 5 pracovních dnů od okamžiku nahlášení vady	Do 20 pracovních dnů od okamžiku nahlášení vady

4.5.10 V případě neodstranění vady v termínu uvedeném v čl. 4.5.9 této přílohy je Poskytovatel povinen na odstranění vady nepřetržitě pracovat až do jejího úplného odstranění.

4.5.11 Způsob ukončení řešení vad či požadavků

Poskytovatel po vyřešení vady/ukončení řešení požadavku vystaví zápis o zásahu (dále jen „zápis o zásahu"), který musí obsahovat zejména:

(i) datum a čas hlášení a evidenční číslo vady či požadavku;

(ii) popis vady či požadavku;

(iii) čas počátku a ukončení řešení požadavku či vady;

(iv) popis příčiny vzniku vady (důvod zásahu);

(v) popis provedených prací a způsobu odstranění vady či vyřešení požadavku;

(vi) jméno pracovníka Poskytovatele provádějícího zásah.

Objednatel zkontroluje obsah zápisu o zásahu a v případě souhlasu s obsahem zápisu o zásahu tento zápis potvrdí. Pokud Objednatel jeho obsah neodsouhlasí, sdělí tuto skutečnost Poskytovateli nejpozději do pěti (5) Pracovních dnů od vyhotovení zápisu o zásahu. Tyto sporné Služby budou řešeny společným jednáním Objednatele a Poskytovatele, přičemž Poskytovatel je povinen připravit zápis z jednání, který zašle do tří (3) Pracovních dnů Objednateli. Pokud Objednatel do deseti (10) Pracovních dnů od vyhotovení zápisu o zásahu tento zápis o zásahu nepotvrdí ani k němu nesdělí žádné připomínky, považuje se takový zápis o zásahu za schválený.

Poskytovatel je povinen vést o řešení všech vad průkaznou systémovou evidenci a na požádání ji poskytnout Objednateli.

Primárním místem průběžné evidence servisních zásahů je systém Helpdesk Poskytovatele s přímým přístupem oprávněných osob ze strany Objednatele. Protokol o zásahu je primárně reprezentován záznamem o servisním zásahu (ticketem) v systému Helpdesk. V případě požadavku objednatele je Poskytovatel povinen záznamy ze systému HelpDesk převést do formy protokolu pro další komunikaci

4.6 Poskytování služeb Správa provozu služby SIEM

Bezpečnostní monitoring probíhá prostřednictvím vyhodnocovacího centra na straně Poskytovatele.

SLUŽBA

- Proaktivní dohled nad zabezpečením infrastruktury pomocí nástroje SIEM, který je ve vlastnictví Objednatele
- Provádění průběžného monitoringu
- Vyhledávání slabých míst
- Pravidelné návrhy na stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí

DOSTUPNOST

Bezpečnostní monitoring probíhá 24/7/365, řešení běžných bezpečnostních incidentů je řešeno prostřednictvím vyhodnocovacího centra denně v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.

ROZSAH SLUŽEB

Minimální rozsah služeb

specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný a požadovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

	Název role	Požadovaný rozsah alokace (z provozní doby 20 člověkodnů měsíčně)	
		Předpoklad Objednatele	Hodnoty garantované Poskytovatelem
role obsazované	Hlavní projektový manažer	1 MD	1 MD
	Specialista řízení IT služeb	1 MD	1 MD

	Specialista bezpečnosti	3 MD	3 MD
	IT specialista na bezpečnostní technologie - SIEM	10 MD	16 MD
	IT specialista na bezpečnostní technologie – penetrační testování a zranitelnosti	2 MD	2 MD
	IT specialista na bezpečnostní technologie – zabezpečení databázových systémů	2 MD	2 MD
	IT specialista LAN/SERVER	1 MD	4 MD

Požadované role obsazované Poskytovatelem

Objednatel uvedl v položce předpokládaný rozsah alokace pro danou roli očekávaný rozsah člověkodnů, které bude pro výkon dané činnosti Poskytovatel alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Poskytovatel doplní skutečné alokace, dle vlastních zkušeností a potřeb, avšak výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Poskytnutí služby bezpečnostního monitoringu

Poskytovatel zajistí **služby vyhodnocovacího centra bezpečnostního monitoringu**. Vyhodnocovacím centrem bezpečnostního monitoringu je myšlen bezpečnostní tým v kombinaci s nástrojem SIEM v majetku Objednatele, na provádění aktivního a proaktivního monitoringu, sběr, analýzu, korelace a kontroly auditních dat a informací shromažďovaných systémy Objednatele.

Účelem a cílem služeb Poskytovatele je **zajištění aktivního sledování, preventivního bezpečnostního dohledu a proaktivního monitoringu systémů Objednatele** to na základě zpracování a vyhodnocení auditních informací vytvářených systémem SIEM.

Provádění průběžného bezpečnostního monitoringu

Poskytovatel bude zajišťovat a provádět průběžný bezpečnostní monitoring systému Objednatele za účelem poskytnutí nepřetržitého dohledu nad stavem bezpečnosti systému, zajištění schopnosti proaktivní, včasné reakce na bezpečnostně relevantní události a shromažďování důkazů a podkladů pro řešení bezpečnostních incidentů.

Poskytovatel bude zajišťovat zejména následující činnosti:

- analytickou činnost nad bezpečnostními událostmi v systémech Objednatele, hledání a nalezení příčin událostí, anomálních chování, bezpečnostních hrozeb a podobně - v současnosti komplexně označováno jako Threat Management,
- sledování anomálií běžného provozu vybraných aplikací a jejich vyhodnocování,
- průběžná optimalizace parametrů chování sledovacích systémů (tresholdů),

označování false positive incidentů,
- kontrola vlastních bezpečnostních pravidel, systémů bezpečnostní infrastruktury,
- detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti,
- Průběžný bezpečnostní audit logů (korelace, agregace, vyhodnocování a uchovávání).

Prováděný bezpečnostní monitoring musí být schopen komplexním způsobem dokládat aktuální stav prostředí z hlediska bezpečnosti a v detailu umožňujícím provedení adekvátních reakcí.

Z hlediska zajištění této klíčové činnosti stanovuje Objednatel následující požadavky:

- vyhodnocovací centrum Poskytovatele bude provozováno nepřetržitě,
- Objednatel nepožaduje v rámci klíčové činnosti průběžného bezpečnostního monitoringu u vyhodnocovacího centra nepřetržitou obsluhu operátorem v režimu 24x7x365. Obsluha bude zajištěna pouze v pracovní dny v režimu 5x10 (08.00-18.00), mimo tuto dobu bude Poskytovatel zajišťovat pouze pohotovost tak, aby byl schopen zareagovat a aktivovat procesy podpory systému Objednatele v případě detekce bezpečnostně relevantních incidentů (např. kybernetický útok).

Vyhledávání slabých míst

Poskytovatel musí být schopen na základě prováděného průběžného bezpečnostního monitoringu identifikovat slabá místa v systému Objednatele a posoudit je z pohledu vhodnosti a dostatečnosti implementovaných bezpečnostních opatření.

Poskytovatel bude sledovat aktuální trendy v oblasti bezpečnosti (nové hrozby, reakce výrobců, způsoby jejich eliminace, atd.) a to v rozsahu technologií a služeb systému Objednatele. V souvislosti se získanými informacemi bude provádět proaktivní ověřování aktuálního stavu prostředí s cílem odhalit slabá a nezabezpečená místa minimálně v těchto oblastech:

- porovnávání aktuálního stavu hardware a software s přehledem známých zranitelností, týkajících se těchto systémů a jejich konkrétních verzí a patchů,
- kontrola provedených aktualizací firmware, operačních systémů, databázových a aplikačních platforem a antivirových řešení s důrazem na implementaci dostupných bezpečnostních update, patchů, hotfixů, servicepacků a virových databází
- kontrola provedených změn v konfiguracích systémů a jejich verifikace,
- doporučení k odstranění nepoužívaných nebo nadbytečných síťových služeb, služeb operačních systémů a aplikací za účelem snížení možných zranitelných míst, nadbytečné komunikace, otevřených portů a provedení hardeningu jednotlivých komponent systému.

V návaznosti na tyto skutečnosti bude vydávat doporučení provozovateli aplikace Objednatele s cílem zajistit instalaci, implementaci nebo rekonfiguraci určených prvků, komponent, konfiguračních položek, případně jiných oblastí.

Poskytovatel bude zajišťovat Služby v oblasti vyhledávání slabých míst **na denní bázi v pracovní dny**.

Stanovování, schvalování a kontrola provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí

Poskytovatel bude po celou dobu poskytování Služeb nedílnou součástí nastavených procesů řízení IT služeb, implementovaných v provozním prostředí Objednatele a zastřešených v rámci ServiceDesku Objednatele.

Jde zejména o procesy:

- Incident a Request Management.
- Change a Release Management.
- Problem Management.
- Configuration Management.
- Service Level Management.

V rámci uvedených procesů bude Poskytovatel zařazen do eskalačních procedur a bude se podílet na řešení jednotlivých požadavků a incidentů a stanovování, schvalování a kontrole provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí Objednatele.

Objednatel požaduje zajištění zejména následujících činností:

- zpracování stanovisek ke změnovým požadavkům z pohledu dopadů navrhovaných změn do bezpečnostních parametrů systému Objednatele,
- schvalování bezpečnostních pravidel, konfigurací bezpečnostních mechanismů a jejich změn u jednotlivých komponent systému Objednatele,
- koordinace činností, změny rozsahu funkcionality, návrh optimalizace a nápravných opatření u bezpečnostních prvků systému Objednatele (FW, IDS/IPS, atd.),
- řešení bezpečnostních incidentů v souladu s výše uvedeným
- verifikace provedení změn v systému Objednatele.

Poskytovatel bude v rámci této klíčové činnosti úzce spolupracovat se správci a administrátory Objednatele a třetích stran, které budou vlastními zásahy a změnami na komponentách systému Objednatele provádět. Poskytovatel je povinen v případě potřeby poskytnout nezbytnou součinnost a odbornou pomoc při koordinaci řešení s třetími stranami.

Omezení služby

Vyhodnocení bezpečnostních událostí převedení v bezpečnostní incidenty s relevantním hodnocením kritičnosti bude prováděno zaměstnanci poskytovatele s certifikovaným školením v oblasti znalosti SIEM systémů a škodlivých kódů. Služba bude omezena počtem max. 10 alertů za den.

Objednatelem požadované pravidelné činnosti – analytická činnost monitoringu SIEM

- Analýza bezpečnostních incidentů v systému SIEM
    - Posouzení incidentu z hlediska false-possitives bezpečnostních incidentů

- Vyhodnocení příčin vzniku bezpečnostních incidentů
- Vyhodnocení dopadu bezpečnostních incidentů (změny v systémech / infrastruktuře, uniklá data, atd.)
- Návrh a konzultace opatření
- Vzdálená kontrola bezpečnostních událostí – incidentů 5x8 (jejich investigace pro jejich klasifikaci)
- Eskalace a informování pověřených osob dle kompetenční a komunikační matice.
  - Eskalace významných událostí ze sítě MEPNET na bezpečnostní tým Objednatele
  - Výměna anonymních informací o aktuálních hrozbách s OTX komunitou (Open Threat Exchange)

- Konfigurace log zdrojů napojených na SIEM
  - Vytváření modulu pro neznámé zdroje v SIEM, aby bylo možné kategorizovat informace obsažené v logu.
  - Kontrola správné funkce infrastruktury a případná náprava nežádoucího stavu
  - Přidávání Log sources
- Vulnerability management
  - Aktivní kontrola zranitelnosti infrastruktury
  - Vyhodnocení bezpečnostního incidentu na základě známé zranitelnosti v infrastruktuře
  - Reporting zranitelností
- Ochrana databází
  - Aktivní kontrola zranitelnosti databází
  - Vyhodnocení bezpečnostního incidentu na základě známé zranitelnosti v infrastruktuře DB
  - Reporting zranitelností
- Správa incidentů – forenzní laboratoř
  - Aktivní kontrola zranitelnosti infrastruktury
  - penetrační testy
  - zátěžové testy
  - řešení bezpečnostních incidentů
  - Vyhodnocení bezpečnostního incidentu na základě známé zranitelnosti v infrastruktuře
  - Reporting zranitelností

- Strukturovaný reporting
    - Reporting zjištěných bezpečnostních incidentů
    - Reporting zjištěných zranitelností v infrastruktuře
    - Reporting anomálií v infrastruktuře
    - Reporting nekorektního chování infrastruktury nebo jejich částí
    - Konzultace nad reporty
- Dashboard
    - Přehled o aktuální bezpečnostní situaci v informačním systému
    - Přehled o správě detekovaných událostí a průběhu analytických činností
    - Přehled o kvalitě služeb bezpečnostní infrastruktury
    - Přehled o dostupnosti služeb a systémů
- Škálování konfigurace na specifické prostředí zákazníka
- Podpora služby v provozním režimu 5x8 s možností telefonní nebo e-mail komunikace přímo se Security Operátorem. V případě významných incidentů i specificky domluveným způsobem.

Součinnost v rámci procesů „Projektového řízení" souvisejících s návrhem změn v infrastruktuře.

- Správa a aktualizace provozní dokumentace v rozsahu:
- Správa a aktualizace technické dokumentace v rozsahu (konzole systému)

Údržba a rozvoj bezpečnostního monitoringu

- S ohledem na požadavek dlouhodobé udržitelnosti bezpečnostního monitoringu je nutné definovat proces zajišťující rozvoj bezpečnostního monitoringu včetně rozvoje technologie SIEM, který je důležitou součástí bezpečnostního monitoringu.
- Proces zajišťující rozvoj technologie SIEM musí zajistit následující činnosti:
- Způsob identifikace nových zdrojů logů a jejich začlení do bezpečnostního monitoringu.
- Návrh nových bezpečnostních use-case, které zajistí ochranu před nově identifikovanými hrozbami a nově vznikajícími hrozbami.
- Optimalizaci stávajících zdrojů logů, včetně hardening stávající infrastruktury.
- Návrh nových korelačních pravidel naplňujících identifikované use-case.
- Návrh nových korelačních pravidel, reagujících na nové hrozby a šetřené incidenty
- Aktualizaci stávajících korelačních pravidel.

- Aktualizaci systému bezpečnostního monitoringu na nové způsoby útoků.
- Aktualizaci a rozvoj reportů včetně druhů reportů.
- Procesy zajištění údržby a aktualizaci systému a všech komponent zajišťujících bezpečnostní monitoring.

4.7 Cena za poskytování služeb dle tohoto čl. 4 je v plném rozsahu zahrnuta v ceně dle čl. 4.1 Smlouvy.

5 ZPŮSOB POSKYTOVÁNÍ SLUŽEB ROZŠÍŘENÉ PODPORY SIEM PODLE ČL. 2.1.3. SMLOUVY

5.1 Služby dle čl. 2.1.3. Smlouvy zahrnují Služby, které souvisejí s programovým vybavením, zejména:

(i) školení uživatelů nad sjednaný rozsah;

(ii) konzultační podpora provozu programového vybavení;

(iii) součinnost při řešení systémových problémů a při implementaci programového vybavení třetích stran;

(iv) spolupráce při tvorbě koncepce a při koordinaci budování informačního systému Objednatele;

(v) úpravy a funkční doplnění programového vybavení.

5.2 Požadavky na poskytnutí Služeb souvisejících s provozem programového vybavení zadává Objednatel formou odeslání výzvy k poskytnutí Služeb Poskytovateli (dále jen „**Návrh výzvy**"). Návrh výzvy zašle Objednatel Poskytovateli elektronickou poštou. Návrh výzvy musí obsahovat zejména následující náležitosti:

(i) Cíl zadání: Stručná definice požadavku na Služby.
(ii) Popis zadání: Podrobná specifikace Služeb v dostatečné úrovni detailu umožňující zahájení prací ze strany Poskytovatele.
(iii) Časový harmonogram: Stanovení odhadu časového rozvrhu na poskytnutí Služeb.

5.3 Poskytovatel po obdržení Návrhu výzvy do jeho znění doplní zejména následující údaje:

(i) Předpoklad nároků na součinnost Objednatele: Odhad věcné a časové součinnosti, které bude Poskytovatel oprávněn požadovat od Objednatele v souvislosti s poskytováním požadovaných Služeb.
(ii) Specifikace postupu předávání Služeb: např. definice způsobu testování a předávání poskytnutých Služeb.
(iii) Prohlášení o záruce: Prohlášení o poskytnutí záruk Poskytovatele v délce nejméně 6 měsíců.
(iv) Detailní časový harmonogram: Uvedení závazných časových termínů pro poskytnutí Služeb, včetně předpokládaného rozsahu člověkohodin nutných pro poskytnutí požadovaných Služeb.
(v) Cena: Uvedení celkové ceny za poskytnutí Služeb vypočtené dle příslušné sazby dle **Přílohy č. 1** Smlouvy a zahrnující veškeré další náklady.
(vi) Autorská práva: Upozornění o vzniku Díla.

5.4 Pokud poskytnutím Služeb na základě Návrhu výzvy dojde nebo může dojít ke vzniku Díla dle obecně závazných právních předpisů, je Poskytovatel povinen v Návrhu výzvy na tuto skutečnost Objednatele upozornit.

5.5 Pokud by plnění Objednatelem stanovených Služeb v Návrhu výzvy vedlo k zhoršení výkonu programového vybavení či vzniku poruch a škod, je Poskytovatel povinen na tuto skutečnost Objednatele upozornit; neučiní-li tak, Poskytovatel odpovídá Objednateli za vzniklé škody v plném rozsahu a čas strávený nápravami těchto poruch a škod není Poskytovatel oprávněn zahrnout do Výkazu poskytnutých Služeb. Pokud Objednatel, i přes upozornění Poskytovatele provedeného dle tohoto článku, na v Návrhu výzvy stanoveném plnění trvá, Poskytovatel neodpovídá za škody vzniklé plněním Služeb dle Návrhu výzvy, ledaže překročil pokyny stanovené v tomto Návrhu výzvy.

5.6 Poskytovatel je povinen zaslat nebo předat vytištěný a podepsaný Návrh výzvy, doplněný o údaje dle článku 5.3 této přílohy zpět Objednateli do 5 pracovních dnů od obdržení Návrhu výzvy. Objednatel do 5 pracovních dnů po obdržení Poskytovatelem doplněného a podepsaného Návrhu výzvy buď (i) tento Návrh výzvy příjme, na důkaz čehož Návrh výzvy podepíše, anebo (ii) sdělí Poskytovateli své výhrady; v tomto případě se sdělení výhrad Objednatelem považuje za doručení nového Návrhu výzvy dle článku 5.2 této přílohy a Poskytovatel dále postupuje dle článku 5.3 této přílohy.

5.7 Jestliže do 30 dnů ode dne doručení prvního Návrhu výzvy Poskytovateli nedojde k podepsání Návrhu výzvy, týkajícího se stejných Služeb, oběma Smluvními stranami, je Objednatel oprávněn od Smlouvy odstoupit.

5.8 Podpisem Návrhu výzvy Poskytovatelem a Objednatelem je její znění pro Smluvní strany závazné, a nadále se označuje jako „**Výzva**“, přičemž platí, že Poskytovatel není oprávněn odepřít poskytování Služeb na základě Výzvy.

5.9 Poskytovatel provede realizaci Výzvy ve Výzvě stanovených termínech a za podmínek ve Výzvě stanovených.

5.10 Úpravy programového vybavení

5.10.1 Půjde-li o Služby spočívající v úpravách programového vybavení, bude pilotní provoz realizován nasazením příslušné úpravy na produkční prostředí za zvýšené podpory Poskytovatele. Pilotní provoz je stanoven v rozsahu jednoho (1) pracovního dne nebo dle dohody oprávněných osob.

5.10.2 Veškeré vady zjištěné v průběhu akceptačních testů a pilotního provozu systému je Objednatel povinen oznamovat Poskytovateli neprodleně v souladu s touto Smlouvou. Veškeré vady je Poskytovatel povinen odstranit ve lhůtách podle Smlouvy. Objednatel je na žádost Poskytovatele povinen písemně potvrdit datum odstranění každé vady zjištěné v průběhu akceptačních testů a pilotního provozu. V průběhu akceptačních testů a pilotního provozu strany průběžně projednávají způsoby řešení nahlášených vad.

5.10.3 V případě, že v průběhu akceptačních testů a/nebo pilotního provozu Objednatel zjistí vady kategorie A nebo dvě a více vad kategorie B, je oprávněn akceptační testy a/nebo pilotní provoz ukončit (tzv. neúspěšné ukončení akceptačních testů a/nebo pilotního provozu). Poskytovatel je povinen opravit zjištěné chyby a úpravu předat k opakovaným akceptačním testům a/nebo pilotnímu provozu.

5.10.4 V případě úspěšného provedení pilotního provozu a akceptačních testů bude předání úpravy provedeno podpisem předávacího protokolu oprávněnou osobou Objednatele.

5.10.5 V průběhu pilotního provozu je Poskytovatel povinen zajistit přítomnost servisního pracovníka přímo na operátorském pracovišti Objednatele na území Prahy.

5.11 Cena za poskytování Služeb dle tohoto čl. 5 bude stanovena ve Výzvě podle článku 5.3. odst. (v) této přílohy, přičemž tato cena je cenou konečnou a zahrnuje veškeré náklady na straně Poskytovatele související s poskytováním Služeb dle Výzvy. Objednatel není povinen hradit poskytnuté Služby nad rámec ceny vymezené ve Výzvě dle článku 5.3. odst. (v) této přílohy.

5.12 O Službách poskytnutých dle tohoto čl. 5 bude vyhotoven zápis, který potvrdí oprávněná osoba Objednatele dle čl. 12.1. Smlouvy. Objednatelem odsouhlasený zápis bude podkladem pro vystavení Výkazu poskytnutých Služeb. Zápis bude vyhotovován vždy až po dokončení všech Služeb, které jsou předmětem příslušné Výzvy.

5.13 Služby dle tohoto čl. 5 mohou být čerpány v maximálním rozsahu 100 člověkodní za celou dobu účinnosti Smlouvy. „Člověkodnem" se rozumí 8 hodin práce příslušného pracovníka u zadavatele včetně všech případných souvisejících nákladů na dopravu, stravování, ubytování apod. Poskytovatel není oprávněn poskytovat služby dle tohoto čl. 5 nad sjednaný rozsah, v případě porušení tohoto zákazu nebude mít nárok na jakékoli finanční plnění ze strany Objednatele, a to ani z titulu bezdůvodného obohacení.