**Příloha č. 1 Výzvy / Příloha č. 1 Smlouvy……**..

**čj.: 1/120/2439949-2019**

**Podrobná specifikace dodávky licencí a služeb**

**Rozvoj SIEM**

Obsah

[A. Zvýšení počtu zpracovávaných událostí za sekundu (EPS) 2](#_Toc25323594)

[1. Současný stav 2](#_Toc25323595)

[2. Požadovaný stav 2](#_Toc25323596)

[B. Technická a systémová podpora SIEM 2](#_Toc25323597)

[1. Správa zařízení SIEM (HW/SW) 2](#_Toc25323598)

[1.1. Provoz zařízení SIEM 2](#_Toc25323599)

[1.2. Správa zařízení SIEM 2](#_Toc25323600)

[2. Pravidelné činnosti - analytická činnost 3](#_Toc25323601)

[2.1. Služby 1. úroveň - Podpora, dohled a analýzy 3](#_Toc25323602)

[2.2. SIEM - Security Information & Event Management 3](#_Toc25323603)

[3. Reporting 3](#_Toc25323604)

[C. Cena 3](#_Toc25323605)

# Zvýšení počtu zpracovávaných událostí za sekundu (EPS)

## Současný stav

Je instalována verze v7.3.1 IBM QRADAR. VoZP má tyto licence včetně SW Subscription & Support do 31.1.2020:

:

* IBM QRadar Software Node Install
* IBM QRadar Software Install
* IBM QRadar Event Capacity 500 Events Per Second

## Požadovaný stav

Zadavatel požaduje rozšíření celkové kapacity EPS na nejméně 1 100, tedy rozšíření o nejméně 500 EPS.

Na nově dodané licence i licence již nainstalované požaduje zadavatel dodání SW Subscription & Support na 12 měsíců.

# Technická a systémová podpora SIEM

Zadavatel požaduje technickou a systémovou podporu v rozsahu **8 hodin měsíčně (2 hodiny týdně).** Tento objem hodin může zadavatel v rámci kvartálu libovolně přesouvat či kumulovat.

|  |
| --- |
| Zadavatel požaduje telefonickou a e-mailovou podporu 8x5 v českém jazyce, jednotné kontaktní místo pro hlášení problémů, incidentů a poruch. V případě významných incidentů i specificky domluveným způsobem.  Rozsah požadovaných činností: Správa zařízení SIEM (HW/SW)Provoz zařízení SIEM  * Profylaktické činnosti, kontrola služeb (na měsíční bázi), * Kontrola provozních logů zařízení (na měsíční bázi), * Návrh případných opatření s cílem předejít možným výpadkům a omezením poskytovaných služeb zařízením SIEM, * Odborná technická podpora a odstraňování závad v předmětné oblasti, * Správa licenčních pravidel.  Správa zařízení SIEM  * Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (na měsíční bázi), * Údržba a zajištění dostupnosti služby SIEM, * Analýza vhodnosti a potřebnosti implementace opravného balíku, * Návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli, * Implementace schválených požadavků na změnu konfigurace služby SIEM. |

## Pravidelné činnosti - analytická činnost

### Služby 1. úroveň - Podpora, dohled a analýzy

* + 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 nápravných a preventivních opatření

### SIEM - Security Information & Event Management

* Vzdálená kontrola bezpečnostních událostí - incidentů 8x5 (investigace pro jejich klasifikaci)
* Eskalace a informování pověřených osob.
* Eskalace významných událostí ze sítě na národním CERT® týmy a CSIRT týmy.
* Konfigurace log zdrojů napojených na SIEM
* Kontrola správné funkce infrastruktury a případná náprava nežádoucího stavu

## Reporting

Zadavatel požaduje vytváření kvartálního reportu o stavu událostí na síti zadavatele a o všech provedených konfiguračních změnách poskytovatelem. Součástí pravidelného reportingu bude:

* + Reporting zjištěných bezpečnostních incidentů a TOP 10 opakujících se hlášení bezpečnostního monitoringu
  + Reporting anomálií v infrastruktuře a nekorektního chování infrastruktury nebo jejich částí
  + Konzultace nad reporty, navrhovaná nápravná opatření
  + Informace o množství přidaných Logsources
  + Informace o zjištěných zranitelnostech a identifikovaných útocích na infrastrukturu
  + Informace o opatřeních, které by se měly provést
* Provoz manažerského rozhraní (Dashboard)
  + Přehled o aktuální bezpečnostní situaci v informačním systému
  + Přehled o správě detekovaných událostí a průběhu analytických činností
  + Přehled o kvalitě služeb bezpečnostní infrastruktury
* Škálování konfigurace na specifické prostředí zákazníka
* Správa a aktualizace provozní dokumentace v rozsahu:
* Postupy pro provoz a správu služby
* Postupy pro obnovu služby ze záloh jednotlivých systémů

# Cena

Nabídková cena bude tvořena z těchto složek:

1. Cena za A. Zvýšení počtu zpracovávaných událostí za sekundu (EPS)
2. Cena za B. Technická a systémová podpora SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| Popis | Cena za 1x Q | Počet | Kč bez DPH |
| A. Zvýšení počtu zpracovávaných událostí za sekundu (EPS) o 500 | ----- | 1 | 0,00 |
| B. Technická a systémová podpora SIEM | 0,00 | 8 | 0,00 |
| Celková nabídková cena (v Kč bez DPH) |  |  | 0,00 |