Příloha č. 1

# Specifikace služeb

## Předmět zakázky

Předmětem zakázky je **komplexní zajištění služeb bezpečnostního dohledu typu Security Operation Center nad prostředím a informačními systémy VOP CZ, s.p.** (dále jen „Služby SOC“) do vyčerpání hodnoty veřejné zakázky.

## Technické požadavky

### Služba proaktivního monitoring – SOC

1. Kybernetický monitoring v režimu 24x7 pro kritiké assety podniku (Active Directory, Informační systémy, zálohy, VPN, o365 cloud, servery, FortiGate Firewall, Honeypoty, perimetr IP adres)
2. Proaktivní vyhodnocování potencionálních incidentů na sítí
3. Včasnou detekci kybernetických incidentů
4. Honeypoty na sítí
5. Alerting do MS Teams, SMS a aplikace Signal
6. Napojení na MISP Feedy
7. Ochrana kybernetického perimetru
8. Uchování security logů po dobu 180 dnů
9. Dashboardy s vizualizací
10. IPSEC šifrovaný tunel pro přenos dat
11. Monitoring privilegovaných účtů

### SLA a reakční časy

Reakce dle klasifikace incidentu:

| Úroveň | Reakce do | Příklad |
|---|---|---|
| Kritická | 15 min | Ransomware, únik dat, kompromitace účtu |
| Vysoká | 1 hodina | Eskalace práv, útok z externí sítě |
| Střední | 4 hodiny | Podezřelé chování, anomálie |
| Nízká | 1 pracovní den | Falešné poplachy, auditní záznamy |

Dostupnost služby:

1. Monitoring (SOC): 24/7
2. Incident Response (reakční tým): 4 hod. × 5

3. SLA dostupnosti portálu/detekce: min. 99,9 % měsíčně
4. Povinnost hlášení při výpadku delším než 30 minut

Závazky poskytovatele

1. Incidenty budou uzavírány v předepsaných časech dle klasifikace
2. Pravidelně aktualizované tickety a stavy
3. Proaktivní návrhy na zlepšení bezpečnostní situace v měsíčních přehledech

**Analytik kybernetické bezpečnosti**

1. Pravidelné schůzky u zákazníka nebo online v minimální četnosti 1 x za dva týdny
2. Pravidelné činnosti a proaktivní bezpečnostní monitoring v režimu 5 x 8 hod. v čase 8:00 – 17:00, zbytek doby bude zajištěna formou pohotovosti.
3. Detekce podezření na kybernetický incident
    a) Identifikace a klasifikace kybernetických incidentů
    b) Navrhování nápravných opatření pro minimalizaci incidentů
    c) Vytváření repotů z incidentů
    d) Forenzní vyšetřování v oblasti SW, HW a sítě.
4. Spolupráce s interním teamem kybernetické bezpečnosti
5. Předávání KNOW-HOW interním zdrojům

**Reporting**

1. Report – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. Prezentace měsíčních reportů v rozsahu 2 hod.
2. Report bude obsahovat minimálně následující:
    a) Kompletní přehled událostí za dané období, agregovaný dle typu události a seřazený dle priorit a porovnání s předchozím obdobím.
    b) Detailní rozbor jednotlivých událostí za dané období dle jednotlivých typů událostí a porovnání s předchozím obdobím.
    c) Přehled nejčastějších zdrojů a cílů událostí za dané období (u událostí typu Upload a High Transfer také přehled podle množství přenesených dat jednotlivých zdrojů).
    d) Přehled pro 10 nejčastějších cílů (IP adres) za dané období.
    e) Přehled pro 10 nejčastějších zdrojů (IP adres) za dané období.
    f) Trendové přehledy a opakující se hrozby.
    g) Změny v detekčních pravidlech a konfiguraci systému.
    h) Doporučení na zlepšení bezpečnostního stavu.

**Online portál a dashboardy**

a) Živý přehled incidentů

b) Historie alertů, tiketů, zásahů