Testovací provoz služby SOC – specifikace

Předmětem objednávky je 4 měsíční zkušební připojení ke službě SOC365. V rámci služby je zajištěn monitoring prostředí, detekce kybernetických událostí, reakce na vyhodnocené události, reporting o bezpečnostní situaci a provozní kondici ICT služeb.

Požadovaná dostupnost operátorů SOC: 5x8

Požadované činnosti:

- Dostupný ServisDesk
- Průběžné sledování provozu
- Posouzení relevance a závažnosti nalezených anomálií
- Odborné posouzení bezpečnostní situace a provozního stavu (na denní bázi)
- Služby analytika (detekce, event & incident management, triage)
- Poskytování zpětné vazby na bezpečnostní otázky, které se přímo netýkají konkrétních událostí klienta, nicméně mohou přispět ke zlepšování služby a interních procesů
- Reporting

Rozsah připojených technologií: Flowmon sondy/kolektor, SIEM QRadar, Vulnerability scanner