Bitdefender - Bezpečnostní dohled

Bezpečnostní dohled antivirového programu je služba poskytovaná certifikovanými odborníky s detailní znalostí použitého systému. Zahrnuje pravidelný dohled, analýzu a vyhodnocování antivirových detekcí a incidentů. Tato služba umožňuje organizacím maximalizovat efektivitu použitého bezpečnostního řešení, identifikovat potenciální hrozby a přijmout preventivní opatření k ochraně svých systémů a dat.

Argumenty pro pořízení služby Bezpečnostního dohledu systému Bitdefender

1. **Maximalizace efektivity antivirového systému**: Odborný dohled umožňuje organizacím využívat svůj antivirový program v plném rozsahu a zabezpečit své systémy proti aktuálním kybernetickým hrozbám.
2. **Profesionální analýza a vyhodnocování**: Specializovaní experti provádějí důkladnou analýzu a vyhodnocování detekcí a incidentů, což umožňuje rychle identifikovat a reagovat na bezpečnostní rizika.
3. **Optimalizace bezpečnostního postupu**: Zpracování a interpretace dat z antivirových detekcí umožňuje organizacím vytvořit a optimalizovat bezpečnostní postupy a politiky.
4. **Uvolnění interních zdrojů**: Outsourcing dohledu antivirového systému umožňuje interním IT týmům soustředit se na další důležité úkoly a iniciativy bezpečnosti, zatímco externí specialisté se starají o monitorování a řízení antivirových systémů.
5. **Přístup k odborným znalostem a zkušenostem**: Spolupráce s externí bezpečnostní firmou umožňuje organizacím využívat odborné znalosti, zkušenosti a nejlepší postupy v oblasti kybernetické bezpečnosti.
6. **Zlepšení celkového bezpečnostního postavení**: Pravidelný dohled a aktualizace antivirových systémů pomáhají organizacím zvýšit jejich celkové bezpečnostní postavení a ochránit své systémy, data a uživatele před kybernetickými hrozbami.

Obvyklé (negarantované) reakční doby

Včasné varování (24h)
- Je-li uzpůsobeno nezákonným jednáním
- Nebo může-li mít dopad na dodavatelský řetězec

Upozornění na incident (72h)
- Aktualizace předchozích varování
- Prvotní posouzení vč. závažnosti a dopadu
- Indikátor kompromitovaného

Final report (1 měsíc)
- Popis incidentu
- Možná příčina
- Návrh zmírnění
- Dopad na dodavatelský řetězec

Průběžný report
- Je-li vyžádán