Zbývající přílohy smlouvy

Příloha č. 2 Smlouvy - SLA Logmanager

Název služby	**SLA LOGmanager**
Popis služby	Specializovaná správa, údržba a servisní podpora centrálního úložiště logů pro plně automatizovaný sběr provozních událostí z kritických provozních systémů LOGmanager. Oblasti: Help desk, změny konfigurací, servisních zásahy, konzultace k auditní a bezpečnostní problematice.
Vymezení služby	
Vstupní konfigurace	Ano
Systém	
Aktualizace software po uvedení od výrobce	Ano
Aktualizace parserů po uvedení od výrobce	Ano
Správa	
Správa systému LOGmanager	Ano
Konfigurace pohledů na logy z napojených systémů	Ano
Konfigurace přístupových práv uživatelů	Ano
Kontrola funkčnosti systému	Ano
Konfigurace Windows Beat Agenta (BEAT)	Ano
Doporučení AD Group Policy	Ano
Definice filtrů událostí	Ano
Automatické reporty	
Konfigurace a generování automatických reportů dle požadavků	Ano
Alerting	
Konfigurace alertů z napojených systémů dle požadavků	Ano
Proaktivní podpora na základě alertů	Ano
Analýza	
Analytické práce s daty, reporty a korelace	Ano
Předávání dat do nadřazených systémů	Ano
Doporučení na rekonfigurace systémů na základě analyzovaných logů	Ano
Podpora dodržování Zákona o kybernetické bezpečnosti	Ne
HW support	
Obnova systému po havárii (ticket u výrobce)	NBD po dodávce HW od výrobce
Dodávka náhradního HW	Ne
Profylaxe	4x za rok
Údržba seznamu napojených zařízení	Ano
Časový rozsah služby / SLA	
Rozsah služby	8x5
Automatické info emaily a alerty	24x7
Reakce na provozní incident	8 hod
Reakce na změnové požadavky	NBD
Zakládání tiketů u výrobce	Ano
Analýza incidentů	Ano
Omezení	Řeší pouze události evidované na LOGmangeru, neřeší hloubkovou analýzu příčiny událostí.
RAS max hod / měsíc za celé SLA dohromady	22
Hodiny se převádějí na další období (kalendářního roku) a je možné je využít i na konzultace nesouvisející s provozem systému centrálního úložiště.	

Prostředí	LOGmanager provádí sběr logů z aplikací a systémů pro potřeby auditu a bezpečnosti.
Dokumentace *4x za rok, při profylaxi*	Implementační dokumentace - dodá zákazník Údržba dokumentace Množina zařízení pro sběr - dodá zákazník Podmínky generující alerty. Je součástí vstupní konfigurace, viz.definice SIEM scénářů. Seznam cílů pro zasílání alertů, příp.proaktivních upozornění – dodá zákazník
Analytický report (píše analytik)	1x za 3 měsíce
Rozdělení minimálně na bezpečnostní (např. chybné přihlášení, podezřelé chování, útoky na IT infrastrukturu…) a provozní incidenty, a to podle uživatelů a četnosti, podle aktiv, podle organizačních jednotek; součástí reportu je doporučení pro další sledovaný následující měsíc ke snížení rizik, grafická část reportu, konfigurace reportů dle požadavků a generování reportů.	