T Business

Garantovaná úroveň poskytovaných služeb

Garantované SLA parametry dostupnosti Služby	Popis služby	Způsob měření
Funkčnost sběru logů (logy jsou dopravovány a sbírány z log kolektoru do SIEM (pokud funguje konektivita)	Provoz technických prostředků za účelem plnění funkce log managementu v režimu 24x7 (mimo předem hlášené odstávky)	Měří se downtime* prostřednictvím provozního monitoringu Služby.
Funkčnost ukládání logů na úložišti Poskytovatele	Provoz technických prostředků za účelem ukládání logů v režimu 24x7 (mimo předem hlášené odstávky)	Měří se downtime* prostřednictvím provozního monitoringu Služby.
Bezpečnostní monitoring SIEM (běží aplikace SIEM a generuje aletry dle korelačních pravidel	Provoz technických prostředků za účelem plnění funkce bezpečnostního monitoringu v režimu 24x7 (mimo předem hlášené odstávky)	Měří se downtime* prostřednictvím provozního monitoringu Služby.
Dostupnost Portálu	Provoz technických prostředků za účelem plnění funkce Portálu v režimu 24x7 (mimo předem hlášené odstávky)	Měří se downtime* prostřednictvím provozního monitoringu Služby.

** Za downtime považujeme časové období, po které určitá komponenta Služby není funkční.*

Garantované SLA parametry zpracování bezpečnostních událostí	Popis služby	Způsob měření
SLA 1 – Potvrzení o přijetí bezpečnostní události ze SIEMu	V případě vygenerování bezpečnostní události garantuje Poskytovatel její převzetí (zahájení zpracování ticketu bezpečnostním analytikem SOC) do 30 minut (dle zvolené varianty S/M/L). *Čas potvrzení přijetí je evidován v ticketovacím nástroji Poskytovatele.*	Měří se čas od okamžiku vytvoření ticketu až po potvrzení přijetí bezpečnostním analytikem SOC.
SLA 2 – Vysoká závažnost	V případě klasifikace bezpečnostní události jako vysoce závažné se Poskytovatel zavazuje do 60 minut (dle zvolené varianty S/M/L) reagovat na událost prostřednictvím Portálu.	Měří se čas od okamžiku potvrzení přijetí události (viz záznam v SLA1) až po první reakci SOCu.
SLA 2 – Střední závažnost	V případě klasifikace bezpečnostní události jako středně závažné se Poskytovatel zavazuje do 240 minut reagovat na událost prostřednictvím Portálu .	Měří se čas od okamžiku potvrzení přijetí události (viz záznam v SLA1) až po první reakci SOCu.
SLA 2 – Nízká závažnost	V případě klasifikace bezpečnostní události jako nízce závažné se Poskytovatel zavazuje do 1440 minut reagovat na událost prostřednictvím Portálu.	Měří se čas od okamžiku potvrzení přijetí události (viz záznam v SLA1) až po první reakci SOCu.

Pozn. SLA2 se nesjednává pro bezpečnostní události vyhodnocené jako NO IMPACT.

Garantované SLA parametry poskytování logů	Popis služby	Způsob měření
Poskytnutí logů přijatých kolektorem v původní nezměněné podobě v době jejich garantované retence na základě požadavku zadaného do Portálu	Provoz technických prostředků za účelem plnění funkce log managementu v režimu 24x7 (mimo předem hlášené odstávky)	Měří se downtime* prostřednictvím provozního monitoringu Služby.