Príloha č. 2 zmluve o poskytnutí služieb
OPIS PREDMETU ZÁKAZKY

1. Pilotná implementácia SOC as a Service

Predmetom realizácie zákazky je poskytnutie služieb v nasledovnom rozsahu:

- Implementácia SOC as a service na infraštruktúre zákazníka,
- Konfigurácia a ladenie systému,
- Pripojenie prostredia na zdroje logovacích dát, implementácia a verifikácia korektného parsovania, vytvorenie analytických prvkov monitorovania bezpečnosti (korelačných scenárov), vytvorenie dashboardov,
- Testovanie funkčnosti nasadenej služby.
- Poskytovanie služieb v zmysle popisu nižšie.

Opis úrovne služieb poskytovaných ako SOC as a Service:

*L1 – služby monitoringu 8x5**

Proces	Názov procesu	Činnosť	Popis
1. Denná prevádzka	**Základný monitoring**	**Kontrola stavu systému**	Kontrola funkčnosti zberu logov
			Kontrola systémových parametrov komponentov riešenia
			Kontrola funkčnosti generovania definovaných reportov
	Základná analýza	**Indikácia udalosti**	Detekcia podozrivých udalosti, vylúčenie False-positive
		Analýza reportovaných udalostí	Identifikácia podozrivých udalostí z generovaných reportov podľa dohody na základe požiadaviek zákazníka pre hlavné monitorované komponenty (napr. sieťové komponenty, servery, firewall , kritické systémy atď.)
		Klasifikácia udalosti	Zber a evidencia udalostí pre následnú analýzu
			Zaradenie udalostí do klasifikačných stupňov**
			Definovanie priorít podľa kategórie a klasifikačného stupňa**
	Oznamovanie	**Notifikácia**	Zasielanie upozornení: **Oznamovanie:** notifikácia zákazníka, resp. eskalácia na L2 v súlade s dohodnutými procesmi **Odozva:** Kritická udalosť - do 30 minút od zistenia Významná udalosť - do 1 h od zistenia Nekritická udalosť - neoznamuje sa

* Všetky časy sa rátajú v pracovnej dobe. Ak sa nedohodne inak, po skončení pracovnej doby sa všetky časy prerušia a pokračujú od začiatku nasledujúceho pracovného dňa.

** Klasifikačné stupne a jednotlivé kategórie (Kritická, Významná, Nekritická) musia byť definované vopred a jednoznačne

*L2 – Služby 8x5**

Proces	Názov procesu	Činnosť	Popis	Parameter
2. Reakcia	**Hĺbková analýza**	**Rozbor**	Rozbor incidentu, rozklad indikácie od abstraktného, všeobecného zistenia ku konkrétnemu popisu podstaty a podrobnosti incidentu	Kritická udalosť - začatie do 30 minút od notifikácie Významná udalosť - začatie do 24 h od notifikácie Nekritická udalosť - začatie do 48 h od zistenia, ak to charakter incidentu vyžaduje
		Identifikácia	Získať, zhromaždiť, uchovať, zabezpečiť a zdokumentovať dôkazy súvisiace s incidentom. Identifikovať zraniteľnosti ktoré boli zneužité.	

	Súčinnosť pri riešení incidentu	**Komunikácia**	Odovzdanie kľúčových informácií o incidente potrebných pre vykonanie následných krokov zákazníkovi.	Kritická udalosť - ASAP podľa výsledkov hĺbkovej analýzy Významná udalosť - ASAP podľa výsledkov analýzy Nekritická udalosť - podľa typu udalosti budú reportované, koordinácia iba v nevyhnutnom prípade
		Izolácia	Súčinnosť pri vymedzení, zastavení a izolácii incidentu dohodnutou formou.	Podľa dohody so zákazníkom
		Náprava	Súčinnosť pri náprave a vrátení napadnutých systémov do bežnej prevádzky dohodnutou formou.	
	Výstup	**Dokumentovanie**	Zdokumentovanie incidentu, identifikácia hlavných príčin a návrh opatrení za účelom eliminácie rizík opakovaného výskytu.	Podľa dohody so zákazníkom

L3 – na vyžiadanie / cena bude stanovená individuálne

3. Postincidentné aktivity		**Forenzná analýza incidentu**	Spracovanie analýzy (forenzná analýza) hlavných príčin s návrhom opatrení na zmiernenie dopadov. Príprava dôkazového materiálu a dokumentovanie incidentu a priebehu vyšetrovania. .	V závislosti od typu incidentu a jeho komplexnosti v zmysle požiadaviek zákazníka
		Návrh opatrení	Návrh krokov pre zmiernenie dopadov incidentu. Návrh nových use-case.	V závislosti od typu incidentu a jeho komplexnosti v zmysle požiadaviek zákazníka
		Realizácia opatrení	Návrh, architektúra a prípadná implementácia technických a organizačných preventívnych opatrení pre zníženie rizika výskytu podobného incidentu v budúcnosti.	V závislosti od typu incidentu a jeho komplexnosti v zmysle požiadaviek zákazníka
		Zvýšenie povedomia	Prediskutovanie a publikovanie poznatkov získaných z incidentu	Podľa požiadavky zákazníka, minimálne však od 7 dní od analýzy

Poskytovanie služby: 12 mesiacov od nasadenia

Príloha č. 2 zmluve o poskytnutí služieb
OPIS PREDMETU ZÁKAZKY

2. Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)

Dodávateľ zadefinuje scenáre rôznych udalostí, ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

- náhla nedostupnosť personálu
- náhla nepoužiteľnosť pracoviska/budovy
- nedostupnosť technologickej infraštruktúry
- náhla nedostupnosť médií
- živelná katastrofa

Dodávateľ stanoví požiadavky na zdroje (adekvátnych finančných, materiálno-technických a personálnych zdrojov), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti musí určiť čo má byť:

- hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch. Cieľom tohto plánu je udržať škodu spôsobenú rušivým incidentom na prijateľnej úrovni,
- strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalších strát a vplyv prostredia.

Dodávateľ vypracuje analýzu funkčných dopadov a kvalifikuje potencionálne dopady a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu je určenie:

- cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
- cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby. Jedná sa o identifikáciu tolerovanej doby pre obnovenie činnosti na prijateľnej úrovni a identifikáciu maximálne prijateľného množstva straty údajov merané v čase – cieľového bodu obnovenia.

Dodávateľ zavedie postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:

a) frekvenciu a rozsah jej dokumentovania a schvaľovania,
b) určenie osoby zodpovednej za zálohovanie,
c) časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,
d) požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,
e) požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
f) požiadavku navykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

Dodávateľ vypracuje plán pravidelného preverenia záloh, testovania obnovy záloh a precvičovania zavedených krízových plánov najmenej raz ročne.

Dodávateľ vypracuje alebo zabezpečí vypracovanie nim.:

- plán kontinuity na stanovenie požiadaviek a zdrojov,
- plán reakcie na incidenty,

- politiku a ciele kontinuity,
- analýzu funkčných dopadov,
- stratégiu riadenia kontinuity vrátane evakuačný postupov,
- plány havarijnej obnovy prevádzky,
- plán údržby a kontroly BCMS.

Objednávateľ požaduje oceniť vytvorenie BCM a zavedenie príslušných procesov:

- Analýzu riešenia
- Vytvorenie kontinuity činností, potrebnej dokumentácie
- Zavedenie procesov riadenia kontinuity