Popis služby Magenta EDR

1 Úvod

Společnost T-Mobile Czech Republic a.s. (dále jen „Poskytovatel“) poskytuje prostřednictvím služby **Magenta EDR** (dále jen „Služba“) řešení pro ochranu vybraných koncových zařízení IT systémů a analýzu bezpečnostních událostí identifikovaných v IT systémech Smluvního partnera, které sestává z bezpečnostní platformy provozované společností Crowdstrike (ta se skládá z cloudové části a softwaru instalovaného na chráněných zařízeních tzn. agent) (dále jen „Bezpečnostní platforma“) a souvisejících služeb.

Jelikož se kybernetickým útokům nedá nikdy zcela zabránit pouze preventivní ochranou IT systémů před jejich napadením, dostávají se do popředí zájmu systémy ochrany založené na detekci bezpečnostních incidentů, které jsou zároveň schopny na detekovaný bezpečnostní incident automaticky zareagovat a eliminovat či zmírnit důsledky incidentu.

Služba je založena na poskytování strojové automatické analýzy bezpečnostních událostí z bezpečnostních systémů a je určena především zákazníkům, kteří chtějí nahradit tradiční antivirové řešení.

Služba je technologicky poskytována z cloudu provozovaného na území EU. Lokálně generovaná data o provozu chráněného koncového zařízení (např. spouštěné procesy apod.) jsou shromažďována pomocí software instalovaného na chráněných zařízeních (dále jen „agent“) a následně předávána prostřednictvím šifrovaných spojení cloudové části Bezpečnostní platformy ke zpracování a uložení.

Serverové komponenty Bezpečnostní platformy Poskytovatele jsou sdílené pro více zákazníků. Data se ukládají pro každého zákazníka zvlášť. Všechny komponenty jsou provozovány v evropských datových centrech Poskytovatele nebo některého z jeho technologických partnerů, prošly povinným interním bezpečnostním auditem Poskytovatele a jsou chráněny přísnými bezpečnostními opatřeními.

Předpokladem pro optimální využití Služby je minimální počet 25 chráněných koncových zařízení (pracovní stanice nebo servery), která jsou aktivně chráněna a monitorována Službou.

2 Charakteristika Služby

2.1 Základní Služba

Základní Služba sestává z následujících funkčních částí:

2.1.1 Bezpečnostní platforma pro ochranu koncových zařízení Smluvního partnera (dále jen „Chráněná zařízení“), detekci hrozeb v koncových zařízeních a reakce na ně.

2.1.2 Implementace služby specialistou Poskytovatele dle specifických potřeb klienta a proškolení odborných pracovníků ve správě technologie. Samotné implementaci předchází vstupní workshop s oprávněnými zástupci Smluvního partnera. Po úvodním nastavení následují dvě kontrolní setkání, během nichž je vyhodnoceno fungování, optimalizováno původní nastavení a v případě potřeby přidány výjimky. Schůzky probíhají výhradně formou videokonference.

2.1.3 Technická podpora Poskytovatele je poskytována po celou dobu poskytování Služby. Smluvní partner má přímý emailový kontakt na tým Security Operation Centrum T Mobile, který mu poskytuje podporu v oblasti nastavení a funkčnosti Bezpečnostní platformy.

2.1.4 Smluvní partner může využít technickou podporu Poskytovatele zasláním dotazu emailovou na adresu [redacted] Přijetí požadavku je potvrzeno Poskytovatelem prostřednictvím emailu. Osoby oprávněné k čerpání technické podpory Poskytovatele budou určeny v rámci úvodního workshopu. Smluvní partner je oprávněn tuto osobu jednostranně změnit emailem na [redacted]

2.1.5 Reporting na pravidelné týdenní bázi formou emailu zahrnujícího přehled o Chráněných zařízení a zachycených detekcích. Smluvní partner je oprávněn deaktivovat reporting v konzoli Bezpečnostní platformy.

2.1.6 Služba konzultace analytika SOC Poskytovatele k Bezpečnostní platformě či zjištěné detekci na chráněném zařízení Smluvního partnera v rozsahu 1 konzultace za dobu trvání Služby sjednané ve Specifikaci služby (dále také jen „Konzultace“). Detaily ke způsobu využití a podmínek poskytování této služby jsou uvedeny v bodech 2.3.2 a 2.5.

2.2 Poskytování Služby

Jakmile je uzavřena Specifikace služby, uspořádá Poskytovatel se Smluvním partnerem úvodní workshop, který bude probíhat v češtině nebo v angličtině formou videokonference. Cílem workshopu je upřesnit detailní aspekty poskytování Služby. Dohodnuté výstupy workshopu budou zaznamenány formou zápisu.

Čas zahájení poskytování Služby je stanoven po dohodě se Smluvním partnerem a je uveden v zápisu z workshopu. Po zahájení poskytování služby je Smluvnímu partnerovi k dispozici Bezpečnostní platforma a Smluvní partner může začít instalovat agenty na vybraná koncová zařízení.

Služba je aktivována dnem sjednaným na úvodním workshopu. Smluvní partner má možnost v průběhu prvního měsíce užívání Služby u Poskytovatele vyžádat dvě konzultační schůzky (každá v maximální délce do 30 minut) prostřednictvím videokonference. Termín těchto konzultačních schůzek bude definován na úvodním workshopu. Předmětem konzultačních schůzek je revize nastavení bezpečnostní platformy a její případná optimalizace.

2.3 Funkční rozsah Základní služby

2.3.1 Pro účely ochrany koncových zařízení před napadením, detekce hrozeb v koncových zařízeních a reakce na ně, je v rámci Služby na příslušná koncová zařízení Smluvního partnera nainstalován agent, který kombinuje ochranu koncových zařízení („Endpoint Protection“, EPP) a detekci hrozeb v koncových zařízeních a reakce na ně („Endpoint Detection & Response“, EDR). To umožní aktivní detekci a prevenci hrozeb a útoků na daném koncovém zařízení. V případě, že Smluvní partner není vlastníkem koncových zařízeních určených k instalaci agenta, je povinen opatřit si od vlastníka zařízení souhlas k instalaci agenta užívaného v rámci Služby. Poskytovatel neodpovídá za jakoukoliv újmu vzniklou či související s instalací agenta na koncové zařízení v rámci Služby (zejména za ztrátu záruky či za interoperabilitu agenta s jiným software na Chráněném zařízení).

V rámci detekce hrozeb v Chráněných zařízeních a reakce na ně jsou shromažďovány a monitorovány aktivity spuštěných procesů na Chráněných zařízeních. Použitá technologie automatizuje shromažďování těchto informací a jejich korelaci a umožňuje tak detekci škodlivého nebo anomálního chování prostřednictvím následujících funkcí:

- Záznam chování procesů: pro každou detekci jsou zaznamenávány aktivity procesů v Chráněných zařízeních (aktivity souborového systému, síťové aktivity, změny v registrech nebo spouštění podprocesů). To umožňuje podrobnější analýzu potenciálních hrozeb.
- Centralizované uložení: shromážděné informace jsou předávány do Bezpečnostní platformy pro jejich správu. To znamená, že s nimi útočník v Chráněném zařízení již nemůže manipulovat a jsou okamžitě dostupné pro analýzu.

- Generování upozornění: jakmile je identifikována bezpečnostní událost, je vygenerováno upozornění, které se zobrazí v konzoli Bezpečnostní platformy.
- Základní modul EPP/EDR služby plně nahrazuje případné stávající antivirové řešení Smluvního partnera.

2.3.2 Služba Konzultace SOC Analytika – podstatou služby je poskytnutí konzultační činnosti Smluvnímu partnerovi ze strany Poskytovatele. Služba Konzultace SOC má následující parametry:

- Jedná se o službu na vyžádání realizovanou výhradně vzdáleným přístupem.
- Konzultační činností ze strany Poskytovatele se rozumí pomoc s porozuměním detekovaných bezpečnostních událostí či doporučení na protiopatření, která realizuje pouze Smluvní partner.
- Konzultační činnosti nezahrnují hloubkové vyšetřování incidentu mimo Bezpečnostní platformu užívanou v rámci Služby, proaktivní vyhledávání útočníka v IT prostředí Smluvního partnera či nápravu proběhlého incidentu.
- Jedna konzultace SOC analytika má časový rozsah maximálně jedné hodiny, tj 60 minut práce SOC analytika.
- Při překročení časového fondu 60 minut na 1 konzultaci, nebo maximálního počtu dostupných konzultací si Poskytovatel vyhrazuje právo konzultaci ukončit. Dodatečné konzultace SOC analytika lze sjednat jako Doplňkovou službu definovanou dle 2.4.7.
- Počátek čerpání konzultační činnosti nastává v momentě doručení notifikace Smluvnímu partnerovi o obdržení jeho požadavku na konzultaci SOC analytika Poskytovatele. Splnění 1 konzultace ze strany Poskytovatele nastane v momentě, kdy SOC analytik Poskytovatele doručí Smluvnímu partnerovi konkrétní reakci či odezvu na jeho žádost. Čas strávený řešením konzultace eviduje Poskytovatel na základě skutečně stráveného času.
- Splněním konzultace dříve, než během maximálního časového fondu 60ti minut nevzniká Smluvnímu partnerovi nárok na kompenzaci či dočerpání zbylého času z maximálního časového fondu jedné konzultace či jinou formu náhrady ze strany Poskytovatele.
- O čerpání může požádat pouze osoba oprávněná k čerpání konzultace. Tuto osobu příp. osoby definuje Smluvní partner během úvodního workshopu. V průběhu poskytování Služby může oprávněnou osobu pro konzultace změnit Administrátor systémových řešení Smluvního partnera emailem zaslaným na adresu [redacted]
- Za účelem poskytnutí služby Konzultace kontaktuje osoba oprávněná k čerpání konzultace Poskytovatele prostřednictvím emailu na [redacted]
- Komunikační platformu pro poskytnutí konzultace volí Poskytovatel v závislosti na předmětu konzultace (např. telefonicky, emailem, MS Teams).
- Přehled čerpání služby Konzultace není součástí Reportingu v rámci Bezpečnostní platformy.
- Celkový počet konzultací v rámci doplňkové služby Konzultace SOC analytika je sjednán ve Specifikaci služby Magenta EDR.

2.4 Doplňkové služby Magenta EDR

Službu lze volitelně doplnit o moduly, které rozšiřují funkční možnosti základní Služby. Předpokladem pro jejich využití je aktivní využívání základní Služby v rozsahu definovaném v sekci 2.1 tohoto Popisu služby.

2.4.1 **rozšiřující modul Falcon Insight** na rozdíl od základní služby definované v 2.3 zaznamenává telemetrická data nepřetržitě. Telemetrickými daty jsou v tomto případě myšleny zejména aktivity souborového systému, síťové aktivity, změny v registrech nebo spouštění podprocesů. Modul usnadňuje vyhodnocení zachycených detekcí, umožňuje provádět hloubkovou analýzu přímo Smluvním partnerem, lépe cílit přijímaná protiopatření a vykonávat forenzní analýzu. Tato varianta služby je současně nezbytná pro využití rozšiřujících modulů Discover (2.4.2) a Spotlight (2.4.3).

2.4.2 **rozšiřující modul Falcon Discover** pomáhá zajišťovat tzv. IT hygienu tím, že poskytuje ucelený pohled na Chráněná zařízení, uživatelské účty a aplikace používané na Chráněných zařízeních. S pomocí ARP Neighbor Discovery mechanismu detekuje koncová zařízení, na kterých není nebo nemůže být instalován agent. Modul pomáhá s identifikací nežádoucí či podezřelé aktivity a s uplatňováním některých vnitřních bezpečnostních pravidel Smluvního partnera prostřednictvím Bezpečnostní platformy či pravidelných reportů. Podmínkou pro využití modulu Falcon Discover je současná aktivace modulu Falcon Insight (2.4.1.)

2.4.3 **rozšiřující modul Falcon Spotlight** provádí detekci a správu softwarových zranitelností na Chráněných zařízeních bez nutnosti instalace dalšího agenta. Všechny nalezené zranitelnosti jsou evidovány v Bezpečnostní platformě a doplněny o širší kontext, který zahrnuje nejen závažnost, ale i popis, pravděpodobnost zneužití a návrhy na potlačení zranitelností. U Chráněných zařízení s operačním systémem MS Windows je možné sledovat nainstalované opravné balíčky operačního systému, sledovat stav implementovaných aktualizací a v případě potřeby vynutit jejich implementaci vzdáleně z cloudové konzole Bezpečnostní platformy. Podmínkou pro využití modulu Falcon Discover je současná aktivace modulu Falcon Insight (2.4.1.)

2.4.4 **rozšiřující modul Device Control** umožňuje získat kontrolu nad využíváním USB rozhraní Chráněného zařízení, a tím snížit rizika související s tímto vektorem útoku. V rámci detailního přehledu jsou k dispozici informace o všech pokusech o připojení zařízení skrze USB rozhraní na Chráněných zařízeních. Pro Chráněná zařízení může Smluvní partner definovat bezpečnostní politiku, která umožňuje povolit nebo zakázat přístup k USB rozhraní Chráněného zařízení. Device Control je podporován na Chráněných zařízeních s operačním systémem Windows a MacOS.

2.4.5 **rozšiřující modul Firewall Management** přináší možnost skupinově definovat, jaký síťový provoz je na Chráněných zařízeních povolen a jaký blokován. K dosažení tohoto cíle je využíváno nativního firewallu na Chráněném zařízení. Centrálně nastavená politika přepisuje nastavení firewallu na Chráněném zařízení. Firewall Management je dostupný pro operační systémy Windows a MacOS.

2.4.6 **rozšiřující modul Falcon Intelligence** obohacuje detekce o širší kontext s cílem poskytnou ucelenější pohled na zachycené aktivity pro rychlejší a informovanější rozhodnutí Smluvního partnera. Součástí modulu je možnost automatického či manuálního zaslání potenciálního malware do sandboxu k provedení hloubkové analýzy a poskytnutí souvisejících indikátorů (IoC feeds). Falcon Intelligence modul také zpřístupňuje databázi aktualizovaných profilů útočníků včetně jejich motivace, cílů a používaných technik.

2.4.7 **doplňková služba Konzultace SOC analytika** k Bezpečnostní platformě Poskytovatele a zjištěným detekcím na chráněném zařízení Smluvního partnera. Tato doplňková služba má identické parametry a pravidla jako Služba Konzultace, která je definována v bodě 2.3.2. Rozsah i ceny Doplňkové služby Konzultace SOC analytika k Bezpečnostní platformě Poskytovatele a zjištěným detekcím na chráněném zařízení Smluvního partnera jsou uvedené ve Specifikaci služby Magenta EDR. Pro optimální fungování doplňkové služby SOC Light doporučuje Poskytovatel i aktivní užívání doplňkového modulu Falcon Insight (2.4.1).

2.4.8 **doplňková služba SOC Light** spočívá v proaktivním dohledu SOC analytiků Poskytovatele v režimu 24x7 nad Chráněnými zařízeními Partnera a v poskytování reakcí i konzultací k bezpečnostním událostem na nich zjištěným Bezpečnostní platformou. Součástí doplňkové služby SOC Light je vždy i služba Konzultace SOC analytika, která definována v bodě 2.3.2. tohoto popisu Služby, a to v rozsahu sjednaném ve Specifikaci služby. Doplňková služba SOC Light nezahrnuje vyšetřování události mimo Bezpečnostní platformu užívanou v rámci Služby či nápravu proběhlé události mimo prostředí Bezpečnostní platformy. Pro optimální fungování doplňkové služby SOC Light doporučuje Poskytovatel i aktivní užívání doplňkového modulu Falcon Insight (2.4.1).

Bezpečnostní platforma automaticky klasifikuje zachycené bezpečnostní události do těchto typů: „informational, „low“, „medium“, „high“ a „critical“. Je na ně reagováno následujícím způsobem:

- Detekce typu „informational“, „low“ a „medium“: jsou automaticky zpracovány a zaznamenány spolu se souvisejícími logy přímo v Bezpečnostní platformě. Smluvní partner má k těmto zjištěním přístup přímo v konzoli Bezpečnostní platformy. O těchto bezpečnostních událostech není Smluvní partner proaktivně informován SOC Analytikem Poskytovatele, nicméně Smluvní partner má možnost si v případě zájmu vyžádat konzultaci SOC analytika Poskytovatele. Na tyto konzultace a poradenské činnosti je čerpán dostupný fond Konzultací SOC analytika sjednaný ve Specifikaci služby.
- Detekce typu „high“: jsou automaticky zpracovány a zaznamenány spolu se souvisejícími logy přímo v Bezpečnostní platformě. Smluvní partner má k těmto

zjištěním přístup přímo v konzoli Bezpečnostní platformy. U této kategorie detekcí je Smluvní partner o události proaktivně informován emailem. Pokud nelze aplikovat automatizovanou reakci, nebo je vyšší pravděpodobnost eskalace bezpečnostní události, je Chráněné zařízení Bezpečnostní platformou umístěno do karantény (síťová izolace Chráněného zařízení). Smluvní partner umístění Chráněného zařízení do karantény zruší buď svépomocí v konzoli Bezpečnostní platformy, nebo jej provede SOC analytik Poskytovatele s e-mailovým souhlasem kontaktní osoby Partnera (ADSR nebo osoba k tomuto úkonu určená Smluvním partnerem na úvodním workshopu). Pokud tyto detekce (či bezpečnostní události s nimi spojené) chce Smluvní partner konzultovat se SOC Analytikem Poskytovatele, je na ně čerpán dostupný fond Konzultací SOC analytika. Uvolnění Chráněného zařízení z karantény je výhradně v kompetenci Smluvního partnera, který za uvolnění Chráněného zařízení a jeho případné následky nese výlučnou právní odpovědnost.

- Detekce typu „critical“: jsou automaticky zpracovány a zaznamenány spolu se souvisejícími logy Bezpečnostní platformou. Smluvní partner má k těmto zjištěním přístup přímo v konzoli Bezpečnostní platformy. Nad rámec automatizované reakce Bezpečnostní platformy může SOC Analytik Poskytovatele dotčená Chráněná zařízení umístit do karantény, pokud hrozí laterální pohyb nebo eskalace bezpečnostní události. SOC Analytik Poskytovatele dále proaktivně informuje Smluvního partnera, poskytuje mu součinnost a konzultační činnost během řešení události. Pokud tyto detekce (či bezpečnostní události s nimi spojené) chce Smluvní partner konzultovat se SOC Analytikem Poskytovatele, není na ně čerpán dostupný fond Konzultací SOC analytika Poskytovatele (čerpání konzultací Partnerem je neomezené). Zrušení z karantény pro Chráněné zařízení provede SOC analytik Poskytovatele se souhlasem oprávněné osoby Smluvní partnera (zaslaným emailem).

2.5 SLA a odpovědnost

2.5.1 Poskytovatel garantuje dostupnost Služby v parametrech uvedených ve Specifikaci služby Magenta EDR.

2.5.2 Nesplnění výše uvedené garantované úrovně Služby se považuje za poruchu Služby. Služba není poskytována s proaktivním dohledem Poskytovatele. Smluvní partner je povinen nahlašovat všechny vady a poruchy Služby prostřednictvím emailu r[redacted]

2.5.3 Poskytovatel uhradí Smluvnímu partnerovi smluvní pokutu ve výši 5% z měsíční ceny Služby za každé nedodržení výše uvedených garantovaných parametrů Služby. Maximální výše smluvní pokuty v jednom měsíci je 50% měsíční ceny Služby. Uhrazení smluvní pokuty je realizováno formou slevy z měsíční ceny za Služby v dotčeném měsíci (dále jen „Sleva“).

2.5.4 Smluvní strany se dále dohodly, že smluvní pokuta za překročení sjednané SLA je zahrnuta ve Slevě (výpočtu Slevy) a Smluvnímu partnerovi tak nenáleží za nedodržení SLA žádná další smluvní sankce, sleva ani náhrada újmy.

2.5.5 Poskytovatel není odpovědný za neposkytnutí nebo vadné poskytnutí Služby, resp. za újmu, vzniklou v důsledku následujících skutečností:

- v případech, kdy za poruchu Služby neodpovídá Poskytovatel v souladu s příslušnými právními předpisy
- poruchy Služby vzniklé vnitřní chybou operačního systému a dalšího programového vybavení Smluvního partnera a jím využívaných dodávek třetích stran (dále jen „třetí strana“). Případnou odpovědnost nese Smluvní partner a/nebo tato třetí strana dle jejich licenčních ujednání.
- poruchy Služby vzniklé v důsledku nefunkčnosti hardware či software Smluvního partnera či třetích stran. Případnou odpovědnost nese Smluvní partner či tato třetí strana.
- nesprávné a nepovolené užívání Služby nebo disponování se software užívaným v rámci Služby ze strany Smluvního partnera
- poruchy Služby zapříčiněné počítačovými viry, červy, spamy apod., pokud není způsobeno zanedbáním povinností Poskytovatele zajištěných v rámci Služby,
- reset, restart či vypnutí Chráněného zařízení,
- doba, po kterou je Smluvní partner v prodlení s poskytnutím součinnosti,
- doba poruchy Služby z příčiny na straně instalovaného software na serveru (zamrznutí, reset apod.)
- nesprávné užití Služby či některé komponenty Služby za strany Smluvního partnera – např. nevhodné nastavení parametrů na Chráněném zařízení apod.,
- plánovaná údržba a Servisní odstávka Služby ze strany Poskytovatele.

2.5.6 Poskytovatel nenese odpovědnost za případnou újmu, kterou Smluvní partner utrpí v důsledku jakéhokoli kybernetického útoku směřovaného na Chráněná zařízení či vedeného prostřednictvím Chráněných zařízení nebo v souvislosti s jakýmkoliv opatřením Poskytovatele učiněným v souvislosti s plněním této Služby. Při poskytování konzultací Poskytovatel postupuje v souladu s doporučeními výrobce Bezpečností platformy, aktuálními standardy na trhu (zejména doporučeními výrobců operačních systémů) a principy Best practice (Nejlepší praxe).

2.5.7 Poskytovatel a jeho subdodavatelé obvykle provádějí údržbové činnosti dvakrát měsíčně. Pokud tyto údržbové činnosti povedou k nedostupnosti Služby, Poskytovatel o tom bude Smluvního partnera předem informovat. Oznámení se zasílá e-mailem na kontaktní adresu ADSR nebo jako zpráva v Portálu. Poskytovatel se zavazuje omezit přerušení provozu Služby způsobená údržbou na nezbytné minimum. Nedostupnost z důvodu provádění údržbových činností se nepovažuje za poruchu Služby a do dobu údržby nelze uplatnit plnění sjednaných SLA.

2.5.8 V rámci Služby garantuje Poskytovatel Smluvnímu partnerovi včasnou implementaci standardních ochranných postupů pro agenty a Bezpečnostní platformu a zajišťuje v rozsahu stanoveném v tomto Popisu služby přístup ke znalostem a dovednostem SOC týmu Poskytovatele a nejnovějším poznatkům inženýrského týmu CROWDSTRIKE. Poskytovatel se zavazuje poskytovat Službu na základě principů Best practice (Nejlepší praxe) s využitím aktuálně dostupné sady funkcí Bezpečnostní platformy. Přestože se Poskytovatel zavazuje vynaložit přiměřené úsilí k identifikaci a omezení dopadu kybernetických útoků, vzhledem k neustálému vývoji nových typů útoků, jejich kombinací a modifikací a rozsahu, nemůže Poskytovatel zaručit, že ochrana bude vždy a bezpodmínečně plně účinná. Poskytovatel nenese odpovědnost za případné škody, které Smluvní partner utrpí v důsledku jakéhokoli kybernetického útoku směřovaného na Chráněná zařízení či vedeného prostřednictvím Chráněných zařízení nebo v souvislosti s jakýmkoliv opatřením Poskytovatele učiněným v souvislosti s plněním této Služby.

2.5.9 Pro vyloučení pochybností se stanoví, že sjednání ani plnění Služby nezakládá závazek Poskytovatele plnit povinnosti Smluvního partnera plynoucí ze zák. č. 181/2014 S., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), popř. nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti pro finanční sektor a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, popř. dalších právních předpisů ukládajících Smluvnímu partnerovi povinnosti související s bezpečnostními incidenty v jeho IT prostředí.

3 Povinnost součinnosti ze strany Smluvního partnera

Smluvní partner je povinen poskytovat součinnost bezplatně, včas a v rozsahu nezbytném pro řádný provoz Služby. Jedná se zejména o povinnosti uvedené níže.

Smluvní partner za účelem implementace Služby jmenuje kvalifikovanou kontaktní osobu oprávněnou činit rozhodnutí a také zástupce, který bude odpovědný za bezproblémovou integraci Služby a její bezproblémový provoz v prostředí Smluvního partnera (Smluvní partner poskytne telefonní číslo a e-mailovou adresu). Kontaktní osoba Smluvního partnera se účastní naplánovaných schůzek a koordinace fází zavádění a hraje aktivní roli v procesech zavádění Služby.

Kontaktní osoby určené Smluvním partnerem musí při kontaktu Poskytovatelem prokázat svoji identitu. Pro řízení incidentů a změn jmenuje Smluvní partner kontaktní osobu s odpovídajícími odbornými znalostmi a rozhodovacími pravomocemi.

Smluvní partner poskytne Poskytovateli všechny potřebné informace a zajistí, aby jeho údaje byly vždy obsahově správné a aktuální.

Smluvní partner zajistí poskytnutí nezbytné součinnosti ze strany svých smluvních partnerů nebo jiných třetích stran, které přináleží ke Smluvnímu partnerovi.

Za účelem využívání Služby Smluvní partner mimo jiné zajistí splnění níže uvedených technických požadavků:

- Přístup k internetu
- Aktualizovaný podporovaný internetový prohlížeč (pro osoby přistupující do administrátorského rozhraní Bezpečnostní platformy.)
- Aktualizované podporované operační systémy na Chráněných zařízeních

Připojení potřebná pro přístup k Bezpečnostní platformě ani potřebné komunikační vybavení nejsou poskytovány v rámci Služby.

Smluvní partner zajistí, aby konfigurace brány firewall a nastavení jeho síťové infrastruktury umožňovaly požadované typy přenosu dat.

Smluvní partner provede samostatně a na vlastní odpovědnost nasazení a instalaci požadovaných agentů na Chráněná zařízení v příslušných systémech.

Aktualizace software agentů jsou k dispozici v různých intervalech. Instalaci lze často provádět též automaticky. Stažení a instalace aktualizací agentů na Chráněných zařízeních je nezbytnou podmínkou pro to, aby Smluvní partner mohl používat aktuální verzi Služby a využívat jejich nejnovější funkce. Poskytovatel upozorňuje, že v případě neprovedení instalace aktualizací nelze funkce používat nebo je lze používat pouze v omezeném rozsahu.

Smluvní partner souhlasí s vytvořením a používáním pro něj určeného prostředí na cloudové Bezpečnostní platformě a se šifrovaným přenosem svých metadat.

Kontaktní osoba Smluvního partnera je povinna bezodkladně informovat Poskytovatele o veškerých změnách v prostředí Smluvního partnera, které mohou mít vliv na fungování Služby.

Po ukončení poskytování Služby musí Smluvní partner do dvou (2) týdnů kompletně odinstalovat podpůrný software (agenty na Chráněných zařízeních) ze systémů v rámci své síťové infrastruktury.

Služba je určena výhradně pro potřeby Smluvního partnera. Smluvní partner není oprávněn postoupit část nebo celou Službu k užívání třetím stranám.

Smluvní partner je povinen spolupracovat při nápravě incidentů. Smluvní partner musí zejména před nahlášením problému provést v maximální míře vlastní kontrolu, aby vyloučil možnost, že příčina incidentu leží v oblasti jeho odpovědnosti.

Smluvní partner je odpovědný za ověření provozuschopnosti podpůrného software (agenta) v konkrétních kombinacích softwaru na Chráněném zařízení před jakýmkoli plánovaným produkčním použitím.

Smluvní partner neprodleně písemně informuje Poskytovatele, pokud není schopen plnit dohodnuté požadavky na spolupráci.

Povinnost Smluvního partnera poskytnout součinnost je základní povinností Smluvního partnera. Pokud Smluvní partner nesplní požadovanou povinnost poskytnout součinnost včas a dohodnutým způsobem nebo ji neposkytne v požadovaném rozsahu, nese následky z toho plynoucí (např. zpoždění, dodatečné náklady či vzniklá újma apod.) Smluvní partner.

4 Minimální doba užívání Služby a ukončení Služby

Minimální doba užívání Služby je 12 měsíců (pokud není ve Specifikaci služby sjednáno jinak) z důvodu předem pořízených licencí pro Smluvního partnera na minimální dobu smluvního závazku. Doba užívání Služby se vždy prodlouží o další jeden celý (1) rok, pokud není Specifikace služby ukončena výpovědí podanou vždy nejméně 3 měsíce před koncem minimální doby užívání Služby nebo příslušného prodloužení. Výpovědní doba potom končí s koncem minimální doby užívání Služby nebo příslušného prodloužení. Po ukončení poskytování Služby budou osobní údaje Smluvního partnera vymazány v souladu Podmínkami zpracování osobních údajů pro službu Magenta EDR.

5 Další podmínky

Uzavřením Specifikace služby Smluvní partner zároveň přijímá licenční podmínky používání software příslušných výrobců a dalších dodavatelů uvedených v nabídce nebo Specifikaci služby jakožto subdodavatelé. Aktuální znění smluvních podmínek dodavatele Bezpečnostní platformy je dostupné na https://www.crowdstrike.com/terms-conditions/

„Podmínky zpracování osobních údajů pro službu Magenta EDR“ jsou přílohou Specifikace služby Magenta EDR.

Seznam podporovaných operačních systémů:

Poskytovatel neustále aktualizuje software, aby ho přizpůsobil novým nebo aktualizovaným verzím operačních systémů. Starší verze operačních systémů jsou podporovány tak dlouho, jak je to možné. Z technických důvodů však nelze podporovat použití software (agentů) na zastaralých verzích operačních systémů neomezeně do budoucna. Poskytovatel si proto vyhrazuje právo ukončit podporu zastaralých verzí operačních systémů, zejména pokud jeho výrobce již neposkytuje služby (např. bezpečnostní aktualizace) pro daný operační systém.

EPP/EDR: Agenti pro koncová zařízení jsou dostupní v cloudové konzoli. Podporovány jsou platformy Windows, MacOS a Linux. Pro získání aktuálního seznamu podporovaných operačních systémů kontaktujte Poskytovatele.