FREEDIVISION
for safety reasons

Služba FreeDivision MDR

Managed Detection and Response

SLA – 8:00 AŽ 18:00 V PRACOVNÍCH DNECH

Služba FreeDivision MDR rozděluje aktivity v rámci kybernetické bezpečnosti na jednotlivé fáze, které jsou aktivovány v závislosti na dvou proměnných hrozbě a času. Následně jsou rozděleny do tří kategorií aktivit**: Reakce, Lov hrozeb** a **Reporting**.

Úvodní schůzka

Náš tým SOC (Security Operations Center) dodá novému klientovi detailní dotazník, který je použit ke zhodnocení několika klíčových bodů, jako jsou specifické podmínky, aktuální infrastruktura, používaný software, minulé útoky atp. Tyto odpovědi jsou poté využity k sestavení přesného rizikového profilu společnosti a také k nastavení jazyka komunikace, podoby reportů a denních aktivit.

Reakce – první oznámení

Ve chvíli, kdy je platformou nahlášena událost, tým SOC bez zbytečného prodlení zahájí proces zhodnocení rizika, díky kterému je událost sledována od samotného počátku s cílem rozpoznat riziko události – zda se jedná o škodlivou, nebo neškodlivou činnost. Do **30 minut** od vyvolání události je klient informován na předem stanovené platformě s předběžnými detaily o výskytu potenciálně škodlivé události a na základě aktivity provedené týmem SOC i o případném potvrzení její škodlivosti.

Reakce – Řešení incidentu

Tým SOC monitoruje každou škodlivou aktivitu až 4 hodiny nebo dokud se nezačne útočníkova aktivita rozšiřovat. Tato fáze je klíčová k získání veškerých informací o stupni inteligence daného útoku (Threat Intelligence), o jeho taktikách (Tactics), technikách (Techniques) a procedurách (Procedures). Tato data jsou poté použita v pozdějších fázích k aktivování podrobného a efektivního Plánu odpovědi na hrozbu (Response Plan). Pokud si klient vyžádá automatickou blokaci souvisejících aktivit, tato fáze je přeskočena, jelikož automatické blokování neumožňuje sběr informací o útoku.

V této fázi tým dedikovaný pro Lov hrozeb začne proaktivně procházet celou infrastrukturu a získávat veškerá potřebná data k pochopení hlavního zdroje útoku a k odkrytí dalších potenciálně infikovaných koncových stanic. Jakmile jsou fáze získávání dat o útoku a lovení hrozeb ukončeny a veškerý důkazní materiál je sesbírán, koncová zařízení jsou zbavena veškerého nežádoucího obsahu, je aktivován Plán odpovědi na hrozbu a všechna nezbytná blokovací pravidla jsou vytvořena. Koncová zařízení, která nemohou – z technických důvodů nebo dle požadavku klienta – být zbavena nežádoucího obsahu jsou izolována pro případ, že bude potřeba detailnější analýza koncového zařízení.

REAQTA
an IBM Company

Reporting – Detailní zpráva o incidentu

Veškeré informace získané při aktivitách po průniku do infrastruktury a výstupy z Lovu hrozeb jsou sesbírány do reportu a dodány zákazníkovi do 48 hodin od vyvolání události. Zpráva o incidentu obsahuje všechny důležité indikátory kompromitace (IoC – Indicator of Compromise), indikátory specifického chování, rekonstrukci cesty útočníka a veškeré další detaily potřebné k pochopení události a k získání praktických informací k posílení obranyschopnosti klienta a jeho systému v dané oblasti.

Lov hrozeb

Ne všechny hrozby mohou být identifikovány automaticky. V některých případech jsou útočníci schopni napodobit aktivity reálných uživatelů, např. krádeží certifikátů nebo hesel které umožní útočníkovi přístup do VPN sítě nebo k jakýmkoliv vnitřním systémům klientovy infrastruktury. V tomto případě nemá systém EDR k dispozici prakticky žádný kontext k aktivitám započatým mimo jeho dohled. K identifikování podobných situací proto nejlépe poslouží lov jednotlivých hrozeb.

Lov hrozeb je proces, který probíhá nepřetržitě, a který těží ze znalostí našeho interního SOC týmu o klientově infrastruktuře. Cílem procesu je identifikovat a izolovat potenciální hrozby bezpečnosti. Tato aktivita je prováděna nejen na základě našich interních znalostí hrozeb – například hledáním známých indikátorů aktivních škodlivých hrozeb – ale i pokročilým vyhledáváním takového chování uživatele, ve kterém jsou detekovány nové nebo neobvyklé charakteristiky.

Pokud je objevena potenciální hrozba bezpečnosti, veškeré dění je předáno do rukou Týmu pro řešení incidentů.

Lov hrozeb – na vyžádání (není součástí tohoto plánu MDR)

Klient si může vyžádat specifické a zvlášť placené aktivity nad rámec služby Lovu hrozeb. Tento proces je zahájen pouze na vyžádání klientem, který identifikoval anomální chování na různých úrovních, a který vyžaduje podrobnější data z koncových zařízení pro pokračování nebo potvrzení jeho analýzy.

Reakce – Specifické požadavky (není součástí tohoto plánu MDR)

Klient si může vyžádat specifické aktivity našeho SOC týmu vč.:

- Tvorby specifických blokovacích pravidel
- Tvorby specifických pravidel výjimek
- Izolace specifických koncových zařízení

REAQTA
an IBM Company

Reporty pro manažery

Každý měsíc náš SOC tým připraví souhrnný manažerský přehled všech aktivit za poslední měsíc. Tento report je vytvořen přímo na míru pro manažery, zdůrazňující nalezené problémy, nalezená rizika a nejlepší preventivní opatření k zamezení podobných útoků v budoucnosti.

Tyto reporty mohou být použity vedením společnosti k identifikování možných slabých oblastí v období klidu. V takovém období může management zadat nevytíženým týmům úkoly, jejichž splnění povede k posílení ochrany infrastruktury v rizikových oblastech, dokud je infrastruktura zabezpečena a není pod útokem.

Placená služba	Položka	SLA	Poznámky	Popis
V ceně MDR	První notifikace na událost	Do 30 minut od nahlášení	Pouze e-mailem	Klient obdrží e-mail od SOC týmu potvrzující škodlivé chování v jeho infrastruktuře.
V ceně MDR	Správa incidentu*1	Do 4 hodin od nahlášení	Pouze pokud je koncové zařízení online	Týmem jsou podniknuty kroky k zastavení škodlivých procesů, Toto zahrnuje: - Lov hrozby pro pochopení závažnosti a možného šíření - Izolace infikovaných stanic (pokud se infekce šíří) - Zastavení všech škodlivých procesů - Nastavení blokačních pravidel na škodlivé procesy - Odstranění/Očištění aplikací a souborů souvisejících s incidentem. * V průběhu vyšetřování incidentu může analytik dle potřeby stáhnout spustitelné soubory související s incidentem za účelem analýzy bez potřebného souhlasu klienta nebo samotného uživatele. Ke stažení souborů uživatele (dokumenty, PDF atp.) je třeba souhlas klienta ke stažení.
V ceně MDR	Detailní zpráva o incidentu	Do 48 hodin od nahlášení	E-mailem	Detailní zpráva o incidentu ve formě dokumentu.

REAQTA an IBM Company

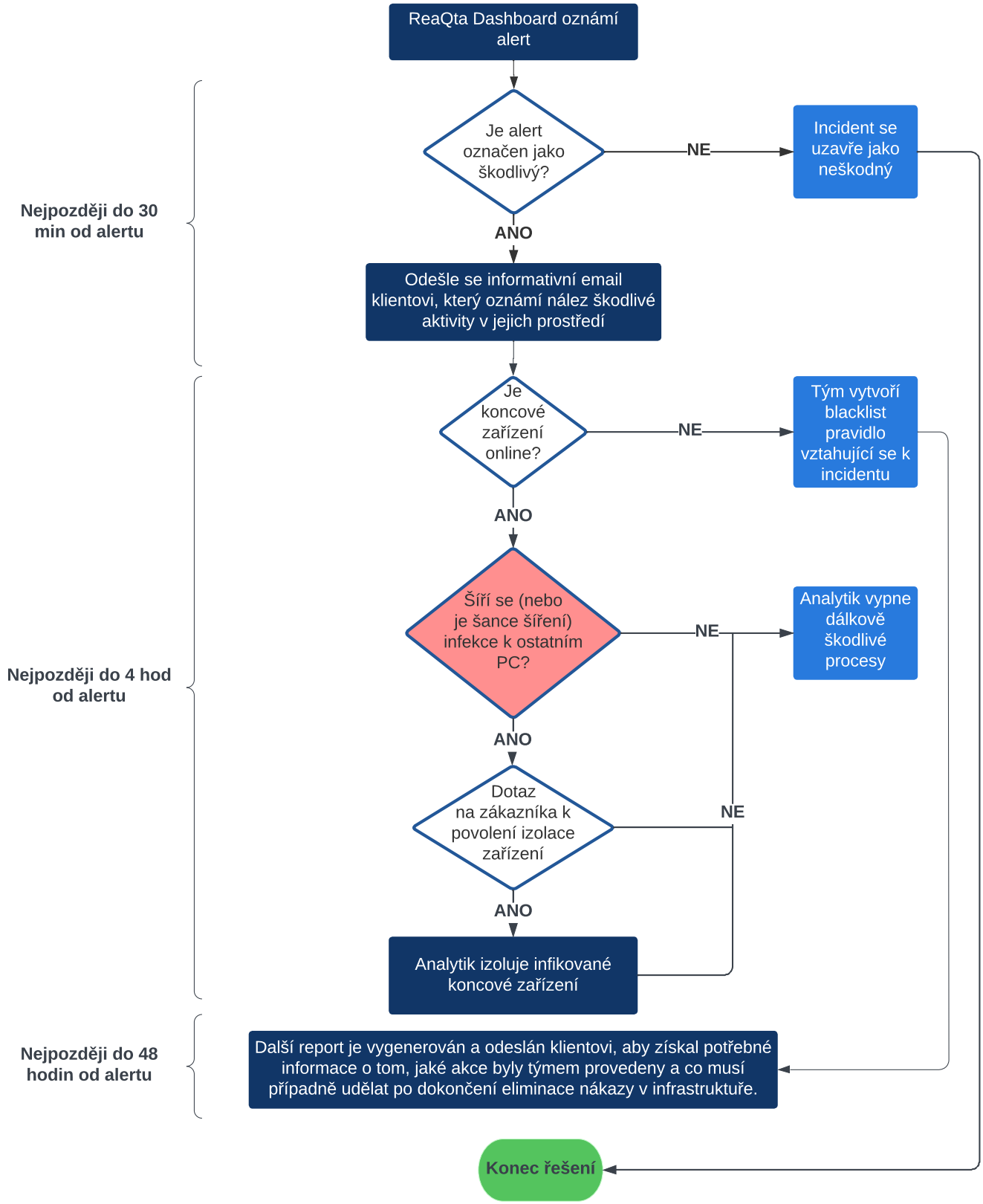
V ceně MDR	Proaktivní lov hrozeb	Není	SOC tým FreeDivision provádí tento lov bez definovaného SLA	Proaktivní lov hrozeb je prováděn alespoň dvakrát denně za účelem hledání podezřelých spojení a procesů, které mohou být nahlášeny detekčním jádrem později. Toto poskytne varování v rané fázi útoku a umožní definovat závažnost nebo aplikovat prevenci před vytvořením škodlivého chování. Navíc, vedle hledání možných indikátorů kompromitace (IoC) tým SOC také hledá nejnovější známé hrozby a „fileless" techniky, které by mohly být využity ke kompromitaci zařízení. Lov hrozeb se může skládat z hledání určitých hashů aplikací nebo specifického chování aplikací (například cmdLine parametr aplikace).
Není v rámci ceny MDR	Lov hrozeb na vyžádání	Do hodiny od vyžádání	Výsledek je odeslán e-mailem. Je možný pouze pokud je cílové zařízení online.	Lov hrozeb na vyžádání závisí na požadavku klienta. Detekují se: - Hashe aplikací - Specifické aplikace (například pokud klient chce vědět, jestli někdo využívá utorrent.exe) Specifické aktivity, které dokáže provést agent ReaQty.
Není v rámci ceny MDR	Požadavek na izolaci zařízení	Do 30 minut		
Není v rámci ceny MDR	Vytvoření blokujícího/povolujícího pravidla	Do 30 minut		
Není v rámci ceny MDR	Vytvoření Destra pravidla	není	Aktivace pravidla v konzoli Destra	
Není v rámci ceny MDR	API aplikace	není	Vytvoření key API	Např. propojení se systémy NAC, SIEM apod.

REAQTA an IBM Company

Není v rámci ceny MDR	Forward alerts	Do 30 minut	Přeposílání alertů do logovacího serveru klienta	
V ceně MDR	Metoda odeslání reportu	není	E-mail	
V ceně MDR	Vyhlášení pohotovosti	není		
V ceně MDR	Měsíční manažerský Report	není	Do prvních 5 pracovních dnů každého měsíce	
V ceně MDR	Možnost kontaktovat tým SOC telefonicky	není	Od 8:00 do 18:00 v pracovních dnech	

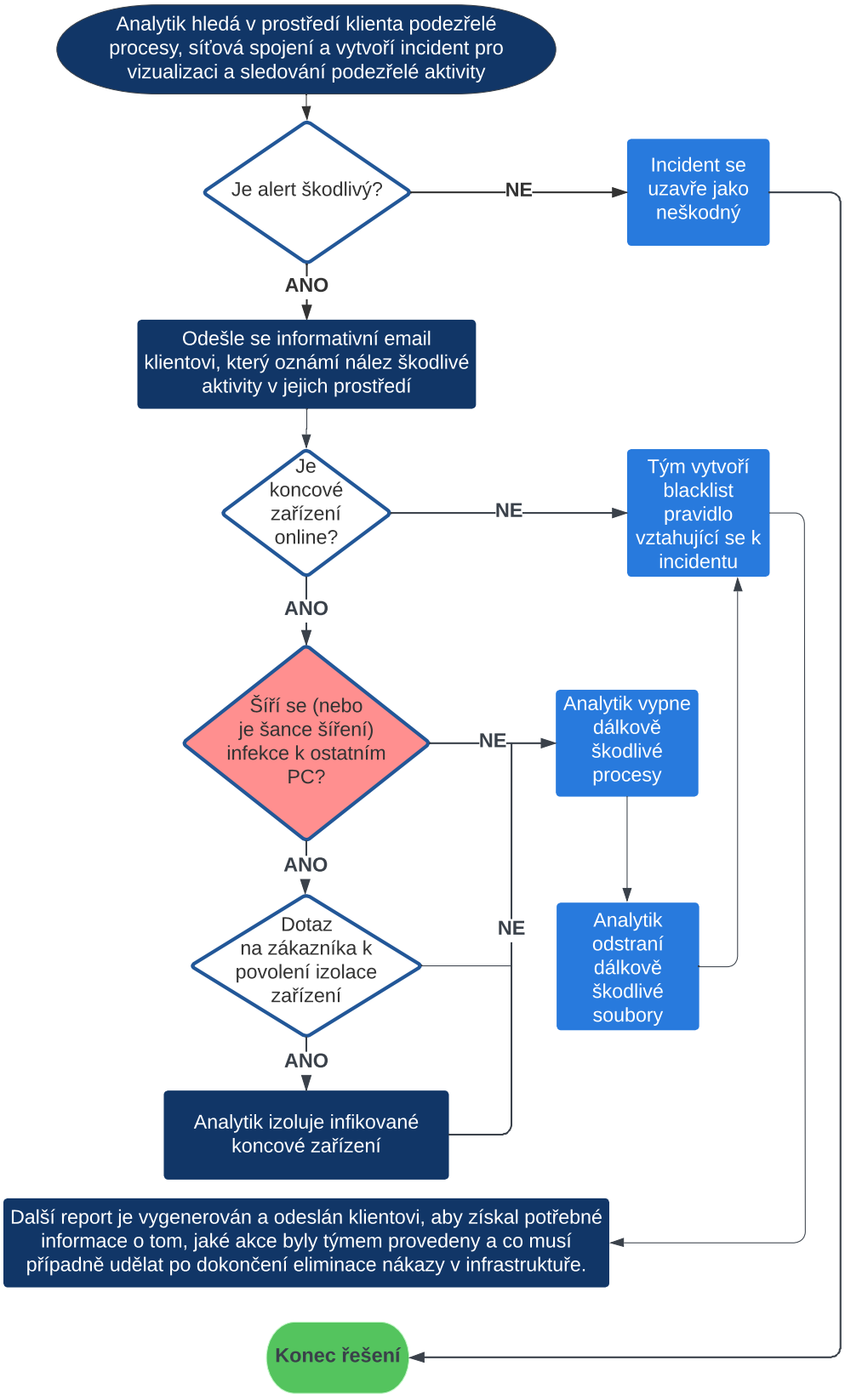
REAQTA
an IBM Company

Pracovní postup zpracování incidentů



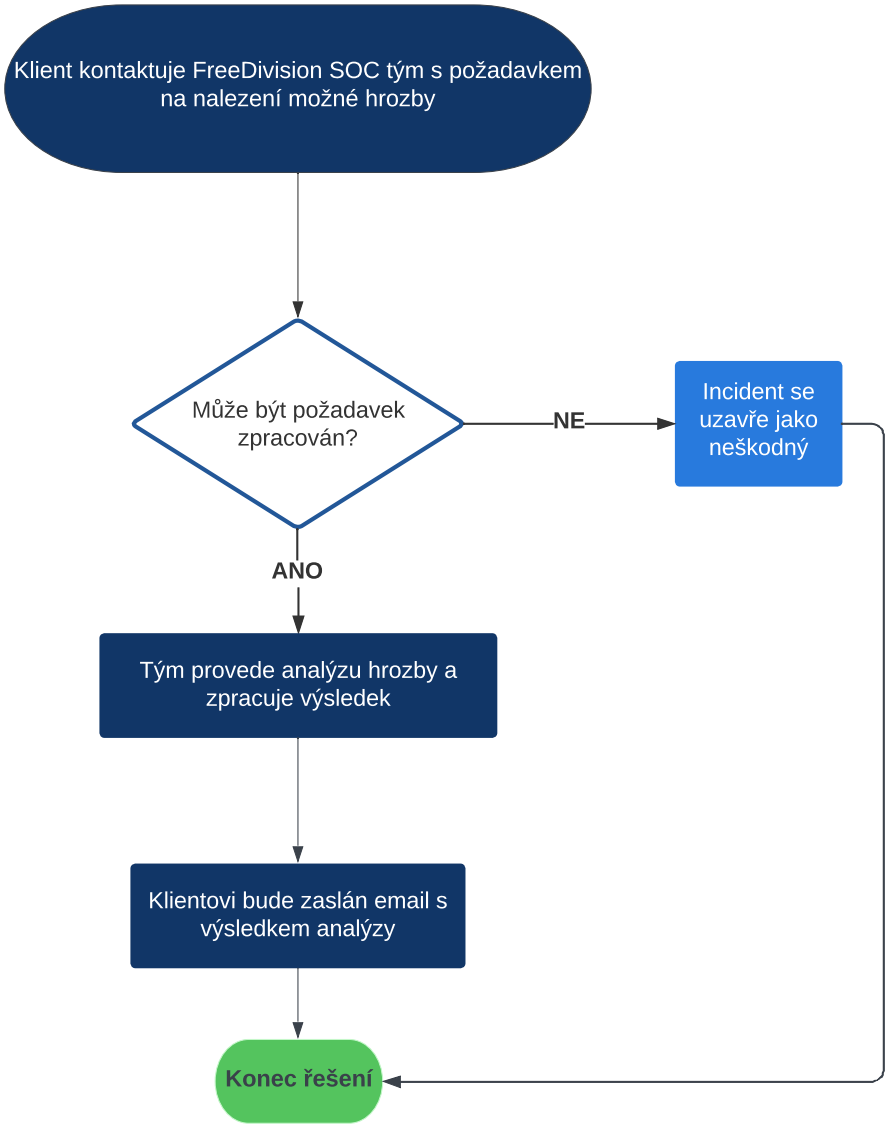
REAQTA
an IBM Company

Proces proaktivního lovu hrozeb



REAQTA
an IBM Company

Proces lovu hrozeb na vyžádání



REAQTA an IBM Company