kaspersky BRING ON THE FUTURE

Kaspersky Managed Detection and Response

Většina bezpečnostních týmů přistupuje k incidentům kybernetické bezpečnosti na základě výstrah a reaguje až poté, co k incidentu došlo. Mezitím se ale mimo dosah radaru pohybují nové hrozby a vy máte falešný pocit bezpečí – doslova. Firmy si stále více uvědomují potřebu aktivně v podnikové infrastruktuře vyhledávat hrozby, které dosud nebyly zjištěny, ale jsou stále aktivní.

Výhody služby:

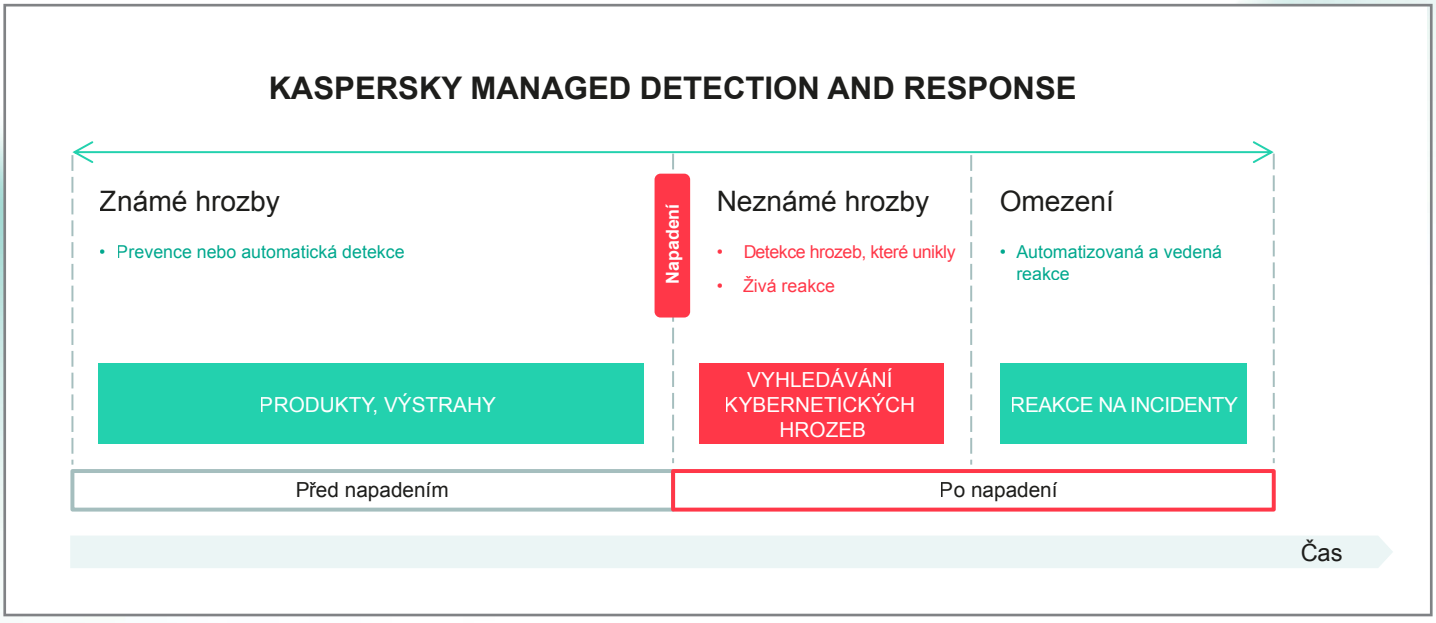
- Jistota vědomí, že jste neustále chráněni i před těmi nejinovativnějšími hrozbami
- Nižší celkové náklady na zabezpečení bez nutnosti zaměstnávat celou řadu interních bezpečnostních specialistů
- Zaměření drahých vlastních zdrojů na kritické úkoly, které skutečně vyžadují zapojení těchto zdrojů
- Všechny zásadní výhody plynoucí z toho, že máte vlastní operační bezpečnostní středisko, aniž byste museli takové středisko skutečně zřizovat

Služba Kaspersky Managed Detection and Response (MDR) poskytuje pokročilou nepřetržitou ochranu před rostoucím množstvím hrozeb, které obcházejí automatické bezpečnostní bariéry, a ulevuje organizacím, které mají problém najít specializované pracovníky nebo mají omezené vlastní zdroje.

Za jejími vynikajícími schopnostmi detekce a reakce stojí jeden z nejúspěšnějších a nejzkušenějších týmů pro hledání hrozeb v tomto odvětví. Na rozdíl od podobných nabídek na trhu Kaspersky MDR využívá patentované modely strojového učení, jedinečnou průběžnou analýzu hrozeb a prokázané výsledky účinného výzkumu cílených útoků. Automaticky posiluje odolnost vašeho podniku vůči kybernetickým hrozbám a zároveň optimalizuje vaše stávající zdroje a budoucí investice do zabezpečení IT.

Nejdůležitější informace o službě

- Rychlé a škálovatelné nasazení na míru přináší okamžité vyspělé zabezpečení IT bez nutnosti investovat do dalších pracovníků nebo odborných znalostí
- Špičková ochrana před i těmi nejsložitějšími a nejinovatějšími nemalwarovými hrozbami, která brání narušení chodu podniku a minimalizuje celkový dopad incidentů
- Plně spravovaná nebo vedená reakce na incidenty umožňuje bleskové zareagování, ale zároveň všechny akce ponechá zcela ve vašich rukou
- Viditelnost všech vašich prostředků a stavu jejich ochrany v reálném čase umožňuje neustálý přehled o situaci prostřednictvím různých komunikačních kanálů



Obrázek 1. KASPERSKY MANAGED DETECTION AND RESPONSE

Podporované produkty:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac[1]
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

Jak to funguje

Služba Kaspersky MDR ověřuje výstrahy produktů, aby zajistila účinnost automatické prevence, a aktivně analyzuje metadata aktivity systému, zda nevykazují známky aktivního nebo hrozícího útoku. Tato metadata jsou shromažďována prostřednictvím sítě Kaspersky Security Network a jsou automaticky v reálném čase porovnávána s nepřekonatelnou analýzou hrozeb společnosti Kaspersky za účelem identifikace taktik, technik a postupů používaných útočníky. Detekci skrytých nemalwarových hrozeb napodobujících legitimní aktivitu umožňují indikátory útoku vyvinuté společností Kaspersky. Služba se během prvních 2–4 týdnů přizpůsobí vaší infrastruktuře a za účelem dosažení nulového počtu falešně pozitivních výsledků vás bude žádat o potvrzení, co je a není legitimní.

Kaspersky MDR má dvě úrovně, které vyhovují potřebám organizací všech velikostí a odvětví. Každá z těchto úrovní má jinou úroveň vyspělosti zabezpečení IT (obrázek 2). **Kaspersky MDR Optimum** okamžitě zvýší vaši úroveň zabezpečení IT, aniž byste museli investovat do dalších pracovníků nebo odborných znalostí, a díky rychlému nasazení poskytuje odolnost vůči skrytým hrozbám. **Kaspersky MDR Expert** zahrnuje všechny funkce verze Optimum a poskytuje rozšířené funkce a flexibilitu pro vyspělé týmy zabezpečení IT, které tak mohou třídění a prošetření incidentů ponechat na společnosti Kaspersky a zaměřit své omezené interní prostředky zabezpečení IT na reakci na doručené kritické výstupy.

Obrázek 2. Úrovně řešení Kaspersky MDR

Automatické vyhledávání hrozeb, které je součástí verze MDR Optimum, využívá automatické detekce prováděné proprietárními indikátory útoku pro další ověřování, prošetření a identifikaci nových hrozeb. Spravované vyhledávání hrozeb ve službě MDR Expert se spoléhá na intenzivní a přímé úsilí našich zkušených odborníků na hrozby aktivně vyhledávajících hrozby, které unikají automatické detekci.

Soubor doplňkových volitelných prvků přizpůsobí funkčnost služby vašim konkrétním požadavkům a v případě potřeby poskytne větší flexibilitu:

- Flexibilní možnosti ukládání a uchovávání vyhovující regulačním požadavkům pro vyšetřování a e-discovery
- Nástroj pro uchovávání reakcí na incidenty, díky němuž lze plně zohledňovat váhu odborných znalostí společnosti Kaspersky pro řešení vašeho bezpečnostního incidentu
- Komplexní posouzení ohrožení bezpečnosti za účelem ověření, zda jsou vaše stávající bezpečnostní opatření dostatečná
- Praktické školení pro analytiky SOC pro zajištění vaší celkové připravenosti na incidenty

Odrážení cílených útoků vyžaduje rozsáhlé zkušenosti i neustálé učení. Jako první dodavatel, který téměř před deseti lety založil specializované centrum pro vyšetřování komplexních hrozeb, zjistila společnost Kaspersky více sofistikovaných cílených útoků než kterýkoli jiný poskytovatel bezpečnostních řešení. S využitím této jedinečné odbornosti maximalizuje služba Kaspersky Managed Detection and Response hodnotu vašich bezpečnostních řešení od společnosti Kaspersky, neboť poskytuje plně spravovanou a na míru přizpůsobenou průběžnou detekci, stanovování priorit, prošetření a reakci. Vy tak získáte všechny hlavní výhody vlastního operačního bezpečnostního střediska bez toho, aniž byste museli takové středisko zřizovat.

[1] Podpora je plánována na Q2 2021
[2] Podpora je plánována na Q1 2021
[3] Podpora je plánována na Q1 2021

Novinky v oblasti kybernetických hrozeb: www.securelist.com
Novinky v oblasti zabezpečení IT: business.kaspersky.com
Zabezpečení IT pro firmy: kaspersky.com/enterprise
Portál Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

Jsme prověření. Jsme nezávislí. Jsme transparentní. Zavázali jsme se k budování bezpečnějšího světa, ve kterém technologie zlepšují naše životy. Proto je zabezpečujeme, aby všichni lidé všude na světě mohli využívat nekonečné možnosti, které přinášejí. Zajistěte si počítačovou bezpečnost pro bezpečnější budoucnost.

Proven. Transparent. Independent.