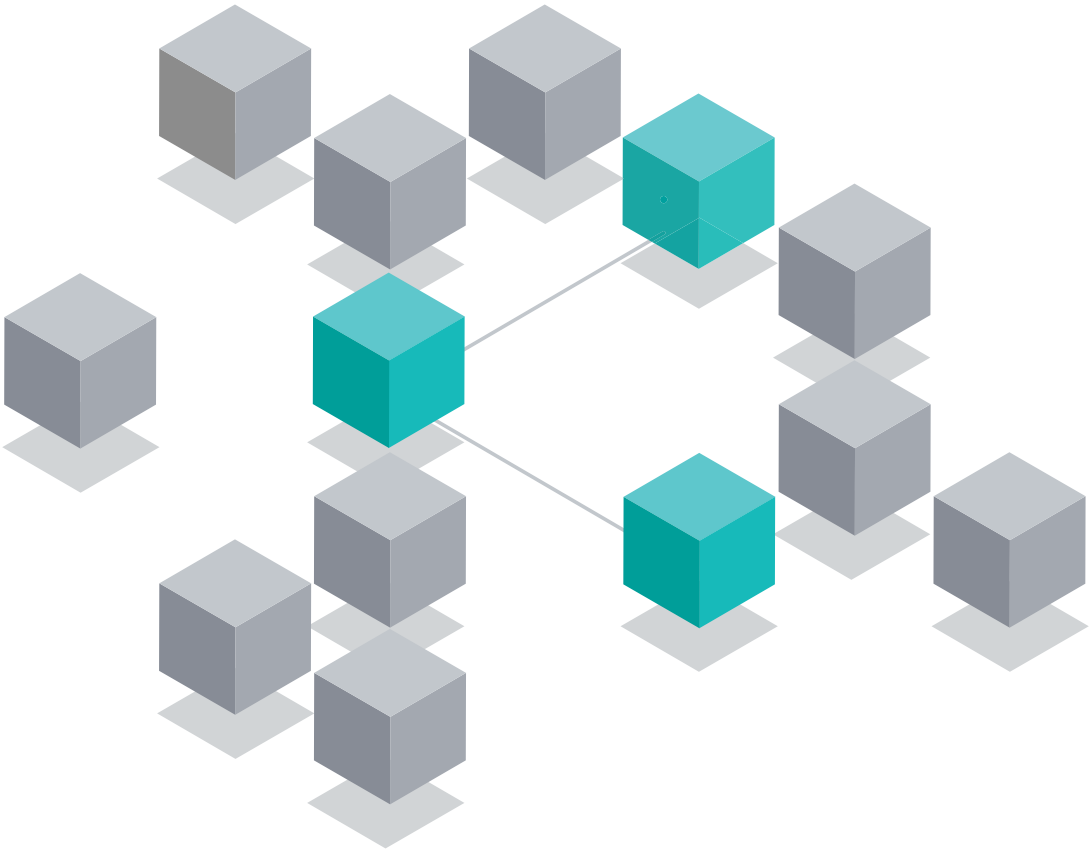
REAQTA
an IBM Company

FREEDIVISION
for safety reasons

IBM Security QRadar EDR



Řešení typu EDR pro detekci hrozeb na koncových bodech a jejich okamžité odstranění jsou důležitější než kdykoli předtím, protože koncové body jsou stále nejvíce ohroženou a zneužívanou částí každé sítě. Nárůst škodlivých a automatizovaných kybernetických aktivit zaměřených na koncové body způsobuje, že organizace bojují proti útočníkům, kteří snadno využívají zranitelnosti nultého dne (Zero Day vulnerability) pomocí přívalu ransomwarových útoků.

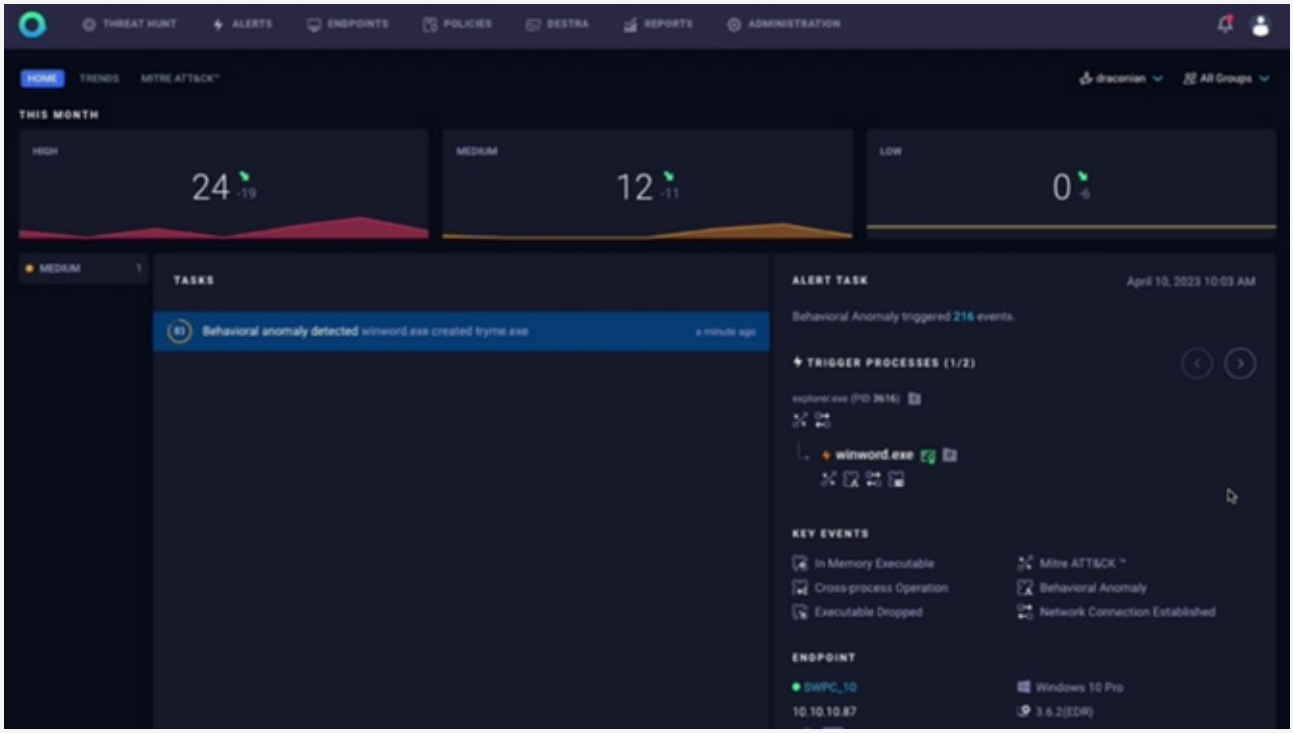
IBM Security® QRadar® EDR poskytuje ucelenější přístup EDR, který:

Odstraňuje známé i neznámé hrozby pro koncové body téměř v reálném čase pomocí inteligentní automatizace.

Umožňuje informované rozhodování pomocí průběhových tabulek s vizualizací činností útočníka.

Automatizuje správu výstrah, čímž snižuje únavu analytiků a soustředí se na důležité hrozby.

Posiluje postavení zaměstnanců a pomáhá zajistit kontinuitu podnikání díky pokročilým schopnostem neustálého učení umělé inteligence a uživatelsky přívětivému rozhraní.



IBM Security QRadar EDR demo (2:45)

Výhody řešení

Získejte jasný přehled
Získejte plnou kontrolu nad veškerou podezřelou aktivitou, kterou aktéři hrozeb vytvářejí na koncových bodech, díky zvýšenému přehledu o celém prostředí. Technologie NanoOS je navržena tak, aby ji protivníci nezjistili, a poskytuje hluboký přehled o procesech a aplikacích spuštěných na koncových bodech.

Automatizujte svou reakci
Naše průběžně se učící umělá inteligence detekuje a reaguje autonomně téměř v reálném čase na dříve nezjistitelné hrozby a pomáhá i nezkušeným analytikům s řízenou nápravou a automatickým zpracováním výstrah.

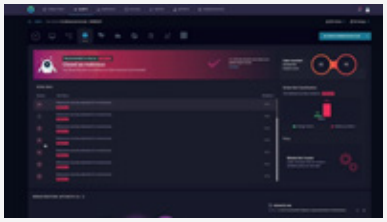
Přejděte od reaktivního k proaktivnímu
Získejte náskok před útočníky díky snadnému vytváření případů použití detekce a reakce, které mají validní výsledky během několika sekund a nechávají spícím hrozbám žádný prostor pro úkryt. Snadno sestavitelné případy použití jsou nasazovány v rámci celé organizace bez přerušení provozu koncového bodu.

Vlastnosti produktu

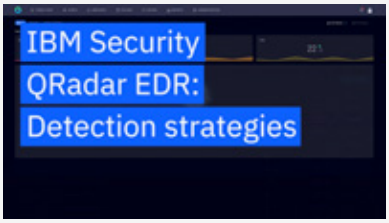
Strom chování
Strom chování poskytuje úplný přehled o výstrahách a útocích. Uživatelsky přívětivá vizualizace děje pomáhá analytikům urychlit vyšetřování a reakci. Odtud mají analytici také přístup k ovládacím prvkům pro omezení výskytu a ke třem fázím reakce na výskyt: třídění, reakce a zásady ochrany.

Kybernetický asistent
Systém správy výstrah s umělou inteligencí pomáhá ulehčit práci analytikům tím, že autonomně zpracovává výstrahy a snižuje počet falešných poplachů v průměru o 90 %. Učí se z rozhodnutí analytiků a poté uchovává intelektuální kapitál a naučené chování, aby mohl poskytovat doporučení a urychlit reakci.

Prevence před ransomwarem
Útoky ransomwaru jsou na vzestupu a jejich četnost a složitost bude nadále narůstat. Antivirové metody již nestačí. QRadar EDR může organizacím pomoci odhalit a zastavit ransomware téměř v reálném čase.



Seznamte se s kybernetickým asistentem QRadar EDR poháněným umělou inteligencí (2:07)



Přizpůsobení zabezpečení koncových bodů pomocí detekčních strategií IBM Security QRadar EDR (1:41)

IBM Security QRadar EDR
On-Premise včetně režimu AirGap

Správa koncových bodů může být náročná.
Zejména organizace, které se řídí bezpečnostními požadavky, regulačními zákony nebo obavami o suverenitu dat, nemusí být schopny používat bezpečnostní řešení dodávaná formou služeb jako SaaS. QRadar EDR, který je nyní k dispozici on-premise jako forma capex investice, poskytuje svobodu výběru možnosti nasazení, která vyhovuje vašemu prostředí a pomáhá splnit cíle v oblasti dodržování předpisů. To je obzvláště užitečné pro klienty, kteří j sou nuceni pracovat v tzv. air-gap prostředích, čili zabezpečených počítačových sítích fyzicky izolováných od sítí, jako je veřejný internet nebo jiné místní sítě.
https://community.ibm.com/community/user/security/blogs/andie-schroeder/2023/10/24/deploy-anywhere-ibm-security-qradar-edr-on-premise

QRadar® MDR

Nechte naše odborníky spravovat detekci hrozeb na koncových bodech a reakci na ně.
Jedná se o kontinuální službu v režimu 8x5, která spočívá v řízené automatizaci strojového učení při detekci hrozeb systémem na koncových bodech s okamžitou reakcí a vyhodnocením. Celý proces je poháněn umělou inteligencí samotné technologie Qradar EDR a dohlížen službou FreeDivision Managed Security Services.

Výhody MDR

Úplná správa výstražných oznámení
Všechny detekce (nízké, střední a vysoké závažnosti) jsou prozkoumány, analyzovány a spravovány bez zapojení úsilí vašeho bezpečnostního týmu.

Rychlé potlačení hrozby
Analytici reagují na aktivní hrozby ukončením a odstraněním škodlivých souborů nebo procesů, vytvořením blokovacích zásad nebo izolací koncových bodů.

Okamžitá a nekompromisní reakce
Incidenty, které vyžadují pozornost, budou hlášeny a obohaceny o relevantní informace o hrozbách a doporučení ke zpřísnění bezpečnostních opatření.

Proaktivní vyhledávání hrozeb
Proaktivní vyhledávání hrozeb je založeno na analýze hrozeb X-Force® a probíhá nepřetržitě prostřednictvím konzole QRadar EDR, která vyhledává potenciální indikátory útoku a kompromitace.

Snížení celkových nákladů na zabezpečení
Vaše bezpečnostní schopnosti mohou být rozšířeny bez dodatečných nákladů spojených s najímáním a udržováním odborníků na kybernetickou bezpečnost.

Bezproblémové rozšíření vašeho týmu
Rozsáhlé časové a finanční prostředky na správu zabezpečení lze díky této službě přesunout na jiné každodenní činnosti a důležité projekty.
https://ibmqradaredr.freedivision.com/brozura/Sluzba-MDR-SLA.pdf

REAQTA
an IBM Company

FREEDIVISION
for safety reasons

O společnosti IBM

Divize IBM Security v rámci společnosti IBM vyvíjí inteligentní řešení a služby zabezpečení, které umožňují organizacím zajistit bezpečnost všude, aby mohly prosperovat tváří v tvář nejistotě.
IBM Security dnes pomáhá chránit vaše podnikání pomocí pokročilého a integrovaného portfolia řešení a služeb kybernetické bezpečnosti s využitím umělé inteligence. Náš moderní přístup k bezpečnostní strategii využívá principy nulové důvěry a umožňuje podnikům sladit, chránit, spravovat a modernizovat ochranu před kybernetickými hrozbami ve stále hybridnějším, multicloudovém světě.

O společnosti FreeDivision

IT bezpečnosti se věnujeme více než 17 let a stále je naším koníčkem. Vyhledáváme to nejlepší z oblasti bezpečnosti a ochrany dat. Zastupujeme několik celosvětově renomovaných výrobců a jejich řešení vám exkluzivně přinášíme spolu s týmem proškolených profesionálů a konzultačními službami.

Výhradní zastoupení pro Českou republiku
FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

www.freedivision.com