IBM SECURITY

QRadar SIEM benefity

IBM

1. Platforma IBM QRadar

IBM Security QRadar je otevřená platforma pro sběr a vyhodnocování bezpečnostních událostí. Řešení umožňuje bezpečnostním analytikům efektivně reagovat na již proběhlé bezpečnostní incidenty, ale dokonce tyto incidenty předvídat a předcházet jim.

V dnešní době už jednoduchý log management nestačí, ale je potřeba dávat informace do širších souvislostí spolu s informacemi o toku v síti, zranitelnostech a míře rizika pro daný segment nebo zařízení. Řešení QRadar poskytuje log management, event management, reporting a analýzy chování pro sítě a aplikace nebo uživatele.

Silnou stránkou řešení je mimo jiné i komplexní chápání různých zdrojů a relevantních bezpečnostních informací, a to zejména díky univerzální a modulární platformě Security Intelligence. Spolu s volitelnými doplňujícími moduly pro rozšíření funkcionality a zpřesnění detekce jakou jsou **Vulnerability Management**, pro efektivní práci a korelaci zranitelností či **Risk Mangement** umožňující tvorbu "Co – Když" analýz a v neposlední řadě také s modulem **Incident Forensics** je řešení QRadar silným partnerem bezpečnostního analytika ve všech fázích – od detekce potenciálních slabých míst, detekci incidentů až po následné investigace chování.

Řešení je možno nasadit formou HW appliance, nebo software na ekvivalentní HW jiného výrobce či velmi oblíbenou formou virtuální appliance a lze snadno nasadit formou tzv. All-in-One řešení. Řešení QRadar out-of-the-box umožňuje bez-agentní sběr z nejrůznějších zdrojů, včetně databázových systémů.

Řešení disponuje podporou normalizace několika stovek nejrůznějších zařízení napříč dodavateli, zároveň je ale možné velmi snadno rozšířit o další zařízení. Řešení též disponuje stovkami předpřipravených korelačních pravidel a reportů, během nasazení se tedy dostavují zejména nezbytné informace pro kontext (sít, kategorizace serverů, ...) a rozšíření o specifická pravidla nebo reporty dle potřeb klienta.

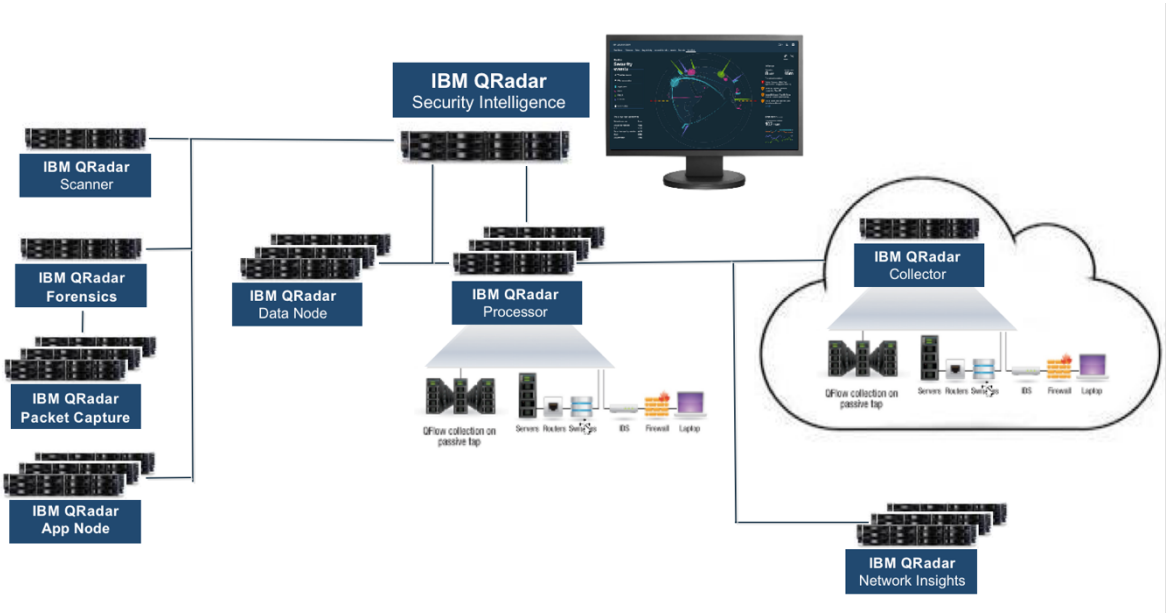
2. Benefity pro zákazníka

Rozšířenost na trhu

Díky mnoha úspěšným implementacím nejen v rámci České a Slovenské republiky, existuje na trhu mnoho spokojených zákazníků, ale i mnoho zkušených partnerů, kteří mohou pomoci při zavádění, údržbě a následném rozšíření QRadar SIEM platformy.

Široká rozšiřitelnost

Celkově je možné řešení neustále rozšiřovat o nové komponenty a funkcionality nad rámec běžného SIEM řešení, jak je naznačeno na následujícím obrázku.



Platforma QRadar Security Intelligence byla vytvořena jako framework pro podporu budoucí expanze a integrace s řešeními třetích stran. Systém QRadar je postaven na operačním systému SIOS (Security Intelligence Operations System).

SIOS umožňuje systému QRadar využít společný rámec pro shromažďování a správu dat, vytváření zpráv, forenzní analýzy a analýzy pro vytváření bezpečnostních inteligentních modulů, které se plně integrují do systému QRadar.

Navíc QRadar poskytuje obousměrné API, které umožňuje integraci i s dalšími doplňkovými řešeními.

Pro umožnění sdílení aplikací mezi zákazníky, vývojáři a obchodními partnery, existuje **IBM Security App Exchange**. IBM a její obchodní partneři se aktivně podílejí na přidávání nových aplikací, které jsou poté dostupné pro všechny uživatele.

Inteligentní tvorba upozornění

Jedinečná schopnost produktu QRadar je korelovat mnoho souvisejících položek do jediného incidentu, na rozdíl od vytváření více incidentů. V detailním pohledu na incident jsou pak uvedeny všechny události, které byly shromážděny v rámci tohoto incidentu. Incidenty jsou neustále obohacovány tím, jak systém QRadar získává další podrobnosti.

Tato inteligence umožňuje analytikům soustředit se pouze na skutečné incidenty a neztrácet čas spojováním si jednotlivých důkazů manuálně.

Out-of-the-box obsah

Systém QRadar obsahuje stovky korelačních pravidel, které implementují nejběžnější Use cases. Dále jsou přiloženy tisíce předpřipravených reportů, desítky dashboardů, a mnoho dalšího. Další pravidla, reporty atd. lze najít a stáhnout z IBM Security App Exchange portálu.

Vysoká míra upravitelnosti

Řešení QRadar se pyšní vysokou mírou upravitelnosti, ať se jedná o grafické úpravy, tvorby vlastních dashboardů, pravidel, reportů atd., tak i jednoduchou úpravou či přidáním nových zdrojů dat.

Do prostředí lze přidat i vlastní grafické prvky spouštějící například uložené skripty, či přidání nových aplikací, které se automaticky integrují do centrálního grafického rozhraní.

To vše bez nutnosti využití profesionálních služeb výrobce.

Široká podpora zdrojů dat

Systém QRadar se pyšní jednou z nejširších podpor zdrojů událostí. Tisíce zařízení je podporováno out-of-the-box. Pokud však zákazník natrefí na nepodporované zařízení, lze jej rychle přizpůsobit a systém QRadar naučit rozpoznat události z takového zdroje. To vše pomocí grafického DSM editoru, ve kterém si zákazník nastaví správné parsování informací obsažených v událostech.

Jednoduché aktualizace

QRadar podporuje velmi snadný způsob aktualizací celého řešení. Aktualizace lze tedy provádět bez nutnosti kontraktování profesionálních služeb.

Podpora pro oddělení podřízených organizací (multi-tenancy)

Řešení Qradar podporuje možnost oddělit prvky infrastruktury pro samostatnou správu částí sítě, například pro podřízené organizace, a to jak ve formě All-in-One appliance tak i v distribuovaném nasazení. Rozdělení podporuje nejen oddělení událostí, ale zahrnuje i toky, aktiva a zranitelnosti.

Překryv IP adres se rozlišuje pomocí rozdělení do domén na úrovni zdroje událostí (log source).

Řízení zranitelností – QRadar Vulnerability Manager

QRadar Vulnerability Manager (QVM) umožňuje, jak aktivně zjišťovat zranitelnosti pomocí vlastního skeneru, tak je také schopen integrovat a pracovat s výstupy skenerů třetích stran. QVM nejen že dokáže zranitelnosti identifikovat a kategorizovat, ale díky každodenním updatům od IBM X-Force Research je databáze vždy relevantní. K tomu jsou přímo v konzoli k dispozici informace o nalezené zranitelnosti, vysvětlení hrozby při jejím potenciálním zneužití, a i případné tipy, jak danou mezeru v zabezpečení odstranit.

Řízení rizik – QRadar Risk Manager

QRadar Risk Manager slouží jako přídavný modul pro IBM Qradar SIEM, jenž obohacuje o nástroje, které jsou nepostradatelné při předcházení budoucích útoků na počítačovou infrastrukturu. K předcházení útokům dochází pomocí identifikace chybně nastavených pravidel u aktivních prvků síťové infrastruktury, jako jsou firewally, routery, switche nebo IPS.

IBM Risk Manager automaticky z konfiguračních souborů a routovacích tabulek z routeru vytváří topologii. Vzhledem k tomu že je topologie vytvářena automaticky z konfiguračních souborů a nevytváří ji uživatel ručně, jsou v ní zahrnuty všechny aktuální trasy mezi jednotlivými sítěmi, které daná konfigurace síťových prvků umožňuje. Topologii sítě poté lze stáhnout ve formátu PNG nebo VDX pro software Microsoft Visio.

Vzhledem k tomu že se jedná o doplněk Qradar SIEM lze QRM spravovat ze stejné konzole.

Monitoring aplikací – Qradar QFlow

Systém QRadar poskytuje síťové monitorování aplikací pomocí technologie nazvané QRadar QFlow. QRadar QFlow je kolektor síťových aktivit, který pasivně shromažďuje, analyzuje a klasifikuje pakety, včetně části payloadu, ze sedmé aplikační vrstvy. QRadar QFlow provádí pokročilou detekci komplexních aplikací, jako je například provoz VoIP, P2P, databázové aplikace a sociální sítě.

Technologie QRadar QFlow je zcela integrována do řešení QRadar SIEM.

Podrobná analýza obsahu – QRadar Network Insights

Stejně jako QFlow kolektor prohledává i část obsahu všech paketů, QRadar Network Insights sonda umožňuje zaznamenání a analýzu celého „payloadu“. Výsledkem analýzy celého paketu může být například informace o „hash“ přenášeného souboru, kterou systém automaticky porovná s databází nakažených souborů. To vše poté systém koreluje s dalšími informacemi a následně vytvoří incident (offense), s upozorněním na přenos nakaženého souboru a které stanice mohou být napadeny.

Forenzní analýza – QRadar Incident Forensics

Qradar Incident Forensics umožňuje přehrát krok po kroku zachycené akce potencionálního útočníka a rychle a jednoduše najít ohrožené části sítě. V případě, že k útoku již došlo, najde data, která s útokem souvisela, a tím významně redukuje čas, který bezpečnostní tým potřebuje k prozkoumání záznamů o útoku. V mnoha případech se probírání záznamů zkrátí ze dnů na hodiny, nebo dokonce minuty. Minimalizuje tak čas nutný k obnově bezpečnosti v síti a brání dalším útokům.

Qradar Incident Forensics umožňuje prozkoumávat data nejen z vlastního zařízení na zachytávání paketů (PCAP), ale také umí pracovat se zařízeními třetích stran.

Agregace síťových toků

Při sledování komunikace pomocí síťových toků je důležité spojovat oba směry konverzace, pro pochopení smyslu přenosu, a tedy možnosti odhalit nekalé chování.

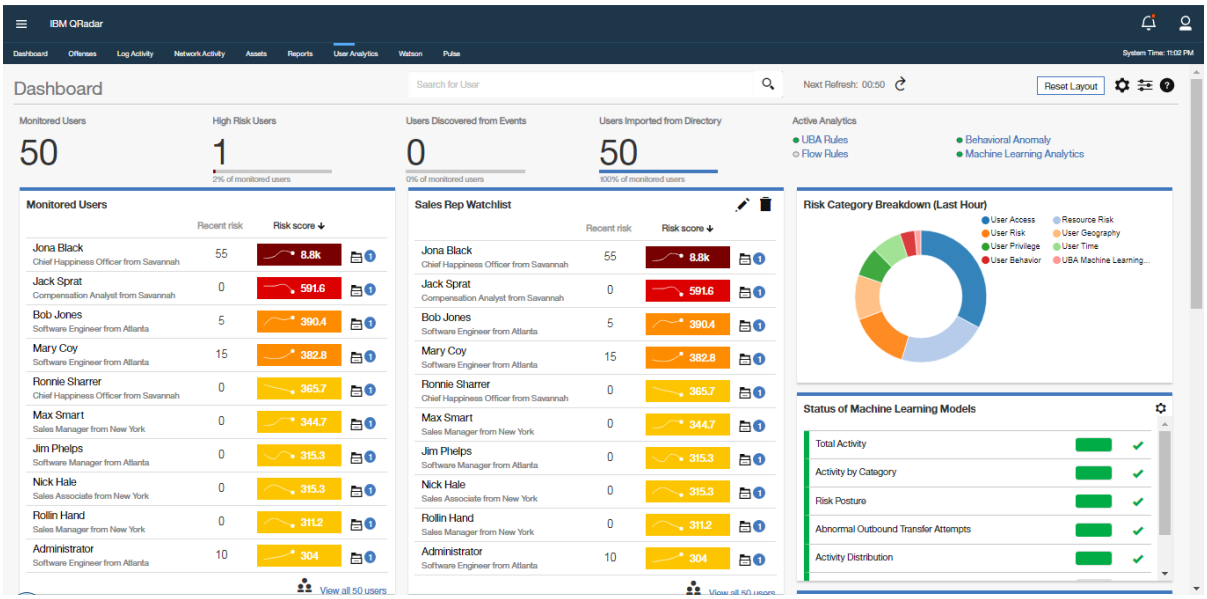
Qradar slučuje obousměrné flows do jednoho záznamu pro lepší analýzu a umožňuje slučování i v případě, že je každý směr datového toku realizován jinou cestou v síti.

Behaviorální analýza uživatelů (User Behavior Analysis)

QRadar User Behavior Analytics analyzuje chování uživatelů pro detekci podezřelého chování. Přidává informace o uživateli do kontextu logů a zranitelností. Hodnotí uživatele podle Risk Score na základě jejich aktivit ze síťových toků a logů.

QRadar User Behavior Analytics spojuje chování uživatelů v prostředí pomocí dostupných identifikátorů a sjednocuje tak události k jednotlivým uživatelům na základě těchto atributů.

QRadar UBA je příklad aplikace, která je volně dostupná na **IBM Security App Exchange**, její využívání je tedy zcela na rozhodnutí zákazníka, zda si ji do systému přidá nebo ne. Výhodou je také to, že pokud nesledujeme stovky tisíc uživatelů, může být UBA nainstalována na centrální konzoli. Pro navýšení výkonu ji poté lze přesunout na samostatný boxu tzv. App Host.



Síťová behaviorální analýza (Network Behavior Analysis)

Standardní součástí řešení QRadar je detekce anomálií pro události a síťové toky. Například systém QRadar se automaticky naučí, jaké jsou obvyklé míry událostí (události za sekundu) pro každou IP nebo zařízení a následně tak může identifikovat náhlé změny v počtu událostí přicházející z konkrétního zařízení.

Systém QRadar také zjišťuje anomálie v síťové komunikaci (např. nový provoz v síti, významné zvýšení nebo snížení síťové komunikace.) To lze rozpoznat na úrovni aplikace, protokolu nebo sítě

Zapojení umělé inteligence

Systém QRadar umožňuje rozšíření o pomocníka pro vyšetřování incidentů ve formě umělé inteligence.

Qradar Advisor with Watson umožňuje bezpečnostním analytikům konzistentní vyšetřování a urychlení a rozhodnější eskalaci incidentů, což má za následek zkrácení doby prodlevy a zvýšení efektivity analytika.

Qradar Advisor with Watson může rozšířit pohled na incident prozkoumáním lokálních informací spolu s externími. Díky tomu získá analytik větší pochopení incidentu a je si i více jistý rozhodnutím, že se jedná o skutečný incident.

3. Závěr

Výše uvedený výčet výhod je pouze zlomkem ze skutečného potencionálu systému QRadar.

IBM QRadar patří dlouhodobě mezi leadery na trhu SIEM systémů. Podle společnosti Gartner je hodnocen již devět let v řadě bez výjimky přímo jako leader.