IBM Security QRadar SIEM

Zlepšete ochranu před hrozbami s využitím integrovaného analytického reportingového systému

Shrnutí

- Integrujte správu logů a technologie pro ochranu sítě do společné databáze s jednotným ovládacím panelem
- Redukujte tisíce bezpečnostních událostí na ty opravdu podstatné potenciální útoky
- Detekujte a sledujte zlomyslné uživatele v delších časových úsecích a odhalte tak sofistikované hrozby, které jsou často jinými bezpečnostními řešeními přehlíženy
- Odhalte interní hrozby s využitím pokročilých funkcí
- Získejte nástroj na sledování regulatorních požadavků a směrnic

Dnešní sítě jsou rozsáhlejší a komplexnější než kdy dřív a chránit je proti zlomyslným aktivitám je nikdy nekončícím úkolem. Firmy, které chtějí ochránit své duševní vlastnictví, chránit identitu svých zákazníků a zamezit výpadkům svých systémů, musejí dělat víc než jen monitorovat logy a síťový provoz – musejí využívat pokročilých nástrojů pro detekci těchto aktivit nějakým uchopitelným způsobem. IBM® Security QRadar® SIEM může sloužit uvnitř datových center malých i velkých firem jako hlavní řešení pro sběr, normalizaci a analýzu síťových analytických funkcí. Výsledkem je pak něco, čemu říkáme security intelligence neboli bezpečnostní zpravodajská činnost.

Srdcem tohoto produktu je vysoce škálovatelná databáze navržená pro zachycování logů událostí a dat o provozu v síti v reálném čase. QRadar SIEM je podnikové řešení, které konsoliduje záznamy o událostech z tisíců zařízení, rozmístěných napříč celou sítí a ukládá každou aktivitu v její původní podobě, přičemž jednotlivé události ihned dává do souvislostí, aby odlišilo reálné hrozby od falešných poplachů. Toto řešení také v reálném čase zachycuje síťový provoz na 4. vrstvě modelu OSI a co je unikátnější – s využitím technologie pro hloubkovou analýzu paketů také aplikační data na7. vrstvě modelu OSI.

Intuitivní uživatelské rozhraní, shodné napříč celou rodinou komponent QRadar, pomáhá pracovníkům IT oddělení rychle identifikovat a odvrátit vznikající útoky podle jejich závažnosti a shrnout stovky upozornění na vznikající anomální aktivity do výrazně menšího počtu potenciálních útoků, které si žádají podrobnější šetření.

Analýza v reálném čase pro detekci a prioritizaci hrozeb

QRadar SIEM poskytuje kontextový a analytický dohled nad celou IT infrastrukturou a pomáhá tak firmám detekovat a eliminovat hrozby, které by jinými bezpečnostními řešeními byly často přehlédnuty. Tyto hrozby mohou zahrnovat neobvyklé využití aplikací, útoky zevnitř, i pokročilé „pomalé“ hrozby, ztracené v „šumu“ milionů událostí.

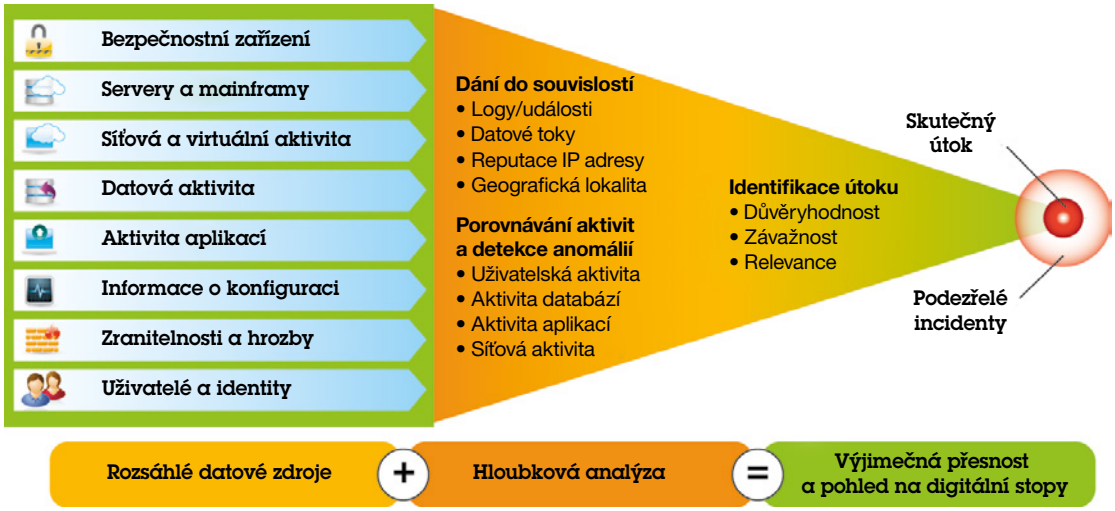
QRadar SIEM sbírá informace, které zahrnují:

- **Bezpečnostní události:** události z firewallů, virtuálních privátních sítí, intrusion detection systémů, intrusion prevention systémů a dalších
- **Síťové události:** události z přepínačů, směrovačů, serverů, koncových stanic a dalších
- **Kontext síťových aktivit:** data aplikací na 7. vrstvě získané ze síťového provozu
- **Uživatelský kontext a kontext zařízení v síti:** kontextová data z uživatelských identit, přístupů a skenerů zranitelností
- **Informace z operačních systémů:** jméno výrobce, číslo verze specifické pro jednotlivé součásti sítě
- **Logy aplikací:** ERP, systémy pro správu workflow, databáze, administrační nástroje a další

Redukce a prioritizace poplachů umožňující zaměřit se na vyšetřování skutečných útoků

Řada firem vytváří miliony či dokonce miliardy událostí každý den. Získat z těchto dat krátký přehled útoků, které je třeba přednostně řešit, může být velice náročné. QRadar SIEM automaticky zkoumá většinu síťových logů zdrojových zařízení a prohlíží datový provoz, aby nalezl a klasifikoval autorizované koncové stanice a servery na síti a sledoval aplikace, protokoly, služby a porty, které využívají. QRadar SIEM tato data sbírá, ukládá a analyzuje a v reálném čase dává jednotlivé události do souvislostí. Toho je využito k detekci hrozeb i auditingu a reportingu plnění regulatorních a bezpečnostních směrnic. Díky tomu mohou být miliardy událostí a datových toků zredukovány a následně prioritizovány do výsledného krátkého seznamu skutečných útoků, setříděných dle jejich dopadů na chod firmy.

Výsledkem toho obvykle je, že bezpečnostní experti poznají skutečnou přidanou hodnotu implementace QRadar SIEM během několika málo dnů namísto měsíců a že je celé řešení možné nasadit i bez armády drahých konzultantů. Funkce automatického prohledávání sítě a přednastavené šablony a filtry pak znamenají, že netrávíte měsíce zadáváním parametrů síťového prostředí do systému jako u jiných, obecnějších nástrojů pro zajištění provozu IT. Architektura QRadar SIEM je variabilní dle potřeb organizace ve formě hardwarových, softwarových i virtualizovaných integrovaných zařízení. Menší instalace mohou začít s jediným all-in-one řešením a následně mohou být snadno upgradovány na implementace využívající konzolu s možností přidat zařízení pro zpracování událostí a datových toků.



IBM QRadar Security Intelligence Platform nabízí 360° bezpečnostní analýzu

Zodpovězení klíčových otázek pro efektivnější správu hrozeb

Bezpečnostní týmy potřebují zodpovědět klíčové otázky, aby plně porozuměly povaze potenciálních hrozeb, kterým čelí: Kdo útočí? Na co útočí? Jaký je vliv útoku na chod firmy? Kde mám začít s vyšetřováním útoku? QRadar SIEM zaznamenává významné incidenty a hrozby a vytváří podpůrná data a související informace. Detaily jako cíle útoku, přesný čas, hodnota zasažených aktiv, stav zranitelností, identita útočících uživatelů, profily útočníků, aktivní hrozby a záznamy předchozích útoků – to vše pomáhá poskytovat bezpečnostním týmům informace, které potřebují pro realizaci příslušných opatření.

Prohledávání historie událostí a datových toků v reálném čase s využitím lokalizačních dat pro podrobnější analýzu a zajištění stop může významně zlepšit schopnosti firmy v oblasti řešení incidentů. Se snadno použitelnými řídicím panelem, časovými pohledy, detailním vyhledáváním, s přehledy obsahu až na úroveň jednotlivých paketů a se stovkami předdefinovaných vyhledávacích dotazů mohou uživatelé rychle získat data potřebná pro shrnutí a identifikaci anomálií.

Získání přehledu o aplikacích a detekce anomálií

QRadar SIEM podporuje širokou škálu funkcí pro detekci anomálií umožňujících identifikovat změny v chování, které ovlivňují aplikace, koncové stanice, servery i jednotlivé síťové prvky. Je možné například rozpoznat provozní špičku u aplikace či cloudové služby, anebo je možné odhalit sezónní výkyvy či schémata aktivity sítě, která jsou nekonzistentní s historickými údaji. QRadar SIEM se učí rozpoznávat tyto denní a týdenní profily provozního zatížení a pomáhá tak pracovníkům IT rychle identifikovat významné odchylky.

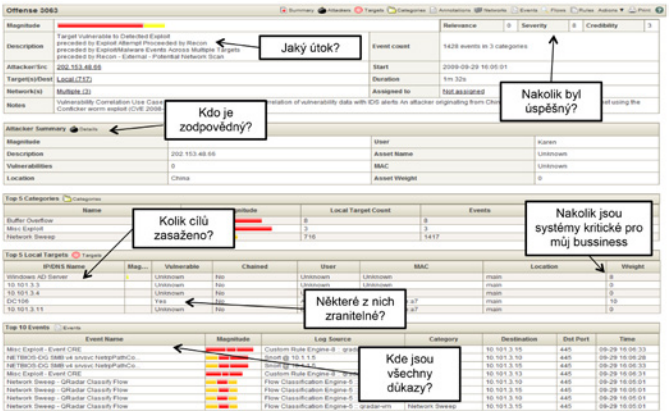
Centralizovaná databáze QRadar SIEM ukládá společně zdrojové logy událostí a síťový provoz, což pomáhá odhalovat souvislosti mezi jednotlivými událostmi a obousměrným síťovým provozem, pocházejícím ze stejného IP zdroje. Je také možné sdružovat síťový provoz a záznamy o aktivitách, které proběhly v krátkém časovém úseku do jediné položky, což následně pomáhá při vyhledávání.

Schopnost detekovat provoz jednotlivých aplikací na 7. vrstvě OSI umožňuje poskytovat přesné analýzy a detailní pohledy na firemní síť. Po přidání integrovaného zařízení IBM Security QRadar QFlow či VFlow Collector může QRadar SIEM monitorovat napříč celou firemní sítí také využití aplikací jako jsou ERP systémy, databáze, sociální sítě, Skype či Voice over IP (VoIP). Tento monitoring zahrnuje detailní pohled na to, kdo a co používá, vyhledává souvislosti s dalšími aktivitami v síti a odhaluje nepřípustné přenosy dat a schémata nadměrného využívání sítě. I když se řešení dodává s řadou předpřipravených pravidel pro behaviorální analýzu a detekci anomálií, mohou bezpečnostní týmy vytvářet i svá vlastní pravidla.

Management prostřednictvím vysoce intuitivní jednotné konzole

QRadar SIEM poskytuje centralizované uživatelské rozhraní, nabízející přístup na základě uživatelských rolí a dle jednotlivých funkcí, i globální pohled umožňující analýzu dat v reálném čase, správu incidentů a reporting. K dispozici je pět základních řídicích panelů – panel bezpečnosti, síťové aktivity, aktivity aplikací, monitoringu systémů a dohledu nad plněním regulatorních požadavků. Uživatelé si však mohou vytvářet a upravovat také své vlastní panely.

Tyto panely usnadňují identifikaci anomálií, které mohou signalizovat začátek útoku. Kliknutí na graf spustí funkci hloubkové analýzy, která umožňuje rychle prověřit zvolené události či datové toky spojené s potenciálním útokem. Pro rychlejší přípravu reportů jsou zde navíc k dispozici stovky šablon spjatých se specifickými rolemi, zařízeními a regulatorními předpisy.



QRadar SIEM nabízí rozsáhlé funkce pro zajišťování digitálních stop skrytých za každým potenciálním útokem i pro odladění existujících pravidel či přidávání nových tak, aby mohlo dojít ke snížení počtu falešných poplachů.

Rozšíření ochrany před hrozbami do virtualizovaných prostředí

S ohledem na to, že virtualizované servery jsou stejně citlivé na bezpečnostní hrozby jako ty fyzické, musí komplexní řešení pro security intelligence zahrnovat také vhodné nástroje pro ochranu aplikací a dat umístěných ve virtualizovaných datových centrech. S využitím integrovaných zařízení QRadar VFlow Collector mohou pracovníci IT oddělení získat lepší přehled o firemních aplikacích, umístěných v jejich virtualizovaných prostředích a mohou také lépe vybrat aplikace vyžadující bezpečnostní monitoring. Operátoři mohou také zachytávat obsah jednotlivých aplikací pro jejich detailnější bezpečnostní analýzu.

Vytváření detailních reportů o aktivitě uživatelů a přístupu k datům potřebné pro naplnění regulatorních požadavků

QRadar SIEM nabízí transparentnost, dohledatelnost a měřitelnost, což jsou kritické faktory pro úspěch firmy v oblasti naplňování regulatorních předpisů i v oblasti reportingu plnění předepsaných směrnic. Toto řešení je schopné analyzovat a pospojovat data z monitorovaných systémů do kompletnějších reportů a poskytnout tak auditorům metriky v oblasti IT rizik. Nabízí také šablony pro stovky reportů a pravidel reflektující regulatorní předpisy pro jednotlivá odvětví.

Firmy mohou efektivně reagovat na požadavky na zabezpečení IT plynoucí z regulatorních požadavků. Stačí jim pouze prostřednictvím automatických updatů rozšířit QRadar SIEM o nové definice. Je možné seskupovat profily všech síťových prvků podle jejich aktuální funkce ve firmě – například lze do jedné skupiny zahrnout servery, které podléhají auditům dle Health Insurance Portability and Accountability Act (HIPAA) apod.

Přednastavené řídicí panely, šablony reportů a pravidel jsou navrženy dle následujících regulatorních opatření: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG a mnohých dalších.

Rozšíření o vysokou dostupnost a disaster recovery

Pro rozšíření o podporu vysoké dostupnosti a disaster recovery je možné spárovat identické systémy mezi sebou a tím docílit vysoké dostupnosti. Toto je dostupné pro všechny komponenty architektury QRadar SIEM.Pro firmy, které požadují odolné firemní aplikace, nabízejí řešení QRadar s vysokou dostupností integrovanou funkci automatického failoveru i plné synchronizace disků mezi HA systémy. Tato řešení lze snadno nasadit s využitím elegantních plug-and-play integrovaných zařízení, takže pro zajištění ochrany proti výpadkům není potřeba využívat žádné dodatečné produkty třetích stran.

Pro firmy, které hledají ochranu a obnovu dat, nabízí řešení QRadar disaster-recovery duplikace dat v reálném čase (např. datových toků a událostí) z primárního systému QRadar na sekundární paralelní systém umístěný v jiné lokalitě.

Analýza zranitelností

IBM Security QRadar Risk Manager rozšiřuje QRadar SIEM o identifikaci nejzranitelnějších prvků. V okamžiku, kdy jsou tyto prvky zapojeny do aktivity, která je potenciálně nebezpečná, dokáže ihned vygenerovat upozornění.

U firem, které například hledají ve svých sítích nezáplatované aplikace, zařízení a systémy, pak určí, které z nich se připojí k internetu, a zároveň nastaví priority odstraňování zranitelností na základě rizikových profilů každé z aplikací.

Pro více informací si, prosím, přečtěte produktový list QRadar Risk Manager.

Zachycení síťových událostí a datových toků s rozsáhlou podporou zařízení

QRadar SIEM podporuje více než 450 produktů od prakticky každého většího výrobce ze segmentu podnikových sítí. Nabízí sběr a analýzu dat i hledání vzájemných souvislostí napříč širokým spektrem systémů, včetně síťových řešení, bezpečnostních řešení, serverů, koncových stanic, operačních systémů a aplikací. Kromě toho lze QRadar SIEM snadno rozšířit o podporu proprietárních aplikací a nových systémů.

Proč IBM?

IBM představuje celosvětově největší firmu v oblasti výzkumu, vývoje a implementace bezpečnostních nástrojů. Řešení od IBM pomáhají firmám eliminovat jejich bezpečnostní zranitelnosti a více se zaměřit na skutečnou podstatu podnikání.

Pro více informací

Pro více informací o tom, jak IBM QRadar SIEM může vyřešit problémy Vaší firmy v oblasti správy hrozeb, kontaktujte svého obchodního zástupce společnosti IBM, partnera společnosti IBM anebo navštivte: **ibm.com**/security.

O bezpečnostních řešeních IBM

IBM Security nabízí jedno z nejpokročilejších a nejvíce integrovaných portfolií bezpečnostních produktů a služeb pro firmy. Toto portfolio, za kterým stojí celosvětově uznávaný výzkum a vývoj v rámci IBM X-Force®, poskytuje nástroje pro security intelligence, které pomáhají firmám komplexně ochránit jejich zaměstnance, infrastrukturu, data i aplikace. IBM Security nabízí řešení pro správu identit a přístupů, zabezpečení databází, vývoje aplikací, správu rizik, zabezpečení koncových stanic, bezpečnost sítí a mnoho dalšího. IBM představuje jednu z celosvětově největších výzkumných, vývojových a implementačních firem v oblasti bezpečnosti. Každý den monitoruje na 13 miliard událostí ve více než 130 zemích světa.

Kromě toho, IBM Global Financing Vám může pomoci získat nástroje, které Vaše firma potřebuje, a to tou nejstrategičtější a cenově nejefektivnější formou. Jsme připraveni Vám nabídnout individuální řešení pro financování IT, které bude vyhovovat Vašim obchodním cílům, umožní vám efektivní řízení cashflow a sníží celkové náklady. Financujte své kritické investice do IT a posuňte svůj business kupředu spolu s IBM Global Financing. Pro více informací navštivte **ibm.com**/financing.

IBM Corporation
Software Group
Route 100
Somer, NY 10589

Vytvořeno ve Spojených státech amerických, leden 2013

Domovskou stránku IBM můžete najít na: ibm.com