IBM Security QRadar Log Manager

Ochrana infrastruktury díky pokročilé správě logů v reálném čase

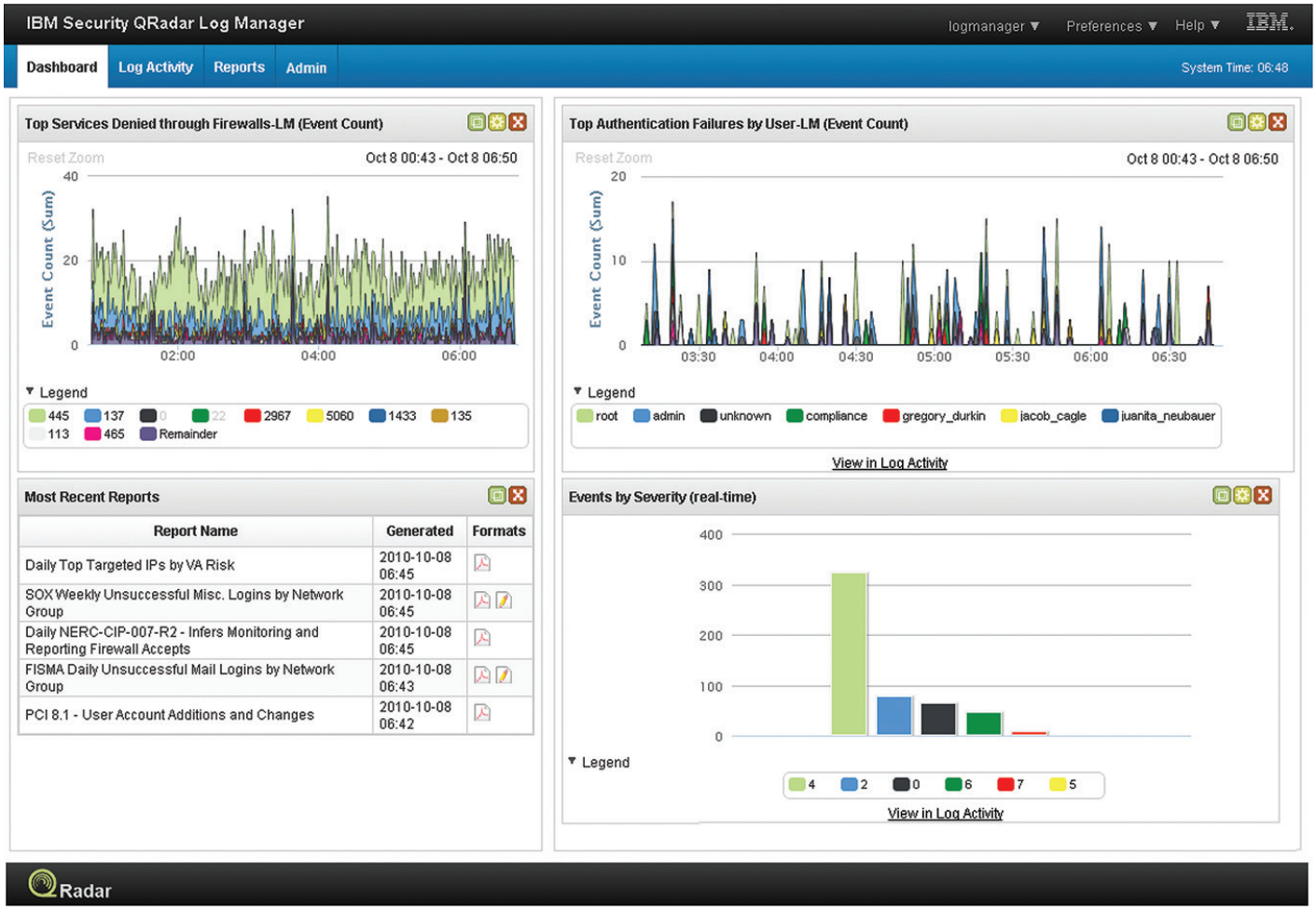
Shrnutí

- Agregace a korelace různorodých sad logů a událostí
- Zachycení událostí ze síťových bezpečnostních prvků, serverů, koncových bodů a aplikací s jednotným globálním pohledem
- Snadné provádění bezpečnostních analýz, řešení problémů s aplikacemi a sítí nad normalizovanými daty umožňující snazší vyhledávání
- Škálování od jednotek po stovky tisíc událostí za sekundu na jeden systém
- Kontrola dodržování regulatorních požadavků, včetně bohatých funkcí v oblasti reportingu
- Ochrana investic díky možnosti dodatečného rozšíření o technologii SIEM (Security Information and Event Management)

Firmy, které hledají nástroje pro sběr, analýzu, archivaci a bezpečné ukládání velkých objemů síťových a bezpečnostních logů událostí, potřebují vysoce výkonný, snadno použitelný a kompletní systém pro správu logů. To je obzvláště důležité v dnešním prostředí, kdy vzájemně propojené systémy generují a ukládají více informací než kdy dřív. IBM® Security QRadar® Log Manager analyzuje data z nejrůznějších sítí a bezpečnostních zařízení, serverů, operačních systémů a aplikací i široké škály koncových bodů, aby mohl poskytovat okamžitý přehled o vznikajících hrozbách.

Získejte nástroj pro analýzu logů

Většina firem dnes generuje velké množství logů, jejichž manuální analýza je náročná a může mít neúměrné požadavky na personální kapacity. Díky flexibilnímu nástroji pro tvorbu dotazů obsaženému v QRadar Log Manager jsou data z různorodých logů agregována a jsou dávána do souvislostí tak, aby bylo možné přijmout provozní opatření, provést zajištění digitálních stop a bylo možné identifikovat schémata útoků, vzniklých anomálií, podezřelých přístupů apod.



Uživatelsky přizpůsobitelný kontrolní panel aplikace QRadar Log Manager nabízí přístup založený na uživatelských rolích i celkový pohled v reálném čase.

Dostaňte se pod povrch a získejte nástroj pro efektivní analýzu událostí

Díky svému vysoce intuitivnímu centralizovanému uživatelskému rozhraní nabízí QRadar Log Manager stabilní základ pro síťové bezpečnostní týmy. V závislosti na typu požadovaných funkcí jsou dostupné standardní ovládací panely a uživatelé zároveň mohou vytvářet a upravovat své vlastní panely tak, aby mohli monitorovat specifické aktivity a dostat se hlouběji k časovým pohledům umožňujícím analyzovat dlouhodobé trendy.

Získejte zařízení pro zaznamenání všech síťových událostí

QRadar Log Manager sbírá data ze široké škály síťových a bezpečnostních zařízení, včetně směrovačů a přepínačů, firewallů, virtuálních privátních sítí (VPN), intrusion detection a prevention systémů (IPS/IDS), antivirových systémů, koncových stanic a serverů, databází, poštovních a webových aplikací, i zákaznických proprietárních aplikací.

Všechny události jsou agregovány s využitím rozhraní Device Support Module. To nabízí pokročilé dvoufázové třídění aplikované na příchozí události. Upravený nástroj pro aplikaci pravidel zpracovává každou příchozí událost v reálném čase a přiřadí jí atributy závažnosti, důvěryhodnosti a relevance. Následně spustí vhodnou reakci prostřednictvím e-mailové notifikace, upozornění na řídicím panelu anebo přidáním události do referenční sady podobných aktivit pro pozdější detailnější analýzu.

Pro rozšíření nasaďte škálovatelné integrované zařízení

Architektura integrovaného zařízení QRadar Log Manager nabízí nejrůznější konfigurace od spojení hardware a software v jednom zařízení až po vysoce výkonnou distribuovanou architekturu využívající centralizované konzole a libovolné množství distribuovaných integrovaných zařízení pro vlastní zpracování a sběr událostí. Řešení lze snadno škálovat tak, aby bylo schopno pokrýt stovky tisíc událostí za sekundu.

Jedno zařízení nabízí až 16 terabajtů úložiště pro ukládání logů a podporuje kontroly integrity logů využitím hash funkcí dle NIST Log Management Standard SHA-x (1-256), aby nedošlo k neoprávněné manipulaci s archivy logů. Distribuovaná architektura umožňuje rozšíření datového úložiště až na stovky terabajtů. Vestavěná účelově navržená databáze je pro zajištění snazšího provozu a nižších nákladů na provoz navržena jako bezúdržbová.

Pro zajištění specifických interních potřeb mohou administrátoři na základě velice detailní systémové politiky nastavit intervaly platnosti dat. Uživatelsky nastavitelné indexování událostí optimalizuje výkon a umožňuje vyhledávat dle libovolného uloženého údaje.

Nechte bezpečnost na jiných

QRadar Log Manager se svými více než 2 000 přednastavenými pravidly a reporty pomáhá firmám bezpečně naplnit požadavky na reporting a auditing v souladu s požadavky bezpečnostních standardů od Payment Card Industry (PCI), přes Health Insurance Portability and Accountability Act (HIPAA) až po Gramm-Leach-Bliley Act (GLBA) nebo Sorbanes Oxley Act (SOX). Automatické upozorňování pomáhá bezpečnostním týmům, aby věděly, co se děje, i když zrovna nejsou přítomny u systému.

Firmy využívají QRadar Log Manager k tomu, aby jim pomohl zvýšit povědomí o zabezpečení infrastruktury a odhalit podezřelé události, které již zapadly v „šumu“ dalších síťových aktivit. QRadar Log Manager, coby součást IBM QRadar Security Intelligence Platform, nabízí možnost plynulého přechodu od běžné správy logů až k plné implementaci technologie SIEM, a to pouhým licenčním upgradem.

Vybudujte bezpečnostní řešení s vysokou dostupností

Rozšíření QRadar o funkce pro zajištění vysoké dostupnosti přináší firmám možnost využít výhod automatického failoveru a plné synchronizace úložišť mezi systémy – tj. funkcí typicky dostupných jen u drahých a dedikovaných úložištích.

Integrovaná zařízení QRadar pro disaster recovery využívají zrcadlení dat na sekundární identické zařízení QRadar a poskytují tak ochranu proti nečekaným událostem.

Proč IBM?

IBM je celosvětově jednou z nejaktivnějších firem v oblasti výzkumu, vývoje a implementací řešení v oblasti bezpečnosti. Aktivity IBM v této oblasti se sestávají z 10 bezpečnostních provozních center, devíti výzkumných zařízení IBM Research, 11 vývojových laboratoří na oblast softwarové bezpečnosti a Institutu pokročilé bezpečnosti s pracovišti v USA, Evropě a oblasti Asie a Pacifiku. Řešení společnosti IBM umožňují firmám omezit jejich bezpečnostní zranitelnosti a zaměřit se na dosažení úspěchu při realizaci jejich strategických iniciativ. Produkty IBM čerpají z odborných znalostí v oblasti bezpečnostní analýzy a ze zkušeností výzkumného a vývojového týmu IBM X-Force® a umožňují tak uplatňovat různá preventivní opatření. Společnost IBM, coby důvěryhodný partner v oblasti bezpečnosti, nabízí řešení, která dokáží ochránit kompletní podnikovou infrastrukturu, včetně cloudu, a to i před těmi nejnovějšími bezpečnostními riziky.

Pro více informací

Pro více informací o IBM Security QRadar Log Manager kontaktujte svého obchodního zástupce společnosti IBM, partnera společnosti IBM anebo navštivte: **ibm.com**/security.

IBM Corporation
Software Group
Route 100
Somer, NY 10589

Vytvořeno ve Spojených státech amerických, leden 2013

Domovskou stránku IBM můžete najít na: ibm.com