NetIQ Sentinel

Výkonná a jednoduchá správa zabezpečení

Úvod

Organizace výrazným způsobem transformují své infrastruktury IT a mění způsob jejich používání. Tyto změny však přinášejí řadu problémů a výzev, které mohou negativně ovlivnit schopnost organizace zabezpečit podnikové prostředí.

Například technologie jako virtualizace, cloud computing a mobilita změnily způsob, jakým společnosti fungují. Tyto technologie umožňují uživatelům pracovat s informacemi a komunikovat mezi sebou novým a moderním způsobem. Umožnily však také vznik distribuovaných a propojených podniků, u nichž je pro analytiky informační bezpečnosti stále náročnější efektivně monitorovat a udržovat bezpečnost.

Aby mohly organizace zvýšit celkovou bezpečnost a činit informovanější rozhodnutí, potřebují okamžité informace o bezpečnostních událostech a jejich rychlou analýzu. Musí být schopny vypořádat se se složitostí správy velkých objemů dat zabezpečení, poradit si se so stikovanými hrozbami a vynucovat neustálý soulad s pravidly. Potřebují zkrátka řešení, jež jim v záplavě dat událostí umožní rychle a přesně určit kritické události a porušení bezpečnosti.

Přehled produktu

NetIQ Sentinel nabízí společnostem okamžitý přehled o veškerých IT aktivitách, díky čemuž mohou eliminovat bezpečnostní hrozby, zdokonalit zabezpečení a automatizaci vynucování bezpečnostních pravidel v rámci fyzických, virtuálních i cloudových prostředí.

Zjednodušuje tradiční správu bezpečnostních informací a událostí (SIEM) a řeší potíže při zavádění systému SIEM tak, aby mohly monitoring využívat všechny organizace. NetIQ Sentinel společnostem nabízí také efektivnější řešení SIEM, a to díky přístupu k okamžitým informacím, detekci odchylek a monitorování aktivity uživatelů. Poskytuje totiž mechanismy včasného varování a přesnější vyhodnocování IT aktivit.

Řešení NetIQ Sentinel přináší na trh jediný systém plně integrovaný se správou identit, která umožňuje spojit uživatele s konkrétními aktivitami ve všech prostředích.
Díky tomu mohou společnosti snadno identi kovat kritická rizika, výrazně zkrátit reakční dobu a rychle řešit hrozby a narušení zabezpečení, dříve než ovlivní chod podniku. Řešení Sentinel díky okamžitým informacím umožňuje společnostem chránit se před vznikem pokročilých hrozeb, zdokonalit procesy zabezpečení a nepřetržitě vynucovat nastavená pravidla.

Možnosti a funkce

• **Zjišťování rizik** – Odhalit události, které vyžadují prošetření, protože by mohly způsobit skutečné nebo potenciální problémy, je často složité. Řešení NetIQ Sentinel však nabízí zjišťování rizik a automatickou identifikaci nesrovnalostí v prostředí vaší společnosti bez vytváření pravidel korelace, u nichž je nutné vědět přesně, co hledáte. Při implementaci řešení Sentinel nastavíte základní úrovně bezpečnosti pro specifické prostředí vaší společnosti, takže okamžitě získáte lepší informace a budete moci rychleji odhalovat neobvyklé aktivity. Porovnávání trendu se základní úrovní umožňuje srovnávat historické vzorce aktivity a následně rychleji vyvíjet modely obvyklých IT aktivit (neboli běžných stavů), díky nimž je snadné zaznamenat nové, potenciálně škodlivé trendy. Chcete-li tyto možnosti rozšířit, můžete základní úrovně svého prostředí a korespondující detekci neobvyklých událostí dále upravit. Řešení NetIQ Sentinel vám navíc ukáže změnu stavu zabezpečení a souladu s pravidly v závislosti na čase.

• **Flexibilní možnosti nasazení** – Řešení NetIQ Sentinel je dodáváno jako softwarová appliance prostřednictvím obrazu ISO (International Organization for Standardization) pro všechny populární hypervizory, například VMware, HyperV a XEN, a jako instalovatelný software pro systémy SUSE® Linux Enterprise Server a Red Hat Enterprise Server. Modely nasazení a licencování řešení NetIQ Sentinel jsou neuvěřitelně flexibilní a umožňují nasadit systém SIEM a správu protokolů v rámci celého podniku podle jeho specifických potřeb. Řešení Sentinel využívá mechanismu flexibilního vyhledávání a předávání událostí, což dovoluje přizpůsobit nasazení produktu vašemu prostředí., a to i v případě vysoce distribuovaného systému.

• **Vysoce výkonná architektura úložišť** – Řešení NetIQ Sentinel využívá úspornou vrstvu k ukládání událostí do souborů pro dlouhodobou archivaci. Úložiště událostí zajišťuje komprimaci 10 : 1 s plnou podporou vyhledávání pomocí indexů. Řešení NetIQ Sentinel vám také nabídne možnost synchronizovat nebo přesunout některá či všechna data o událostech společnosti do tradiční relační databáze. Vylepšené vyhledávání omezuje dobu nutnou k vyhledání dat a vygenerování sestav. Díky architektuře úložiště Sentinel již nebudete potřebovat licencovanou databázi třetí strany. Vaše celkové výdaje na vlastnictví se tedy sníží.

• **Grafická tvorba pravidel** – Řešení NetIQ Sentinel umožňuje rychle vytvářet pravidla korelace událostí přímo z událostí, které shromáždí ve vašem prostředí. Výhodou také je, že správci nemusí absolvovat náročná školení nebo se učit speciální skriptovací jazyk. Pravidla navíc můžete testovat před jejich nasazením, abyste omezili falešné pozitivní výstrahy, zdokonalili korelaci událostí a celkově zlepšili detekci zneužití. Díky tomu lze výrazně urychlit návratnost vašich investic a snížit celkové náklady na vlastnictví.

Novell-Praha, s.r.o.
Novodvorská 1062/12
142 00 Praha 4

tel.: +420 220 410 540
fax: +420 220 410 549

www.microfocus.com
www.netiq.cz
NCCC@novell.cz

• **Obohacení identit** – Díky unikátní integraci s produktem NetIQ Identity Manager nabízí řešení NetIQ Sentinel na trhu jedinečnou a bezešvou integraci správy identit, která spojuje uživatele s konkrétními aktivitami v rámci celého podniku. Obohacení dat zabezpečení o unikátní informace o identitách uživatelů a správců poskytuje výrazně lepší přehled o tom, kdo, kdy a kde k systému přistupuje. Zahrnutím identit do dat pro řešení událostí NetIQ Sentinel navíc inteligentně chrání vůči vnitřním hrozbám a nabízí lepší mechanismy zjednání nápravy. Řešení NetIQ Sentinel zahrnuje také integraci identit se službou Microsoft Active Directory a již brzy bude zahrnovat také integraci s dalšími produkty pro správu identit.

• Zjednodušené filtrování, vyhledávání a hlášení – Řešení NetIQ Sentinel zjednodušuje shromažďování událostí v IT infrastruktuře, čímž umožňuje automatizaci náročných funkcí zajišťování shody s předpisy, auditu a hlášení, a výrazně redukuje složitost a časovou i finanční náročnost vyhledávání a přípravy dat, která auditoři požadují. Díky tomu mohou společnosti rychle vyhovět vládním nařízením a průmyslovým standardům.

• **Zdokonalené a rozšířené balíčky sestav** – Řešení NetIQ Sentinel zjednodušuje hlášení prostřednictvím možností agregace a normalizace dat, předpřipravených sestav a přizpůsobitelných zásad a možností rychlého vyhledávání. Pouhým stisknutím jednoho tlačítka můžete generovat sestavy pro okamžité výsledky vyhledávání, takže můžete neprodleně vytvářet potřebné sestavy dat bez nutnosti otravného upravování pevně přednastavené šablony.

• **Jedno sjednocené řešení** – Řešení NetIQ Sentinel kombinuje správu protokolů se systémem SIEM do jednotného celku.

Klíčové diferenciátory

Na rozdíl od taktických řešení SIEM, která jsou jednoduchá, ale nejsou určena ke skutečnému monitoringu bezpečnosti, a tradičních řešení SIEM, jež jsou výkonná, ale vyžadují vysokou úroveň dovedností a hůře se přizpůsobují měnícímu se prostředí, nabízí řešení NetIQ Sentinel 7 maximální hodnotu v oblasti informací o zabezpečení. Nabízí totiž vše, co potřebujete k zajištění dostatečné úrovně zabezpečení, tedy jednoduchost a výkon.

• Forma virtuálního appliance umožňuje rychlé a snadné nasazení. Ve srovnání s hardwarovými řešeními je virtuální appliance flexibilnější v případě růstu a zvyšování kapacity.

• Obohacení identit poskytuje široký kontext pro bezpečnostní události, a tedy větší přehled o zjišťování a předcházení vnitřních hrozeb.

• Zjednodušená správa nabízí grafická rozhraní pro tvorbu pravidel a plánování kapacity. Správci mohou během implementace rychle vytvářet pravidla korelace a snadno je udržovat a aktualizovat při měnících se potřebách podniku, což umožňuje snížit celkové náklady na vlastnictví.

• Ovládací panely s informacemi o zabezpečení umožňují monitorovat zabezpečení společnosti téměř okamžitě po instalaci produktu.

• Intuitivní vyhledávání dat umožňuje bezpečnostním správcům zabezpečení nalézt potřebná data a z výsledků vyhledávání rychle vytvořit sestavu..