IBM Security
QRadar SIEM

IBM Security QRadar je otevřená platforma pro sběr a vyhodnocování bezpečnostních událostí. Řešení umožňuje bezpečnostním analytikům efektivně reagovat na již proběhlé bezpečnostní incidenty, a 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, reporting a analýzy chování pro sítě a aplikace nebo uživatele.

Řešení QRadar disponuje podporou normalizace několika stovek zařízení napříč nejrůznějšími dodavateli.

Inteligentní koncentrace informací o událostech z logů a síťových toků z tisíců zařízení umístěných v celé síti

Velké množství předpřipravených korelačních pravidel, reportů, dashboardů a široká podpora zdrojů logů

Behaviorální analýza uživatelů a síťová behaviorální analýza, korelace historických dat pro odhalování nekalých činností

Vysoká rozšiřitelnost pomocí stovek dostupných aplikací

Vysoce škálovatelné řešení jak pro menší, tak i velké organizace

IBM

Behaviorální analýza uživatelů – QRadar User Behavior Analytics

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 UBA je příklad aplikace, která je zdarma dostupná na portálu **IBM Security App Exchange**

Řízení zranitelností a rizik – QRadar Vulnerability & Risk 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.

QRadar Risk Manager 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 například firewally, routery, switche nebo IPS.

Podrobná analýza obsahu – QRadar Network Insights

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

Zapojení umělé inteligence – QRadar Advisor with Watson

Systém QRadar umožňuje rozšíření o pomocníka pro vyšetřování incidentů ve formě umělé inteligence. QRadar Advisor with Watson umožňuje bezpečnostním analytikům provádět konzistentní vyšetřování a urychluje eskalaci incidentů, což má za následek zkrácení doby prodlevy a zvýšení efektivity bezpečnostního týmu.

QRadar Advisor with Watson může rozšířit pohled na incident prozkoumáním lokálních informací o bezpečnostních hrozbách spolu s externími. Díky tomu analytik dosáhne lepšího pochopení incidentu a je si i více jistý rozhodnutím, zda se jedná o skutečný incident.