RAPID7 nexpose® metasploit®

Vulnerability management a penetrační testování

FORRESTER WAVE™ Leader Q1 2018

Analytické řešení a zabezpečení dat, ***Rapid7 Nexpose,*** *sbírá a dává (v reálném čase) do souvislostí, rozsáhlé množství korelovaných dat a poskytuje tak podrobný přehled o zranitelnostech. Na rozdíl od tradičních skenů zranitelností nebo správy incidentů, se Rapid7 Nexpose dívá na síť optikou útočníka a donutí Vás rychleji zasáhnout proti zranitelnostem, které jsou opravdovým rizikem, ne jen teoretickou hrozbou. Rapid7 Nexpose dokáže velmi úzce spolupracovat s nástrojem pro penetrační testování - Rapid7 Metasploit, a pomocí něj dokáže skutečně ověřit, zda je bezpečnostní hrozba zažehnána či je stále aktuální.*

Rapid7 Nexpose je řešení pro správu hrozeb, které dynamicky **sbírá data a analyzuje rizika pro detekci zranitelností**, přičemž hlavní funkcí je provádění auditů a monitorování operačních systémů, serverů, síťových prvků, databází a webové aplikace na známé či neznámé hrozby. Nexpose je navržen tak, aby bezpečnostní týmy mohly jednoduše identifikovat, vyhodnotit a reagovat na kritické a nenadálé bezpečnostní hrozby. Nexpose jako klíčová komponenta platformy Rapid7 pro ochranu a analýzy dat představuje aktivní a analytický přístup k počítačové bezpečnosti.

Nexpose Remediation Workflow přináší konverzi velkého množství dat do srozumitelné podoby pro uživatele a upřednostňuje akce, které mají vysokou bezpečnostní prioritu (určenou na základě pravděpodobnosti použití v útoku, citlivosti dat, stupně důležitosti apod.). Administrátoři tak mohou efektivněji spravovat nalezená bezpečnostní rizika v operačních systémech, softwarech třetích stran, webových aplikacích, prohlížečích a databázích. Za pomocí Nexpose získáváme real-time data pro posouzení bezpečnostního rizika. Reálná data se získávají buď pomocí agentů, nebo bez agenta. Nexpose automaticky vyhodnotí změny a snižuje tím tak čas potřebný k nápravě

Unikátní kombinace Rapid7 Metasploit, RealRisk score a kontextové business inteligence dělá z Nexpose jednotné řešení pro správu rizik a umožní organizacím **být v souladu s bezpečnostními předpisy** a audity pro Risk Management, Vulnerability a Configuration Management, jako jsou ISO 27002, PCI DSS, SNS, HIPAA, HITECH, FISMA (USGCB/FDCI a včetně SCAP shody), Sarbanes-Oxley (SOX), Top 20 CSC a NERC CIP.

Vysoká škálovatelnost

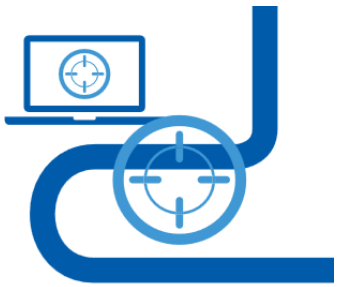
Rapid7 Nexpose nabízí distribuovanou architekturu a pokročilé vyhledávací funkce (včetně integrace VMware a DHCP), které usnadňují správu zranitelností (nezáleží na tom, zda spravujete tisíc nebo milion IP adres každý den). Pomocí Nexpose Adaptive Security se přizpůsobí povaze Vašeho prostředí a umožní automatickou detekci a skenování nových zařízení, jakmile se připojí k síti a dokáže určit, která zařízení mají kritické zranitelnosti.

Silné stránky Rapid7 Nexpose:

- **Pravidelné hodnocení sítě –** pravidelné audity zaměřené na specifické oblasti infrastruktury.
- **Cílené skenování a reportování** – skenování a reportování zaměřené na určité oblasti (interní a externí síť, webové aplikace, databáze atd.)
- **Bezpečnostní kontroly** – poskytuje přehled o výsledku a stavu kontrol.
- **ScoreCard** – sledování úspěšnosti bezpečnosti pomocí metricky řízené ScoreCard.
- **Analýza zranitelnosti** – pomáhá stanovit priority a přijmout rozhodnutí na základě prioritního plánu, kategorizace dat a ověřování zranitelností v aktuálním softwaru.
- **Automatizovaný ticketing** – při zjištění hrozby automaticky vytvoří ticket a po jeho vyřešení jej zruší.
- **Holistický pohled** - Poskytuje podrobné informace o nainstalovaných aplikacích na koncových zařízeních.
- **Asset Management** – pomáhá odhalit kdo a co vlastní, dále určí, která aktiva jsou pro společnost více či méně důležitá a automaticky zvýší/sníží risk score.

Snadná integrace

Nexpose může být velmi užitečným a bohatým zdrojem dat při kombinaci se SIEM a Firewally. Pomocí otevřeného API se Nexpose dokáže snadno integrovat se s více než 50 bezpečnostními technologiemi (LogRhythm, ManageEngine, McAfee Nitro Security, Amazon Web Services, ArcSight, Cisco, FireEye, Google Apps, Microsoft, Office 365, VMware a další). Integrace s Metasploit, nejpoužívanějším Frameworkem na penetrační testování na světě, poskytuje real-time detekci, které zranitelnosti systémů jsou aktuální, a u kterých se pracuje na jejich odstranění.



Nexpose Live dashboard

Nexpose nabízí live dynamický dashboard, který využívá **real-time data z Threat Exposure Analytics** nástroje a dokáže transformovat tato data do podrobných vizualizací tak, že umožnuje soustředit potřebné zdroje na důležité akce a okamžitě je sdílet s bezpečnostními týmy.

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

Analýza zranitelností

Dvě zranitelnosti nemusí být stejně závažné, záleží na mnoha aspektech. Porozumění, které zranitelnosti jsou závažnější, vyžaduje holistický přístup ke kritickým datům. Nexpose se automaticky ptá na relevantní požadavky a výsledek těchto dotazů pomůže stanovit priority, na co se zaměřit, jakou akci provést jako první a jaký bude bezpečnostní dopad. Nexpose je jediným Vulnerability Assessment nástrojem, který využívá expozice, dostupnost malware a pohlíží na zranitelnosti očima útočníka.

InsightVM

Rapid7 nabízí rozšířenou platformu pro holistické řízení analýzy zranitelností. Tato unikátní cloud-based platforma v sobě sdružuje výsledky výzkumu zranitelností z Nexpose, podrobnou znalost exploitů z Metasploit, datový kontext získaný z monitoringu koncových stanic, analýzu odhalených útoků a real-time reporting, tzv. Liveboards. InsightVM je designována tak, aby co nejefektivněji získávala informace o zranitelnostech systémů a minimalizovala riziko s nimi spojené, skenovací engine tak nadále zůstávají umístěny v segmentech sítě zákazníka dle potřeby a v neomezeném počtu. InsightVM využívá proaktivní přístup, který automaticky reaguje a vyhodnocuje každou změnu v monitorovaných systémech. Rapid7 Insight Agent poskytuje administrátorům viditelnost do koncových stanic a zároveň prioritizuje problémy, které se v systémech generují.

Tabulka: Rapid7 Vulnerability Management varianty

	Nexpose	InsightVM
Max. počet IP (asset)	Dle licence	Dle licence
Počet Administrátorů	Neomezeno	Neomezeno
Scanovací enginy	Neomezeno	Neomezeno
Automatický update	Ano	Ano
Vulnerability scan	Ano	Ano
Exception management	Ano	Ano
Scan scheduling & alerting	Ano	Ano
RealContext classification	Ano	Ano
Web Application Scan	Ano	Ano
PCI compliance	Ano	Ano
Open API and third party integration	Ano	Ano
Virtual scanning (Vmware NSX)	Ano	Ano
Dynamic Discovery scanning	Ano	Ano
Policy manager	Ano	Ano
Dynamic LiveDashboard vizualizace	Ne	**Ano**
Distributed scanning	Ano	Ano
Endpoint Agents	Ne	**Ano**
Live data querying	Ne	**Ano**
Scan IP adres třetích stran	Ano	Ano
Adaptive Security with automated actions	Ano	Ano
User role customization	Ano	Ano
MS Azure / AWS support	Ano	Ano
Remediation Projects / Live assignment of remediation duties	Ne	**Ano**
Licenční model	Subscripce	Subscripce

Rapid7 Metasploit - podrobte Vaši bezpečnost penetračním testům!

Rapid7 vyvinul řešení pro penetrační testování, **Metasploit**, které pomáhá zvýšit produktivitu penetračních testerů, ověřuje zranitelnosti, odhaluje phishingové hrozby a pomáhá zvyšovat bezpečnost odstraněním slabých míst v infrastruktuře. Simuluje reálné útoky s cílem najít slabá místa dřív než škodlivý kód/útočník. Nabízí i možnosti jako jsou Smart Exploitation, Password Auditing, Vulnerability Verification, Web Application Scanning a Social Engineering. Nalezení slabé stránky je ovšem jen polovina bitvy. Cílem penetračního testu je provést důkladné posouzení závažnosti a navrhnout protiopatření, aby se riziko snížilo. Metasploit open-source Framework umožňuje přístup k expliotačním a průzkumným modulům pro urychlení testování zranitelností. Využívá technik jak se vyhnout anti-virům a najít slabé místo v síti. Metasploit se opírá o rozsáhlou komunitu a nabízí největší exploit databázi na světě (průměrně přibude jeden exploit denně), v současné době obsahuje více než 1300 exploitů a více než 2000 modulů

AppSpider - skenování webových, cloudových i mobilních aplikací

Rapid7 AppSpider dynamicky skenuje veškeré využívané aplikace (webové, mobilní či v cloudu) a testuje tyto aplikace na zranitelnosti napříč všemi možnými technologiemi. AppSpider provádí nepřetržité monitorování sítě a identifikuje změny v celém spektru využívaných aplikací a identifikuje jejich zranitelnosti. Díky rychlé analýze dat umožní vytvářet interaktivní reporty, které se chovají jako webové stránky. Dále nabízí možnost automatického patchování aplikací či nabízí možnost shody s předpisy (PCI, FISMA, SOX, HIPAA, GLBA, OWASP a další).

Rapid7 InsightIDR – získejte vhled do svých systémů a vytvořte si vlastní HoneyPots

Incident Detection and Response Tool od společnosti Rapid7 v sobě kombinuje funkcionality nástrojů jako SIEM, User Behavioral Analytics a Endpoint Detection and Response. Celé řešení je dostupné jako cloudová platforma a přináší vhled do monitoringu koncových zařízení, logů ale i cloudových služeb. InsightIDR efektivně zpracovává data získaná z koncových stanic do smysluplného kontextu, a to bez narušení uživatelské aktivity. Dokáže spolehlivě vystopovat zneužití lokálních účtů, nebezpečné procesy nebo manipulaci s logy. Využívá technologii machine-learning, díky čemuž se celé řešení průběžně vyvíjí společně s proměnným chováním útočníků. Cloudová bezpečnostní platforma InsightIDR licencována *per asset* a má velmi jednoduché nasazení, čímž se stává dostupnou také pro malé a střední podniky.