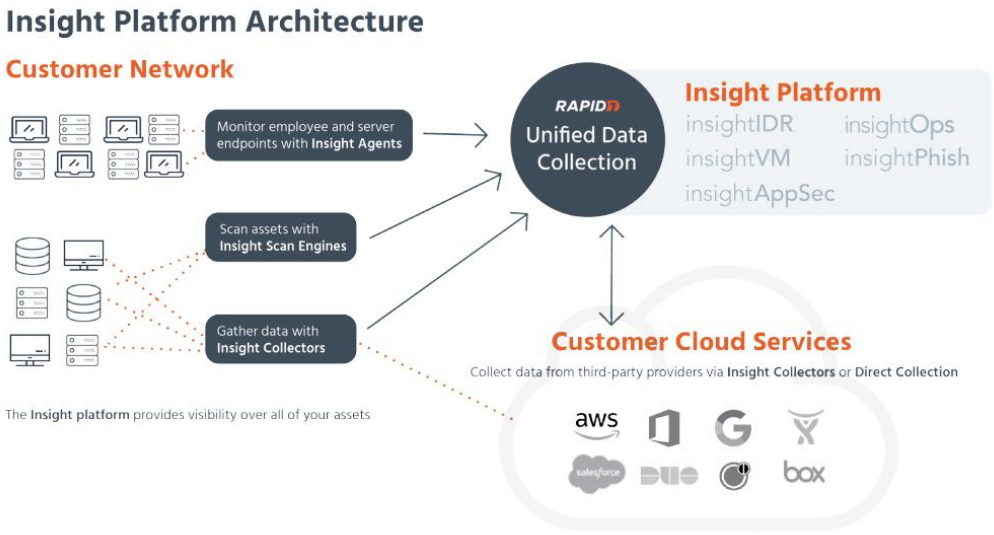
COMGUARD

RAPID7 insightVM

Rapid7 Vulnerability Management

Zneužití známé zranitelnosti je pro útočníka nejjednodušší cesta, jak proniknout do dané společnosti. S kvalitním vulnerability managementem by firmy dokázaly bezpečnostnímu incidentu plně předejít. Vulnerability Management od Rapid7 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 dívá na síť optikou útočníka a donutí společnost rychleji zasáhnout proti zranitelnostem, které jsou opravdovým rizikem, nejen teoretickou hrozbou.

Celé portfolio Rapid7 je spojeno do unikátní centralizované bezpečnostní platformy **Insight Platform**. Spojuje celé portfolio produktů – Xtended Detection and Response (XDR), SIEM, Threat Intelligence, ochrana cloudových aplikací a management zranitelností, včetně webových a mobilních aplikací. Insight Platform sbírá data z celého IT ekosystému a umožňuje bezpečnosntím IT týmům efektivně spolupracovat při analýze sdílených dat. Produkty z řady Insight využívají jednotného agenta a kolektory a díky tomu je škálování celého řešení velmi snadné.



Rapid7 InsightVM

Rapid7 InsightVM vyhledává zranitelnosti v prostředí společnosti a pomáhá určit jejich prioritu díky tzv. Real Risk Score. Na základě pravděpodobnosti jejich zneužití navrhne optimální harmonogram aplikace záplat. Dokáže velmi úzce spolupracovat s nástrojem pro penetrační testování – Metasploit, který uchovává podrobnou znalost exploitů a pomocí něj dokáže ověřit, zda je hrozba stále aktuální. InsightVM poskytuje live management zranitelností, stejně jako analýzu koncových bodů za účelem sledování hrozeb v reálném čase. Poskytuje také ucelené a přehledné reporty, které mohou sloužit pro management organizace.

Real Risk Score

Real Risk Score je vlastní metodika od Rapid7, která posuzuje rizika podle teoretických hrozeb CVSS a existence reálné hrozby, např. zda již existuje exploit nebo nikoliv. Výsledkem této metriky je výrazné snížení počtu zranitelností k řešení.

Skenování

Rapid7 InsightVM usnadňuje správu zranitelností bez ohledu na to, zda spravujete tisíc nebo milion IP adres každý den. Díky skenování pomocí DHCP umožní skenování zařízení, jakmile se připojí k síti. Skenování automaticky proběhne na základě nových hrozeb s vysokou závažností. Před samotným skenováním je možné si specifikovat kritické stroje v infrastruktuře.

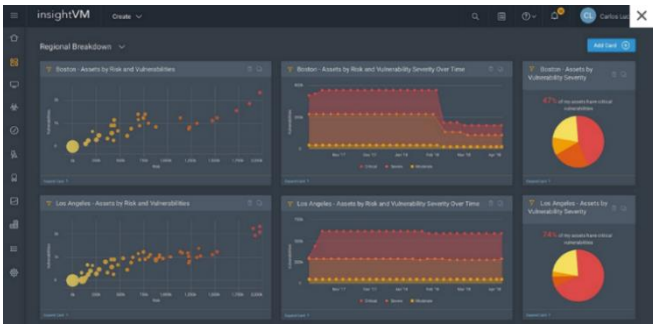
COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

COMGUARD

RAPID7

Integrace

InsightVM je velmi užitečným a bohatým zdrojem dat při kombinaci se SIEM a Firewally. Pomocí otevřeného API se dokáže snadno integrovat 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.



Klíčové vlastnosti Rapid7 InsightVM

- **Real Risk Score** – prioritizace nalezených zranitelností
- **Asset Management** – informace o nejzranitelnějších strojích
- **Remediation planning** – souhrn jednoduchých kroků, které pomohou při nápravě
- **Cílené skenování a reportování** – skenování a reportování zaměřené na určité oblasti (interní a externí síť, webové aplikace, databáze atd.)
- **Dívá se na síť z pohledu útočníka** a donutí vás zasáhnout proti hrozbě, která je opravdovým rizikem, a ne pouze teoretickou hrozbou
- **Lehký agent** pro koncové body
- **Pravidelné hodnocení sítě** – pravidelné audity zaměřené na specifické oblasti infrastruktury
- **Holistický pohled** – Poskytuje podrobné informace o nainstalovaných aplikacích na koncových zařízeních.
- Lze pořídit jak ve verzi **on-premise**, tak i pro **cloud**

	InsightVM	Nexpose
Počet administrátorů	Neomezeno	Neomezeno
Počet scanovacích enginů	Neomezeno	Neomezeno
Automatic vulnerability updates and Microsoft Patch Tuesday vulnerability updates	✓	✓
Scan scheduling and alerting	✓	✓
Basic web application scanning	✓	✓
Policy assessment (PCI, CIS, DISA, and more)	✓	✓
Advanced report and scan customization	✓	✓
RESTful API, OpenAPI, and third-party integrations	✓	✓
Dynamic discovery scanning (VMware, Mobile)	✓	✓
Dynamic, live dashboards with 50+ cards	✓	X
Endpoint agents	✓	X
Live data querying	✓	X
AWS and Microsoft Azure Support	✓	✓
Dynamic asset groups and tagging	✓	✓
Real Risk Score	✓	✓
Report templates and uploading	✓	✓
Integrated vulnerability validation with Metasploit	✓	✓
Custom tags and system criticality tags	✓	✓
Access to public and proprietary threat feeds	✓	X
Remediate		
Executive and remediation reporting	✓	✓
User role customization	✓	✓
Remediation Projects	✓	X
Automation-Assisted Patching	✓	X
Ticketing integrations (API)	✓	✓
Deployment options		
Software installation	✓	✓
Virtual appliance	✓	✓
Physical appliance	✓	✓
Private cloud	✓	✓
Managed Service	✓	✓

Tabulka: Srovnání verze InsightVM a Nexpose

Vulnerability management lze pořídit ve verzi onpremise, která je pod názvem Nexpose. A hybridní verzi InsightVM, kdy samotné nasazení agentů a skenovacího engine je on premise a live management zranitelností je napojen do cloudu.

Unikátní kombinace Rapid7 Metasploit a Real Risk Score dělá z vulnerability managementu 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.

insightAppSec **Rapid7 InsightAppSec** je cloud-based řešení zabezpečující dynamic application security testing (DAST). Skenuje jak jednoduché, tak komplexní, interní i externí webové aplikace s cílem otestovat jejich rizikovost a poskytnout informace potřebné k případné rychlejší nápravě. Identifikuje XSS, CSRF, SQL injections a mnoho dalších zranitelností z Rapid7 knihovny, která obsahuje více než 90 typů útoků. Generuje interaktivní HTML reporty prostřednictvím Attack Replay a sdílí je s vašim vývojovým týmem a zainteresovanými stranami. DAST řešení je možné také pořídit v on-prem verzi – AppSpider Enterprise/Pro.

COMGUARD
communication security

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