RAPID7

insightIDR insightVM
insightConnect insightOps insightAppSec

Rapid7 Insight – Centralizovaná Bezpečnostní Platforma

Nedostatečný vhled do spravovaných systémů, nesourodost bezpečnostních technologií a chybějící nástroje pro efektivní reakci na bezpečnostní incidenty. Tyto problémy se dají označit jako moderní výzvy, kterým čelí bezpečnostní a IT týmy. Bezpečnostní cloudová platforma ***Rapid7 Insight*** *byla vyvinuta jako odpověď na problémy IT a bezpečnostních týmů moderní doby. Jedná se o intuitivní řešení, díky kterému mají Bezpečnostní, IT a vývojové týmy nyní přístup jedním kliknutím ke správě zranitelností, zabezpečení cloudových aplikací, detekci a reakci na události, automatizaci a další.*

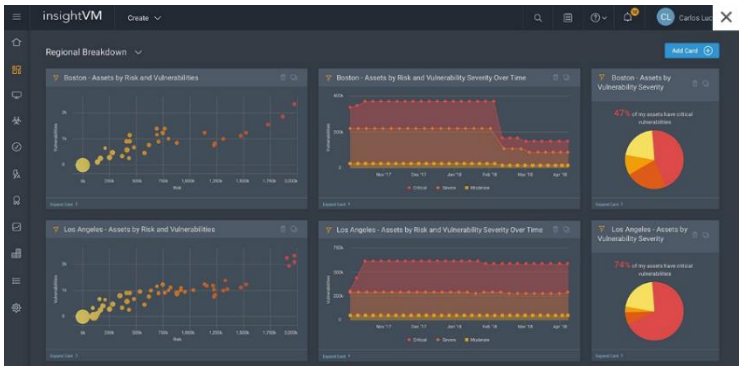
Rapid7 Insight je centralizovaná bezpečnostní platforma pro technologie*:*

SIEM | Vulnerability management | Incident response | Application Security | Security Automation
Event & Log Management | IT Monitoring | Security Orchestration

Insight Platform je unikátní centralizovaná bezpečnostní platforma, která spojuje celé portfolio produktů z oblasti IT Security, IT Operations, Automation, Vulnerability Management a SIEM. Insight Platform sbírá data z celého korporátního IT ekosystému a umožnuje bezpečnostním, IT a DevOps týmům efektivně spolupracovat při analýze sdílených dat. Produkty z řady Insight využívají jednotné kolektory, díky tomu a cloudové architektuře, je škálování celého řešení velmi snadné. Insight platformu lze velmi efektivně a jednoduše integrovat s většinou konvenčních řešení, a proto funguje jako násobitel síly pro již nasazené technologie – zajišťuje rychlou analýzu dat, efektivní prioritizaci eventů a poskytuje vhodná nápravná opatření pro bezpečnostní incidenty.

---

insightVM InsightVM poskytuje live management zranitelností, stejně jako analýzu koncových bodů za účelem sledování hrozeb v reálném čase. Hlavní úlohou InsightVM je najít zranitelnosti, informace z nich efektivně spravovat, a tak šetřit čas bezpečnostním týmům. InsightVM dokáže nasbírat informace o zranitelnostech a exportovat je do jiných nástrojů v rámci Insight Platform, čímž zvyšuje bezpečnostní inteligenci celého prostředí.



- **Kontinuální sledování koncových stanic pomocí nástroje Insight Agent**: Rapid7 Insight Agent automaticky sbírá data ze všech koncových bodů IT infrastruktury, a to i od zaměstnanců mimo firemní síť a také včetně citlivých zařízení, která nemohou být aktivně skenována, nebo která se zřídka připojují k podnikové síti. Spojením InsightVM s InsightIDR získáte úplný přehled o rizicích, které mohou představovat zařízení vaší IT infrastruktury a jejich uživatelé.
- **Liveboards, žádné Static Dashboards**: Zpracovávají čerstvá data o zranitelnostech, InsightVM Liveboards jsou neustále aktuální a interaktivní. Můžete snadno vytvářet vlastní přizpůsobitelné karty a úplné dashboardy pro každého – od systémových administrátorů po CISO, stejně jako dotazovat každou kartu pomocí běžných termínu pro sledování průběhu vašeho bezpečnostního programu.
- **Cloud, Virtual a Container Assessment**: InsightVM lze integrovat s cloudovými službami, virtuální infrastrukturou a CI/CD nástroji. InsightVM automaticky detekuje nová zařízení nasazená v Amazon Web Services, Microsoft Azure nebo přes VMware, a proto máte jistotu, že vašemu managementu zranitelností podléhají všechna zařízení dynamické infrastruktury. InsightVM dokáže nejen identifikovat již nasazené kontejnery, ale také jej lze přidat do repozitáře, ze kterého budou nové kontejnery vznikat.
- **Remediation planning**: Po dokončení skenu zranitelností InsightVM nabídne tzv. REMEDIATION PLAN – souhrn jednoduchých kroků, které povedou k výraznému navýšení zabezpečení infrastruktury. Administrátor může přiřazovat řešení zranitelností na své kolegy a následně průběžně sledovat stav řešení - aplikaci nápravných opatření. InsightVM lze integrovat s tiketovacími systémy (např. Atlassian Jira a ServiceNow), což napomáhá lepší spolupráci bezpečnostním týmům a díky evidenci incidentů podporuje také shodu s bezpečnostními nařízeními. InsightVM spolupracuje také s **Rapid7 Komand** – bezpečnostní a automatizační platformou, která napomáhá odhalení nejkritičtějších chyb a automatizuje proces patchování.
- **Attacker-Based analýza rizika**: InsightVM prioritizuje rizika, která jsou pro útočníka nejpřitažlivější k využití. Využívá desetiletí znalostí a zkušeností útočníků pro spolehlivou analýzu rizik. Jedinečné 1-1000 Real Risk skóre od Rapid7 bere v úvahu skóre CVSS, expozici na malware, *exploit* expozice (a pravděpodobnost jeho zneužití) a věk samotné zranitelnosti. Toto skóre zjednodušuje prioritizaci zranitelností určených pro nápravu a to přesněji než samotný systém CVSS využívaný konkurencí. Rapid7 Project Sonar přenáší data a *threat feeds* do InsightVM dashboardu, aby mohl uživatel vidět, která externí síťová dvířka jsou stále otevřená a které zranitelnosti útočníci aktivně zneužívají.

COMGUARD
security & networking

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

RAPID7

insightIDR insightVM
insightConnect insightOps insightAppSec

insightIDR

Rapid7 InsightIDR je technologie typu SIEM, která seskupuje *User Behavior Analytics (UBA), Attacker Behavior Analytics (ABA), Endpoint Detection and Response (EDR)* agenty, vizualizovanou časovou osu a centralizovaný log management za účelem efektivní prioritizace bezpečnostních hrozeb. 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.

Gartner
Magic Quadrant
SIEM - December, 2018
VISIONARIES

Klíčové vlastnosti Rapid7 InsightIDR:

- **Vyhledává a vizualizuje** data bezpečnostních událostí
- **Detekuje** kompromitované uživatele a laterální pohyb.
- **Identifikuje** rozvíjející se útočníkovo chování.
- Generuje časovou osu významných událostí.
- **Kontextuje data** z koncových stanic, a to bez narušení uživatelské aktivity
- **Zkracuje reakční čas –** Rozšířené vyhledávání InsightIDR umožňuje bezpečnostním analytikům přejít od ověření události k rychlému určení jejího rozsahu

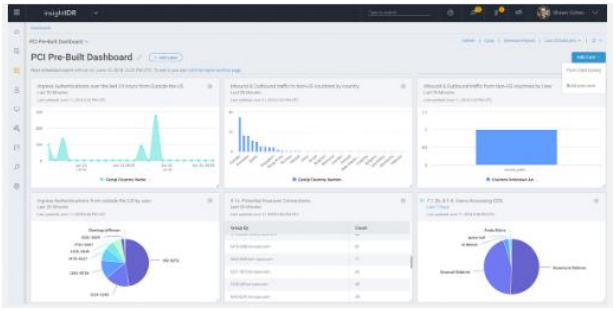
Řešení InsightIDR využívá analýzy útočníkova chování v reálném čase za účelem včasného detekování jeho aktivity v řetězci útoku, čímž minimalizuje tvz. *false-positives* eventy a tedy šetří čas a práci bezpečnostním pracovníkům. InsightIDR dokáže jednoduše identifikovat kompromitaci účtu s admin oprávněním a odhaluje tzv. laterální pohyb (technika postupu útočníků, kteří postupně „prochází" sítí za účelem nalezení a zneužití klíčových dat). Dalším bezpečnostním prvkem InsightIDR je nástroj k vytváření tzv. *honeypots* – systém, který se pro útočníka tváří legitimně a přitažlivě, ale obsahuje mechanismus, který slouží k odhalení záměru a strategie útoku.

Cloudová architektura

Díky cloudové architektuře a intuitivnímu rozhraní je možné v centralizovaném systému InsightIDR analyzovat data za účelem nalezení záznamu o incidentu již během několika minut. Nástroje jako UBA a ABA jsou automaticky aplikované na všechna data, pomáhají tedy detekovat útoky napříč celou infrastrukturou a umožňují na ně pohotově reagovat.

Strojové učení

Díky strojovému učení se celé řešení neustále vyvíjí stejně jako chování útočníků. Proto dokáže automaticky upozornit na použití ukradených hesel nebo na neobvyklý laterální pohyb. Nespamuje každou anomálii v datech – doručuje jednotky upozornění denně zvýrazňující klíčové věci, které je zapotřebí znát za účelem ochrany sítě. Každé podezřelé uživatelské chování se ukládá do *Risky User Ranking,* jehož data pomáhají bezpečnostním týmům určit, jakým oblastem je třeba se věnovat přednostně.



Synchronizovaný Attacker Behavior Analytics

Bezpečnostní analytici společnosti Rapid7 neustále pracují na odhalování variant zatím neznámých úspěšných útočných technik a zpracovávají je do formy tzv. detekcí. Tyto detekce jsou následně přiřazeny k odpovídajícím událostem v InsightIDR. Jedná se tedy o kontexty útoků, které jsou obohacené o doporučené návrhy řešení. Výsledkem celého procesu je upozornění pro všechny bezpečnostní administrátory v plném kontextu potenciálního útoku.

Automaticky zahrnuje kompromitované uživatele a zařízení

Vyšetřováním hrozeb v InsightIDR se získává důležitý kontext útoků, lze však také okamžitě podniknout kroky k nápravě probíhajících bezpečnostních incidentů. Pomocí integrovaného Insight Agent lze zastavit škodlivé procesy nebo odpojit infikované koncové stanice ze sítě. InsightIDR shromažďuje informace z *Active Directory, Access Management, EDR* a firewallu – díky tomu budou mít bezpečnostní týmy všechny hrozby na úrovni uživatele, koncového zařízení, ale i sítě pod kontrolou.

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 vaším vývojovým týmem a zainteresovanými stranami. DAST řešení je možné také pořídit v on-prem verzi – AppSpider Enterprise/Pro.

insightOps

InsightOps je technologie určená pro Event a Log Management, která sbírá a normalizuje logy ze serverů, aplikací, Active Directory, databází, firewallů, DNS, VPNs, Amazon WS a jiných cloudových služeb. Dokáže sledovat a monitorovat CPU, RAM a zatíženost disku v každém zařízení v síti. Automaticky generuje upozornění, když je výkon serveru, aplikace, nebo služby silně postižen – nabízí live dashboardy a plánované reporty monitorující výkon. InsightOps řadí mezi své přednosti „lidský jazyk" log managementu, díky kterému nikomu nedělá problém porozumět otázkám týkajících se inspekce síťových zařízení. REST API a *out-of-the-box* integrace dovolují jednoduše obsáhnout InsightOps do DevOps stacku pro složitější IT automatizace.

insightConnect

InsightConnect je Security Orchestration and Automation Response (SOAR) systém, který obsahuje více než 200 pluginů určených pro zabezpečení připojení bezpečnostních nástrojů a který jednoduše automatizuje opakující se úlohy pomocí workflow – bez nutnosti kódování. InsightConnect tedy automatizuje práci prostřednictvím pracovních postupů (workflow), kde jenom stačí nastavit rozhodovací body, na základě kterých bude InsightConnect postupovat. Jelikož InsightConnect je cloud-based, uživatel je schopen měnit pracovní postupy v programu kdykoli a kdekoli, bez jediného řádku kódu

COMGUARD
security & networking

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