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 dnes čelí bezpečnostní a IT týmy. Bezpečnostní cloudová platforma ***Rapid7 Insight*** *byla vyvinuta jako odpověď na tyto problémy. Jedná se o intuitivní řešení, díky kterému mají Bezpečnostní, IT a vývojové týmy jedním kliknutím přístup ke správě zranitelností, k zabezpečení cloudových aplikací, umožňuje jim detekci a reakci na události, automatizaci a další pomocné nástroje.*

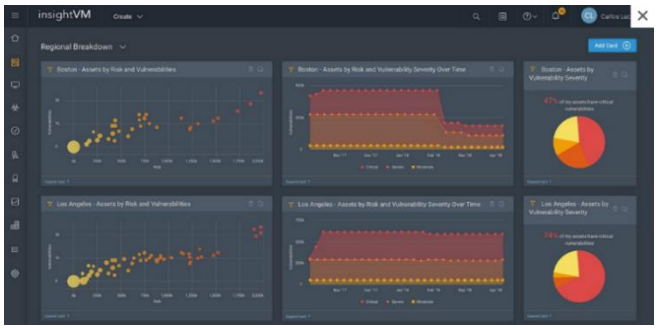
Rapid7 Insight je centralizovaná bezpečnostní platforma pro technologie:

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

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.



Klíčové vlastnosti:

- **Real Risk Score** – prioritizace nalezených zranitelností
- **Asset Management** – informace o nejzranitelnějších strojích
- **Remediation planning** – souhrn jednoduchých kroků, které pomohou při nápravě
- **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

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 – February 2020
LEADERS

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. Díky cloudové architektuře a intuitivnímu rozhraní je možné v centralizovaném systému InsightIDR analyzovat data za účelem nalezení záznamu o incidentu již během několika minut.

Jednoduchá (multitenantní) architektura = Cloud centrální správa + agenti na koncových bodech

COMGUARD
communication security

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

Rapid7 Insight – Centralizovaná Bezpečnostní Platforma

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 na 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 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.

insightCloudSec

V posledních letech se setkáváme s velkým nárustem zavádění cloudu v organizacích. Rychlost těchto změn v kombinaci se zvýšeným objemem zdrojů a jejich složitosti v cloudovém prostředí často nutí organizace, aby přijaly neřízené riziko.

InsightCloudSec pomáhá chránit i ty nejkomplexnější multi-cloudy a kontejnerová prostředí před nesprávnou konfigurací, porušením zásad, hrozbami. Pomáhá se správou identity a přístupem (IAM). Řešení umožňuje automatickou nápravu v reálném čase, což má za cíl pomoct zákazníkům rychle reagovat na bezpečnostní rizika. **InsightCloudSec je plně integrovaná cloudová nativní platforma**, která obsahuje sadu nástrojů pro zabezpečení v cloudu. V jediném řešení platforma pomáhá zákazníkům porozumět, auditovat a monitorovat jejich stav zabezpečení napříč všemi cloudovými zdroji.

Stěžejní funkcionality Rapid7 InsightCloudSec:

- Umožňuje monitorovat všechny cloudové služby na jedné uživatelsky přívětivé platformě
- Zajišťuje viditelnost všech assetů v cloudu na jednom místě
- Customizovatelný compliance reporting
- Real-time Data Collection
- Vulnerability assessment
- Cloud Identity & Access Management

Podporované platformy:

Amazon | Microsoft | Google | Alibaba | Kubernetes

Možnosti integrace: Slack, Jira, ServiceNow, PagerDuty, Splunk, MS Teams, Tenable, InsightVM, InsightIDR

THREAT COMMAND

Bezpečnostní oddělení se zpravidla dívají na to, co se děje uvnitř společnosti a díky tomu jsou schopni reagovat a odhalit jen aktuálně probíhající útoky.
Threat Command je **pokročilá Threat Intelligence**, která přináší komplexní přehled a snižuje tak riziko hrozeb v organizaci a vytížení členů bezpečnostního týmu. Dává pohled ven, sleduje informace, které unikly a které mohou nasvědčovat tomu, že se společnost stane terčem kybernetického útoku. Současně ochráníte infrastrukturu před útočníky, kteří se snaží **zneužít jméno vaší společnosti.**
Prochází **dark i clear web** a informuje o externích hrozbách, které jsou členěné do několika kategorií:

- **Brand Security** – monitoring sociálních sítí, zda se někdo nevydává za konkrétní osobu zneužívající logo a název společnosti na sociálních sítích
- **Phishing** – sleduje, zda si někdo neregistruje podobnou doménu využívanou organizací a která by následně mohla být zneužita k phishingu
- **Data Leakage** – sleduje, zda se na dark webu neobchoduje s ukradenými přihlašovacími údaji zaměstnanců, platebními kartami konkrétní banky apod.
- **Exploitable data** – prochází logovací stránky v organizaci, otevřené porty a místa, kde by mohla být z externího pohledu organizace zranitelná

COMGUARD communication security

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