COMGUARD

RAPID7

Rapid7 InsightIDR

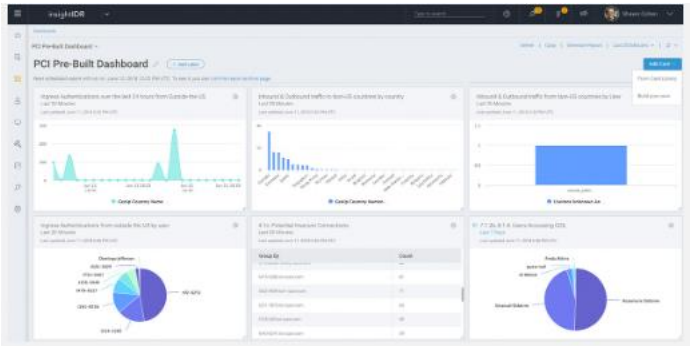
Pohled z XDR perspertivy

*E**X**tended **D**etection and **R**esponse (XDR) byl v portfóliu Rapid7 ještě dříve, než se z něj stal aktuální trend kyberbezpečnosti. Spojením EDR a SIEM vznikla unikátní centrální bezpečnostní platforma nabízející holistický pohled na zabezpečení celé organizace. Právě kombinace těchto technologií je klíčová – zajišťuje technologický náskok před hrozbami.*

Rapid7 InsightIDR

Je **centralizovaná bezpečnostní platforma**, která vznikla spojením toho nejlepšího z technologií *Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), User Behavior Analytics (UBA) a Attacker Behavior Analytics (ABA).* Vizualizuje časovou osu a poskytuje 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 - June 2021
LEADERS



InsightIDR využívá **analýzy útočníkova chování v reálném čase** za účelem včasného detekování jeho aktivity v řetězci útoku, čímž minimalizuje *false-positives* a tak šetří čas a práci. Dokáže jednoduše identifikovat kompromitaci účtu s admin oprávněním a odhaluje laterální pohyb (technika útočníků, kteří postupně „prochází" sítí za účelem nalezení a zneužití klíčových dat). Dále umožňuje vytvářet tzv. *honeypots* – zdánlivě legitimní prvek infrastruktury (server, stanice, databáze), který však obsahuje mechanismus sloužící k odhalení záměru a strategie útoku.

Synchronizovaný Attacker Behavior Analytics

Bezpečnostní analytici společnosti Rapid7 neustále pracují na odhalování variant zatím neznámých 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 obsahují i 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 získáváte 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.**

Klíčové vlastnosti

- **Vyhledává a vizualizuje** data bezpečnostních událostí.
- **Detekuje** kompromitované uživatele a laterální pohyb.
- **Identifikuje** rozvíjející se útočníkovo chování.
- **Generuje** časovou osu významných událostí.
- **Dává do kontextu 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.
- **Kombinuje** kontext síťového provozu a funkcionality EDR a SIEM v moderní **XDR**.

COMGUARD
communication security

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

Rapid7 InsightIDR

Cloudová architektura

Jednoduché a rychlé nasazení **v řádu jednotek dnů** vyžaduje pouze instalaci koncových agentů nebo on-prem collectorů. Pomocí intuitivního uživatelského 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 rychle 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**. Každé podezřelé uživatelské chování se ukládá do *Risky User Ranking,* jehož data pomáhají bezpečnostním týmům určit, jakým oblastem je třeba se věnovat přednostně.

Network Traffic Analysis (NTA) je modulem řešení InsightIDR, který poskytuje komplexní vhled do síťových aktivit organizace. Jedná se o důležitý nástroj, díky kterému lze odhalit bezpečností incidenty ještě dřív, než stihnou napáchat nevratné škody. Díky analýze síťového provozu lze snadněji identifikovat anomálie, které jsou velmi často ukazatelem probíhajícího bezpečnostního incidentu. NTA disponuje vbudovaným Intrustion Detection System (IDS) s řadou vlastních signatur. Jedná se tedy o další bezpečnostní vrstvu, která doplňuje SIEM o důležitý kontext z pohledu síťové bezpečnosti. NTA je také hojně využíváno pro optimalizaci síťového provozu za účelem navýšení jeho výkonu.

Nejčastěji využívané use-cases NTA

- Sběr real-time a historických záznamů síťových aktivit
- Detekce malware (např. aktivita ransomware)
- Troubleshooting pomalé sítě
- Odhalení využívání zranitelných protokolů a šifer
- Vylepšení přehledu o síťovém provozu a eliminace slepých míst

Výhody XDR oproti EDR

- Shromažďováním důležitých informací umožňuje přesnou zpětnou analýzu po kybernetickém útoku
- XDR sleduje celou infrastrukturu, ne jenom koncová zařízení
- Dramaticky odlišný poměr signálu k šumu, detekce jsou přesné

Security Orchestration and Automation Response (SOAR) systém je součástí InsightIDR. Obsahuje více než 200 pluginů určených pro zabezpečení připojení bezpečnostních nástrojů a jednoduše automatizuje opakující se úlohy pomocí workflow bez nutnosti kódování. Stačí nastavit rozhodovací body na základě kterých bude postupovat. Jelikož je cloud-based, uživatel je schopen měnit pracovní postupy v programu kdykoli a kdekoli bez jediného řádku kódu.

InsightIDR balíčky	Essential	Advanced	Ultimate
Centralized log management, search, reporting dashboard	✓	✓	✓
Compliance dashboards	✓	✓	✓
File Integrity Monitoring with Insight Agent	✓	✓	✓
Intrusion Detection System (IDS) and Network Traffic monitoring with Insight Network Sensor	✓	✓	✓
Custom rule creation and alerting	✓	✓	✓
Threat Intelligence, Endpoint Detections (EDR), and Attacker Behavior Analytics		✓	✓
Investigations console		✓	✓
User Behavior Analytics		✓	✓
Deception Technology		✓	✓
Core Automated Response Workflows		✓	✓
Enhanced Endpoint Telemetry			✓
Enhanced Network Traffic Analysis			✓
Unlimited SOC Automation			✓
Customer Support	✓	✓	✓
Deployment & Training	Basic Onboarding Support	1-Day Quickstart Included	2-Day Quickstart Included
APIs		✓	✓
Search and Retention	All models include 13 months of data retention (90 days hot and 300 days warm)		

COMGUARD
communication security

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