

Security Intelligence Platform

SIEM | Log Management | File Integrity Monitoring | Host & Network Forensics



Ochrana před rychle se vyvíjejícími hrozbami vyžaduje detailní porozumění a přehled nad celou IT infrastrukturou organizace. Útoky přicházejí z mnoha stran a jejich odhalení je možné na základě logů a dat z různých zařízení. Kvalifikovanější přehled je získáván pomocí cíleného forenzního monitoringu uživatelů, koncových zařízení a síťového provozu. Pokud je tento přístup implementován v rámci vícerých automatizovaných analytických technik, navzájem propojených, jsou hrozby odhalitelné jako nikdy předtím.

LogRhythm přináší řešení pro řízení životního cyklu hrozeb, next-generation SIEM, log management, endpoint/network monitoring vč. forenzní analýzy a bezpečnostní analytické nástroje v ucelené „Security Intelligence Platform“. Tato platforma poskytuje nekompromisní vhled do potenciálních hrozeb a z nich plynoucích rizik dříve, než způsobí reálné bezpečnostní incidenty. LogRhythm přesně detekuje širokou škálu indikátorů potenciální kompromitace, což umožňuje okamžitou reakci a aplikaci preventivních opatření. Hluboké porozumění rizikům poskytované řešením LogRhythm Security Intelligence Platform umožňuje udržet síť skutečně bezpečnou a ve shodě s regulatorními požadavky.

Klíčové charakteristiky:

- ⇒ Next-generation SIEM
- ⇒ Obsahuje **dedikovaný GDPR modul** pro kontrolu compliance s EU nařízením
- ⇒ Nezávislá forenzní analýza koncových zařízení a File Integrity Monitoring
- ⇒ Forenzní analýza sítě vč. „Application ID“ a „Full Packet Capture“
- ⇒ Pokročilá korelace a rozpoznání vzorků (pattern)
- ⇒ Vícerozměrné analýzy a detekce anomálií chování na úrovni uživatele, sítě i koncových zařízení
- ⇒ Rychlé, inteligentní vyhledávání
- ⇒ Analýzy velkých objemů dat, jejich vizualizace, procházení k detailnějším vrstvám
- ⇒ Automatické odezvy dle workflow – via technologii SmartResponse™
- ⇒ Integrovaný „Case Management“

Analýzou všech dostupných logů i dat ze zařízení a jejich kombinací a hloubkovou analýzou na úrovni koncových i síťových zařízení je dosaženo skutečného přehledu nad infrastrukturou organizace. To je následně využito technologií AI Engine

pro automatizované, kontinuální analýzy veškerých aktivit v daném prostředí. AI Engine umožňuje organizaci vidět dříve neviditelné hrozby a z nich plynoucí rizika. Integrovaná architektura zajistí, že je v případě detekce hrozby v reálném čase vidět globální přehled dané aktivity a zajištěna okamžitá reakce.

Ekonomičnost a jednoduchost řešení

Je jedno, jste-li středně velká organizace, nebo globální SOC (Security Operations Center), vždy je třeba se dívat na celkové náklady vlastnictví a návratnost v čase. Integrovaná architektura LogRhythm spolu se zaměřením na intuitivnost a jednoduchost umožňuje zákazníkům rychle využívat veškeré funkce. LogRhythm si zakládá na vytváření jednoduchých řešení pro složité problémy. LogRhythm Labs™ poskytují strategické out-of-the box zázemí pro zákazníky, kteří se mohou věnovat pouze svému businessu. Veškerý vývoj a sledování hrozeb je zákazníkům



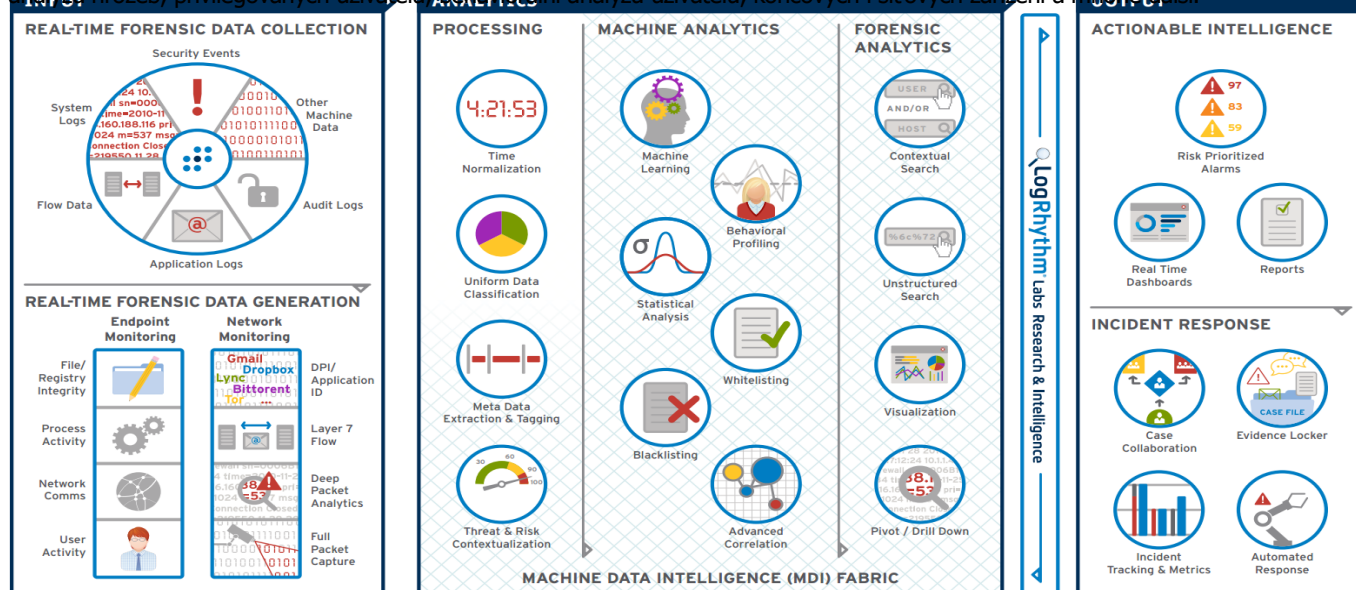
automaticky k dispozici.

Využití umělé inteligence

Celé řešení lze jednoduše rozšířit o **LogRhythm CloudAI** - jedinečnou technologii, která na data v SIEMu aplikuje algoritmy strojového učení a samo-zdokonalující se umělou inteligenci. Jde o plně integrovaný add-on, určen především pro detekci bez-signaturových a skrytých hrozeb. Díky své cloudové architektuře jej lze velmi jednoduše nasadit a také následně spravovat.

Zajištění shody

LogRhythm nabízí jako jediný výrobce ve svém řešení již integrovaný dedikovaný **GDPR modul** a další automatizované nástroje pro řízení shody s se standardy jako např.: ISO 27001, PCI, SOX, HIPAA, FISMA, GLBA, DODI 8500.1, NERC/CIP a dalšími, které zahrnují analýzu hrozeb, privilegovaných uživatelů, behaviorální analýzu uživatelů, koncových i síťových zařízení a mnohé další.



Security Intelligence Platform

SIEM | Log Management | File Integrity Monitoring | Host & Network Forensics



Detekce cíleného malwaru s Host Behavior Anomaly Detection

Výzva: Cílený malware připojený k neznámému typu útoků je navržen tak, aby překonal standardní bezpečnostní mechanismy, které staví na signaturách a známých vzorcích chování.

1. LogRhythm zaznamenává „normální“ chování hosta a vytváří whitelist akceptovatelných aktivit.
2. Host Activity Monitoring nezávisle detekuje start nového procesu.
3. LogRhythm automaticky rozpoznává, že nový proces není ve whitelistu.
4. Automatická analýza vyhodnocuje událost jako abnormální síťový provoz a aktivitu přisuzuje vysoké riziko.
5. Je zasláno upozornění bezpečnostnímu administrátorovi, který využije přístup k forenzní analýze pro zjištění dalších detailů.

Odhalení kompromitovaných přihlašovacích údajů s User and Entity Behavior Analytics (UEBA)

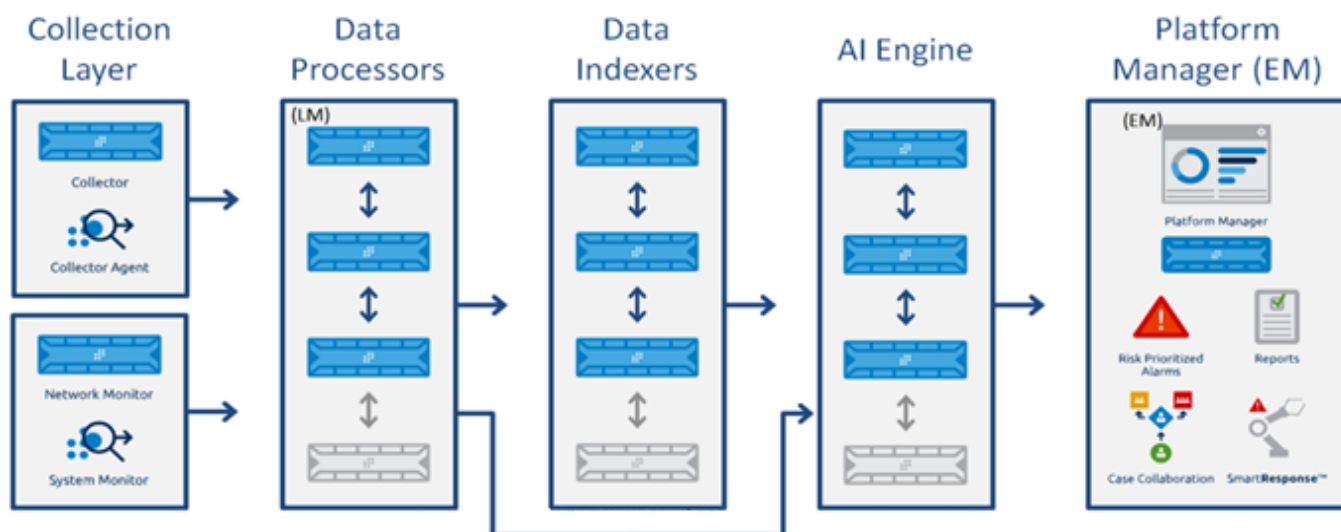
Výzva: K trendům, které zhoršují rozpoznávání „ne/normálního“ chování uživatelů indikující kompromitaci přihlašovacích údajů, patří zvyšující se mobilita uživatelů a BYOD.

1. LogRhythm automaticky vytváří profil pro každého uživatele, zahrnující seznam akceptovaných aktivit a vzorců.
2. AI Engine detekuje odchylku v podobě přihlášení z podezřelé lokality, snaha o přístup k vyšším objemům dat a jejich kopírování na neznámá úložiště nebo do cloudu.
3. SmartResponse™ automaticky deaktivuje účet nebo odezvy systémů přesouvá do karantény pro forenzní analýzu a validaci daných uživatelských aktivit.

Identifikace „vysávání“ dat s Network Behavior Anomaly Detection

Výzva: Konstantní datové toky do a ze sítě organizace znesnadňují detekci citlivých dat putujících z organizace ven.

1. Network Monitor poskytuje strategicky důležitý přehled na síťové vstupní a výstupní body, technologie SmartFlow™ detailní vzhled do paketů každého síťového spojení a aplikace.
2. Automatické analýzy LogRhythm ustavují normy chování napříč sledovanými síťovými aktivitami, využívajíc meta dat poskytnutých technologií SmartFlow™.
3. Odchylky v síťovém provozu jsou identifikovány a porovnány s dalšími logy a daty z různých zařízení pro přesné vyhodnocení rizika.
4. Technologie SmartCapture™ sbírá všechny pakety související s podezřelým spojením pro jejich kompletní forenzní analýzu.



Možnosti nasazení a popis architektury

Řešení LogRhythm lze zakoupit jako soubor jednotlivých komponent nebo tzv. **All-in-one** (XM) Appliance, která obsahuje funkce PM, DP, DC a AIE. **Platform Manager** (PM/EM) provádí vyhodnocování událostí (alarmy), management incidentů, automatizaci workflow a centrální správu. **Data Processor** (DP/LM) poskytuje výkonné parsování logů a jejich normalizaci pro následující zpracování. **Data Collector** (DC) agentsky i bezagentsky sbírá logy, flow a data ze zřízení, zabezpečuje přenos ze vzdálených lokalit. Volitelný **Data Indexer** (DX) provádí ukládání originální a unifikovaných logů a indexace dat. **AI Engine** (AIE) pokročilé korelace a analýzy chování, vč. histogramů, statistických profilování a whitelistů a patentované automatizované analýzy. **Network Monitor** (NM) nabízí úplný přehled o síťovém provozu, identifikuje anomálie a aplikace pomocí hloubkové inspekce paketů.

Další možností nasazení je **LogRhythm Cloud**, tedy SaaS řešení umožňující velmi flexibilní nasazení. Hlavní výhodou je to, že kompletní správu SIEM infrastruktury řeší výrobce a tím umožní IT a bezpečnostním administrátorům se plně soustředit pouze na zabezpečení a ochranu svého podniku. LogRhythm Cloud je stejně robustní řešení jako jeho on-premise ekvivalent, nejedná se o žádný kompromis. Samozřejmě poskytuje tedy všechny funkcionality, které naleznete u on-premise řešení, a to dokonce včetně zabudovaného systému SOAR (Security Orchestration, Automation, and Response).