COMGUARD

cyber security masters

LogRhythm

Security Operations Center ready SIEM

Roman Jiráček | Senior Account & Vendor Manager

18.09.2023

COMGUARD

"Cyber-attacks, rather than natural catastrophes, will become uninsurable as the disruption from hacks continues to grow." ***— Mario Greco, CEO of Zurich Insurance***

60%

of organizations that had a ransomware attack did not have a SIEM

Microsoft's 2022 Digital Defense Report

67%

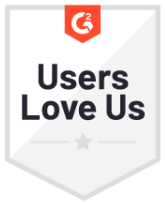
lost a business deal due to a prospect's lack of confidence in their security strategy

Dimensional research survey of 1,175 security professionals

COMGUARD

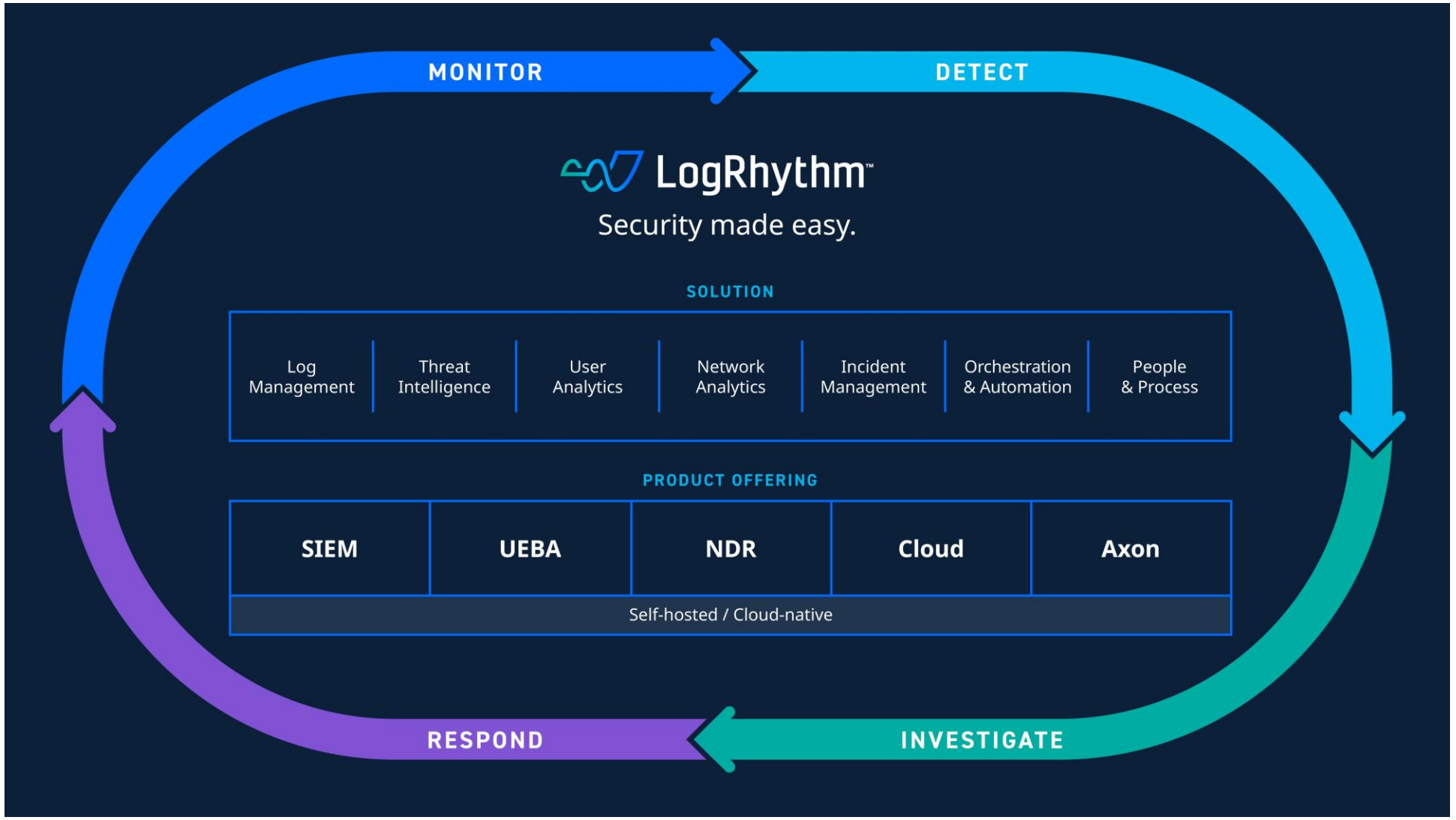
LogRhythm

- Společnost založena v r
- Global Operations
  - USA, EMEA, APAC
- 7th generace SIEM



Splunk Enterprise by Splunk	4.3	(786 ratings)
LogRhythm SIEM by LogRhythm	4.5	(685 ratings)
QRadar SIEM by IBM	4.3	(549 ratings)
Trellix Security Manager by Trellix	4.4	(459 ratings)
Splunk Enterprise Security by Splunk	4.4	(412 ratings)
Logpoint - SIEM by Logpoint	4.2	(364 ratings)
Securonix Next-Gen SIEM by Securonix	4.8	(346 ratings)
Elastic (ELK) Stack by Elastic	4.3	(314 ratings)
InsightIDR by Rapid7	4.3	(285 ratings)

LogRhythm Portfolio



LogRhythm SIEM / NDR | SOC Visibility Triad

Tři pilíře

- Log Monitoring (SIEM/UEBA)
- Endpoint Monitoring (EDR)
- Network Monitoring (NDR)

Benefity tohoto modelu

- Komplexní viditelnost
- Brzká detekce
- Rychlejší odezva na incidenty
- Každý pilíř rozšiřuje druhý z pohledu viditelnosti
- Snížení počtu false positives/negatives

Architektura Appliance

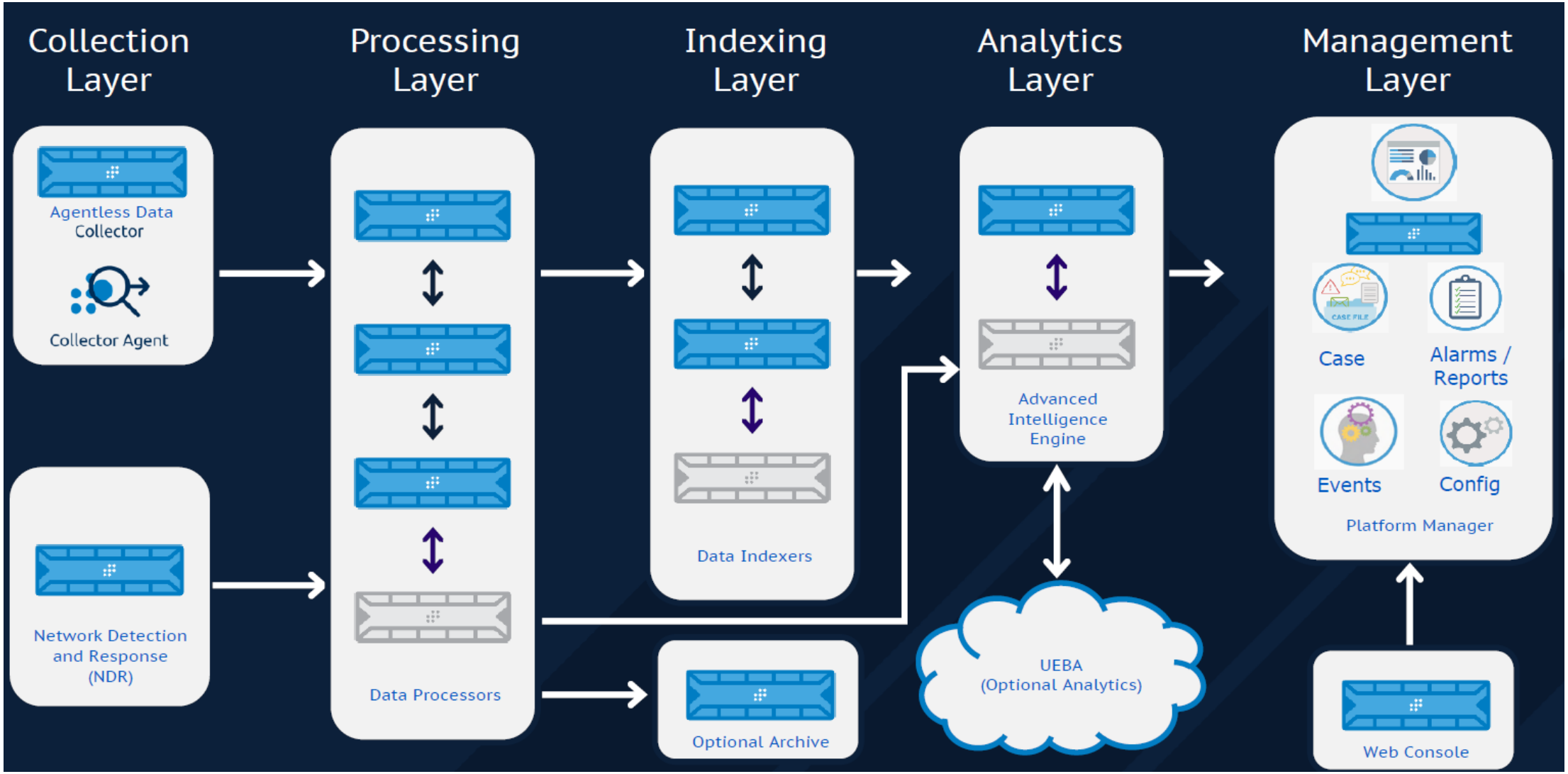
Dedikované Appliances /SW/VM

- Centralizovaný management
- Horizontální škálovatelnost
- Podpora pro distribuovaná prostředí

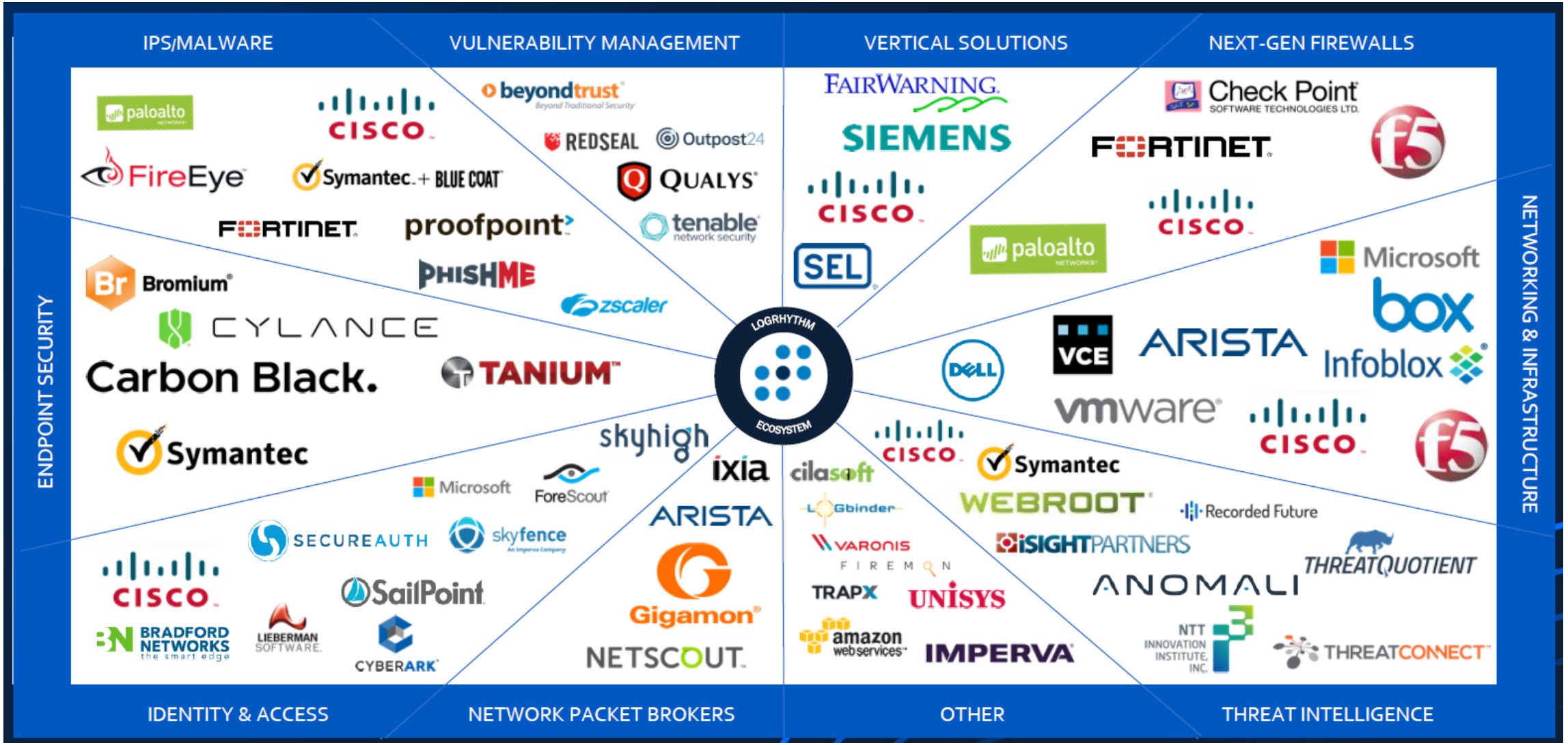
XM Single Appliance /SW/VM

- All-in-one řešení
- Jednoduché a flexibilní nasazení
- Kompletní sada funkcí

LogRhythm SIEM – architektura



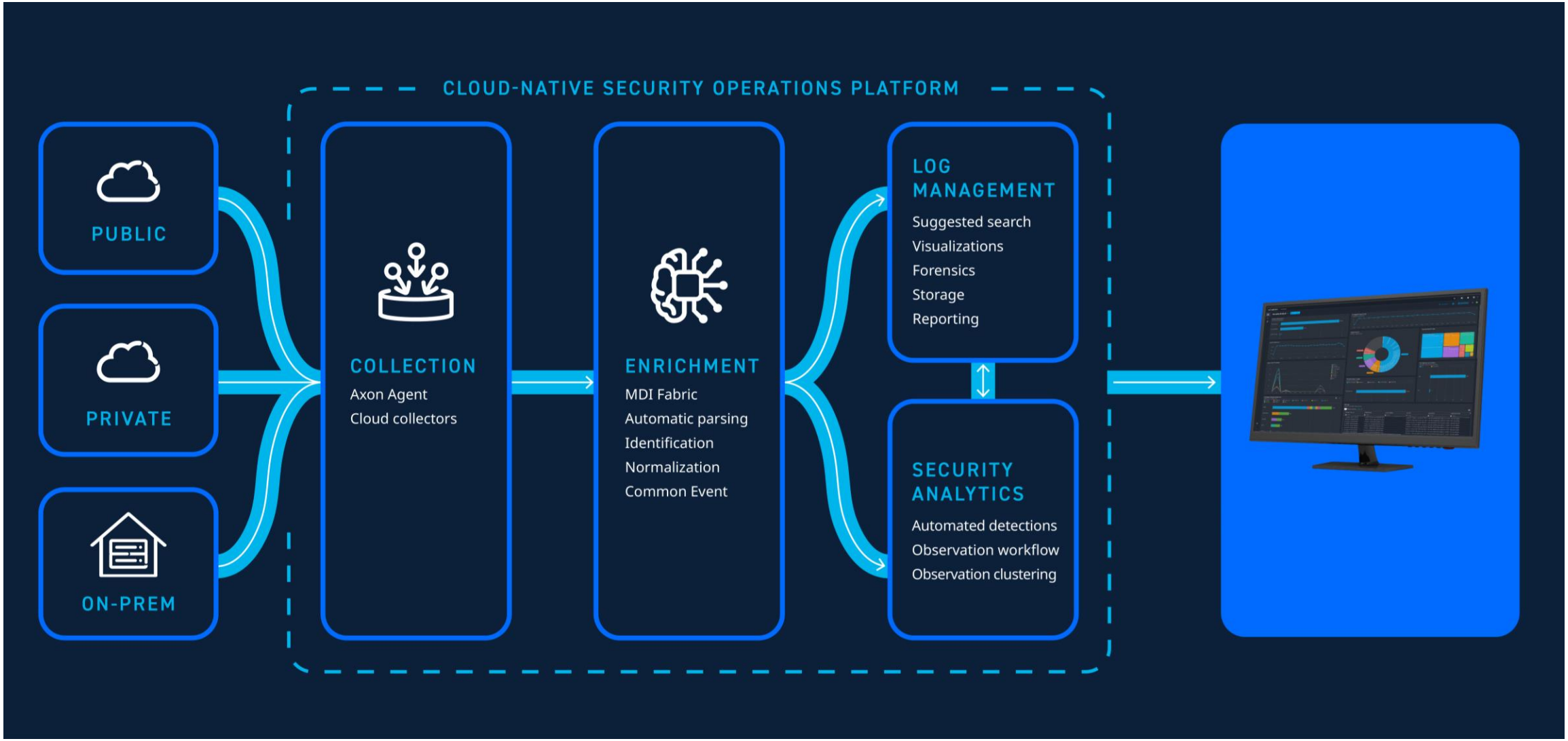
Technologičtí partneři



COMGUARD

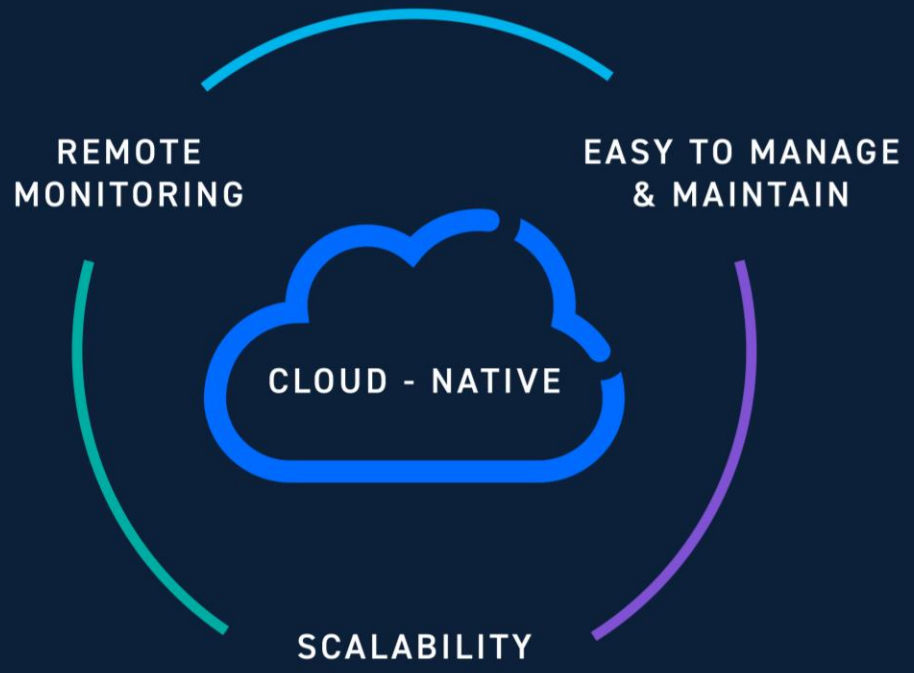
On-premise SIEM vs. Cloud SIEM

LogRhythm Axon



Cloud-Native Saas Platform

CLOUD		
DEPLOYMENT	SOFTWARE • SIEM platform • Collector agents • Packaged content	Included Included Included
	INFRASTRUCTURE • Hardware • High availability • Disaster recovery	Included Included Included
PLATFORM UPKEEP / EVOLUTION	SRE UPGRADES PLATFORM MONITORING	Included Included Included

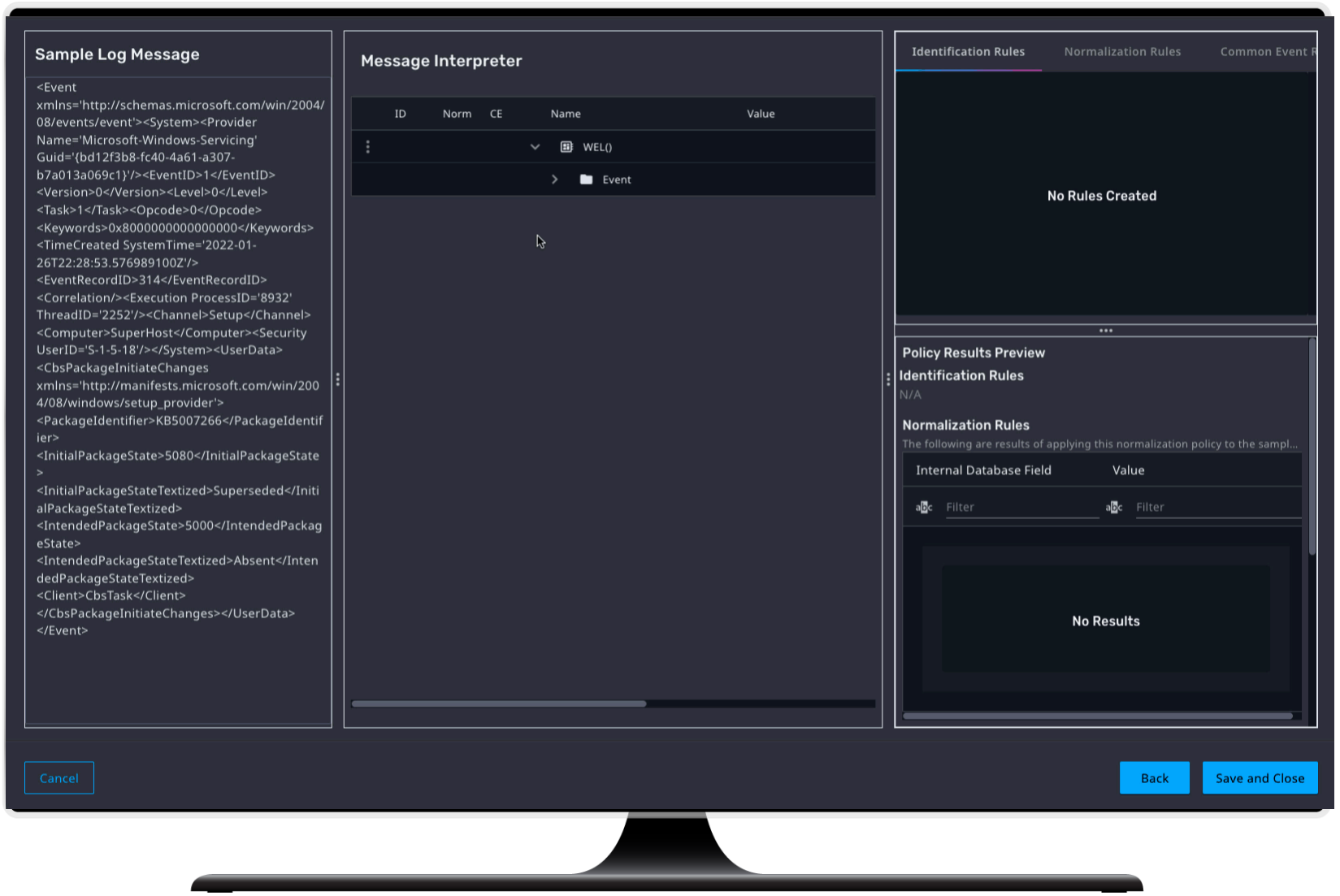


COMGUARD

LogRhyhtm Axon – pokročilé vyhledávání

COMGUARD

LogRhythm Axon – vyváření politik



Srovnání funkcionalit

		LogRhythm SIEM	LogRhythm Axon
Infrastructure	Managed Infrastructure	✓	✓
	Managed Software Updates		✓
	Managed Knowledge Base Updates		✓
	Knowledge Base	✓	✓
	Active Directory Integration	✓	Roadmap
	Rest API Access	✓	✓
	Single Sign On (SSO)	✓	✓
	High Availability	✓	✓
	Disaster Recovery	✓	✓
	Role Based Access Control	✓	Limited
	Multifactor Authentication (MFA)	✓	✓
Analytics & Detections	User & Entity Behavior Analytics (UEBA)	✓	✓
	Network Detection & Response (NDR)	✓	✓
	Behavior-based Detections	✓	Oct 2023
	Analytics Rule Authoring	✓	✓

		LogRhythm SIEM	LogRhythm Axon
Data Management	Entity, Network, & Host Management	✓	Roadmap
	Data Archiving	✓	Roadmap
	Hosted Collectors		✓
	Generic Webhook	Limited	✓
	Auto-Log Source Identification & Onboarding		✓
	Automatic Metadata		✓
	Message Processing Engine (MPE) Rule Creation	✓	✓
	Graphical Policy Builder		✓
Analyst Tools	Reporting	✓	✓
	Case Management	✓	Oct 2023
	Web Console	✓	✓
	Custom Dashboards	✓	✓
	SmartResponse	✓	Roadmap
	Suggested Search	Limited	✓
	Playbooks	✓	Roadmap
	Simple Lists	✓	✓
	Multi-column Lists		✓
	Compliance	✓	Roadmap
	Email Notification	✓	✓

CASE STUDY – pojišťovací společnost

- Společnost je na trhu od roku 1993
- Působnost společnosti na 18 evropských trzích
- Velikost společnosti:
  - 22 000 pracovníků
  - 15 mil. klientů (3 mil. klientů v ČR a SK)

Stěžejní změny ve společnosti:

- Říjen 2020 – akvizice další pojišťovací společnosti a rozšíření produktů a služeb

Co bylo hlavním důvodem, proč se začali zajímat o řešení SIEM?

- Pojišťovny mají povinnost dohledávat pojišťovací fraud pro forenzní analýzu u jednotlivých incidentů, takže **SIEM je NUTNÁ POLOŽKA**.

Centrální SIEM

LogRhythm

Logy & Eventy

ČR

LogRhythm

Logy & Eventy

Akvírovaná společnost

SK

LogRhythm

Realizace projektu

1. Pre-sales konzultace

- COMGUARD a.s. + partner + zákazník – řešila se integrace SK pobočky (LogRhythm SIEM) do ČR pobočky (LogRhythm SIEM) a nezávislého akvírovaného subjektu (konkurenční řešení)
- **Časová náročnost** = několik hodin v rámci pre-sales workshopů a schůzek
- **Hlavní téma** – výkonnost nového HW deploymentu na centrále v Praze

2. Migrace současného LogRhythm na výkonnější deployment

- Centrální řešení SIEM pro celý holding v Praze
- Původní HW se využil jako analytický nástroj nového SIEMu
- **Časová náročnost** = 5 měsíců práce technického týmu
- **Hlavní téma** - migrace všech politik na výkonnější HW

LogRhythm

Realizace projektu

3. Integrace SK pobočky

- Instalace datových collectorů na jednotlivých pobočkách SK
- Integrace datových collectorů z poboček do centrály v Praze
- **Časová náročnost** = 3 měsíce práce technického týmu
- **Hlavní téma** – integrace SK pobočky do centrály v ČR

4. Integrace akvírovaného subjektu – AKTUÁLNÍ FÁZE

- Integrace společnosti, která řešila problematiků Logů a Eventů na jiné SIEM technologii
- Separátní tým pro správu předchozího řešení – komunikační problémy
- Bude využita multi-tenance celého řešení LogRhythm SIEM, kdy jednotlivé pobočky uvidí pouze Logy a Eventy, které se jich týkají
- **Časová náročnost** = fáze integrace stále probíhá!

Realizace projektu

5. Vznik globálního Security Operation Center – BUDOUCÍ FÁZE

- Tento tým bude řešit globálně IT security pro celý holding – hledají abnormality z výstupů ze SIEM
- Lokální týmy budou řešit provozní záležitosti jednotlivých poboček

6. Rozšíření stávajícího SIEM řešení o další prvky – BUDOUCÍ FÁZE

- Security orchestration, automation and response (SOAR)
- Network Detection & Response (NDR)
- CloudAI
- User and Entity Behaviour Analytics (UEBA)

Závěr

- Splnění požadavku na možnost analyzování a zabránění incidentů v IT infrastruktuře
  - Forenzní analýza pro dohledávání úniků dat
  - Alertování a reportování – Security tým je včas upozorněn na jednotlivé incidenty, které následně prochází a kontroluje dané nálezy
- Splnění požadavků multi-tenance – jednotlivé týmy vidí pouze informace, které vidět mají (rozdělení na globální a lokální týmy)
- Modulární řešení = možná úspora finančních prostředků
  - Rozdělení projektu na jednotlivé fáze – SIEM + další moduly v budoucnu

COMGUARD

cyber security masters

Děkujeme za pozornost!

Roman Jiráček | roman.jiracek@comguard.cz