COMGUARD

cyber security masters

Exabeam

Security Operations Center: Proč nepodcenit rostoucí trend

Roman Jiráček, Senior Account & Vendor Manager

20.09.2024

COMGUARD

LogRhythm je nově Exabeam

exabeam Platform Solutions Resources Why Exabeam EN Contact Us Get a Demo

Home > Press Releases

Exabeam and LogRhythm Complete Merger and Announce New Company Details

Share Jul 17, 2024 4 minutes to read

The combined organization will empower customers with a best-of-breed, AI-driven security operations platform fortified with high-integrity data ingestion

BROOMFIELD, Colo. and FOSTER CITY, Calif. — July 17, 2024 – In a strategic move set to define the future of the cybersecurity landscape, Exabeam, delivering industry-leading AI and automation for accelerated threat detection, investigation, and response (TDIR), and LogRhythm, renowned for its high-integrity, trusted data ingestion, today announced the successful completion of their previously announced merger. The merger combines unparalleled technological innovation with reliable data to create an AI-driven security operations platform that delivers the most efficient and accurate security information and event management (SIEM) and user and entity behavior analytics (UEBA) solutions in the industry.

Moving forward, the company will leverage the best of both organizations to create a best-of-breed cybersecurity vendor relentlessly focused on empowering security analysts, security engineers, and CISOs with the tools, intelligence, and guidance needed to safeguard their organizations against cyberthreats. The company will retain the Exabeam name and refresh the visual brand to represent the merging of two industry leaders and honor the legacy of the long-established LogRhythm brand.

Exabeam has also unveiled its product roadmap and strategy, highlighting the proven, cloud-native AI-driven

Recent Press Releases

Exabeam Appoints Kish Dill as Chief Customer Success Officer
September 10, 2024

Exabeam® Named To Newsweek's 2024 List of Top 100 Most Loved Workplaces®
June 11, 2024

LogRhythm and Exabeam Announce Intent to Merge, Harnessing Collective Innovation Strengths to Lead the Future of

LogRhythm now exabeam Products Solutions Industries Work With Us Resources About Request Info

LogRhythm and Exabeam Announce Intent to Merge, Harnessing Collective Innovation Strengths to Lead the Future of AI-Driven Security Operations

LogRhythm exabeam

Posted on May 15, 2024
Category: General
Type: Press Releases

The combined company will bring together two cybersecurity SIEM and UEBA innovation leaders with renowned and demonstrated track records in serving customers with effective threat detection, investigation, and response (TDIR)

Co přinese Exebeam?

- Lepší **behaviorální analýza a UEBA** pro detekci anomálií.
- Pokročilejší **automatizace a SOAR**, což umožňuje rychlejší reakce na incidenty.
- **Cloudová škálovatelnost** bez nutnosti velkých investic do infrastruktury.
- **Jednodušší nasazení a uživatelsky přívětivé rozhraní**.
- **Transparentní licencování** bez přímého vztahu k objemu dat, což může být nákladově efektivnější.
- **Pokročilé analytické nástroje** a schopnost automatizovat časové osy incidentů.

LogRhythm

exabeam

COMGUARD

Současné IT výzvy pro společnosti

- End Point / Server protection & communication
- Protection on Business Services
- SecOps – Security and IT Operation Optimization
- Cloud and Hybrid Environment Security
- IoT – Industrial devices Security
- Compliance Achievement
- Facing the amount of Network Data to Analyze
- IT Security Team / SOC Efficiency
- Support new initiative reducing Risks
- Visibility, Measure and Report risks to ELT
- CyberSecurity Assurance *
- Spiraling Costs of Security Infrastructure
- Recruiting and Retaining Security Teams
- Reducing Blind Spot, anticipate attacks (APTs, Ransomware, Phishing …)

COMGUARD

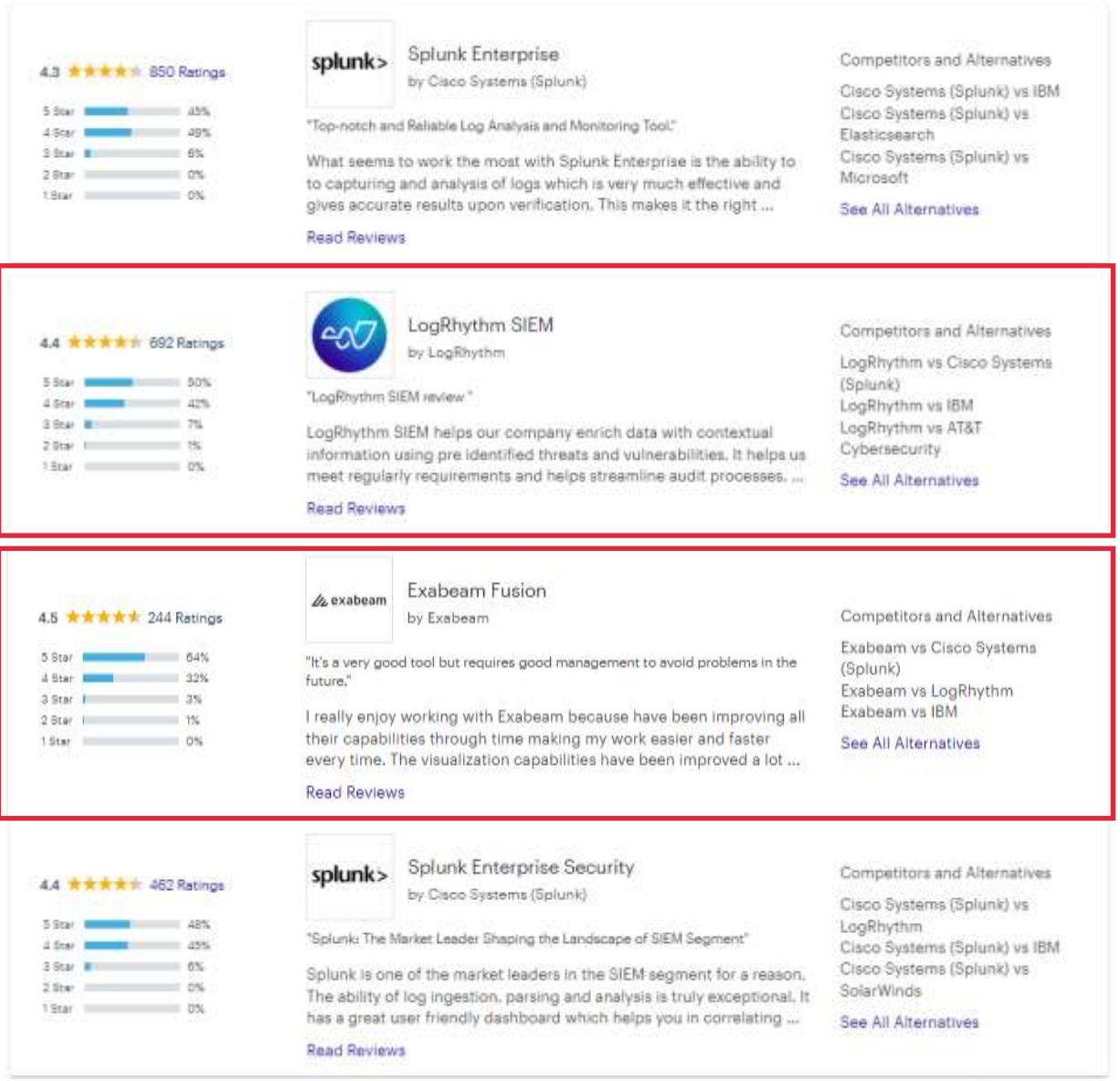
Nesourodá řešení zahlcují bezpečnostní týmy

COMGUARD

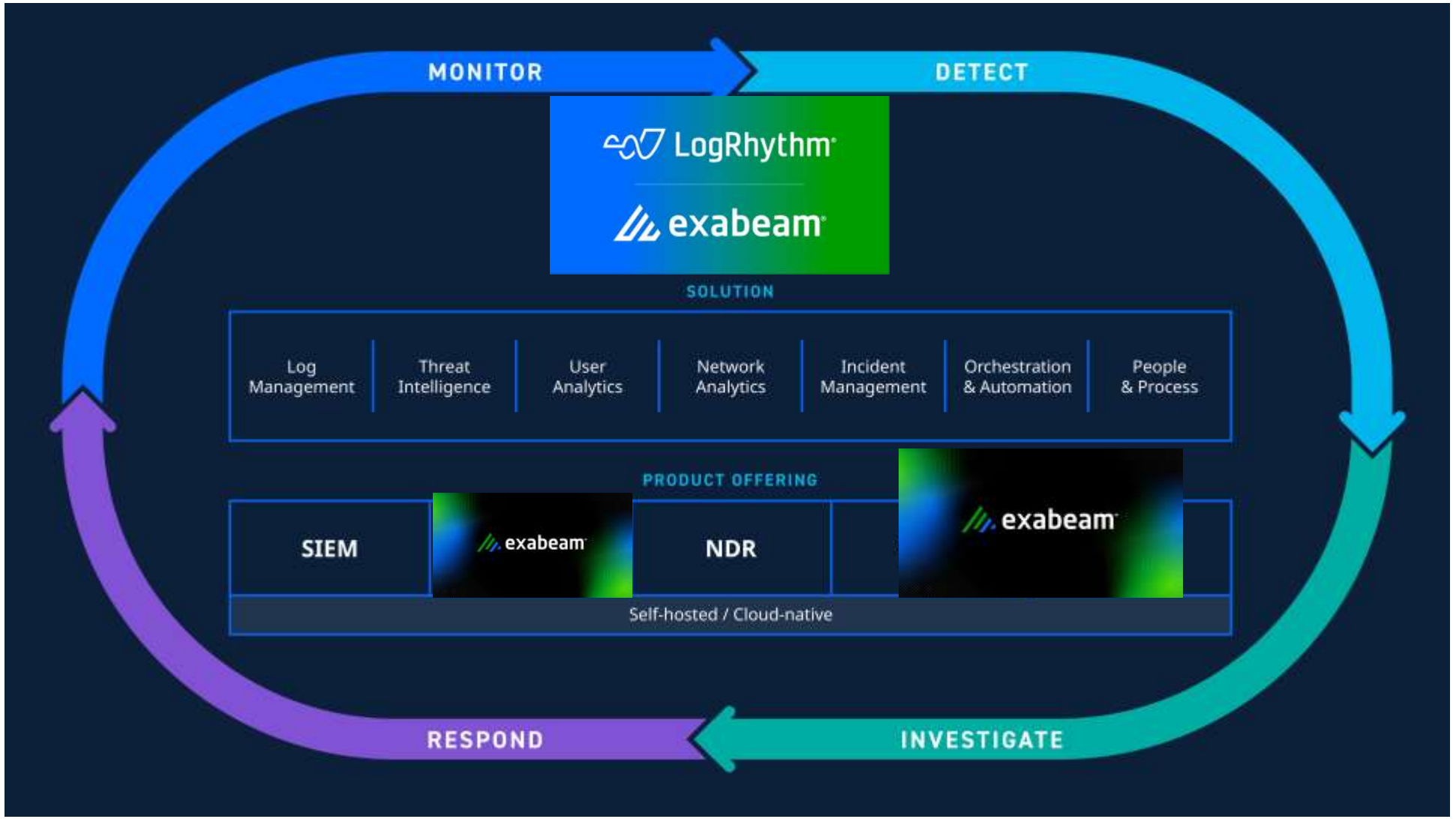
LogRhythm

exabeam

- Společnost založena v roce 2003/2
- Global Operations
  - USA, EMEA, APAC
- 7th generace SIEM
- Přes 4 tis. zákazníků



Exabeam Portfolio



Exabeam 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

LogRhythm
exabeam

Architektura Appliance

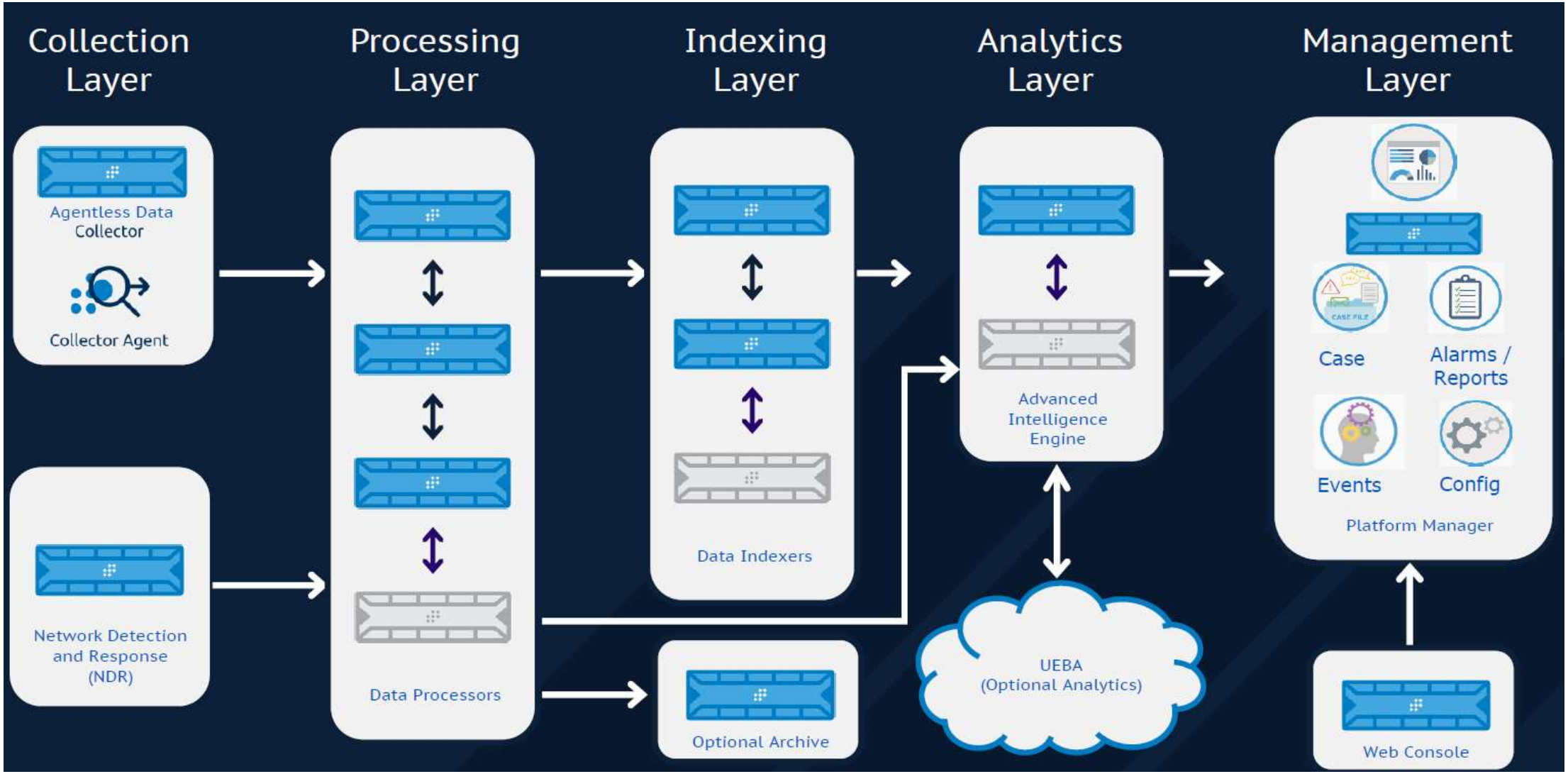
Dedikované Appliances /SW/VM

- Centralizovaný management
- Horizontální škálovatelnost
- Podpora pro distribuovaná prostředí

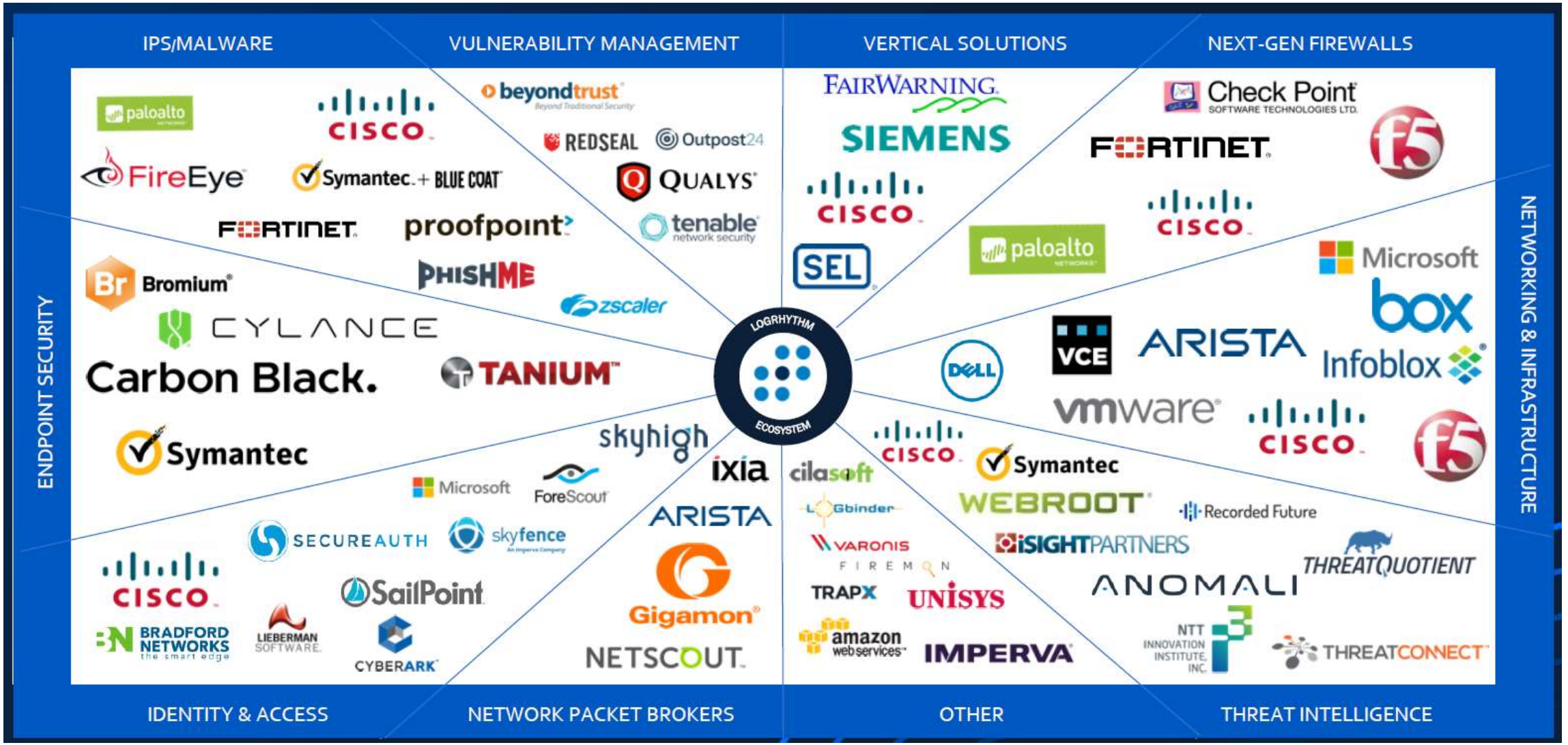
XM Single Appliance /SW/VM

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

LogRhythm SIEM – architektura



Technologičtí partneři



On-premise SIEM vs. Cloud SIEM

On-Prem SIEM

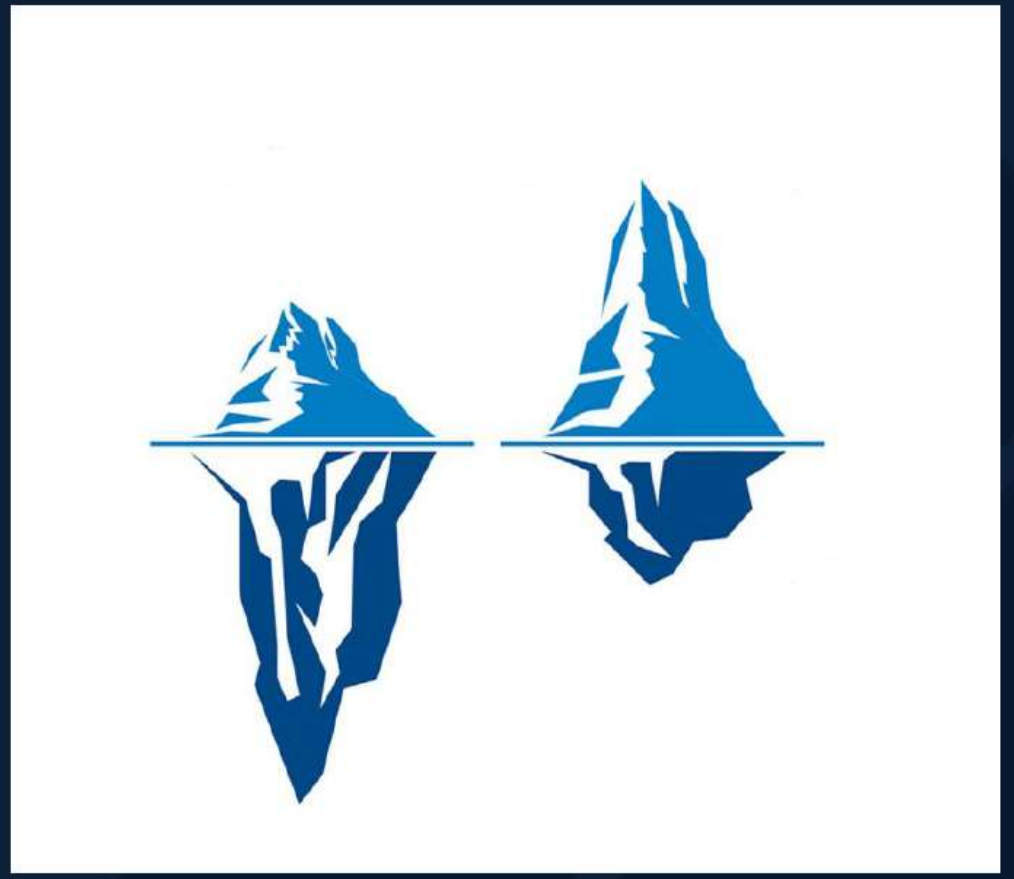
Software Licensing Cost

Platform Infrastructure Cost

Management & Maintenance Cost

Services Cost

Downtime



LogRhythm

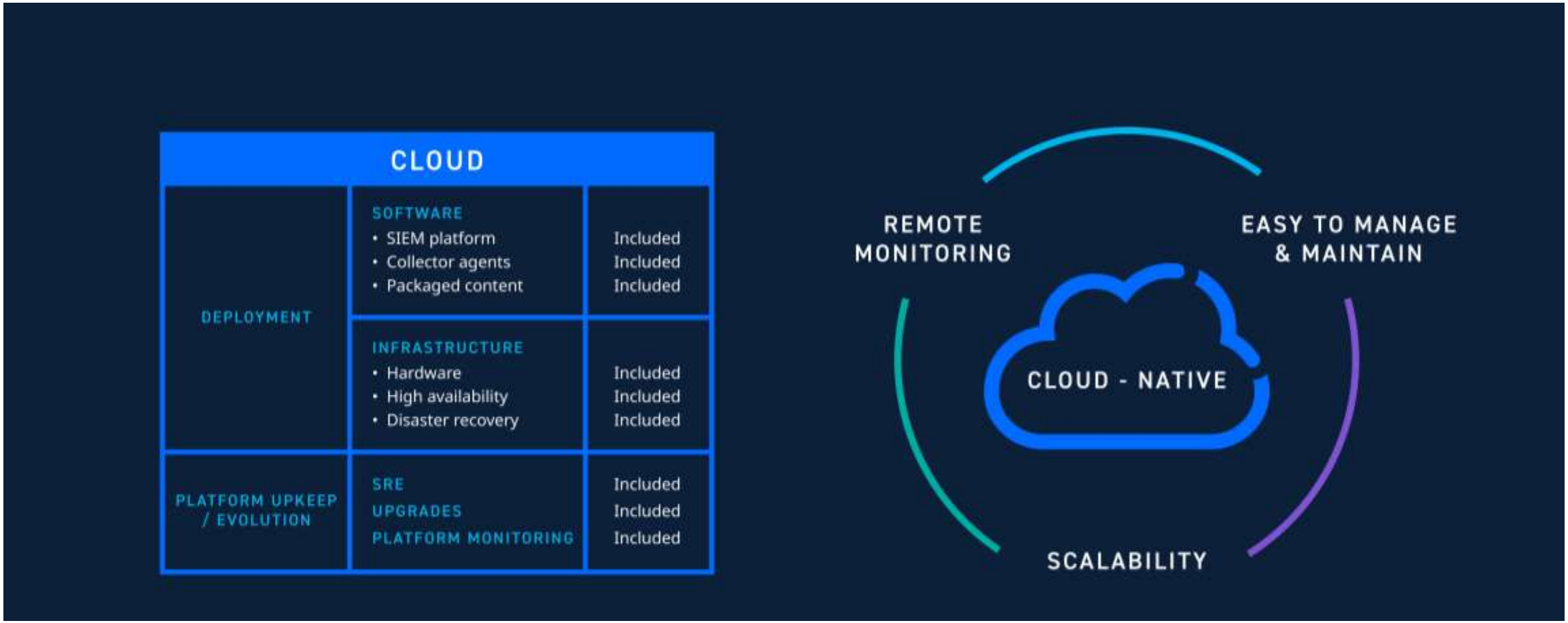
exabeam

Cloud

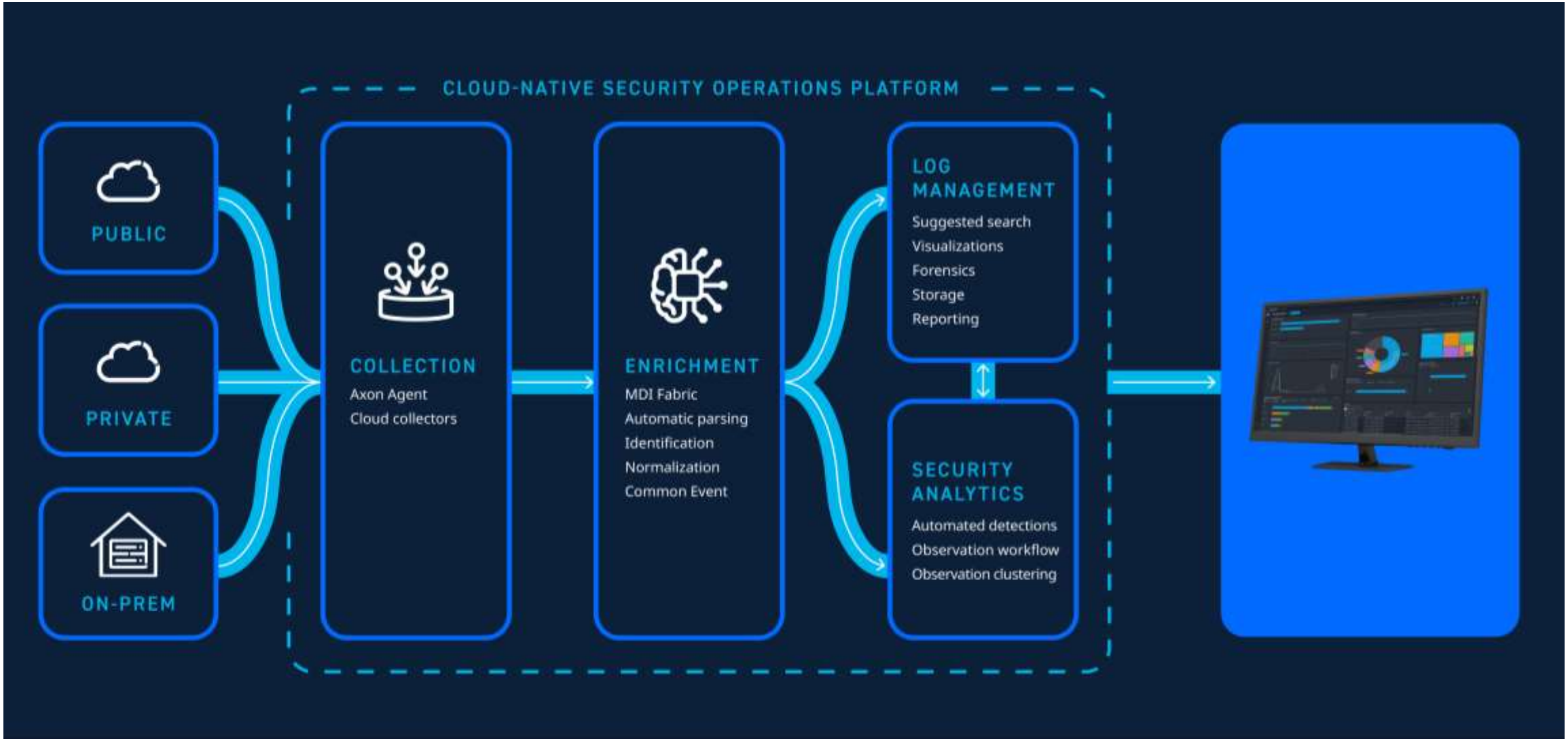
Subscription Cost

Implementation, Customization, & Training

Cloud-Native Saas Platform



Exabeam SaaS



CASE STUDY – pojišťovací společnost

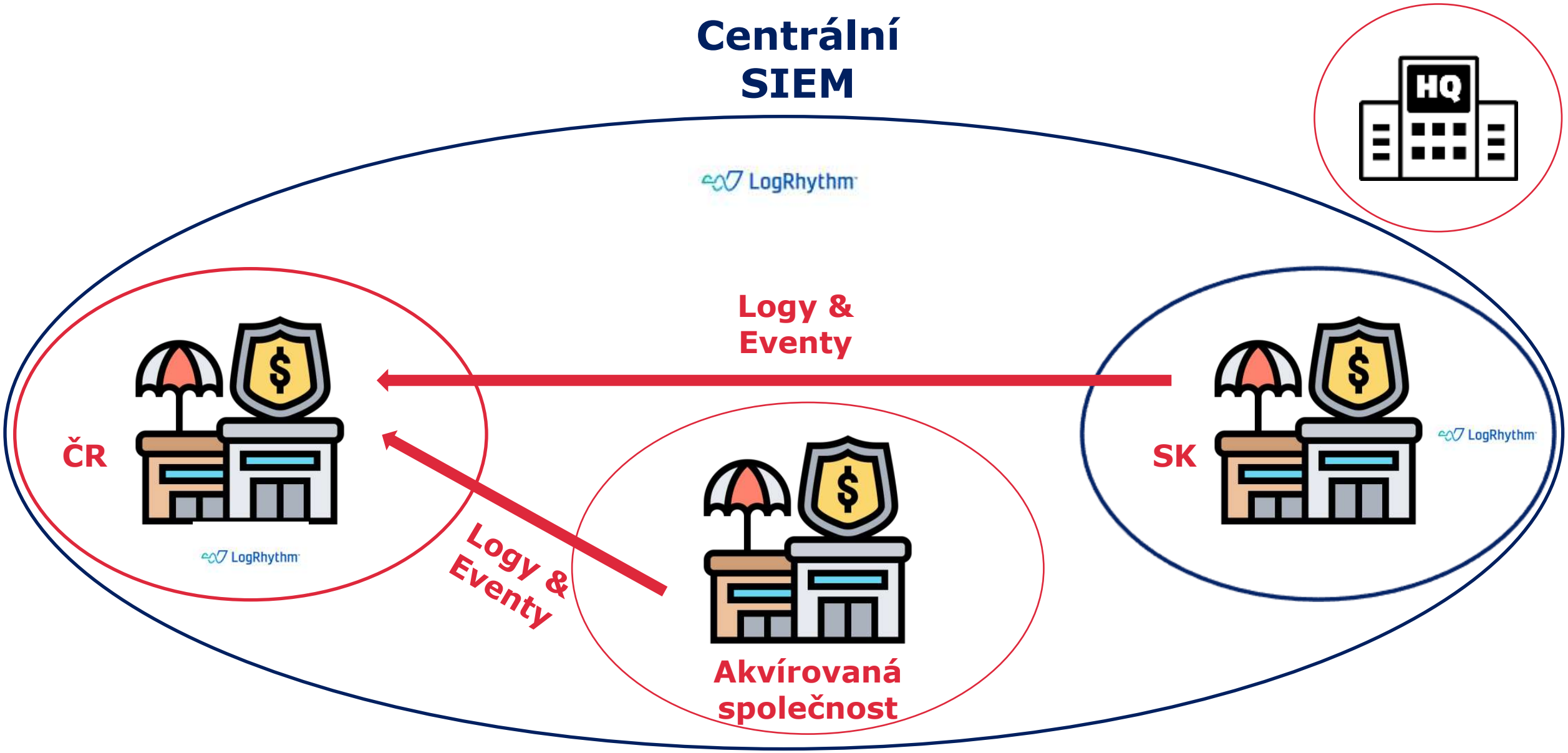
- Společnost je na trhu od roku 1993
- Působnost společnosti na 18 evropských trzích
- Velikost společnosti:
  - 22 000 pracovníků
  - 15 mil. klientů (3 mil. klientů v ČR a SK)

Stěžejní změny ve společnosti:

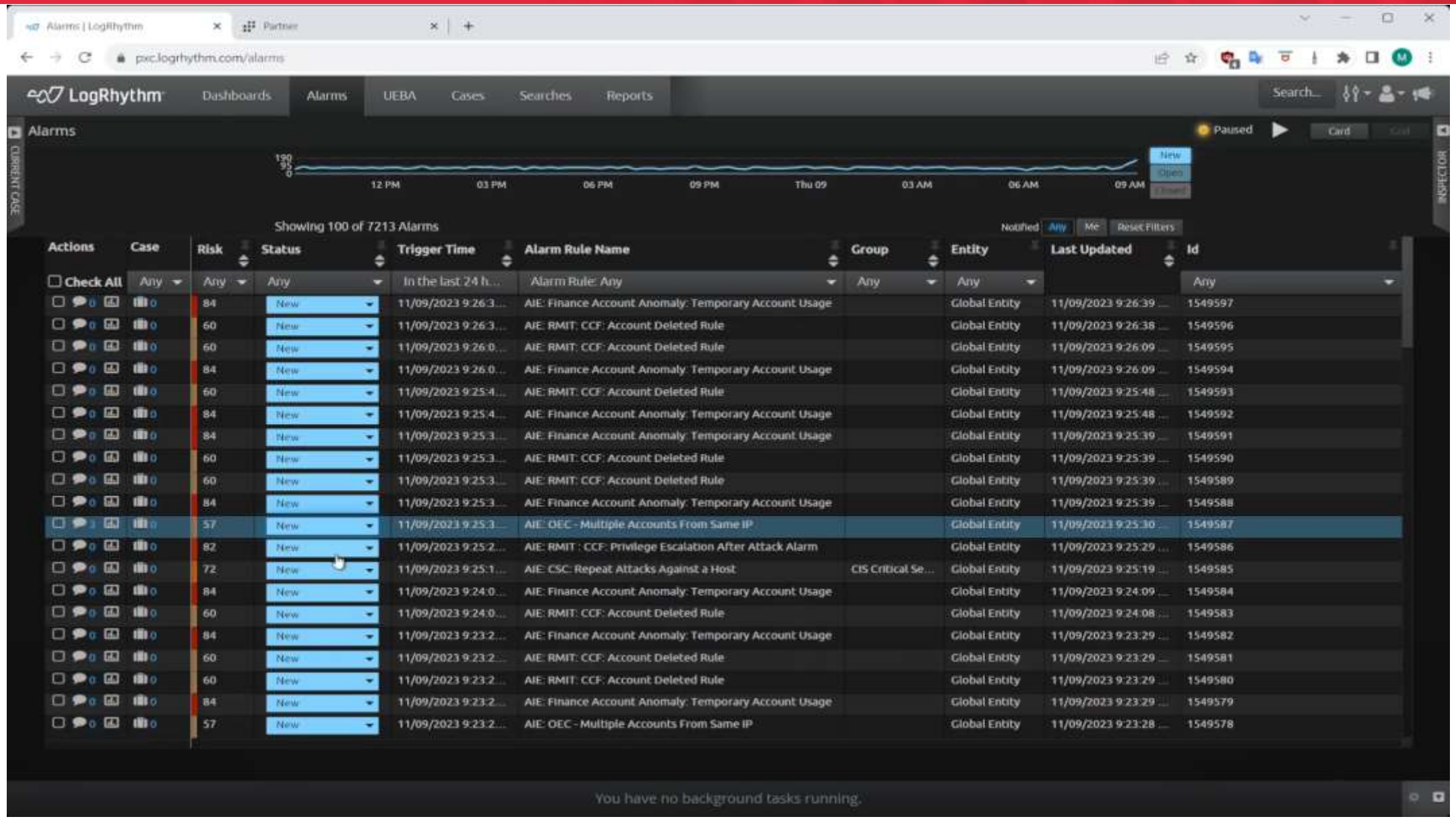
- Říjen 2020 – akvizice další pojišťovací společnosti a rozšíření produktů a služeb

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
HQ
LogRhythm
Logy &
Eventy
ČR
LogRhythm
Logy &
Eventy
Akvírovaná
společnost
SK
LogRhythm

COMGUARD


Alarms | LogRhythm
Partner
pxc.logrhythm.com/alarms
LogRhythm
Dashboards
Alarms
UEBA
Cases
Searches
Reports
Search...
Alarms
Paused
Card
12 PM
03 PM
06 PM
09 PM
Thu 09
03 AM
06 AM
09 AM
New
Open
Closed
Showing 100 of 7213 Alarms
Notified
Any
Me
Reset Filters
Actions
Case
Risk
Status
Trigger Time
Alarm Rule Name
Group
Entity
Last Updated
Id
Check All
Any
In the last 24 h...
Alarm Rule: Any
Global Entity
11/09/2023 9:26:39
1549597
11/09/2023 9:26:38
1549596
11/09/2023 9:26:09
1549595
11/09/2023 9:25:48
1549593
11/09/2023 9:25:39
1549591
11/09/2023 9:25:30
1549587
11/09/2023 9:25:29
1549586
11/09/2023 9:25:19
1549585
11/09/2023 9:24:09
1549584
11/09/2023 9:24:08
1549583
11/09/2023 9:23:29
1549582
11/09/2023 9:23:28
1549578
AIE: Finance Account Anomaly: Temporary Account Usage
AIE: RMIT: CCF: Account Deleted Rule
AIE: OEC - Multiple Accounts From Same IP
AIE: RMIT : CCF: Privilege Escalation After Attack Alarm
AIE: CSC: Repeat Attacks Against a Host
CIS Critical Se...
You have no background tasks running.

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