

**COMGUARD**  
communication security



# LogRhythm – Získejte detailní přehled o dění ve Vaší IT

Roman Jiráček, Account & Vendor Manager

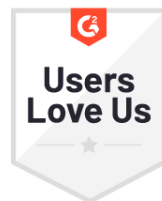
 LogRhythm™

# Agenda prezentace

- Představení společnosti – LogRhythm
- LogRhythm SIEM a NDR
- Klíčové vlastnosti LogRhythm
- USE CASE – nasazení technologie v pojišťovací společnosti
- Přínosy technologie pro tuto společnost



- Společnost založena v roce 2003
- Global Operations
  - USA, EMEA, APAC
- 7<sup>th</sup> generace SIEM
- Dlouhodobý LEADER v SIEM řešeních



**SC Awards Winner**

Certifications & Validations

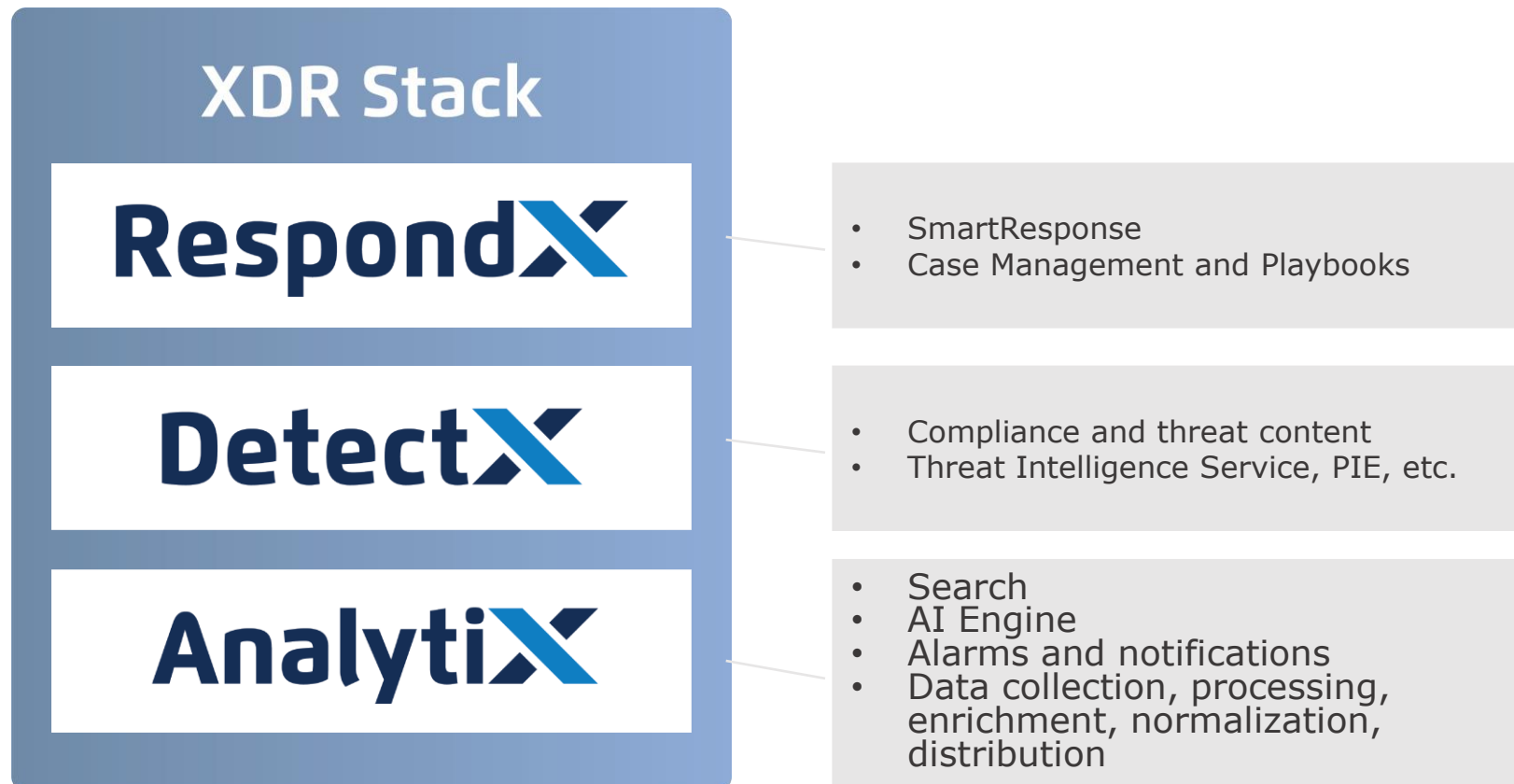
ONC Certified HIT

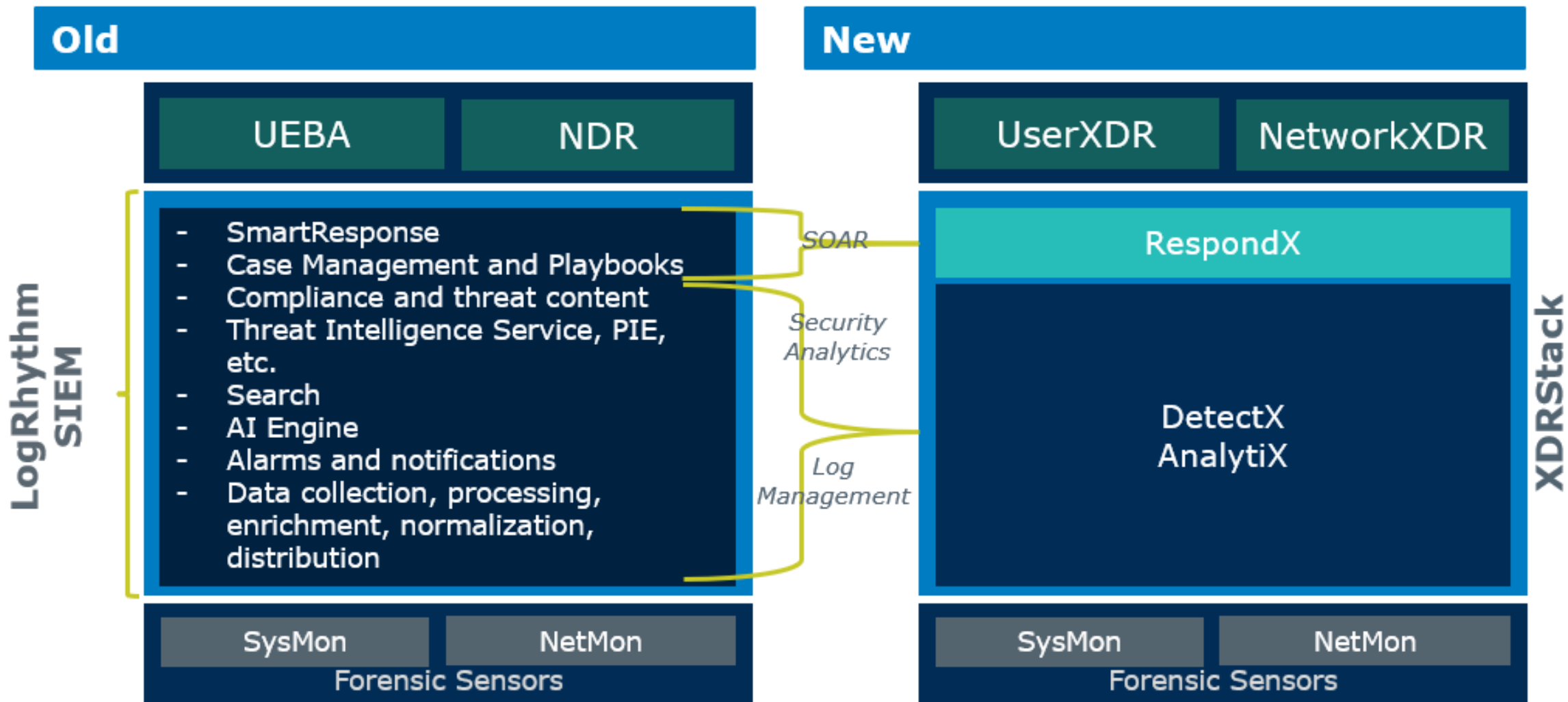
**Gartner visionář pro SIEM řešení od roku 2007 a lídr trhu od roku 2012!**



Source: Gartner (June 2021)

# Nezbytné prvky LogRhythm SIEM





Capabilities	AnalytiX	DetectX	RespondX	UserXDR	NetworkXDR
Machine Data Collection	X	I		I	I
Machine Data Processing, Enrichment, Distribution	X	I		I	I
Core Search Analytics (Dashboards, Analysis, Reporting)	X	I		I	I
Core Machine Analytics (AI Engine)	X	I		I	I
Alarm and Notification Workflow	X	I		I	I
LogRhythm supported ELM "apps" (e.g., Kibana)	X	I		I	I
Core Compliance Content (CCF mod, PCI Mod, etc.)		X		I	I
Core Threat Content (Core Threat Module, MITRE Module, etc.)		X		I	I
LogRhythm supported ESA "apps" (e.g., PIE)		X		I	I
Threat Intelligence Service		X		I	I
Case Management			X	I	I
SmartResponse			X	I	I
Playbooks			X	I	I
SOAR Roadmap			X	I	I



# Současné problémy v IT bezpečnosti

- **Rozšiřující se vektory útoků:**
  - Multi-cloud, hybridní infrastruktury, BYOD
- **Útoky, které jednoduše obcházejí starší technologie**
  - Bezpečnostní mezery v koncových bodech, sítích a cloudu
- **Nedostatek analytiků v IT bezpečnosti**
  - Pouze pro odborníky – pro některé jedince forma „černé magie“
- **Vylepšení schopností útočníků**
  - Útočníci využívají stále složitější techniky

17  
tis.

Celkový počet alertů  
za týden

96%

Procento alertů, které  
nejsou daný týden  
prozkoumány

14%

Procento incidentů,  
které nespustí  
upozornění

# Proč je nutná NDR technologie?

## Sít'ová data často poskytují nejčastější indikátory kompromitace IT infrastruktury

- Odstranění slepých míst v infrastruktuře s pomocí strojového učení a NDR založeného na definovaných pravidlech
- Minimalizace Mean Time to Repair (MTTR)
- Snížení provozních nákladů – v případě snadného škálování
- Efektivní ochrana datového centra a cloudu pomocí detekce v reálném čase



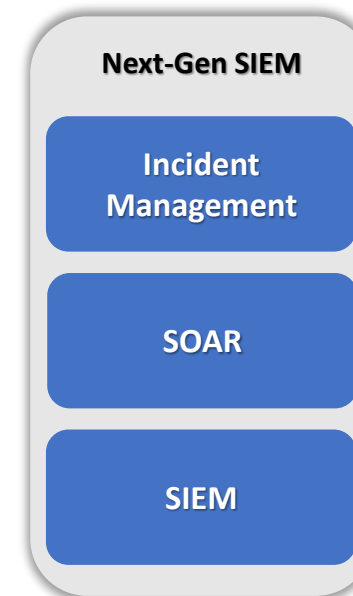
# Flexibilní reakce na incidenty

NetworkXDR jako **samostatná bezpečnostní platforma** nebo jako **senzor pro širší bezpečnostní strategii**



**Standalone**

Schopnost zvládat incidenty včetně souběžného vyhledávání, správy jednotlivých případů a schopnosti reagovat na síti



**se SIEM**

Obousměrná integrace využívá pokročilé funkce Incident Managementu, SOAR a SIEM.

# Typické nasazení technologie

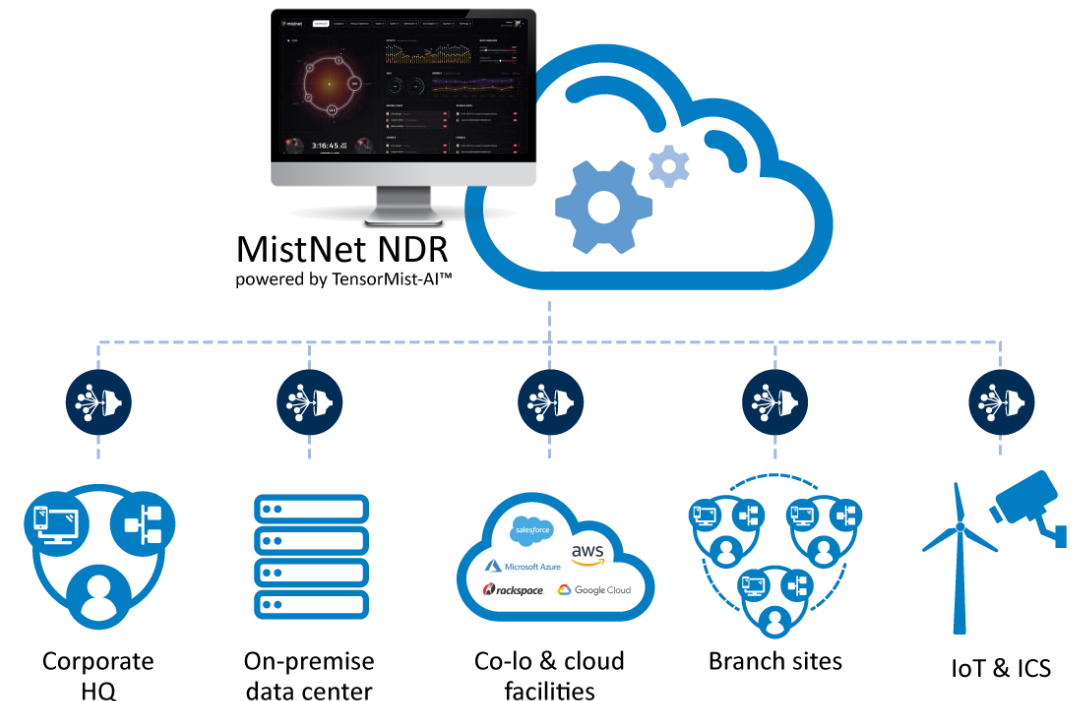
Detekce a odezva na hrozby v cloudu a datovém centru, která využívá škálování a výkon pomocí speciálních výpočtů

## Cloud Front-End:

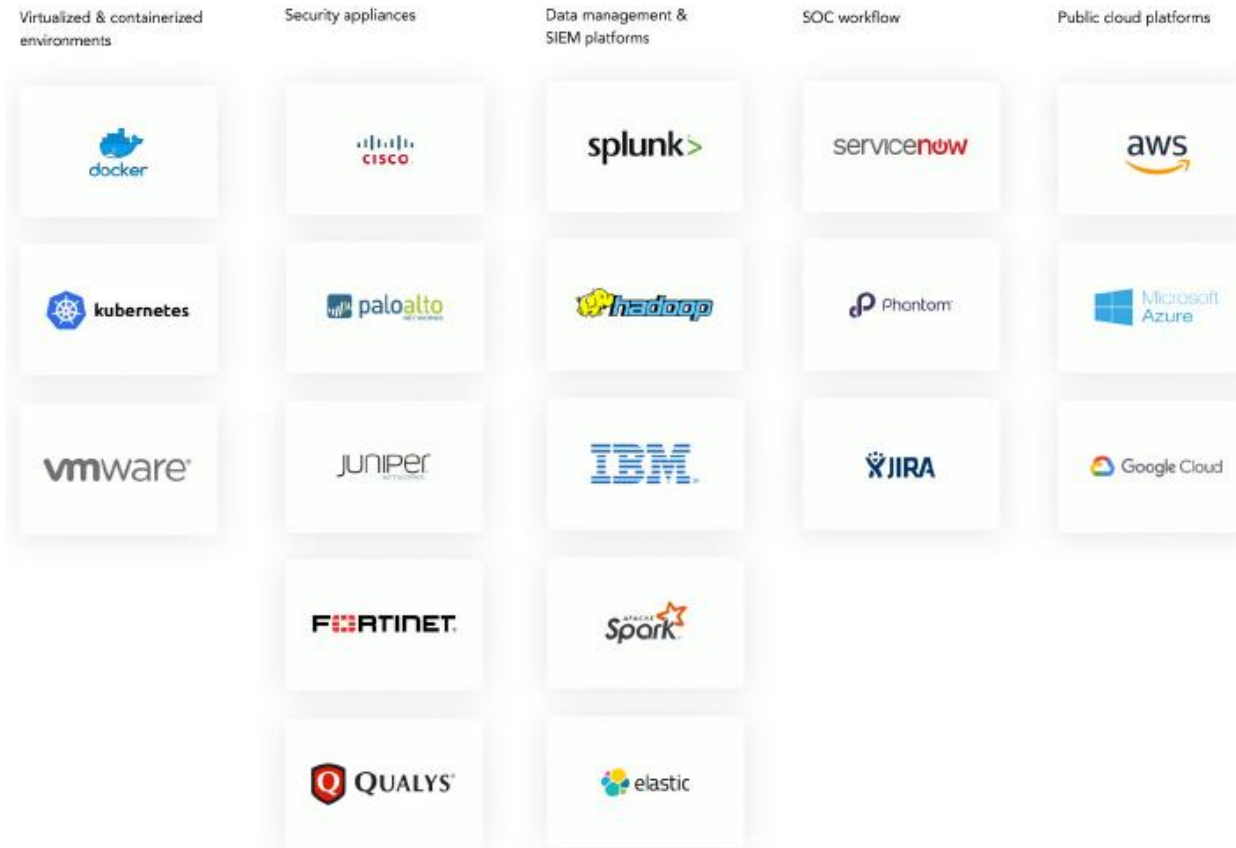
- Public nebo privátní cloud
- Analýza v reálném čase i retrospektivně
- Integrace se službou Active Directory
- Patentované detekční algoritmy
- Rozšířená architektura uložení

## Kolektor/Analytický Node

- Virtuální nebo HW Appliance
- Zachycování metadat SecOps
- Streamování analýzy a strojového učení



# Jednoduchá integrace s dalšími technologiemi





# 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.**



## Výchozí stav u zákazníka – organizace fungovaly separátně:

- **Mateřská společnost** – využívá konkurenční řešení
- **Česká pobočka zákazníka** – využívala konkurenční řešení, se kterým byla spokojena
  - **Benefity** – granulární reporty z této technologie
  - **Negativa** – složitá integrace Windows zařízení
- **Slovenská pobočka zákazníka** – využívala technologii LogRhythm

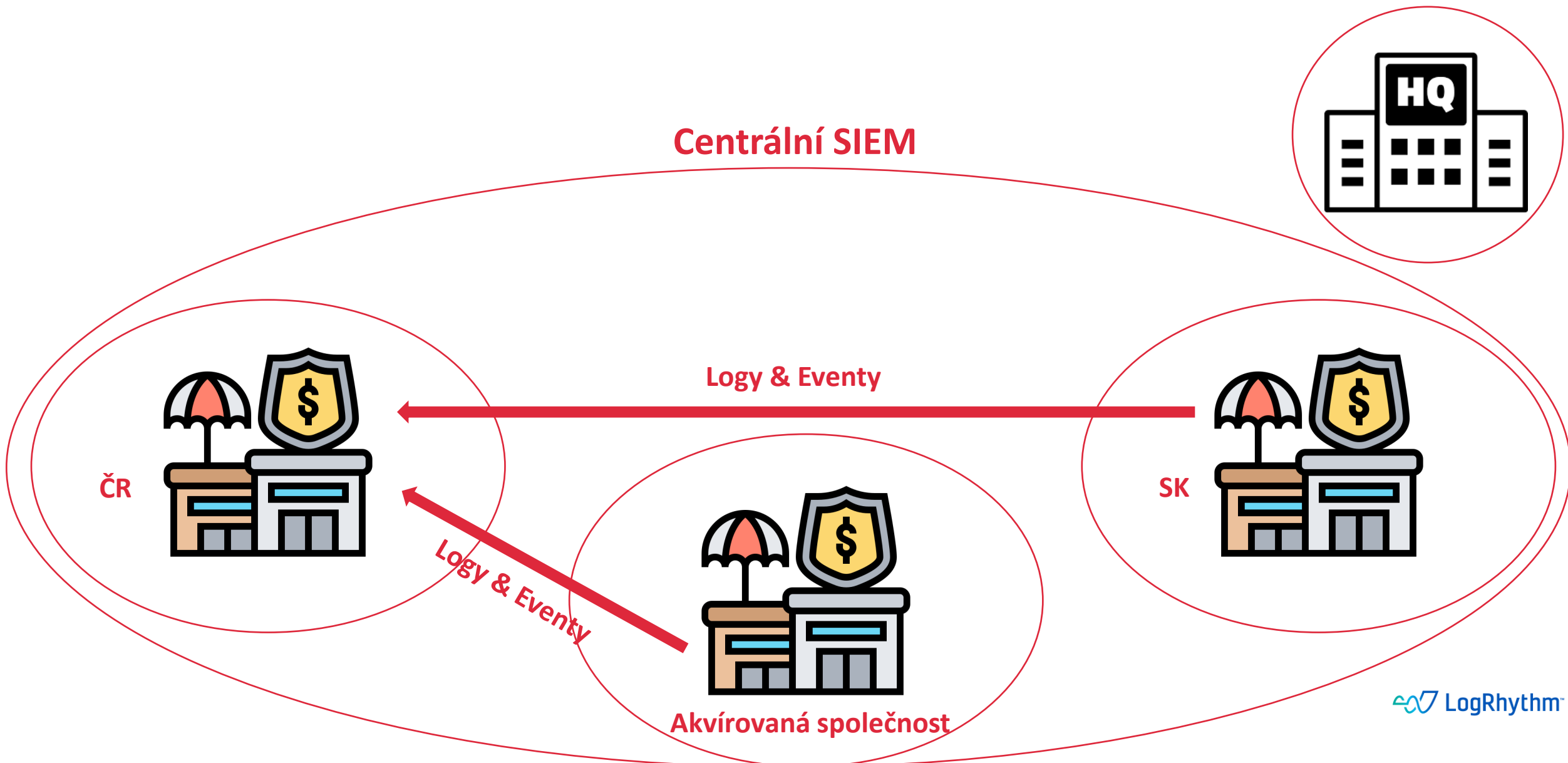
## Změna Security Managera – došlo k reorganizaci celé IT infrastruktury a vztahů v organizaci

- Konkurenční řešení na české pobočce muselo být vyměněno – začala se řešit pre-sales část na LogRhythm s partnerem
- ČR – nasazení LogRhythm SIEM

## Akvizice další pojišťovací společnosti – integrace jednotlivých subjektů pod jednu „značku“

- Vybudování centrály v Praze = integrace IT infrastruktury do ČR
  - Vyšší požadavky na SIEM deployment (Navýšení MPS = vyšší výkon HW Appliance + HA cluster)







# 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



# 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**
  - Forezní 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

# Klíčové vlastnosti



- Nezávislá forenzní analýza koncových zařízení a File Integrity Monitoring
- Forenzní analýza sítě vč. „Application ID“ a „Full Packet Capture“
- V ceně je již zahrnut GDPR modul pro snadnější dosažení/kontrolu shody s GDPR
- Pokročilá korelace a rozpoznání vzorků (pattern)
- Vícerozměrné analýzy a detekce anomálií chování na úrovni uživatele, sítě i koncových zařízení
- Rychlé a inteligentní vyhledávání
- Analýzy velkých objemů dat, jejich vizualizace, procházení k detailnějším vrstvám
- Automatické odezvy dle workflow – díky unikátní technologii SmartResponse™
- Integrovaný „Case Management“
- Jednoduchá škálovatelnost – lze rozšířit MPS pomocí software upgrade
- Možnost rozšíření o řadu dalších modulů (SOAR, NDR, CloudAI, UEBA, ..)

**COMGUARD**  
communication security



**Děkujeme za pozornost!**

**Přednášková část je nyní u konce.**

**Dotazy?**



**COMGUARD**  
communication security



**TOMBOLA**

**Hodně štěstí!**