

# COMMGUARD

cyber security masters

# Exabeam

**Security Operations Center: Proč nepodcenit rostoucí trend**

Roman Jiráček, Senior Account & Vendor Manager

20.09.2024

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

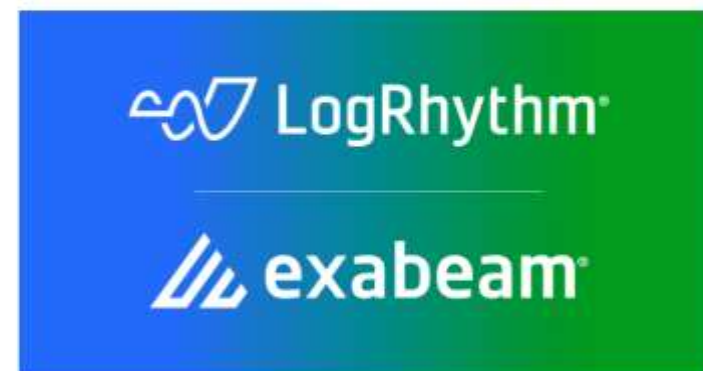
### Recent Press Releases

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



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)***

- 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.

The logo for LogRhythm, featuring a stylized white icon of a pulse or waveform on a blue background, followed by the text "LogRhythm" in white.The logo for Exebeam, featuring a stylized white icon of three slanted bars on a green background, followed by the text "exebeam" in white.



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 ... )

## Nesourodá řešení zahltují bezpečnostní týmy



# COMGUARD

LogRhythm

exabeam

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

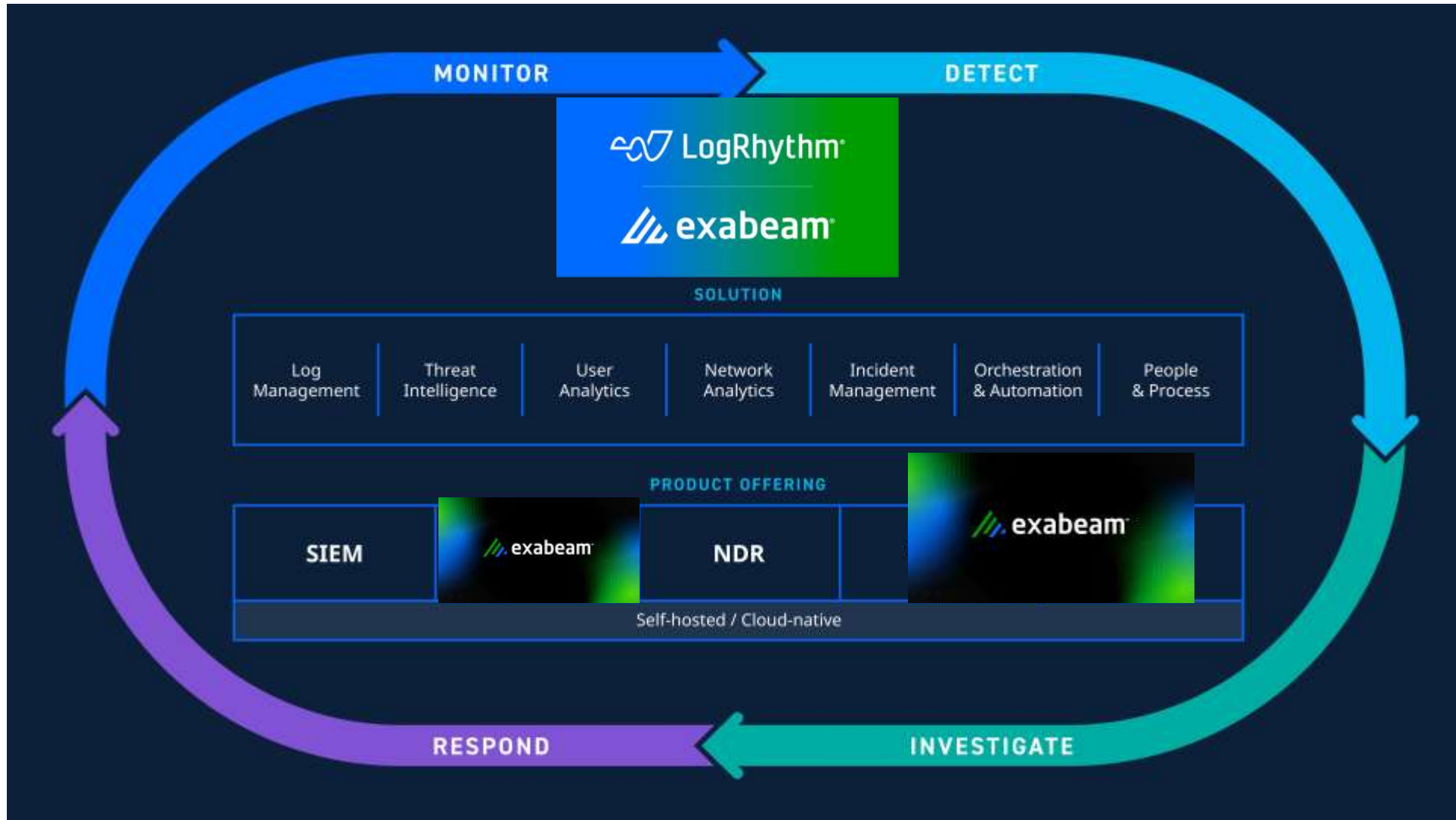


## Certifications & Validations



ONC.Certified

|   |  |  |
|---|--|--|
| <p>4.3 ★★★★★ 850 Ratings</p> <p>5 Star 45%</p> <p>4 Star 49%</p> <p>3 Star 6%</p> <p>2 Star 0%</p> <p>1 Star 0%</p> | <p><b>splunk</b> Splunk Enterprise<br/>by Cisco Systems (Splunk)</p> <p>"Top-notch and Reliable Log Analysis and Monitoring Tool"</p> <p>What seems to work the most with Splunk Enterprise is the ability to capture and analyze logs which is very much effective and gives accurate results upon verification. This makes it the right ...</p> <p><a href="#">Read Reviews</a></p>                                      | <p>Competitors and Alternatives</p> <p>Cisco Systems (Splunk) vs IBM</p> <p>Cisco Systems (Splunk) vs Elasticsearch</p> <p>Cisco Systems (Splunk) vs Microsoft</p> <p><a href="#">See All Alternatives</a></p> |
| <p>4.4 ★★★★★ 692 Ratings</p> <p>5 Star 50%</p> <p>4 Star 42%</p> <p>3 Star 7%</p> <p>2 Star 1%</p> <p>1 Star 0%</p> | <p><b>LogRhythm</b> LogRhythm SIEM<br/>by LogRhythm</p> <p>"LogRhythm SIEM review"</p> <p>LogRhythm SIEM helps our company enrich data with contextual information using pre-identified threats and vulnerabilities. It helps us meet regularly requirements and helps streamline audit processes. ...</p> <p><a href="#">Read Reviews</a></p>   | <p>Competitors and Alternatives</p> <p>LogRhythm vs Cisco Systems (Splunk)</p> <p>LogRhythm vs IBM</p> <p>LogRhythm vs AT&amp;T Cybersecurity</p> <p><a href="#">See All Alternatives</a></p>                  |
| <p>4.5 ★★★★★ 244 Ratings</p> <p>5 Star 64%</p> <p>4 Star 32%</p> <p>3 Star 3%</p> <p>2 Star 1%</p> <p>1 Star 0%</p> | <p><b>exabeam</b> Exabeam Fusion<br/>by Exabeam</p> <p>"It's a very good tool but requires good management to avoid problems in the future."</p> <p>I really enjoy working with Exabeam because have been improving all their capabilities through time making my work easier and faster every time. The visualization capabilities have been improved a lot ...</p> <p><a href="#">Read Reviews</a></p>                   | <p>Competitors and Alternatives</p> <p>Exabeam vs Cisco Systems (Splunk)</p> <p>Exabeam vs LogRhythm</p> <p>Exabeam vs IBM</p> <p><a href="#">See All Alternatives</a></p>                                     |
| <p>4.4 ★★★★★ 462 Ratings</p> <p>5 Star 48%</p> <p>4 Star 45%</p> <p>3 Star 6%</p> <p>2 Star 0%</p> <p>1 Star 0%</p> | <p><b>splunk</b> Splunk Enterprise Security<br/>by Cisco Systems (Splunk)</p> <p>"Splunk: The Market Leader Shaping the Landscape of SIEM Segment"</p> <p>Splunk is one of the market leaders in the SIEM segment for a reason. The ability of log ingestion, parsing and analysis is truly exceptional. It has a great user-friendly dashboard which helps you in correlating ...</p> <p><a href="#">Read Reviews</a></p> | <p>Competitors and Alternatives</p> <p>Cisco Systems (Splunk) vs LogRhythm</p> <p>Cisco Systems (Splunk) vs IBM</p> <p>Cisco Systems (Splunk) vs SolarWinds</p> <p><a href="#">See All Alternatives</a></p>    |



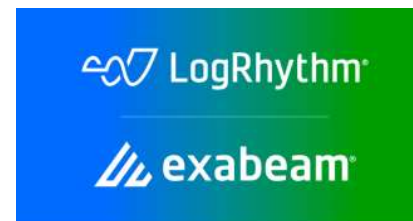
# Exabeam SIEM / NDR | SOC Visibility Triad

## 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





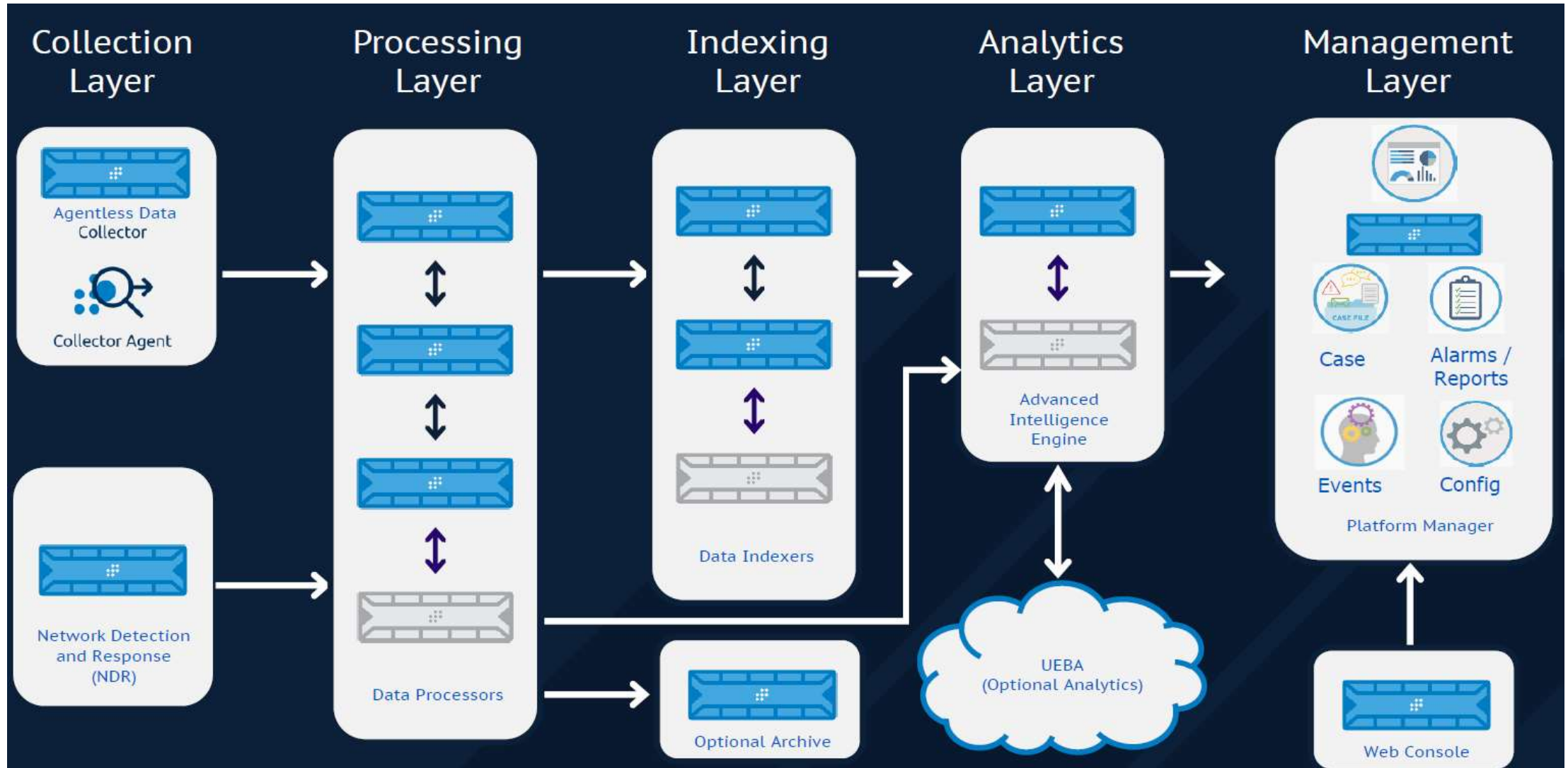
### Dedikované Appliances /SW/VM

- Centralizovaný management
- Horizontální škálovatelnost
- Podpora pro distribuovaná prostředí

### XM Single Appliance /SW/VM

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

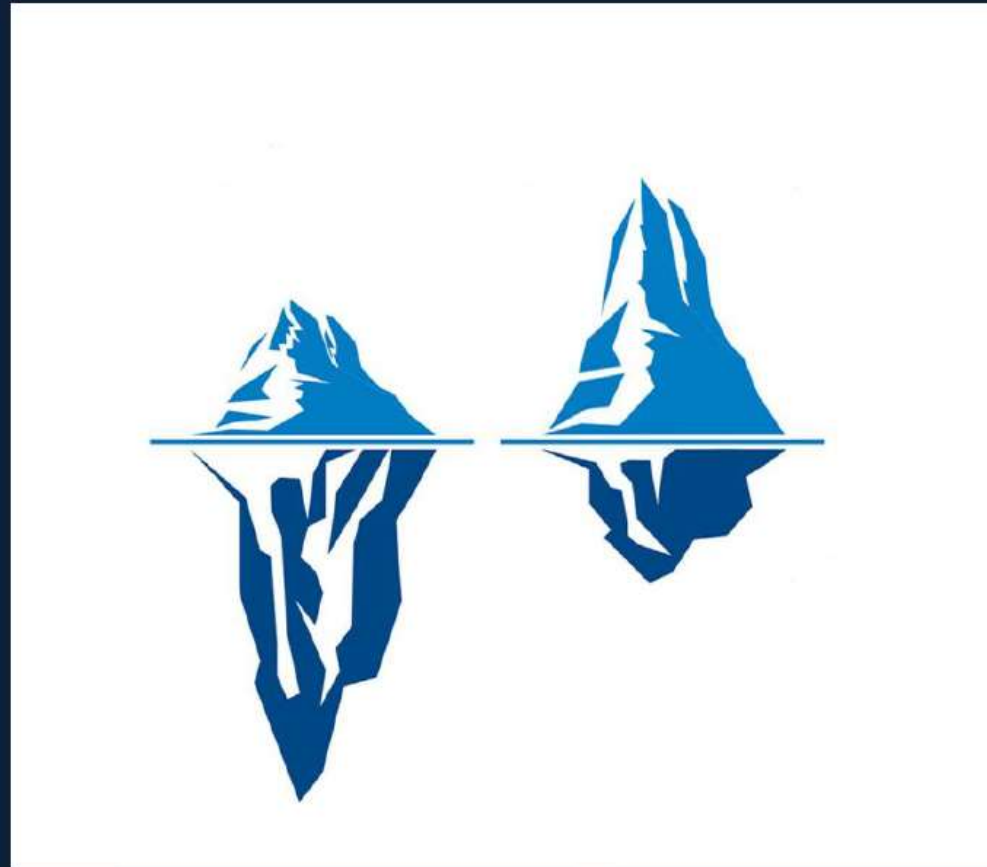






## On-Prem SIEM

- Software Licensing Cost
- Platform Infrastructure Cost
- Management & Maintenance Cost
- Services Cost
- Downtime



LogRhythm

exabeam

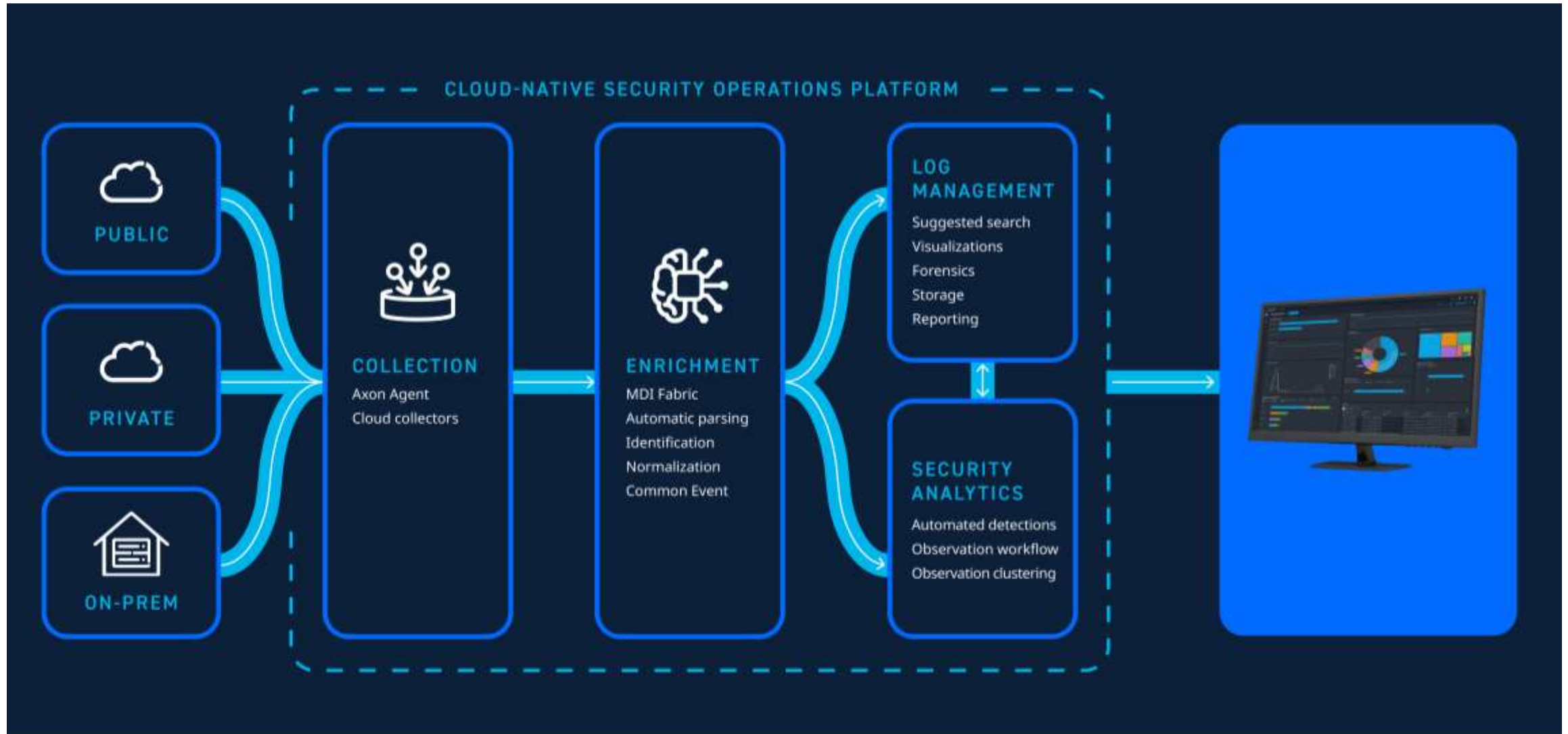
## Cloud

- Subscription Cost
- Implementation, Customization, & Training

# Cloud-Native SaaS Platform

| CLOUD                       |  |                                  |
|-----------------------------|--|----------------------------------|
| DEPLOYMENT                  | <b>SOFTWARE</b> <ul style="list-style-type: none"><li>• SIEM platform</li><li>• Collector agents</li><li>• Packaged content</li></ul>    | Included<br>Included<br>Included |
|                             | <b>INFRASTRUCTURE</b> <ul style="list-style-type: none"><li>• Hardware</li><li>• High availability</li><li>• Disaster recovery</li></ul> | Included<br>Included<br>Included |
| PLATFORM UPKEEP / EVOLUTION | <b>SRE</b><br><b>UPGRADES</b><br><b>PLATFORM MONITORING</b>  | Included<br>Included<br>Included |





## 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

SK



LogRhythm

Logy & Eventy



Akvírovaná společnost



The screenshot displays the LogRhythm Alarms interface. At the top, there is a navigation bar with tabs for Dashboards, Alarms, UEBA, Cases, Searches, and Reports. A search bar is located on the right. Below the navigation bar, there is a status bar showing 'Paused' and a 'Card' view selector. A line graph at the top shows alarm activity over time, with a peak around 12 PM. Below the graph, a table displays a list of 100 alarms. The table has the following columns: Actions, Case, Risk, Status, Trigger Time, Alarm Rule Name, Group, Entity, Last Updated, and Id. The 'Status' column for all visible alarms is 'New'. The 'Alarm Rule Name' column contains various rules such as 'AIE: Finance Account Anomaly: Temporary Account Usage', 'AIE: RMIT: CCF: Account Deleted Rule', and 'AIE: OEC - Multiple Accounts From Same IP'. The 'Entity' column for all visible alarms is 'Global Entity'. The 'Last Updated' column shows timestamps from 11/09/2023 9:23:28 to 11/09/2023 9:26:39. The 'Id' column shows numerical values ranging from 1549578 to 1549597. At the bottom of the interface, a message states 'You have no background tasks running.'

| Actions                            | Case | Risk | Status | Trigger Time         | Alarm Rule Name   | Group              | Entity        | Last Updated           | Id      |
|------------------------------------|------|------|--------|----------------------|---|--------------------|---------------|------------------------|---------|
| <input type="checkbox"/> Check All | Any  | Any  | Any    | In the last 24 h...  | Alarm Rule: Any   | Any                | Any           |                        | Any     |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:26:3... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:26:39 ... | 1549597 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:26:3... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:26:38 ... | 1549596 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:26:0... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:26:09 ... | 1549595 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:26:0... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:26:09 ... | 1549594 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:25:4... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:25:48 ... | 1549593 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:25:4... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:25:48 ... | 1549592 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:25:3... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:25:39 ... | 1549591 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:25:3... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:25:39 ... | 1549590 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:25:3... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:25:39 ... | 1549589 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:25:3... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:25:39 ... | 1549588 |
| <input type="checkbox"/>           |      | 57   | New    | 11/09/2023 9:25:3... | AIE: OEC - Multiple Accounts From Same IP               |                    | Global Entity | 11/09/2023 9:25:30 ... | 1549587 |
| <input type="checkbox"/>           |      | 82   | New    | 11/09/2023 9:25:2... | AIE: RMIT: CCF: Privilege Escalation After Attack Alarm |                    | Global Entity | 11/09/2023 9:25:29 ... | 1549586 |
| <input type="checkbox"/>           |      | 72   | New    | 11/09/2023 9:25:1... | AIE: CSC: Repeat Attacks Against a Host                 | CIS Critical Se... | Global Entity | 11/09/2023 9:25:19 ... | 1549585 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:24:0... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:24:09 ... | 1549584 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:24:0... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:24:08 ... | 1549583 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:23:2... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:23:29 ... | 1549582 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:23:2... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:23:29 ... | 1549581 |
| <input type="checkbox"/>           |      | 60   | New    | 11/09/2023 9:23:2... | AIE: RMIT: CCF: Account Deleted Rule                    |                    | Global Entity | 11/09/2023 9:23:29 ... | 1549580 |
| <input type="checkbox"/>           |      | 84   | New    | 11/09/2023 9:23:2... | AIE: Finance Account Anomaly: Temporary Account Usage   |                    | Global Entity | 11/09/2023 9:23:29 ... | 1549579 |
| <input type="checkbox"/>           |      | 57   | New    | 11/09/2023 9:23:2... | AIE: OEC - Multiple Accounts From Same IP               |                    | Global Entity | 11/09/2023 9:23:28 ... | 1549578 |

## 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](mailto:roman.jiracek@comguard.cz)**