

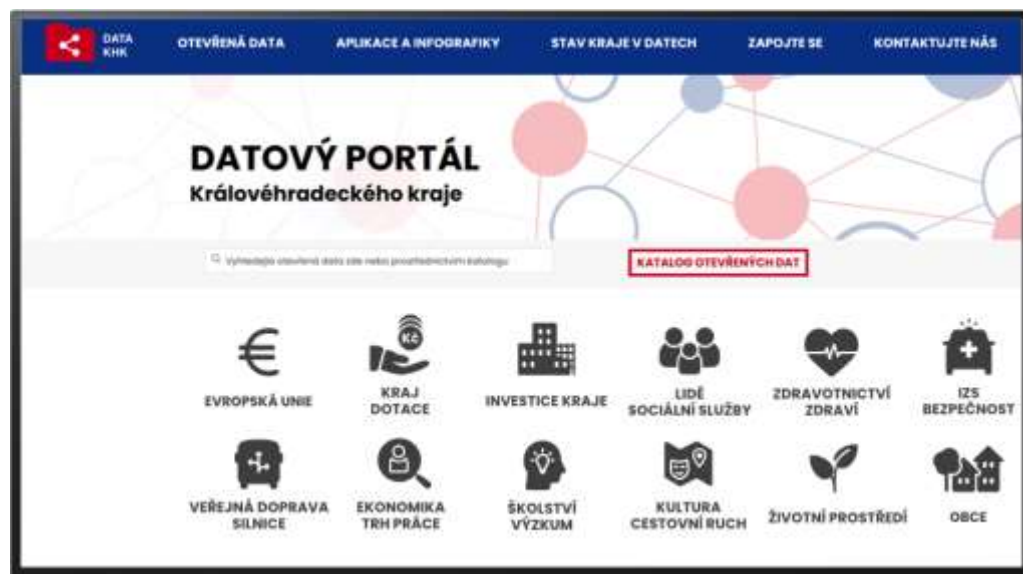
# BEZPEČNOST OTEVŘENÝCH DAT PRO SMART CITY

RADMILA VELNEROVÁ – KRÁLOVÉHRADECKÝ KRAJ

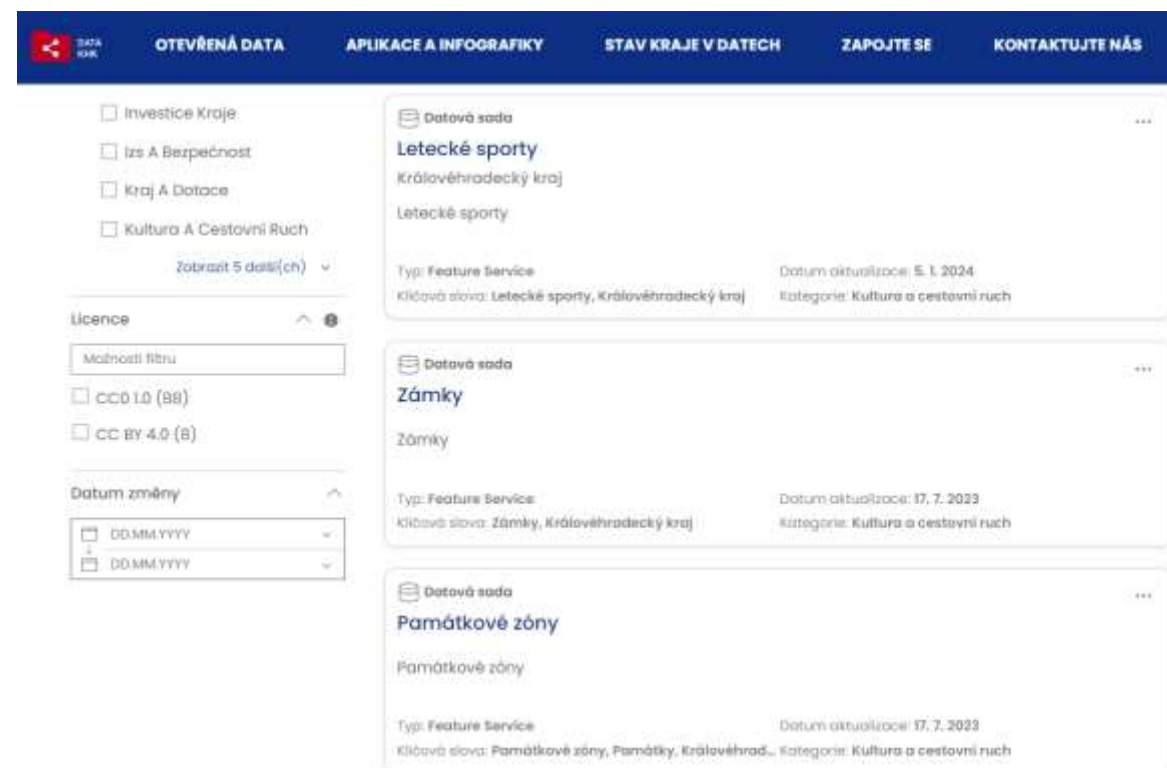
JOSEF HORÁLEK – FAKULTA INFORMATIKY A MANAGMENTU,  
UNIVERZITA HRADEC KRÁLOVÉ

# DATOVÝ PORTÁL KRÁLOVÉHRADECKÉHO KRAJE DATA KHK

## LKOD



Centrální informační místo pro veřejnost



# OTEVŘENÁ DATA KRAJE

## Mapové výstupy

Data KHK

Školy a školská zařízení

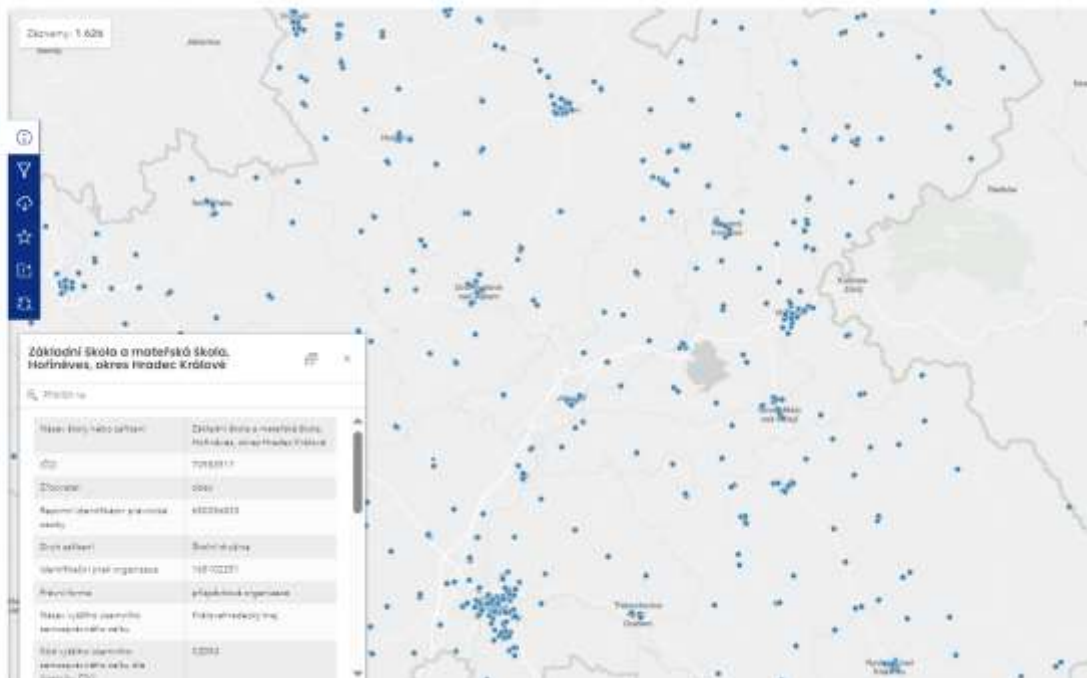
- Soukromý člen
- Soukromá organizace

Zobrazit všechny podrobnosti

Stahování

Podrobnosti

- Datová sada  
Feature Layer
- Ročně  
Informace aktualizovány: 25. září 2022
- 25. září 2022  
Data aktualizována
- 1. listopadu 2021  
Datum vydání
- Záznamy: 1 626  
Zobrazit tabulku dat
- Všechny  
Každý svůj tento atribut
- Licence CC0 1.0  
Zobrazit podrobnosti licence



## Popis datové sady

**Počet studentů v oborech vyšších odborných škol zřizovaných krajem**

Soukromý člen  
Soukromá organizace

Prohlédnout mapu | Zobrazit | Více

**Shrnutí**

Počet studentů v oborech vyšších odborných škol zřizovaných krajem

Datová sada s prostorovou lokalizací vyškolených odborných škol zřizovaných krajem včetně přehledu počtu studentů a jednotlivých školách. Data jsou až školní rok 2022/2023. Zdrojem dat je Odbor školství Krajského úřadu Královéhradeckého kraje.

[Zobrazit a vyjmout](#)

**Podrobnosti**

- Datová sada  
Feature Layer
- Ročně  
Informace aktualizovány: 20. února 2022
- 17. února 2022  
Data aktualizována
- 30. února 2022  
Datum vydání
- Záznamy: 17  
Zobrazit tabulku dat
- Všechny  
Každý svůj tento atribut
- Licence CC0 1.0  
Zobrazit podrobnosti licence
- Bezúplatná plocha

**Atributy**

- Název
- ICZ
- Právní forma
- Regionální identifikátor právnické osoby
- Identifikační znak organizace
- Název výššího územního samosprávného celku

[Další informace o grazech](#)

# KATALOGY OTEVŘENÝCH DAT

98  
datových  
sad

LKOD

datakhk.cz



DATA  
KHK

NKOD

data.gov.cz

OTEVŘENÁ DATA

EU

data.europa.eu



Evropská  
komise

# OTEVŘENÁ DATA KRÁLOVÉHRADECKÉHO KRAJE

- Aplikace nad otevřenými daty
- Hackathony
- Data veřejně dostupná
- Zdroj dat - veřejná správa
- Zajištění integrity a důvěryhodnosti
- Klasifikace dat u zdroje, během zpracování, při prezentaci
- Nutnost nastavení modelu logování k zajištění integrity

# BPMN (BUSINESS PROCESS MODEL AND NOTATION)

- Řešení bezpečnostní analýzy otevřených dat využívaných v Datovém portálu Královéhradeckého kraje Data KHK za využití Business Process Model and Notation (BPMN). Standardní model BPMN je rozšířen pro CyberSecurity nadstavbu (BPMN\_SC), jež umožňuje efektivně navrhnout relevantní bezpečnostní opatření zaměřené na kvalitu a dostupnost otevřených dat. Prezentovaný systém jedinečným způsobem spojuje mapování podnikových procesů s kyberbezpečnostní klasifikací dat využívaných jako zdroj následných procesů ve Smart City.

# PŘEDSTAVENÍ PROJEKTU ARTISEC

- Projekt ARTISEC se zaměřuje na využití umělé inteligence pro zajištění kybernetické bezpečnosti.
- Cílem projektu je navrhnout a ověřit komplexní bezpečnostní model využití umělé inteligence pro zajištění kybernetické bezpečnosti Smart City založený na datové analýze primárních a podpůrných datových aktiv využívaných v rozsahu Smart City.

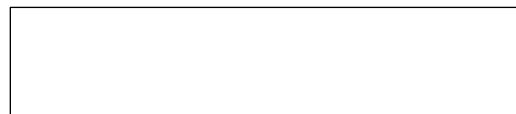
# JAK NA KYBERBEZPEČNOST SMART CITY

- Mapování procesů
- Stanovení parametrů CIA (Confidentiality, Integrity, Availability)
- BIA (Business Impact Analysis)
- Využití AI pro zajištění integrity



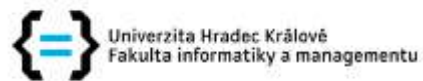
# CONFIDENTIALITY, INTEGRITY, AVAILABILITY

Confidentiality



Availability

Integrity



# CONFIDENTIALITY, INTEGRITY, AVAILABILITY

- Availability
  - RTO (Recovery Time Objective)
  - RPO (Recovery Point Objective)
  - MIPD (Maximum Initial Programmed Delay)
  - MTPD (Maximum tolerable period of disruption)
  - MTDL (Maximum Tolerable Data Loss)
- Confidentiality
  - Klasifikace informací
- Integrity
  - Kryptografické hashovací funkce
  - Digitální podpisy
  - Kontrolní součty (Checksums)
  - Message Authentication Codes (MACs)
  - Digitální certifikáty

## BIA (BUSINESS IMPACT ANALYSIS)

BIA je proces, který jsme využili k identifikaci, hodnocení a prioritizaci rizik a jejich potenciálního vlivu na provoz a cíle podnikání.

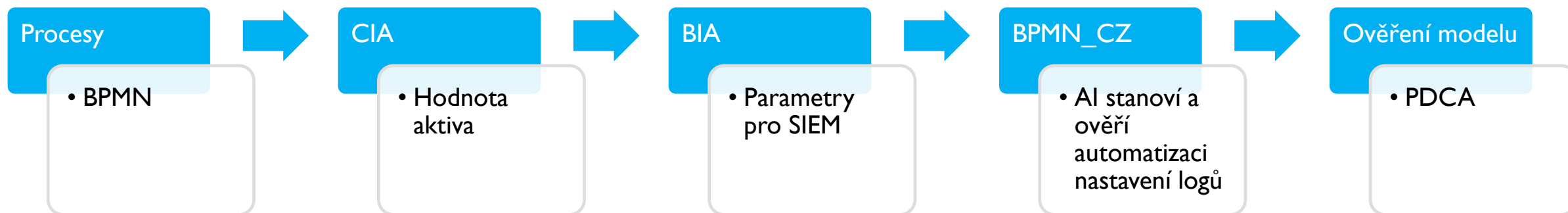
Jednou z hlavních částí procesu je určení kritických aktivit, procesů a systémů, které jsou nezbytné pro kontinuitu podnikání.

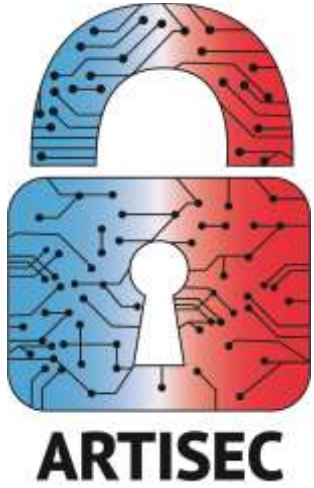
# ARCHITEKTURA LOGOVÁNÍ SIEM

Řešení SIEM provádí činnosti v podobě sběru informací (protokolů), normalizace, kategorizace, rozboru, analýzy a korelace:

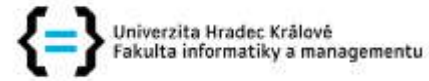
- **Sběr protokolů** - základní funkce systému SIEM, která zahrnuje sběr informací z různých zdrojů v infrastruktuře.
- **Normalizace** - proces, při kterém systém SIEM převádí data z různých formátů do jednotného formátu. To umožňuje efektivnější analýzu a usnadňuje porovnávání dat z různých systémů.
- **Kategorizace** - označuje proces třídění protokolů a událostí do různých kategorií na základě jejich typu nebo povahy, jako jsou systémové události, bezpečnostní události, chyby aplikací atd.
- **Rozbor** - syntaktický rozbor je proces rozkladu jednotlivých protokolů na strukturované součásti, jako jsou zdrojové a cílové IP adresy, časy výskytu, typy událostí a další klíčové informace. Parsování je nezbytné k získání užitečných informací z různých formátů protokolů, které generují různé zdroje informací.
- **Analýza a korelace** - Po shromáždění, normalizaci, kategorizaci a rozboru protokolů provádí systém SIEM analýzu a korelaci dat na základě definovaných scénářů detekce a korelace. Cílem je identifikovat podezřelé vzory nebo aktivity, které by mohly indikovat bezpečnostní incident. Pokročilé systémy mohou pro detekci anomálií a pokročilou korelaci využívat strojové učení a další sofistikované algoritmy.

# JAK UMÍME VYUŽÍT AI





## I. Workshop projektu ARTISEC



DĚKUJEME ZA POZORNOST