MUNI
FI

Process-aware Insider Threat Detection and Mitigation in Organizations

Martin Macák
macak@mail.muni.cz

Faculty of Informatics, Masaryk University

August 31, 2020

Introduction

- Malicious users with authorization to an organization’s resources.
- Insiders can work together to perform an attack.
- The attacks do not need to be intentional.
- The process of insider attacks may be very complicated and highly inconspicuous.

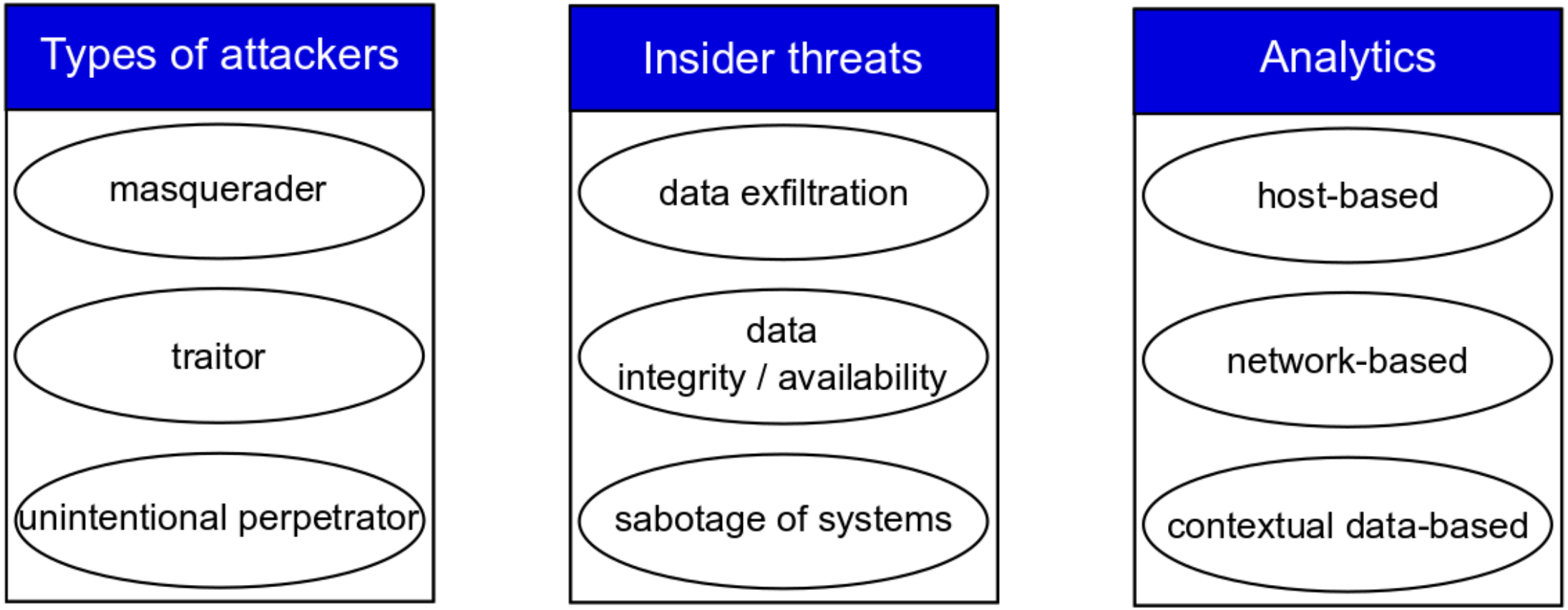
Process mining

- Promising research discipline that focus on the process analysis.
- Process mining is successful in:
  - process discovery,
  - conformance checking,
  - process enhancement.
- It can help understand the detected behavior of entities and provide a better insight into the performed operations.

Process mining in cybersecurity

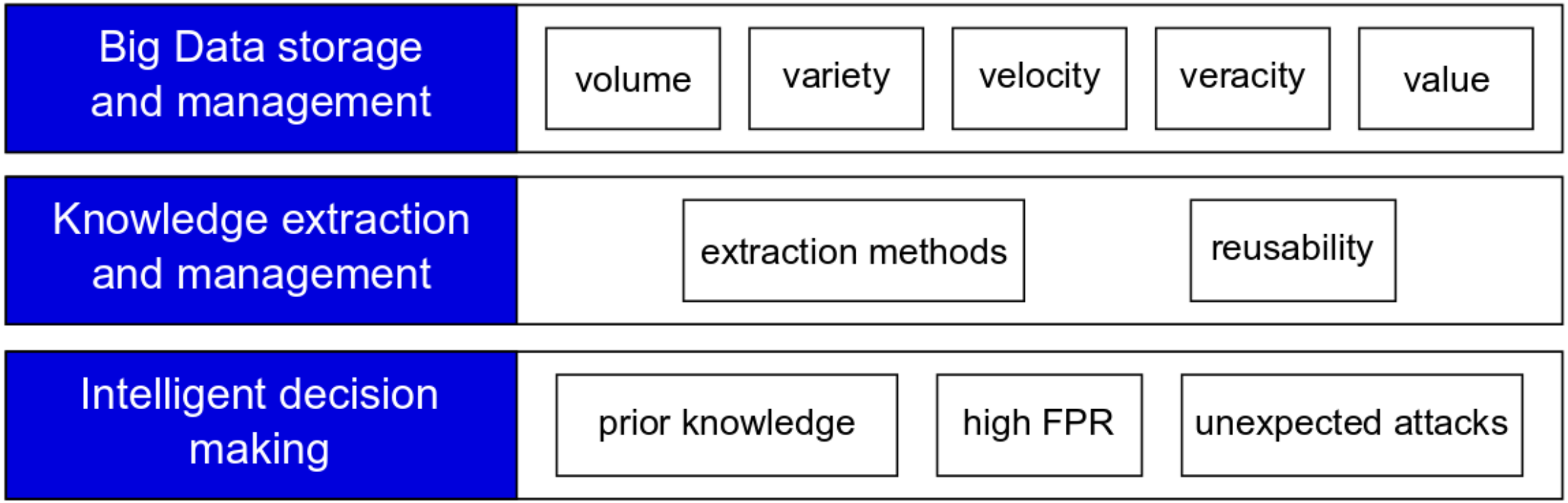
- A promising candidate to address the challenges in cybersecurity [1].
- We need to analyze the sequences of events.
- For example: detect, mitigate or prevent threats from audit logs, detect attack vectors, analyze cybersecurity training session runs, …

Existing research in insider attacks



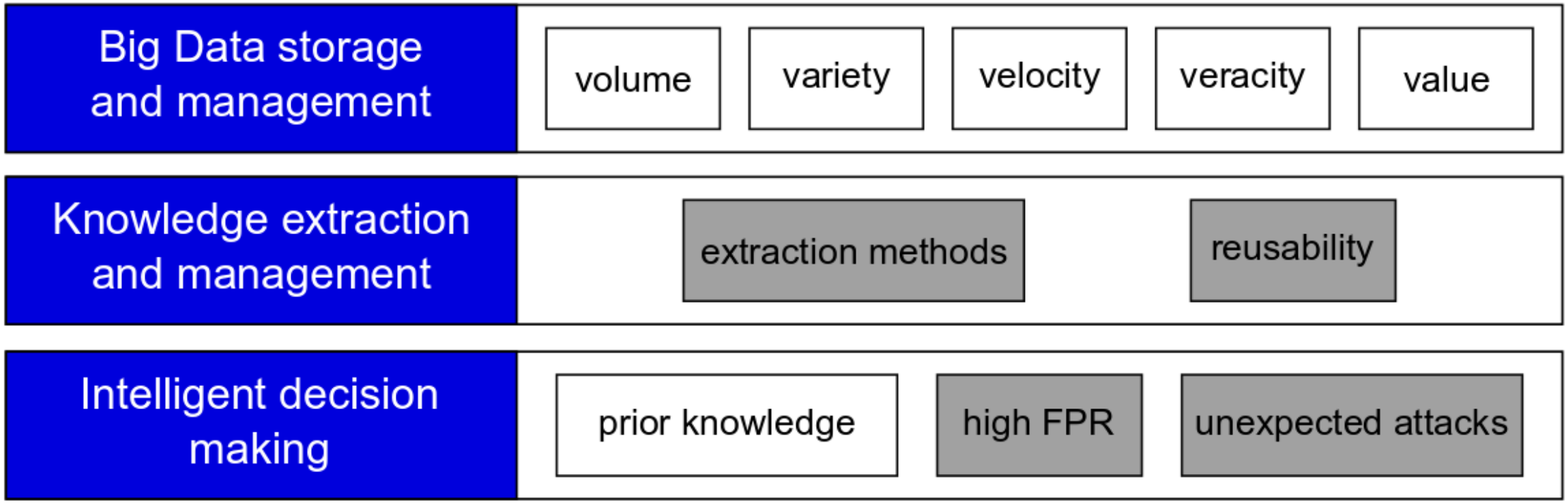
MUNI
FI

Challenges of insider threat detection



MUNI FI

Process mining utilization

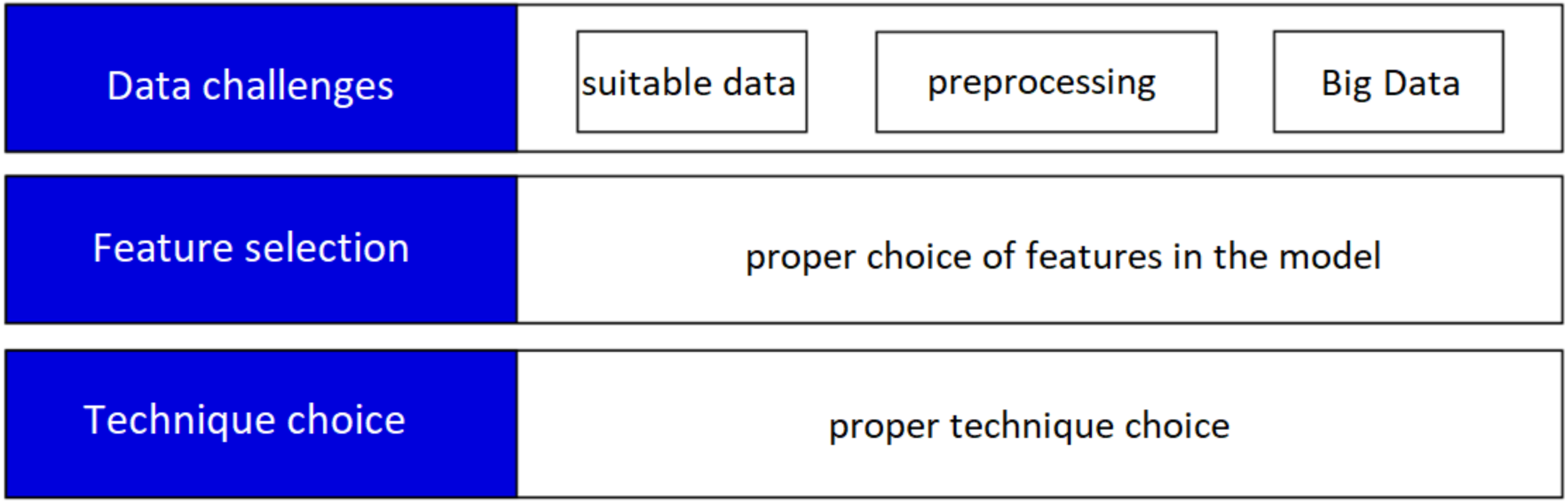


MUNI FI

Problem statement

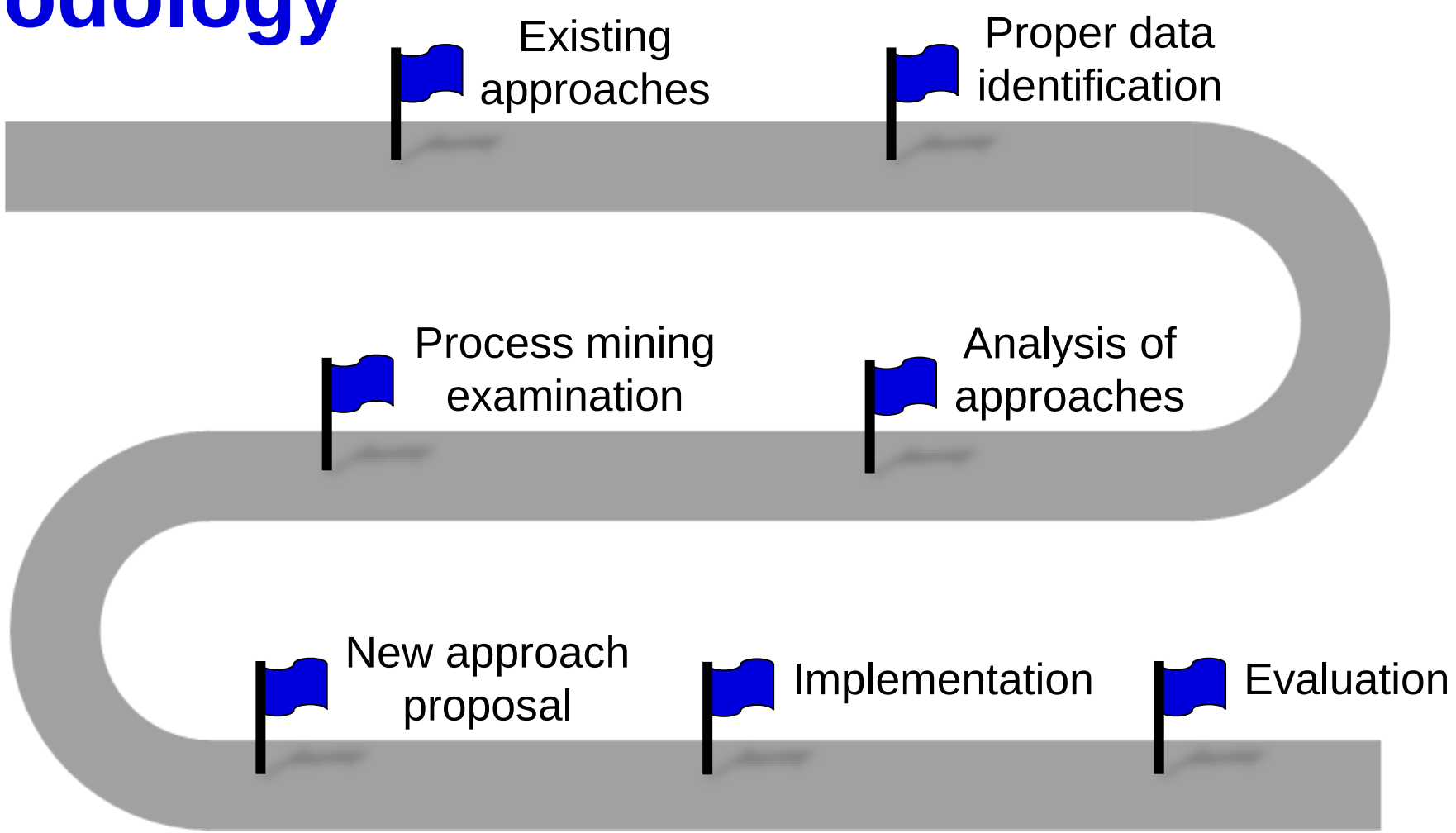
Despite decades of research, threats from malicious insiders currently lead to huge losses in organizations. The problem is identified to be threefold. First, insider threat detection techniques are too rigid, and the models might not be accessible, or they are too abstract or complex. Second, the designers of cybersecurity training sessions are not provided with appropriate analytical tools. Last, the unintentional insider attack vector cannot be easily obtained.

Challenges of process mining utilization



MUNI FI

Methodology



MUNI FI

Main outcomes

An approach for the detection and mitigation of security threats posed by insiders in organization.

- **Insider threat detection**
  - Anomaly detection technique.
- **Insider threat mitigation**
  - Enhancement of cybersecurity training session design.
- **Unintentional insider attack vector identification**
  - Identification of attack vectors, implemented and evaluated on case study.
- **Big Data**
  - Better utilization of Big Data in this context.

Current accepted publications

[1] **MACÁK, Martin**, Agáta KRUŽÍKOVÁ, Lukáš DAUBNER a Barbora BÜHNOVÁ. Simulation Games Platform for Unintentional Perpetrator Attack Vector Identification. In The 1st International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS). : ACM, 2020.

[2] **MACÁK, Martin**, Matúš ŠTOVČIK, Barbora BÜHNOVÁ a Michal MERJAVÝ. How well a multi-model database performs against its single-model variants: Benchmarking OrientDB with Neo4j and MongoDB. In Proceedings of the 2020 Federated Conference on Computer Science and Information Systems: IEEE, 2020.

[3] **MACÁK, Martin**, Matúš ŠTOVČIK and Barbora BÜHNOVÁ. The Suitability of Graph Databases for Big Data Analysis: A Benchmark. In The 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020). : SciTePress, 2020.

[4] **MACÁK, Martin**, Hind BANGUI, Barbora BÜHNOVÁ, András J. MOLNÁR a Csaba István SIDLÓ. Big Data Processing Tools Navigation Diagram. In The 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020). : SciTePress, 2020.

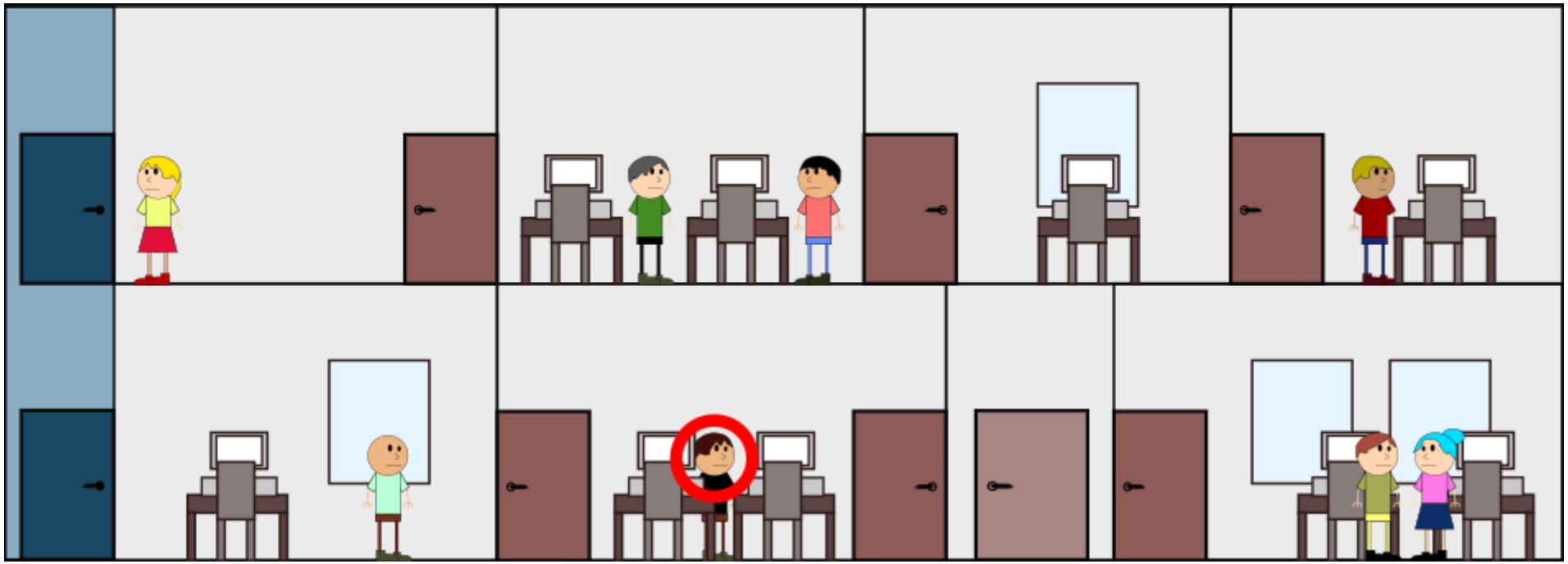
*[5] **MACÁK, Martin**, Mouzhi GE and Barbora BÜHNOVÁ . A Cross-Domain Comparative Study of Big Data Architectures. International Journal of Cooperative Information Systems.*

[6] DAUBNER, Lukáš, **Martin MACÁK**, Barbora BÜHNOVÁ a Tomáš PITNER. Verification of Forensic Readiness in Software Development: A Roadmap. In 35th ACM/SIGAPP Symposium On Applied Computing. Brno, Czech Republic: ACM, 2020. 4 s. doi:10.1145/3341105.

[7] LIPČÁK, Peter, **Martin MACÁK** and Bruno ROSSI. Big Data Platform for Smart Grids Power Consumption Anomaly Detection. In Proceedings of the 2019 Federated Conference on Computer Science and Information Systems. New York: IEEE, 2019. s. 771-780, 10 s. ISBN 978-1-5386-8005-6. doi:10.15439/2019F21

MUNI FI

Thank you for your attention



Contact me: macak@mail.muni.cz

MUNI FI