A Process Mining Framework for Insider Attack Detection

Martin Macák

Faculty of Informatics, Masaryk University, Brno

April 6th, 2023

lasaris

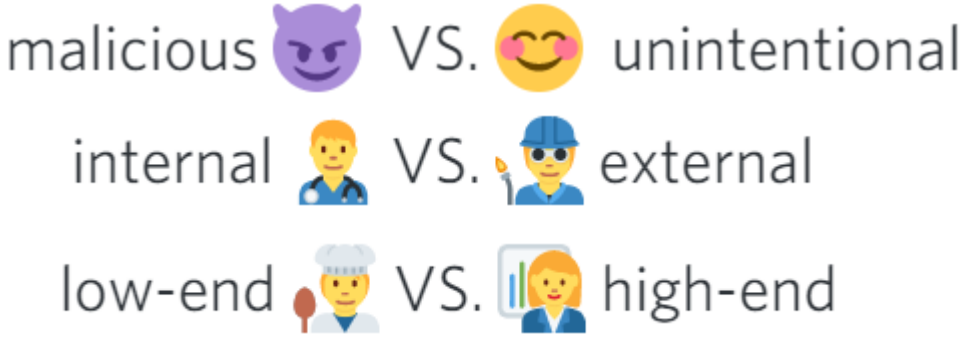
Outline

1. Insider domain
2. Process mining domain
3. Process mining framework for insider attack detection

lasaris

Classification of insiders

- Insider
  - A person with legitimate access to an organization’s resources.



- Affiliate
  - Do not have any justified and legitimate reason to enter the organization.

lasaris

Reasons for insider attacks

- Malicious
  1. Self-motivated – get a job promotion, avenge the injustice against them, …
  2. Planted – steal intellectual property
  3. Recruited – perform a malicious act for their benefit

  The motivation can be financial, political, or personal.

- Unintentional
  1. Underminers – life is easier when I don't respect security policies
  2. Overambitious – when I want to be more effective, I have to bypass security
  3. Socially engineered – I was tricked by someone
  4. Data leakers – ooopsie, I just leaked something

  No motivation or intent to cause harm.

lasaris

Defense solutions

- Mitigation and prevention
- Decoy-based solutions
- Detection and assessment

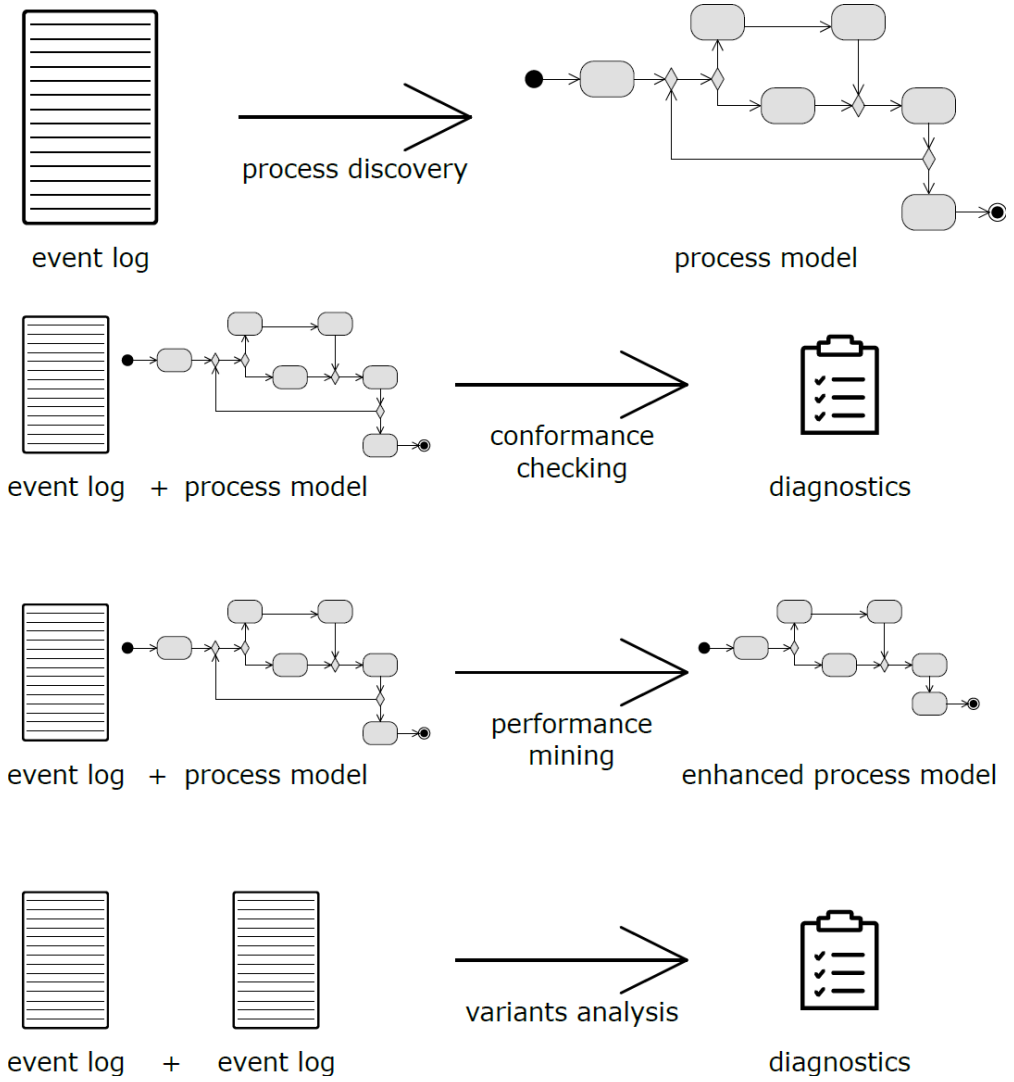
lasaris

Research gaps in detection and assessment

- The insider behavior is often encoded into a mathematical model that might not be accessible or is very abstract / complex.
- The proper response to a detected case is challenging.
- It is hard to detect previously not seen insider attacks.

lasaris

Process Mining

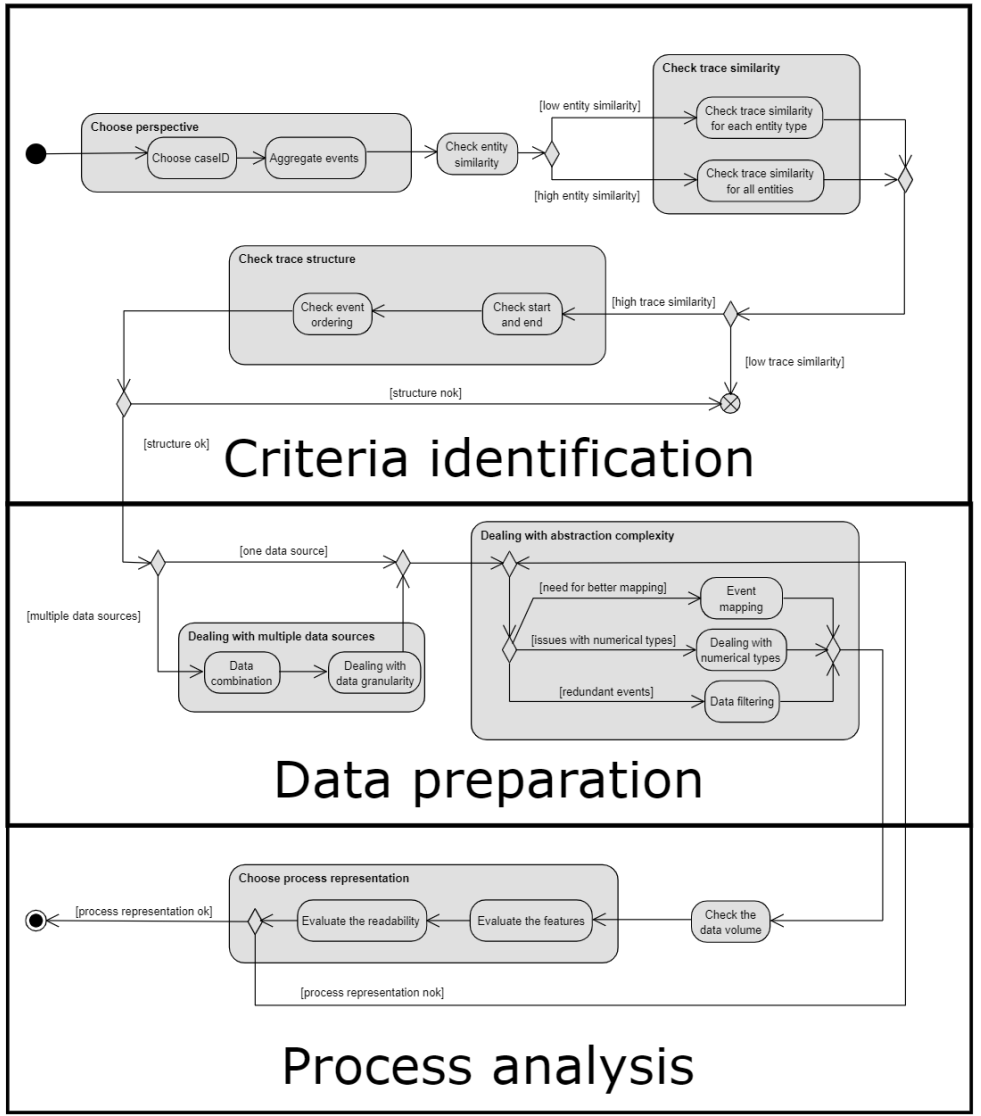


Challenges of Process Mining in insider attack detection

- Criteria identification
- Data preparation
- Process analysis

lasaris

Process Mining Framework for Insider Attack Detection



lasaris

Criteria identification

1. Choose a process perspective
   - Personal perspective
   - Production perspective
   - Manipulation perspective
2. Check for similarity between entities
3. Check for similarity between traces
4. Check trace structure
   - Check start and end
   - Check event ordering

lasaris

Data preparation

1. Deal with multiple data sources
   - Data combination
   - Data granularity
2. Deal with abstraction complexity
   - Data filtering
   - Deal with numerical types
   - Data mapping

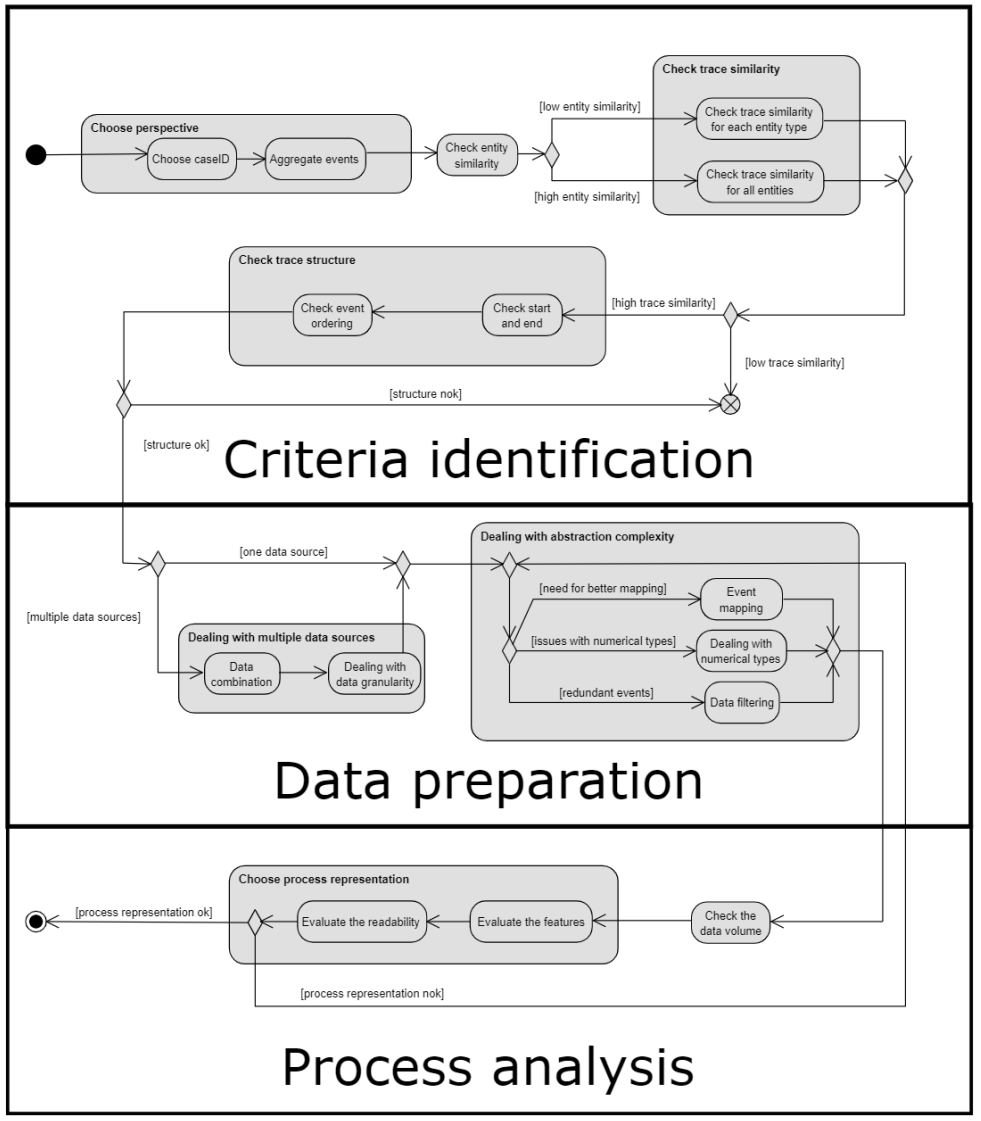
lasaris

Process analysis

1. Handle data volume
2. Choose a process representation
   - Evaluate the features
   - Evaluate the readability
     - Compactness, Intuitiveness, Interactive view, Storytelling, Rapid workflow

lasaris

Conclusion


Choose perspective
Choose caseID
Aggregate events
Check entity similarity
[low entity similarity]
[high entity similarity]
Check trace similarity
Check trace similarity for each entity type
Check trace similarity for all entities
Check trace structure
Check event ordering
Check start and end
[high trace similarity]
[low trace similarity]
[structure nok]
[structure ok]
Criteria identification
[one data source]
[multiple data sources]
Dealing with multiple data sources
Data combination
Dealing with data granularity
Dealing with abstraction complexity
[need for better mapping]
Event mapping
[issues with numerical types]
Dealing with numerical types
[redundant events]
Data filtering
Data preparation
Choose process representation
[process representation ok]
Evaluate the readability
Evaluate the features
Check the data volume
[process representation nok]
Process analysis