MUNI

Identification and Assessment of Active Cyber Threats

Ph.D. Research Proposal

Lukáš Sadlek, Pavel Čeleda, Daniel Tovarňák
sadlek@fi.muni.cz

Masaryk University

November 12, 2020 @ CODE 2020

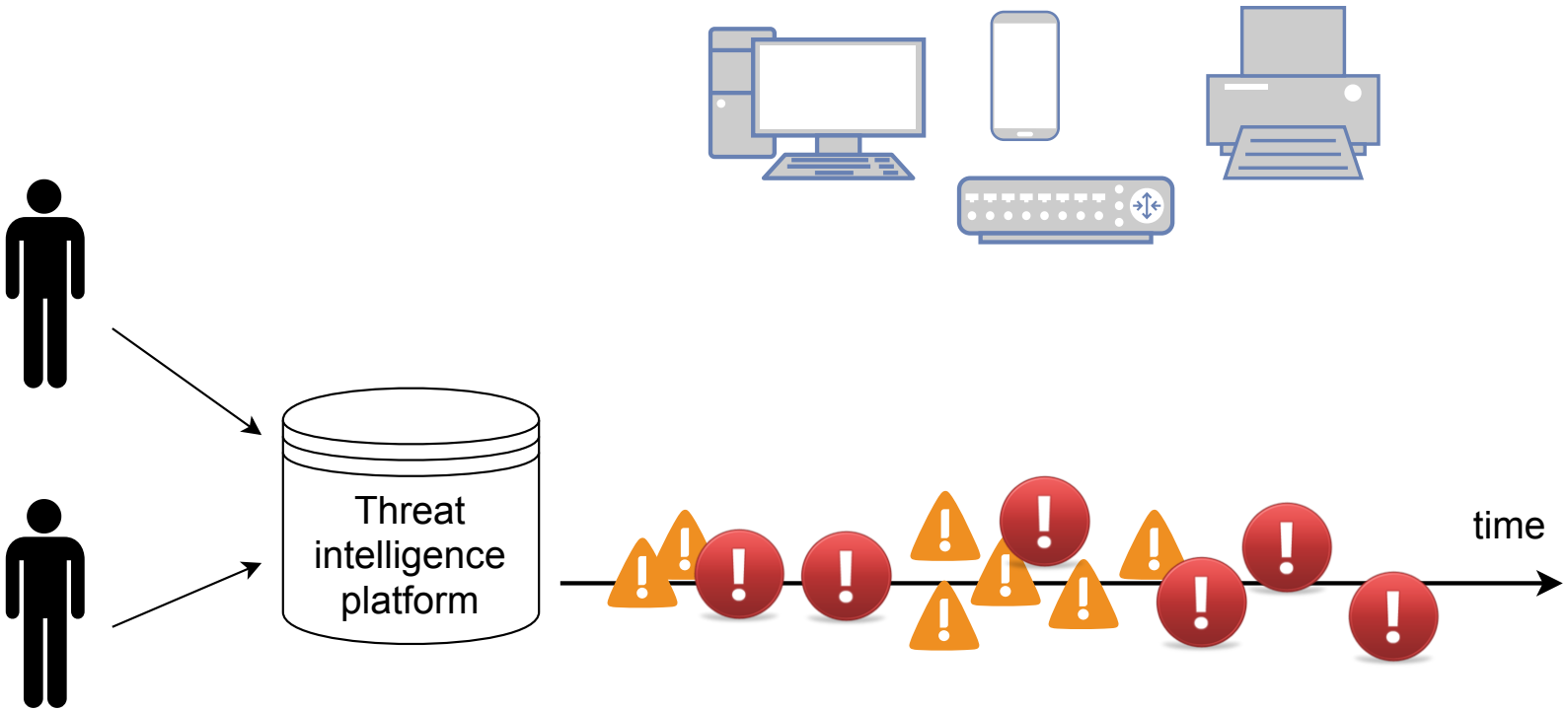
Motivation

- **Large volume** of cyber threat data is shared
- Only some **fraction** is related to protected assets
- Threat data processing can be **improved**

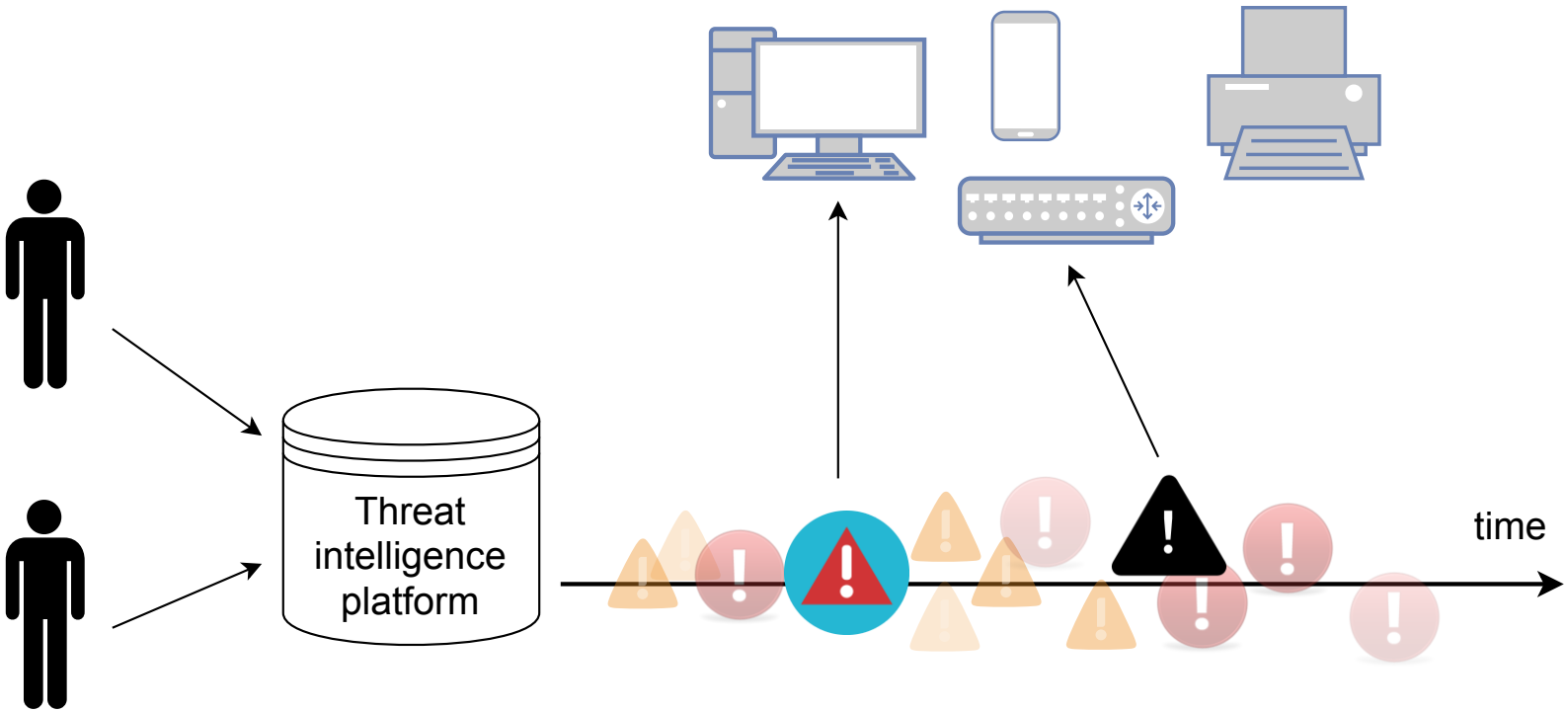
Selected Area	**Not Satisfied**
Cleanliness and quality of data	37.4%
Context	35.4%
Location-based visibility	42.5%
Machine learning	55.9%

Table: 2019 SANS CTI Survey Results

Research Problem



Research Problem



Research Questions

RQ1

How can we **identify** active cyber threats based on globally shared data and local knowledge about assets?

Research Questions

RQ1

How can we **identify** active cyber threats based on globally shared data and local knowledge about assets?

RQ2

How can we **assess** and prioritize active cyber threats based on the impact on assets?

RQ1: Active Cyber Threat Identification

- **Actionable** information about cyber threats should be
  - Relevant
  - Timely
  - Accurate
  - Complete
  - Ingestible
- Address **relevance** and **accuracy** of results

RQ1: Current State

Existing methods

- Enumerations and sharing standards
- Methods for determining properties of assets

RQ1: Current State

Existing methods

- Enumerations and sharing standards
- Methods for determining properties of assets

Issues

- Mutual **interoperability**
- Some methods are applicable under specific **conditions**
- Data processing must be **fast**

RQ1: Proposed Approach – Threat Data

Data conforming to information sharing standards

- CVE, CVSS, CPE, CWE, CAPEC, MITRE ATT&CK
- We can **trust** the content
- Enumerations cover a **broad landscape**

Open-source cyber threat intelligence

- Information about ongoing campaigns or attacks
- **Trust issues**

RQ1: Proposed Approach – Local Context

- Select relevant threats by introducing **local context**
- Knowledge about assets:
  - Passive monitoring – IP flows
  - Active monitoring – data from scanners
  - Logs extraction – application logs

RQ1: Contribution

- Improve the combination **beyond simple joins** of data
- Consider also assets **influenced** by the vulnerable ones
- Improve **relevance** and **accuracy** of results

RQ2: Cyber Threat Assessment

Methods

- **Simple** metrics or tables
  - **Fast** computation
  - No complex assessment
  - Example: CVSS score
- **Sophisticated**
  - **Longer** computing time
  - Suitable for multistep attacks
  - Example: Attack graphs

RQ2: Current State

- MulVaL is an efficient attack graph generator
  - **Quadratic** complexity
  - **Logical** programming
- Comparison of severity
  - Bayesian Attack Graph uses probability
  - **Exponential** complexity

RQ2: Proposed Approach and Contribution

- Data from RQ1
- Attack graphs for **near real-time assessment**
- Improvement using state-of-the-art technologies and methods
  - Graph databases with their algorithms
  - Machine learning

Summary

- **Contextualization** of threats with knowledge about assets
- Improved **interoperability** concerning relevance and accuracy
- **Fast** threat assessment using attack graphs
- Step further to successful **threat mitigation**

MASARYK
UNIVERSITY