



# SÉMANTICKÉ PUBLIKOVANIE SPRAVODAJSKÝCH DÁT O BEZPEČNOSTNÝCH HROZBÁCH

Bc. Matej Rychtárik

Projektový seminár 2

# ZÁKLADNÉ ÚDAJE

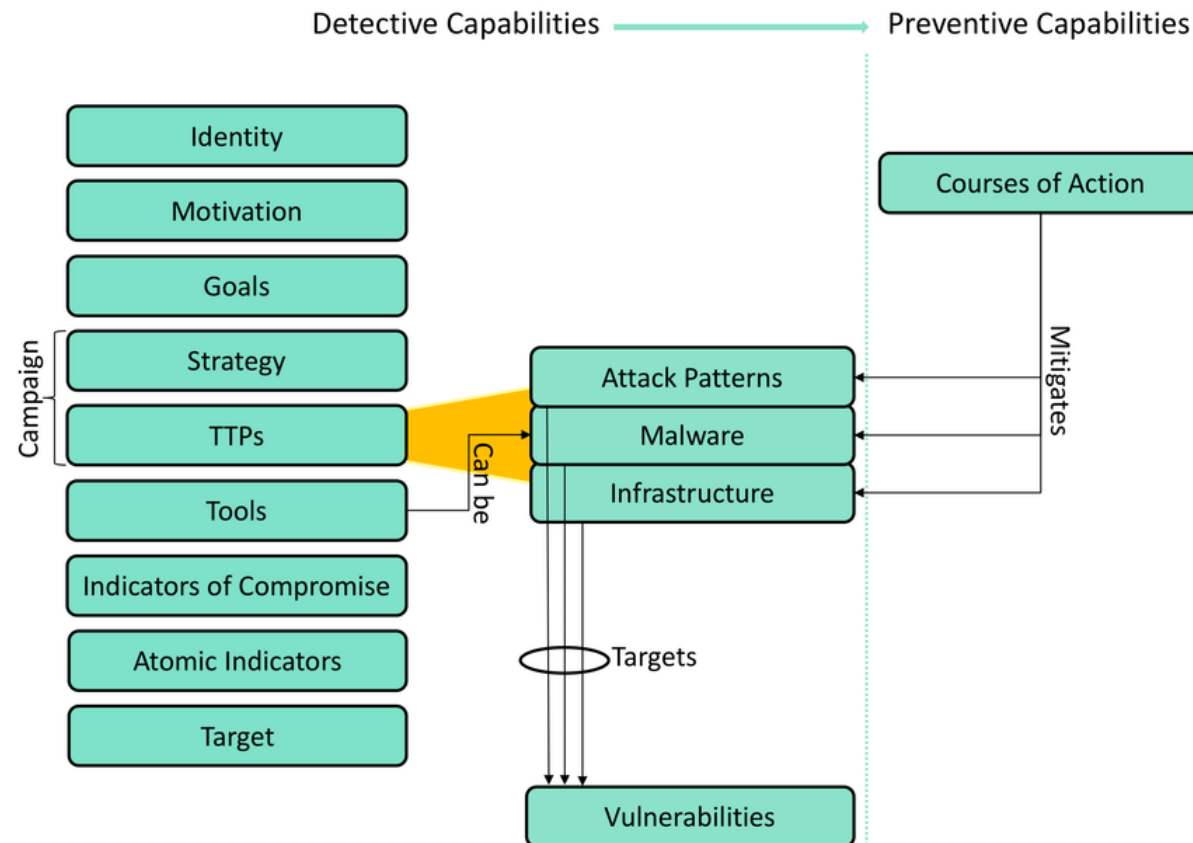
- **Študent:** Bc. Matej Rychtárik
- **Vedúci:** doc. RNDr. Martin Homola, PhD.
- **Konzultant:** Ing. Štefan Balogh, PhD. – FEI STU
- **Ciel':**

Cieľom je navrhnuť vhodnú ontológiu pre publikovanie spravodajských dát o bezpečnostných hrozbách a vytvorenie repozitára za týmto účelom v sieti prepojených dát.

# AKTUÁLNY STAV

- Tvorba článku v spolupráci s vedúcim práce a p. **Ing. Štefan Balogh, PhD.**
  - Moje úlohy – spracovanie ontologických riešení v doméne Cyber Security
- Napísané časti práce
  - Sémantický web
  - Úvod do ontológií
  - Existujúce riešenia
  - Podrobná analýza ontológie, z ktorej vychádzame + čiastočne navrhnuté úpravy na zlepšenie
- Rozbehané prostredie na vývoj ontológií – Protégé
  - Práca s týmto systémom, dotváranie ontológie a jej úpravy

# CTI MODEL



# PRESKÚMANÉ ONTOLÓGIE NA PREPOJENIE

- <https://cwe.mitre.org/index.html>
- <https://cve.mitre.org/index.html>
- <https://capec.mitre.org/>
- <https://cyboxproject.github.io/>

# UCO - ZHRNUTIE

- Unified Cybersecurity Ontology
- Ontológia s najväčšími prepojeniami na už existujúce dáta

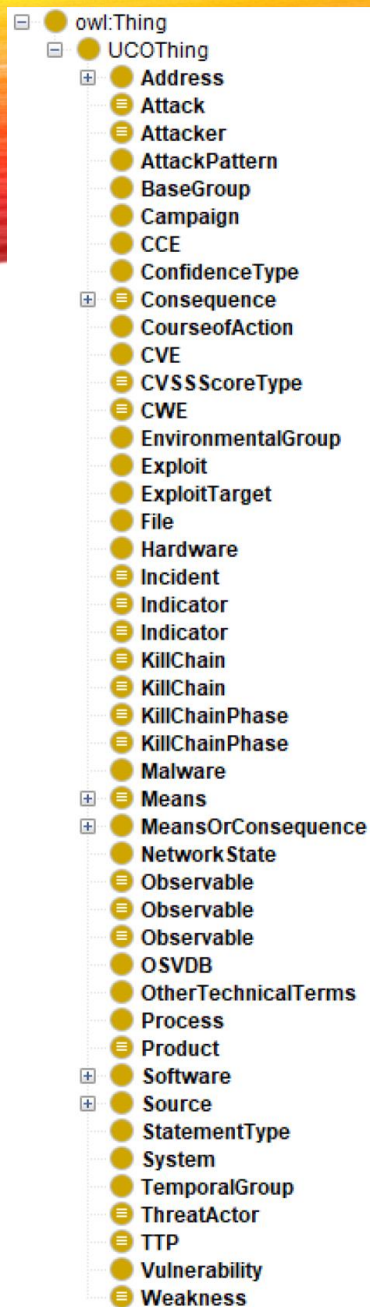
- Zdroj: <https://github.com/Ebiquity/uco2>

- Článok:

Zareen Syed, Ankur Padia, Tim Finin, M. Lisa Mathews, and Anupam Joshi.  
UCO: A unified cybersecurity ontology. In David R. Martinez, William W. Streilein, Kevin M. Carter, and Arunesh Sinha, editors,

Artificial Intelligence for Cyber Security, Papers from the 2016 AAAI Workshop, Phoenix, Arizona, USA, February 12, 2016, volume WS-16-03 of AAAI Workshops. AAAI Press, 2016.





# UCO – ZISTENIA

- Veľa dát sa ale ešte dá prepojiť – CWE, CVE, CyBox, ...
- Predpripravená implementácia pre niektoré existujúce riešenia, ale nedotiahnuté úpravy prepojení
- Nepokrýva všetky dáta z CTI modelu
- Nevyužíva výhody ontológií a jazyka OWL

# POSTUP DO ODOVZADNIA

- Praktická:
  - Dokončiť podrobnú analýzu UCO2
  - Zapracovať navrhované zmeny
  - Vloženie existujúcich dát
  - Validácia a robustnosť
- Dokument:
  - Dopísať kapitoly o syntaxe ontológií, CTI modelu, návrhu riešenia, testovaní a výsledku práce



# VALIDÁCIA A ROBUSTNOSŤ

- Ontológia – Tbox
  - Kontrola konzistentnosti výslednej ontológie
  - Kontrola splniteľnosti tried
- Ontológia – Abox
  - Kontrola konzistentnosti dát
  - Kontrola splniteľnosti dopytu
- Vytvorenie Test Case, ktoré budú musieť byť splnené
- Program *OntoClean*

# PREŠTUDOVANÉ MATERIÁLY 1

- Christian Bizer, Tom Heath, and Tim Berners-Lee. **Linked data**: The story so far.
- Tim Berners-Lee, James Hendler, and Ora Lassila. **The semantic web**.
- Nicola Guarino, Daniel Oberle, and Steen Staab. **What is an ontology?**
- Michael Iannacone, Shawn Bohn, Grant Nakamura, John Gerth, Kelly Huer, Robert Bridges, Erik Ferragut, and John Goodall. **Developing an ontology for cyber security knowledge graphs**. – STUCCO
- Vasileios Mavroeidis and Siri Bromander. **Cyber threat intelligence model**: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence.

# PREŠTUDOVANÉ MATERIÁLY 2

- Leo Obrst, Penny Chase, and Richard Markelo. Developing an ontology of the cyber security domain. Zareen Syed, Ankur Padia, Tim Finin, M. Lisa Mathews, and Anupam Joshi. **UCO**: A unie
- A.T. Schreiber and Raimond. Ontotext and, **sparql** overview. <https://www.w3.org/TR/2013/REC-sparql11-overview-20130321/>
- A.T. Schreiber and Raimond. **Rdf framework**. <https://www.w3.org/TR/rdf11-primer/>
- Malek Ben Salem and Chris Wacek. Enabling new technologies for cyber security defense with the **icas** cyber security ontology.

# PREŠTUDOVANÉ MATERIÁLY 3

- Takeshi Takahashi, Bhola Panta, Youki Kadobayashi, and Koji Nakao. Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information.
- Alessandro Oltramari, Lorrie Faith Cranor, Robert J Walls, and Patrick D McDaniel. Building an ontology of cyber security.
- John Pinkston, Jerrey Undercoer, Anupam Joshi, and Timothy Finin. A target-centric ontology for intrusion detection.



ĎAKUJEM ZA POZORNOST