Ontology Description

## Ontology for Cybersecurity Education

The objective is to develop an ontology to build AI systems (knowledge graphs) for cybersecurity education which can allow students to learn the concepts at their pace.

### Key Entities

Based on the analysis of course material, entities extracted from NER and using domain knowledge, we created following categories for cybersecurity related entities -

* Concept
* Application
* Role

The different types of entities under each category can be defined as follows:

| **entityCategory** | **entityType** | **entityName (example)** |
| --- | --- | --- |
| Concept | feature | private key, cookies, protocol, port |
|  | function | snort rules, hash, XOR |
|  | attack | css, sql injection, spyware |
|  | vulnerability | bad config, weak password |
|  | technique | honeypot, risk assessment |
|  | data | Files, logs, messages, packet |
|  |  |  |
| application | tool | burp, wireshark, snort, sniffer |
|  | system | linux, server, host |
|  | app | browser, webapp |
|  |  |  |
| role | attacker | black hat, attack host |
|  | securityTeam | security engineer, white hat, ethical hacker, network admin |
|  | user | employee, user |

#### Entity Metadata /or attributes

* entityID
* entityName
* entityType
* entityCategory

### Relations

Based on the data analysis we identified the following relations -

| **relation** | **Example** |
| --- | --- |
| has\_a | Snort ***has\_a*** Packet Decoder |
| is\_a | Trojan ***is\_a*** malware |
| can\_analyze | Packet decoder ***can\_analyze*** header anomaly |
| can\_expose | Home network ***can\_expose***Land Attack |
| can\_exploit | Attack host ***can\_exploit*** TCP SYN Packet |
| implements | Snort rules***implements*** ICMP rules |
| uses | Team defense ***uses*** home network |

We plan to use property graphs because they allow us to add more attributes to the edges. We can add an attribute ‘action’ to the edge. That will help in explaining any action or specific detail associated with that triple.

For Example:

| **Entity** | **Relation** | **Entity** | **Action** |
| --- | --- | --- | --- |
| IDS | is\_a | Intrusion Detection System | means |
| Snort | can\_analyze | network attacks | detect |
| Snort | can\_analyze | previous attack pattern | match |
| Preprocessor | can\_analyze | HTTP anomaly | verify |

*P.S. : I think it will be a useful detail for the students or any one trying to learn cybersecurity. Please let me have your thoughts.*

### Triple Schema

The dataset or triples follows below schema:

| **Schema Edges** |
| --- |
| (system, can\_expose, attack), |
| (system, can\_expose, vulnerability), |
| (app, has\_a, feature), |
| (tool, part\_of, tool) |
| (tool, has\_a, function), |
| (tool, can\_analyze, function), |
| (tool, can\_analyze, apps), |
| (tool, can\_analyze, vulnerability), |
| (tool, implements, technique), |
| (tool, has\_a, feature), |
| (function, can\_expose, attack), |
| (function, has\_a, feature) |
| (function, uses, tool) |
| (attack, implements, feature) |
| (feature, can\_expose, attack), |
| (attacker, can\_exploit, vulnerability), |
| (attacker, can\_exploit, feature), |
| (securityTeam, can\_analyze, vulnerability), |
| (securityTeam, can\_analyze, feature), |
| (securityTeam, can\_exploit, app), |
| (securityTeam, uses, technique), |
| (securityTeam, implements, function), |
| (securityTeam, uses, system), |
| (securityTeam, uses, tool), |
| (user, uses, system), |
| (user, can\_expose, vulnerability), |