Continuous Ontology Delivery For Security Analysis and Reasoning

Project Vision and Objectives

Vision: Create a unified cybersecurity ontology through the federation of diverse cybersecurity data resources

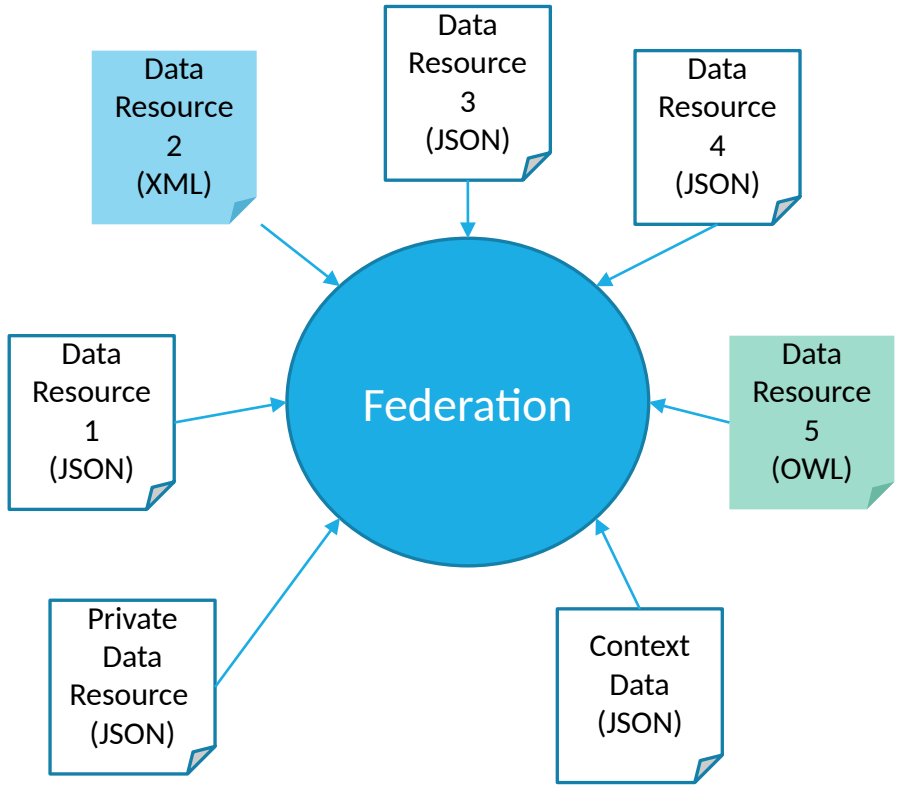
- **Objectives**:
  - Federate multiple cybersecurity databases and standards
  - Enable seamless integration, updates, and sharing of threat intelligence
  - Provide adaptable and context-sensitive cybersecurity insights

Problem Statement

- Increasing complexity and variety of cyber threats
- Fragmented cybersecurity resources leading to isolated and inconsistent data
- Lack of interoperability limits effective cybersecurity reasoning and intelligence sharing

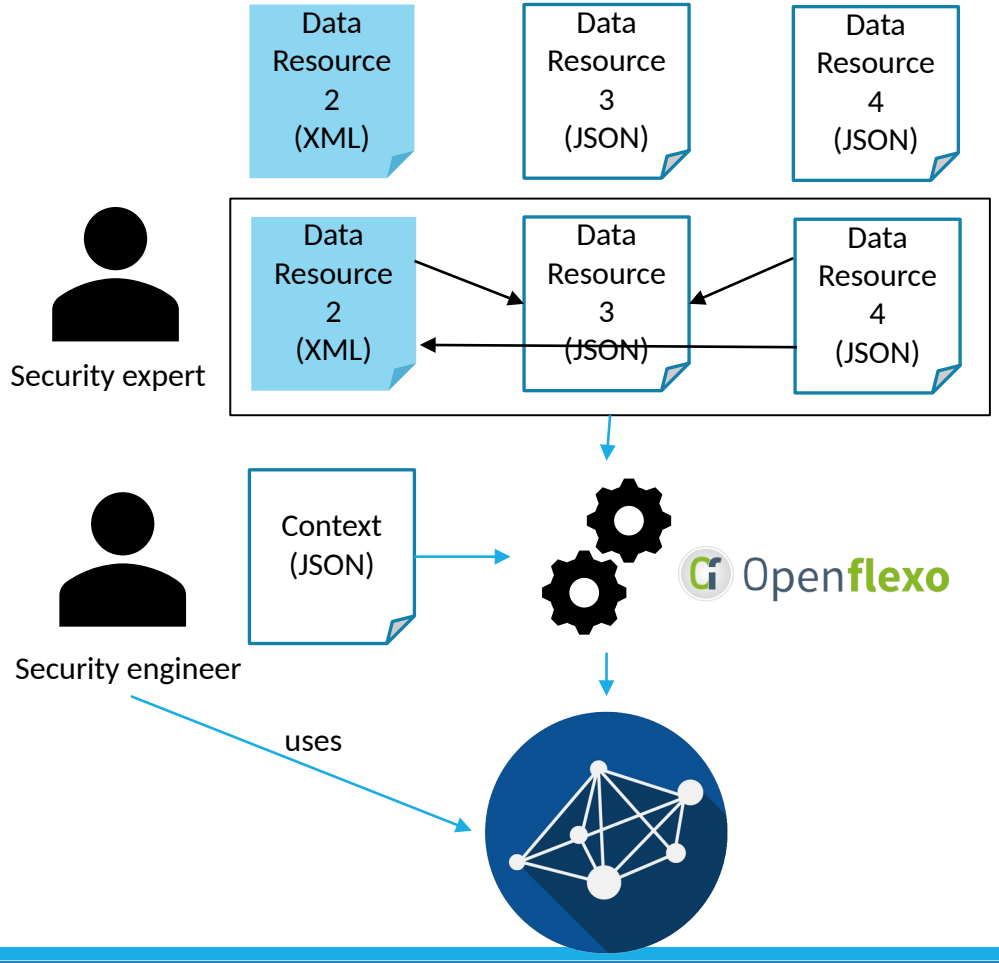
Importance of Federation

- Creates a unified data structure for holistic cybersecurity analysis
- Supports scalability and adaptability to newly emerging threats and defenses
- Ensures consistent, contextually relevant data, reducing redundancy
- Preserves original data integrity and context (including the format)



Project Methodology Overview

- Gathering data from cybersecurity resources
- Mapping both explicit and implicit relationships
- Conceptual integration of the mapped information (Federation)
- Creation of a cybersecurity ontology



Key Cybersecurity Resources to Federate

- MITRE ATT&CK: Adversary tactics and techniques
- MITRE D3FEND: Defensive measures and countermeasures
- CVE & CWE: Standardized vulnerability and weakness information
- CAPEC: Comprehensive catalog of common attack patterns
- NVD & ExploitDB: Detailed repositories for vulnerabilities and exploits

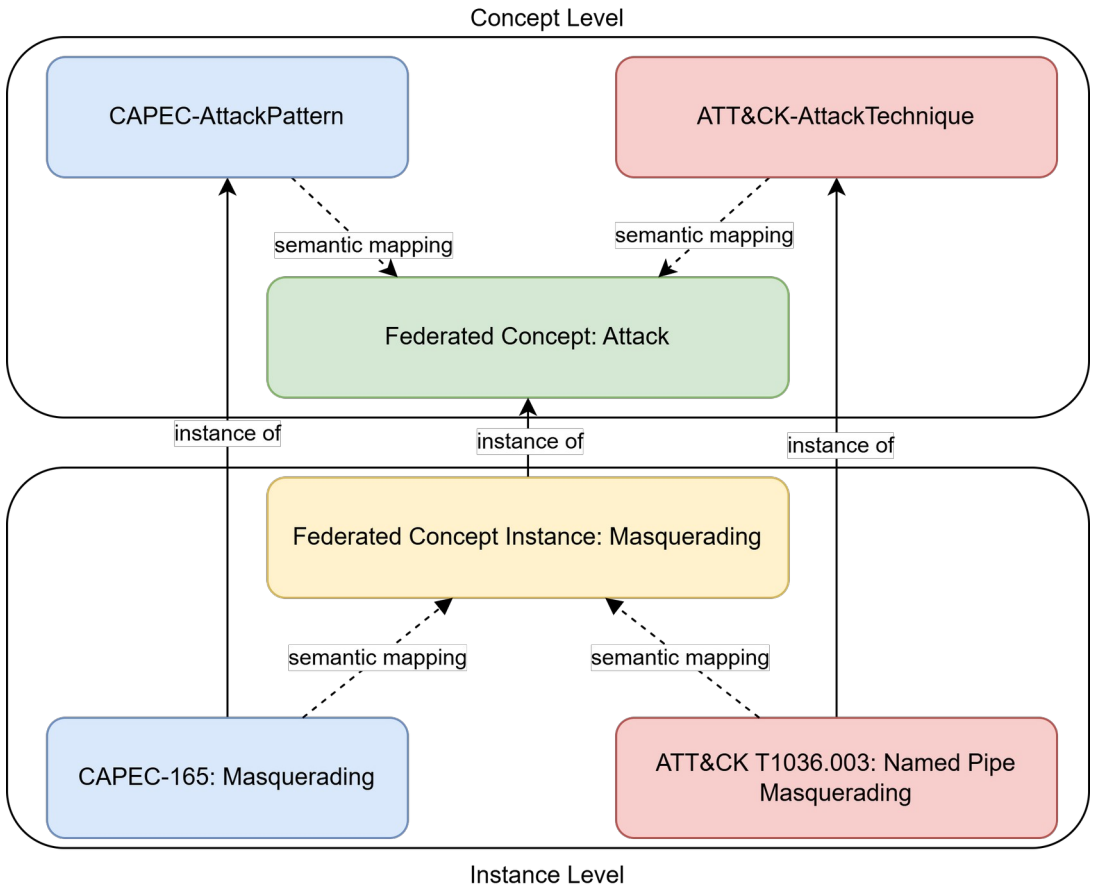
Mapping Techniques

- Explicit mappings using standardized cybersecurity identifiers

- Implicit mappings using semantic and contextual analysis by experts

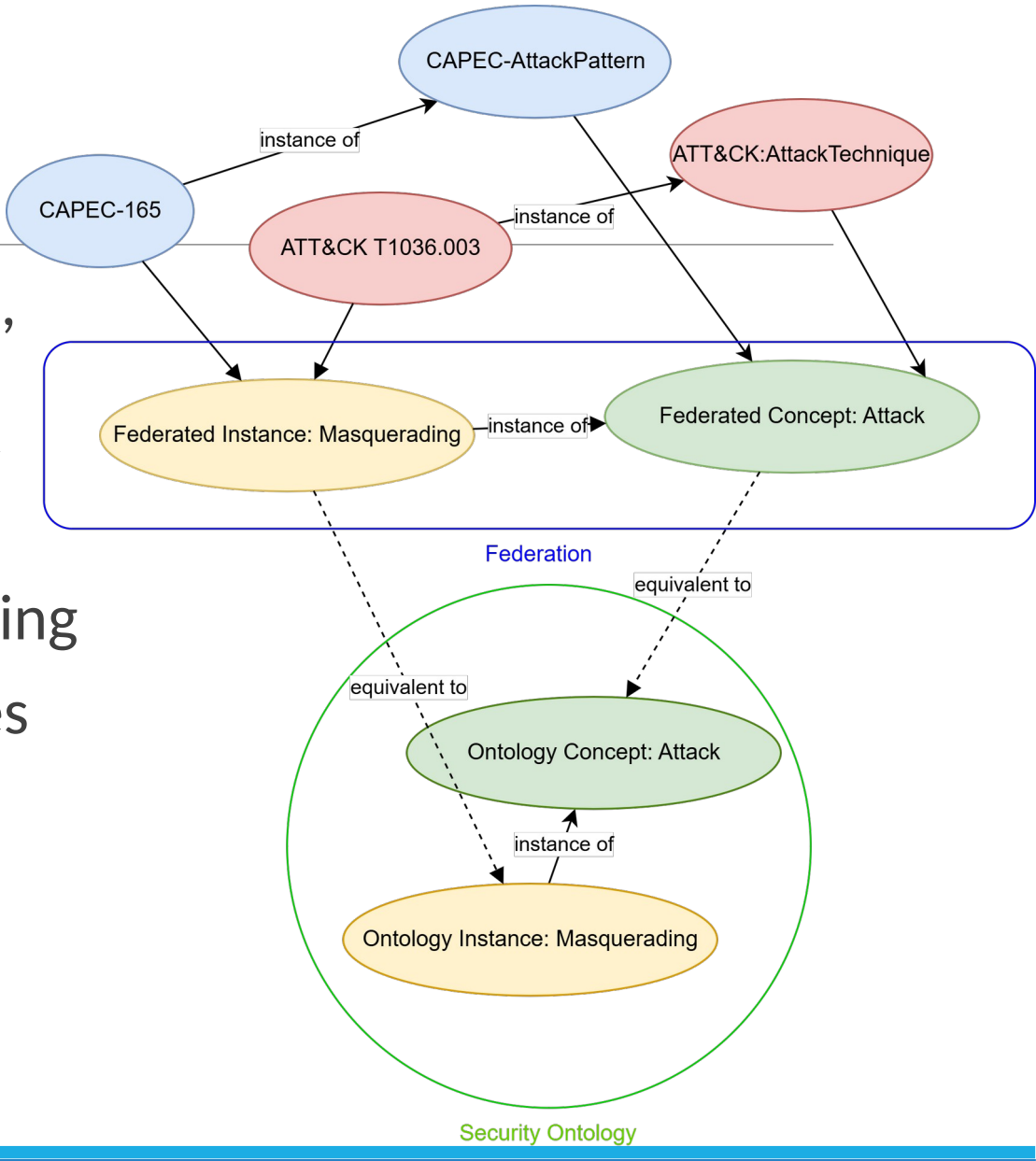
Concept Federation Process

- Unifying threat intelligence sources
  - Mapped cybersecurity concepts from multiple sources are semantically unified.
  - A federated conceptual model is built to represent common meaning across sources.
  - Each original source remains intact and independent.
  - Forms the backbone of the cybersecurity ontology.



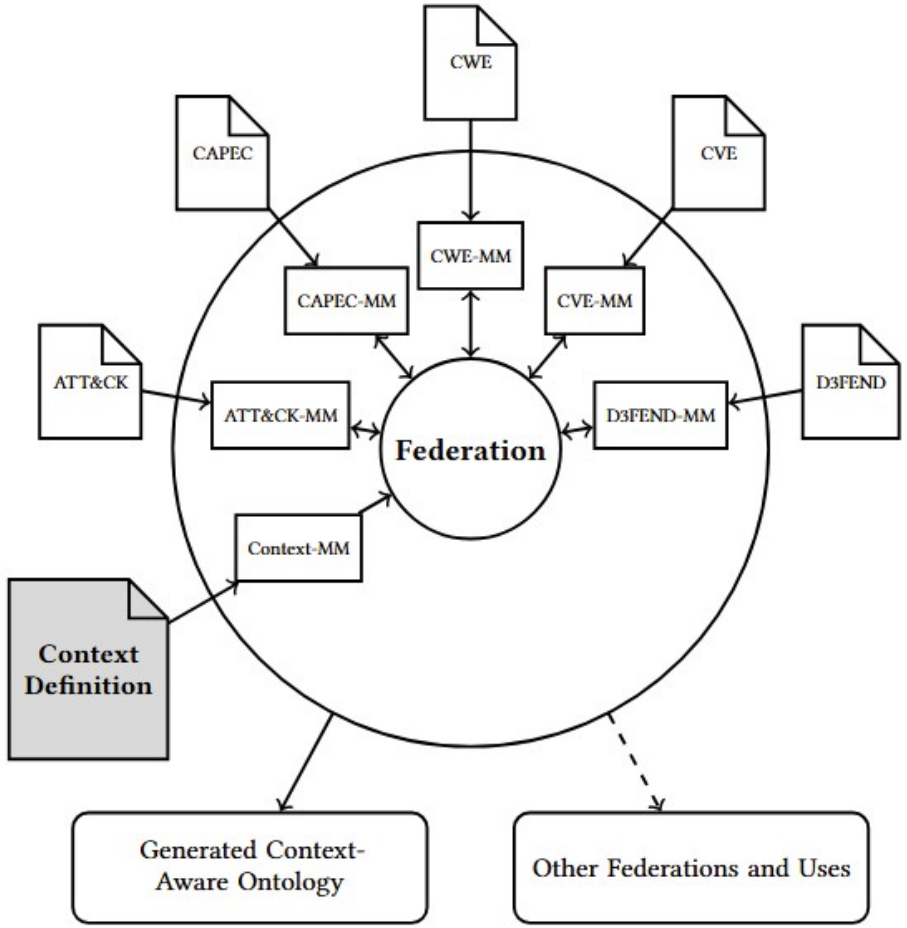
Ontology Generation

- Application of ontology in threat detection, risk assessment, and response strategies
- Structured representation of cybersecurity data
- Enhanced semantic clarity and understanding
- Allows the inclusion of private Data Sources
- Adapted to the context
- Improved threat intelligence and proactive decision-making capabilities



Project Implementation Milestones

- Established foundational federation metamodels
  - Metamodels of the resources modeled in openflexo
- Implementation via Openflexo (FML)
  - Some of the mappings were implemented using FML
- Currently integrating technology adapters to read the data resources.



Technical Challenges Encountered

- Variability in cybersecurity data formats
  - Technology adapters
- Resolving taxonomic inconsistencies
  - NLP techniques
- Ensuring accuracy and real-time updates

Anticipated Project Outcomes

- Real-time, continuously updated cybersecurity intelligence
- Effective decision-making through comprehensive federated insights
- Strengthened proactive context-aware cybersecurity

Evaluation Metrics and Approaches

- Defined Key Performance Indicators (KPIs):
  - Completeness and accuracy
  - Ontology alignment precision
- Performance assessments through response time and scalability tests
  - Query Efficiency and Response Time: Measuring query performance before and after federation
  - Quantifying system performance and increasing the number of data sources.

Future Roadmap and Enhancements

- Expand real-time data federation capabilities
- Inclusion of additional cybersecurity resources
- Generate the ontology
- Use of advanced ontology reasoning and inference
- Continuous improvement in the framework’s performance, scalability, and responsiveness