Towards a Dataspace for Cyber Threat Intelligence

Navid Rahimi Danesh

RWTH Aachen, Informatik 5
Lehrstuhl Prof. Decker

Advisors: Mehdi Akbari Gurabi, Ömer Sen

Motivation

The Crucial Role of Collaboration in Cybersecurity

- Constant challenge of cyber defense
- Interconnected nature of threats
- Collective defense
- Reinventing the wheel
- Sharing information
  - Attacker motivations, targets, techniques
  - Vulnerability severity and risk level
  - Incident response strategies

Approach: sharing cyber threat intelligence (CTI)

Motivation

The Challenges of Collaborative CTI [1]

- Operational
  - Inconsistent definitions and terminology
  - Validating quality
  - Achieving interoperability and automation
  - Safeguarding sensitive information
- Organizational
  - The risk of reputation damage
  - Establishing trust among participants
- Economic
  - Loss of client's confidence and satisfaction
- Legal/Policy
  - The risk of violating privacy laws
  - Inconsistent regulation in different countries

Challenge:
Control the access and usage of data while keeping the benefits of sharing

1. *Adam Zibak and Andrew Simpson. 2019. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19)*

Motivation

Existing Solutions for Sovereign Data Sharing

- Data sovereignty and usage control
  - Right of owner to control the data
- Dataspaces and data sovereignty
- Example: International Dataspaces (IDS)
- Reference Architecture Model
- Requirements
  - Data ecosystem
  - Security and trust
  - Federated and open
  - Data sovereignty

Thesis Goal

Investigating the Suitability of Dataspaces for CTI Sharing Use Case

- Identifying CTI sharing requirements and scenarios
- Challenges of adopting dataspace for identified scenarios
- Effect of usage control in protecting sensitive data in different scenarios

Background and related work

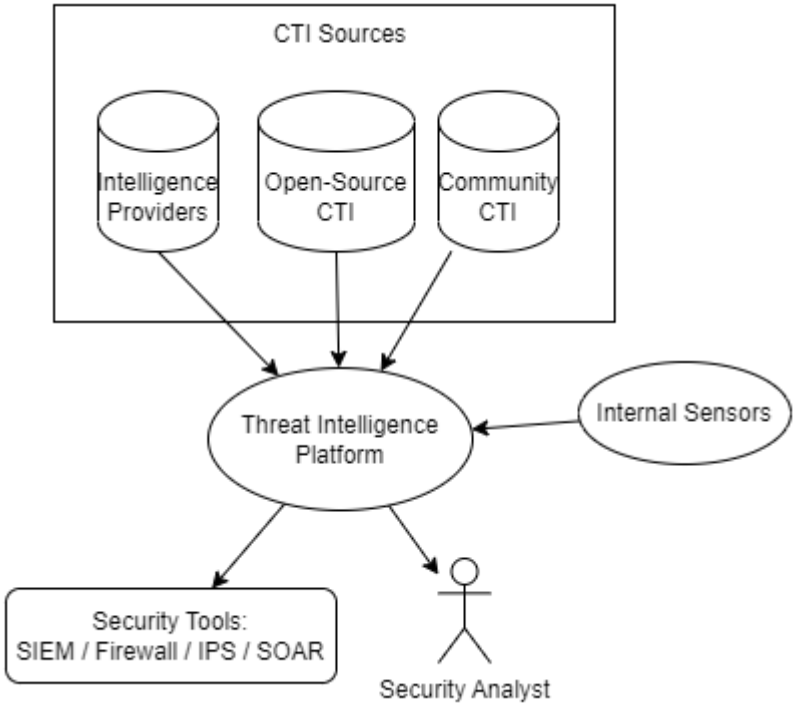
What is Cyber Threat Intelligence

CTI type	Focus	Concerned actor	Lifecycle	Benefit
Strategic – High level insights	Overall threat landscape, attacker motives, attack impacts	Executive management	Long-term	Data driven risk management
Tactical – How?	TTPs, vulnerabilities, mitigation strategies	Security Operations Center (SOC) managers, Security Analysts	Long-term	Efficiency, faster incident response
Technical – What?	Indicator of compromise (IOC) – malware signatures, malicious IPs	System admins, SOC staff	Short-term	Automation

Background and related work

Automation in Cyber threat intelligence

- Skip human delay
- Reduce costs
- Machine-readable formats
  - STIX
  - VERIS
  - IODEF



Background and related work

Existing Platforms for Cyber Threat Intelligence

Proprietary CTI feeds and services	Community platforms	Open-Source Platforms
☑ Premium curated feeds	☑ Collaborative	☑ Collaborative
☒ Not collaborative	☒ Centralized	☑ Decentralized
☒ Vendor lock-in	☒ Liability and privacy risks	☒ Hard establishment of trust
		☒ Liability and privacy risks

Background and related work

Initiatives towards dataspace standardization in Europe

- Importance of data in businesses
- European data strategy – Data governance act
  - Increate trust in data sharing
  - Increase data availability
  - Overcome technical obstacles to the reuse of the data
- GDPR
- Notable initiatives
  - International Dataspaces (IDS)
  - GAIA-X
  - FIWARE
  - Big Data Value Association (BDV)
- Goals
  - Facilitate cooperation
  - Create data and service economy
  - Data sovereignty

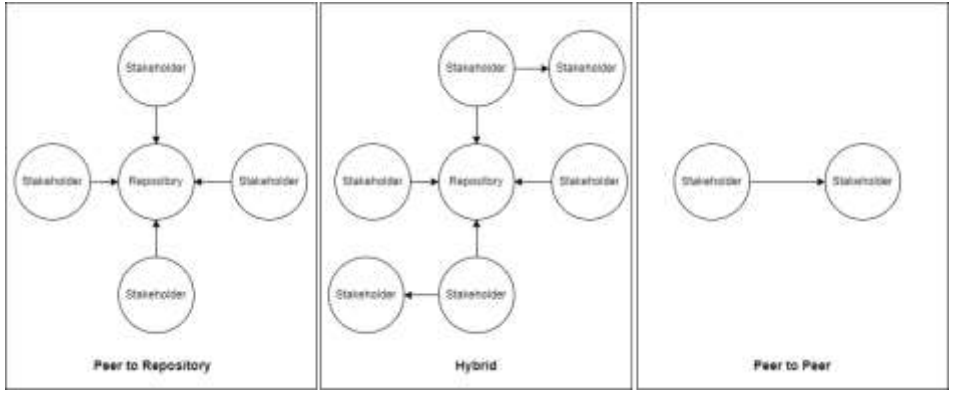
Background and related work

IDS Use Cases and Adoptions

Methodology

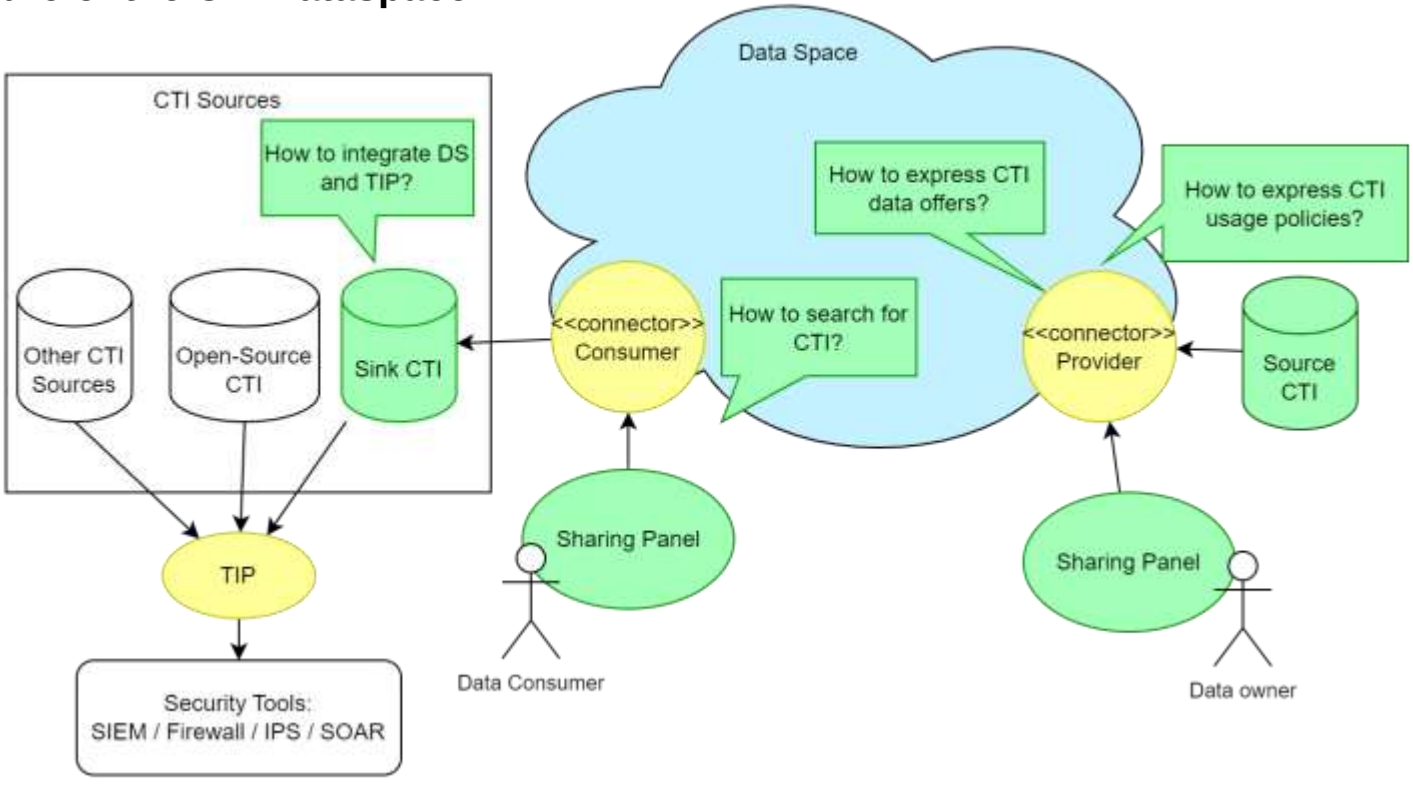
Use case and requirements

- Use case: energy sector
- Scenarios:
  - Trusted peer – Peer to peer
  - Community – Peer to repository
  - Marketplace -- Hybrid
- Requirements
  - Trust and transparency
  - Data protection (security, privacy, usage control)
  - Compliant with regulations
  - Interoperability and actionability
  - Bidirectional and collaborative



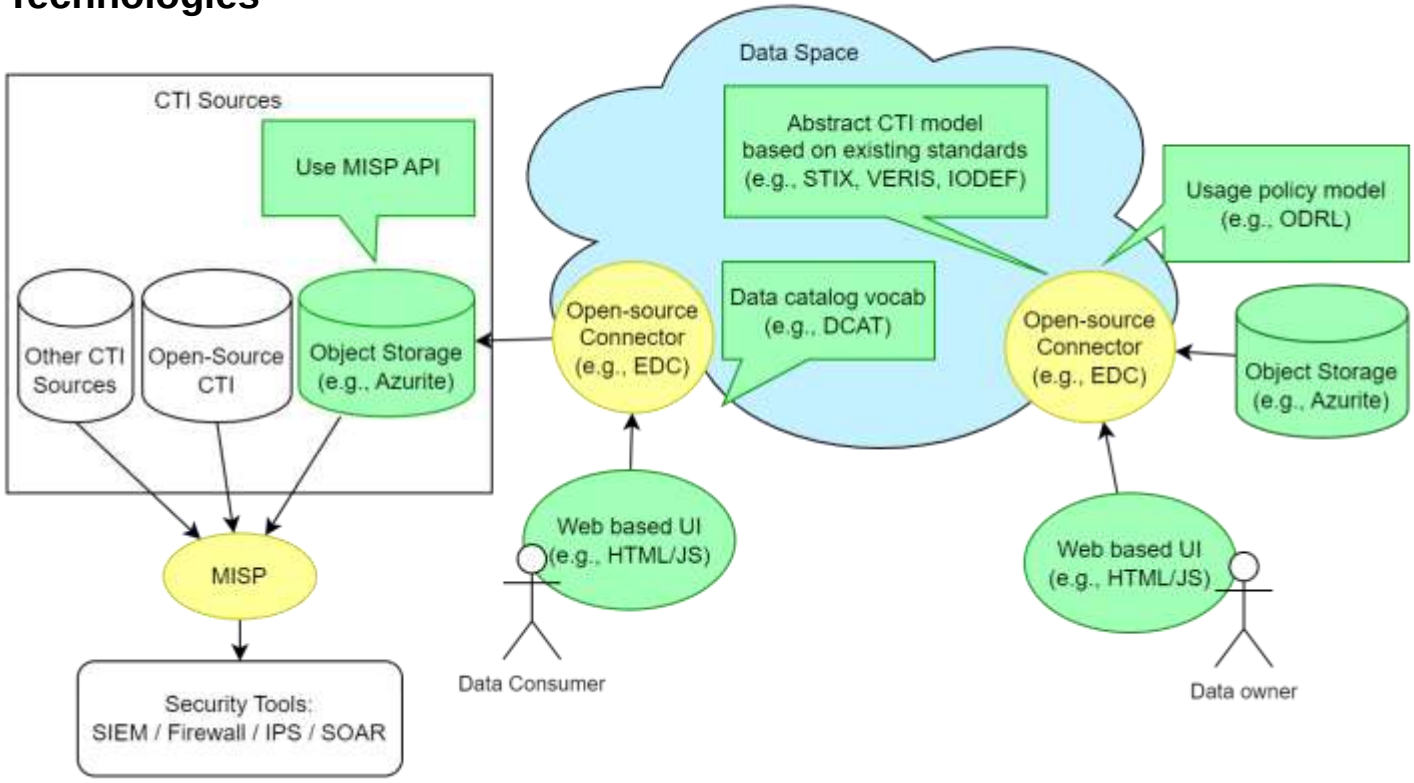
Conceptual approach

Architecture of the CTI Dataspace



Realization / Implementation

Selected Technologies



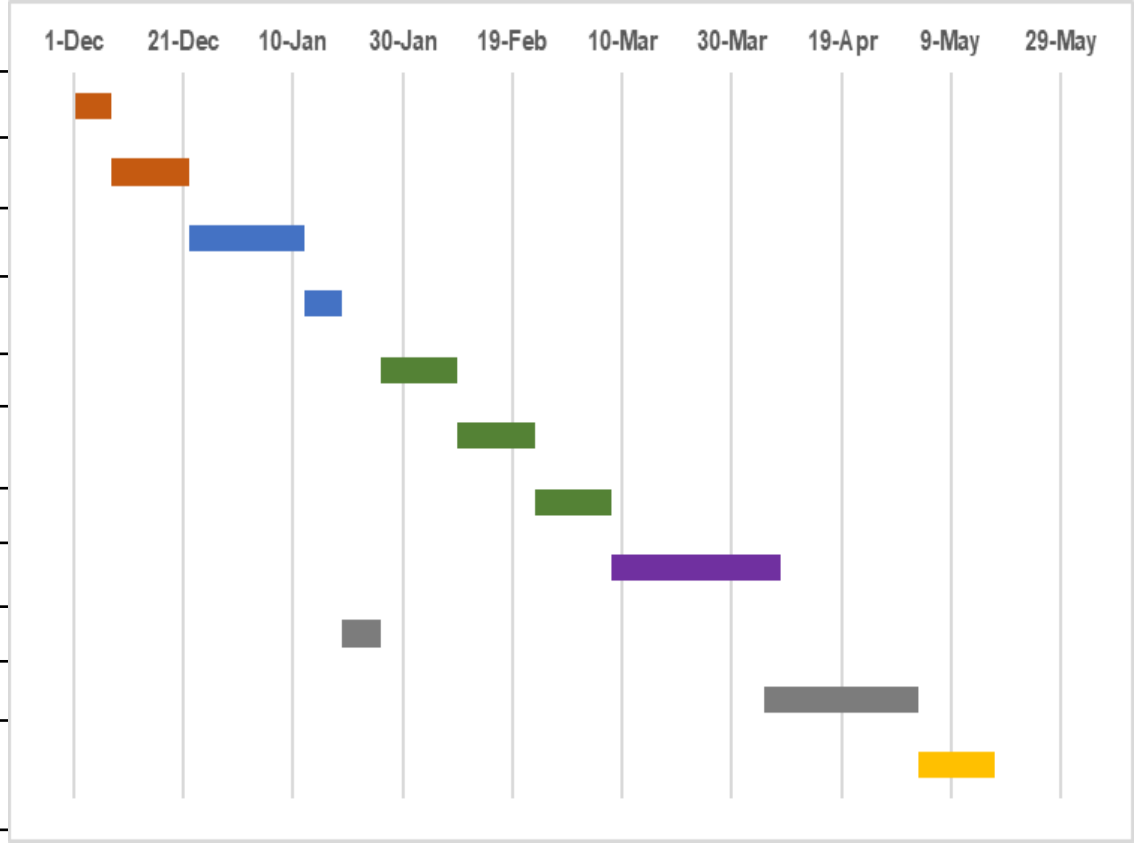
Evaluation

- Verify the architecture
  - To what extend do the design and models address the requirements?
- Comparative security analysis
  - Baseline: MISP
  - Which risks are avoided by applying usage control?
  - Analyze vulnerabilities and threats
  - How about threats in the energy sector?
- Dynamic testing using the prototype
  - Run scenarios
  - Measure performance
  - Simulate some attacks
- (Optional) User survey

Project plan / timeline / milestones

Milestones

Foundation	Related works
	Define use case scenarios
Analysis and modelling	Information Modelling
	System Design
Prototype implementation	Setup dataspace
	Integration with TIP
	Sharing panel
Evaluation	
Writing	Phase 1
	Phase 2
Buffer	

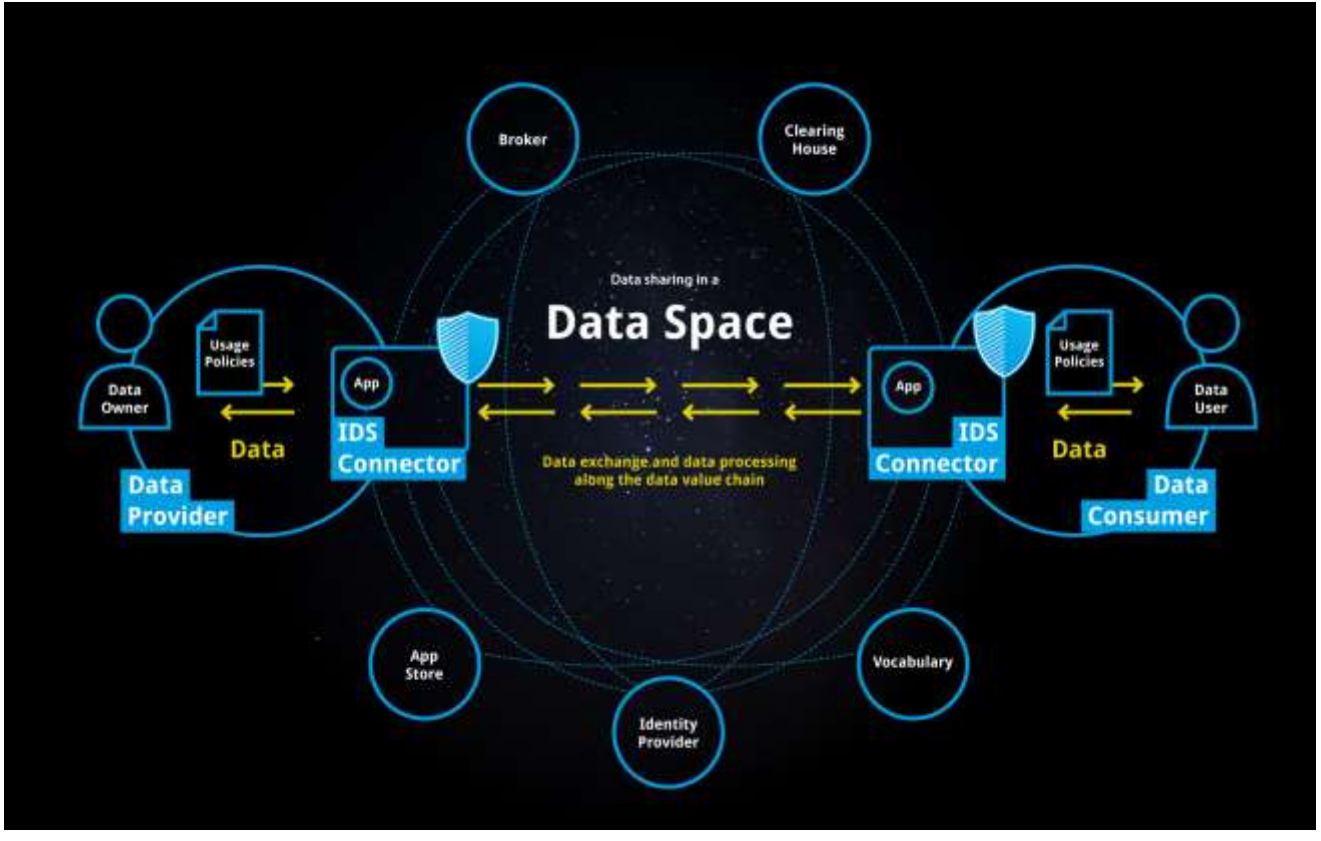


Thank you for your attention

Appendix – Dataspace Architecture

International Dataspaces

- Goals
  - Secure
  - Sovereignty (Keep control over data)
  - Federated (not a big player)
  - Data sharing
  - Data economy
- Deliverables
  - Reference architecture model – IDS-RAM
  - Certification



https://internationaldataspaces.org/why/data-spaces/