Enhancing Cyber Threat Intelligence Sharing through Data Spaces in Critical Infrastructures

Mehdi Akbari Gurabi
Fraunhofer FIT &
RWTH Aachen University
Aachen, Germany
mehdi.akbari.gurabi@fit.fraunhofer.de

Ömer Sen
Fraunhofer FIT &
RWTH Aachen University
Aachen, Germany
oemer.sen@fit.fraunhofer.de

Navid Rahimidanesh
RWTH Aachen University
Aachen, Germany
navid.danesh@rwth-aachen.de

Andreas Ulbig
Fraunhofer FIT &
RWTH Aachen University
Aachen, Germany
andreas.ulbig@fit.fraunhofer.de

Stefan Decker
Fraunhofer FIT &
RWTH Aachen University
Aachen, Germany
stefan.decker@fit.fraunhofer.de

***Abstract*—Complex cyber threats in interconnected critical infrastructures, such as smart grids and power systems, demand cooperative defense. Although sharing Cyber Threat Intelligence can strengthen cybersecurity, existing platforms often lack interoperability, trust, and data sovereignty. To bridge these gaps, we propose a data space framework that leverages IDS Connectors, Metadata Brokers, and formal policy negotiation, ensuring a decentralized environment in which organizations retain full control over shared intelligence. While data spaces are well-established in other fields, their application in sharing the threat information remains underexplored. Our evaluation demonstrates enhanced trust, data sovereignty, and practical viability of the solution for critical infrastructure sectors.**

***Index Terms*—Cyber Threat Intelligence, Data Spaces, Data Sovereignty, Critical Infrastructures**

I. Introduction

In today's evolving cyber threat landscape, effective Cyber Threat Intelligence (CTI) sharing is crucial for proactive incident response and the security of critical infrastructures such as energy and industrial control networks. Despite its benefits, organizations hesitate to share sensitive intelligence due to concerns over confidentiality and data sovereignty [9]. Recent studies [9], [13], [14] reveal that barriers include regulatory constraints, reputation risks, and challenges in maintaining trust. To overcome these, our research leverages data spaces, as defined to provide a decentralized, federated environment where data providers retain full control through robust usage policies and formal certification [5]. By employing open standards such for CTI specification, exchange procedure and integrating dynamic trust management, our solution enhances interoperability and supports rapid threat intelligence dissemination, critical for incident response in high-risk sectors [15].

This paper makes four main contributions: we propose a novel CTI sharing architecture based on data spaces that ensures secure and sovereign intelligence exchange; we demonstrate how integrating formal trust mechanisms and usage control can overcome limitations of existing open-source and commercial CTI platforms; we evaluate the framework's interoperability and dynamic trust management through a detailed feature analysis; and we situate our work within existing literature, including comparative studies on CTI sharing and incident response [15], outlining clear future directions for enhancing collaborative cybersecurity.

Our approach bridges the gap between the promise of CTI sharing and its practical adoption, enhancing incident response capabilities and fostering a resilient, cooperative cybersecurity ecosystem.

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101070052 (TANGO project) and from BMBF (03SF0694A, Beautiful).

II. Background and related work

The digitalization of critical infrastructures, such as smart grids, has significantly boosted efficiency but also expanded the attack surface [27]. Adversaries exploit this complexity with data injection [29], DDoS [28], APTs [30], and ransomware [31], underscoring the need for robust cybersecurity and effective CTI sharing. Regulatory frameworks reflect this urgency: the EU's NIS and forthcoming NIS2 Directives [17], ISO/IEC 27001, the Digital Operational Resilience Act (DORA) for financial services, the Cyber Resilience Act (CRA) for critical products, and the U.S. Defense Cyber Crime Center's DC3/DCISE program, and U.S. policies such as CISA and EO13636 [9], all require or strongly encourage reporting and sharing [25], often with legal penalties for noncompliance. While mandating collaboration, these regulations also provide safeguards, standardized procedures, and cross-border coordination [10]. Our data space architecture directly addresses these requirements by embedding compliance rules into usage control and certification processes, enabling secure, sovereign information exchange across diverse jurisdictions.

CTI, defined as the collection, analysis, and dissemination of threat information [19], is organized into strategic, tactical,

and technical levels [11]. Effective CTI sharing, however, faces challenges such as lack of standardization, trust issues, data accuracy, free-riding [19], and varying privacy laws [8]. Early sharing models used centralized repositories and peer-to-peer networks [11], while platforms like Information Sharing and Analysis Centers (ISACs) and Threat Intelligence Platforms (TIPs) have limitations regarding scalability and data control. Chantzios *et al.* [12] compare current platforms on criteria such as interoperability and flexibility, noting that open-source platforms like MISP [20], which support de facto standards like STIX [21], rely heavily on manual vetting, while commercial systems compromise data sovereignty.

Research on sharing communities [13] and studies on open, crowd-sourced CTI [14] reveal that social trust and non-standardized practices hinder effective sharing. Blockchain and privacy-preserving techniques have been explored [38], but they introduce scalability issues. A promising alternative is the application of data space concepts, as seen in International Data Spaces (IDS) and Gaia-X [3], which offer a federated, decentralized framework. In particular, IDS is a standardized, secure architecture enabling trustworthy data exchange among organizations while ensuring data sovereignty through mechanisms such as connectors, brokers, and usage control policies. This framework ensures that data providers retain control through enforceable usage policies and digital certificates, while supporting open standards for interoperability. Although the data spaces demonstrated maturity through projects in other domains [6] and were also explored in the field of digital energy [7], their potential for knowledge sharing in cybersecurity remains underexplored. As a supporting claim for this potential, we refer to Schlette *et al.* [15], who highlight that effective incident response requires fast and secure data exchange while preserving provider rights.

An analysis of relevant literature [33], [34], [35], [32] reveals a clear need for a CTI sharing framework that: (a) leverages open standards for interoperability across diverse systems, (b) incorporates formal trust mechanisms through participant certification and dynamic trust management, (c) provides robust usage control [4] to maintain data sovereignty even after sharing, and (d) supports rapid incident response through automated, secure intelligence exchange. By bridging the technical and social dimensions of intelligence sharing, our framework offers a scalable and secure solution particularly suited for critical infrastructure sectors, where delayed or insecure CTI exchange can have severe consequences. Our conceptual design represents the first exploration of this approach in the CTI domain, aligning with initiatives like IDS, which promote secure and sovereign data infrastructures in Europe [5]. To conclude this section, Table I summarizes the key aspects addressed in the relevant literature and details how we address these aspects in our solution.

III. Methodology

This work employs a Design Science Research (DSR) methodology [1] to develop and evaluate a data space artifact, based on the IDS framework, enhancing CTI sharing in critical infrastructures. A prototype was built and tested against criteria such as performance, security, compliance, and usability, demonstrating its effectiveness and providing evidence-based insights for future research.

TABLE I
SUMMARY OF RELATED WORKS ON CHALLENGES IN CTI SHARING AND ADDRESSED ASPECTS

Aspect	[33]	[34]	[35]	[32]	This Work
Data Sanitization	✓	✓	✓	✓	✓
Sharing Policies			✓	✓	✓
Trust Modeling		✓		✓	✓
Energy Sector Application			✓		✓
Usage Control					✓

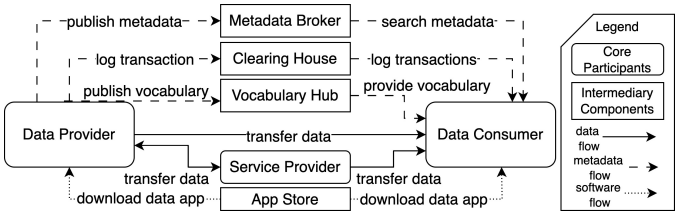

Fig. 1. IDS roles and their interactions, adapted from [2].

A. Research Approach

A thorough Requirements Analysis defines the functional and non-functional needs for designing a data space solution that enables CTI sharing while meeting stakeholder and regulatory requirements. Requirements were gathered by: (1) analyzing existing research on CTI sharing, data sovereignty, and data spaces, with key studies highlighting challenges; (2) reviewing relevant EU directives and regulations; and (3) crafting scenarios based on qualitative insights from our case studies.

1) Stakeholder Identification: The first step involved identifying all relevant stakeholders to understand their needs, expectations, and constraints. Table II lists the categories of entities involved in cybersecurity CTI sharing along with their descriptions.

TABLE II
CATEGORIES AND DESCRIPTIONS OF ENTITIES IN CYBERSECURITY CTI SHARING FOR CRITICAL INFRASTRUCTURES

Category	Description
Critical Infrastructure Operators	Entities responsible for operating essential services like smart grids.
Security Operation Centers (SOCs)	Entities responsible for securing services and systems in critical infrastructures.
Cybersecurity Agencies and CERTs	National and regional CERTs that coordinate responses to cyber incidents.
Regulatory Bodies	Organizations ensuring compliance with regulations such as NIS 2 and GDPR.
Technology Providers	Vendors supplying cybersecurity solutions and platforms.
Standardization Bodies	Groups like OASIS that develop CTI standards (e.g., STIX/TAXII, CACAO).

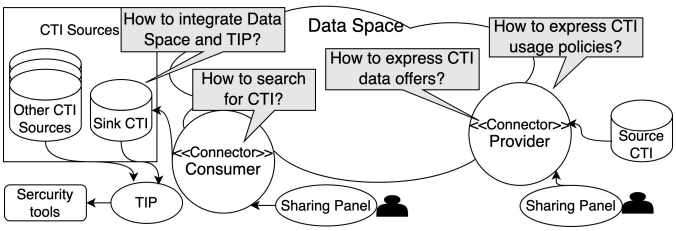

Fig. 2. The conceptual design of a data space for CTI sharing and the four main design questions essential for its realization at a technical level.

2) Requirements: Based on the information obtained, the functional and non-functional requirements were identified and listed as F.R:* and N.F.R.*, respectively, in the table III.

B. Conceptual Design

Based on the derived requirements, we developed a CTI sharing framework that leverages the data space paradigm, drawing specifically on the IDS reference architecture [2]. Our design creates a federated, secure environment where organizations can exchange CTI data while retaining control over its usage. This is accomplished through IDS Connectors, deployed by each organization as gateways that enable standardized, secure communication without a central authority. Figure 2 presents the conceptual design and outlines four key technical design questions necessary for its realization.

Our design enhances existing CTI sharing solutions by embedding trust and usage control into the technical infrastructure, ensuring secure and automated intelligence exchange while preserving data sovereignty. Various CTI sources, such as security tools and external feeds, generate threat intelligence, which is aggregated and processed by a TIP before being collected and prepared for sharing within the data space. We define a TIP as a specialized system that aggregates, correlates, and normalizes threat data (e.g., IoCs, TTPs) from multiple sources before forwarding it to the data space. The design allows multiple TIP instances or parallel data flows to distribute the processing load and avoid bottlenecks. The data space provides a secure environment for exchanging CTI, where connectors facilitate interactions between CTI providers and consumers, ensuring compliance with security policies and data sovereignty principles; providers supply CTI data and define usage policies, while consumers search for, request, and integrate intelligence into security tools. This approach addresses key challenges, including integrating data spaces with TIPs, defining structured and interoperable CTI data offers, enforcing usage policies for security and compliance, and enabling efficient search within the data space.

IV. Realization

We used the 4 + 1 architecture model [26] to develop and validate our prototype, demonstrating the core functionality, evaluating performance, and ensuring alignment with the conceptual framework.

Central to our design is the IDS Connector, which securely exchanges CTI data, enforces machine-readable usage policies to ensure compliance and data sovereignty, and establishes trust through digital certificates and dynamic attribute provisioning. As an example of the data sovereignty enhancement, data providers can limit distribution to specific recipients (e.g., to exclude direct competitors). A policy-based exclusion list enables providers to define rules so that intelligence is accessible only to authorized non-competing parties. This feature mitigates competitive risks and preserves trust in a multi-organization sharing ecosystem. To support data sharing agreements, the architecture includes Metadata Brokers for registering CTI assets, Vocabulary Providers for standardizing data models, and automated Policy Negotiation mechanisms that facilitate contract agreements.

1) Scenario: We present three practical scenarios for CTI sharing in critical infrastructure settings. In the first scenario, an organization complies with regulatory mandates by sharing incident data with a national CERT after detecting a breach via its managed security service provider, ensuring sensitive information is handled according to strict usage policies. The second scenario illustrates a collaborative environment where multiple security vendors jointly process and enhance incident data, starting with event collection, followed by analysis and incident response, while maintaining control over data usage for potential commercial benefits. In the third scenario, a national CERT notifies a constituent organization about an emerging threat, employing automated response systems and enforced access controls (e.g., via TLP labels) to ensure rapid and secure incident mitigation. These scenarios collectively demonstrate that the proposed CTI sharing framework effectively addresses data sovereignty, trust, and interoperability challenges in diverse use cases.

2) Functional view: For the Functional View we decomposed the high-level requirements for CTI sharing into distinct, interrelated components mapped from the IDS architecture. Specifically, interoperability is achieved through standardized data exchange via connectors and metadata brokering, while flexibility is supported by shared vocabularies, data adapters, and extensible data apps that integrate seamlessly with diverse CTI sources. Security and trust are ensured by establishing digital identities and implementing dynamic trust and reputation monitoring, which continuously verify participants' credentials. In parallel, data privacy and sovereignty are enforced through technical usage contracts and automated sanitization processes that control data distribution and usage. Finally, commercial activities are enabled through mechanisms for billing, data processing services, and an app store, thus fostering a sustainable, federated ecosystem for CTI sharing that meets both operational and regulatory demands [12] [16].

3) Process view: The Process View illustrates the dynamic interactions and data flows among the various components of the CTI sharing platform. It details the end-to-end processes starting with the onboarding and certification of participants, ensuring that only trusted entities gain access through formal evaluation and digital certificates. Once onboarded, data offers

TABLE III
FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

ID	Requirement	Requirement Description	Rationale
F.R.1	Interoperability with CTI Standards	The system must support standard CTI formats and protocols such as MISP and STIX to facilitate seamless data exchange.	Ensures compatibility with existing tools and allows participants to share intelligence without format barriers.
F.R.2	Secure Data Sharing Mechanisms	Implement secure communication channels (e.g., TLS encryption) for all data exchanges.	Protects sensitive CTI data from interception and unauthorized access during transmission.
F.R.3	Data Sovereignty and Usage Control	Enable data providers to define and enforce usage policies on shared CTI, using technologies like Attribute-Based Access Control (ABAC) and Usage Control models.	Allows organizations to retain control over their data, addressing concerns over misuse and compliance.
F.R.4	Participant Authentication and Trust Management	Provide robust authentication mechanisms (e.g., digital certificates) and manage participant identities and roles.	Establishes trust in the network by ensuring only authorized and verified entities can participate.
F.R.5	Auditability and Traceability	Log all transactions and data accesses for auditing purposes, maintaining a tamper-evident record.	Supports accountability, compliance reporting, and incident investigation.
F.R.6	Dynamic Discovery of Data and Services	Allow participants to discover available CTI data and services dynamically through metadata catalogs or brokers.	Facilitates efficient sharing by making relevant intelligence easily accessible.
N.F.R.1	Compliance with Regulations	The solution must comply with the regulations such as NIS and NIS 2 Directives, CRA, and GDPR.	Ensures legal operation (e.g., within the EU) and builds trust among participants.
N.F.R.2	Scalability	The architecture should support scaling to accommodate increasing numbers of participants and larger volumes of CTI data.	Enables wider adoption and long-term usability.
N.F.R.3	Performance Efficiency	The system should minimize latency in data sharing to allow timely threat detection and response.	Timeliness is critical in cybersecurity to mitigate threats effectively.
N.F.R.4	Reliability and High Availability	Ensure continuous operation with minimal downtime, possibly through redundancy and failover mechanisms.	Critical infrastructures require dependable systems to maintain security posture.
N.F.R.5	Usability and Accessibility	Provide user-friendly interfaces and support for automation to encourage adoption.	Lowering the barrier to entry increases participation and effectiveness.
N.F.R.6	Modularity and Extensibility	Design the system with modular components that can be updated or replaced without affecting the whole system.	Facilitates maintenance, upgrades, and integration of new technologies.

are published through connectors and metadata brokers, where contract negotiation processes establish enforceable usage agreements. Subsequently, the actual data exchange occurs between provider and consumer connectors via secure communication protocols, with the Policy Engine enforcing the agreed-upon usage control policies through its various components (Policy Administration Point, Policy Decision Point, Policy Execution Point, and Policy Information Point). This orchestrated flow—augmented by mechanisms, for instance, Dynamic Attribute Provisioning for real-time trust validation to ensure that all exchanges are both secure and compliant with data sovereignty requirements.

4) Development view: The Development View outlines the technical architecture of the IDS-based CTI sharing platform by detailing the core and supporting components that facilitate secure and sovereign data exchange. At its center is the Connector, which provides the necessary APIs for data exchange and implements IDS protocols to handle communications, remote attestation, and application container management. The system also integrates IDS Apps for specialized data processing, a Policy Engine that enforces usage control policies and manages contract negotiation, and an Identity Provider that issues digital certificates and dynamic tokens to ensure authenticated interactions. Together, these components enable distinct roles for provider and consumer connectors, ensuring that data is securely transmitted and its usage is strictly controlled, while maintaining interoperability, data sovereignty, and dynamic trust in alignment with IDS principles [2].

5) Physical view: The Physical View defines the ecosystem in which our IDS-based CTI sharing platform operates by outlining distinct roles and their interactions. Core participants, including data providers, consumers, and service providers, are responsible for executing secure transactions with well-defined usage policies, while intermediary roles (such as metadata brokers, vocabulary intermediaries, app store providers, and clearing houses) enable efficient data discovery, standardized exchange, and economic settlement. Supporting roles, such as software developers and certification bodies, ensure that the technological components are robust, compliant, and continuously updated. This structured business model not only facilitates a sustainable and commercially viable CTI sharing network but also reinforces trust and accountability through formal certification and dynamic trust management mechanisms, addressing key challenges identified in the literature on CTI sharing and open communities [13] [14] [12].

A. Prototype Development

To demonstrate the feasibility of enhancing CTI sharing through data spaces in critical infrastructure contexts, we developed a prototype based on the IDS framework. This section outlines the key steps and considerations involved in the prototype development, focusing on system architecture, component selection, integration, and deployment. We identified and assessed the most suitable open-source components for implementing our IDS-based CTI sharing platform. We compared several IDS connectors, IDS Dataspace Connector (DSC) [1], Eclipse Dataspace Connector(EDC) [2], the TRUsted

[1]https://github.com/International-Data-Spaces-Association/DataspaceConnector

[2]https://github.com/eclipse-edc/Connector

Engineering (TRUE) [3], Trusted Connector by Fraunhofer AISEC [4], IDS Integration Toolbox [5], and TNO Security Gateway (TSG) [6] connectors, against criteria such as active maintenance, comprehensive documentation, and support for usage control enforcement. Based on these factors, only EDC, TRUE, and TSG met the first requirement and consequently, only EDC and TRUE met our second criterion. Concurrently, we assessed MYDATA [7], LUCON [8], Degree [9], Platoon [10], and EDC as available policy engines on Technology Readiness Level (TRL), flexibility, completeness of supported policy classes, and documentation quality. We ultimately selected MYDATA as the most appropriate solution. It is more mature (i.e., TRL 7-8 compared to 5 (LUCON) and 4 (Degree)); second, it supports policy enforcement in the infrastructure (e.g., database and external systems) and client systems and services (e.g., operating system, external servers); and third, it supports all IDS-defined policy classes [36]. A compatibility analysis further confirmed that the TRUE Connector, with its built-in support for MYDATA, provided the optimal foundation for our prototype.

The prototype architecture adheres to the IDS Reference Architecture Model and includes several key components. IDS connectors act as gateways for data exchange between organizations, with both a Provider Connector and a Consumer Connector implemented. The usage control system enforces data sovereignty by implementing usage policies through a policy enforcement framework. A metadata broker facilitates the discovery of data assets by cataloging and advertising available CTI resources. An identity provider, which includes a certification authority and dynamic attribute provisioning service, manages identity, authentication, and authorization for participants. Custom applications, known as Data Apps, are deployed within the connectors to handle specific data processing tasks, such as data sanitization or format translation. Figure 3 depicts the resulting components.

We adopted the Usage Control Policy Language (UCPL), an extension of the Open Digital Rights Language (ODRL), to specify usage policies. We integrated a policy enforcement engine compatible with the IDS Connector to enforce these policies on both the data provider and consumer sides. The metadata broker was implemented based on existing IDS infrastructure to facilitate data asset discovery. Furthermore, we set up a certification authority to issue X.509 certificates and deployed a Dynamic Attribute Provisioning Service (DAPS) to provide dynamic attributes for authentication and

[3]https://github.com/Engineering-Research-and-Development/true-connector

[4]https://github.com/Fraunhofer-AISEC/trusted-connector

[5]https://git.openlogisticsfoundation.org/archive/ids/ids-integration-toolbox

[6]https://gitlab.com/tno-tsg

[7]https://www.dataspaces.fraunhofer.de/en/software/usage-control/mydata.html

[8]https://industrial-data-space.github.io/trusted-connector-documentation/docs/usage_control/

[9]https://www.dataspaces.fraunhofer.de/en/software/usage-control/d.html

[10]https://github.com/Engineering-Research-and-Development/true-connector-uc_data_app_platoon

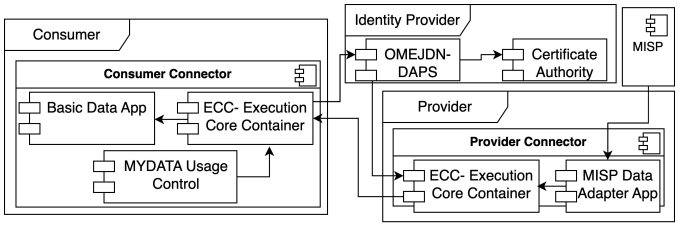

Fig. 3. Deployed components of CTI sharing data space and their interactions.

authorization. Custom Data Apps were developed for CTI-specific data processing tasks, such as a Data Sanitization App that removes sensitive information from CTI data prior to sharing, and a Format Translation App that converts CTI data into MISP format. The Usage Control Engine was deployed within the connectors to enforce policies. Usage policies were defined to specify permissions, prohibitions, and obligations for shared CTI data, and these policies were deployed to the Policy Enforcement Point within the connectors. The Provider Connector published metadata about available CTI data assets to the metadata broker, ensuring compliance with the IDS Information Model for compatibility. Participants and components were registered with the identity provider, and the necessary certificates and tokens were issued to enable secure communication between entities. The prototype was deployed in a controlled virtualized environment that simulated multiple organizations, with secure communication channels configured using TLS to encrypt data in transit. While the prototype focused on core functionality, the architecture was designed for scalability, allowing for the addition of more connectors and participants.

V. Evaluation and Analysis

The investigation procedure was structured to comprehensively evaluate the CTI sharing solution across four independent dimensions. First, we applied the system to real-world use case scenarios to demonstrate its practical applicability in critical infrastructure settings. Second, we validated the policy framework by comparing its expressiveness and enforcement capabilities against established standards, such as the Information Exchange Policy 2.0. Third, we conducted technical tests to measure performance metrics, including latency and resource consumption, ensuring that the system operates efficiently under realistic loads. Lastly, we performed an analytical verification of the overall solution, assessing whether the solution meets the identified requirements and outperforms existing CTI sharing platforms in terms of trust, interoperability, and data sovereignty.

A. Use Case Application and scenario-based analysis

We proceed with the scenario we described in section IV-1 and refine it with more details to be able to simulate it with our prototype. It comprises three data exchanges with different data and associated policy, which is illustrated in Fig. 4.

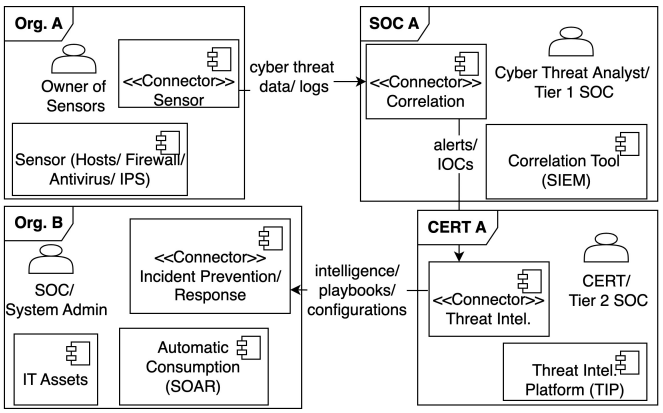

Fig. 4. Validation scenarios: four participants, each operating a connector and using respective backend systems exchanging different data types.

1) SC1: Organization Outsourcing Security Analysis: Org. A, a small electricity provider operating a smart grid (a Critical Infrastructure subject to incident reporting), outsources its security monitoring to an external SOC (*SOC A*) because it lacks an in-house SOC. *Org. A* continuously shares its security sensor data with *SOC A*, which promptly notifies it upon detecting an anomaly. To test this exchange, a log dataset (containing personal data and internal network topology) was used, necessitating GDPR compliance. A Sanitization App (an IDS App developed by peers in the energy sector) automatically anonymizes personal data, and usage policies are set via a Policy Administration Point interface to restrict data access, allowing only a specific IDS App for log management (similar to a SIEM) and granting access exclusively to EU-based participants, with further restrictions for external apps (only aggregated data accessible in Germany).

2) SC 2: SOC Sharing Incident Data with the Community: After analyzing data from *Org. A*, *SOC A* detects an incident and extracts the related IoCs. *SOC A* then shares these IoCs within its CTI sharing community (an energy-sector ISAC) to assist peers and obtain financial incentives. The community utilizes a provider-defined billing scheme and a metadata broker to catalog available intelligence. New members are registered with the identity provider, and their membership is recorded in the DAPS as an attribute. Consequently, *SOC A* verifies each consumer's DAT token to ensure that only approved community members gain access. In our scenario, *CERT A* is the consumer.

3) SC3: National CERT Notifying a Constituent Organization: In this scenario, a national CERT (*CERT A*) alerts a constituent organization (*Org. B*) about a high-risk threat. To ensure proper handling, *CERT A* enforces a usage policy that restricts access exclusively to the Security Orchestration, Automation, and Response (SOAR) system of *Org. B*, enabling rapid, automated response while safeguarding classified details. Additionally, the CERT issues a detailed threat report for manual review by the SOC analyst in *Org. B*, with TLP labels applied to control further dissemination.

We evaluate our prototype by simulating these distinct CTI sharing scenarios that represent common use cases in critical infrastructure environments. In the first scenario, an electricity provider outsources its security monitoring to an external SOC; here, data is sanitized and shared under strict usage policies to ensure regulatory compliance. The second scenario demonstrates a CTI sharing community where a SOC disseminates incident data, such as IoCs and threat indicators, for collaborative analysis and commercial benefits among trusted partners. Finally, the third scenario involves a national CERT notifying a constituent organization about a new threat, with usage policies that restrict access to designated incident response systems. Together, these scenarios confirm that our solution effectively enforces data usage policies and maintains data sovereignty, and supports secure information exchange for incident response.

B. Validation of the Policy Framework

We validate our IDS-based policy framework by benchmarking it against the widely recognized Information Exchange Policy (IEP) framework [37]. We evaluated the expressiveness of our policy specification language by mapping each IEP policy class to corresponding IDS vocabulary elements and then assessed the feasibility of automatically enforcing these policies using our policy engine. A four-level scale, ranging from ZERO (no additional enforcement needed) to HIGH (requiring significant extension or strict monitoring), was employed to estimate the implementation effort for each policy class. The results showed that while the IDS information model sufficiently covers several key policy classes (e.g., ENCRYPT-IN-TRANSIT, TLP:CLEAR), some classes such as CONTACT FOR INSTRUCTION and TLP:AMBER necessitate vocabulary extensions and additional enforcement mechanisms. Overall, the evaluation confirms that our policy framework effectively addresses the critical requirements for controlled CTI sharing, ensuring robust data sovereignty and secure incident response while highlighting areas for future enhancement. Table IV shows the assessment of the policies.

TABLE IV
MAPPING OF IEP TO IDS POLICY ENGINE; COLUMN 2: THE SUGGESTED IDS INFORMATION MODEL OBJECT TO EXPRESS EACH IEP POLICY CLASS. COLUMN 3: AN ESTIMATE OF THE IMPLEMENTATION EFFORT TO ENFORCE THE POLICY AUTOMATICALLY.

IEP Policy Class	IDS Information Model Object	Imp. Difficulty
ENCRYPT-IN-TRANSIT	ids:DistributeEncryptedAgreement	ZERO
CONTACT FOR INSTRUCTION	odrl:Duty & Extended Vocabulary Needed	HIGH
INTERNALLY VISIBLE	Extended Vocabulary Needed	HIGH
EXTERNALLY VISIBLE INDIRECT	Extended Vocabulary Needed	HIGH
EXTERNALLY VISIBLE DIRECT	Extended Vocabulary Needed	ZERO
NOTIFY-AFFECTED-PARTY	ids:Permission and odrl:Distribute & Additional Vocabulary (Affected)	LOW
TLP:RED	ids:Prohibition & odrl:Distribute	LOW
TLP:AMBER	Extended Vocabulary Needed (Need-to-know)	HIGH
TLP:GREEN	odrl:Distribute & odrl:Recipient & odrl:Refinement & odrl:NextPolicy	LOW
TLP:CLEAR	odrl:Permission & odrl:Distribute	ZERO
PROVIDER-ATTRIBUTION	odrl:Distribute & odrl:Attribute	LOW
UNMODIFIED-RESALE	odrl:Commercialize & odrl:Distribute	MED.

C. Technical evaluation

We present the technical evaluation of the CTI sharing prototype by measuring performance metrics such as latency and resource consumption. In these tests, data extracted from a public MISP feed was segmented into various file sizes, and the average time taken to transfer the data from a provider connector to a consumer connector was recorded. The experiments, conducted on a virtual machine with an Intel Xeon processor and 32GB RAM, demonstrated that the entire process, including authentication, authorization, and policy enforcement, adds only a minimal overhead, with latency ranging between 1 and 3 seconds. We assumed the latency acceptable based on typical CTI use cases, where rapid but not strictly sub-second delivery is sufficient for most incident response workflows. The delay corresponds to a single file transmission from one provider to one consumer under moderate load; however, the system supports parallel transmissions rather than strictly sequential sends. If expanded to hundreds or thousands of subscribers, throughput can be increased by deploying additional connector instances or scaling the underlying infrastructure, reducing the possibility of severe lengthy delays. These results demonstrate the feasibility of a proof-of-concept for the IDS-based CTI sharing solution, which is operated in specified scenarios, ensuring timely dissemination of threat intelligence. The measurements are illustrated in Figure 5.

D. Analytical Verification

We provide an analytical verification of the proposed solution by systematically mapping its design features to the

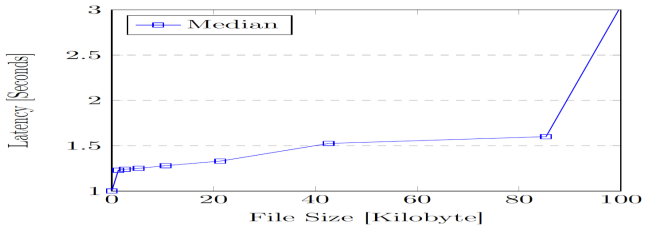

Fig. 5. Measurement of latency of a data exchange in our platform.

critical requirements identified in our earlier analysis. In this phase, we assess how the integration of IDS-based components, such as secure connectors, dynamic policy enforcement via the policy engine, and robust identity management, satisfies key criteria like interoperability, trust management, and data sovereignty. We compare our solution with MISP, a widely used open-source solution, and ThreatConnect[11], a proprietary solution. The evaluation demonstrates that our architecture meets its design objectives by enabling controlled, federated CTI sharing with minimal performance overhead. This verification confirms that our solution not only aligns with IDS principles but also addresses the challenges in CTI sharing and incident response. Table V shows the summary of our analysis.

VI. DISCUSSION

This study shows that integrating CTI sharing into a data space framework based on IDS can address common barriers related to trust, interoperability, and data sovereignty. By ensuring only authorized entities access CTI, the proposed solution alleviates misuse concerns. It also supports integration with standards like MISP or STIX, enabling broader collaboration across sectors and aligning with emerging EU regulations (e.g., NIS2). Moreover, the approach leverages economic incentives such as data monetization and flexible billing, driving more active, high-quality CTI sharing. In this way, this secure, interoperable, and scalable platform supports more effective collaborative cyber defense strategies.

Regarding operational oversight, our data space can be managed by existing bodies like CERTs or ISACs, leveraging their authority. Alternatively, each subscriber may deploy its own connector in a federated model without requiring a new central operator. Stakeholders can tailor their setup, fully decentralized or partially centralized, to comply with sector-specific needs, legal requirements, and resources. This makes the concept transferable to other CTI sharing contexts as well.

Despite encouraging results, this work has several limitations. The prototype was evaluated in a controlled, virtualized environment with few participants, which may not mirror large-scale, heterogeneous deployments. Integrating the IDS-based solution with legacy systems is not trivial and might require significant customization. Furthermore, adoption of the IDS framework and certifications is not guaranteed, given resource constraints or technological skepticism. While usage

[11]https://threatconnect.com

TABLE V
SUMMARY OF OUR ANALYSIS FOR COMPARISON OF SOLUTIONS

Category	Feature	Our Solution	MISP	ThreatConnect
Interoperability	Open Standards	Yes (IDS standard)	Yes (open formats)	No (proprietary aspects)
	Supporting Various Formats	High	High	Medium
Flexibility	Multi-Data Model Support	High (very extensible)	High (extensible via community)	Limited (vendor-defined)
	External Integration	High (connectors/APIs for integration)	High (APIs, many integrations)	Limited (controlled by vendor)
Trust	Component Certification	Third-Party (formal cert. of connector)	Local/Community (no formal cert)	Self (vendor internal)
	Participant Vetting	Third-Party (orgs certified to join)	Possible (manual vetting outside platform)	By Vendor (platform-managed)
	Multi-Level Trust	Yes (differentiated trust levels)	No (all-or-nothing trust)	No (uniform trust)
	Dynamic Trust	Yes (real-time trust revocation)	No (static trust groups)	Limited (manual/slow)
Commercial	Data/Service Marketplace	Yes (flexible data marketplace)	Limited (primarily free sharing)	No (no user-driven marketplace)
	Digital Rights Mgmt	Yes (enforceable usage licenses)	No	No
Data Sovereignty	Distribution Control	At Source (provider-controlled)	In Platform (once shared, platform controls)	In Platform (vendor controls)
	Usage Control Enforcement	Yes (policies enforced on use)	No (trust-based only)	No (trust/legal only)
	Auto Sanitization	Yes (supported via apps)	Yes (supports anonymization)	Yes (limited support)

control enhances data sovereignty, it can add overhead that may affect real-time sharing. Additionally, requiring each contributor to manually vet DAT tokens becomes cumbersome as membership grows; this could be addressed by shifting to a centralized membership framework (e.g., via an ISAC, CERT) or using automated checks based on organizational attributes. Another open question is the scalability of policy enforcement when confronted with highly complex, dynamic rules. Finally, human factors, such as organizational culture, legal considerations, and trust-building, were not explored extensively, yet remain vital for widespread practical adoption.

Nevertheless, applying a data space approach to CTI exchange in critical infrastructure offers a solid foundation for managing trust, interoperability, and data sovereignty. By leveraging standardized connectors, enforceable usage policies, and dynamic trust mechanisms, this model supports secure, policy-compliant information exchange among diverse stakeholders. Moreover, integrating a certified data marketplace with digital rights management fosters a sustainable, economically viable ecosystem, encouraging broader engagement and higher-quality threat intelligence sharing.

VII. CONCLUSION

Our study demonstrates that leveraging data spaces within the IDS framework overcomes longstanding barriers in CTI sharing for critical infrastructures. Our approach integrates automated trust mechanisms, dynamic usage control, and standardized data exchange protocols, ensuring each organization retains control over shared intelligence. Evaluation results indicate limited data exchange latency and performance overhead, while significantly enhancing trust and data sovereignty. Moreover, our framework addresses EU regulations (e.g., NIS2, GDPR), laying a solid foundation for more resilient, collaborative cyber defense strategies.

Future research should prioritize real-world deployments to refine it based on user feedback, enhance interoperability with legacy systems via standardized adapters, simplify certification for broader SME adoption, and evaluate performance. Additionally, optimizing usage control mechanisms, expanding policy frameworks, addressing human and organizational factors, and ensuring compliance with international regulations will improve scalability, usability, and global adoption.

ACKNOWLEDGMENT

We thank Dr. Roman Matzutt and Dr. Avikarsha Mandal for their feedback and scientific support.

AI systems (GPT-4.1 and GPT-4o-mini) have been used for editing and grammar enhancement.

This is the authors' version of the paper. For the official published version by IEEE, please refer to: https://doi.org/10.1109/CSR64739.2025.11130001. Additionally, please use the official version for citations: M. A. Gurabi, Ö. Sen, N. Rahimidanesh, A. Ulbig, and S. Decker, "Enhancing Cyber Threat Intelligence Sharing through Data Spaces in Critical Infrastructures," 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Crete, Greece, 2025, pp. 83-90, doi: 10.1109/CSR64739.2025.11130001.

REFERENCES

[1] A. R. Hevner, S. T. March , J. Park, and S. Ram, "Design Science in Information Systems Research." MIS Quarterly, 28(1), 2004, 75-105.

[2] B. Otto, S. Steinbuss, A. Teuscher, and S. Lohmann, and others, "IDS Reference Architecture Model(Version 3.0)." International Data Spaces Association, 2019.

[3] S. Autolitano, and A. Pawlowska. "Europe's quest for digital sovereignty: GAIA-X as a case study." IAI papers, volume 21, number 14, 2021.

[4] A. Pretschner, M. Hilty, and F. Schütz, C. Schaefer, and T. Walter "Usage control enforcement: Present and future." IEEE Security & Privacy, 2008.

[5] M. Akbari Gurabi, F. Hermsen, A. Mandal, and S. Decker, "Towards Privacy-Preserving Machine Learning in Sovereign Data Spaces: Opportunities and Challenges." Privacy and Identity Management. Sharing in a Digital World. IFIP Advances in Information and Communication Technology, vol 695. Springer, Cham. 2024.

[6] B. Steiner, and C. Münch. "Leveraging digital data spaces in purchasing and supply management: Paving the way to the circular economy exemplified by Catena-X." Journal of Purchasing and Supply Management, Volume 30, Issue 4, 2024.

[7] L. Coppolino, A. De Crecchio, R. Nardone, A. Petruolo, L. Romano, and F. Uccello. "Exploiting Data Spaces to Enable Privacy Preserving Data Exchange in the Energy Supply Chain." Proceedings of the ITASEC, 2024.

[8] A. Albakri, E. Boiten, and R. De Lemos. "Sharing cyber threat intelligence under the general data protection regulation." Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Proceedings 7, P. 28–41, 2019.

[9] T. D. Wagner, K. Mahbub, E. Palomar and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions." Computers & Security, Volume 87, p. 101589, 2019.

[10] M. Akbari Gurabi, L. Nitz, A. Bregar, J. Popanda, C. Siemers, R. Matzutt, and A. Mandal, "Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation." Digital Threats 5, 3, Article 34 (September 2024), 11 pages, 2024.

[11] M. Lee. "Cyber threat intelligence." Oxford, UK ; Hoboken, NJ, USA: Wiley, 2023. ISBN: 978-1-119-86176-8

[12] T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V.G. Bilali, and D. Kavallieros. "The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform." DATA, pp. 369-376. 2019.

[13] T. Geras, and T. Schreck. "Sharing Communities: The Good, the Bad, and the Ugly." ACM SIGSAC Conference on Computer and Communications Security, pp. 2755-2769. 2023.

[14] V. Jesus, B. Balraj, and C. Victor. "Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence." IEEE Transactions on Engineering Management 71. 2023.

[15] D. Schlette, M. Caselli, and G. Pernul. "A comparative study on cyber threat intelligence: The security incident response perspective." IEEE Communications Surveys & Tutorials 23, no. 4, 2021.

[16] L. Nitz, M. Akbari Gurabi, M. Cermak, M. Zadnik, D. Karpuk, A. Drichel, S. Schäfer, B. Holmes, and A. Mandal, "On Collaboration and Automation in the Context of Threat Detection and Response with Privacy-Preserving Features." Digital Threats. 2024.

[17] NIS 2 Directive EU. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." 2022.

[18] T. MacDonald, P. McKitrick, and M. Kaeo. "IEP 2.0 Framework Definition." FIRST — Forum of Incident Response and Security Teams. Nov. 6, 2019. [Online]. Available: https://www.first.org/iep/iep_framework_2_0 (visited on 03/03/2025).

[19] A. Zibak and A. Simpson. "Cyber Threat Information Sharing: Perceived Benefits and Barriers." Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES 19. pp. 1–9. Aug. 2019.

[20] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody. "Misp: The design and implementation of a collaborative threat intelligence sharing platform." Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, 2016.

[21] S. Barnum. "Standardizing cyber threat intelligence information with the structured threat information expression (stix)." Mitre Corporation 11: p. 1-22, 2012.

[22] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka. "Guide to cyber threat information sharing." NIST special publication 800, no. 150, 2016, DOI: 10.6028/NIST.SP.800-150

[23] M. Akbari Gurabi, A. Mandal, J. Popanda, R. Rapp, and S. Decker. "SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks." Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). ACM, New York, NY, USA, Article 109, 1–8, 2022.

[24] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, J. and Komárková. "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling." Computers & Security, vol. 115, p. 102609, 2022.

[25] M. Akbari Gurabi, L. Nitz, C. Mayuresh Joglekar, A. Mandal "Strengthening Cyber Defence through Cooperative Development and Shared Expertise in Incident Response Playbooks." ERCIM News 139, P. 44-46, Oct. 2024.

[26] P. B. Kruchten, "The 4+1 View Model of architecture." IEEE Software, vol. 12, no. 6, pp. 42-50, Nov. 1995.

[27] T. Wallis and R. Leszczyna. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector." Energies 15.6, Mar. 2022, p. 2170.

[28] Q. Wang, W. Tai, Y. Tang, H. Zhu, M. Zhang, and D. Zhou. "Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services." Energies 12.13, Jan. 2019. p. 2493.

[29] R. Deng, P. Zhuang, and H. Liang. "False Data Injection Attacks Against State Estimation in Power Distribution Systems." IEEE Transactions on Smart Grid 10.3, pp. 2871–2881, May 2019.

[30] R. Leszczyna. "Cybersecurity in the electricity sector: managing critical infrastructure." Cham: Springer, 2019. ISBN: 978-3-030-19538-0

[31] M. Keshavarzi and H. R. Ghaffary. "I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion." Computer Science Review 36, May 1. 2020, p. 100233.

[32] D. W. Chadwick, W. Fan, G. Costantino, R. De Lemos, F. Di Cerbo, I. Herwono, M. Manea, P. Mori, A. Sajjad, and X. Wang. "A cloud-edge based data security architecture for sharing and analysing cyber threat information." Future generation computer systems 102, P710-722, 2020.

[33] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez. "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing." computers & security, 127-141, 69 2017.

[34] D. Homan, I. Shiel, and C. Thorpe. "A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology." 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–6, June 2019.

[35] D. Skias, S. Tsekeridou, T. Zahariadis, A. Voulkidis, T. Velivassaki, and K. Fotiadou. "Pan-European Cybersecurity Incidents Information Sharing Platform to support NIS Directive." Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021.

[36] A. Eitel et al. "Usage Control in the International Data Spaces." International Data Spaces Association, March 2021, [Online]. Available: https://zenodo.org/record/5675884, DOI:10.5281/ZENODO.5675884

[37] T. MacDonald et al. "Information Exchange Policy 2.0 Framework Definition." FIRST — Forum of Incident Response and Security Teams. Nov. 6, 2019. [Online]. Available: https://www.first.org/iep/FIRST_IEP_Framework_v2.0.pdf

[38] A. El-Kosairy, N. Abdelbaki, and H. Aslan. "A survey on cyber threat intelligence sharing based on Blockchain." Advances in Computational Intelligence 3.3. May 23, 2023.