Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence

Vitor Jesus, Balraj Bains, and Victor Chang

***Abstract*—Cyber threat intelligence (CTI) is widely recognized as an important area in cybersecurity but it remains an area showing silos and reserved for large organizations. For an area whose strength is in open and responsive sharing, we see that the generation of feeds has a small scale, is secretive, and is nearly always from specialized businesses that have a commercial interest in not publicly sharing insights at a speed where it could be effective in raising preparedness or stopping an attack. This article has three purposes. First, we extensively review the state and challenges of open, crowd-sourced CTI, with a focus on the perceived barriers. Second, having identified that confidentiality (in multiple forms) is a key barrier, we perform a confidentiality threat analysis of existing sharing architectures and standards, including reviewing circa one million of real-world feeds between 2014 and 2022 from the popular open platform MISP toward quantifying the inherent risks. Our goal is to build the case that, either by redesigning sharing architectures or simply performing simple sanitization of shared information, the confidentiality argument is not as strong as one may have presumed. Third, after identifying key requirements for open crowd-based sharing of CTI, we propose a reference (meta-) architecture.**

***Managerial Relevance*—CTI is widely recognized as a key advantage toward cyber resilience in its multiple dimensions, from business continuity to reputation/regulatory protection. Furthermore, as we review in this article, there are strong indications that the next generation of approaches to cybersecurity will be centered on CTI. Whereas CTI is an established business area, we see little adoption, closed communities, or high costs that small businesses cannot afford. For an area that, intuitively, should be open, as velocity and accuracy of information is crucial, we shed light on why we have no significant open, crowd-sourced CTI. In other words, why is usage so lacking? We identify reasons and deconstruct unclear and unhelpful rationales by looking at a wide range of literature (research and professional) and an analysis of nearly ten years of open CTI data. Our findings from current data indicate two types of reasons. One, and dominant, is unhelpful perceptions (e.g., confidentiality), and another stems from market factors (e.g., "free-riding") that need collective movement as no single player may be able to break the cycle. After looking at motivations and barriers, we review existing technologies, elicit requirements, and propose a high-level open CTI sharing architecture that could be used as a reference for practitioners.**

Manuscript received 2 January 2023; revised 3 April 2023; accepted 13 May 2023. Review of this manuscript was arranged by Department Editor Marina Dabic. *(Corresponding author: Vitor Jesus.)*

Vitor Jesus is with Aston University, Computer Sceince Department, B4 7UP Birmingham, U.K (e-mail: v.jesus@aston.ac.uk).

Balraj Bains is with the Computer Science Department, Aston University, B4 7ET Birmingham, U.K. (e-mail: 190206866@aston.ac.uk).

Victor Chang is with the Aston Business School, B4 7UP Birmingham, U.K. (e-mail: v.chang1@aston.ac.uk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TEM.2023.3279274.

Digital Object Identifier 10.1109/TEM.2023.3279274

***Index Terms*—Confidentiality, cybersecurity, cybersecurity management, cyber threat intelligence (CTI).**

I. Introduction

CYBER threat intelligence (CTI) consists of any information that helps an organization to be better prepared for a specific cybersecurity risk. For example, suppose a certain malware strain has been identified in a previous attack. In that case, defenders can scan their devices for its specific signatures and indicators or configure an intrusion detection system (IDS) to scan network traffic.

After a period when cybersecurity was mainly prescriptive and open looped, risk-based cybersecurity is now the chief approach. Whereas CTI is not, strictly speaking, a new area, it can be argued [1] that risk-based approaches and associated enterprise architectures [2] should be augmented with CTI, thus, moving practitioners to what can be called intelligence-based cybersecurity. The key motivation is that the increasing sophistication, diversification, and agility (and often creativity) of threat actors must be met with equal performance. Overall, we are looking into obtaining an awareness advantage.

To a certain extent, prescriptive, rule-based cybersecurity, was predominant until the early 2000s. It can protect against *known knowns*, which is to say that, for example, passwords need to have a minimum level of entropy and be selected outside known dictionaries. Risk-centricity is the current paradigm championed by, among others, ISO/IEC 27001, which helps protect against *known unknowns*. Whereas many high-profile cyberattacks are seen as avoidable in hindsight (e.g., by not patching vulnerable software), many others could have been prevented by taking directed measures had the organization known that a well-identified adversary 1) selected them as a preferential target, and 2) used well-characterized tactics, techniques, and procedures (TTP). For example, in April 2022, CloudMensis was identified as a new MacOS backdoor and malware likely to be part of a coordinated campaign. Its characteristics were quickly identified and detection measures derived. As with others, this campaign will likely fade within a few months, so organizations should increase effort and attention dedicated to it, but only for its duration, reverting back to default measures once it subsides, so that risk reduces to an acceptable level.

This type of threat is, thus, part of the *unknown unknowns*, unless the organization has a CTI capacity that is able to share and consume external information. Therefore, with CTI, unknown-unknowns become known-knowns and specific, actionable, and effective measures can be applied, dramatically reducing risk.

Thus, CTI is able to drive a new approach to cybersecurity that can have unparalleled effectiveness.

Despite the benefits of operationalizing CTI, it is still not a common capability across organizations; at best, it exists in large organizations and often only in certain sectors such as banking. We also note that CTI needs both consumers and producers, ideally, with every participant in the network able to take on both roles. In fact, intuitively, one would imagine that CTI would be widely shared in order to take advantage of a network effect that quickly shares alerts and lessons. The metaphor here is that a tactic is only successful once because information quickly spreads. In this manner, and rather intuitively, the whole community would be stronger, similar to a vaccination effect. This motivates the idea of *open crowd-sourced CTI*. While this is a possibility, we observe little adoption and conflicting views.

A. Aims

We ask four questions in this article. The first two are the following.

1) *Why is the integration of CTI so low?*
2) *Why are there no multiple, large and open initiatives to source and consume CTI?*

As we review the literature, it is clear that the top consideration is not a technical or operational one; it is, in fact, *confidentiality* and related requirements such as regulatory compliance or market advantage. Even if an organization is able to generate CTI, and is willing to do so, they prefer not to take the risk of sharing confidential and tactical information. The first contribution of this article is to break down confidentiality requirements so as to argue they may not be as stringent.

Our subsequent third and fourth research questions are, therefore, the following.

3) *What are the safety requirements of a CTI sharing architecture?*
4) *Considering the barriers, both perceived and technical, can we design a CTI-sharing architecture that is open and safe?*

B. Methodology and Contributions

Our methodology is mixed, as illustrated by Fig. 1. *First*, we review the literature across three key areas: 1) socio-technical factors contributing to barriers to open sharing of CTI; 2) CTI sharing formats; 3) technical gaps. From the literature review, we will primarily argue that open, crowd-sourced CTI can be safe, provided the underlying sharing technical architecture has certain requirements. To support our position, we elaborate on two streams investigating its safety, both using data analysis and theoretical frameworks.

1) Sharing standards: We analyze over 500 distinct attributes in existing sharing standards.
2) Publicly shared events: We analyze over 1 000 000 events publicly shared since 2014.
3) Theoretical frameworks: We perform an analysis of confidentiality requirements for the specific CTI sharing scenario by: 1) adapting the LINDDUN framework [3] to the CTI case, originally aimed at Privacy threat modeling; and 2) by looking at Fisk [4] framework of first-principles for sharing CTI.

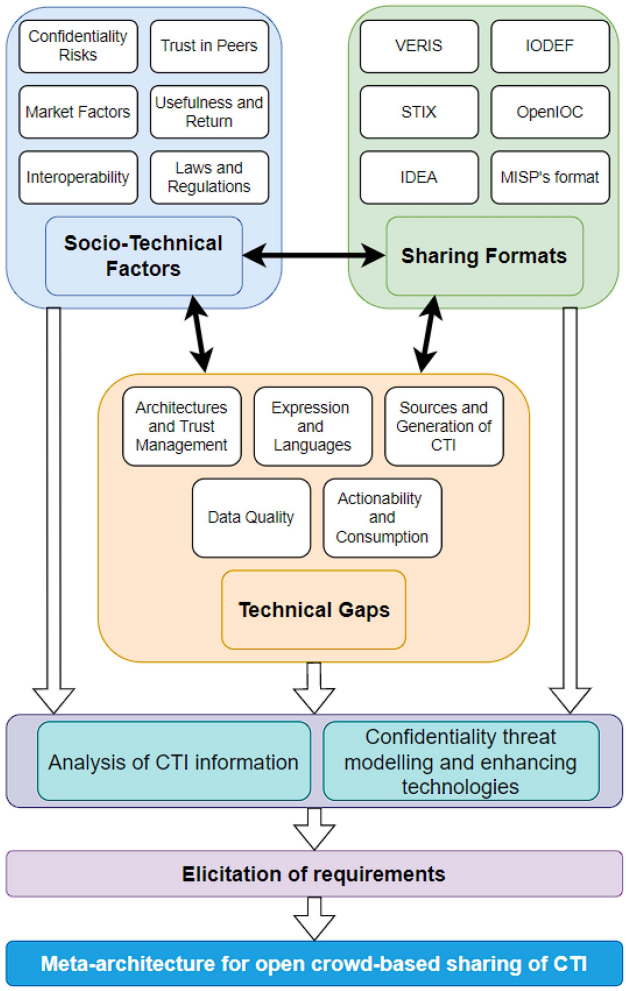

Fig. 1. Methodology.

We, thus, elicit requirements on two dimensions. First, we acquire a clear view of the inherent safety of sharing standards; second, we raise and collate new requirements toward open crowd-based sharing of CTI, including proposing a reference meta-architecture. By meta-architecture, we mean that we do not immediately propose an implementation or even a set of technologies, which will be for future work.

Contributions: The contributions of our article are multiple.

1) We offer a comprehensive, integrated, updated literature review snapshot of CTI sharing with a particular focus on the barriers and enablers toward open sharing, along with corresponding technical approaches; in particular, we break down the notion of confidentiality in multiple aspects to argue that the problem is more perceptional than practical and that open, crowd-sourced CTI seems feasible.
2) From a confidentiality perspective, we analyze in detail major sharing formats in order to quantify risk and safety, supported by an analysis of CTI data consisting of about 1 000 000 events since 2014, showing that a mere 0.1% of

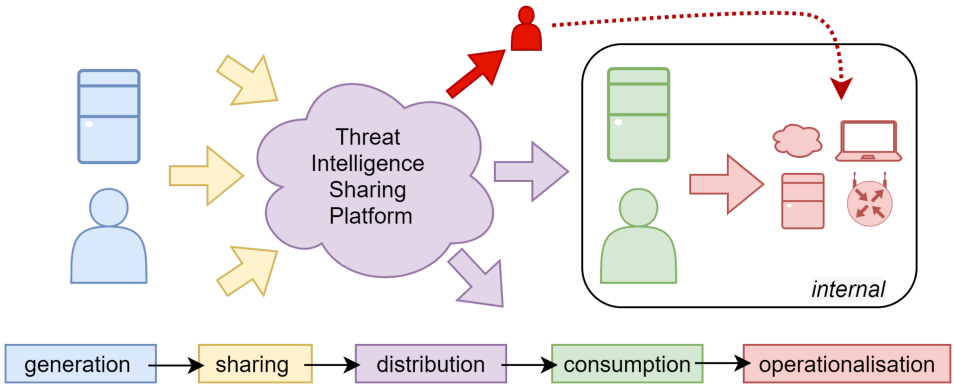

Fig. 2. Life cycle of CTI.

potentially confidential information exists and which can be further reduced by sanitizing data.

3) We develop a confidentiality threat analysis of the problem of open CTI.
4) We elicit, identify, and collate safety requirements toward open crowd-sourced sharing of CTI for which we propose an architecture.

To the best of our knowledge, these are novel contributions, including the literature review that focuses on deconstructing perceptions with confidentiality at the top. The collection of requirements we identify and the architecture we propose are, thus, informed by literature, theory, and practice.

C. Article Structure

The rest of this article is organized as follows. We start with an integrated review of the literature identifying barriers and incentives to open sharing of CTI, while reviewing CTI architectures (Section II). We then build the case that confidentiality may not be as significant a risk as thought. Since it is ultimately reflected in the languages and protocols used to transport CTI, Section II-B reviews well-known languages (Veris, IODEF, STIX, OpenIOC, MISP internal format, and IDEA) while attempting to quantify the associated risk. Section III analyzes the risks of sharing CTI from two angles. First, in Section III-A, we check what exactly sharing standards allow sharing and any associated safety features; then we look at a large dataset of CTI shared between 2014 and 2022 to measure risk. In the second part of this section, Section III-B develops a confidentiality analysis using privacy assessment models (e.g., LINDDUN framework [3] and Fisk's early model [4]). We complement the section with a review of privacy-enhancing technologies. Building on the literature review, the analysis of sharing formats, and the analysis of real-world events, Section IV-A proposes a set of requirements and a reference architecture that enables open sharing of CTI. Finally, Section V concludes this article.

II. Barriers and Approaches

In this section, we break down the life cycle of CTI and discuss key challenges by extensively reviewing literature. To help guide the following subsections, a high-level perspective of CTI is shown in Fig. 2. A producer of CTI creates a new feed (Section II-C3) based on their own research (e.g., by analyzing malware), derived from their own operations (e.g., honeypots), or simply reusing/enriching a past feed. We note that this last type often raises problems regarding the quality of data (Section II-C4). When deemed of interest and is vetted for sharing (e.g., because of accidental disclosure of confidential information (Section III), it is either published on a local repository (such as a website, common for white papers in natural language) or converted into a common format and published on a well-known platform. Sharing platforms will usually meet a number of socio-technical requirements (Section II-A), notably a form of membership that manages trust between members (Section II-C1). The new feed will then generate a new notification that consumers of the particular topic or source will receive. The new information is then acted upon (Section II-C5) in two ways: 1) it is internally analyzed by a human, who will integrate the intelligence into the internal operations; and/or 2) it is integrated with internal defense systems by automating the process, if possible. For example, suppose a new network signature is published in a format that is used by the popular Snort, an intrusion detection system. In that case, it can be automatically integrated with the local databases. If that signature is detected in traffic, an automatic action can be taken.

It is important to note that, given the public or semipublic nature of CTI platforms, a malicious party could be listening and analyzing the feeds with adversarial intentions. This is represented by the dark red figure and arrow. Amongst other risks, the party may aim at producing counter-intelligence or use it to perform reconnaissance and learn more about a target. These risks will be later analyzed in detail.*Methodology for the literature review*—In the following sections, we extensively review literature, both academic and industry or practice-based. We performed a simple search by `("Cyber" OR "Threat") AND "Intelligence"` from 2013 across key publishers such as IEEE, ACM, Springer, Elsevier, Emerald, etc. We also used popular online search engines to find grey and industry literature. From each paper, we reviewed their references and respective citations (when available) to find further literature, including those dated before 2013. In total, we reviewed about 400 papers, of which about 100 were selected as relevant.

Referring to Fig. 1-top, we start by analyzing literature on barriers to open CTI across the following dimensions:

1) confidentiality risks;
2) market factors;
3) interoperability;
4) trust in peers;
5) usefulness and return;
6) laws and regulations.

We then further review sharing formats, most standardized in some form, and then technical approaches mostly to address the socio-technical barriers as above.

A. Barriers

CTI is necessarily a technical area, but the process of sharing is driven by a mix of socio-technical factors. Some are internal to the organization, such as a lack of capacity to use CTI, but we mostly see external factors, such as market forces or legal risks.

1) Legal and Regulatory Constraints: There may be two broad reasons why CTI cannot be shared due to the legal, regulatory, or even political context [5]. On the one hand, sharing may create liability from product-based contracts to nondisclosure agreements. For example, it may disclose a vulnerability in a product that the vendor protects by limiting disclosure [6]. Furthermore, it may reveal or offer indications that the organization has been breached, which may lead to regulatory fines. Data protection considerations also apply even if this aspect needs more research [7] and, in general, falls under confidentiality consideration. On the other hand, national security policies may prevent sharing [8].

2) Interoperability: A frequent theme raised as a barrier to openly share CTI is the lack of interoperable formats [5], [6], [9], [10]. To be precise, the reason is not a lack of standard formats since several have existed, in some form, since the early 2010 s (see Section II-C2). First, different formats have proliferated recently, as we discuss later, which can cause confusion and unproductive redundancy. Second, some standard formats are, in fact, proprietary and not always useful to share certain types of CTI, particularly as we go up in the so-called pyramid of pain [11], [12]. The pyramid of pain captures the notion that whereas it is straightforward to share and act on the signature of a malware file, it is much more difficult to capture a multistep tactic of a sophisticated actor, such as escalation of privileges and lateral movement. Similarly, we note that CTI is still significantly shared over long textual reports or white papers, in natural language [13], that are difficult, or time-consuming, to convert into machine-readable formats and hence leverage automation. Third, we note that the existing sharing formats may need to be rethought, contemplating the fact that MISP [14], a popular platform to share CTI, has developed its own format, in parallel with the most popular format STIX [9], [15].

Another aspect related to interoperability is how different platforms, mostly closed-source and proprietary, do not easily integrate with each other [9], [16], [17], creating duplication of effort. This is often by design as there might be commercial interests to be protected (Section II-A4).

3) Usefulness and Return: The practical usefulness and cost/benefit return of CTI have been challenged [5], [9], [18] even if both academic and industry [1], [15] literature point at it progressively being a key differentiator for cyber resiliency. An example of success is the banking sector [1]. The issues raised seem mostly perceptional and compound the overall issues this section overviews, such as legal liability, lack of open platforms, etc. Other factors exist that are associated with lack of scale and difficulty in operationalizing CTI as "a product" [18]—examples are the cost to run a CTI team [19] and the lack of professional skills [8], [19]. A further challenge is operationalizing CTI to effective and practical measures [6], [8], [10], [20], often connected to the quality of the information shared or how to integrate a CTI function transversally in an organization, e.g., CTI as a (internal) service [21]. It is, nevertheless, recognized that CTI helps with reducing response times [22], usually in the order of months [23].

4) Market Factors: Market factors are currently acting as deterrents to open sharing in two ways. First, there are reputational issues. Sharing CTI will help with reputation by showing expertise and availability of resources for proactive cyber resilience. However, sharing CTI may inadvertently reveal internal weaknesses or a low maturity of their cyber operations. This ties to a second factor: managing competitors. Despite an open, collaborative approach to CTI being accepted to be of benefit to the whole community [24], it has been shown [19] that organizations generating CTI are conscious about what they share. They are willing to share simple indicators of compromise (IoC) (e.g., malware hashes), but less willing to share more complex defense strategies as they may give away a competitive advantage to competitors.

Furthermore, this is closely related to the perception that most participants will consume CTI and only a few will contribute, creating a free-riding effect or a "forward paying" attitude where participants share only if others do [19], [25]. There is clearly a network effect, similar to the well-known Metcalfe's law of networks, where the value of a network is quadratic with the number of participants. This can only be unlocked by changing collective perceptions.

The net result is that the current CTI market is essentially siloed with three types of structures;

1) professional and for-profit CTI firms [26], who are very protective of their PI and will only share with paying members;
2) sector-specific, invitation-only networks such as banking [1];
3) government-funded, national, semiclosed platforms, such as the U.K.'s CiSP [27] or the US's CISCP [28].

Considering the self-protective attitude and market structure, it is therefore very difficult to design a system of public or market incentives [16], [29], [30], [31] or public policies [32]. Numerous attempts, such as EU's GDPR or NIS mandate to disclose breaches (2016) or the recent (2022) US's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), address this fact to an extent. Whereas closed or semi-closed platforms do solve membership and trust challenges, it is in direct opposition

to open, responsive, collaborative, crowd-sourced CTI, our key focal point in this article.

The final angle is that of cyber insurance. It seems that cyber insurance premiums are not affected by a CTI capability [5], but this is likely due to it being a new trend. Intuitively, one can imagine that sharing information will have an effect of *reducing premiums* by showing robust (by consuming CTI) and mature (by sharing CTI) cyber-operations; on the other hand, it will *increase premiums* should confidential information about weak cyber posture become public.

5) Trust in Peers and Adversarial Usage: CTI needs to be shared in platforms where members should trust each other; however, it is unclear what trust entails. Literature seems to indicate that trust is not a true requirement; furthermore, it is either "mostly neglected" [9] or is a soft barrier that is quickly ignored as long as there is confidentiality [25]. The term trust may also mean that information can be trustworthy and actual, rather than low-quality copies or not actionable or useful [33] (see Section II-C4. Trust may also mean that there is good faith in terms of the ratio sharing/consuming [5], [10], which is simply the "free-riding" problem discussed.

Finally, trust also means that consumers of CTI will not use it against the member that shared the information [10], [18], [29]. This adversarial utilization of CTI needs more work, but we note that most attacks start with a reconnaissance phase, where adversaries gather information about the target in order to find weaknesses, and uncontrolled sharing of CTI may offer an advantage, significantly defeating the purpose of CTI. Such unintended consequence can be helped by, e.g., a better understanding of risks or standardizing processes [34]. Furthermore, another form of adversarial CTI is to generate fake CTI in order to sow confusion and doubt [35], likely diverting resources, and making CTI less useful or effective, particularly if used strategically.

6) Confidentiality Risks: Confidentiality risks are usually the top concern and reason for not sharing [5], [6], [7], [9], [17], [19], [25], [26], [29], [36], [37], even if at times under the umbrella of trust, regulatory compliance, or market factors, as discussed. As has been identified (e.g., [9], [25]), this is often an inconsequential perception effect that quickly becomes unimportant. Nevertheless, it should be recognized that uncontrolled disclosure of information or too much sharing can be problematic for reasons already pointed out (such as disclosure of internal information that a malicious party can take advantage of). Although there are proposals to tackle this problem and share CTI in a more safe way (as discussed in the next sections), including first-principles methodologies [4], the second part of this article will counter propose that it is either easy to control what is shared or, as a baseline, the risk of sharing critical information is low, given current practices.

B. Sharing Formats

This section reviews common sharing formats as they form an essential part of the overall sharing process: VERIS, IODEF, STIX, OpenIOC, IDEA, and MISP's internal format.

1) VERIS: The Vocabulary for Event Recording and Incident Sharing (VERIS) [38] gives means to record security incidents in a standard format. It is structured around what the authors call the 4As: Actor–Action–Asset–Attribute. VERIS is focused on recording and measuring internal incidents and less alerting for unrealized threats. It captures an "incident narrative": a ticket assignment with a local incident identifier, then recording the affected users, and then detailing the response taken. The data schema and taxonomy of attributes take an enterprise focus: incident details, affected assets and people, IoCs, etc. It uses the popular JSON format, which means it is extensible albeit somewhat unacknowledged, as most popular JSON libraries are designed to ignore unknown fields. VERIS is perhaps most associated with the yearly Verizon data breach investigations Report (DBIR) [39] as incidents analyzed are recorded in this format [40].

Listing 1 shows a sample of a breach in 2010 obtained from a public Veris dataset of incidents. It details how the database associated with a Web application was compromised on the 28 October 2010, likely using SQL injection as the attack vector. A search online[1] for the incident reveals that "A database web server, containing the electronically protected health information (EPHI) of 9493 individuals, was breached by an unknown, external person(s) for use as a game server. Although there was no indication of access to EPHI, the EPHI on the database web server included names, dates of birth, types of x-rays, and dates of x-rays." It also reveals that the breach was reported on 15 October 2010, likely due to regulatory obligations as this is classified as a "Healthcare Provider."

2) IODEF: The Incident Object Description Exchange Format (IODEF) was originally developed by the Internet Engineering Task Force (IETF, the main standardization body of the Internet) in 2007 and is currently in version 2 [41]. It was developed to automate communication between Computer Security and Incident Response Centers (CSIRTs) but also as a language that network elements, notably Intrusion Detection Systems (IDS), could understand via the intermediary format IDMEF [42]. In this sense, a newly discovered threat could be shared in IODEF format, converted into IDMEF and automatically ingested into an IDS that is then able to raise an alert or even stop an attack.

A JSON example of an IoC shared via IODEF is shown in Listing 2. The original format of IODEF is XML, which can be inefficient given its verbosity, and JSON is now being used [43]. It is a fictitious sample that shares a domain name (`kj290023j09r34.example.com`) being used as a Command & Control (C2), typically used as a central point to control botnets. The threat actor has been named as `Aggressive Butterfly` while pursuing a campaign named `Orange Giraffe`. This is an example of how CTI can be automatically mapped onto defense systems: an IDS could parse the feed's JSON, extract the malicious domain name, and, on detecting traffic to or from it, raise an alert and/or block by signaling a firewall. Of worthy mention to this article is that potentially confidential data was also included: `CSIRT for example.com` as the name of who shared this feed (an organization, in the case),

[1] https://www.rpubs.com/tg-xu/540846 (accessed on 9 August 2022).

```
{
  "action": {
    "hacking": {
      "variety": [ "Unknown" ],
      "vector": [ "Web application" ]
    }
  },
  "actor": {
    "external": {
      "country": [ "Unknown" ],
      "motive": [ "Unknown" ],
      "region": [ "000000" ],
      "variety": [ "Unknown" ]
    }
  },
  "asset": {
    "assets": [
      { "variety": "S - Web application" },
      { "variety": "S - Database" }
    ],
    "cloud": [ "Unknown" ]
  },
  "attribute": {
    "confidentiality": {
      "data": [ {
          "amount": 9493,
          "variety": "Medical"
        } ],
      "data_disclosure": "Yes",
      "data_total": 9493
    }
  },
  "discovery_method": { "unknown": true },
  "impact": { "overall_rating": "Unknown" },
  "incident_id": "084F33FE-B3DC-4389-9A97-2
  F40D7276820",
  "plus": {
    "analysis_status": "First pass",
    "created": "2013-04-12T22:29:56Z",
    "master_id": "084F33FE-B3DC-4389-9A97-2
  F40D7276820",
    "modified": "2014-04-27T19:37:02Z",
    "timeline": { "notification": {} }
  },
  "schema_version": "1.3.6",
  "security_incident": "Confirmed",
  "source_id": "vcdb",
  "summary": "",
  "timeline": {
    "discovery": {
      "unit": "Months",
      "value": 2
    },
    "incident": {
      "day": 28,
      "month": 10,
      "year": 2010
    }
  },
  "victim": {
    "country": [ "US" ],
    "employee_count": "1 to 10",
    "government": [ "NA" ],
    "industry": "621111",
    "region": [ "019021" ],
    "state": "WA",
    "victim_id": "SW Seattle Orthopaedic and
  Sports Medicine"
  }
}
```

Listing 1. VERIS record of an incident dated 28 October 2010.

```
{
 "version": "2.0",
 "lang": "en",
 "Incident": [{
   "purpose": "watch",
   "restriction": "green",
   "IncidentID": {
     "id": "897923",
     "name": "csirt.example.com"
   },
   "RelatedActivity": [{
     "ThreatActor": [{
       "ThreatActorID": ["
        TA-12-AGGRESSIVE-BUTTERFLY"
       ],
       "Description": ["
        Aggressive Butterfly"
       ]}],
     "Campaign": [{
       "CampaignID": ["C-2015-59405"],
       "Description": ["Orange Giraffe"]
     }]
   }],
   "GenerationTime":
    "2015-10-02T11:18:00-05:00",
   "Description": [
    "Summarizes the Indicators of
    Compromise for the Orange Giraffe
    campaign of the Aggressive Butterfly
    crime gang."
   ],
   "Assessment": [{
     "Impact": [{"BusinessImpact": {
        "type": "breach-proprietary"}
     }]
   }],
   "Contact": [{
     "type": "organization",
     "role": "creator",
     "ContactName": [
        "CSIRT for example.com"
     ],
     "Email": [{
       "EmailTo":
        "contact@csirt.example.com"
     }]
   }],
   "Indicator": [{
     "IndicatorID": {
       "id": "G90823490",
       "name": "csirt.example.com",
       "version": "1"
     },
     "Description": ["C2 domains"],
     "StartTime":
        "2014-12-02T11:18:00-05:00",
     "Observable": {
       "BulkObservable": {
         "type": "domain-name",
         "BulkObservableList":
            "kj290023j09r34.example.com"
       }
     }
   }]
 }]
}
```

Listing 2. IODEF example (in JSON) sharing a C2 domain name.

and the email address `contact@csirt.example.com`. In this particular case, these values do not seem sensible, but we see that mechanisms exist to share personal or confidential information. We also note that free text fields such as `Description` are difficult to control for confidentiality.

3) STIX: Structured Threat Information eXpression (STIX), currently in version 2.1 [44], is perhaps the most popular format given its flexibility to represent a wide range of cases while being a language than can embed other formats. It lends itself to be converted into other formats, even if with a potential loss of information. An example is converting STIX to IODEF, or

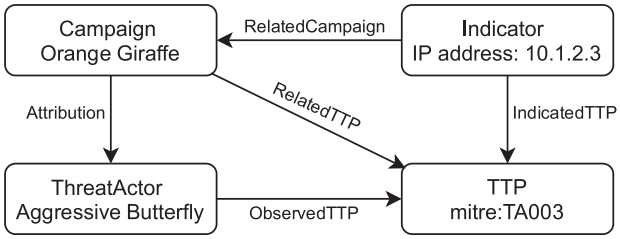

Fig. 3. Example of STIX relationships.

simply embedding it in an appropriate object and then injecting it into the rule base of an IDS. MITRE has the copyright of STIX, but it is sponsored by the US's Department of Homeland Security (DHS), which promotes openness and collaboration. By virtue of history (e.g., integration of CybOX [45]) and aim, it is more complex than any other formats, particularly when aiming at automation.

It further embeds the notion of relationships, thus supporting complex information ontologies. Fig. 3 shows a simple example where a threat actor `Aggressive Giraffe` is running a campaign and is using machines behind the IP address `10.1.2.3`. It is also known that this campaign uses a tactic denoted by Mitre as `TA003`, which was observed to be in use by the threat actor. The four represented objects—`Campaign`, `ThreatActor`, `Indicator`, `TTP`—can be individual objects and `Indicator` could be a single IODEF object. STIX 2.1 uses JSON as the preferred format. Listing 3 shows an example adapted from the official documentation. It shows a bundle of three objects, two indicators and a relationship. The indicators are malware being hosted at http://malwarexyz.tld/4712/ and the type of malware identified as `malwarexyz backdoor`, which is known to map to the phase `establish-foothold` of the attack model named `mandiant-attack-life cycle-model`. Attack models are colloquially known as "Cyber Kill Chains" after Lockheed Martin adapted the military concept of "Kill Chains" to cybersecurity [46]. A set of fingerprints of this malware can be found in further feeds that, likely, will link back to this particular feed. The third object is a relationship that expresses that `indicator-d81f86b9-975b` (the hosting domain) points to (`indicates`) the indicator `malware-162d917e-766f` (the malware).

4) OpenIOC: OpenIOC is a mature standard developed by Mandiant in the early 2010s [47] that substantially focuses on sharing actionable IOCs such as malware signatures or configuration entries such as the registry of MS Windows. As it was common at the time, XML was used. It is somewhat limited in scope and seemingly decreasing in popularity [15], perhaps because of lack of maintenance and the emergence of other more flexible standards such as STIX, where an IOC is one object out of many others.

5) IDEA: The Intrusion Detection Extensible Alert (IDEA) [48] is a further sharing format, but that falls under the remit of directly actionable intelligence for devices such as firewalls or IDSes, similarly to the combination of IODEF and IMDEF. In other words, it is a modern format in the sense of being aligned with current architectures of modern network

```
{   "type": "bundle",
    "id": "bundle--56be2a3b-1534",
    "objects": [
    {   "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--d81f86b9-975b",
        "created": "2014-06-29T13:49:37.079Z",
        "modified": "2014-06-29T13:49:37.079Z",
    "name":
        "Malicious site hosting downloader",
    "description": "This organized threat
        actor group operates to create
        profit from all types of crime.",
    "indicator_types": [
        "malicious-activity"
    ],
    "pattern":
        "[url:value =
            'http://malwarexyz.tld/4712/']",
    "pattern_type": "stix",
    "valid_from": "2014-06-29T13:49:37.079Z"
    },
    {   "type": "malware",
        "spec_version": "2.1",
        "id": "malware--162d917e-766f",
        "created": "2014-06-30T09:15:17.182Z",
        "modified": "2014-06-30T09:15:17.182Z",
        "name": "malwarexyz backdoor",
        "description": "This malware attempts
            to download remote files after
            establishing a foothold as a
            backdoor.",
        "malware_types": [
            "backdoor",
            "remote-access-trojan"
        ],
        "is_family": false,
        "kill_chain_phases": [
            {   "kill_chain_name":
                "mandiant-attack-lifecycle-model",
                "phase_name": "establish-foothold"
            }
        ]
    },
    {   "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--864af2ea-46f9",
        "created": "2020-02-29T18:03:58.029Z",
        "modified": "2020-02-29T18:03:58.029Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--d81f86b9-975b",
        "target_ref": "malware--162d917e-766f"
    }]
}
```

Listing 3. STIX example: sharing information about malware.

elements; it is kept simple and lean, yet flexible, recognizing that network devices need simplicity to increase operationality.

6) MISP's Internal Format: MISP is a popular open-source CTI platform that has its own format. Even though literature does not typically consider MISP as a standard format, we consider it as such given its adoption and attempts to standardize [49]. Furthermore, considering how popular MISP is, their internal format might incidentally be the most used by volume. Similar to STIX, MISP's format has a rich set of taxonomies. However, it does not aim at comprehensiveness but instead relies on unmanaged community contributions. In a sense, it seems to be more active than other standards (including STIX). This is perhaps because of their community-driven approach, which

indirectly gets sponsored by national authorities [e.g., NIS' (EU directive of 2017) incident reporting format or a taxonomy for illicit drugs, often used in spam emails]. A peculiar characteristic of MISP's format is the use of unexpected terminology (such as "galaxies" or "taxonomies" for the tagging system). It also gives an impression of unnecessary complexity while being at the apparent complexity level of STIX.

It is able to represent complex ontologies and meet different goals, from incident reporting to sharing simple IOCs, as long as the needed objects are available. The underlying model is based on three structures around the notion of *event* (which we interchangeably have been calling "feed"): sharing metadata, event attributes and objects, and augmenting context. Metadata consists of the list of objects being shared, such as unique identifiers, sharing settings (such as to which communities), or a date of sharing. The objects contain the specifics of the cyber intelligence, typically chosen from an existing object template and list of attributes. Finally, the context consists of sightings (next discussed) or simple tags to organize information and is mostly readable by humans.

An interesting notion in MISP is *distribution lists*. Whereas much-needed concepts in CTI, it is mostly motivated by the fact that MISP is, above all, a sharing platform. It also embeds the critical concept of *community*. For example, with great granularity, each object is associated with a level of re-distribution that roughly ranges between internal, selected group/community, or open. It is unclear, however, how to, at scale and if one decouples the platform from the format, enforce distributed lists and without using MISP's platform – raising interoperability issues and increasing the silo effect.

Another key notion concerns the re-distribution of a previously shared event. On the one hand, one has the `Sighting` object that allows someone to confirm that the threat has been seen, thus improving confidence. On the other hand, we have `ShadowAttributes`, which allows us to augment a past event's information. This, and other elements, help raise the quality of the information and, perhaps more importantly, reduce low-quality intelligence. We note, however, that these can also be used adversarially.

Listing 4 shows an example adapted from MISP's official documentation. It only represents a single object and not a whole event. It reports a malware file `StarCraft.exe`. It has a clearance of `3`, which means it can be freely shared.

```
    "Object": {
        "id": "588",
        "name": "file",
        "meta-category": "file",
        "description":
        "File object describing a file
        with meta-information",
    "template_uuid": "688c46fb-5edb-40a3",
    "template_version": "3",
    "event_id": "56",
    "uuid": "398b0094-0384-4c48-9bf0",
    "timestamp": "1505747965",
    "distribution": "3",
    "sharing_group_id": "0",
    "comment": "",
    "deleted": false,
    "ObjectReference": [],
    "Attribute": [
        {
            "id": "7822",
            "type": "filename",
            "category": "Payload delivery",
            "to_ids": true,
            "uuid": "59bfe3fb-bde0-4dfe-b5b1",
            "event_id": "56",
            "distribution": "0",
            "timestamp": "1505747963",
            "comment": "",
            "sharing_group_id": "0",
            "deleted": false,
            "disable_correlation": false,
            "object_id": "588",
            "object_relation": "filename",
            "value": "StarCraft.exe",
            "ShadowAttribute": [],
            "first_seen": null,
            "last_seen": null
        },
        "first_seen":
            "2019-06-02T22:14:28.711954+00:00",
        "last_seen": null
    ]
}
```

Listing 4. MISP format sample.

C. Technical Gaps and Approaches

Whereas the previous sections identified barriers and the wider considerations affecting the open sharing of CTI, this section reviews technical approaches toward safer sharing of CTI. In particular, we highlight conflicting requirements when thinking of open sharing. We break down approaches into: 1) architectures and trust management; 2) expression and languages; 3) sourcing and generation of CTI; 4) data quality; 5) actionability and consumption.

1) Architectures and Trust Management: A number of technical architectures have been proposed that either look at the end-to-end process or enforce trusted membership, noting that, as discussed, the notion of trust can vary depending on the angle. Since the ideal form of CTI sharing (as we focus here) is distributed and uncoordinated, very similar to how the Internet is organized even today, a model of reputation needs to be established. TAXII [50] is a well-known architecture that is often seen as a companion of STIX. It was developed in the early 2010s by the US's DHS and MITRE as a protocol and architecture to mediate trust bindings, the transmission of information (e.g., hub and spoke), or the discovery of servers. TAXII, particularly in combination with STIX (now incorporating CyBox), seems to be the *de facto* standard to build collaborative networks in CTI.

Beyond protocols, building distributed networks of trust is a key issue and a problem similar to what in the late 1990s became known as the Web of Trust [51] for the Internet. "Pretty Good Privacy," mostly for email, is based on that notion and is still the current most feasible model to distribute identities (in the form of cryptographic public keys). Essentially, reputation is a graph of relationships $G = (V, E)$, where edges E can have only a few values which are, typically, *trusted*, *nontrusted*, *marginal*. The

full graph of trust then takes advantage of trilateral $A - B - C$ relationships to derive trust for any arbitrary node $e \in E$. Steinberger et al. [33] propose MiRTrust that mirrors this approach by locally updating trust in sources (from the trust graph) as CTI information is confirmed or invalidated and broadcast to adjacent members. This approach is similar to what others call Traffic Light Protocol which is used, for example, in the U.K.'s CiSP platform, where a green light means encouragement to share anything as the trust level is high [25].

If one assumes a hub and spoke model (see, e.g., [52] where web-based APIs are suggested), information is pushed onto a central hub and spokes broadcast it. The hub, thus, could be untrusted as long as the receivers do trust each other. In a simple model, the information (always through the hub, so over an untrusted open channel) is protected by secret cryptographic keys whose knowledge defines membership [53] or cryptographic schemes such as direct anonymous attestation [54]; or taking advantage of homomorphic encryption allowing operations over encrypted data [55]. If information itself is not protected, then access control is necessary, such as attribute-based encryption (ABE) [56], which further offers auditability mechanisms, an essential requirement to allow organic improvement of the global trust graph and at small granularity.

Distributed ledger technologies (DLT), often simplified to "blockchains," are a recent technology that is still maturing but quickly recognized as a natural fit to help with open, collaborative problems, of which open CTI is a case. This is because of their underlying paradigm of trustlessness and decentralization over a public, untrusted network.[2] Whereas distributing information is not its vocation due to low bandwidth and long transaction times (e.g., Bitcoin has updates every 10 min and Ethereum about every 12 s), they can be used in asserting and/or validating authenticity and confirming membership [57], managing reputation [57], [58], [59], or leveraging the native connection of payments and blockchains to build incentive systems [57].

2) Expression and Languages: Even though it is claimed that most CTI, by volume, is shared in the form of reports in natural language [37], [60] (usually by specialized businesses), expressive, machine-readable formats to represent and share CTI, including reporting formats for regulatory purposes [61], have existed for more than two decades. We have reviewed major formats in Section II-B.

However, we note that sharing formats, especially those aiming at widespread adoption, must have an underlying data model that is either extensible (such as STIX) or risks being short-lived, as it will only support certain types of CTI. This is the (most popular) case of sharing CTI about low-complexity information such as (hashes of) malware files, IP addresses, or malicious domain names. Therefore, sharing builds on top of underlying taxonomies or ontologies. A starting point is capturing the who-what-when-where-why-how [62] from the perspective of threat characterization; an alternative is to model relevance-likelihood-impact which may lead to risk quantification [63]. Ideally, one should be able to represent higher-level considerations such as tactics, techniques, and procedures (TTPs), a difficult problem that is sometimes called the pyramid of the pain of CTI [11], [12], [64]. This is particularly important for advanced persistent threats (APT) [65], which are organized, usually well resourced and often state-funded groups that operate in a consistent fashion for months or years.

Beyond extraction of direct values such as file hashes, using ontologies and knowledge representation, so to express values and relationships (such as is_a, is_part_of, or is_target_of) is a central goal of sharing CTI, even if not straightforward [37]. As discussed, MISP's internal format (to some degree) and STIX already support a mature level of semantics ("relationships" [44]), but since they use their own format, it is not easy to leverage techniques already developed for generic ontologies. However, it has been shown that common formats can be translated into well-known ontological languages such as Web Ontology Language (OWL) or Resource Description Framework (RDF) [66], [67]. Representing CTI as ontologies is a promising direction [37], [60], [63], [68], [69], [70], [71], [72] as it can allow higher-level reasoning over the same raw data and across different feeds, a process that could further support more advanced machine learning and data analytics approaches.

3) Sources and Generation of CTI: An equally important problem is the generation of the data itself from the perspective of those producing it. We note that sources of CTI can have a wide range of meanings. On the one hand, there are straightforward sources, such as IP addresses deemed malicious; on the other hand, there are highly complex and abstract behaviors, such as multistep tactics observed in APTs. We note that CTI can range in, broadly speaking, operational, tactical, or strategic [19], [73], and it can either be directed—identifying threats to a specific organization [74]—, or undirected (the most common case).

A survey of literature identifies four broad categories: 1) open source intelligence (OSINT); 2) dedicated machines collecting activity that should not otherwise exist ("honeypots" or "telescopes"); 3) internal analysis of log files; 4) using dedicated threat intelligence sharing platforms (TISP), usually paid.

OSINT refers to analyzing and collating publicly available information, from social media profiles to dark web discussions. It is an expanding area in terms of research that naturally is also used to gather CTI. One application in cybersecurity is to use OSINT in a directed way, such as to find whether a particular organization has been named in a breach [74] while monitoring discussion groups (often in the darkweb). A further application is in detecting malicious insiders, such as an employee who turned rogue, a very challenging problem [75]. OSINT can have many types of sources [13], [76]: the darkweb [77], [78], print reports, discussion forums, chat groups (e.g., on Telegram), social media (Twitter, Facebook, etc.), personal or business blogs, file or code repositories, public logfiles. The challenging problem is that these sources are in natural language [74] and unstructured (one can imagine a mobile chat group), and require processing information to generate CTI that is concise, structured and better fit to an automated standard and later to be shared on a platform [79], [80], [81]. Another problem is correlation [82]:

[2]We are here only considering public blockchains since permitted blockchains are increasingly recognized to have unclear applicability.

to build actionable CTI about a specific threat, one is likely to need to correlate multiple sources and at multiple events.

A common strategy to generate CTI is to deploy honeypots [64], [83], [84], [85], [86]. A honeypot is a machine or resource of some type (web/files servers, firewall facing the public internet, a file monitored for access, etc.) whose sole function is not to provide the advertised or expected service but to collect attempts to use or access it. The immediate logic is that if there is any activity, it must be malicious. A particularly useful feature is that, since the machine is dedicated to CTI collection, it can be prepared to generate pre-formatted records that can be, past a vetting stage, immediately shared or used internally to strengthen security measures. The simplest example is a firewall that blocks a specific IP address upon activity in the honeypot. A further advantage of honeypots in CTI is that it gathers first-hand, accurate information that is thus very reliable [85], [86]. A variation of honeypots are dedicated services looking at (broadly speaking) Internet activity with the intention of drawing patterns, particularly in terms of consistent and undirected campaigns to identify as early as possible who is being targeted [87] [88].

Analyzing internal log files is another source of CTI [12], [20], [80], e.g., web servers. These are easy to process as they are structured and often use well-known formats (e.g., Windows or Linux) or can be annotated, often simply by adding headers to rows of events. Log files can generate very rich information when combined with data mining techniques, and multiple files exist from multiple vantage points. This technique to raise CTI is also applicable to specific environments such as IoT [89] or industrial control systems [90], which are more deterministic and certain techniques such as Markov chains can be used [91].

The final category consists of TISP themselves. These are often commercial services [16], [26] and CTI frequently comes in the form of lengthy investigation reports, therefore, not easily integrated with automated CTI, despite natural language processing becoming increasingly reliable, including extraction of CTI [92]. A note should be made that (open) platforms about vulnerability disclosures (e.g., Mitre's CVE [93] or NIST's NVD [94]) are also a source of CTI and very reliable; however, they are necessarily delayed as the process to discover, verify, and submit a new vulnerability can take time. One can also use known TISP to create new CTI as often an actor of threat changes over time and different events can be correlated. However, it is a known effect that a substantial volume of public CTI is either repeating or low-quality derivatives, a problem we discuss in Section II-C4.

One should make a mention of a growing phenomenon as anecdotally perceived by the authors of this article. There seems to be a growing community of independent threat hunters, often young professionals trying to make a name for themselves. This might be similar to independent grey hats looking to win bug bounties. To the best of our knowledge, there are no platforms to support this work formally.

4) Data Quality: By low-quality data, one that has low levels of correctness, relevance, utility and actionability, or uniqueness and originality [10], [13]. Several factors contribute to this. First, even though, to the best of our knowledge, there is no systematic and large-scale study on the quality of CTI, it has been reported that public CTI has at least 50% duplicates [60] which contribute to processing time without adding value and is associated with the previously discussed effect of "free riding." We also see that data may be unreliable, motivating the design of quality indexes [73], [90], [95], [96], although with limited success as criteria and calculation methods (e.g., using weighting matrices [73]) quickly become subjective or case-dependent, or are based on qualitative information such as OSINT that essentially needs the judgment of a human.

From a high-level perspective, we note that this problem is not too different from what social media faces, except that, given the tendency to use structured formats, CTI is an easier problem. Detection of duplicates, for example, seems not to be a hard problem from simple comparison field-by-field, or by detecting keywords or named entities [74], to using simple techniques in machine learning [95] or taking advantage of data-driven or Big Data methods to assert relevance from high volumes of data [87], [97], [98]. Another alternative, complementary, is to design architectures with native ranking mechanisms [57], [95], [99]. We note that the problem quickly becomes one of reputation [57], [58], [59], [96], [100] (and, overall, of trust) and it seems inevitable that it is tied to identity or membership of a trusted group.

A final dimension affecting the quality of CTI is the fact that counter-intelligence, or adversarial CTI, is in itself a threat vector. Literature is scarce and "fake CTI" is likely not to be prominent currently. The use of AI is bringing great benefits to the wider area of cybersecurity but it brings in itself new risk directions [101]. However, if CTI is to be open and with large volumes, one will expect to see activity that: 1) will try to mislead or reduce the effectiveness of high-quality CTI [100]; and/or 2) make it more difficult to process, e.g., by generating large volumes of false information [102].

5) Actionability and Consumption: CTI is ultimately concerned about how useful data is from a cost/benefit perspective, which means addressing the gap between awareness and action. In other words, if a threat is shared as CTI, it should be actionable, so it is quickly reflected on the security level of the environment. One simple example is a malware file hash that endpoint protection software (e.g., a laptop) should integrate so that further scans take it into account. Operationalizing CTI is not a trivial problem beyond simple IoCs [9], [15]. On one hand, it is notoriously difficult to formally model attacks, unless sufficiently simple [103], [104], [105], [106], [107], that are accurate for forecasting, despite a number of promising techniques existing [108]. On the other hand, higher level, more abstract constructs, such as tactics of an APT, will necessarily imply higher human intervention [9] also due to the perception that CTI becomes increasingly more vague [19]. Literature shows this specific area needs more research, but some discussion exists on how to integrate with business operations [109], [110], [111], understand the level of risk or characterize actors [65], [112]. A further challenge is how to integrate CTI into security playbooks [113] [110]. A playbook is an evolution of incident response, particularly important in cloud computing, given the level of infrastructure automation. We now see its

importance increase as cybersecurity detection and monitoring increasingly adopts a security orchestration, automation, and response (SOAR) paradigm [114] in the hopes of automating detection to response without significant human involvement.

D. Discussion

Whereas it is unclear how many organizations are needed to attain "critical mass" for responsive and comprehensive CTI, it is intuitive that not many are needed, considering that cybersecurity is a global and cross-industry problem and virtually all are facing the same threats if one ignores specific and localized contexts. Ignoring confidentiality considerations (often and misleadingly, taken as an inter-party trust problem), which can indeed raise liability and reputation as well as increase breach risks, there seems to be no strong argument that can justify the poor state of open and collaborative CTI. We note that risk, in itself, is difficult to apprehend, particularly in an operational/organizational scenario, as it has multiple dimensions and its links to the ultimate objective of cybersecurity can be elusive [34]. Technically speaking, we have standard formats and architectures, even if recognizing their limitations, open-source products, and a market of specialized businesses or large organizations who are interested in quickly sharing intelligence (such as cloud or mobile vendors). We note that technical approaches often somewhat miss the key barriers and the insights from focus groups, but it should be recognized that the technology building blocks exist and are mature.

This state of the art can be justified, as a whole, with two factors. The first factor concerns market forces that respond to two problems. First, we see a "chicken and egg" problem, alternatively worded as "I share in the hopes others share" [8]. The second direction is about the business model of CTI that makes it protective and subscription-based. This overall deadlock can only be broken by public policy and collective self-initiative (and we hope this article so contributes).

The second factor is technical trust, which, looking at literature, effectively means *confidentiality*. The second part of this article will look at this component and attempt to create the case that confidentiality can be trivially achieved if looking at CTI shared over more than a decade. It can be achieved by two complementary mechanisms. The first, which is a soft argument and a passive approach, is simply running a risk assessment and realizing that whatever information is shared is likely not to raise the risk significantly because there is not enough internal detail. The second argument is that it seems to be straightforward to anonymize shared information, both directly revealing data and indirectly, as used in inference attacks. Finally, access controls are not essentially necessary as long as CTI is shared anonymously. This raises problems (e.g., quality of information or misinformation), but that can be handled with separate mechanisms.

III. Confidentiality Analysis

After extensively reviewing the literature, we now take a closer look at what is the highest (perceived) risk of sharing CTI: loss of confidentiality. We start by analyzing direct disclosure risks by looking at sharing formats. Then we apply privacy threat models, noting that, since CTI is mostly an organization-to-organization activity and not about personal individual information, it is more appropriate to call it *confidentiality modeling*. Consequentially, some privacy modeling techniques will only directly apply with modifications. Furthermore, except for a case-by-case analysis, there is no generic framework to transversally and formally model confidentiality (or privacy); however, there are methodologies one can use and combine, particularly when looking at three dimensions: the data shared on an event basis, the process by which data is created and shared, and the confidentiality risks of sharing large volumes of information which, even if individually anonymized, could still enable inference.

Considering that, ultimately, any confidentiality risks can be identified by analyzing sharing languages and frameworks, and we start by looking at risks of direct or accidental disclosure, that is, fields in CTI sharing formats that, if not sanitized, will have confidential information. A simple example is email addresses. We then look at the sharing process and analyze confidentiality with the LINDDUN framework (for privacy modeling) combined with the CTI confidentiality analysis of Fisk et al. [4]. A third technique, looking at inference attacks, is applying dataset anonymization techniques (e.g., k-anonymity or differential privacy). Finally, we take a brief look at several privacy-enhancing techniques (PET) combined with side-channel inference attacks for completeness.

A. Disclosure Risks

By direct disclosure, one means sharing confidential information when sharing a CTI event. A simple example is to share an internal email address. Disclosure could also happen by accident if the sanitization process is not robust or methodical. We analyze six CTI formats and look for fields that could hold confidential information. The six formats are VERIS, IODEF, STIX 2.1, OpenIOC, MISP's internal format, and IDEA. These were reviewed in Section II-B. In the second part, we look at actual events shared and collected from public CTI and draw conclusions about the actual confidential information shared from a direct disclosure perspective and as per current practices.

1) Methodology: We built a template from the specification for each format and linearly exported all possible fields to create a flat (nonhierarchical) list of attributes. By linearly, we mean that we removed the hierarchical structure of most CTI feed schemas (notably, STIX) and simply listed all the attributes without a structure. We note that because we are looking at schemas and the actual feeds being shared are combinations of an arbitrary number of these fields, this is not the proportion of disclosure risks. However, it gives an indirect indication of the risk in itself and the difficulty of sanitization. Manually, each field was tagged as "yes" or "no" depending on the answer to "is there a confidentiality risk?" and in isolation. We took a conservative approach so that, in case of doubt, we would mark the field as "yes." In case the answer was "yes," we would mark it as follows.

TABLE I
NUMBER OF FIELDS ANALYZED PER FORMAT

Format	Total Fields
Veris	77
IODEF	82
STIX 2.1	155
OpenIOC	40
MISP	184
IDEA	83
total	**621**

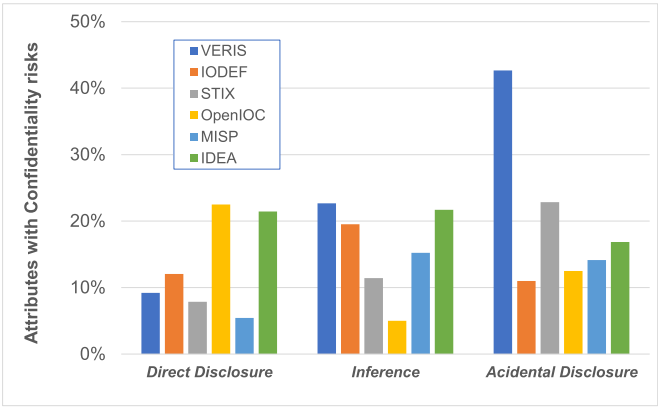

Fig. 4. Proportion of attributes with risks to confidentiality.

1) *Direct disclosure*, if the attribute may directly lead to the disclosure of information that may be trivially mitigated and automated with a sanitization procedure (e.g., detection of email addresses and redaction).
2) *Indirect or inference risk*, which is an attribute that does not directly disclose information but it may: 1) given enough events from the same source; 2) events sufficiently rich; 3) vulnerable to reidentification attacks; and/or 4) organizations vulnerable to being tricked into reporting an incident with custom data and thus be detected, similar to dust attacks [115] for some cryptocurrencies; or
3) *Accidental disclosure*, in fields where the format is not strongly constrained or specified (e.g., no data type such as a comment in free text) and accidental disclosure is more difficult to detect. If "direct disclosure" was "yes," then we would set "accidental disclosure" to yes as well.

The attributes were tagged by three different people with expertise in cybersecurity: one in social sciences, two others in computer science. When there was disagreement, a consensus was sought over a number of meetings. Overall, we analyzed the number of fields as in Table I.

2) Attributes in Sharing Formats: Fig. 4 shows our findings. Overall, and ignoring VERIS, the risk has an upper bound of about 20%, with direct disclosure commonly under 10%, particularly for the two most popular formats, STIX and MISP.

We can see that the proportion of attributes that carry a confidentiality risk aligns, on the one hand, with the nature of the format. Strikingly, VERIS shows a high risk of accidental disclosure, but one should note that it is a format with a strong focus on documenting incidents with as much detail as possible. It has a number of "notes" fields that are free text and difficult to control. Furthermore, most objects will have a "vector" field that likely needs a human, free-text explanation about how the internal systems were first breached. IODEF is highly structured, showing less risk with accidental disclosure, suggesting it is easier to automate field sanitization. The extended attributes it allows, however, may allow for inference, but given the constrained data types, we opted to mark them as safe from inference. Free form attributes, even though most have a specific purpose (e.g., email address), may allow for accidental disclosure. We also assume that language attributes will not disclose information as there will be a common language among members (e.g., if an international community, it will likely be English). STIX allows for far more uncontrolled input, which raises the risk of accidental disclosure or inference. As expected, STIX is also much richer in information. An example is `primary_motivation (optional)`, which captures the motivation of the threat actor, which in itself, should not disclose confidential information but that, since it is an open, free-form field, may allow accidental disclosure. OpenIOC consists of mostly string data types that raise accidental disclosure risks; however, fields are well-defined, facilitating sanitization automation. Even though it shows high direct disclosure risk, we note that we were highly conservative, so the value we have may not reflect an actual utilization of the format. For example, "Registry Path" and "Registry Text" (about malware) likely will not disclose confidential information but were still tagged as "yes." MISP has free-text fields, including general-purpose "comment" fields raising accidental disclosure. It uses UUIDs, which are a safe way of creating uniqueness of identifiers while not being inferable. All timestamps, however, are assumed to be inferable such as `first_seen` and `last_seen`. An example of something that, ultimately, is inferable is `template_version`, but we note that this only applies if using old versions.

3) Analysis of Shared Events: We now turn to look at actual shared events. We used the open CTI platform MISP to collect events from known feed sources. Feeds were, in their original names, "CIRCL OSINT feed," "The Botvrjj.eu Data," "Alienvault reputation generic," "malshare.com," "DigitalSide Threat -Intel OSINT," "Threatfox," "URLHaus." In total, we analyzed 1 048 570 feeds between October 2014 and June 2022.

Methodology—For each feed, we took the same approach as when analyzing schemas. We started by flattening the feed we received to create a simple list of data. Each element was tagged by the three people with expertise in cybersecurity: one in social sciences, two others in computer science. When there was disagreement, a consensus was sought over a number of meetings. A difference was that we simply classified each element as having confidential information or not. Due to a large number of events, we took a coarse but conservative approach: when in doubt, the feed would be classified as containing confidential data. In this way, we obtained a higher bound for the frequency of disclosure of confidential data. We also tried to automate as much as possible by looking for personal information such as common English forenames ("Paul"), email addresses (strings containing "@"), or countries ("Canada"). On sampling and manual inspection, we note that, for example, most email addresses were, in fact, part of the core CTI information, such as source email addresses

TABLE II
INFORMATION DISCLOSURE IN MISP EVENTS

Class	Total Feeds	Proportion
Potential Confidentiality Breaches	912	0.087%
Safe Sharing	1,047,663	99.913%
Totals	1,048,575	100%
External Indicators only	953,199	90.90%

TABLE III
EXAMPLES OF INDICATORS

Summary of Indicator
Financial fraud, btc, 1GxXGMoz7HAVwRDZd7..., Bad Rabbit
Attribution, campaign-id, dr.decrypter @bk.ru, ransom note
Network activity, ip-dst/port, 195.123. 220.133:443, CS botnet
Payload delivery, sha256, 6322bba692a8b907f0b1f..., Emotet payload
Network activity, url, https ://techsaphelper. com:8443/cs.html, CS botnet

Space characters were added to prevent accidental clicking.

in phishing campaigns and owners of (legitimate but abused) domain names.

Results—Table II shows the results we obtained. It suggests the risk of unintended disclosure of confidential information is very low. Furthermore, we note that even if so, the information shared takes a public vantage point in the sense that only simple indicators are shared, such as malicious IP addresses or malware hash files. Examples are shown in Table III. These amount to (at least, given our conservative sampling strategy) 90.90% of all information shared. This is equivalent to receiving a malware file, extracting its signature, and sharing it: beyond the fact that malware was seen, it reveals very little about the internal systems or procedures.

Whereas these results strongly suggest that disclosure of confidential data is very low risk, we note the following.

1) We only looked at feed sources that are open and free, noting that MISP supports closed communities that were not easily accessible. There is also the case of paid feeds, but these ones are likely not to have confidential information as they are highly curated and commonly produced by intelligence businesses.
2) There may be a methodological fallacy: since sharing is not common, people will only share what is perceived as safe (such as malware hashes). If sharing became widespread, we might see an increase in disclosure. In practice, it is a difficult hypothesis to test.

B. Confidentiality Model

This section will analyze CTI sharing from an end-to-end process perspective, that is, beyond the risks of the actual data being shared. To a point, the process of creating and sharing carries greater risks. This requires a privacy/confidentiality threat modeling framework that should be systematic and thorough. Whereas security threat models exist, privacy ones are less common. We chose a combination of the two.

The first is LINDDUN [3]. It is oriented to privacy risks, in the sense of personal information, and hence an adequate tool for data protection assessments; we have, thus, to adapt and think of confidentiality risks rather than breaches of personal data. LINDDUN is an acronym that stands for its seven identified privacy properties (or goals): linkability, identifiability, nonrepudiation, detectability, disclosure of information, content unawareness, and policy and consent noncompliance. LINDDUN commonly uses four dimensions of analysis: 1) entity; 2) data flow; 3) data storage; 4) process. For CTI, only *entity* and *process* are relevant, as the rest is related to how personal data (the original context of LINDDUN) is handled and stored. The following subsection briefly reviews each property, then aligns its rationale considering confidentiality goals, and then discusses its applicability to our specific scenario of CTI.

The second confidentiality framework derives from Fisk et al. [4], who take a first-principles approach specifically to sharing of CTI. The first one, the principle of least disclosure, is rather straightforward and encompasses managing data collection points (should be minimized as a starting goal) and internal disclosure (e.g., access controls). The second is the principle of qualitative evaluation, which addresses the balance between risk and benefit, including regulatory obligations and the natural limitations of any technical control. The third is the principle of forward progress which captures the notion that sharing, albeit carrying risks, might be a necessity that, rather than stopped, should be managed. To a large extent, this aligns with the pervasive notion of accepting the "free-riding" (or "forward playing") problem as discussed in Section II-A4.

1) Linkability and Identifiability: We combine the first two properties since, from a CTI confidentiality perspective, they often merge together. Linkability refers to the notion that two sets of data can be correlated to unveil meaningful relationships. Identifiability refers to the degree to which an individual feed allows identification of the source. Whereas, linkability necessarily requires multiple data points so information can be combined, identifiability may need only one.

They are important requirements if full confidentiality of the source is desired. Sanitization of attributes becomes important to prevent disclosure. A common case is to combine two data sets that, individually, cannot identify a person but that, together, can if there is a pseudoidentifying attribute that is common between the two data sets. In terms of confidentiality, and specifically for CTI, this is a central property, especially noting that public CTI will likely be augmented with OSINT. CTI sources are expected to share numerous feeds that, together, will reveal patterns of operation, technologies used, or people and systems. They may also contain, quite straightforwardly, unique attributes that repeat across different feeds. Beyond sanitization and randomization of attributes, this is a difficult threat to mitigate and addressed by Fisk's least disclosure. However, we note that the threat only becomes substantial with fast sourcing of CTI, giving enough volume for malicious actors to be able to correlate data and gain knowledge useful in an attack.

2) Nonrepudiation: Nonrepudiation is typically associated with security threats to make parties and systems accountable and unable to deny a specific action that took place. When thinking of confidentiality, it takes an interesting role as we want the opposite. As mentioned, a key barrier preventing the open sharing of CTI is the legal and regulatory liabilities it

potentially brings. In other words, sharing CTI needs to be wrapped in *plausible deniability* so that shared CTI cannot be used as evidence. To note that plausible deniability may be achieved using several means, including technical ones as used in the off-the-record messaging protocol [116] by deliberately not utilizing digital signatures.

3) Detectability: This property concerns how distinct confidential information is from the channels it uses or whether confidential information can be obtained using, e.g., side channels. We note that, whereas there is a degree of interest, this does not apply to the scenario of public, open, crowd-sourced sharing of CTI, in general. The main reason is that the information should be public and widely accessible, so any confidential information not immediately visible will eventually be found. By design, all feeds should be open and readable by anyone, including malicious parties.

Therefore, we propose we redefine this property, for our case of interest, as the effort needed to: 1) identify nonimmediate confidential information; and 2) the mechanisms by which the sourcing party can be privately notified. Similar to (responsible) vulnerability disclosure, the vulnerable party should be able to receive private communications, particularly if they shared confidential information that only later was deemed so.

4) Disclosure of Information: Disclosure of information directly ties to security breaches which are outside the scope of our problem where parties consciously and voluntarily share information.

5) Content Unawareness: Content unawareness is defined as the data subject releasing too much information in the personal data domain, which creates more breach opportunities for the data controller just by managing more data. In fact, this is aligned with the EU's GDPR, the data minimization requirement of collecting solely on what is strictly needed. Interestingly, in our CTI confidentiality model, the roles are reversed: rather than a data controller putting effort in limiting what they receive from the user, the CTI sharer needs to put deliberate effort into safe sharing. This ties in with previous requirements, such as sanitization. To this end, we would rename this requirement as *content awareness*.

Interestingly, this is a central requirement, whereas in the original LINDDUN framework, it is classified as a somewhat minor requirement that falls under soft privacy, as opposed to hard privacy, which implies that data controllership is transferred. This is correct in the case of Personal Data (users necessarily lose control of data), but in our scenario, assurance roles are reversed. In this sense, Content Awareness becomes perhaps the central assurance requirement. This agrees with Fisk et al. and their principle of least disclosure and, to an extent, the other two principles of qualitative evaluation and forward progress.

6) Policy/Consent Noncompliance: Policy/consent noncompliance should be understood in the context of, e.g., EU GDPR, where Consent needs to meet specific requirements. Therefore, it only very weakly applies to our scenario. We note, however, that there is a sensible reinterpretation of this property. Sharing organizations will need to align and comply with laws, regulations, and customer requirements. In contrast, there are still policies in place that should be fulfilled to make them more adaptable and compliant. Therefore, we propose to rename this to simply *noncompliance*.

C. Privacy-Enhancing Technologies (PET)

PETs are a family of technologies that assist in data minimization or controlling access to data sets. It can also encompass what is sometimes called transparency-enhancing technologies (TET) [117], which support transparency, explainability, and auditing of (typically) processing flows of personal data. We briefly discuss the applicability of PETs to open CTI sharing.

1) Dataset Anonymization: We here include techniques that primarily aid in anonymizing datasets that are to be shared. Somewhat simplifying, the key goal is to share a dataset with private data $x \in D_{in}$ so that, by applying a transformation, it does not disclose the private individual data to a customizable degree of confidence. In contrast, the output dataset $y \in D_{out}$ is still useful for the intended use. Four well-known techniques exist in the literature.

1) k-anonymity, in which at least k equal records y exist in D_{out} so individual records are indistinguishable; a simple way to apply this is to simply remove private information and counting $k = min\{count(y), \forall y\}$ which becomes a measure of privacy.
2) l-diversity, in which k-anonymity is enhanced by not allowing external information to be combined that potentially re-identifies individual records.
3) t-closeness, in which l-diversity is enhanced by taking into consideration the expected statistical properties of the original dataset (potentially revealing information) by, e.g., decreasing granularity as mitigation.

The fourth technique is differential privacy, popularized by Apple. If ignoring the complexity of the strategy, it can be understood as a generalization of the previous anonymization strategies while offering a measure of loss of privacy. Formally yet simplifying, ϵ-privacy is defined as follows. A transformation algorithm $\mathcal{A}$ operating over D_{in} will create D_{out} such that, for any query for value x, one obtains $y = \epsilon x$. In other words, the output dataset adds noise. A small value of ϵ indicates that the whole dataset will have similar values, which increases indistinguishability, thus increasing privacy. However, this will also decrease the utility of the dataset.

Applying such strategies to sharing CTI is not trivial nor of clear benefit for (at least) two reasons. First, intelligence indicators are typically discrete values, often nonnumeric, and a transformation algorithm $\mathcal{M}$ cannot easily apply noise without likely destroying its utility. For example, it is not possible to add noise to a source IP address or hash of malware while keeping the utility of the information. Second, the notion of privacy is aggregate: it is best measured by looking at a dataset rather than at an individual value.

Nevertheless, individual feeds can be anonymized in those attributes that risk disclosing information about the sharing party. To this end, the simple k-anonymity (perhaps l-diversity) seems to be the most useful when combined with data masking (as below).

2) Data Masking: Data masking is a trivial case of obfuscating or sanitizing private data. Several techniques exist and they provide simple replacement with blank data, substitution with meaningless characters (often used with credit card numbers), or encryption (which raises key management challenges). Whereas the techniques are usually straightforward, the process of detecting and acting on these fields is perhaps the most challenging part. However, as mentioned before, we note that using well-known sharing formats, such as STIX, greatly helps automated sanitization or quantifies risk appetite.

3) Secure Computation: By secure computation, one means multiple forms:

1) secure multiparty computation, where parties achieve a common result operating over partial and/or obfuscated data;
2) homomorphic encryption, where direct operations are possible over encrypted data, thus, preserving confidentiality or privacy;
3) zero-knowledge proofs, when a party needs to prove or verify knowledge of data without revealing the data; and
4) trusted execution environments, offering secure execution of software (usually by using special hardware functionality) with tampering detection and attestation of software.

Despite literature approaching the usefulness of these techniques in CTI (see, e.g., [56]), it would likely not promote open, crowd-sourced sharing of CTI since the ultimate goal is the public sharing of information. However, as we discuss in the next section on Identity, it does have a role in asserting (ultimately) the reputation or membership of a sharer, necessarily linked to some form of identity.

4) Identity: Regardless of the sharing model, Identity of participants is inevitable for at least three key reasons, which, in turn, raise three different requirements. First, a *reputation and incentives system* needs to be in place in order to control the quality of submissions, which, as discussed, can be misleading or malicious on their own. Furthermore, a consuming party may want to ignore certain sources while privileging attention to others. A reputation system will thus require persistent identities, yet ideally anonymous, associated with cryptographic material (e.g., a simple self-signed public-key certificate stored in a public repository).

Second, it is likely that closed membership groups will coexist so levels of sharing, perhaps delayed, can be supported. This is the problem of proving membership of a group while preserving anonymity for which solutions exist [54].

Third, there may be the need to contact directly a sharing party, such as in case of the responsible disclosure of a vulnerability—(in alignment with the *Detectability* requirement we previously identified. Considering full anonymity, one can envision a number of solutions to this problem, such as each sharing party publishing a public key that is used to encrypt a broadcast communication that only the receiving party can read. This is important to meet the requirement of plausible deniability, as previously discussed.

IV. Toward an Architecture

In this section, we consolidate our overall findings of this article to arrive at a set of requirements and a meta-architecture, or design pattern, for open crowd-sourced sharing of CTI. We remind ourselves that the problem is multidimensional. First, we have socio-techno challenges, particularly those that involve some degree of misconceptions about the practices of sharing CTI. As the public is aware, it has yet to be proven that confidentiality risks are significant and our multipronged survey indicates it is not. Challenges related to "free-riding" or economic incentives might be more difficult to tackle. Second, we have technical challenges, but the ones we raise are either addressable by common technologies or, most interestingly, reflect the lack of a common understanding of sharing CTI and the underlying requirements. For example, we see that the architectures proposed in the literature assume different aims—such as restricted sharing groups. Third, there are operational challenges, such as generating CTI from internal data and end-to-end automation from feed to devices. This is, however, outside the scope of this article. Fourth and final, we have novel requirements such as reputation management and plausible deniability, which are only partially tackled by literature, at least in the context of CTI.

A. Requirements

Table IV lists and elaborates on the requirements for an architecture which we summarize as follows. Table V maps our requirements on previous sections of our article and, thus, reviewed literature.

Identity—Each participating party and CTI event must have a unique identity that must persist in time. We stress that this identity must allow anonymity while not making it a strict requirement as there are use-cases where full attribution is desired.

Bidirectionality—CTI should be an interactive process that evolves over time and require communication inside the communities, for example, to allow messaging. We break this requirement in two. First, we need communication means that can support full anonymity. Second, a feedback mechanism to enrich and re-annotate events are needed. In other words, once a feed is released, the community as a whole is able to add more information to it.

Collaboration model—The model of collaboration is critical. It needs to be flexible in order to allow self-sovereignty, which maps onto four subrequirements. First, it must allow decentralized topologies so that self-organization is possible while not depending on a particular central point. Second, a viable architecture needs to be instrumented so that data analytics is possible. Third, and related, it must support incentives, either run by the community in itself or supported and promoted by a inter/national agency. Finally, the model must support reputation models and tracking.

Actionability—CTI must be as actionable as possible; furthermore, it should allow for a progressively more complex representation of threats well beyond simple indicators. This

TABLE IV
REQUIREMENTS OF AN OPEN, CROWD-SOURCED, CTI SHARING ARCHITECTURE

Category	#	Requirement	Elaboration
Identity	**ID1**	persistent, anonymous identities	Parties generating and sharing CTI should remain anonymous by default, unless otherwise desired. However, identities need to be persistent over time so that, for example, reputation can be built over time. Note that the identity subsystem needs to offer authenticity means such as, for example, strong signatures.
Bidirectionality	**BI1**	confidential messaging	By bidirectionality we mean that, beyond sharing information from sharer to communities, one may need communication mechanisms – and confidential – directed at a specific sharing party. An example is a confidential notification about a vulnerability or confidential information inadvertently shared. Since **ID1** requires anonymity, special messaging mechanisms need to be designed.
	BI2	event re-annotation	Parties must be able to annotate and augment previously shared information. A simple but notable example is MISP's `last-seen` field that gives confidence to an indicator. Another example is flagging duplicates. A more complex example is an indicator of a campaign using IP addresses that keep getting updated in a collaborative fashion.
Collaboration Model	**CO1**	decentralized membership topologies	There should be no central coordinating party nor any dependence on a particular point. Beyond reliability and security, this is mostly for trust and accountability, as a coordinating entity may hold linkable information about parties that other parties do not (e.g., metadata about sharing patterns). From a different angle, a central point would also hold power over the network and make difficult the creation of trust communities that re-share based on internal policies. Similarly, the architecture should support group membership (up to closed or gated communities) while running over the open architecture.
	CO2	sharing analytics	The architecture must be instrumented in a way that allows confidential and aggregate, but authentic, data analytics. For example, a sharing party may need to assert to a third party (e.g., cyber insurance or authorities) it is level of contribution to the CTI communities.
	CO3	incentive mechanisms	The architecture must support incentive schemes to promote sharing and safety, of CTI. A straightforward example is enabling monetization of sources, but it could be in other forms.
	CO4	collaborative reputation models	Reputation is a central element for reasons such as data quality, disinformation, etc. Reliable and helpful parties should be rewarded and the opposite discredited.
Actionability	**AC1**	standard, machine-readable formats	This is a requirement that is now widely met: sharing standards should be open, extensible, machine-readable, and support semantics so that ontological models can be built. For example, the ability to express a Tactic is still challenging.
Safety	**SA1**	sanitization of shared data	sanitization at the source must be supported, and in multiple forms from obfuscation to blanking, including by aggregates supporting data set anonymity models.
	SA2	plausible deniability	Safe sharing also requires that sharing parties are immune to liability from sharing information. Therefore, CTI must be protected from being used as evidence against the sharing party.

TABLE V
REQUIREMENTS MAPPED AGAINST LITERATURE REVIEW; SECTIONS NAMES ARE ABBREVIATED

Requirement	**Legal** Section II-A1	**Interoperability** Section II-A2	**Usefulness** Section II-A3	**Market** Section II-A4	**Trust** Section II-A5	**Confidentiality** Section II-A6
Identity	×			×	×	×
Bidirectionality		×	×		×	
Collaboration Model			×	×	×	
Actionability		×	×			×
Safety	×			×	×	×

requirement is likely to be addressed by (potentially small) redesigns of existing standards.

Safety—Finally, CTI sharing should be safe, considering the risks it represents. By safety we mean both sanitization of confidential data prior to sharing and plausible deniability so that, e.g., regulatory liabilities cannot be incurred.

At first glance, none of the requirements seem technically unfeasible and in need of novel technologies. For example, anonymous identities can rely on self-generated cryptographic certificates that are stored in a publicly accessible location. In particular, distributed ledgers may offer a straightforward and elegant solution for this specific problem. *Plausible deniability*

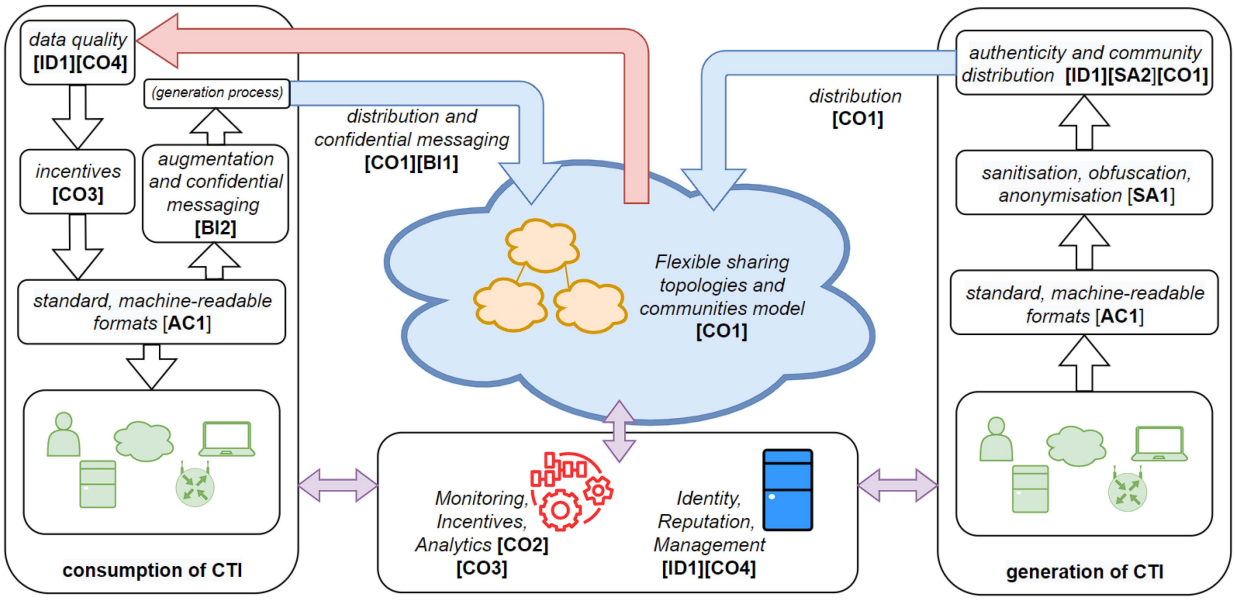

Fig. 5. Meta-architecture for open crowd-sourced sharing of CTI.

might be more challenging, particularly where it might conflict with other requirements. A simple approach is to offer a solution similar to the previously mentioned off-the-record protocol. This topic, along with the overall integration of all requirements, needs further research.

B. Meta-Architecture

In this final section, we propose a reference (meta) architecture that can potentially meet the requirements as laid out. We are terming it *meta-architecture* as we do not advance specific technologies or guidelines; we focus instead on a systems approach akin to eliciting functional requirements aligned and constrained by the socio-technical dimensions.

Fig. 5 shows how we envision an open crowd-sourced CTI sharing architecture as per the identified requirements (noted as **RQ**). The CTI data are stored on public infrastructure such as open cloud servers. The precise topologies and ownerships of the servers should be kept open and free, also to support private membership or delayed release of information (**CO1**). Keeping the platform open will further enable and/or promote data analytics for performance, trust, etc. (**CO2**) and incentive schemes (**CO3**). Sourcing CTI needs an established process. First and foremost, standard and machine-readable formats are needed (**AC1**). Before sharing, two key aspects must be contemplated. First, it needs sanitization to the degree the sharing organization is comfortable with (**SA1**). Second, CTI should be signed in some form and these identities should be publicly accessible for performance (**CO2**) and auditing (**CO4**) purposes which include tracking the reputation of an entity. We stress that we do not need real identities but only persistent ones (**ID1**), similar to an online shop where customers have a reputation index associated even if their real identity is not known. In fact, even in the case that a sharing party is willing to disclose its identity, it is likely to require plausible deniability (**SA2**).

Beyond processing and actuating on the sharing CTI, the receiving side takes two important roles. One is to support and encourage incentive schemes (**CO3**). A second role is to provide a feedback loop for two reasons (**BI2**). First, whenever there is an opportunity, it should augment the existing CTI, even if simply to confirm existing CTI, thus, contributing to increasing data quality and removal of duplicates or misleading CTI. Furthermore, whenever CTI has confidential information or suggests a vulnerability, an alert should be broadcast that must be confidential (**BI1**) yet using the public infrastructure (e.g., by encrypting with a public key associated with the identity). We note that these reannotation processes should follow the generation process for safety.

V. Conclusion

We argued that the vision of open crowd-based sharing of CTI was feasible as long as there was a thorough integration of different dimensions: social, regulatory, technical, and organizational. In particular, we laid out the case that confidentiality—the barrier more frequently raised—included a mixture of different requirements. In fact, not only does each requirement seem to be addressable with existing technology, but the requirement itself was quickly neglected in practice past the first step. Other requirements, such as regulatory compliance, are far more decisive but less recognized and seemingly addressable. In essence, we were left with two main challenges. First, a collective adherence to open sharing would benefit all but was perceived as a competitive disadvantage. A combination of public policy and incentives might change this condition. The second key aspect concerned the automation of the process beyond simple indicators and aiming at approaching automated

characterization of tactics, techniques, and procedures. We had thus, proposed a first-principles architecture that future work needs to validate, particularly at scale.

REFERENCES

[1] Bank of England, "Cbest intelligence-led testing–understanding cyber threat intelligence operations (version 2.0)," 2016. [Online]. Available: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

[2] G. Appiah, J. Amankwah-Amoah, and Y.-L. Liu, "Organizational architecture, resilience, and cyberattacks," *IEEE Trans. Eng. Manag.*, vol. 69, no. 5, pp. 2218–2233, Oct. 2022.

[3] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requirements Eng.*, vol. 16, no. 1, pp. 3–32, 2011.

[4] G. Fisk, C. Ardi, N. Pickett, J. Heidemann, M. Fisk, and C. Papadopoulos, "Privacy principles for sharing cyber security data," in *Proc. IEEE Int. Workshop Privacy Eng.*, San Jose, CA, USA2015, pp. 193–197. [Online]. Available: http://www.isi.edu/%7ejohnh/PAPERS/Fisk15a.html

[5] A. Zibak and A. Simpson, "Cyber threat information sharing: Perceived benefits and barriers," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, 2019, pp. 1–9.

[6] O. Serrano, L. Dandurand, and S. Brown, "On the design of a cyber security data sharing system," in *Proc. ACM Workshop Inf. Sharing Collaborative Secur.*, New York, NY, USA, 2014, pp. 61–69.

[7] C. Sullivan and E. Burger, "In the public interest: The privacy implications of international business-to-business sharing of cyber-threat intelligence," *Comput. Law Secur. Rev.*, vol. 33, no. 1, pp. 14–29, 2017.

[8] CSRIC, WG5: Cyber Security Information Sharing, "Information sharing barriers," 2015. [Online]. Available: https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5InfoSharingReport062016.pdf

[9] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," *Wirtschaftsinformatik und Angewandte Informatik*, 2017.

[10] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, "Rethinking information sharing for threat intelligence," in *Proc. 5th ACM/IEEE Workshop Hot Topics Web Syst. Technol.*, New York, NY, USA, 2017, pp. 1–7.

[11] D. Blanco, "The pyramid of pain," 2014, Accessed: Aug. 9, 2022. [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[12] M. Landauer, F. Skopik, M. Wurzenberger, W. Hotwagner, and A. Rauber, "A framework for cyber threat intelligence extraction from raw log data," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 3200–3209.

[13] C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, "An analysis and classification of public information security data sources used in research and practice," *Comput. Secur.*, vol. 82, no. C., pp. 140–155, May 2019.

[14] "Misp: Malware information sharing platform," Accessed: Aug. 9, 2022. [Online]. Available: https://www.misp-project.org

[15] SANS Institute, "Who's using cyberthreat intelligence and how?," Tech. Rep., 2015. [Online]. Available: https://www.sans.org/webcasts/cyberthreat-intelligence-how-1-definitions-tools-standards-99052/

[16] S. Abu, S. R. Selamat, A. F. M. Ariffin, and R. Yusof, "Cyber threat intelligence–issue and challenges," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 10, pp. 371–379, 2018.

[17] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, 2018.

[18] K. Oosthoek and C. Doerr, "Cyber threat intelligence: A product without a process?," *Int. J. Intell. CounterIntelligence*, vol. 34, no. 2, pp. 300–315, 2021.

[19] A. Zibak and A. Simpson, "Towards better understanding of cyber security information sharing," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment*, 2019, pp. 1–8.

[20] J. M. Ahrend, M. Jirotka, and K. Jones, "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment*, 2017, pp. 1–10.

[21] J. Kotsias, A. Ahmad, and R. Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation," *Eur. J. Inf. Syst.*, vol. 32, no. 1, pp. 35–51, 2023.

[22] P. Fonash and P. Schneck, "Cybersecurity: From months to milliseconds," *Computer*, vol. 48, no. 1, pp. 42–50, 2015.

[23] Verizon, "Data breach investigations report," 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[24] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *J. Accounting Public Policy*, vol. 34, no. 5, pp. 509–519, 2015.

[25] S. Murdoch and N. Leaver, "Anonymity vs. trust in cyber-security collaboration," in *Proc. 2nd ACM Workshop Inf. Sharing Collaborative Secur.*, New York, NY, USA, 2015, pp. 27–29.

[26] J. Vos, Z. Erkin, and C. Doerr, "Compare before you buy: Privacy-preserving selection of threat intelligence providers," Cryptol. ePrint Arch., Paper 2021/1260, 2021. [Online]. Available: https://eprint.iacr.org/2021/1260; https://eprint.iacr.org/2021/1260

[27] UK National Cyber Security Centre, "Cyber security information sharing partnership (CiSP)," Accessed: Nov. 1 2022. [Online]. Available: https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

[28] U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA), "Cyber information sharing and collaboration program (CISCP)," Accessed: Nov. 1 2022. [Online]. Available: https://www.cisa.gov/ciscp

[29] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana, "Shall we collaborate? A model to analyse the benefits of information sharing," in *Proc. ACM Workshop Inf. Sharing Collaborative Secur.*, New York, NY, USA, 2016, pp. 15–24.

[30] Z. Rashid, U. Noor, and J. Altmann, "Network externalities in cybersecurity information sharing ecosystems," in *Proc. 15th Int. Conf.*, 2019, pp. 116–125.

[31] W. Xie, X. Yu, Y. Zhang, and H. Wang, "An improved shapley value benefit distribution mechanism in cooperative game of cyber threat intelligence sharing," in *Proc. IEEE INFOCOM - IEEE Conf. Comput. Commun. Workshops*, 2020, pp. 810–815.

[32] Z. Rashid, U. Noor, and J. Altmann, "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem," *Future Gener. Comput. Syst.*, vol. 124, pp. 436–466, 2021.

[33] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, "In whom do we trust - sharing security events," in *Management Security Age Hyperconnectivity*, R. Badonnel, R. Koch, A. Pras, M. Drašar, and B. Stiller, Eds. Cham, Switzerland: Springer, 2016, pp. 111–124.

[34] P. Radanliev, D. De Roure, P. Burnap, and O. Santos, "Epistemological equation for analysing uncontrollable states in complex systems: Quantifying cyber risks from the Internet of Things," *Rev. Socionetwork Strategies*, vol. 15, no. 2, pp. 381–411, Nov. 2021.

[35] P. Ranade, A. Piplai, S. Mittal, A. Joshi, and T. Finin, "Generating fake cyber threat intelligence using transformer-based models," in *Proc. Int. Joint Conf. Neural Netw.*, pp. 1–9, 2021.

[36] A. Albakri, E. Boiten, and R. De Lemos, "Risks of sharing cyber incident information," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, 2018, New York, NY, USA, 2018, pp. 1–10.

[37] S. Bromander et al., "Investigating sharing of cyber threat intelligence and proposing a new data model for enabling automation in knowledge representation and exchange," *Digit. Threats*, vol. 3, no. 1, pp. 1–22, Oct. 2021.

[38] Vocabulary for Event Recording and Incident Sharing (VERIS), Accessed: Aug. 9, 2022. [Online]. Available: http://veriscommunity.net

[39] Verizon,Data Breach Incident Report (yearly), Accessed: Aug. 9, 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[40] VERIS Community Database, Accessed: Aug. 9, 2022. [Online]. Available: https://github.com/vz-risk/VCDB

[41] R. Danyliw, "The incident object description exchange format version 2," RFC 7970, Nov. 2016.

[42] B. Feinstein, D. Curry, and H. Debar, "The intrusion detection message exchange format (IDMEF)," RFC 4765, Mar. 2007.

[43] T. Takahashi, R. Danyliw, and M. Suzuki, "JSON binding of the incident object description exchange format," RFC 8727, Aug. 2020.

[44] OASIS, "Stix version 2.1," 2019. [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html

[45] OASIS, "Cyber observable expression (cybox) archive website," Accessed: Aug. 9, 2022. [Online]. Available: https://cyboxproject.github.io/

[46] M. Muckin and S. C. Fitch, "A threat-driven approach to cyber security," Bethesda, MD, USA, Lockheed Martin Corporation, White Paper, 2019.

[47] Fireeye, "Openioc," Accessed: Aug. 9, 2022. [Online]. Available: https://github.com/fireeye/OpenIOC_1.1

[48] e-Infrastruktura, CESNET, "Intrusion detection extensible alert (idea)," Accessed: Aug. 9, 2022. [Online]. Available: https://idea.cesnet.cz/

[49] "Misp format," work in progress, Accessed: Aug. 9, 2022. [Online]. Available: https://github.com/MISP/misp-rfc

[50] J. Connolly, M. Davidson, and C. Schmidt, "The trusted automated exchange of indicator information (TAXII)," The MITRE Corporation, 2014. [Online]. Available: http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_May_2014.pdf

[51] P. R. Zimmermann, "Why I wrote PGP: Essays on PGP," Phil Zimmermann & Associates LLC., 1999. [Online]. Available: http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

[52] M. Liu, Z. Xue, X. He, and J. Chen, "Cyberthreat-intelligence information sharing: Enhancing collaborative security," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 17–22, May 2019.

[53] J. M. de Fuentes, L. González-Manzano, J. E. Tapiador, and P. Peris-López, "Pracis: Privacy-preserving and aggregatable cybersecurity information sharing," *Comput. Secur.*, vol. 69, pp. 127–141, 2017.

[54] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, 2004, pp. 132–145.

[55] S. Badsha, I. Vakilinia, and S. Sengupta, "Privacy preserving cyber threat information sharing and learning for cyber defense," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf.*, 2019, pp. 0708–0714.

[56] D. Preuveneers, W. Joosen, J. Bernal Bernabe, and A. Skarmeta, "Distributed security framework for reliable threat intelligence sharing," *Secur. Commun. Netw.*, vol. 2020, Aug. 2020, Art. no. 8833765.

[57] R. Riesco, X. Larriva-Novo, and V. A. Villagra, "Cybersecurity threat intelligence knowledge exchange based on blockchain," *Telecommun. Syst., Model., Anal., Des. Manage.*, vol. 73, no. 2, pp. 259–288, Feb. 2020.

[58] Y. Wu, Y. Qiao, Y. Ye, and B. Lee, "Towards improved trust in threat intelligence sharing using blockchain and trusted computing," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur.*, 2019, pp. 474–481.

[59] S. Purohit, P. Calyam, S. Wang, R. Yempalla, and J. Varghese, "Defensechain: Consortium blockchain for cyber threat intelligence sharing and defense," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Serv.*, 2020, pp. 112–119.

[60] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, 2020, Art. no. 824.

[61] F. Menges and G. Pernul, "A comparative analysis of incident reporting formats," *Comput. Secur.*, vol. 73, pp. 87–101, 2018.

[62] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proc. ACM Workshop Inf. Sharing Collaborative Secur.*, New York, NY, USA, 2014, pp. 51–60.

[63] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Comput. Secur.*, vol. 67, pp. 35–58, 2017.

[64] H. Al-Mohannadi, I. Awan, J. A. Hamar, A. J. Cullen, J. P. Disso, and L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl.*, 2018, pp. 900–906.

[65] V. Mavroeidis, R. Hohimer, T. Casey, and A. Jesang, "Threat actor type inference and characterization within cyber threat intelligence," in *Proc. 13th Int. Conf. Cyber Conflict*, 2021, pp. 327–352.

[66] E. Asgarli and E. Burger, "Semantic ontologies for cyber threat sharing standards," in *Proc. IEEE Symp. Technol. Homeland Secur.*, 2016, pp. 1–6.

[67] S. Lee, H. Cho, N. Kim, B. Kim, and J. Park, "Managing cyber threat intelligence in a graph database: Methods of analyzing intrusion sets, threat actors, and campaigns," in *Proc. Int. Conf. Platform Technol. Serv.*, 2018, pp. 1–6.

[68] Z. Liu et al., "Stix-based network security knowledge graph ontology modeling method," in *Proc. 3rd Int. Conf. Geoinformatics Data Anal.*, New York, NY, USA, 2020, pp. 152–157.

[69] Y. Zhao, B. Lang, and M. Liu, "Ontology-based unified model for heterogeneous threat intelligence integration and sharing," in *Proc. IEEE 11th Int. Conf. Anti-Counterfeiting, Secur., Identification*, 2017, pp. 11–15.

[70] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *Proc. Eur. Intell. Secur. Inform. Conf.*, 2017, pp. 91–98.

[71] A. Piplai, S. Mittal, M. Abdelsalam, M. Gupta, A. Joshi, and T. Finin, "Knowledge enrichment by fusing representations for malware threat intelligence and behavior," *in Proc. IEEE Int. Conf. Intell. Secur. Inform.*, 2020, pp. 1–6.

[72] S. N. Narayanan, A. Ganesan, K. P. Joshi, T. Oates, A. Joshi, and T. W. Finin, "Early detection of cybersecurity threats using collaborative cognition," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput.*, 2018, pp. 354–363.

[73] Q. Li, Z. Jiang, Z. Yang, B. Liu, X. Wang, and Y. Zhang, "A quality evaluation method of cyber threat intelligence in user perspective," in *Proc. IEEE 17th Int. Conf. Trust, Secur. Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng.*, 2018, pp. 269–276.

[74] X. Wang et al., "Dnrti: A large-scale dataset for named entity recognition in threat intelligence," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, 2020, pp. 1842–1848.

[75] F. L. Greitzer, J. Purl, Y. M. Leong, and P. J. Sticha, "Positioning your organization to respond to insider threats," *IEEE Eng. Manag. Rev.*, vol. 47, no. 2, pp. 75–83, Secondquarter 2019.

[76] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2016, pp. 755–766.

[77] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Commun. Surv. Tut.*, vol. 18, no. 2, pp. 1197–1227, Secondquarter 2016.

[78] J. Robertson et al., *Darkweb Cyber Threat Intelligence Mining*. New York, NY, USA: Cambridge Univ. Press, 2017.

[79] K. Li, H. Wen, H. Li, H. Zhu, and L. Sun, "Security osif: Toward automatic discovery and analysis of event based cyber threat intelligence," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.*, 2018, pp. 741–747.

[80] M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "A literature review on mining cyberthreat intelligence from unstructured texts," in *Proc. Int. Conf. Data Mining Workshops*, 2020, pp. 516–525.

[81] H. Jo, Y. Lee, and S. Shin, "Vulcan: Automatic extraction and analysis of cyber threat intelligence from unstructured text," *Comput. Secur.*, vol. 120, 2022, Art. no. 102763.

[82] R. Azevedo, I. Medeiros, and A. Bessani, "PURE: Generating quality threat intelligence by clustering and correlating OSINT," in *Proc. IEEE 18th Int. Conf. On Trust, Secur. Privacy Comput. Commun./IEEE 13th Int. Conf. Big Data Sci. Eng.*, 2019, pp. 483–490.

[83] V. E. Urias, W. M. S. Stout, and H. W. Lin, "Gathering threat intelligence through computer network deception," in *Proc. IEEE Symp. Technol. Homeland Secur.*, 2016, pp. 1–6.

[84] I. Vakilinia, S. Cheung, and S. Sengupta, "Sharing susceptible passwords as cyber threat intelligence feed," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, 2018, pp. 1–6.

[85] P. Pathak, M. Raj Jaiswal, M. Kumar Gupta, S. Sharma, and R. Singhnayak, "Leveraging research honeypots for generating credible threat intelligence and advanced threat analytics," *River Publishers Ser. Digit. Secur. Forensics*, pp. 67–110, 2021.

[86] J. Thom, Y. Shah, and S. Sengupta, "Correlation of cyber threat intelligence data across global honeypots," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf.*, 2021, pp. 0766–0772.

[87] E. Bou-Harb, M. Husák, M. Debbabi, and C. Assi, "Big data sanitization and cyber situational awareness: A network telescope perspective," *IEEE Trans. Big Data*, vol. 5, no. 4, pp. 439–453, Dec. 2019.

[88] F. Iglesias and T. Zseby, "Pattern discovery in internet background radiation," *IEEE Trans. Big Data*, vol. 5, no. 4, pp. 467–480, Dec. 2019.

[89] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, and G. Srivastava, "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 18, no. 9, pp. 6358–6367, Sep. 2022.

[90] S. Gong, J. Cho, and C. Lee, "A reliability comparison method for OSINT validity analysis," *IEEE Trans. Ind. Inform.*, vol. 14, no. 12, pp. 5428–5435, Dec. 2018.

[91] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.

[92] M. R. Rahman, R. M. Hezaveh, and L. Williams, "What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–36, Mar. 2023.
[93] "MITRE, common vulnerabilities and exposures (CVE)," Accessed: Aug. 9, 2022. [Online]. Available: https://cve.mitre.org/
[94] "NIST, national vulnerability database," Accessed: Aug. 9, 2022. [Online]. Available: https://nvd.nist.gov/
[95] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat, and L. Njilla, "Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence," 2017. [Online]. Available: https://arxiv.org/abs/1702.00552
[96] T. Schaberreiter et al., "A quantitative evaluation of trust in the quality of cyber threat intelligence sources," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, 2019.
[97] A. Yeboah-Ofori et al., "Cyber threat predictive analytics for improving cyber supply chain security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021.
[98] M.-E. Paté-Cornell and M. A. Kuypers, "A probabilistic analysis of cyber risks," *IEEE Trans. Eng. Manag.*, vol. 70, no. 1, pp. 3–13, Jan. 2023.
[99] R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever, "Feedrank: A tamper- resistant method for the ranking of cyber threat intelligence feeds," in *Proc. 10th Int. Conf. Cyber Conflict*, 2018, pp. 321–344.
[100] S. Mitra, A. Piplai, S. Mittal, and A. Joshi, "Combating fake cyber threat intelligence using provenance in cybersecurity knowledge graphs," *Proc. IEEE Int. Conf. Big Data*, 2021, pp. 3316–3323.
[101] P. Radanliev, D. De Roure, C. Maple, and U. Ani, "Super-forecasting the 'technological singularity' risks from artificial intelligence," *Evolving Syst.*, vol. 13, no. 5, pp. 747–757, Oct. 2022.
[102] P. Ranade, A. Piplai, S. Mittal, A. Joshi, and T. Finin, "Generating fake cyber threat intelligence using transformer-based models," in *Proc. Int. Joint Conf. Neural Netw.*, 2021, pp. 1–9.
[103] A. Berady, M. Jaume, V. V. T. Tong, and G. Guette, "From TTP to IoC: Advanced persistent graphs for threat hunting," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1321–1333, Jun. 2021.
[104] Y. Gao, X. Li, H. Peng, B. Fang, and P. S. Yu, "Hincti: A cyber threat intelligence modeling and identification system based on heterogeneous information network," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 2, pp. 708–722, Feb. 2022.
[105] Y.-T. Huang, C. Y. Lin, Y.-R. Guo, K.-C. Lo, Y. S. Sun, and M. C. Chen, "Open source intelligence for malicious behavior discovery and interpretation," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 776–789, Mar./Apr. 2022.
[106] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in iot-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2472–2481, Feb. 2023.
[107] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks," *Evolving Syst.*, vol. 11, no. 3, pp. 479–490, Sep. 2020.
[108] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 640–660, Firstquarter 2019.
[109] Y. Xu, Y. Yang, and Y. He, "A business process oriented dynamic cyber threat intelligence model," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.*, 2019, pp. 648–653.
[110] P. Amthor, D. Fischer, W. E. Kühnhauser, and D. Stelzer, "Automated cyber threat sensing and responding: Integrating threat intelligence into security-policy-controlled systems," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, 2019, pp. 1–10.
[111] M. van Haastrecht et al., "A shared cyber threat intelligence solution for smes," *Electronics*, vol. 10, no. 23, 2021, Art. no. 2913.
[112] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler, "Acquiring cyber threat intelligence through security information correlation," in *Proc. 3rd IEEE Int. Conf. Cybern.*, 2017, pp. 1–7.
[113] V. Mavroeidis, P. Eis, M. Zadnik, M. Caselli, and B. Jordan, "On the integration of course of action playbooks into shareable cyber threat intelligence," in *Proc. IEEE Int. Conf. Big Data*, 2021, pp. 2104–2108.
[114] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Commun. Surv. Tut.*, vol. 23, no. 4, pp. 2525–2556, Fourthquarter 2021.
[115] F. A. AlShlawi, N. K. AlSa'awi, W. Y. Bin Saleem, and A. Ara, "Dustmask: A framework for preventing bitcoin's dust attacks," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur.*, 2020, pp. 1–6.
[116] "Off-the-record messaging protocol version 3," Accessed: Aug. 9, 2022. [Online]. Available: https://otr.cypherpunks.ca/
[117] P. Murmann and S. Fischer-Hübner, "Tools for achieving usable ex post transparency: A survey," *IEEE Access*, vol. 5, pp. 22965–22991, 2017.

Vitor Jesus received the M.Sc. and Ph.D. degrees in computer science, cybersecurity, and privacy from University of Aveiro, Portugal, in 2006 and 2013.

He has 20 years of experience split between industry and academia. Having held lead technical roles at large and small organizations, he is currently a Lecturer in trusted systems, cyberecurity, and privacy with the Computer Science Department, Aston University, Birmingham, U.K. He is also a Consultant, especially interested in working with start-ups and small businesses looking to different approaches to architectures, security, and privacy. His research interests include designing trusted, secure, efficient and usable systems, across multiple application areas and disciplines.

Dr. Jesus chairs and is an active Member in several communities and standards organizations and a frequent reviewer in conferences and journals.

Balraj Bains received the B.Sc. degree in cybersecurity from Aston University, Birmingham, U.K., in 2023.

Mr. Bains research interests include cyber threat intelligence, Internet of Things, and the application of AI to enhance cybersecurity.

Victor Chang has been a Professor with the Department of Operations and Information Management, Aston Business School, Aston University, Birmingham, U.K., since May 2022.

Dr. Chang has received many awards and achievements, including a European Award on Cloud Migration in 2011, 2015 IEEE Outstanding Service Award, best papers in 2012, 2015, and 2018, 2016 European award: Best Project in Research, 2016–2018 SEID Excellent Scholar, Suzhou, China, Outstanding Young Scientist award 2017, 2017 special award on Data Science, 2017–2023 INSTICC Service Awards, Top 2% Scientist 2017/2018, 2019/2020, 2020/2021 and 2021/2022, the most productive AI-based Data Analytics Scientist (2010–2019), Highly Cited Researcher 2021, and numerous awards.