The CTI Oligopoly's Contractual Firewall: Restrictive Licensing as a Structural Barrier to Collective APT Defence

Raymond Andre Hagen
Norwegian University of Science and technology (NTNU), Norway

Raymond.Andre.Hagen@digdir.no

Abstract: Cyber threat intelligence (CTI) is widely promoted as indispensable for modern cyber defense, yet collective defense in practice is constrained by market concentration and restrictive licensing imposed by a small number of dominant vendors. This study analyses 34 publicly available documents; licence agreements, terms of service, API documentation, and pricing materials, across 15 major commercial CTI providers. Following a thematic analysis approach, we code restrictions across six dimensions: (1) access pathways and subscription gating, (2) redistribution and collaboration rights, (3) automation interfaces and rate limits, (4) portability and interoperability, (5) pricing transparency and contract flexibility, and (6) geographic and jurisdictional constraints. Findings confirm a highly concentrated oligopolistic market in which the top five to ten vendors control an estimated 50–80% of global revenue and a disproportionate share of APT telemetry. Recent consolidation, including Mastercard's USD 2.65 billion acquisition of Recorded Future in December 2024, further reinforces this concentration. Licence terms systematically prohibit redistribution to third parties, constrain automation through non-cumulative quotas and unstable APIs, and obscure pricing behind enterprise sales funnels. These patterns constitute what we term a *contractual firewall*, a structural barrier that prevents threat intelligence from flowing between defenders even where policy frameworks encourage sharing. The contractual firewall creates asymmetries in defensive capability that disproportionately affect SMEs, public-sector entities, and sector consortia. These constraints do in some instances conflict with European collective defense mandates like NIS2, but fundamentally fragment the defender ecosystem, leaving smaller entities vulnerable to sophisticated threat actors. We suggest some procurement-focused recommendations for redistribution carve-outs, export and portability requirements, API stability guarantees, and multi-source resilience strategies. Future work should validate these patterns against negotiated enterprise terms and assess operational impact in incident response environments. We conclude that resource-constrained defenders facing APTs are caught in a systemic double bind: the 'contractual firewall' restricts the intelligence access necessary for pro-active defense, while regulatory frameworks like NIS2 impose sharing mandates that these commercial restrictions effectively render impossible to fulfill.

Keywords: CTI, Threat intelligence, AI

1. Introduction

Cyber threat intelligence (CTI) is widely marketed as the missing component that makes detection and response effective at scale. In practice, CTI is embedded in complex socio-technical systems where information must be shared, integrated, and acted upon in real-world defensive workflows.

This paper investigates whether publicly available materials from commercial CTI providers, including license agreements, terms of service, API documentation, and pricing information, reveal patterns of market concentration and how these patterns affect collective defense against

APTs. It examines constraints across six operationally relevant dimensions: (i) access pathways and subscription gating, (ii) redistribution and collaboration rights, (iii) automation interfaces and rate limits, (iv) portability and interoperability, (v) pricing transparency and contract flexibility, and (vi) geographic and jurisdictional constraints.

Based on these dimensions, the paper demonstrates that the CTI market exhibits a set of systemic barriers that are incompatible with mandates for collective defense, such as those reflected in the EU NIS2 Directive (NIS2). (European Union, 2022)

The analysis is limited to publicly accessible documents captured between January and October 2025 and does not assess detection efficacy or indicator quality.

Contribution. The paper contributes three elements: (i) a conceptual framing of a "contractual firewall" as a systemic barrier to CTI sharing, (ii) an empirical analysis of 15 leading providers based on public documents, and (iii) practical procurement guidance aimed at mitigating lock-in and enabling collective defense.

To structure the investigation, we pose three research questions:

RQ1: What patterns of market concentration are visible in the commercial CTI landscape based on publicly available contractual and technical materials?

RQ2: How do access terms, redistribution rights, and automation constraints influence the practical use of CTI in operational security processes?

RQ3: What are the implications of these patterns and terms for European collective defense and policy goals, such as those reflected in the EU NIS2 Directive (NIS2)? (European Union, 2022)

Structure of the paper. Section 2 provides background and defines the scope; Section 3 reviews related work; Section 4 describes the method; Section 5 presents the main findings; Section 6 discusses practical and policy implications; Section 7 offers recommendations for procurement teams; Section 8 addresses limitations and future work; Section 9 concludes.

2. Background and Scope

Commercial cyber threat intelligence (CTI) supports organizations by providing indicators of compromise (IoCs), actor tracking, detection logic, and contextual analysis. It is positioned as a crucial layer for defending against advanced persistent threats (APTs) which are long-lived, cross-border by nature, and often exploit asymmetries between national and commercial defenders.

At the policy level, European frameworks increasingly emphasize information sharing and cooperative resilience. The EU NIS2 Directive (Directive (EU) 2022/2555) strengthens obligations for incident reporting, risk management, and cross-sector cooperation, and it encourages voluntary information-sharing arrangements (Article 29). (European Union, 2022)

This paper focuses on the intersection between these policy aims and the commercial CTI market. It treats licensing terms, access pathways, and technical integration constraints as first-order determinants of whether organizations can participate effectively in collaborative defense.

3. Related Work

The intersection of commercial CTI markets and collective defense has received limited systematic attention in the academic literature, though related threads of research inform this study.

3.1 CTI Quality and Operationalization

Research on CTI quality has established frameworks for evaluating intelligence outputs. Schlette et al. (2020) developed metrics for measuring and visualizing CTI quality, highlighting the gap between raw indicators and actionable intelligence. Böhm et al. (2018) introduced graph-based visual analytics approaches for CTI, enabling analysts to identify patterns across large indicator sets. More recently, Chatziamanetoglou and Rantos (2025) proposed weighted quality criteria for CTI assessment within the MISP data model, demonstrating ongoing efforts to standardize evaluation.

Systematic reviews have mapped the broader CTI landscape. Saeed et al. (2023) establish that organizational cybersecurity resilience depends critically on timely access to high-quality threat intelligence, a dependency that becomes problematic when access is constrained by commercial terms. Aboelfotoh et al. (2025) examine the role of artificial intelligence in enhancing threat detection, noting that AI-driven capabilities are increasingly concentrated in well-resourced commercial platforms.

3.2 Information Sharing and Collective Defense

The theoretical case for threat intelligence sharing rests on classic public goods arguments: threat information is non-rivalrous and exhibits positive externalities when shared. CISA's evolving approach emphasizes "threat-informed cybersecurity" enabled by rapid dissemination (Cybersecurity and Agency, 2023). Similar principles underpin sectoral sharing organizations (ISACs) and coordinated disclosure frameworks (Alliance, 2025). The MITRE framework for world-class security operations centers identifies threat intelligence integration as a core capability (MITRE, 2022), yet assumes access to quality intelligence sources without examining the contractual barriers that may prevent such access.

3.3 Market Structure and Policy Frameworks

The global threat intelligence market has attracted significant analyst attention. Multiple market reports estimate 2025 valuations between USD 6–15 billion with double-digit growth rates (MarketsandMarkets, 2025; Research, 2025b; Intelligence, 2025; Insights, 2025). Industry analyst reports consistently identify a small set of dominant vendors (Research, 2025a; Gartner, 2025; Exabeam, 2025), but systematic analysis of how their contractual terms affect collective defense remains scarce.

European policy frameworks increasingly mandate information sharing and cooperative resilience. The EU NIS2 Directive (Article 29) encourages voluntary cybersecurity information-sharing arrangements, while Article 21 requires essential entities to implement risk management measures that implicitly depend on access to timely threat intelligence (European Union, 2022). The ENISA Threat Landscape provides annual assessments of the evolving threat environment (ENISA, 2025), and the World Economic Forum highlights the widening gap between well-resourced and under-resourced defenders (Forum, 2025).

This policy-market tension, where mandates assume shareable intelligence while commercial terms prohibit sharing, forms the empirical focus of our analysis.

4. Method

We conducted a document analysis of 34 publicly accessible documents covering 15 commercial CTI providers, following a thematic analysis approach (Braun and Clarke, 2006). Data collection occurred between January and October 2025.

4.1 Material Collection

Commercial CTI providers were identified using a combination of industry reports, market ana-lyses, and public directories, including Gartner Magic Quadrant for Security Threat Intelligence Services, Forrester Wave for External Threat Intelligence, and vendor aggregators (Gartner, 2025; Research, 2025a; G2, 2025; Capterra, 2025). Providers were selected based on market prominence, visibility in European procurement, and availability of publicly accessible licensing documentation. The selection focused strictly on dedicated CTI products, excluding generalist cybersecurity firms lacking specific intelligence offerings. Table 1 lists the analyzed providers.

Data collection was conducted manually, utilizing exclusively publicly accessible documents (licence agreements, terms of service, datasheets, API documentation, and pricing pages where available) retrieved via direct website navigation without authentication or paid access. Document types were limited to those detailing CTI features, contractual terms, and technical specifications.

4.2 Inclusion and Exclusion Criteria

Inclusion and exclusion criteria were defined to ensure relevance and reproducibility, aligning with established practices in cybersecurity systematic reviews (Saeed et al., 2023; Aboelfotoh et al., 2025).

Included: Provider-facing materials published or updated within the study window that ex-plicitly address the six operational dimensions: access pathways, redistribution rights, automation interfaces, portability/interoperability, pricing transparency, and geographic constraints.

Excluded: (1) Non-public or customer-only materials; (2) evaluations of technical detection efficacy; (3) reverse engineering of content or APIs; (4) unverifiable claims not grounded in documents; and (5) general marketing materials lacking specific contractual terms (Aboelfotoh et al., 2025; Böhm et al., 2018).

4.3 Analysis Procedure

The analysis followed a structured, multi-stage workflow resembling an expansion-contraction model, designed to manage the complexity and volume of the dataset (Braun and Clarke, 2006). **Phase 1: Domain Scoping and Selection.** Initially, we established a baseline understand-ing of the CTI landscape through a review of general industry reports and market definitions.

This phase focused on identifying key market players and establishing the six operational dimen-sions for analysis, effectively framing the scope before engaging with the high-volume vendor documentation.

Phase 2: Corpus Expansion and Deep Analysis. The core analysis involved a significant expansion in data volume, ingesting 34 specific vendor documents (licenses, API references, pricing models). Given the density of this legal and technical material, we employed digital text analysis tools to cross-validate findings across the vendor pool. This "all-against-all" verification ensured that identified restrictions were not isolated anomalies but systemic patterns within the oligopoly.

Phase 3: Normative Synthesis. Finally, the analysis converged by mapping the validated vendor constraints against specific problem-oriented frameworks, primarily the EU NIS2 Directive and CISA sharing guidelines. This phase focused on interpreting the operational impact of the identified restrictions specifically within the context of collective defense mandates.

5. Findings

5.1 Market Structure and Concentration Signals

Multiple market intelligence reports estimate the global CTI market in 2025 at USD 9–17 billion and growing at high single to double-digit rates (MarketsandMarkets, 2025; Research, 2025b;

Intelligence, 2025; Insights, 2025). Across these reports, the top vendors are consistently ranked with a substantial share of revenue concentrated in a small set of providers. Estimates vary but commonly place the top five to ten vendors at 50–80% of global revenue (MarketsandMarkets, 2025; BitSight, 2025).

The functional implication is that a limited number of platforms control high-volume telemetry, actor tracking, and APT narrative framing. Smaller vendors and community feeds exist (Flare, 2023), but their coverage, automation maturity, and historical depth are limited. Table 1 summarizes the analyzed providers and their restriction patterns.

Table 1: Analyzed CTI Providers and Key Restriction Patterns

Provider	Redistribution	API Limits	Pricing	HQ
CrowdStrike	Prohibited	Rate-limited	Opaque	US
Recorded Future[a]	Prohibited	Quota-based	Opaque	US
Palo Alto Networks	Prohibited	Rate-limited	Opaque	US
Microsoft Defender TI	Limited	Tiered	Partial	US
Mandiant (Google)	Prohibited	Rate-limited	Opaque	US
IBM X-Force	Prohibited	Rate-limited	Opaque	US
Cisco Talos	Prohibited	Rate-limited	Opaque	US
Fortinet FortiGuard	Prohibited	Bundled	Opaque	US
ThreatConnect	Prohibited	Quota-based	Opaque	US
Rapid7	Prohibited	Rate-limited	Partial	US
Group-IB	Prohibited	Negotiated	Opaque	SG[b]
EclecticIQ	Limited	Configurable	Opaque	NL
Sekoia	Limited	Tiered	Partial	FR
Anomali	Prohibited	Rate-limited	Opaque	US
Intel 471	Prohibited	Negotiated	Opaque	US

[A]Acquired by Mastercard (December 2024, USD 2.65B). [B]Relocated headquarters from Russia to Singapore.

5.2 Recent Market Consolidation

Market concentration intensified during 2024–2025 through significant acquisitions. Most notably, Mastercard completed its USD 2.65 billion acquisition of Recorded Future in December 2024, absorbing what had been characterized as "the world's largest threat intelligence company" with over 1,900 clients across 75 countries, including governments of 45 nations and more than half of the Fortune 100 (MarketsandMarkets, 2025). This transaction exemplifies how CTI capabilities are being absorbed into larger financial and technology conglomerates, potentially further consolidating market power and raising questions about long-term pricing and access terms.

5.3 Access Pathways and Subscription Models

Non-trial access to full-featured CTI is directed exclusively through enterprise sales funnels and annual commitments (CrowdStrike, 2025b; Future, 2024). Trial offerings, where available, are generally restricted in scope: limited time, limited content, sometimes community feeds only, and lacking API access or historical data (Microsoft, 2025).

Contractual rigidities create further barriers: minimum contract commitments commonly range from 12 to 36 months, often with automatic renewal clauses (CrowdStrike, 2025c; Future, 2025b). This economic gating is reinforced by explicit messaging that distinguishes large enterprises from SMEs already at the marketing layer.

5.4 Redistribution and Collaboration Rights

Analysis of the license agreements confirms a near-universal restriction on sharing CTI content with third parties, including sector peers, joint ventures, subsidiaries, and external coordination mechanisms. Representative clauses (verbatim or near-verbatim) include:

- Recorded Future (Terms v7.0, Oct 2025): "Customer shall not ... disclose, [...] or use for the benefit of any third party" (Future, 2025b).
- CrowdStrike Falcon Intelligence Terms (2025): "non-exclusive, non-transferable, non-sublicensable license for internal business purposes only" (CrowdStrike, 2025c).
- Palo Alto Networks End User Agreement (2025): "You shall not ... transfer the Software except in accordance with Palo Alto Networks license transfer procedure" (Networks, 2025).
- IBM X-Force Exchange Terms (2025): "Sharing outside of the licensed organization is prohibited unless expressly authorized in writing. (IBM, 2025)"

In practice, these restrictions hinder the creation of shared sector baselines, shared indicator repositories, and defensive collaboration in multi-organization incident response, precisely the activities encouraged under NIS2 Article 29 (European Union, 2022).

5.5 Automation Interfaces and API Constraints

Even where APIs exist, access is often rate-limited, quota-constrained, and governed by terms that restrict automated redistribution, scraping, or bulk extraction (CrowdStrike, 2025a; Future, 2025a; ThreatConnect, 2025). Observed constraints include:

- Hard rate limits and credit-based quotas that reset monthly and cannot be carried over, inhibiting essential retrospective analysis.
- Pagination and query complexity limits that make bulk historical retrieval impractical.
- Schema changes without deprecation periods. Recorded Future and CrowdStrike reserve the right to modify APIs "at any time", increasing integration cost and operational risk (Future, 2025a; CrowdStrike, 2025a).

These patterns make CTI integration less like a stable infrastructure dependency, and more like a fragile vendor-controlled interface.

5.6 Pricing Transparency and Contract Flexibility

Pricing transparency for full-featured CTI offerings is minimal. Procurement teams face "contact sales" funnels and non-disclosed bundles, making it difficult to compare offers and assess switching costs. The only transparent pricing signals found were:

- CrowdStrike Falcon Go (SMB bundle) —USD 59.99/user/year (limited intelligence) (Crowd-Strike, 2025b),
- Microsoft Defender TI Standard —free (community feed only) (Microsoft, 2025),
- Rapid7 Threat Command —"starting at" figures on request pages (Rapid7, 2025).

All other vendors rely on negotiations. Renewal terms and uplift structures can exceed 15–20%, creating budget uncertainty and long-term commitment pressure.

5.7 Geographical and Regulatory Constraints

The market is dominated by U.S.-jurisdiction providers: every large vendor in the sample is U.S.-based or falls under U.S. export control regimes, requiring careful consideration by non-American users regarding data sovereignty and regulatory compliance.

The lack of jurisdictional diversity is notable: based on our document analysis, none of the examined vendors offered a regionally hosted instance of their full CTI platform, forcing defenders to rely on a single legal framework for critical intelligence processing. The two European providers in our sample (EclecticIQ, Sekoia) offer more flexible terms but lack the telemetry depth of their U.S. counterparts.

5.8 Systemic Implications for APT Defence

Taken together, the evidence demonstrates that the commercial CTI market embeds a structural access asymmetry: it concentrates high-value telemetry and actor narratives in a handful of vendors, restricts

redistribution, limits automation, and exhibits opacity around pricing and contract structure. This asymmetry is repeated across contract patterns and technical terms, conflicting with mandates for coordinated, cross-border information sharing (European Union, 2022).

The implications extend beyond individual organizations: when CTI cannot flow between defenders, the ecosystem loses network effects that would otherwise strengthen collective resilience, while threat actors face no equivalent constraints on sharing among themselves (Center for Strategic and International Studies, 2022).

6. Discussion

The preceding analysis indicates what we define as a CTI oligopoly is characterized by concen-trated access, restrictive redistribution rights, and integration constraints. These constraints are not merely legal formalities; they have operational consequences for incident response and collective defense.

6.1 Contractual Firewall as a Coordination Barrier

A contractual firewall emerges when organizations are legally and technically prevented from sharing CTI outputs with trusted peers, sector partners, or coordinating institutions. This firewall is reinforced by non-portable data formats, non-transparent pricing, and asymmetric renewal structures.

The concept parallels established observations in cybersecurity economics: information asymmetries between attackers and defenders are well-documented (Center for Strategic and International Studies, 2022), but less attention has been paid to information asymmetries *among* defenders created by commercial licensing. Where attackers freely share tools, techniques, and target information through underground forums, defenders face contractual prohibitions on equivalent collaboration (ENISA, 2025). The contractual firewall thus represents a structural disadvantage that policy frameworks alone cannot resolve without addressing the underlying market dynamics.

6.2 Implications for SMEs and Public-Sector Defenders

For SMEs and public-sector entities, high subscription costs, limited trial access, and lengthy minimum contract terms can prevent entry into full-featured CTI ecosystems (Forum, 2025). These organizations may remain dependent on community feeds and ad hoc sharing, creating capability gaps relative to large enterprises.

This observation reveals a duality: smaller defenders understand the need for CTI, but lacking economic power, they attempt to build capabilities independently, incurring substantial costs in personnel and skill reallocation that might be more productively deployed in day-to-day security operations. The World Economic Forum has highlighted this widening gap between well-resourced and under-resourced defenders as a systemic risk to global cybersecurity (Forum, 2025).

The implications extend to national security. Public-sector entities responsible for critical infrastructure protection may find themselves unable to access the same intelligence available to private-sector peers, or unable to share threat information received under restrictive licenses with other government agencies (Cybersecurity and Agency, 2023).

6.3 Policy Tension and Cooperative Resilience

NIS2 Article 29 encourages voluntary information sharing and cooperative resilience, specifically enabling exchange of “cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, [and] adversarial tactics” (European Union, 2022). However, the commercial baseline terms documented here restrict precisely these forms of redistribution and inhibit the development of sector-level shared baselines.

This creates a structural tension: European policy assumes that entities can share threat intelligence within trusted communities, while commercial contracts prohibit such sharing. Organizations complying with vendor terms may inadvertently undermine the cooperative security posture that NIS2 seeks to establish.

Furthermore, since APT actors are sophisticated and employ diverse tactics across campaigns (Gan et al., 2023; Splunk, 2025), effective defense often requires correlating intelligence from multiple sources. Organizations subscribing to a single vendor may develop incomplete threat pictures, potentially creating a false sense of security by addressing only the risks visible through their available intelligence sources. The documented restrictions may thus fragment the defender ecosystem precisely where unity would provide the greatest advantage.

7. Recommendations and Actionable Guidance

Based on the observed contractual and technical constraints, we believe these restrictions can significantly reduce an organization's ability to defend against APTs. We also acknowledge that commercial interests are integral to the specialized CTI market; nonetheless, we offer recommendations that may improve organizational APT defence posture, recognizing that some provisions may be difficult to negotiate in procurement processes.

7.1 Possible advisories for procurement teams and security leaders:

1. **Redistribution carve-out for defence:** Permit sharing of indicators, detections, and analytical findings with trusted partners for defensive purposes, aligning with NIS2 Article 29 information-sharing provisions (European Union, 2022).
2. **Explicit export and portability:** Require bulk export in structured formats, including historical data, with defined frequency and without punitive fees (Alliance, 2025).
3. **API stability and change control:** Include minimum notice periods for breaking changes, versioning guarantees, and rate-limit terms that support automation at scale.
4. **Interoperability commitments:** Require documented integration paths to SIEM/SOAR/EDR tooling, with clear terms for connector usage and third-party enrichment.
5. **Pricing and exit transparency:** Make pricing units, overage costs, and data-retention or egress costs explicit, and require an end-of-contract export clause that remains valid after termination.
6. **Jurisdiction and data residency:** Specify geographic restrictions, data residency options, and any limitations on cross-border operational use of CTI outputs.
7. **Operational minimums:** Define minimum deliverables to better implement the CTI platform output into your security operations.
8. **Multi-source resilience:** Where feasible, design for at least one secondary CTI source or community feed to reduce single-vendor dependency and to have the possibility to correlate multiple CTI sources.

8. Limitations and Future Work

This study relies on publicly available documents, so it cannot capture negotiated enterprise agreements, NDAs, or operational practices that may materially alter the baseline constraints reported here. Large enterprises may secure more favorable terms than the public baselines suggest; conversely, smaller organizations may face even stricter conditions. Additionally, while conservative coding practices were applied to mitigate ambiguity, the qualitative nature of thematic analysis involves a degree of subjective interpretation (Braun and Clarke, 2006).

We do not assess detection efficacy, indicator quality, or comparative product performance, dimensions that would require access to operational environments and controlled testing (Schlette et al., 2020). The corpus reflects a fixed time window (January–October 2025), and terms and interfaces can change with limited notice, as explicitly permitted in several of the analyzed agreements.

Future work should (i) compare public baselines with negotiated contracts under controlled access, (ii) validate operational impact through case studies of CTI use in incident response and information-sharing workflows, (iii) conduct longitudinal monitoring of licensing and API com-mitments to quantify stability over time, and (iv) examine whether recent market consolidation affects pricing and contractual flexibility for existing customers.

9. Conclusion

Across 34 public documents and 15 commercial CTI providers, we identify recurring constraints that limit redistribution, automation, portability, and pricing predictability. Together, these patterns function as a *contractual firewall* that hinders cross-organizational coordination and disproportionately disadvantages SMEs, public-sector entities, and sector consortia.

The findings reveal a structural tension between commercial CTI licensing practices and European policy frameworks that mandate cooperative resilience and information sharing (European Union, 2022). Recent market consolidation, exemplified by Mastercard's acquisition of Recorded Future, suggests this concentration may intensify rather than dissipate.

The recommendations translate findings into concrete procurement requirements that improve portability, enable defensive sharing within trusted settings, and reduce lock-in risk. Future work should validate these patterns against negotiated enterprise terms and evaluate operational impact in incident response environments.

The current market structure creates a double failure in APT defense: (1) Economic gating excludes smaller defenders from essential intelligence, while (2) restrictive licensing prevents the collective ecosystem from compensating for this gap through sharing. Consequently, NIS2 mandates for collective resilience are rendered inoperable not by lack of will, but by commercial contract design.

Ethics declaration: This study analyses publicly available documents and does not involve human participants, personal data, or interventions. No ethical clearance was required. To support double-blind review, self-identifying references in the manuscript were removed where not essential to the argument.

Declaration of generative AI and AI-assisted technologies in the writing process: The author used AI-assisted tools to support language editing and LaTeX formatting, including improving clarity and grammar, reducing dyslexia-related spelling and ordering errors, and troubleshooting bibliography and layout issues. All AI-suggested changes were reviewed and approved by the author, who takes full responsibility for the final manuscript and any remaining errors.

References

A. Aboelfotoh et al. A systematic review of cyber threat intelligence: The effectiveness of artificial intelligence in enhancing threat detection and response. Sensors, July 2025. URL https://www.mdpi. com/1424-8220/25/14/4272.

BitSight. A 2025 guide to cyber threat intelligence platforms based on industry, October 2025. URL https: //www.bitsight.com/guides/best-cyber-threat-intelligence-solutions-per-industry.

Capterra. Threat intelligence software reviews 2025, 2025. URL https://www.capterra.com/ threat-intelligence-software/.

Center for Strategic and International Studies. Emerging cyber threats: No state is an island in cyberspace, 2022.URL https://www.csis.org/analysis/ emerging-cyber-threats-no-state-island-cyberspace. State-sponsored collaboration and policy incentives.

Chenquan Gan, Jiabin Lin, Da-Wen Huang, Qingyi Zhu, and Liang Tian. Advanced persistent threats and their defense methods in industrial internet of things: A survey. Mathematics, 11(14):3115, July 2023. doi: 10.3390/math11143115. URL https://www.mdpi.com/2227-7390/11/14/3115.

CrowdStrike. Documentation - crowdstrike developer center, October 2025a. URL https://developer. crowdstrike.com/docs.

CrowdStrike. Endpoint, cloud & identity protection products pricing, October 2025b. URL https: //www.crowdstrike.com/en-us/pricing/.

CrowdStrike. Terms and conditions, October 2025c. URL https://www.crowdstrike.com/en-us/ legal/terms-conditions/.

Cyber Threat Alliance. Cti sharing guidelines and scope definitions, 2025. URL https://www. cyberthreatalliance.org/cti-sharing-guidelines-and-scope-definitions.

Cybersecurity and Infrastructure Security Agency.Enabling threat-informed cy-bersecurity: Evolving cisa's approach to cyber threat information sharing, December 2023. URL https://www.cisa.gov/resources-tools/resources/ enabling-threat-informed-cybersecurity-evolving-cisas-approach-cyber-threat-information-sharing.

Daniel Schlette, Fabian Böhm, Marco Caselli, and Günther Pernul. Measuring and visualizing cyber threat intelligence quality. International Journal of Information Security, 20:21–38, 2020. doi: 10.1007/ s10207-020-00490-y. URL https://link.springer.com/article/10.1007/s10207-020-00490-y.

Dimitrios Chatziamanetoglou and Konstantinos Rantos. Weighted quality criteria for cyber threat intelligence: Assessment and prioritisation in the misp data model. International Journal of Information Security, 24:160, June 2025. doi: 10.1007/s10207-025-01080-6. URL https://link.springer.com/ article/10.1007/s10207-025-01080-6.

ENISA. Enisa threat landscape 2025, November 2025. URL https://www.enisa.europa.eu/ publications/enisa-threat-landscape-2025.

European Union. Directive (eu) 2022/2555 on measures for a high common level of cybersecurity across the union (nis2). Official Journal of the European Union, 2022. URL https://eur-lex.europa.eu/ eli/dir/2022/2555/oj/eng. CELEX:32022L2555.

Exabeam. Best threat intelligence platforms: Top 10 solutions in 2025, 2025. URL https://www.exabeam.com/explainers/cyber-threat-intelligence/ best-threat-intelligence-platforms-top-10-solutions-in-2025/.

Fabian Böhm, Florian Menges, and Günther Pernul. Graph-based visual analytics for cyber threat intelli-gence. Cybersecurity, 1(1):1–16, 2018. doi: 10.1186/s42400-018-0017-4. URL https://cybersecurity. springeropen.com/articles/10.1186/s42400-018-0017-4.

Flare. Threat intelligence feeds: 9 valuable sources of cti, January 2023. URL https://flare.io/learn/ resources/blog/threat-intelligence-feeds/.

Forrester Research. The external threat intelligence service providers land-scape, q1 2025, January 2025a. URL https://www.forrester.com/report/ the-external-threat-intelligence-service-providers-landscape-q1-2025/RES181939.

Fortune Business Insights. Threat intelligence market size, share & industry analysis, by component (solutions, services), by type (strategic, tactical, operational), by deployment (cloud, on-premise), by enterprise type (smes, large enterprise),

by end-user (bfsi, it & telecom, manufacturing, healthcare, energy & utilities, retail, others), and regional forecast, 2025-2032, November 2025. URL https: //www.fortunebusinessinsights.com/threat-intelligence-market-102984.

G2. Best threat intelligence software in 2025, 2025. URL https://www.g2.com/categories/ threat-intelligence.

Gartner. Security threat intelligence products and services (transitioning to cyber threat in-telligence technologies), February 2025. URL https://www.gartner.com/reviews/market/ security-threat-intelligence-products-and-services.

Grand View Research. Threat intelligence market size, share & growth report, 2025-2030, 2025b. URL https://www.grandviewresearch.com/industry-analysis/threat-intelligence-market. USD14.59B in 2023, projected to USD 36.53B by 2030, CAGR 14.7%.

IBM. Ibm x-force exchange terms of use, 2025. URL https://www.ibm.com/legal/terms-of-use.Terms governing X-Force Exchange threat intelligence sharing.

MarketsandMarkets. Threat intelligence market size, share & growth fore-cast 2030, 2025. URL https://www.marketsandmarkets.com/Market-Reports/ threat-intelligence-security-market-150715995.html.

Microsoft. Microsoft defender threat intelligence, 2025. URL https://www.microsoft.com/en-us/ security/business/siem-and-xdr/microsoft-defender-threat-intelligence.

MITRE. 11 strategies of a world-class cybersecurity operations center, 2022. URLhttps://www.mitre.org/sites/default/files/publications/ pr-18-0001-11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.

Mordor Intelligence. Threat intelligence market size & share analysis - growth trends & fore-casts up to 2030, July 2025. URL https://www.mordorintelligence.com/industry-reports/ threat-intelligence-market.

Overview of 29 providers, focusing on top 10–12 for market prominence.

Palo Alto Networks. End user license agreement, February 2025. URL https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf.

Rapid7. What is a threat intelligence feed? types & benefits, 2025. URL https://www.rapid7.com/ fundamentals/threat-intelligence-feeds/.

Recorded Future. Api terms of use, April 2025a. URL https://www.recordedfuture.com/ api-terms-of-use.

Recorded Future. Terms of use, April 2025b. URL https://www.recordedfuture.com/legal/ terms-of-use.

Recorded Future. Top 7 threat intelligence tools for improved cybersecurity, June 2024. URL https: //www.recordedfuture.com/threat-intelligence-101/tools-and-technologies.

Saqib Saeed, Sarah A. Suayyid, Manal S. Al-Ghamdi, Hayfa Al-Muhaisen, and Abdullah M. Almuhaideb. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16):7273, August 2023. doi: 10.3390/s23167273. URL https://www.mdpi.com/1424-8220/ 23/16/7273.

Splunk. Advanced persistent threats (apts): What they are and how to defend against them, June 2025.

ThreatConnect. Rest api — threatconnect developer docs, May 2025. URL https://docs. threatconnect.com/en/latest/rest_api/rest_api.html.

URL https://www.splunk.com/en_us/blog/learn/apts-advanced-persistent-threats.html.

Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2):77–101, 2006. doi: 10.1191/1478088706qp063oa.

World Economic Forum. Global cybersecurity outlook 2025, January 2025. URL https://www.weforum. org/publications/global-cybersecurity-outlook-2025/. Skills gaps, ransomware, and AI-driven attacks.