Magic Quadrant for Cyberthreat Intelligence Technologies

4 May 2026 - ID G00839252 - 69 min read

By Jonathan Nunez, Carlos De Sola Caraballo, and 1 more

Cybersecurity leaders struggle to know what threats constitute real concerns or how to operationalize threat data within their cybersecurity programs. They must select the right cyberthreat intelligence technologies to understand and respond more effectively to the most impactful threats.

Strategic Planning Assumption

By 2028, more than 50% of organizations adopting cyberthreat intelligence (CTI) technologies will prioritize platforms that natively operationalize intelligence through automated detection rule generation, enforcement actions and takedown workflows over those that primarily deliver enrichment and reporting.

Market Definition/Description

The cyberthreat intelligence market encompasses solutions that provide actionable insights, context and guidance regarding cybersecurity threats, threat actors and related issues. These products deliver information and data designed to help organizations understand the identities, motives, behaviors and methods — often called tactics, techniques and procedures (TTPs) — of potential adversaries. The goal is to enhance decision making and strengthen security measures, ultimately reducing both the risk and impact of cyber incidents.

Cyberthreat intelligence (CTI) technologies play a crucial role throughout every stage of the CTI life cycle. This includes establishing clear goals and objectives, gathering and processing intelligence from diverse sources, analyzing the information, and distributing actionable insights to relevant stakeholders across the organization. Continuous feedback is also integrated to refine and enhance the overall process. By supporting ongoing security investigations and helping to prevent future incidents, these solutions enable organizations to prioritize and strengthen their infrastructure. While CTI technologies are most often delivered as cloud-based platforms, they are also available in “as-a-service” models.

Mandatory Features

The mandatory features for technologies in this market include:

- **Indicators of compromise (IoCs) and enrichments:** Provide comprehensive coverage of IoCs (e.g., IP addresses, URLs, domains, file hashes) with maliciousness/suspiciousness ratings, along with out-of-the-box enrichments such as geolocation information, registration data and TTP enrichment.
- **Vulnerability/exposure intelligence:** Tailored intelligence for vulnerability and exposure prioritization, highlighting actively exploited vulnerabilities and associated IoCs, TTPs and threat actor details.
- **Digital risk protection (DRP) monitoring:** Provide monitoring and alerting for common DRP use cases, such as deep web and dark web coverage, domain abuse, brand protection, third-party risk, social media monitoring, and geopolitical/physical security monitoring.
- **Integration and sharing:** Provide out-of-the-box, machine-to-machine, integrations (JSON, APIs, STIX/TAXII) for pushing and pulling intelligence artifacts across solutions, with capabilities for automatic sharing with private or public communities (e.g., ISACs).
- **User portal and analysis:** An interactive portal offering contextualized dashboards, configurable alerting, search features and built-in analysis functionalities.
- **Reporting:** Delivery of finished intelligence reports (e.g., technical/tactical, operational, strategic).

Common Features

The common features for this market include:

- **External telemetry enrichment:** External network telemetry/signal enrichments, such as passive DNS, sinkhole traffic and global-sensor-network telemetry.
- **External attack surface:** The ability to discover or ingest external attack surface data or digital asset information for the purposes of filtering or curating organization-specific risk insights.
- **Advanced DRP use cases:** Monitoring and alerting coverage across social media networks, messaging/collaboration platforms, news sites, and generally the open internet for mis/disinformation, deepfakes or sentiment analysis.
- **Preemptive rule generation:** Automatically generate rules and syntax for monitoring or enforcement in security products, including but not limited to security information and event management (SIEM) systems, firewalls, intrusion prevention and detection systems (IPDS) or endpoint detection and response (EDR).
- **Malware analysis capabilities:** Support for both static and dynamic malware analysis through sandboxing, enabling detailed examination of suspicious files and executables to identify behaviors, extract IoCs and assess potential threats in a controlled environment.
- **Vendor support services:** Vendor-provided investigation support options, including ad hoc requests for information, longer-term analysis, recurring analyst augmentation and takedown services (e.g., removing illicit domains/websites and hijacked accounts).

Magic Quadrant

Figure 1: Magic Quadrant for Cyberthreat Intelligence Technologies

Gartner

Vendor Strengths and Cautions

Axur

Axur is a Niche Player in this Magic Quadrant. Its AI-powered Axur Platform unifies cyberthreat intelligence, digital risk protection and external attack surface monitoring. The platform consolidates telemetry from surface, deep and dark web sources with AI-driven enrichment to identify brand abuse, credential leaks, impersonation, scams and infrastructure risks. Axur primarily supports enterprises in sectors with high exposure to fraud, digital impersonation and online brand misuse, including financial services and e-commerce. Its unified data lake enables correlation of large-scale external signals to organizational assets and industry context.

Axur offers standardized workflows, automated enrichment pipelines and cloud-native service delivery. The company supports integrations such as REST API, webhooks and STIX/TAXII for SOC, CTI and incident response teams. Automated takedown operations are embedded directly into the platform, reducing manual effort for security teams. The platform continuously ingests millions of new websites per day and normalizes threat, exposure and brand intelligence.

The roadmap emphasizes predictive analytics, expanded collection depth, multimodal detection for brand impersonation and agent-assisted takedown workflows. Its long-term direction focuses on AI-driven contextual analysis and the consolidation of external risk functions into a single operational system aligned with threat exposure management.

Strengths

- **Fraud and brand abuse specialization:** Axur offers deep expertise in financial services and e-commerce fraud, combining sector-aware risk scoring with automated takedown workflows. AI-driven pipelines detect behavior-based anomalies and create visualizations of sector-specific threats that bypass traditional text- or indicator-based methods.
- **Privacy-by-design response:** Axur's fraud-centric model prioritizes rapid removal of malicious content while minimizing retention of personal data. Privacy-by-design workflows limit downstream exposure but still support brand protection and fraud response in highly regulated industries.
- **Visual-first AI detection:** Axur's proprietary multimodal AI, including a vision-language model, identifies brand abuse even when visual and textual cues are intentionally removed. Agentic automation validates takedown enforceability, executes notices and escalates responses autonomously for accelerated mitigation.

Cautions

- **Missing analyst tools:** Axur provides no browser extension, mobile app or automated SIEM/EDR rule generation, which creates gaps where analysts expect in-context tooling. This limits Axur's ability to support investigation, enrichment and response directly at the point of analyst workflow.
- **Constrained commercial scale:** Axur's smaller customer base, revenue and growth rate may slow its ability to advance innovation or broaden capabilities at the same pace as larger vendors. This could result in more gradual product evolution and

ecosystem expansion, which buyers should consider when evaluating long-term alignment.

- **Regional concentration:** The customer base is primarily located in Latin America, raising questions about operational experience across diverse global markets and indicating limited commercial traction in regions where many enterprise buyers expect proven deployments.

Bitsight

Bitsight is a Visionary in this Magic Quadrant. Its threat intelligence platform combines dark web, surface web and sector-aligned intelligence with AI-powered enrichment and analytical workflows. The platform is greatly improved by the recent acquisition of Cybersixgill, expanding dark web and adversary intelligence capabilities. Bitsight primarily serves enterprise and public-sector organizations seeking continuous understanding of adversary behavior, ransomware activity, vulnerabilities and third-party risk.

The platform integrates with SIEM, SOAR, TIPs, identity tools, EDR/XDR, cloud, case management and data-marketplace environments. Delivery options include SaaS, on-premises, stand-alone modules and managed services, supporting diverse operational and regulatory requirements. Capabilities within IQ, Bitsight's GenAI Engine, generate summaries, classification, and tagging and prioritization across collected intelligence, while dashboards, sector mapping and news feeds deliver role-aligned visibility. Continuous normalization and enrichment pipelines process intelligence across sectors, geographies and threat categories.

The roadmap emphasizes predictive intelligence, expanded automation and deeper AI-driven contextualization across exposure intelligence, ransomware and sector modules. Long-term priorities include enhanced correlation between threat, exposure and environmental context, greater reporting automation and continued unification of intelligence use cases across vulnerability, incident response and third-party ecosystems.

Strengths

- **Roadmap discipline:** Bitsight maintains a clearly articulated roadmap with commitments around third-party intelligence fusion, geopolitical insight, AI-driven analysis and continuous threat exposure management alignment. Frequent

incremental releases paired with quarterly strategic updates demonstrate sustained execution on both innovation themes and foundational platform improvements.

- **Privacy controls:** Bitsight demonstrates maturity in privacy compliance with annual audits aligned to major regulation frameworks. The company has well-documented processes for data minimization, user consent, data retention and cross-border data transfers, with specific controls and retention policies in place.
- **Transparent pricing:** Bitsight's modular pricing model offers predictable list pricing for user access, API consumption and add-on intelligence modules. Presales engagement reinforces transparency through tailored demonstrations and high-touch onboarding. Bitsight uses a mix of direct sales and partners to support enterprise customers and broaden its market reach.

Cautions

- **Brand intelligence maturity:** Bitsight's brand intelligence is less mature than established vendors and differentiation relies on successful integration of Cybersixgill's dark web and adversary intelligence into the broader platform. Ongoing integration introduces near-term variability in feature depth, coverage consistency and user experience as the combined stack matures.
- **Commercial scale:** Bitsight's revenue profile and expansion rate place it below market leaders. Slower expansion may impact long-term resourcing or pace of capability advancement. Procurement teams should validate investment prioritization and product-line stability (e.g., product updates, roadmap execution) across future cycles.
- **Proof-of-concept consistency:** Bitsight's presales engagement is high-touch but can be improved with standardized POC success criteria and formal documentation. This inconsistency may introduce variability in how potential buyers assess real-world value, places greater dependence on individual solution engineers and may complicate objective comparisons with competing vendors.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant. CrowdStrike Falcon Adversary Intelligence integrates adversary tracking, malware intelligence, infrastructure analysis and digital risk monitoring with broad enrichment capabilities. The company supports global enterprises across regulated sectors and high-value industries that require real-

time adversary context and continuous external visibility. The platform combines Falcon telemetry, dark web intelligence, human-led investigations and finished reporting into a single operational model. Intelligence is sourced from the Falcon platform, validated underground communities, malware repositories, credential networks and incident response engagements to align external threat behavior with sectors, geographies and technology stacks.

CrowdStrike offers platform integrations across SIEM, SOAR, XDR, case management and asset management and inventory systems, with intelligence delivered natively in the Falcon platform and through APIs, marketplaces and partner workflows, supporting SOC, CTI and threat hunting teams. A Chrome extension provides in-page contextual enrichment, while agentic workflows automate summarization, hunting queries and technical analysis. Platform scalability is supported by trillions of daily telemetry events, proprietary infrastructure tracking and analytic validation for accuracy and relevance.

The roadmap emphasizes AI-agent intelligence delivery, autonomous threat hunting, expanded public-data coverage, enhanced infrastructure correlation and integrated remediation logic. Long-term direction centers on delivering intelligence at the point of decision making, strengthening security architecture analytics and unifying real-time intelligence with exposure and detection workflows across the Falcon ecosystem.

Strengths

- **Intelligence expertise:** CrowdStrike's intelligence division includes reverse engineers, human intelligence collectors, malware analysts and collection engineers, blending human-led and machine-scale intelligence for custom adversary insights, infrastructure correlation and high-fidelity threat reporting at a level most vendors cannot match.

- **Integration ecosystem:** The platform supports broad integrations across SIEM, SOAR, cloud, SASE, email security and intelligence platforms with validated, production-grade connectors. This versatility allows organizations of any size to adopt and scale threat intelligence within existing environments without disruption.

- **Privacy governance:** CrowdStrike maintains a mature privacy and data-protection program with a dedicated privacy team, documented controls and a three-lines-of-defense governance model. Although its use of legitimate interest for certain tradecraft activities requires continual oversight, the company's approach is

reinforced by high-assurance certifications and demonstrates strong privacy governance.

Cautions

- **Pricing complexity:** CrowdStrike uses an endpoint-based or employee-based pricing model with multiple tiers, making total cost of ownership variable. Threat intel capabilities are often intertwined with the broader Falcon platform, which may require an integration for organizations seeking a stand-alone CTI solution.
- **Regional revenue concentration:** Despite a strong global presence, most of CrowdStrike's intelligence and digital risk protection revenue is concentrated in North America, with significantly lower contributions from Asia/Pacific and Latin America. Some regions may receive lighter investment where customer presence remains comparatively small, relative to other vendors.
- **Channel strategy variability:** CrowdStrike's revenue mix shows strong dependence on existing products, and channel and services partners, which introduces variability in customer experience, deal orchestration quality and postsale alignment across regions. This structure presents the possibility of channel conflict and consistency, especially as its internal sales force expands globally.

CTM360

CTM360 is a Niche Player in this Magic Quadrant. Its Digital Risk Protection stack consolidates EASM, DRPS and CTI into a unified cloud-native environment. The platform integrates proprietary datasets, surface and dark web visibility, global domain and infrastructure telemetry, and fraud or impersonation intelligence to deliver continuous discovery and preemptive detection. CTM360 primarily serves regulated industries, national CERTs, financial institutions and critical infrastructure sectors, including oil and gas, aviation, healthcare, and education. Sector profiles are built from more than 1.4 million profiled organizations.

Integrations span internal modules, SIEM, SOAR, cloud providers, collaboration tools and enforcement partners. SaaS-only delivery emphasizes rapid onboarding with premapped organizations and automated enrichment, investigation and response workflows. Automated detection is combined with analyst validation using AI-driven similarity analysis, campaign tagging and rule-based checks. The platform also provides takedown

support, incident tracking and approvals, and cross-module correlation through internal and external integrations. Data normalization and sector tagging support SOC, fraud and intelligence teams. Mobile access is offered through dedicated mobile applications for awareness and incident review.

The roadmap emphasizes AI-driven pattern recognition, cross-module correlation, next best action recommendations and increased automation for escalation and takedown workflows. Long-term direction focuses on delivering a converged external exposure management model unifying DRPS, CTI and EASM into a single risk-based operational framework that supports end-to-end prioritization, automation and remediation.

Strengths

- **Scam life cycle analysis:** The platform offers agentic automation through CTM360 WebHunt, scam-kit clustering, similarity analytics and CTM360 Scam Navigator for depth in detecting infrastructure reuse and synthetic media scams. Its focus on regulated industries and national-level sector mapping reinforces differentiated value.
- **Purpose-built EASM:** The platform integrates DNS, WHOIS, certificate transparency, IP/ASN intelligence, registrar telemetry and major cloud provider data to deliver continuous, high-fidelity discovery and attribution of internet-facing digital assets.
- **Agile release model:** CTM360 delivers frequent feature enhancements and annual product updates through a continuous agile release model driven by threat observations and customer feedback to ensure rapid adaptation to evolving industry requirements.

Cautions

- **Front-end innovation gaps:** CTM360 lacks a browser-based extension, which limits real-time, in-context threat enrichment and analyst workflows at the point of investigation. The absence of awarded patents leaves core capabilities without formal intellectual property protection, reducing defensible differentiation and increasing the risk of replication by competitors.
- **Limited market traction:** The company has a relatively small customer footprint, annual recurring revenue and modest year-over-year growth compared to market average. This suggests limited market traction and scale, which may impact its ability to invest in innovation or expand reach.

- **Team size constraints:** CTM360 operates with a relatively small analyst and support team for a global provider, which may limit its ability to deliver high-touch investigations or sustained local coverage across major regions. This lean structure signals greater reliance on automation to compensate for gaps in human capacity.

Cyble

Cyble is a Challenger in this Magic Quadrant. Its AI-native Cyble Vision intelligence platform integrates surface, deep and dark web telemetry with proprietary sensor networks, malware intelligence, fraud ecosystem monitoring, exposure intelligence and external attack surface management. The platform supports organizations across finance, energy, telecom, government and other sectors that require visibility into ransomware activity, identity compromise, brand exposure and infrastructure-level threats. Cyble processes a large and continuously expanding ecosystem of cybercrime channels, dark web telemetry and internet-scale web content, enabling the continuous monitoring of stealer logs, compromised payment cards, mobile app stores and emerging cybercriminal communities. AI pipelines enrich collected intelligence through entity extraction, attribution, clustering and TTP mapping aligned to MITRE.

Cyble offers SaaS-only delivery and expanding integrations across SIEM, SOAR, TIP, cloud and ITSM platforms. Automated pipelines support normalization, contextualization and alerting with Cyble Blaze AI, an embedded AI-native reasoning and workflow capability that augments analyst workflows through summarization, prioritization, confidence scoring, false-positive reduction and guided investigative support. Cyble provides a browser extension for IOC extraction and multitenant capabilities for MSSPs and regulated industries seeking scalable intelligence operations.

The roadmap emphasizes enhanced contextualized intelligence, expanded brand and mobile app monitoring, agentic takedown workflows, mailbox-as-intel-source capabilities, sector-specific investigation tooling and deeper enterprise integrations. Long-term direction prioritizes AI-driven analysis, threat actor correlation and fusion of cyber, brand, fraud and geopolitical intelligence into a converged threat exposure model.

Strengths

- **Takedown capability:** Cyble demonstrates strong end-to-end takedown execution for phishing, impersonation, rogue apps and brand abuse, backed by mature workflows, automation and dedicated response operations, emphasizing actionability over passive intelligence.

- **Multidisciplinary coverage:** Cyble delivers an integrated SaaS platform combining native CTI, DRP, EASM, malware analysis and vulnerability intelligence for cohesive workflows that reduce operational fragmentation. Proprietary telemetry, sensor-derived signals and in-house research are converted directly into analytics, supporting a smoother transition from detection to response.
- **Global go-to-market strategy:** Cyble has established sales and marketing operations across all major geographic regions with coordinated demand generation, field marketing, channel partner enablement, analyst engagement and direct sales activities. This global reach ensures customers receive accessible, localized engagement and support.

Cautions

- **Modest revenue:** Cyble's annual recurring revenue remains comparatively modest compared to leading peers, reflecting a smaller market footprint and limited scale. While growth momentum is evident, the company's current position may constrain long-term investment opportunities for expansion, ecosystem depth or sustained innovation.
- **Integration depth:** Native out-of-the-box integrations across SIEM, SOAR, TIP, cloud and ITSM are limited. Many integrations rely on generic APIs or custom development rather than ready-made connectors, increasing operational lift, an area of product strategy that trails Leaders and influences its position as a Challenger.
- **Shorter product tenure:** Cyble's flagship AI-native platform was established in 2020, placing it behind legacy competitors with longer operating histories. For some buyers, this may introduce additional due diligence around scalability, roadmap durability, and execution consistency when compared with vendors that have supported complex enterprise requirements over a longer period.

CYFIRMA

CYFIRMA is a Visionary in this Magic Quadrant. Its integrated external threat and exposure intelligence platform, DeCYFIR by CYFIRMA, unifies nine intelligence pillars, including attack surface discovery, vulnerability analysis, brand protection, digital risk monitoring, third-party oversight, situational awareness, predictive intelligence, adaptive training and deception. The platform serves enterprises, governments, critical

infrastructure operators and MSSPs that require early visibility into adversary intent, reconnaissance activity, credential abuse, impersonation and geopolitical risk. DeCYFIR correlates structured and unstructured telemetry from surface, social, deep and dark web ecosystems with identity, infrastructure and sector-aligned risk indicators to deliver actionable, attribution-driven insights.

CYFIRMA supports integrations across SIEM, SOAR, CSPM, EDR/XDR, ITSM, NDR, data analytics, governance and fraud platforms. Its cloud-native architecture enables SaaS, hybrid or private cloud deployment for regulated and air-gapped environments. The platform standardizes enrichment, prioritization, escalation and personalization of intelligence within existing workflows, reducing noise and increasing analytic precision. CYFIRMA's Ask DeCYFIR AI agent provides natural language access to correlated intelligence while continuous monitoring links external exposures to internal asset inventories and operational processes.

The roadmap emphasizes DeCYFIR 4.0 with enhanced risk remediation sequencing, sector-specific deception engines, threat-adaptive awareness, AI attack surface defense and upgraded deepfake detection. Long-term direction centers on adversary-driven intelligence, automated contextualization and convergence of external risk domains into its unified extract, transform, load, monitor (ETLM) model as an operational layer.

Strengths

- **Adversary-weighted intelligence:** CYFIRMA's adversary-centric, sector-weighted intelligence model aligns threats to business processes, regulatory exposure and monetization pathways rather than generic indicators. The ETLM framework maps attacker intent, exploit feasibility, and sector sensitivity into predictive escalation and enforcement workflows across cyber, fraud and brand domains.
- **Risk convergence platform:** DeCYFIR converges CTI, identity abuse, fraud operations, brand exploitation and supply chain exposure into a single adversary-centric control plane that mirrors real attacker workflows. Native correlation enables coordinated detection, prioritization and enforcement across traditionally siloed risk functions.
- **Execution-grade intelligence:** The platform translates intelligence directly into enforcement actions across security, identity, fraud, brand and third-party workflows using native orchestration and playbooks, minimizing manual handoffs for containment.

Cautions

- **Scale and ecosystem maturity:** CYFIRMA demonstrates strong innovation, but its long-term stability is more dependent on achieving greater scale, partner support and broader global adoption than larger, more established competitors. Buyers with lower risk tolerance may want additional assurance around the vendor's ability to maintain continuity, expand capacity and sustain operational resilience.
- **Market clarity:** Product evolution is strategically well-defined, but buyer-facing articulation of changes, integrations and roadmap outcomes can lag technical substance, creating friction for customers who prioritize clearly packaged capabilities.
- **Geographic imbalance:** CYFIRMA's customer base is heavily concentrated in Asia/Pacific, with limited adoption in other major enterprise markets. This may reduce the availability of localized expertise, in-region support and relevant proof points for buyers operating outside APAC, making it more challenging for customers to assess capability fit or depend on in-region support.

Flare

Flare is a Niche Player in this Magic Quadrant. Its cloud-based, agentless Threat Exposure Management platform focuses on identifying illicit activity across dark web forums, marketplaces, Telegram channels, paste sites, breach repositories, stealer logs and open web sources. The platform serves security teams seeking rapid visibility into identity exposures, ransomware activity, account takeover risk and operationally relevant threat signals. Flare enables organizations to define their own business context through configurable identifiers such as domains, brands, applications and executive identities, so sector relevance emerges organically from customer-specific assets.

Machine learning classifies relevance across large-scale criminal ecosystems and provides AI-generated summaries to accelerate analyst investigations. Automated deduplication, noise reduction and contextual enrichment support SOC, CTI, fraud and incident response teams. The platform emphasizes fast onboarding, continuous monitoring and dashboards for investigation and reporting. Its focus on identity exposure data offers high signal clarity without requiring on-premises infrastructure or managed service dependencies.

The roadmap centers on scaling with AI-enabled investigations, enhanced reporting automation and deepening context extraction from illicit ecosystems. Long-term

direction prioritizes analyst augmentation over autonomy with human-validated intelligence and accelerated exposure triage.

Strengths

- **Identity-centric intelligence:** Flare focuses on identity exposure management using customer-defined identifiers like Microsoft Entra ID attributes, credentials or sessions to drive high relevance and practical remediation outcomes. This model differentiates Flare by delivering actionable intelligence for rapid response.
- **Growth momentum:** Flare reports year-over-year revenue growth, signaling strong market traction. The fusion of CTI and DRPS simplifies adoption for customers who want fewer platforms and strong external-threat signal consolidation.
- **AI and privacy controls:** The platform implements encryption at rest, point-in-time database recovery and data minimization by design. Customers can disable AI data sharing entirely via feature controls, supporting privacy needs for regulated or risk-averse teams.

Cautions

- **Integration breadth:** Flare offers fewer out-of-the-box integrations than competitors, which may constrain product fit or time-to-value for larger or more complex environments that expect broader plug-and-play coverage.
- **Limited automation:** AI is used in a supportive, not decisional, role and is primarily focused on contextual summarization, relevance scoring, noise reduction and analyst-driven interpretation. The platform lacks predictive analytics and agentic automation, with limited closed-loop automation, including IOC-to-rule generation, placing Flare behind more automated platforms.
- **Support depth:** Flare's lean support model may constrain responsiveness and scalability as deployments grow, compared with peers offering broader, regionally distributed support operations.

Flashpoint

Flashpoint is a Challenger in this Magic Quadrant. Its cloud-native intelligence platform centers on primary-source collection from closed, illicit and high-signal environments, integrating underground forums, encrypted messaging channels, criminal marketplaces,

fraud communities, ransomware leak sites and curated OSINT into a unified analytical workflow. The company serves enterprises, government agencies and regulated sectors that require visibility into cybercrime, fraud, identity exposure, geopolitical risks and operational threat activity. Flashpoint's intelligence model emphasizes authenticated access into hard-to-reach communities and correlation of threat actor behavior, infrastructure, vulnerabilities and victimology across multilingual ecosystems.

Its SaaS platform delivers centralized intelligence, automated enrichment, structured reporting and analyst engagement with tailored reporting, RFIs and proactive threat actor engagement. Normalized pipelines include OCR, translation, clustering and entity extraction to reduce noise and accelerate triage. Flashpoint prioritizes integration depth and workflow alignment validated by customer feedback. The acquisition of VulnDB by Risk Based Security elevates its portfolio with market-leading vulnerability intelligence, supporting risk prioritization and remediation.

The roadmap focuses on predictive and autonomous operations, including agentic AI capabilities, expanded brand and fraud intelligence, adversary entity exploration, breach intelligence and automated takedown workflows. Long-term direction prioritizes consolidation of cross-domain intelligence and improved actionability through enriched context, collaborative investigation and continuous alignment to evolving customer requirements.

Strengths

- **Primary source access:** Analyst-managed access to closed criminal forums, underground markets and encrypted communities supports collection of original intelligence across cybercrime, fraud and extortion ecosystems. This approach enables earlier and higher-confidence threat intelligence than solutions relying primarily on open-source collection.
- **Vulnerability analytics:** Independent CVSS scoring from VulnDB across multiple versions, including pre-NVD and non-CVE vulnerabilities, combines a proprietary exploited vulnerability catalog, EPSS modeling for vulnerabilities, supplemental ransomware likelihood and social risk signals. These capabilities support more threat-informed vulnerability prioritization than severity-only approaches.
- **Operational workflows:** The platform unifies case management, advanced image and geospatial enrichment, managed attribution and takedown operations within a

consolidated investigation workflow. Strong SIEM and SOAR integrations plus Flashpoint Firehose streaming API architecture enable operational use at scale.

Cautions

- **Automation gaps:** Flashpoint lacks proprietary external attack surface scanning or out-of-the-box EDR connectors, relying instead on SOAR or TIP integrations. IOC life cycle management is not fully automated, and mobile app monitoring is intel-driven without static or dynamic code analysis. The platform also excludes passive DNS or sinkhole data in its detection methodology.
- **Geographic concentration:** Customer base and operations remain North America-centric with a comparatively lean total headcount, which may affect follow-the-sun coverage and regional depth versus larger, globally distributed vendors. This more limited footprint reduces maturity in geographic strategy.
- **Integration breadth:** Although Flashpoint's roadmap is presented at a high level, its integration catalog is modest. Some cloud or network uses require middleware or customer-built solutions such as AWS Lambda for IOC lists while AEV (formerly BAS) has no native out-of-the-box integrations. These integration gaps reflect product-strategy areas still developing relative to market Leaders in this Magic Quadrant.

Google

Google is a Leader in this Magic Quadrant. Its unified threat intelligence platform integrates global infrastructure telemetry, community-driven intelligence from VirusTotal and frontline expertise from Mandiant Threat Intelligence into a unified operational ecosystem. The platform serves enterprises, government agencies and cloud-forward organizations that require large-scale visibility into malware, phishing, adversary campaigns and sector-specific threat activity. Google aggregates telemetry from billions of threat signals, supported by VirusTotal's open contributor community and deep file and URL-analysis pipelines. This multisignal model enables broad detection of malicious infrastructure, high-fidelity observables and early insight into commoditized and targeted attack techniques.

Google's cloud-native platform leverages REST APIs, STIX/TAXII 2.1 feeds and Model Context Protocol to support agentic AI workflows. A browser extension provides immediate enrichment, IOC extraction and pivot paths into Google Threat Intelligence

for deeper investigation. The platform also operates as a foundational layer within Google's broader security ecosystem, enhancing Google Workspace, Chrome, Google Security Operations, Google Cloud Security Command Center, and other Google Cloud Security solutions through embedded threat context and protection signals.

The roadmap emphasizes leading agentic intelligence experiences, adversary campaign mapping as well as dark web and brand intelligence enhanced industry- and country-threat profiling, and automated rule creation integrated with Google SecOps. The acquisition of Wiz strengthens the long-term direction, which is focused on AI-guided operationalization, improved detection coverage and a converged intelligence fabric spanning cloud, endpoint and enterprise security platforms.

Strengths

- **Internet-scale telemetry:** Google brings visibility through VirusTotal, Mandiant and Google Cloud with over two decades of frontline incident response data and global infrastructure that no pure-play threat intelligence vendor can replicate. This supports broad coverage across web, malware, infrastructure and threat actors with both historical and real-time depth.
- **Agentic AI and detection:** Google Threat Intelligence's agentic threat intelligence capabilities go beyond generic AI assistant use cases by analyzing malware reverse-engineering output, extracting TTPs, simulating threat actor behavior, identifying detection gaps and automatically generating and pushing rules, especially within Google SecOps.
- **Analyst-workflow acceleration:** The platform's browser extension offers automatic IOC highlighting on any webpage, hover-based verdicts, one-click pivots, private collections, graph visualization and immediate sandboxing across more than 70 malware detection engines and 20 sandboxes.

Cautions

- **Ecosystem centricity:** While Google Threat Intelligence integrates broadly, the most advanced automation such as agentic rule generation, closed-loop policy enforcement and behavioral simulation are optimized for Google SecOps. Non-Google SIEM or EDR users may not realize the same end-to-end value.
- **Complexity for smaller teams:** The platform's enterprise-grade complexity and tiered pricing may be challenging for smaller teams. Premium capabilities like private

scanning, advanced AI or automation can accumulate quickly while teams with lower AI or CTI maturity may struggle to operationalize the full stack efficiently.

- **Workflow gaps:** There is no native mobile application (only mobile-optimized web interface) and some tasks require copy-paste on mobile. Certain capabilities such as full agentic workflows or deep automation remain platform-centric rather than universally embedded across all access points.

Group-IB

Group-IB is a Leader in this Magic Quadrant. Its unified threat intelligence and digital risk platform integrates adversary tracking, malware intelligence, ransomware ecosystem visibility, brand protection, fraud intelligence, external attack surface monitoring and cloud security posture management into a consolidated operational environment. Group-IB serves enterprises, financial institutions, telecommunications providers, law enforcement agencies and government entities that require deep visibility into threat actors, infrastructure reuse and campaign-level behaviors. The platform leverages proprietary underground intelligence, malware analysis, darknet monitoring, phishing detection and infrastructure correlation (enriched by telemetry from XDR deployments, antifraud solutions, active incident response and global law enforcement cybercrime partnerships) to deliver high-fidelity insights grounded in real-world attacker behavior.

Group-IB supports cloud-based deployment as well as on-premises or isolated deployments for regulated sectors. A browser extension and mobile app streamline enrichment and alerting workflows. AI capabilities include an LLM-based orchestrator for correlation, anomaly detection, pattern recognition, signature generation and remediation guidance as well as autonomous, real-time production of finished cyberthreat intelligence through agentic research workflows. Scalable APIs, custom integrations and an evidence-driven data lake enable operational alignment across SOC, CTI, fraud and incident response teams.

The roadmap emphasizes expanded AI orchestration, advanced research modes, integrated hunt and response automation, and deeper unified intelligence across Group-IB's risk platform. Long-term direction focuses on tighter convergence of detection, investigation, fraud and intelligence workflows into a unified prediction-first ecosystem.

Strengths

- **Verticalized intelligence:** Group-IB is especially strong in financial services, telecommunications, and government and law enforcement sectors by combining dark web and closed-group access, incident response validation, proprietary fraud telemetry, and unique capabilities like BGP threat monitoring and a cyberfraud fusion model.
- **Platform breadth and cost:** The platform functions as a unified intelligence data lake across threat intelligence, fraud, managed XDR, sandboxing and investigations, supporting integrations across SIEM, SOAR, TIP, cloud and firewalls. Unlimited users, APIs, hunting rules and takedowns provide cost predictability for large teams.
- **Innovation trajectory:** Group-IB's detailed short-term and long-term roadmap clearly articulates a shift from detection to prediction-first defense, including attack-path modeling, predictive fraud disruption through Cyber Fraud Fusion and unified incident management across TI, ASM, DRP and CSPM.

Cautions

- **Limited North American presence:** Although operating globally, Group-IB has comparatively small market penetration in North America, creating a meaningful gap given the region's influence in cybersecurity purchasing, ecosystem expectations and enterprise-level peer validation.
- **AI availability:** Advanced predictive AI capabilities remain future deliverables rather than fully available features. The current platform relies largely on rules-based logic, analyst-driven workflows and reactive enrichment, placing it short of the more autonomous experience outlined in its long-term strategy.
- **Operational complexity:** The platform is best suited to organizations with mature threat intelligence teams. Organizations with less experience may require additional onboarding, process definition and tuning to fully realize value, though vendor guidance and structured workflows can help mitigate this learning curve.

Intel 471

Intel 471 is a Niche Player in this Magic Quadrant. Its Verity471 cyber intelligence platform delivers deep underground access, as well as malware, hunt and geopolitical intelligence, blending human-curated intelligence with automated collection across a broad spectrum of threat vectors and sources.

Additionally, its cyberthreat exposure bundle delivers a unified third-party risk, attack surface management and brand protection offering to power proactive, intelligence-led security programs. The platform serves enterprises, government agencies and law enforcement organizations requiring validated insight into adversary tooling, preattack planning, credential compromise and malware infrastructure activity. Intelligence combines closed-forum visibility, instant messaging channels, patented malware emulation systems and structured reporting to deliver behavior-driven intelligence across adversary ecosystems. Intel 471 emphasizes persistent access, linguistic expertise and contextual interpretation for relevance and accuracy.

The cloud-based platform offers API-driven integrations, and semiautomated and automated rules as well as indicator generation across malware, infrastructure, vulnerabilities and credentials. Its patented, automated Malware Intelligence monitoring and data extraction identifies active C2 infrastructure, obtains commands, and publishes normalized indicators and events consumable via portal or security tooling. Customer feedback drives a downstream operationalization strategy with alerts integrated into tools like Slack, Teams and ServiceNow rather than mobile or browser extensions. The platform supports intelligence-driven threat hunting, YARA rules, Snort signatures and broad XDR or SIEM detection content.

The roadmap includes an agentic AI system to enhance data accessibility, correlation and usability across exposure, intelligence and hunt modes. Long-term direction emphasizes scalable underground visibility, automated malware-driven intelligence and actionable content to accelerate analyst workflows.

Strengths

- **Human-led adversary intelligence:** Intel 471's core differentiation is high-fidelity HUMINT inside closed cybercrime ecosystems validated by experienced analysts rather than heavy automation alone. This yields strong credibility in threat actor profiling. Infrastructure context such as bulletproof hosting and C2, and underground tradecraft is valued by sophisticated teams.
- **Global footprint:** Few vendors achieve Intel 471's near-parity revenue and support split between North America and EMEA, enabling effective follow-the-sun operations across the two largest security markets. This reflects a mature, intentional international strategy.

- **Direct sales traction:** Intel 471's sales and product teams demonstrate strong ability to identify buyer challenges and align solution configurations to those needs. Their high POC-to-win conversion rate reflects how effectively they translate customer requirements into tailored workflows and service plans, enabling experienced CTI buyers to quickly understand and operationalize the platform's value.

Cautions

- **Focused automation:** Intel 471 prioritizes human analysis, specialized insights and sensitive source protection over the production of end-to-end automation and advanced AI workflows; foundational AI capabilities exist for intelligence summarization and report generation. A suite of out-of-the-box API-driven integrations are available, but the breadth of connectors is less than industry peers.
- **Scaling risk**: Intel 471 runs a high-expertise, low-headcount model, which supports quality but also introduces risk in scalability, coverage expansion and sustained velocity as customer demand grows.
- **Analyst experience gaps**: Intel 471 does not offer a browser extension, mobile application or agentic AI-driven workflows, instead prioritizes depth in downstream API workflows. While integrations are available; some are custom-built rather than turnkey, which can reduce day-to-day analyst convenience compared with vendors that emphasize a variety of analyst experiences.

KELA

KELA is a Niche Player in this Magic Quadrant. Its cybercrime-focused threat intelligence platform integrates deep underground visibility, real-time identity compromise detection, ransomware ecosystem monitoring and adversary infrastructure tracking. The company serves enterprises, financial institutions, government agencies and critical infrastructure providers needing early insight into access brokers, stealer log activity, sector targeting and malicious infrastructure reuse. Collections span hard-to-reach criminal forums, ransomware leak sites, access-as-a-service markets, botnet logs, closed messaging channels, and decentralized darknet services enriched with multilingual processing and analyst validation for high-confidence intelligence.

KELA offers integrations across SIEM, SOAR and collaboration platforms with data exchange via REST APIs, STIX/TAXII feeds, webhooks and a Splunk app for SOC

workflows. Analytic modules such as Threat Landscape, Investigate, Identity Guard and Brand Control correlate compromised identities, exposed assets, infrastructure clusters and threat actor behaviors, supporting sector-specific dashboards and investigations. AI-driven automations validate compromised accounts, classify incidents and generate executive-ready reporting with automated response actions integrating with Active Directory for account suspension or session termination when high-risk exposures are identified.

The roadmap emphasizes expanded automation, deeper analytics on underground ecosystems, improved identity correlation and continued scalability across enterprise and government environments. Long-term direction prioritizes unifying cybercrime intelligence, exposure monitoring and automated response within a converged external threat operations model.

Strengths

- **Underground intelligence:** KELA gathers intelligence from hard-to-reach underground ecosystems, including ransomware groups, infostealer logs, botnet markets, closed messaging channels, leaked databases and network-access listings. This data is automatically enriched and analyst-validated for high-confidence results.
- **Malicious AI monitoring:** The company actively monitors the malicious AI ecosystem such as dark AI tools like WormGPT and FraudGPT, and tracks emerging jailbreak techniques used by cybercriminals to compromise AI systems. KELA's AiFort platform provides automated adversarial testing to identify vulnerabilities such as prompt injection and data leakage in GenAI applications.
- **Sector targeting insights:** KELA focuses on underground cybercrime economies by aligning industry intelligence with the ways access brokers, ransomware groups and fraud actors target different sectors. Sector exposure is mapped through compromised identities, network access listings and malware telemetry tied to industry-relevant attack paths.

Cautions

- **Geography imbalance:** KELA's commercial and staffing footprint is uneven across global regions with heaviest concentrations outside of North America, creating gaps in regional presence and local support.

- **Limited operational support:** The company's lean headcount means fewer analysts, engineers and customer-facing roles compared to larger vendors, which may impact scalability, support depth and product development speed.
- **Pricing transparency:** KELA's pricing model lacks a clear, standardized structure and can vary based on factors like deployment scope or feature mix, which may introduce uncertainty during procurement. This may make it more challenging for buyers to benchmark costs, evaluate total cost of ownership or move efficiently through internal approval processes.

NSFOCUS

NSFOCUS is a Visionary in this Magic Quadrant. Its threat intelligence platform unifies proprietary product telemetry, open-source intelligence, commercial feeds, dark web monitoring and advanced research from its global security laboratories. The platform serves enterprises, critical infrastructure operators and government organizations requiring region-specific intelligence, vulnerability insights, industry-aligned reporting, and comprehensive visibility into attacker behavior across Asia Pacific and global threat ecosystems. Intelligence sources include honeypots, incident response engagements, sandbox analysis, malware tracking, vulnerability research, and thousands of dark web, forum and social media sources.

NSFOCUS integrates with its own NDR, WAF, IPS/IDS, UTS, endpoint, SOC, SOAR, TVM, LLM and antifraud systems. External interoperability includes platforms such as Anomali, VirusTotal, Splunk, OpenCTI, Palo Alto, KINGSOFT and INCHTEK. Its browser extension enables automated IOC detection, risk scoring, context enrichment, workflow automation and AI-driven event summarization. The mobile application offers intelligence queries, vulnerability alerts and APT activity updates powered by NSFOCUS's proprietary large language model, optimized for a Chinese language security context. Deployment options include SaaS, cloud and fully on-premises models with offline package ingestion for restricted environments.

The roadmap emphasizes expanded AI-driven normalization, predictive analytics, automated attribution and dynamic report generation with agent-based workflows. Long-term direction focuses on deepening industry-specific intelligence, improving extraction accuracy, and integrating NSFGPT to enhance analyst decision making across intelligence production and operations.

Strengths

- **AI innovation:** NSFOCUS delivers an AI-powered browser extension that automatically highlights IOCs on webpages, enriches them in place, summarizes content, provides real-time risk scoring and allows analysts to take actions without leaving the tab. The company integrates NSFGPT AI models within its intelligence platform, offering advanced threat intelligence experiences.
- **Regional-context advantage:** NSFOCUS provides unique visibility into Chinese-language and APAC-origin adversaries, powered by its self-developed LLM tuned specifically for Chinese threat content. This supports superior extraction, interpretation and contextualization of region-specific malware families, APT behaviors, underground forums and sector-targeted campaigns.
- **Automated classification:** NSFOCUS applies LLM techniques to automatically categorize dark web, OSINT, social media and incident intelligence by industry, then pushes it into sector-specific queues, reducing manual triage. This automation delivers targeted industry-aligned insights beyond traditional manual curation.

Cautions

- **Global coverage imbalance:** NSFOCUS's footprint is heavily centered in APAC, which limits presence in other major regions. This may reduce effectiveness for organizations requiring strong local support and intelligence outside its primary market.
- **Ecosystem dependency:** Many capabilities function best when paired with NSFOCUS's own platforms, which may limit flexibility for organizations with heterogeneous security stacks or those seeking vendor-agnostic integrations.
- **Conservative release cadence:** The company operates on a traditionally structured release model, delivering major feature updates at a predictable but infrequent rhythm, which lags behind competitors leveraging continuous or high-velocity delivery for faster innovation.

Recorded Future

Recorded Future is a Leader in this Magic Quadrant. Its cloud-native threat intelligence platform is powered by Recorded Future Intelligence Graph, correlating entities, infrastructure, malware, vulnerabilities and threat actor activity at internet scale. The

company serves large global enterprises, government agencies and MSSPs needing continuous visibility across the threat landscape, brand, identity, third-party and attack surface risk. Recorded Future ingests intelligence from more than 1 million open web sources, dark web forums, ransomware sites, malware repositories, network telemetry, image datasets, malware analysis pipelines, customer security telemetry, and collective customer insights to produce contextualized intelligence aligned with organizations, sector and geopolitical priorities.

Integrations include SIEM, EDR, SOAR, firewall and cloud security platforms delivered via APIs, native connectors and content packages. The browser extension provides in-page IOC enrichment and risk scoring for domains, IPs, URLs, hashes and CVEs, while the mobile app supports push notifications, triage and AI sessions for conversational access to the Intelligence Graph. Insikt Group research-driven automated rule generation includes YARA, Sigma, Suricata or Snort, correlation rules, Nuclei templates and prevention blocklists with translation into platform-specific detection languages. Multitenant capabilities support large, distributed enterprises and MSSPs.

The roadmap emphasizes expanded AI-assisted reasoning, predictive analytics, automated report production and deeper convergence of identity, brand, third-party and attack surface intelligence. Long-term direction focuses on unifying customer-specific sources, external threat data, and internal enterprise telemetry to strengthen contextualized risk prioritization and accelerate response.

Strengths

- **Engineering depth:** Recorded Future operates at rare enterprise staffing scale with a massive engineering investment behind the Intelligence Graph, with more than 200 billion nodes over 15 years and petabytes of data. This enables continuous, high-volume, automated collection paired with multilingual analyst validation for tactical alerting and strategic reporting at global scale.

- **Industry-embedded intelligence:** Industry context is embedded directly into the Intelligence Graph, combining historical telemetry with public-private peer sharing and analyst-validated sector research. Formal partnerships with industry and government provide privileged sector-specific intelligence unavailable through generic commercial feeds.

- **Commercial maturity:** Recorded Future demonstrates strong commercial maturity through a long-standing market presence, a well-defined go-to-market model and

consistent enterprise adoption across regulated and global industries. It has established its brand with clients moving beyond early stage innovation into durable, scaled execution.

Cautions

- **Platform complexity:** Recorded Future's breadth comes with a large matrix of modules and tiers. Achieving full value often requires multiple add-ons, which can increase procurement complexity and total cost of ownership, especially for teams that grow beyond the entry-level Threat Intelligence Foundation package.
- **Geographic imbalance:** While Recorded Future has a global presence, its revenue and support remain heavily concentrated in North America and EMEA, with limited maturity in Latin America. Organizations that prioritize deep, localized expertise in emerging regions may find fewer resources or less coverage.
- **Automation depth:** Recorded Future excels at correlation and contextualization but places less emphasis on closed-loop agentic disruption, such as automated response execution and adaptive playbooks. Advanced intelligence often relies on downstream tools for response actions.

ReliaQuest

ReliaQuest is a Visionary in this Magic Quadrant. Its threat intelligence and digital risk protection capabilities are embedded within the ReliaQuest GreyMatter AI platform, integrating external intelligence, detections, exposure insights and response orchestration into a single operational model. The platform supports large organizations, managed security service providers, and globally dispersed security teams needing continuous visibility into dark web activity, exposed credentials, stealer-log data, ransomware signals and malicious infrastructure. Intelligence is aggregated from diverse dark and open web sources, enhanced by proprietary collection systems designed to uncover malicious indicators, infrastructure and threat behaviors. ReliaQuest complements this with human-led threat research across criminal forums and structured pipelines that is embedded into the platform to correlate indicators, assets, adversaries and vulnerabilities.

Integrations span SIEM, SOAR, EDR or XDR, data lakes and cloud environments. The GreyMatter AI Mobile App extends alerts, intelligence review and response actions to

mobile devices with biometric authentication, encrypted sessions and real-time notifications. Detection engineering is supported by GreyMatter Query Language, built on OCSF to abstract syntax across technologies. Automated rule creation, tuning, backtesting and false positive reduction streamline operational workloads. Agentic AI capabilities produce investigation writeups, summarize intelligence and drive autonomous analysis of alerts across integrated environments.

The roadmap emphasizes expanded multiagent detection engineering, deeper alignment between intelligence and exposure workflows, increased automation of detections and investigations, and broader support for heterogeneous enterprise environments. Long-term direction focuses on converging threat intelligence, detection and response into a unified operational ecosystem.

Strengths

- **AI-orchestrated decisioning:** ReliaQuest embeds agent-driven automation and AI-supported workflows directly into its unified platform, enabling analysts to move from intelligence discovery to investigation and response without switching tools. ReliaQuest's GreyMatter AI automated response playbooks and consolidation into a single operational environment position it ahead of competitors that rely on fragmented intelligence feeds and manual triage.

- **Integrated data fabric:** The integration strategy is anchored by architecture that allows detection logic, enrichment and response actions to be executed natively across a broad ecosystem of third-party security tools, eliminating the dependence on centralized data ingestion and reducing operational overhead. At-source detection design, combined with extensive support for open standards and APIs, positions GreyMatter AI as an orchestration layer.

- **Customer engagement:** ReliaQuest demonstrates effective commercial execution with a hands-on, direct-sales model that cultivates deep customer engagement and reinforces market traction. Balanced revenue across major Western regions signals mature go-to-market motion in North America and EMEA.

Cautions

- **Ecosystem lock-in:** Dependence on less common interfaces like GraphQL interface instead of OpenAPI or Swagger, and use of Intel Push rather than outbound TAXII, may create friction for organizations expecting open-standard interoperability. This may

hinder adoption in large enterprises seeking portability, vendor diversity and standards-aligned integrations.

- **Opaque pricing:** High-level pricing inputs are tied to broad deployment identifiers without accompanying packaging details, tiers or publicly accessible rate structures, leaving buyers with little clarity on total cost of ownership or comparative value. This may introduce friction in procurement cycles, forcing reliance on custom quotes.
- **Channel limitations:** Absence of a scalable channel strategy limits ReliaQuest's ability to localize go-to-market beyond core Western markets, potentially slowing entry into emerging regions or constraining competitiveness against vendors leveraging broad partner networks for global reach.

SOCRadar

SOCRadar is a Visionary in this Magic Quadrant. Its cloud-based agentic Extended Threat Intelligence (XTI) platform integrates digital risk protection, threat intelligence and attack surface monitoring into a unified operational system. The platform serves enterprises, MSSPs and government organizations requiring visibility across surface, deep, and dark web ecosystems, enriched with identity, brand, infrastructure and vulnerability intelligence. SOCRadar's collection model spans underground forums, marketplaces, ransomware leak sites, carding shops, credential databases, OSINT feeds, phishing repositories, exploit hubs, infrastructure scanners and government advisories, enabling broad coverage across cybercrime, fraud and exposure domains.

SOCRadar offers a cloud-native PaaS architecture with flexible deployment options, including SaaS, managed-service, hybrid and selective on-premises models for data sovereignty needs. Integrations via API, webhooks, and native connectors support SIEM, SOAR, EDR and ticketing tools. The mobile application provides real-time alarm notifications, asset monitoring, vulnerability tracking and incident review with SSO and biometric authentication. SOCRadar MCP Server and Copilot provide AI-driven insights, adversary attribution, alert prioritization, supply chain risk analysis and phishing detection through modular agent-based logic.

The roadmap emphasizes expanded AI tooling, enhanced multilingual contextualization, broader brand protection analytics and increased automation across IOC analysis, identity intelligence, ransomware monitoring and impersonation detection. Long-term

direction focuses on converging agentic AI XTI functions into a unified operational platform supporting enterprise and MSSP workflows.

Strengths

- **Broad industry coverage:** SOCRadar pulls from industry-aligned sources such as dark web BIN data, ICS and OT feeds, and medical device advisories, mapping threats to MITRE for ICS and regulatory frameworks to deliver contextualized intelligence. Customers get industry-tailored risk scoring, heatmaps and PIR-aligned reporting that are more specific than generic CTI feeds.
- **Global distribution:** Customer presence spans North America, EMEA, Asia-Pacific and Latin America, indicating broad adoption rather than reliance on a single region. This breadth positions SOCRadar among the more geographically diversified players in this evaluation.
- **Rule generation automation:** The XTI platform produces detection and enforcement rules in the correct syntax for multiple security products and can automatically deploy them through API-based integrations. Bulk management and rollback features allow security teams to manage detections-as-code and recover quickly when rule-update issues occur.

Cautions

- **Support staff imbalance:** Most support personnel are located in the Asia/Pacific region, resulting in thin staffing for North America despite the market significance. This may constrain customers who prefer close geographic proximity to the vendor.
- **Mobile app limitations:** Issues such as alert-count discrepancies and ongoing UX fixes indicate that the mobile experience is still stabilizing. The app also lacks clarity on integrations with enterprise tools and alert-delivery mechanisms beyond basic notifications.
- **Market tenure:** With limited years in the market, SOCRadar has not yet accumulated the long-term operational credibility established by pre-2015 incumbents. This shorter track record may give buyers fewer long-standing references or maturity indicators to rely on when assessing sustained performance, roadmap execution or long-term stability.

ZeroFox

ZeroFox is a Leader in this Magic Quadrant. Its external cybersecurity platform unifies digital risk protection, cyberthreat intelligence, and adversary disruption for enterprises, government agencies and global brands needing visibility into impersonation threats, fraud activity, malicious infrastructure, synthetic media, identity exposure and external attack surface risks. The platform collects intelligence from surface, deep and dark web ecosystems, social platforms, code repositories and encrypted or semiopen messaging channels, enriched through proprietary crawlers and human validation. Use cases include phishing detection, brand protection, credential monitoring, and geopolitical and influence-driven threat monitoring.

ZeroFox delivers intelligence through a SaaS platform, managed services and hybrid models, such as structured intelligence feeds and API-based delivery, supporting integrations with SIEM, SOAR, TIP and case management workflows. AI capabilities include enrichment models, language and sentiment detection, facial comparison, synthetic media identification and contextual explanations tailored to analyst workflows, all reinforced by human-in-the-loop validation. The ZeroFox enterprise mobile app provides real-time alerting, incident triage and takedown requests secured through enterprise authentication.

The roadmap emphasizes expanded AI-driven detection, broader disruption, enhanced campaign analytics, and unified analysis across identity, brand, infrastructure and physical security intelligence. Long-term direction focuses on converging automated detection, human analysis and adversary disruption into a single operational platform.

Strengths

- **Operational scale:** ZeroFox operates a large analyst, HUMINT and takedown operation that enables continuous collection across social platforms, dark web forums, mobile app stores and adversary infrastructure at a depth few competitors replicate. This allows preemptive attack response by pairing early intelligence with rapid in-house disruption.

- **Execution-ready roadmap:** The roadmap provides concrete deliverables such as natural language CTI search, automated asset discovery, bulk disruption workflows, campaign-level graphing, and AI-generated output showing a direct correlation between platform vision and operational use cases. ZeroFox also demonstrates maturity across cyber, brand and physical domains, reflecting convergence that aligns with modern SOC needs.

- **Ecosystem integration:** ZeroFox demonstrates sustained commercial adoption supported by deep integration coverage, including multiplatform SOC, CTI, takedown and exposure management interoperability. This ecosystem depth helps customers embed DRP and intelligence workflows into existing operational stacks without major architectural changes.

Cautions

- **Regional concentration:** ZeroFox's customer base remains heavily centered in North America, resulting in comparatively limited presence in other regions. Buyers operating outside of North America may encounter fewer localized references, in-region expertise or tailored support, which can affect evaluation confidence and regional fit.
- **Sales execution limits:** Channel partners drive most customer acquisition, which can reduce direct visibility into customer needs and create slow feedback cycles. Early stage sales processes emphasize proposal scoping over technical validation, which may slow adoption for buyers seeking evidence-based evaluations.
- **Pricing complexity:** Asset-based pricing plus a takedown bucket model increases forecasting complexity, especially for enterprises with intricate brand, domain or executive protection requirements. Charging for additional integrations can also penalize multitool SOC architectures that rely on broad interoperability.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, each vendor must:

- Have had an established market presence, with commercially available threat intelligence and DRPS products, supported by sales, marketing and customer support operations as of 1 January 2022.
- Have 250 or more paying, enterprise customers as of 30 October 2025, or earned at least $50 million in direct or indirect sales during the previous 12 months (from 30 October 2024 to 30 October 2025). All sales must be related to threat intelligence and/or DRPS products and services.
- Have at least 100 employees supporting product development, sales/marketing and customer delivery.
- Have an established global presence with customers in at least two other geographical regions outside of the headquarters' native region.
- Provide indicators of compromise (IoCs), including maliciousness or suspiciousness ratings, such as IP addresses, URLs, domains and file hashes.
- Provide a framework for cataloging adversary tactics, techniques, and procedures for understanding and investigating cyberattacks and the threat actors responsible.
- Provide additional out-of-the-box enrichments to IoCs, such as attribution information, geolocation data and registration information.
- Provide vulnerability intelligence tailored for vulnerability/exposure prioritization, highlighting actively exploited vulnerabilities and the associated IoCs, TTPs and threat actor information.
- Provide machine-to-machine integrations to either push or pull intelligence artifacts through to multiple solutions, using JSON, APIs or STIX/TAXII formats. This must also include the ability to automatically push or pull intelligence with private or public intelligence sharing communities, such as the information sharing and analysis centers (ISACs).
- Provide timely reporting of geopolitical events and trends that could impact business operations, including political unrest, regulatory changes and regional security events.

- Provide investigation support options, including ad hoc requests for information, longer-term analysis or recurring analyst augmentation.
- Provide finished intelligence reporting, including technical/tactical analysis reports as well as operational and strategic intelligence products.
- Provide an interactive user portal with built-in analysis functionalities such as contextualized dashboards, configurable alerting and search features. The portal must allow for:
  - Direct technical intelligence collection or research, enabling the consumer to tailor collection or search functionality for relevant insights.
  - Configuration of alerting thresholds based on predefined criteria.
  - Industry- and region-specific curation, such as advanced search filters, specific query parameters and dashboards.
  - Visual representation of weighted connections between intelligence artifacts and threat actors, most commonly represented in nodal network graphs.
  - Built-in priority intelligence requirements development and governance.
  - Metrics reporting tailored for operational governance.
  - Integration of large language model (LLM) capabilities to automatically contextualize and summarize threat intelligence data.
- Provide at least three of the below capabilities:
  - Monitoring and alerting coverage of the deep and dark web across illicit threat actor forums, marketplaces and encrypted messaging platforms.
  - Monitoring and alerting coverage across social media networks for anomalous, malicious or fraudulent activity, including account takeovers/hijacking.
  - Domain abuse monitoring for threats associated with typosquatting and phishing.
  - Third-party risk monitoring, geared toward evaluating the risks associated with an entity’s supply chain based on threat intelligence activity.

    - Deliver continuous monitoring and alerting of unauthorized use of brand assets, including but not limited to logos, trademarks and images across digital channels, identifying brand abuse.
    - Takedown services for the remediation of detected findings, such as illicit domain/website removals and hijacked account revocations.
- Be actively developing new features and capabilities that enhance the detection, contextualization, and operational use of threat intelligence to reduce risk and improve decision making across security operations and risk management functions.

Excluded from consideration were:

- Vendors offering threat intelligence and DRPS products and services that must be bundled with other software, hardware (including but not limited to: extended detection and response, security information and event management, security orchestration and automated response, threat intelligence platforms), or managed services will not be included in this Magic Quadrant evaluation.
- Threat intelligence vendors offering 2 DRPS use cases or fewer will not be included in this Magic Quadrant evaluation.

Honorable Mentions

The CTI technologies market has many vendors. Of these, 17 were found relevant to our clients and were selected for evaluation in this Magic Quadrant. However, the exclusion of a provider does not mean that the vendor lacks viability. The following are noteworthy vendors not included in the formal analysis. These vendors could be appropriate for clients, contingent on their intelligence requirements:

- **CrowdSec:** CrowdSec offers a collaborative and open-source model that enables organizations to share and benefit from real-time intelligence on malicious IPs and attack behaviors. The CrowdSec Security Engine integrates easily into existing infrastructure, analyzing logs and network activity to detect threats and automate defensive measures. Its blocklisting feature leverages data from CrowdSec's global community to provide up-to-date, actionable lists of hostile IP addresses, helping users proactively block emerging threats. The platform supports a wide range of environments, from cloud to on-premises, offering flexible deployment options. By combining community-driven intelligence, automated blocklisting and a versatile

security engine, CrowdSec helps organizations strengthen defenses and respond quickly to evolving cyber risks.

- **Dragos:** Dragos stands out in the CTI market by focusing on ICS and OT environments, offering intelligence tailored to critical infrastructure sectors. The company combines deep expertise in industrial threats with advanced analytics to help organizations identify, contextualize and respond to risks unique to OT networks and systems. Dragos provides actionable intelligence, incident response support and expert-led threat hunting, enabling high-availability asset owners to strengthen defenses against targeted attacks on industrial control systems and reduce operational risk. This focus on industrial environments makes Dragos a partner for organizations seeking to enhance visibility and resilience in complex, low-disruption settings.

- **Filigran:** Filigran delivers a threat intelligence solution by integrating its OpenCTI platform with the extended threat management (XTM) Suite and agentic AI capabilities. Filigran provides organizations with a structured environment to collect, correlate and analyze threat intelligence from multiple sources, supporting detailed mapping of adversaries and incidents. The XTM Suite enables users to model attack scenarios and understand risks specific to their environment, facilitating more informed prioritization and response planning. Agentic AI features automate intelligence processing, enrichment and analysis, allowing security teams to focus on high-value tasks and accelerate decision making. This combination of modular multisource intelligence management, scenario-driven threat modeling and AI-driven automation positions Filigran as a partner for organizations seeking to operationalize threat intelligence and proactively address current and emerging cyber risks.

- **GreyNoise:** GreyNoise Intelligence focuses on analyzing mass internet scanning and exploitation activity targeting edge infrastructure, such as firewalls, VPN gateways and network-exposed devices where host-based agents are typically not present. The platform leverages telemetry from a distributed sensor network operating across multiple geographies to provide near-real-time visibility into observed activity. Common use cases include supporting detection and response for attacks against internet-facing assets, highlighting vulnerabilities under active exploitation to inform prioritization, and helping security teams reduce alert noise associated with widespread scanning. This approach makes GreyNoise valuable for organizations with substantial internet-facing infrastructure to improve signal-to-noise ratios.

- **HYAS:** HYAS distinguishes itself through its threat intelligence approach centered on adversary infrastructure analysis. The HYAS Insight platform enables investigators to map relationships between threat actors and the infrastructure they use, making it easier to connect campaigns and accelerate attribution. HYAS Protect adds a layer of defense by using protective DNS to block access to malicious domains before threats reach internal systems. The HYAS Adversary Infrastructure Platform supports proactive risk management by providing visibility into attacker resources, while the HYAS Insight Intel Feed delivers intelligence on malware infrastructure for threat detection and response. Collectively, these tools provide organizations with actionable context and infrastructure-focused protection, positioning HYAS as a partner for strengthening investigative capabilities and preemptively disrupting threats.

- **Silobreaker:** Silobreaker transforms fragmented, unstructured threat data into a connected intelligence ecosystem spanning cyber, physical and geopolitical domains. Its platform contextualizes signals through dynamic link analysis, timelines and network graphs, revealing relationships between actors, campaigns, vulnerabilities and global events. Its requirement-driven approach ensures intelligence aligns with organizational priorities, while AI-powered automation accelerates enrichment and reporting, enabling analyst oversight. This combination of multidomain visibility, mission-centric workflows and advanced visualization makes Silobreaker an intelligence partner, helping organizations anticipate and act on complex, cross-border risks.

- **SpyCloud:** SpyCloud specializes in recaptured data such as usernames, passwords, session cookies and other personal or authentication-related information, enabling organizations to proactively mitigate risks from compromised credentials and identity exposures. Its Enterprise Protection solutions leverage a comprehensive repository of breached, phished and malware-exfiltrated data, empowering security teams to detect and remediate account takeover threats before adversaries can exploit them. With Consumer Protection, SpyCloud extends intelligence to safeguard customer accounts, providing insights that help organizations prevent fraud and protect brand reputation. Additionally, SpyCloud's AI-powered Investigations platform equips analysts with tools to trace threat actors, map criminal infrastructure and attribute malicious activity by correlating underground crime data with real-world identities. This multipronged approach, supported by continuous data recapture and

enrichment, positions SpyCloud as a provider that not only alerts on exposures but also facilitates disruption of cybercriminal operations.

- **Team Cymru:** Team Cymru transforms vast adversarial network signal telemetry into pinpointed, actionable insights, helping customers reduce noise during investigations. Its Pure Signal Recon platform continuously aggregates and correlates global BGP routing data, passive DNS, NetFlow traffic, X.509 certificates, open ports and Whois information, delivering a granular view of adversary infrastructure while minimizing false positives. Building on this foundation, Pure Signal Scout provides analysts with real-time enrichment, mapping suspicious artifacts to historical threat behaviors to expedite investigations. Team Cymru's Total Insights Feed supplies a curated, unified entity model of IPs and domains, with risk scores and contextual metadata tagging. By blending deep telemetry, modular deployment options, and a research-driven approach to data fidelity, Team Cymru can help organizations transition from reactive defense to proactive threat hunting.

- **ThreatBook:** Threatbook is an established specialist in Asia/Pacific-centric threat intelligence, underpinned by AI-enhanced analytics and hands-on research tools. The ThreatBook Advanced Threat Intelligence (ATI) platform uses machine learning models to ingest and normalize large telemetry sets such as malware samples, network flows and dark web signals, flagging novel indicators, and TTP clusters with minimal false positives. ThreatBook Investigator, the interactive console, layers natural language processing and AI-assisted reverse engineering into research workflows, enabling analysts to pivot from raw artifacts to highly contextualized dossiers. ThreatBook's curated APAC intelligence feed distills region-specific actor profiles, sector-relevant IOCs and localized campaign trends, helping organizations prioritize risks unique to their operations. The DRPS extends these capabilities by automating takedowns of phishing domains, fraudulent apps and impersonation accounts while providing enriched context like hosting history and malware associations. Additionally, ThreatBook offers an NGTIP, the next-generation (on-premises) threat intelligence platform, delivering life cycle management for intelligence querying, analysis, production and sharing.

- **VulnCheck:** VulnCheck is an established specialist in vulnerability-centric threat intelligence focused on exploit intelligence and attacker tradecraft rather than broad, multidomain threat intelligence aggregation. Its platform emphasizes early identification of exploited and weaponized vulnerabilities by continuously tracking

exploit development, proof-of-concept code, and attacker adoption across public and private sources. VulnCheck curates this intelligence into structured datasets that link CVEs to exploit availability, exploitation status and relevant TTPs, enabling security teams to prioritize remediation based on real-world attacker behavior rather than theoretical severity. While well-aligned to vulnerability and exposure management use cases, VulnCheck's offering is narrower in scope than full-spectrum threat intelligence platforms, with limited coverage of digital risk protection, brand monitoring and geopolitical intelligence.

Evaluation Criteria

Product/Service: This criterion evaluates a vendor's ability to provide product functions in core CTI technology areas, such as the breadth and depth of intelligence-source collection, digital risk protection use cases, investigative/analysis functionalities, reporting capabilities and response features.

Overall Viability: This criterion includes an assessment of a vendor's financial health, the financial and practical success of its overall company, the likelihood that it will continue to invest in CTI technology features and functions, as well as CTI's contribution to revenue growth.

Sales Execution/Pricing: This criterion evaluates a vendor's success in the CTI technology market and its capabilities in presales activities. Considerations include the size and growth of its CTI revenue and install base, flexibility of pricing models, its presales support, and the distribution and inclusivity of its sales channel. The level of interest and reviewed experiences from Gartner clients is also considered.

Market Responsiveness/Record: This criterion evaluates the delivered features and alignment to client demand for CTI capabilities, as well as the track record of delivering new and differentiated functions in line with the changing needs of the market. Considerations include roadmapped functionalities, feature-release cadence and annualized product-update volumetrics.

Marketing Execution: This criterion evaluates a vendor's CTI market messaging in light of Gartner's understanding of customers' needs. Promotion of the brand, increasing awareness of products and influence on the CTI technology market are evaluated, in addition to Gartner client level of interest.

Operations: This criterion evaluates a vendor's resources for maintaining appropriate support staff capacity, stability of its product delivery teams and its ability to deliver privacy compliance/data protection practices.

Ability to Execute

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	NotRated
Operations	Medium

Source: Gartner (May 2026)

Completeness of Vision

Offering (Product) Strategy: This criterion evaluates a vendor's approach to product development and delivery, with an emphasis on ecosystem compatibility and future release strategies.

Vertical/Industry Strategy: This criterion evaluates the vendor's capability to provide tailored threat intelligence and visibility that addresses the unique risks, challenges and requirements of specific industries or sectors.

Innovation: This criterion evaluates a vendor's development and delivery of CTI technology that is differentiated from that of its competitors. We consider product capabilities and customer use in areas such as front-end solutions, AI, automated response and awarded patents.

Geographic Strategy: Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of their global sales and marketing reach as well as global vendor support staff.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	NotRated
Marketing Strategy	NotRated
Sales Strategy	NotRated
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (May 2026)

Quadrant Descriptions

Leaders

Leaders represent vendors that excel in both execution and vision, making them the benchmark for the market. They consistently deliver comprehensive, feature-rich platforms that meet diverse customer needs, including scalability, integration and advanced analytics. Leaders combine strong financial stability, global reach, and proven operational performance with a forward-looking roadmap that anticipates emerging technologies and evolving threat landscapes. They influence industry standards, drive innovation, and maintain high customer satisfaction through robust support and continuous enhancements. Organizations typically select Leaders for enterprise-grade deployments where reliability, breadth of functionality and adaptability to future requirements are critical. These vendors not only perform well today but also demonstrate the ability to sustain leadership as the market evolves.

Challengers

Challengers are vendors that excel in operational execution and have significant market presence, often backed by strong financial resources and a large install base. They deliver dependable, well-supported solutions that meet mainstream requirements effectively, making them attractive for organizations prioritizing stability and proven performance. However, their strategic vision may lack differentiation or aggressive innovation compared to Leaders. While they focus on incremental improvements and operational excellence, they may not be as proactive in shaping future market trends or introducing disruptive capabilities. Challengers are ideal for customers seeking predictable outcomes and mature offerings rather than cutting-edge features, especially in environments where risk tolerance for emerging technologies is low.

Visionaries

Visionaries stand out for their innovative approach and ability to anticipate future market needs, often introducing unique capabilities, advanced AI-driven analytics or novel delivery models that challenge traditional paradigms. These vendors play a critical role in shaping the market by driving innovation and influencing long-term strategies. While Visionaries may lack the scale, global reach or execution maturity of Leaders, they appeal to organizations seeking early adoption of transformative technologies and differentiated features. Their solutions often cater to emerging use cases and forward-thinking security strategies, making them attractive for enterprises that value innovation and are willing to partner on evolving capabilities. Visionaries are essential for pushing the boundaries of what is possible, even if their operational footprint is still developing.

Niche Players

Niche Players focus on specialized segments, industries or geographic regions, offering deep functionality tailored to specific use cases such as compliance, sector-specific threat intelligence or localized risk management. While they lack the breadth and global scale of Leaders or Challengers, their strength lies in delivering highly customized solutions that address unique customer requirements. These vendors often excel in agility and responsiveness within their chosen niche, providing targeted capabilities that larger platforms may overlook. Niche Players are best suited for organizations with well-defined needs or those seeking specialized expertise rather than broad platform coverage. Their offerings can deliver significant value in scenarios where precision and domain-specific knowledge outweigh the need for expansive functionality.

Context

The CTI technologies market has undergone a significant transformation, driven by the increasing sophistication of cyberthreats and the growing need for proactive security strategies. Over the past few years, the boundaries between traditional threat intelligence and digital risk protection services (DRPS) have blurred, resulting in a convergence that empowers organizations to gain deeper, context-rich insights into external threats. This integration enables security teams to not only detect and analyze threats but also to monitor digital assets, brand exposure, and third-party risks across the open, deep and dark web. The market is also characterized by rapid innovation, with vendors continuously enhancing automation, data enrichment and integration capabilities to deliver actionable intelligence at scale, ultimately driving our decision to launch this Magic Quadrant.

Market Overview

CTI technologies have become essential for proactively identifying, analyzing and responding to cyberthreats. As the market matures, core capabilities such as native or proprietary threat-data collection and advanced analytics remain highly valued, which is reflected in the strong positioning of established CTI vendors. At the same time, innovation is accelerating and today’s Leaders face pressure from vendors introducing novel approaches to discovery, contextualization and operational integration.

Market momentum is fueled by rising threat frequency and sophistication, tighter linkage between CTI and broader security programs, and a demand for actionable, context-rich outputs. While machine learning and automation have long supported detection and prioritization, recent advances in generative AI and autonomous AI agents are transforming downstream processes, including intelligence-enabled incident response, threat hunting and exposure prioritization.

At its core, CTI helps organizations identify and prioritize risks from emerging malware and targeted campaigns to supply-chain exposure based on relevance, severity and potential impact. Leading platforms layer in threat-actor profiling, attack-scenario analysis, integration with existing security controls, and support for digital risk protection to drive practical outcomes rather than static reporting.

Two product philosophies are visible: some vendors emphasize deep contextual analysis and flexible integrations for mature teams that need granular control over collection, correlation and response; others emphasize outcome-driven designs that prioritize automation, intuitive UX, and rapid time-to-value for lean or earlier-stage teams. Each path entails trade-offs between power and simplicity.

Recent Trends in the CTI Market

These dynamics set the context for several trends shaping the market:

Operationalization over observability. CTI is shifting from passive intelligence consumption to response-forward outcomes. The market is prioritizing capabilities that convert intelligence into detection content, enforcement actions, takedowns, and exposure-driven prioritization reducing manual handoffs and accelerating time-to-defense. Top performers autogenerate and tune rules for Sigma (SIEM), YARA (malware/EDR), Snort/Suricata (IDS/IPS), as well as firewall/DNS blocks and native query languages. Some attach rules to campaign objects with ATT&CK mapping, back-test to reduce false positives, and push via APIs/content packs closing the loop between observation and enforcement.

AI inside core workflows. Providers are embedding multiagent assistants, LLM-driven summarization/enrichment and orchestration workflows that turn raw signals into decision-ready outputs. These capabilities now span collection (e.g., IOCs, social media, deep and dark web), correlation (e.g., actor/TTP mapping) and dissemination (e.g., executive briefs, hunt packs), with human-in-the-loop controls to manage false positives.

Platform convergence. The market is consolidating CTI, DRPS, and EASM into unified external-threat platforms built on internal data models that normalize indicators, identities, infrastructure and brand assets. This native consolidation enables correlation across adversary campaigns, exposed assets and abuse vectors without reliance on third-party tools. The objective is a single investigation and prioritization workflow, supported by campaign graphs, sector views and asset-aware risk scoring generated within the platform.

Vendor Differentiation

As CTI capabilities become more standardized, differentiation is no longer driven by the presence of features but by how effectively vendors deliver intelligence that alters outcomes across security programs. Providers separate themselves through the fidelity of their intelligence inputs, the maturity of their automation in production environments, the depth of their operational coupling with security controls, and the extent to which human expertise is integrated into day-to-day workflows. Performance against these capabilities determine whether intelligence meaningfully reduces exposure or remains advisory.

Across evaluated vendors, the strongest differentiation is observed where capabilities are difficult to replicate, notably: original data access, validated attribution, closed-loop operationalization and analyst engagement. Vendors relying primarily on open-source feeds, shallow enrichment or loosely coupled integrations struggle to demonstrate durable advantage as baseline CTI functionality becomes increasingly commoditized.

Proprietary intelligence collection and attribution

The most differentiated vendors demonstrate persistent access to nonpublic threat data and the operational discipline to translate that access into reliable attribution. This includes vendor-managed presence in closed forums and marketplaces, proprietary infrastructure tracking, and long-running visibility into ransomware, fraud and access-broker economies. The value lies not in raw data volume but in continuity, validation and historical depth, which enables confident linkage between indicators, campaigns, infrastructure reuse, and adversary intent.

Vendors that excel here move beyond indicator-centric delivery by structuring intelligence around actors, infrastructure clusters and monetization paths, often mapped to frameworks such as MITRE ATT&CK. This attribution depth supports earlier detection,

improved prioritization and more decisive response compared to platforms that rely primarily on opportunistic OSINT aggregation or short-lived telemetry.

From assistive AI to autonomy in intelligence operations

In today's market, automation is less about the presence of AI and more about where it is trusted to operate without friction. Leading platforms integrate AI directly into core intelligence workflows (e.g., prioritization, correlation, reporting) so outputs are generated in-line with operational processes rather than delivered as stand-alone analyst-assist features. At this level, AI increases speed, scale and consistency across large intelligence volumes, but decision authority remains human-controlled, with analysts retaining responsibility for acceptance and enforcement.

More advanced implementations extend beyond workflow acceleration into decision support and execution, marking a higher trust boundary that defines how much influence AI has over outcomes. These systems apply AI to shape and carry out operational decisions (e.g., evidence-backed response actions, automated content life cycle management, continuous false-positive tuning). Here, AI doesn't simply inform analysts, it governs prioritization, initiates changes within defined guardrails and adapts behavior based on measured results.

Platforms that reach this level of advancement demonstrate materially lower analyst intervention and more durable performance at scale. Alternatively, platforms that limit AI to summarization or search augmentation may improve analyst efficiency, but leave core decisioning and execution bottlenecks intact resulting in limited operational impact in high-volume or highly distributed environments.

Closed-loop integrations support faster response

At higher levels of operational maturity, differentiation is driven by how completely intelligence is wired into enforcement and validation, not solely by the number of integrations listed. Leading platforms design integrations as a closed control loop, where intelligence is not only delivered to downstream systems but is also natively capable of changing control state, measuring effects and correcting course without manual intervention.

Strong performers integrate intelligence directly into enforcement layers/security controls so actions like rule deployment, reprioritization, blocking, suppression, takedowns and rollback can be executed and governed in-line. These integrations are

bidirectional and state-aware; controls report outcomes back to the intelligence layer, enabling validation of efficacy (e.g., false positive rates, suppression impact, coverage gaps) rather than assuming success.

In fully closed-loop architectures, intelligence doesn't terminate at alerting or orchestration. Instead, it continuously drives control behavior, evaluates whether actions achieved the intended effect and adjusts logic based on observed performance. This feedback loop is what enables sustained response speed and stability at scale, particularly in environments where static integrations and human confirmation become bottlenecks.

By contrast, vendors that rely on one-way feed delivery, customer-built scripts or external orchestration layers may provide high-quality intelligence but fail to close the loop operationally. In those models, enforcement remains brittle, validation is manual and often delayed, and response velocity is constrained by integration friction.

Embedded analyst services help drive better outcomes

Despite advances in automation, human expertise remains a differentiator where precision, judgment and adversary understanding matter most (particularly for targeted campaigns, high-impact incidents and strategic risk assessments). Vendors that embed analysts directly into customer workflows, rather than delivering periodic, stand-alone reports, function as an extension of the internal team. These engagements support continuous campaign tracking, adversary monitoring, tailored RFIs and coordinated takedown or disruption efforts aligned to active operations.

Analyst services are most differentiated when they are operationally integrated, with validated human insights flowing directly into detection logic, response decisions and executive-level communication. In this model, analysts do not operate in parallel to the platform; they shape collection/detection, refine prioritization and reinforce confidence in automated actions by grounding them in real-world adversary tradecraft and investigative context.

Providers that treat analyst engagement as episodic, report-driven or predominantly advisory deliver incremental value but limit operational impact. Sustained outcomes are achieved when human expertise is embedded to support execution by continuously informing automation, closing decision gaps and strengthening trust in intelligence-driven response.

Acronym Key and Glossary Terms

AEV	adversarial exposure validation
API	application programming interface
APT	advanced persistent threat
ASM	attack surface management
BAS	breach attack simulation
BGP	Border Gateway Protocol
BIN	bank identification number
C2	command and control
CISA	Cybersecurity and Infrastructure Security Agency
CERT	Computer Emergency Response Team
CSPM	cloud security posture management
CTI	cyberthreat intelligence
CVSS	Common Vulnerability Scoring System
DNS	domain name system
DRP	digital risk protection

EAP	exposure assessment platform
EASM	external attack surface management
EDR	endpoint detection and response
EPSS	Exploit Prediction Scoring System
GPT	Generative Pre-trained Transformer
ICS	Industrial Control System
IDS	intrusion detection system
IOC	indicator of compromise
IPS	intrusion prevention system
KEV	Known Exploited Vulnerabilities
LLM	large language model
NCSC	National Cyber Security Centre
NDR	network detection and response
NLP	natural language processing
NVD	National Vulnerability Database
OCR	optical character recognition

OOTB	out-of-the-box
OSCF	Open Cybersecurity Schema Framework
OSINT	Open Source Intelligence
OT	operational technology
POC	proof of concept
PaaS	platform as a service
PIR	priority intelligence requirement
REST	Representational State Transfer
RFI	request for information
SaaS	software as a service
SASE	secure access service edge
SIEM	security information and event management
SOAR	security orchestration and automated response
SOC	security operations center
STIX	structured threat information expression
TAXII	trusted automated exchange of intelligence information

TIP	threat intelligence platform
TTP	tactics, techniques and procedures
TVM	threat vulnerability management
UTS	universal transfer switch
UX	user experience
VM	vulnerability management
WAF	web application firewall
XDR	eXtended Detection and Response

⊕ Evaluation Criteria Definitions