Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Digital Threat Intelligence Management, Q2, 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

April, 2023

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Digital Threat Intelligence Management solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading Digital Threat Intelligence Management vendors in the form of SPARK Matrix™. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market positions.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines Digital Threat Intelligence Management as "technology and services that offer unified insight into external threats to organizational digital-facing assets. The technology aggregates and processes threat intelligence from multiple sources and provides comprehensive information about threat actors to enable improved investigation, threat hunting, and cyber defense."

The cyber threat landscape continues to evolve with the bad actor utilizing new and emerging technologies to launch cyber attacks that are not only novel in type, such as Ransomware as a Service or RaaS and state-sponsored bad actors trying to steal Ips, but are also getting increasingly sophisticated. Therefore, it is important for organizations to stay on top of the latest threats and vulnerabilities to stay ahead of the attackers. To this end, organizations are looking for solutions that can provide information regarding security threats and other security-related issues to stop the threats in real time. Digital Threat Intelligence Management serves as a solution to their security-related issues by helping to protect their digital assets and data. Therefore, DTIM has become an important aspect of any organization's cybersecurity strategy.

While newer technologies like machine learning and AI are being misused by bad actors, they are also playing a key role in Digital Threat Intelligence Management products. These technologies allow threat intelligence solutions to analyze large amounts of data and identify patterns that could initiate potential threats. As more organizations move their infrastructure to the cloud, digital threat intelligence solutions have evolved to support cloud-based environments and also begun to integrate with other security solutions like SIEM to provide a comprehensive view of the organizations' security postures.

Digital Threat Intelligence Management solutions provide real-time information about the threats and help to protect organizations' digital assets from cyberattacks that have infiltrated their IT systems. Digital Threat Intelligence solutions enable organizations to detect threats early and prevent them from causing any damage by analyzing data from various sources, including the deep web and the dark web. The solution identifies potential threats and alerts the organizational security teams. It also helps organizations to continuously discover, monitor, protect the organization's digital surface, and enhance the efficiency and productivity of existing security operations workflows.

The following are the key capabilities of a Digital Threat Intelligence Management solution:

- **Threat Intelligence-** A Digital Threat Intelligence Management solution continuously monitors and analyzes all digital assets, including the deep web, the dark web, IP addresses, DLP indicators, mobile apps, and media pages, and utilizes its threat intelligence capabilities to alert the security team about any spotted threats to allow them to manage and mitigate threats in real-time. The solution allows organizations to understand and mitigate active threats and improve the robustness of organizational cybersecurity operations by safeguarding digital assets. A Digital Threat Intelligence Management solution also enables users to enhance their defenses against digital threats by delving deeply into the methods used by cyber attackers to launch digital assaults against organizational IT systems.

- **Automated enhancement and IOC control-** A Digital Threat Intelligence Management solution automatically collects threat feeds and prioritizes IOCs (Indicators of compromise) in a single threat management platform to enable quick threat analysis, response, and remediation. Digital Threat Intelligence Management allows organizations to detect and analyze digital threats to all their digital-facing assets, security, and SOC (Security operations center) teams to work effectively and efficiently and help mitigate and secure the system, users, and all the networks in real time.

- **Dynamic Scoring–** A Digital Threat Intelligence Management solution provides the dynamic scoring capability that automates the scoring process and prioritizes internal and external intelligence based on organizational needs. The capability also enables customers to customize how data is analyzed within the platform based on their configuration and risk profiles. A Digital Threat Intelligence Management solution enables the security teams and SOC (security operations center) teams to prioritize threat incidents for further investigation and mitigation by providing the score to the IoCs. Additionally, the capability helps identify the intensity of digital threats outside and inside the network perimeter, increase the productivity of SOC teams and identify the digital threats in real time.

- **Holistic Reporting-** A Digital Threat Intelligence Management solution provides detailed information about threats, unusual behavior, and past enforcement data to executives and analysts. Additionally, the solution provides visibility into the threat landscape, network performance, and complete organizational security posture. It signifies the risk level of digital threats on organizational IT systems, and helps to create security policies.

- **Threat Intelligence dashboard-** A Digital Threat Intelligence Management solution provides a threat intelligence dashboard that allows organizations to track and monitor inbound and outbound threat activity as well as current shielding posture. A Digital Threat Intelligence Management solution provides a comprehensive view of threat events, incidents, and risk scores in real-time and allows organizations to make decisions and mitigate digital threats.

- **Risk Monitoring-** A Digital Threat Intelligence Management solution allows organizations to continuously monitor advanced risks to different sources to secure their infrastructure, brand reputation, data, and systems in real time. The solution enables organizations to analyze the intensity of cyber threats and mitigate them by providing real-time information regarding external threats. Additionally, it monitors the surface web, the deep web, the dark web, and helps strengthen organizations' security postures.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Digital Threat Intelligence Management vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Digital Threat Intelligence Management market. This study includes an analysis of the key Digital Threat Intelligence Management vendors, including Anomali, BitSight, Cofense, Centripetal, CrowdStrike, Cyberint, Cybersixgill, Cyware, DarkOwl, EclecticIQ, Flashpoint, Group-IB, IBM, Intel471, IntSights, Kaspersky, Microsoft, Outpost 24, Recorded Future, ReliaQuest, Secureworks, Security Scorecard, Trellix, ThreatQuotient, ThreatBlockr, ThreatConnect, ThreatBook, and ZeroFox.

Anomali, CrowdStrike, Cyberint, IBM, Kaspersky, ReliaQuest, Recorded Future, Trellix, Threat Blockr, ThreatQuotient, and ZeroFox are the top performers and technology leaders in the global Digital Threat Intelligence Management market, and have been positioned as the top technology leaders in the 2023 SPARK Matrix™ analysis of the Digital Threat Intelligence Management (DTIM) market. These companies provide a sophisticated and comprehensive technology platform to detect, analyze, and provide unified insights into external threats for all digital-facing assets in real-time.

Anomali offers digital threat intelligence through its products, Anomali ThreatStream and Anomali Lens. The Anomali ThreatStream solution automates the threat intel collection and management lifecycle. It provides relevant and actionable intelligence to security teams that enables them to make informed decisions. Anomali Lens is an NLP-based solution that automatically scans digital content for threat-related information and communicates the information to the concerned executives. Anomali Threat Intelligence Solution allows organizations to minimize the risk of security breaches by automating security controls and enhancing operational efficiencies with automated intel collection, curation, and enrichment. Anomali offers extended threat intelligence support through its marketplace offering that includes threat intelligence feeds, threat analysis tools and enrichments, and security system partners.

CrowdStrike provides Digital Threat Intelligence Management through its CrowdStrike Falcon platform. CrowdStrike's threat intelligence solutions include CrowdStrike Falcon Intelligence, CrowdStrike Falcon Intelligence Premium, CrowdStrike Falcon Intelligence Elite, and CrowdStrike Falcon Intelligence Recon.

Additionally, the Falcon platform allows organizations to stop bad actors in their tracks, protects from the most relevant threats, provides access to CrowdStrike IoCs, easily integrates with countermeasures, saves time, effort, and money, and offers seamless endpoint integration.

Cyberint offers a robust Digital Threat Intelligence Management solution titled Argos Edge. The solution offers automatic and full visibility into organizational digital presence by uncovering known and unknown assets and access points. Argos Edge Attack Surface Monitoring provides full visibility into the threats and weaknesses of the organizational digital environment, including the cloud, as well as associated risks from the third-party partners, and actionable recommendations to effectively respond to threats with near-zero false positives and detailed response actions, such as takedowns and incident containment.

IBM offers a cloud-based threat intelligence platform titled IBM X-Force Exchange. The platform enables organizations to access global threat intelligence, make informed decisions using actionable intelligence, consult security experts, and boost security operations. IBM's comprehensive threat intelligence offerings include IBM X-Force Exchange, IBM Advanced Threat Protection Feed, IBM X-Force Exchange Commercial API, IBM Early Warning Feed, and IBM X- Force Premium Threat Intelligence Reports.

Kaspersky offers a threat intelligence portfolio that includes a threat intelligence platform titled CyberTrace, as well as threat data feeds, threat lookup, threat analysis, threat intelligence reporting, and on-demand threat intelligence expertise services. Kaspersky's threat intelligence provides a comprehensive view of the organizations' security postures and offers recommendations regarding threat mitigation and defensive implementations.

Recorded Future offers threat intelligence through its threat intelligence cloud module. The module uses automated analytics, expertly finished intelligence, and advanced analysis and search capabilities to provide organizations with a comprehensive view of the threat landscape. The module provides threat research and reporting, proactive threat hunting and detection, dark web investigations, as well as adversary prioritization and intelligence requirements. Recorded Future also offers intelligence graphs to provide actionable insights and timely threat intelligence.

ReliaQuest offers robust Digital Threat Intelligence Management as a part of its security operations platform titled GreyMatter. The platform offers integrated and

actionable threat intelligence and provides context behind the threat data, which increases the security teams' ability to handle emerging threats. The platform provides organizations with a comprehensive view of their security environment, helping them to identify and prioritize potential security risks.

Microsoft provides threat intelligence through Microsoft Defender Threat Intelligence (Defender TI). It is a platform that provides security teams with the insights and tools they need to stay ahead of the evolving threat landscape. It aggregates and enriches data from a variety of sources, including Microsoft's own threat intelligence team, to provide a holistic view of threats and threat actors.

Trellix also offers multiple threat intelligence solutions, namely Trellix Insights, Trellix ATLAS, Trellix Global Threat Intelligence, Trellix Private Global Threat Intelligence, Trellix Threat Intelligence Exchange, and Trellix Intelligence as a service. The solutions enable organizations to respond immediately to threats and strengthen their security posture. Additionally, Trellix also has a dedicated Threat Intelligence Group (TIG) that uses accurate data and analytical analysis to ensure that customers receive proper Indications and Warnings (I&W).

ThreatBlockr provides a SaaS-based platform that offers a network security solution that provides intelligence-driven protection to stop known threats from reaching the organization's network and automates enforcement, deployment, as well as analysis of cyber intelligence at a massive scale.

ThreatQuotient offers a robust, open, and extensible threat intelligence platform titled ThreatQ that enhances data-driven security operations. The platform works through its unique DataLinq Engine, Threat Library, ThreatQ Investigations, and ThreatQ Marketplace. ThreatQ provides an integrated, self-tuning threat library, adaptive workbench titled ThreatQ investigations, and open exchange that allows organizations to rapidly identify threats, make better decisions, and respond to the threats.. The platform focuses on enhancing the efficiency and productivity of organizations' existing security operations workflows by integrating different data sources, technologies, and teams to accelerate threat detection and response.

ZeroFox offers digital threat intelligence through an AI-based platform. The ZeroFox platform provides dark web threat intelligence to identify threat actors, get a view of the dark web forums, and evaluate cyber and physical threats.. The platform uses a combination of machine learning, AI-driven algorithms, and human experts to process and operationalize threat data.

BitSight, COFENSE, Cybersixgill, Flashpoint, IntSights, Secureworks, SecurityScorecard, and ThreatConnect have been positioned among the primary strong contenders. These companies provide comprehensive technology capabilities and are gaining significant market traction in the global Digital Threat Intelligence Management market. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2023 SPARK Matrix™ include Centripetal, Cyware, DarkOwl, EclecticIQ, Group-IB, Intel 471, Outpost24 and ThreatBook.

All the vendors captured in the 2023 SPARK Matrix™ of the Digital Threat Intelligence Management market are improving their capabilities to detect external threats in real-time and secure organizations from different external threats. Additionally, the vendors are focusing on increasing their customer base, geographical presence, different industry verticals, and expanding use case support. Vendors are also looking at expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

Following are the key competitive factors and differentiators for the evaluation of Digital Threat Intelligence Management solutions and vendors. While a majority of the digital threat intelligence management solutions may provide all the core functionalities, the breadth and depth of functionalities may differ by different vendors' offerings. Some of the key differentiators include:

Sophistication of technology platform: Users should evaluate a Digital Threat Intelligence Management Solution that offers comprehensive features, including threat intelligence, automated enhancement and IOC control, dynamic scoring, holistic reporting, a threat intelligence dashboard, and risk monitoring. The vendor should support seamless integration with traditional security solutions and third-party integration, easy functionality and management, operability in a cloud-native environment (public, private, and hybrid), automated threat detection in real-time. Also, users should look for the vendor's reputation & expertise, guaranteed SLA availability, and bandwidth. The vendor should offer an intelligent AI-driven platform so that they can fulfill the user's industry-specific and use case-specific requirements. Additionally, the vendors' customer value proposition may vary in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of use cases, global support, flexible & elastic subscription service, and such others.

Vendors' strategy and roadmap: The vendors' capability to formulate a comprehensive and compelling technology roadmap is a crucial factor for users prior to the adoption of the Digital Threat Intelligence Management solution. The vendor should have a firm understanding of the market dynamics to analyze the potential investments of their assets. The vendor should have strong strategic objectives as well as the ability to identify the trends that can be implemented across their business to gain a competitive edge or become a pioneer in the security industry. Users should look for vendors considering multiple horizons and adopting workflows and technologies core to their business in the future. Vendors should implement a gap analysis to determine priorities and deliver value to their stakeholders. The vendors' roadmap strategy execution should include specific timelines. There should be a specialized team of delegations responsible for the success of the roadmap and growth strategy. Users should evaluate vendors that are well-versed with the upcoming opportunities in the Digital Threat Intelligence

Management market and have the ability to devise compelling strategies to overcome unprecedented events. Additionally, the vendors' vision to incorporate predictive and advanced analytics in the platform will provoke smart decision-making and anticipate the probability of events. Organizations are also focusing on enhancing their cloud, mobile, and vulnerability intelligence, adding new detection capabilities, including new sources and a new vulnerability intelligence module, and developing vulnerability intelligence, integrating external attack surface intelligence with internal asset inventory/asset enumeration to provide total visibility into a company's cyber-attack surface and collaborative threat intelligence analysis, increasing the number of threat intelligence data sources available in Cyber Intelligence Marketplace, including free and premium feeds.

Integration and Interoperability: Users should look for a Digital Threat Intelligence Management Solution that offers seamless integration with the organizations' traditional security tools and processes. The vendors should provide integration with SIEM, Firewalls, ISAC/ISAOs, IPS, EDR, SOAR, and other systems to enable insights into security events, streamline incident processing, and manage digital threats in real time. Additionally, some of the vendors are integrating external attack surface intelligence with internal asset inventory/asset enumeration to provide total visibility into a company's attack surface and offer collaborative threat intelligence analysis.

Vendor's Expertise and Domain Knowledge: Organizations should evaluate vendors' expertise and domain knowledge in understanding their unique business problems, use cases, and industry-specific requirements. Organizations are advised to conduct a comprehensive evaluation of different Digital Threat Intelligence Management Solutions and vendors before making a purchasing decision. Users should employ a weighted analysis of the several factors important to their specific organization's use cases and industry-specific requirements.

Scalability and Flexibility: A digital threat intelligence vendor should offer a holistic solution that can automatically identify and respond to digital threats in real time. The solution should be capable of securing distributed environments and protecting more centralized, higher throughput environments. Additionally, the vendor should be able to meet the need of all-sized organizations and government agencies, meet increasing workloads without affecting performance, and collect large-scale data and threat intelligence to assist sector-based monitoring and reporting.

Wide Service and User Support: The Digital Threat Intelligence Management solution should support numerous form factors (PDF, HTML, Office 365), unstructured attack description identification and translation into MITRE ATT&CK methods, automatic IoC import into TS Threat Bulletins, Investigations, Sandbox detonations, lens detected intelligence, associated threat models, SOC analyst research to CTI threat investigation workflow, and exporting capabilities for investigation distribution and collaboration. Additionally, the vendor should support different deployment options, including on-prem, in the cloud, and as a fully hosted SaaS solution and customized integrations.

Scalable Cloud-Native Architecture: Digital threat intelligence solutions resist digital threats intrusions into the cloud ecosystem to protect the core digital assets of the system. The end users are looking for solutions that help them to store their information on the cloud, and according to the organizational requirement, and also allows them to upscale and downsize cloud-based entities to store the data. The vendors should provide Digital threat intelligence solutions that track and monitor digital threat events in cloud-based entities, issue alerts, and help deliver a faster response to digital threats.

Threat Intelligence Expert: Some digital threat intelligence vendors offer threat intelligence solutions with access to security expert teams that help the end users protect themselves against adversaries targeting their organizations and also provide personalized support. End users can look for vendors that offer expert services along with their threat intelligence products.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and provides strategic insights into how each supplier ranks related to their competitors concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **The Sophistication of Technology:** The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others.

- **Competitive Differentiation Strategy:** The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.

- **Application Diversity:** The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability:** The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.

- **Integration & Interoperability:** The ability to offer a product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and open API support and services.

- **Vision & Roadmap:** Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

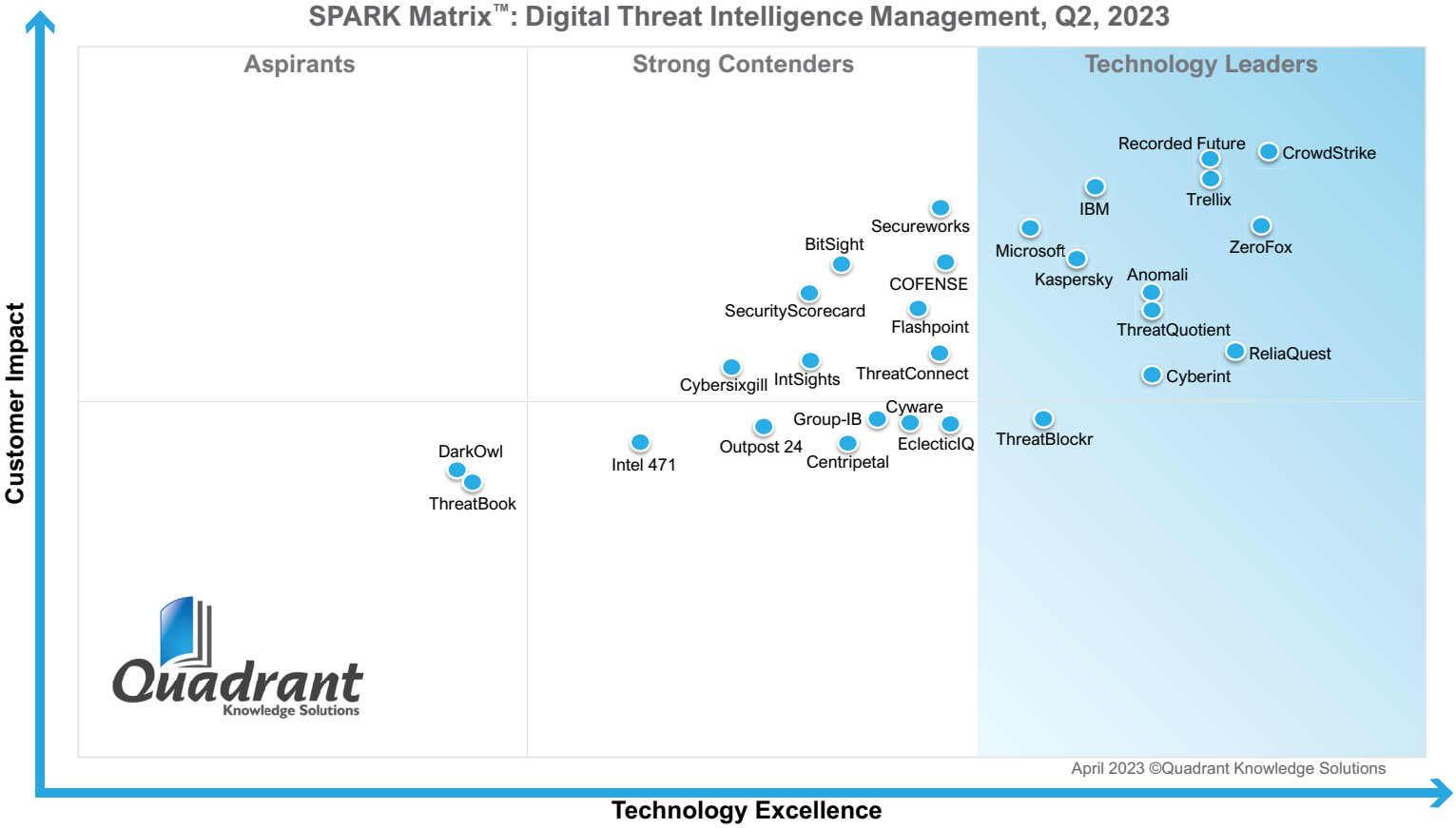
SPARK Matrix™: Digital Threat Intelligence Management

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™

Strategic Performance Assessment and Ranking)

Digital Threat Intelligence Management



Vendor Profiles

Following are the profiles of the leading Digital Threat Intelligence Management vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding Digital Threat Intelligence Management solutions and vendor selection based on research findings included in this research service.

Anomali

URL: https://www.anomali.com/

Founded in 2013 and headquartered in Redwood City, CA, Anomali provides cybersecurity solutions that modernize, , and maintain Internet security software for collective threat identification, analysis, and management. Anomali offers threat intelligence solutions through its Anomali ThreatStream platform and Anomali Intelligence channels.

Anomali ThreatStream automates raw data collection and processing, filters out noise, and transforms legitimate data into valuable, actionable insights and threat intelligence for security teams. Anomali Threat Intelligence Channels delivers customized threat intelligence that is curated by The Anomali Threat Research team.

Analyst Perspective

The following is the analysis of Anomali's capabilities in the Digital Threat Intelligence Management market:

- Anomali offers artificial intelligence and a cloud-based threat intelligence platform. Anomali ThreatStream and Anomali Threat Intelligence channels to collect global threat data and provide visibility into the threat landscape through diversified, specialized intelligence sources without increasing administrative load. Anomali ThreatStream aims to minimize the risk of security breaches by automating the provision of intelligence to security controls and enhancing operational efficiencies with automated intel collection, curation, and enrichment.

- Anomali ThreatStream processes and enhances raw data from a wide range of sources in the field of threat intelligence. These sources include curated feeds from Anomali Labs, publicly available open-source intelligence (OSINT) feeds, specialized premium feeds, and data from information sharing and analysis centers (ISACs). The platform offers real-time dashboards and machine-readable threat intelligence, facilitating security teams in their efforts

to efficiently evaluate, prioritize, and take proactive measures to mitigate threats.

- Anomali ThreatStream provides various capabilities, including intelligence feeds that draw insights from OSI, premium, and Anomali intel feeds to gain actionable insights. It also uses ML-based scoring to improve intel efficiency. Some of the differentiators of Anomali ThreatStream include enhanced security alerts by incorporating information related to threat actors, campaigns, tactics, techniques, and procedures (TTPs), and other relevant data points, and enhances incident response efforts by gaining a deep understanding of potential adversaries, anticipating their future actions, and taking proactive measures to minimize the impact of security breaches.

- Anomali Intelligence Channels optimize the process of gathering and utilizing relevant intelligence by evaluating data related to potential adversaries and making threat information actionable. This ability facilitates ongoing threat monitoring, defense prioritization, and appropriate responses. Anomali Intelligence Channels' differentiators include defense against sector-specific attacks by recognizing actors, malware, and associated activities, SecOps integration by providing crucial intel into security workflows, and integrated dashboards to accelerate decision-making by providing up-to-the-minute insights into relevant threats.

- Anomali has a strong presence in the US. From an industry perspective, the company has a presence across a wide variety of industry verticals, including govt and public sectors, banking and financial services, IT & and telecom, healthcare and life sciences, energy and utilities, media and entertainment, and education. From a use case perspective, Anomali's primary use cases include automated intelligence gathering, enhancing the effectiveness of security controls, sharing threats across trusted communities, ingesting updated data on IOCS, operationalizing MITRE ATT&CK, and determining impact quickly.

CrowdStrike

URL: https://www.crowdstrike.com

Founded in 2011 and headquartered in Sunnyvale, CA, CrowdStrike is a global provider of cloud-delivered protection for endpoints, cloud workloads, identities, and data. CrowdStrike provides Digital Threat Intelligence Management through its CrowdStrike Falcon platform by incorporating threat intelligence into endpoint protection, automating incident investigations, and accelerating breach response. The CrowdStrike Falcon® platform is powered by cloud-scale AI running on the proprietary Threat Graph database and patented smart-filtering technology.

CrowdStrike's threat intelligence portfolio includes CrowdStrike Falcon Intelligence, CrowdStrike Falcon Intelligence Premium, CrowdStrike Falcon Intelligence Elite, and CrowdStrike Falcon Intelligence Recon.

Analyst Perspective

The following is the analysis of CrowdStrike's capabilities in the Digital Threat Intelligence Management market:

- CrowdStrike offers an automated threat intelligence solution through its CrowdStrike Falcon Intelligence solution. The solution automatically investigates incidents and provides actionable and customized intelligence to handle future attacks. Falcon Intelligence enables automated investigations for malware analysis and malware search, which further reduces the time of the attacker and prescribes countermeasures. It also delivers custom IoCs for security orchestration.

- CrowdStrike offers another threat intelligence subscription called the Falcon Intelligence Premium that assists organizational IT systems in identifying and avoiding e-Crime and hacktivist attacks. Falcon Intelligence Premium offers internal security, incident response, and cyber threat intelligence teams with all the productive insights for rapidly identifying, processing and taking remedial actions against dangerous cyberattacks. The subscription also provides intelligence reports that include daily alerts and exposes malicious

actors, tools, and methods. Additionally, it offers tailored intelligence and orchestrates defenses with YARA and SNORT rules to reduce false positives by identifying, classifying, and attributing sophisticated threats. In addition to the features offered by Falcon Intelligence, the subscription includes quarterly threat briefings, expert malware analysis, APIs and pre-built integrations, and access to RFI packs.

- The third tier of CrowdStrike's threat intelligence offering is the Falcon Intelligence Elite. A major capability offered with this subscription is access to an intelligence analyst who assists the security team in securing organizational IT assets from threats and is also responsible for product integrations, onboarding, intelligence clarifications, training, personalized threat briefings, and intelligence research. In addition to the features offered by Falcon Intelligence Premium, the subscription includes RFIs priority intelligence requirements to align intel activity with company strategy, threat briefings, beta program participation, and threat graph inquiries.

- CrowdStrike Falcon automatically analyzes all the risks reaching the endpoints, offers custom IOCs to protect against evasive threats and complete information on attacks to enable faster and better decisions, enhances SOC teams by providing analysis from CrowdStrike Intelligence experts, and simplifies operations by integrating seamlessly with the CrowdStrike Falcon platform.

- CrowdStrike has a strong presence in North America, particularly the US. From an industry perspective, the company has a presence across a wide variety of industry verticals, including healthcare, govt & public sectors, banking & financial services, retail & eCommerce, healthcare & life sciences, energy & utilities, and such others. From a use case perspective, CrowdStrike supports threat intelligence management, threat hunting, incident response, spear phishing, alert triage, and vulnerability management.

- The primary challenges for CrowdStrike include growing competition from emerging vendors with innovative technology offerings. These vendors have successfully gained a strong market position with increased penetration amongst small to mid-market organizations and are among the primary targets for mergers and acquisitions. Additionally, the company might face challenges in expanding its presence in the Asia Pacific and Latin America due to the presence of other players with higher brand visibility. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, CrowdStrike is

well-positioned to maintain and grow its market share in the Digital Threat Intelligence Management market.

- Regarding the future roadmap, CrowdStrike is focusing on investing in its innovation-driven research and development to capture opportunities that come along the way as the market expands.

Cyberint

URL: https://cyberint.com

Founded in 2009 and headquartered in Petah Tikva, Israel. Cyberint is a global provider of digital risk protection and threat intelligence products. Cyberint offers digital threat intelligence management solutions through its Argos Edge™ platform.

The Argos Edge™ platform provides automatic and complete insights into organizational digital presence and identifies security concerns and vulnerabilities that potential attackers can exploit. The Argos Edge™ platform supports real-time threat intelligence modules that include attack surface management, cyber threat intelligence, phishing detection, social media monitoring, supply chain intelligence, forensic canvas, vulnerability intelligence, risk intelligence feeds, and dashboard and reporting capabilities.

Analyst Perspective

The following is the analysis of Cyberint's capabilities in the Digital Threat Intelligence Management market:

- Cyberint's Argos Edge™ platform offers automatic and full visibility into organizational digital presence by uncovering known and unknown assets and access points. The platform's attack surface monitoring capability provides full visibility into the threat and weakness of the digital environment, cloud, and associated risks from the third-party partners, as well as actionable recommendations to effectively respond to threats with near-zero false positives and detailed response actions, such as takedowns and incident containment.

- The Argos Edge™ platform allows organizations to understand their security posture, continuously tracks changes in digital presence, and enables access to continuously evolving analytics that provides visibility into security flaws, shadow IT, and potential risks across the supply chain ecosystem. Some key differentiators of the Argos Edge Attack Surface Monitoring capability include its holistic and integrated approach, agile and flexible DRP offering, advanced discovery and accurate attribution of assets, and focused and relevant alerts.

Additionally, the capability allows customers to access a data lake for research purposes with additional charges.

- The Argos Edge™ platform offers effective handling and management by fine-tuning and prioritizing all detected assets. It enables organizations to track an issue's lifecycle from detection to resolution, calculate security scores to analyze and prioritize threats, automatically resolve addressed issues, and historical snapshots of issue resolution, and provide Ad-hoc and periodic reports.

- The Argos Edge™ platform has various capabilities, including attack surface management that identifies both known and unknown vulnerabilities and weaknesses, ranging from exposed web interfaces and cloud storage exposure to email security problems and open ports. Argos' autonomous discovery process creates a map of the external vulnerabilities and prioritizes them for effective resolution. Additionally, it offers cyber threat intelligence or dark web intelligence, which provides access to immediate, practical threat intelligence for a better understanding of emerging threats from various sources like the open web, deep web, dark web, chat platforms, social media, and more. This enables quicker and more informed decision-making.

- Some other capabilities offered are risk intelligence feeds that enhance the security infrastructure with risk intelligence, featuring risk scores, context, and playbooks through the Argos data lake. It also offers customized vulnerability intelligence designed for external attack surfaces. Similarly, it provides supply chain intelligence, social media monitoring, and phishing detection.

- The key differentiator of the Argos Edge™ platform is Forensic Canvas. This tool facilitates in-depth exploration of specific entities, enabling comprehensive investigation of Indicators of Compromise (IOCs) and threat actors. It achieves this by swiftly establishing correlations and intelligent connections, allowing users to seamlessly transition from a single entity to an entire attack infrastructure and the individual responsible for it with just a simple click.

- Cyberint has a strong presence in the Middle East & Africa, and the USA. From an industry perspective, the company has a presence across a wide variety of industry verticals, including financial services, retail & eCommerce, media & gaming, healthcare, and digital enterprises, and such others. From a use case perspective, Cyberint's key use cases include warning against phishing, attackware, brand, data and ransomware, fraud, and digital footprint attacks.

IBM

URL: https://www.ibm.com/products/xforce-exchange

Founded in 1911 and headquartered in New York, NY, IBM is a leading provider of hardware, infrastructure, and solutions that cater to various segments. IBM enables organizations to transform and develop in the digital era with its comprehensive, cutting-edge technologies, including artificial intelligence, cloud computing, and quantum computing.

IBM offers Digital Threat Intelligence Management through IBM® X-Force® Exchange. This cloud-based platform provides real-time insights into emerging threats and vulnerabilities. IBM also offers other threat intelligence features, such as IBM Advanced Threat Protection Feed, IBM X-Force Exchange Commercial API, IBM Early Warning Feed, and IBM X-Force Premium Threat Intelligence Reports.

Analyst Perspective

The following is the analysis of IBM's capabilities in the Digital Threat Intelligence Management market:

- IBM X-Force Exchange is a comprehensive threat intelligence platform that is supported by both human and machine-generated intelligence. The platform helps organizations protect their networks and data from cyberattacks by providing them access to a global network of security experts and data feeds.

- The IBM platform offers various capabilities, including the IBM Advanced Threat Protection Feed, which has been created to facilitate efficient monitoring and protection of the environment. It offers machine-readable indicators that can be seamlessly integrated with various security tools, including firewalls, intrusion prevention systems, and SIEM, by utilizing open standards.

- The platform also offers the IBM X-Force Exchange Commercial API, which aids in the contextualization of security events by providing programmatic access to external threat intelligence. It serves as a complementary feature to the IBM X-Force Exchange collaborative platform, utilizing open standards to

expedite the response time to security incidents. Additionally, the IBM X-Force Exchange includes a SOAR platform that helps organizations automate their security response. This automation can help to reduce the time taken to respond to attacks and mitigate damage.

- IBM differentiates its offering from other vendors by providing IBM Early Warning Feeds. This feed has been developed to provide early alerts regarding numerous new malicious domains identified daily through IBM's partnership with Quad9. This distinctive content can be accessed via the Advanced Threat Protection Feed and the X-Force Exchange Commercial API. Additionally, IBM also provides IBM X-Force Premium Threat Intelligence Reports. These reports offer timely access to contextual threat intelligence that is published and curated by the X-Force team. They are accessible through the X-Force Exchange Commercial API and are categorized into four types: Threat Activity, Malware, Threat Group Profiles, and Industry Analysis.

- IBM has a strong presence in North America, particularly the USA, followed by the EMEA and the APAC region. From the industry vertical perspective, the top verticals for IBM include aerospace and defense, financial services, education, electronics, energy and utilities, healthcare, life sciences, manufacturing, media and entertainment, retail, and government & public sectors.

- From a use case perspective, IBM supports different use cases, such as threat detection and response, compliance monitoring, insider threat detection, network security monitoring, cloud security monitoring, incident response, and threat hunting.

Kaspersky

URL: https://www.kaspersky.com/

Founded in 1997 and headquartered in Zurich, Switzerland, Kaspersky is a global provider of cybersecurity and digital privacy products. Kaspersky's product portfolio includes security products & services for threat intelligence, managed detection & response, and securing endpoints, networks, emails, cloud environments, and IT/OT devices, among others.

Kaspersky's threat intelligence portfolio includes a threat intelligence platform CyberTrace, Threat Data Feeds, Threat Lookup, Threat Analysis, Threat Intelligence Reporting, Digital Footprint Intelligence, and on-demand threat intelligence expertise services. The threat intelligence solution is provided via Cloud/SaaS and on-premises deployment (air-gapped) models.

Analyst Perspective

The following is the analysis of Kaspersky's capabilities in the digital threat intelligence management market:

- Kaspersky's threat intelligence portfolio offers many threat intelligence solutions and services. The Threat Intelligence (TI) portfolio provides a comprehensive view of the organization's security posture and gives recommendations for threat mitigation and defensive implementations.

- Kaspersky's TI portfolio offers strong capabilities through its TI portal. It also provides actionable and trusted intelligence with contextualized analysis and alerts to ensure that security teams move swiftly to prevent, detect, respond, and mitigate external threats. It also delivers all the knowledge acquired by Kaspersky about cyber threats, legitimate objects, adversaries, and their relationships.

- Kaspersky offers up-to-the-minute TI feeds that can be integrated with security systems, such as TI platforms, SIEM, SOAR, and XDR. It also gives security teams enough information about suspicious or harmful IPs to start a triage process and take decisions on further investigation. It is a vast collection

of data feeds for any requirements, and the threat feeds are generated in real time and are available in formats such as JSON, CSV, OpenIOC, STIX, Suricata, and Yara, delivered via HTTPS/TAXII and provided with connectors for SIEMs/ TIPs/SOARs.

- Another important capability offered by Kaspersky is its multifunctional TI platform, CyberTrace, which integrates data feeds with SIEMs. The platform includes a research graph that enables the visual representation of data and detection and a dashboard feature that displays statistical data and highlights the best feeds. It also offers native integration of Kaspersky TI with Kaspersky's IRP and XDR systems.

- Kaspersky's TI solution provides an on-prem Research Sandbox and a Threat Attribution Engine. The Research Sandbox is also available in a cloud version. It is a comprehensive tool that investigates sample file origin, gathers IoCs based on behavioral analysis, and detects undiscovered malicious objects. The Threat Attribution Engine is a premium threat analysis tool available as an on-prem or cloud service. It enables instant access to a repository with curated data about Advanced Persistent Threats (APTs), and it rapidly attributes files to known APT actors to understand tactics, techniques, and procedures (TTPs).

- Kaspersky differentiates its TI solution for other vendors in this space through its global sensor network that provides a comprehensive view of the threat landscape and in-depth visibility. The data from the sensory network is distributed to the SOC teams across the globe. Additionally, Kaspersky uses independently sourced intelligence, which gives a unique ability to understand, analyze, and distribute vetted information from cybercriminal communities.

- Another important differentiator offered by Kaspersky is its ask-the-analyst service, which offers exclusive access to technical experts to answer all questions related to intelligence reports or ongoing research. It provides additional intelligence regarding published reports, TI support, and additional information about certain indicators. It enables security experts to quickly respond to new threats and vulnerabilities and reduce the damage caused by advanced attacks. It also provides recommendations on further remediation actions, a comprehensive malware sample analysis, and requests for ICS-related information.

- From a geographical perspective, the company has a significant presence in Europe, followed by the Middle East & Africa, Asia Pacific, the USA, Canada, and Latin America. Kaspersky delivers industry-specific solutions to the government and public sectors, banking and financial services, IT and telecoms, energy and utilities, and other industries, such as professional services, construction, transportation, and warehousing.

- Kaspersky also offers a use case-specific Digital Footprint Intelligence service that helps organizations view company resources, discover potential attack vectors, and accordingly plan the defense. It provides a comprehensive view of attack status, identifies weak spots, and provides evidence for past, present, and planned attacks and also provides organizations with insights into their digital footprint - the online presence and activity of their employees, partners, and third-party vendors - in order to identify potential digital risks and vulnerabilities.

- From a use case perspective, Kaspersky TI supports alerting & blocking, campaign tracking through its Global Research & Analysis Team (GReAT), security telemetry enrichment, incidence response, threat hunting, brand protection, vulnerability monitoring, and attack surface monitoring.

- For the technology roadmap, Kaspersky plans to align its focus on consolidating its TI offerings to deliver unified value for its customers. It also focuses on tailoring the TI offerings according to the needs of the specific organizations. It plans to introduce a “Similarity” technology for files, which provides additional context when analyzing incidents to expand the analysis perimeter for threat hunting. Some more focus points in the coming years include brand intelligence improvements, integrating TI more tightly with Kaspersky’s single management platform, and extending integrations of TI with third-party security controls.

Microsoft

URL: https://www.microsoft.com/en-in/

Founded in 1975 and headquartered in Washington, USA, Microsoft is a global provider of computer software, hardware, mobile and gaming systems, and cloud services. Microsoft offers Digital Threat Intelligence Management capabilities through its Microsoft Defender Threat Intelligence Platform.

The Microsoft Defender Threat Intelligence platform provides the organization's security teams with the insights and tools they need to stay ahead of the evolving threat landscape. The platform aggregates and enriches data from a variety of sources, including Microsoft's threat intelligence team, to provide a holistic view of threats and threat actors.

Microsoft acquired cybersecurity company RiskIQ in 2021 to strengthen its efforts to identify and defend organizations' attack surfaces.

Analyst Perspective

The following is the analysis of Microsoft's capabilities in the Digital Threat Intelligence Management market:

- Microsoft Defender Threat Intelligence is a comprehensive threat intelligence platform. This tool supports security experts in evaluating and responding to internet-derived signals obtained through a widespread global network. These signals undergo analysis by a combination of security professionals and machine-learning technology. The resulting datasets reveal the internet infrastructure connections within the global threat landscape. This insight is useful in exposing the external vulnerabilities of an organization and empowering security teams to delve into the specific tools and systems employed in attacks against it. Defender Threat Intelligence enhances the investigation of internal security incidents by providing external context through the utilization of SIEM and XDR functionalities within the Microsoft Sentinel and Microsoft 365 Defender platforms.

- Microsoft Defender Threat Intelligence provides capabilities that include continuous threat intelligence. This feature scans the internet and makes notes of everyday changes. It also unveils the identities of threat actors and delves into their intricate strategies. This knowledge helps the security teams gain a comprehensive understanding of the specific adversary groups orchestrating online attacks, the intricate methods they employ, and their typical modus operandi.

- Microsoft Defender Threat Intelligence fosters a collaborative and unified approach to threat hunting. Teams can seamlessly join forces to investigate and analyze potential threats, leveraging the collective expertise of various departments. It facilitates the sharing of critical threat insights through Intel Profiles, ensuring that knowledge about emerging threats is readily accessible and can be applied to enhance overall cybersecurity readiness. The tool also protects internal resources by unveiling malicious entities and blocking those internet resources.

- Microsoft, through its Microsoft Defender Threat Intelligence platform, differentiates itself by providing alert investigations that augment the data within Microsoft Sentinel and Microsoft 365 Defender incident reports with external threat intelligence. This integration allows security teams to gain a comprehensive perspective on the scope and complexity of a potential threat or attack. Additionally, it offers incident response by investigating and eliminating malicious infrastructure, including domains and IP addresses, as well as any known tools and resources employed by attackers or specific threat families.

- From a geographical presence perspective, Microsoft has a significant presence in North America, particularly the US and Europe, followed by Asia Pacific. From an industry vertical perspective, the primary verticals for Microsoft include automotive, government, healthcare, manufacturing, financial services, and retail. From a use case perspective, Microsoft Defender Threat Intelligence can used for incident response, threat hunting, vulnerability management, and risk management.

Recorded Future

URL: https://www.recordedfuture.com/

Founded in 2009 and headquartered in Somerville, MA, Recorded Future provides security and threat intelligence through its Intelligence platform.

The Recorded Future Intelligence Platform includes different modules, such as Brand Intelligence Module, SecOps Intelligence Module, Threat Intelligence Module, Vulnerability Intelligence Module, Third-Party Intelligence Module, Geopolitical Intelligence Module, Identity Intelligence, and Fraud Intelligence Module that help secure user organizations against various threats.

Analyst Perspective

The following is the analysis of Recorded Future's capabilities in the Digital Threat Intelligence Management market:

- Recorded Future's robust threat intelligence platform is equipped with a threat intelligence Module that provides actionable intelligence and a comprehensive view of the threat landscape. Recorded Future Intelligence platform offers intelligence graphs, integrations, browser extensions, and a mobile app for Android and iOS devices.

- Recorded Future Intelligence Platform, with its threat intelligence modules, offers various capabilities that include Recorded Future Links™ that offer solid, evidence-backed links between clues to enhance investigations and tracking through for faster results. It also provides dark web intelligence, which uses Recorded Future's real-time data from the dark web, including various online forums, to gain insights into potential threats and adversaries. Additionally, the moduleprovides an advanced query builder to perform thorough, specific searches in Recorded Future's intelligence database and save or share those searches for convenient access to relevant information.

- The threat intelligence module also offers intelligence cards that provide information about a specific investigation topic that can also be used as a starting point for triage or to pivot other intelligence during an investigation.

Additionally, the module provides access to a catalog of commonly used workflows tailored to industry trends, threat types, and team needs. The module also allows users to easily customize and establish alerts for intelligence goals that match their specific requirements.

- The key differentiators of the Recorded Future Intelligence platform include the Recorded Future Intelligence Graph, which gathers, organizes, and examines threat data from various internet sources, making it into useful insights. The graph collects and arranges information about active threat actors and victims from text, images, and technical sources. It uses natural language understanding and machine learning to analyze and connect billions of pieces of data in real-time.

- The other differentiators of the Recorded Future Intelligence platform are offered through the threat intelligence modules. These include threat maps providing automated visuals showing threat actors and malware that are relevant to the organization, third parties, and the specific industry. Users can observe how threat trends change over time to help them identify and prioritize the threats most important to them. Another differentiator is a sandbox solution for fast and scalable performance. The solution offers automatic data intake via an API, allowing for full customization of the testing environment, real-time control over the execution process, malware labeling, and additional features to assist with investigations and proactive threat mitigation.

- The threat intelligence modules also offer custom alerting capabilities that enable the organizations to receive immediate notifications via email, mobile app, or portal whenever new intelligence that aligns with your requirements is identified. Additionally, it provides threat-hunting packages to equip the security and TI team with detection tools, including YARA, Snort, and Sigma rules, to actively search for adversaries, malware, or noteworthy network activity.

- Regarding geographical presence, Recorded Future has a strong presence in the US. From an industry perspective, the company has a presence across a wide variety of industry verticals, including healthcare, govt and public sectors, banking and financial services, retail and eCommerce, healthcare and life sciences, energy and utilities, and others. From a use case perspective, Recorded Future’s primary use cases include threat intelligence management, vulnerability intelligence, third-party intelligence, geopolitical intelligence, identity intelligence incident response, spear phishing, alert triage, and vulnerability management.

ReliaQuest

URL: https://www.reliaquest.com/

Founded in 2007, headquartered in Tampa, FL. ReliaQuest is the provider of a security operations platform titled GreyMatter. ReliaQuest offers Threat Intelligence (TI) as part of the GreyMatter platform. The GreyMatter platform is built on an open XDR architecture. The platform enables bi-directional integration across security tools, which helps the SecOps teams to unify the detection and response process with singular visibility, reduced complexity, and managed risk across the security ecosystem.

In June 2022, ReliaQuest acquired Digital Shadows to extend its detection and response capabilities with Digital Shadow's threat intelligence and digital risk technology. GreyMatter Threat Intelligence increases the ability to handle emerging threats by offering integrated and actionable threat intelligence and also providing context behind the threat data.

Analyst Perspective

The following is the analysis of ReliaQuest's capabilities in the Digital Threat Intelligence Management (DTIM) market:

- The GreyMatter platform uses threat intelligence data as a foundation for the detection, investigation, and response process. Hence, GreyMatter Threat Intelligence provides organizations with a comprehensive view of their security environment, helping them to identify and prioritize potential security risks.

- ReliaQuest offers strong capabilities through GreyMatter Threat Intelligence (TI), including providing an integrated view of the TI and data feeds with continuous updates and detection embedded in the organization's security environment. Additionally, GreyMatter provides actionable intelligence with track and drill-down threat advisories and weekly intelligence summaries.

- GreyMatter Threat Intelligence has a user-friendly and understandable threat intelligence homepage with commercially available threat feed subscriptions, IoC threat advisory, and detect patterns and commonalities of potential threats.

This helps the users understand the motives and moves of the threat actors. Additionally, GreyMatter provides widgets that allow organizations to have a comprehensive and actionable view of the IoCs.

- ReliaQuest differentiates its offerings from other vendors in the market by providing "Bring your Own" threat feeds that allow organizations to add commercially available threat feeds that are crucial to them. It provides customizable threat feeds so that the users can add, remove, and update feeds at any time. Another key feature is the threat intelligence updates and real-time alerts, so the organizations are aware of the latest and potential threats.

- From a geographical perspective, the company holds a strong presence in North America, particularly the United States, and is expanding its presence in Europe, the Middle East, and Asia Pacific. From an industry perspective. ReliaQuest serves clients across various industries, including healthcare, financial services, retail, hospitality, and technology, among others. ReliaQuest offers several use cases to enhance an organization's cybersecurity posture, including real-time threat detection, proactive threat hunting, malware analysis, and compliance monitoring.

ThreatBlockr

URL: https://www.threatblockr.com/

Founded in 2014 and headquartered in Tysons, VA, ThreatBlockr is a provider of threat intelligence and network defense products. The company's Threat Intelligence (TI) platform operationalizes threat indicators and uses cyber intelligence from 50 leading sources to block known threats before they reach the network firewall. The ThreatBlockr platform includes TI, automation, and network enforcement into a single, simple-to-deploy and-manage solution.

The SaaS-based ThreatBlockr platform is a network security solution that provides intelligence-driven protection to stop known threats from reaching the organization's network and automates enforcement, deployment, as well as analysis of cyber intelligence at a massive scale.

Analyst Perspective

The following is the analysis of ThreatBlockr's capabilities in the Digital Threat Intelligence Management (DTIM) market:

- ThreatBlockr offers a robust, easy-to-use, cloud-based platform that utilizes simple, innovative technologies and threat intelligence to protect networks, data, and users in real-time. The platform automatically blocks attacks from malicious IPs and domains in real-time with no latency. The platform can also easily integrate with any data source and evaluate an organization's security posture.

- ThreatBlockr platform offers Syslog export capabilities that enable seamless integration with SIEM and log management solutions, and the rich log data provides visibility into threats targeting the network, improving the detection and monitoring efforts.

- The platform provides multi-tenant management capabilities that allow ThreatBlockr Node deployments across multiple sites and organizations. Another important capability is automation and orchestration, which makes

it possible for the threat intelligence data to be automatically updated in real-time and automatically deployed to ThreatBlockr Edge nodes for enforcement, hence improving protection and eliminating the need for manual work.

- ThreatBlockr allows organizations to deploy the ThreatBlockr platform on either side of NGFW (Next Generation Firewall). When deployed in front, it provides immediate and on-demand blocking as close as possible to the ISP point without compromising the network performance. When deployed behind the firewall, it acts as a single point of truth for security analysis, protects multiple physically separate networks, and analyzes all endpoints before being NAT'd by the firewall.

- ThreatBlockr differentiates itself from its competitors on the basis of scalability by blocking up to 150 million IP and domain indicators with no measurable latency. Additionally, it provides point-and-click integration with ISACs, ISAOs, threat intelligence platforms (TIPs), SIEMs, SOARs, and other systems.

- Another differentiating factor of ThreatBlockr is the deployment options to block threats in the cloud through an intuitive management console that enhances visibility and control, integrating threat intelligence from any source. The platform also blocks threats to the network by deploying an inline gateway in front or behind the firewall, which uses threat intelligence to block malicious or unwanted requests. The activity logs are delivered to SIEM and are automatically updated.

- Regarding geographical presence, ThreatBlockr has a strong presence in North America, particularly the USA. From an industry vertical perspective, the company has a presence across a wide variety of industry verticals, including financial services, retail & eCommerce, media & gaming, healthcare, and digital enterprises, and others.

- The primary challenges for ThreatBlockr include the competition from well-established vendors with innovative technology offerings. Additionally, the company might face some challenges in expanding its presence across Canada, the Middle East & Africa, and Latin American markets due to the presence of other players with higher brand visibility. However, with its comprehensive functional capabilities, compelling technology differentiation, and robust customer value proposition, ThreatBlockr is well-positioned to maintain and grow its market share in the Digital Threat Intelligence Management market.

ThreatQuotient

URL: https://www.threatq.com/

Founded in 2013 and headquartered in Reston, Virginia. ThreatQuotient offers a platform that aims to improve the efficiency and effectiveness of security operations. The ThreatQ platform provides threat intelligence capabilities that automate the threat intelligence lifecycle and enable faster threat detection and response that aid in making informed decisions.

The ThreatQ platform works through its unique DataLinq Engine, Threat Library, ThreatQ Investigations, and ThreatQ Marketplace. The platform offers additional features, including dynamic scoring, TDR Orchestrator, ThreatQ Data Exchange, a customizable data model, and smart collections. The platform offers flexible deployment options, including on-prem, cloud-based, virtual instance, and air-gapped.

Analyst Perspective

Following is the analysis of ThreatQuotient's capabilities in the Digital Threat Intelligence Management market:

- The ThreatQ platform centrally controls and integrates all external sources with internal security and analytics solutions in a single pane of glass to provide contextual and operationalized intelligence. The platform focuses on enhancing the efficiency and productivity of organizations' existing security operations workflows by integrating different data sources, technologies, and teams to accelerate threat detection and response.

- The ThreatQ platform is equipped with a dedicated Threat Library, which serves as an organizational memory by storing and prioritizing the data collected from previous detections, investigations, and incidents. The threat library consists of an expiration feature that uses built-in logic to observe the context of data, a scoring feature that uses a drag-and-drop scoring logic to apply weight to contextual information, and a report feature to generate reports about malware.

- The platform also consists of a TDR Orchestrator to simplify orchestration and automation through a data-driven approach that "puts the smarts into the platform." It is an automation module. ThreatQ enables orchestration through data curation and extracts much of the complexity of process-driven playbooks. The platform needs to be updated once. There is no need to update dozens of playbooks. The use of data ensures high-fidelity inputs before initiating a playbook, reduces the number of playbooks runs and ensures relevance and priority of actions taken.

- Another capability offered by ThreatQ is ThreatQ Investigations, a cybersecurity situation room designed for collaborative threat analysis, shared understanding, and coordinated response. ThreatQ Investigations embeds visualization and documentation in a shared environment to allow users gain to a greater understanding of the investigations and focus throughout the analysis process.

- Additionally, ThreatQ Data Exchange enables and manages intel collaboration across organizations or multiple organizations of any size and complexity. It enables bi-directional sharing of all of the intelligence data within the ThreatQ platform and scale sharing across many teams and organizations of all sizes. Another key capability of ThreatQ is the ThreatQ Marketplace which includes integrations of intelligence feeds, security tools, enrichment services, sandboxes, and many more.

- The company differentiates its product from other vendors through its DataLinq engine. This adaptive data engine imports and aggregates external and internal data, curates and analyzes data for decision-making and action, and exports a prioritized data flow across the infrastructure for improved prevention and accelerated detection and response. The engine aims to add value to existing data and systems that exist in the operational environment.

- ThreatQ has a customizable data model that allows customers to update their system to support additional object types for their business requirements. ThreatQ's Threat Library is built on a custom object data model so that users can take advantage of all the default objects that ship out of the box and add and use objects as they would any other object.

- ThreatQ offers a smart collections framework through which users can quickly create highly refined data collections using the flexible filter controls in the Threat Library. The collections are used to drive analysis in dashboards,

feeds in ThreatQ Data exchange, automation in ThreatQ Orchestrator, or custom integrations built on top of the API. ThreatQ also provides granular, configurable user controls for each collection so that only users that need to edit/view them can do so.

- From a geographical perspective, the company has a significant presence in North America and Europe, followed by the Middle East, Africa, Asia Pacific, and Latin America. ThreatQuotient delivers an industry-specific solution to sectors such as IT& telecom, government and public sectors, banking and financial services, energy and utilities, retail and e-commerce, healthcare and life sciences, and education.

- From a use case perspective, some of the top use cases for ThreatQuotient are aggregation, storage and analysis of threat data, operationalization of threat data across disparate defensive systems, creation of bespoke threat intelligence, as well as incident management and response.

- The company continues to work on its vision for data-driven automation for Threat Intelligence as well as threat detection and response use cases. It also focuses on a data retention policy that enables the customers to choose what types of data, from what sources, is retained for how long. Also, the company focuses on innovating and leading in scoring and prioritization to include additional use cases within SecOps and the wider SOC, resulting in improved business outcomes for the end users. ThreatQ plans to work on the completion of the next generation of the ThreatQ Cloud architecture to enable further scalability for both cloud-hosted and on-premises deployments.

Trellix

URL: https://www.trellix.com/en-us/index.html

Founded in 2022 and headquartered in Milpitas, CA. Trellix is the provider of an XDR platform equipped with advanced cyber threat intelligence. Trellix's dedicated Threat Intelligence Group (TIG) uses accurate data and analytical analysis to ensure that customers receive proper Indications and Warnings (I&W). The TIG provides valuable context and information to the users through its product integrations, custom intelligence solutions, and in-depth research.

Trellix also offers multiple threat intelligence solutions, namely Trellix Insights, Trellix ATLAS, Trellix Global Threat Intelligence, Trellix Private Global Threat Intelligence, Trellix Threat Intelligence Exchange, and Trellix Intelligence as a service. As part of Threat Intelligence (TI), Trellix offers products, services, and research, as well as a TI product titled Trellix Threat Intelligence Exchange.

Analyst Perspective

The following is the analysis of Trellix's capabilities in the Digital Threat Intelligence Management (DTIM) market:

- Trellix's Threat Intelligence (TI) Solutions offer custom products to organizations, along with actionable real-time intelligence and insights into malware, ransomware, and cybersecurity threats. The solutions enable organizations to respond immediately to threats and strengthen their security posture.

- Trellix Threat Intelligence Exchange combines the local TI from the organization with the TI from global sources (such as Trellix Global Threat Intelligence) and third-party sources. This combined intelligence is then shared across the security ecosystem using Trellix Data Exchange Layer (Trellix DXL). This shared intelligence enables the security solutions in the organization to act upon it and operate as one to mitigate the threat and enhance organizational security. Trellix DXL helps the security solutions to join the Threat Intelligence Exchange ecosystem, which enables the security solutions to block attacks.

- Trellix Threat Intelligence Exchange offers capabilities, such as custom threat intelligence, which enables the organization to customize the comprehensive threat information for an instant response in case of any future threats. The capability allows the organizational security teams to assemble, override, augment, and tune the threat intelligence according to the protection they want for their environment.

- Trellix differentiates itself by offering advanced threat analytics, which provides more information on a suspected file sent by the TIE to Trellix's advanced analytics solution. This solution analyzes potential threats and then checks the reputation of the suspected file. Another differentiator is security event management, which is done through Trellix Enterprise Security Manager. It investigates the IoCs identified by the Threat Intelligence Exchange and enhances the security posture by accessing historical security information and creating an automated watch list for the same.

- Trellix Global Threat Intelligence (GTI) is a cloud-based reputation service that is integrated into Trellix products. It provides correlated threat data and a variety of reputations, including file reputation, IP reputation, web reputation, and network connection reputation. It also offers air-gapped network support.

- Trellix Private Global Threat Intelligence is an extension to GTI service, which delivers threat reputation across the enterprise. It provides telemetry data for advanced analytics to detect threats as well as custom reputations and supports private network and analyst research.

- Trellix Insights is the first endpoint to XDR. It uses comprehensive intelligence developed by human-machine teaming to predict threats and prescribes what measures can be taken to prevent the attack and optimize the security infrastructure. It identifies global threats, tracks and prioritizes threats that may lead to an attack, analyzes threats using machine learning, and provides preemptive prescribed protection.

- Trellix also offers Intelligence as a Service, which is an on-demand threat intelligence service. This service enables users to seek support from threat intelligence analysts (on-site) and provide custom intelligence reporting as well as analysis of domains and IP addresses.

- Regarding geographical presence, Trellix has a strong presence in North America, followed by APAC and EMEA. From an industry vertical perspective, the company holds a strong customer base in education, financial services, government, healthcare, energy, retail, manufacturing, and others. From a use case perspective, the company offers threat detection, threat hunting, and threat visibility as well as malware, and ransomware detection.

ZeroFox

URL: https://www.zerofox.com/

Founded in 2013 and headquartered in Baltimore, MD. ZeroFox is a cybersecurity vendor that offers a unified cloud-native SaaS external cybersecurity platform. ZeroFox offers end-to-end external cybersecurity through its AI-powered platform, external expert services, and rapid remediation. The ZeroFox platform uses diverse data sources and AI-based analysis to identify and remediate a wide range of attacks.

The ZeroFox platform provides ZeroFox threat intelligence, including cyber threat intelligence, intelligence search, dark web operations, physical security intelligence, intelligence feeds, finished intelligence reporting, and on-demand investigations.

Analyst Perspective

The following is the analysis of ZeroFox's capabilities in the Digital Threat Intelligence Management market:

- The ZeroFox platform provides threat intelligence that enables organizations to gather and process huge amounts of threat data, access threat research from the dark web, and act on the insights received. ZeroFox provides tailored threat intelligence according to organizations' security needs. ZeroFox searches through massive datasets on the surface, deep, and dark web by employing AI processing, deep learning algorithms, and black ops agents to provide relevant, timely, and actionable intelligence.

- ZeroFox threat intelligence provides organizations with dedicated dark web intelligence as well as global threat intelligence teams having a presence in the dark web underground community. ZeroFox uses a tailored dark web ops approach to curate relevant intelligence and monitor specific threats that are important to the organization. Dark ops intelligence protects the organization's assets through real-time intelligence, gaining early warning for emerging or impending threats, bad actor attribution, risk mitigation, threat actor engagement, and malware infections.

- Another capability offered by ZeroFox threat intelligence is threat intelligence feeds. The intelligence feeds are grouped according to their relevance into three categories, identity and fraud, network and vulnerability, and dark web intelligence. These threat intelligence data feeds automate protection and help organizations in the decision-making process and decide the correct course of action. The threat intelligence feeds can be directly integrated with the existing security stack and provide the security team with insights to block IOCs, change passwords, and other remediation actions.

- ZeroFox differentiates its threat intelligence solution from other vendors in this space through on-demand investigations. The company provides organizations with a team of experienced intelligence analysts who conduct risk assessments and investigations along with delivering managed access to deep-dive reports, threat actor and campaign research, cybersecurity forensics, and review of critical queries with recommendations.

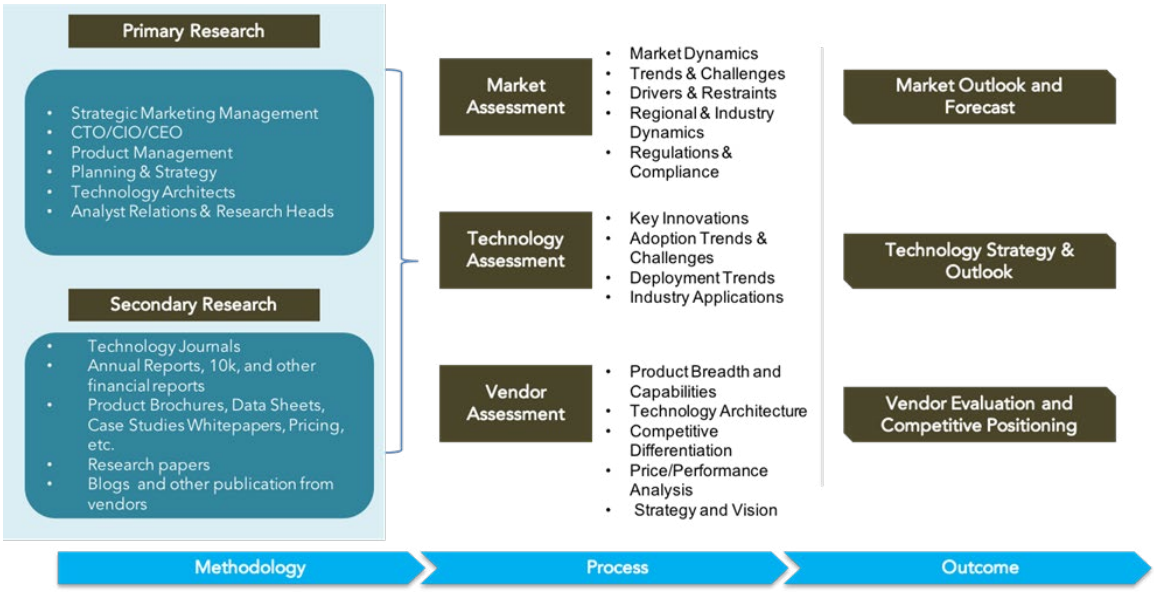
- Another differentiator offered by ZeroFox threat intelligence is the intelligence search feature. This provides a searchable interface with access to ZeroFox's threat intelligence data lake containing information about attacks and IoCs. The security expert teams can search through all finished intelligence, datasets, and raw data that are curated as per organizational requirements.

- ZeroFox threat intelligence also offers physical security intelligence. It monitors a variety of digital sources and risk events and maps these with the location marked as critical by an organization, and then provides real-time alerts on physical threats in the digital space. Physical security intelligence supports the organization with an all-time active security operations team that provides complete coverage for all concerned locations. Additionally, it offers a granular alert policy and rule set, precise location definition, multiple communication formats for alerts, and extensive alert translation support.

- From a geographical perspective, ZeroFox has a strong presence in the US, followed by the UK, Australia, and India. From an industry vertical perspective, the company caters to various sectors, including financial services, healthcare, retail, technology, government, and education.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products

- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage

with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix:
Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com