Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Digital Threat Intelligence Management, Q2, 2024

Market Insights, Competitive Evaluation, and Vendor Rankings

May, 2024

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 that offers 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 rapid evolution of the cyber threat landscape is allowing malicious actors to utilize new and emerging technologies to launch complex attacks. These attacks range from the readily available "Ransomware as a Service" (RaaS) models to newer tactics such as supply chain attacks and theose exploiting emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT). In this ever-evolving environment, organizations need proactive solutions to stay ahead of the curve. Digital Threat Intelligence Management plays a crucial role by providing real-time threat intelligence on the latest threats, vulnerabilities, and attacker tactics. This allows organizations to proactively defend their systems.

Modern Digital Threat Intelligence Management solutions leverage advanced analytics powered by Machine Learning (ML) and Artificial Intelligence (AI). These tools can analyze massive data sets, identify patterns, and predict potential threats. As more organizations move their infrastructure to the cloud, digital threat intelligence solutions have evolved to support cloud-based environments. Also, these solutions can integrate with Security Information and Event Management (SIEM) and other security tools to provide a holistic view of the organization's security posture.

The newer Digital Threat Intelligence Management solutions also offer capabilities beyond mere threat detection. They offer features like dark web and deep web monitoring to identify potential threats hidden in corners of the internet. They also continuously monitor an organization's digital surface to identify vulnerabilities and proactively search for hidden threats within the network. Additionally, the solutions streamline security workflows, enabling faster and more efficient incident response and improving the overall effectiveness of security operations.

In conclusion, with the ever-changing threat landscape, Digital Threat Intelligence Management acts as a critical component of an organization's cybersecurity strategy. By leveraging advanced analytics, real-time threat intelligence, and

integration with existing security tools, DTIM enables organizations to proactively defend their digital assets and stay ahead of attackers.

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.

- **Threat Intelligence feeds-** Digital Threat Intelligence Management solutions provide curated intelligence streamsabout potential cyber threats and vulnerabilities. These feeds aggregate data from diverse sources, including security researchers, industry experts, government agencies, and global cybersecurity communities.These threat intelligence feeds allow organizations to gain access to valuable insights into emerging threats, malware variants, attack techniques, and indicators of compromise (IOCs).

- **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, Centripetal, Cogility TacitRed, CrowdStrike, Cyberint, Cybersixgill, Cyware, EclecticIQ, Flashpoint, Group-IB, IBM, Intel471, Kaspersky, Mandiant, Microsoft, Netcraft, Outpost 24, Rapid7, Recorded Future, ReliaQuest, SecurityScorecard, ThreatQuotient, Threater, ThreatConnect, ThreatBook, Trellix, and ZeroFox.

Anomali, Cogility TacitRed, CrowdStrike, Cyberint, Group-IB, Kaspersky, Mandiant, Netcraft, ReliaQuest, Recorded Future, Trellix, 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 2024 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 platform, and Anomali Intelligence channels. Anomali ThreatStream is a threat intelligence management platform that is part of the Anomali Platform. 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 deliver threat intelligence that is curated by The Anomali Threat Research team. Anomali offers extended threat intelligence support through its marketplace offering that includes threat intelligence feeds, threat analysis tools and enrichments, and security system partners.

Cogility TacitRed is a tactical attack surface intelligence solution. The solution covers threat intelligence, external attack surface management, and third-party risk functionality. The SaaS solution leverages its complex event stream processing and advanced behavioral analytic technologies to provide real-time, curated threat intelligence. TacitRed delivers on-demand, continuously curated, prioritized, and detailed findings to enable decisive mitigation - removing the need

for iterative search, pivots, or validation.
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.

Group-IB offers threat intelligence capabilities through a unified risk platform as well as products, including threat intelligence, fraud protection, managed XDR, attack surface management, digital risk protection, and business email protection. Group-IB Threat Intelligence solution offers extensive insights into adversaries and aims to enhance the efficiency of all security components through strategic, operational, and tactical intelligence.

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.

Mandiant Threat Intelligence offers assistance to security teams in establishing or modifying their security strategy by improving comprehensive intelligence on pertinent malware, vulnerabilities, and adversaries targeting them. This includes insights into the tactics, techniques, and procedures employed in attacks.

Netcraft offers digital threat intelligence management through its threat intelligence platform. The platform offers organizations tools for monitoring and analyzing online threats. It provides data and real-time monitoring capabilities to identify potential risks such as phishing attacks and malware distribution. With features for alerting and investigating suspicious activity, it enables organizations to defend against cyber threats and safeguard their digital assets.

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.

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).

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.

Cybersixgill, Flashpoint, IBM, Intel471, Microsoft, Rapid7, 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 2024 SPARK Matrix™ include Centripetal, Cyware, EclecticIQ, Outpost24, Threater, and ThreatBook.

All the vendors captured in the 2024 SPARK Matrix™ of the Digital Threat Intelligence Management market ar enhancing 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), and automated threat detection in real time. 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.

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 security systems to enable insights into security events, streamline incident processing, and manage digital threats in real-time. Additionally, some vendors are providing API accessibility, which enables users to develop custom integrations as needed.

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 threat 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.

Custom Threat Intelligence Reports- Digital Threat Intelligence Management vendors offer tailored insights, granular detail, actionable recommendations, proactive insights, seamless integration with existing systems, and a demonstration of expertise. The end users are looking for vendors who provide the users with personalized intelligence that is directly relevant to their unique needs, enabling them to stay ahead of evolving threats and bolster their security defenses effectively.

Leveraging AI and ML – Users should look for digital threat intelligence management vendors whose products leverage AI and ML to deliver advanced threat detection, predictive analytics, behavioral analysis, automated response, contextual insights, and adaptive defense mechanisms. By harnessing AI and ML capabilities, DTIM vendors offer end users with proactive and effective security solutions that help them mitigate risks and strengthen their defenses against cyber threats efficiently and comprehensively.

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 on 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
Threat Analysis	20%
Data Collection and Aggregation	20%
Threat Intelligence Feeds	15%
Competitive Differentiation strategy	15%
Real-time Monitoring and Alerting	10%
Integration Capabilities	10%
Reporting and Compliance	5%
Scalability	5%

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

- **Threat Analysis:** The advanced analytics techniques to identify patterns, trends, and relationships among disparate threat data for comprehensive analysis.
- **Data Collection and Aggregation:** The capability to efficiently collect, aggregate, and normalize diverse threat intelligence data from various sources.
- **Threat Intelligence Feeds:** The ability to access a wide range of high-quality threat intelligence feeds, both open-source and premium, to enhance the depth and breadth of threat detection.
- **Competitive Differentiation strategy:** The ability to differentiate from the competitors in terms of capabilities, innovations, technologies used, or customer value proposition.
- **Real-time Monitoring and Alerting:** The ability to provide real-time monitoring of threats and timely alerts to enable proactive response measures.
- **Integration Capabilities:** The ability to integrate with other security solutions like SIEM, SOAR, and XDR.
- **Reporting and Compliance:** The ability to comply with industry standards and regulations, along with robust reporting capabilities for audits and managerial insights.
- **Scalability:** The ability to have a scalable architecture for handling large volumes of threat intelligence data.

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.

- **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.

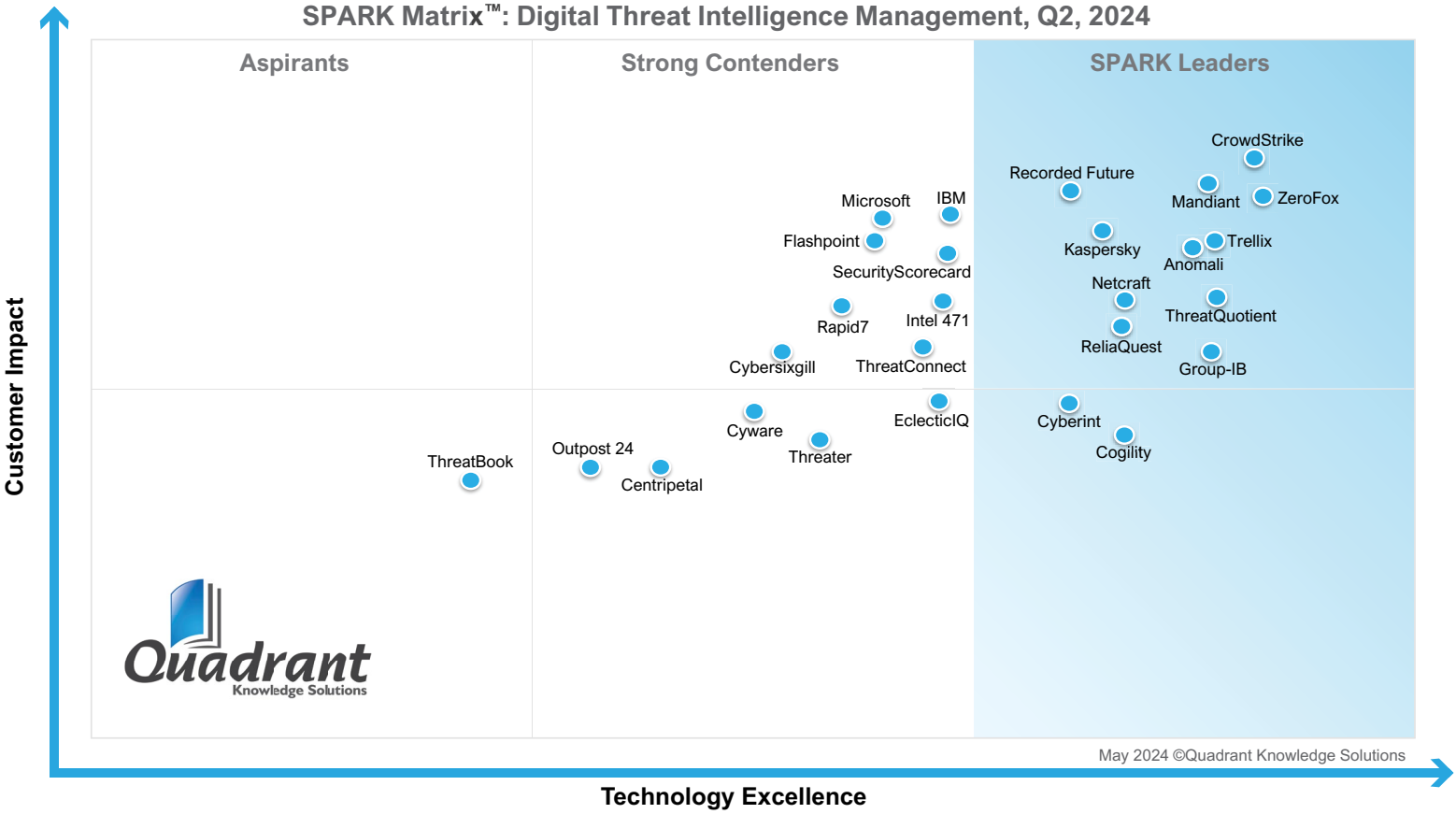
- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

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

SPARK Matrix™: Digital Threat Intelligence Management

Strategic Performance Assessment and Ranking

Figure: 2024 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/

Company Introduction:

Founded in 2013 and headquartered in Redwood City, CA, US, Anomali is a provider of intelligence-driven cybersecurity solutions. Anomali offers threat intelligence solutions through its Anomali ThreatStream platform and Anomali Intelligence channels. The Anomali platform is a security operations and disruptive security analytics platform.

Product Introduction:

Anomali ThreatStream is a threat intelligence management solution that is part of the Anomali Platform. Anomali ThreatStream automates raw data collection and processing, filters out noise, and transforms legitimate data into valuable, actionable insights and threat intelligence. Anomali Threat Intelligence Channels deliver threat intelligence curated by The Anomali Threat Research team.

Technology Perspective:

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

- Anomali Threat Intelligence channels 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 functions by converting raw data into practical threat intelligence and insights, enabling informed decision-making, rapid response, and real-time threat prevention. The platform curates, centralizes, and enriches threat intelligence from various sources, offering context for Security Operations Center (SOC) alerts and investigations. It automatically disseminates pertinent intelligence to existing security controls, aiming to prevent

breaches and fortify the attack surface. It is equipped with an integrated investigations workbench that enhances insight and speeds up threat research. The platform also offers real-time dashboards and machine-readable threat intelligence that help security teams in their efforts to efficiently evaluate, prioritize, and proactively 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.

- The key 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. The Anomali Intelligence Channels also provide customizable/extendible dashboards, which aid in proactive defense and provide rapid detection and response.

Market Perspective:

- Regarding geographic presence, Anomali has a strong presence in the US. From an industry vertical 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 ThreatStream supports use cases that include threat landscape monitoring, automation and intelligence lifestyle management, security control efficacy, enriching SecOps workflow, and accelerating incident response. The Intelligence Channels' use cases include curated channels, unlocking intelligence initiatives, and defending against sector-specific attacks.

Centripetal

URL: https://www.centripetal.ai/

Company Introduction:

Founded in 2009, headquartered in Reston, Virginia. Centripetal Networks is a cybersecurity company that provides solutions for threat detection and mitigation. Centripetal Networks offers protection against various cyber threats, including malware, phishing attacks, and data breaches. Centripetal offers threat intelligence solutions for the cloud and enterprise.

Product Introduction:

Centripetal offers threat intelligence through it's CleanINTERNET® and CleanINTERNET® for cloud solutions. The CleanINTERNET solution provides capabilities including actionable threat intelligence, real-time enforcement, and augmented human analytics. The CleanINTERNET for cloud provides threat intelligence capabilities for entire enterprise in AWS and AZURE environmants.

Technology Perspective:

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

- Centripetal Networks offers a Threat Intelligence solution tailored for both cloud and enterprise environments. This solution is designed to provide organizations with comprehensive visibility and control over potential cyber threats. Centripetal leverages threat intelligence from diverse sources, including global threat feeds, and uses its proprietary data analytics to enable organizations to proactively identify and respond to emerging threats.

- Centripetal CleanINTERNET for enterprise offers actionable threat intelligence, which provides an expansive repository of commercially sourced threat intelligence. This intelligence is integrated into organizational defenses, ensuring they evolve and respond in tandem with the ever-changing threat landscape. Additionally, Centripetal's CleanINTERNET enables real-time enforcement, which integrates the packet filtering technology and seamlessly deploys at

the network's edge without introducing any latency. This integration enables the utilization of billions of threat indicators, ensuring that malicious threats are intercepted before they can penetrate the network.

- Another capability offered by Centripetal CleanINTERNET is augmented human analysis where Centripetal Networks employs a team of highly skilled analysts, augmented by AI technology, to oversee network operations. This collaborative approach enables automated shielding mechanisms based on real-time intelligence, complemented by the validation of human expertise.

- Centripetal differentiates its threat intelligence offering from other vendors by providing augmented intelligence analysis, which uses machine learning, heuristics, and data science techniques, to evaluate threat events, and assigns scores based on attack characteristics, severity, and reportability.

- Another differentiating feature offered by CleanINTERNET is a real-time intelligence application that offers comprehensive dashboards and reporting functionalities, enabling cyber analysts to gain insights into both inbound and outbound threats. These tools provide a holistic view of the threat landscape, equipped with workflow applications and analytics capabilities.

- Centripetal's CleanINTERNET for cloud safeguards assets in cloud environments while enforcing cybersecurity policies through the application of billions of Indicators of Compromise (IOCs). This comprehensive approach monitors and bi-directionally shields assets without disrupting business processes. CleanINTERNET® is compatible with both AWS and Azure environments, offering seamless deployment to protect application and data storage assets in the cloud.

Market Perspective:

- From a geographical perspective, Centripetal Network has a major presence in the North America region. From an industry perspective, Centripetal caters to diverse sectors such as finance, healthcare, government, manufacturing, and technology.

- From a use case perspective, Centripetal Networks threat intelligence solution supports proactive threat intelligence, phishing protection, threat detection and response, and security event volume reduction.

Cogility TacitRed

URL: https://tacitred.com/

Company Introduction:

Headquartered in Irvine, California, US, Cogility Software is a provider of AI Expert-based continuous intelligence solutions. The company's product portfolio includes TacitRed SaaS threat intelligence built on Cogility's Cogynt real-time continuous intelligence platform (Cogynt).

Product Introduction:

Cogility TacitRed is a tactical attack surface intelligence solution. TacitRed straddles threat intelligence, external attack surface management, and third-party risk. TacitRed provides thoroughly curated threat intelligence leveraging its advanced event stream behavioral processing. TacitRed capabilities include attack surface enumeration and visuals, threat scoring; actionable insights on active compromised and at-risk assets with attack type; attack chain stage and validated evidence; threat actor activity monitoring; compromised assets, credentials, and session insight; malware and ransomware insight; deep threat context for investigation and incident response; third-party threat scoring and context sharing; and API-based data integration capabilities.

Technology Perspective:

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

- Cogility's TacitRed SaaS solution removes the security analyst's effort on iterative searches, pivots, copying, and filtering through different threat data by providing on-demand access to its thoroughly curated and detailed threat intelligence. The security analyst simply inputs a company domain name to see findings from a global attack surface perspective. It enables the users to gain insights into the assets that are under active attack or are at risk – each finding being supported by comprehensive evidence. The solution also aids security analysts in identifying and helping to mitigate third-party risk - as third-party entities make up an extended attack surface.

- Cogility TacitRed presents comprehensive features to support its tactical attack surface intelligence value proposition. TacitRed offers continuous external attack surface discovery, analysis, mapping, and monitoring. It constantly gathers and analyzes comprehensive internet signals and threat intelligence globally to map internet-facing assets, vulnerabilities, and active exposures based on cyber adversary activity. The findings include threat scoring based on severity for prioritization, attack type, and attack chain stage, and supporting facts to enable full investigation.

- Under the hood, Cogility's TacitRed applies real-time, high-speed analytics through hierarchical complex event processing (HCEP) technology (Cogility's Cogynt platform) to continuously analyze terabytes of threat signal and intelligence data which enables active attack surface enumeration and curated findings on demand. The approach also employs intelligence data synthesis which combines proprietary and public data sources, including those with advanced reconnaissance techniques, to identify exposures and unwanted activity between an organization's digital presence and threat actors.

- TacitRed also provides malicious command and control identification, which continuously monitors network traffic and internet-facing server behavior, pinpointing customer interactions with known or ascertained malicious commands and control (c2) servers, including those shielded within bulletproof hosting providers. It can correlate interactions between threat actors and the third-party entities that a customer does business with. Detailed evidence, down to the IPs and hostname, allows for faster investigation and prioritized response to mitigate these threats, such as blocking communications and isolating the affected assets.

- TacitRed provides compromised credential and session insights by dynamically analyzing diverse threat intelligence data feeds to validate active attacks - providing customers with details of what credentials are being actively used by cyber adversaries and sessions that are at risk – allowing for prioritized re-issuing of credentials. TacitRed also offers comprehensive malware insights that enable operators to gain detailed malware and ransomware threat intelligence, conveying the stage and extent of infection, as well as other malicious software details to help identify propagation within the user's infrastructure.

- TacitRed supports improving incident response by providing the nature, stage, and extent of the attack or exposure with valid supporting evidence. This allows organizations to reduce discovery and remediation time for proactive or post-incident actions.

- Additionally, TacitRed capabilities aid third-party risk reduction through extended attack surface intelligence by allowing the customer to gain third-party security posture insights, such as threat score and critical security exposure findings, and to be able to share details with the third parties to facilitate their corrective actions.

- Cogility TacitRed's integration capabilities are supported through its REST-API, which follows the Open Cybersecurity Schema Framework (OCSF).

- Cogility's curated threat intelligence solution's key differentiator is the combination of event stream processing technology, intelligence data synthesis, and AI-Expert based HCEP threat modeling that enables ingestion and analytics flexibility, efficiency, and capacity at scale than that of conventional, query-based systems. This provides curated intelligence with true positive attack identification and an overall greater propensity for timely, active, and accurate findings.

- Another differentiating factor is the holistic emphasis on presenting curated, actionable insights. TacitRed prioritizes active threats based on risk factors like exploitability, severity, potential impact, attack chain stage, active exploits, and historical threat actor behavior so that organizations can focus on preventing impactful security exposures, often before they can be fully exploited.

Market Perspective:

- From a geographical business perspective, Cogility is building its presence in the North American Market. From an industry perspective, Cogility holds a solid customer base catering to federal agencies, followed by BFSI, healthcare, manufacturing, transportation and media, retail, and telecommunication sectors.

- From a use case perspective, Cogility TacitRed supports attack surface detection, threat intelligence, incident response enhancement, third-party risk intelligence (such as partners, subsidiaries, M&A targets, and suppliers), and cybersecurity insurance underwriting.

Roadmap:

- Cogility plans to expand TacitRed's analytic capabilities, add emerging threat feeds, using Open-Source Intelligence (OSINT), and incorporate more industry-specific threat intelligence.

- Cogility also plans to enhance collaborative analytics, enable tailored threat prioritization, and extend its integration features.

- Additionally, Cogility plans to expand TacitRed's means to gather telemetry from on-premises sensors to enrich curated findings and risk analysis with insights gathered from behind the firewall.

Crowdstrike

URL: https://www.crowdstrike.com

Company Introduction:

Founded in 2011 and headquartered in Sunnyvale, CA, US, 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.

Product Introduction:

CrowdStrike's threat intelligence portfolio includes CrowdStrike Falcon Intelligence, CrowdStrike Falcon Intelligence Premium, CrowdStrike Falcon Intelligence Elite, and CrowdStrike Falcon Intelligence Recon. CrowdStrike Falcon Intelligence enables the integration of threat intelligence into endpoint protection.

Technology Perspective:

Following is the analysis of CrowdStrike's capabilities in the global 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 attack and prescribes countermeasures. It also delivers custom IoCs for security orchestration.

- CrowdStrike offers another threat intelligence subscription titled 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, as well as 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 expose malicious actors, tools, and methods. Additionally, the subscription offers tailored intelligence and helps orchestrate 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. This subscription provides users with 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 RFI priority intelligence requirements to align intel activity with company strategy, as well as 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 combined Crowdstrike Falcon Intelligence and CrowrdStrike Falcon OverWatch threat-hunting teams to form CrowdStrike Counter Adversary Operations, which serves as a solution to rising identity-focused attacks. CrowdStrike Counter Adversary Operations offers the capabilities of both threat intelligence and threat hunting, which offer methods to stop advanced breaches.

Market Perspective:

- Regarding geographical presence, CrowdStrike has a strong presence in North America, particularly the US. From an industry vertical 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 e-commerce, healthcare and life sciences, and energy and utilities.

- From a use case perspective, CrowdStrike supports threat intelligence management, threat hunting, incident response, spear phishing, alert triage, and vulnerability management.

Cyberint

URL: https://cyberint.com

Company Introduction:

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

Product Introduction:

Cyberint's Argos Edge™ is an intelligence platform that provides automatic and complete insights into an organization's digital presence and identifies exploitable security concerns and vulnerabilities. The Argos Edge™ platform provides ealtime 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.

Technology Perspective:

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

- Cyberint's Argos Edge™ platform offers automatic and full visibility into an organization's digital presence by uncovering known and unknown assets and access points. The platform's attack surface monitoring capability provides full visibility into the threats and weaknesses of the digital environment, cloud, and associated risks from third-party partners and provides 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 provide visibility into security flaws, shadow IT, and potential risks across the supply chain ecosystem. Some key differentiators of the Argos Edge include attack surface monitoring capability

using a holistic and integrated approach, an agile and flexible DRP offering, advanced discovery and accurate asset attribution, and focused and relevant alerts. The capability also provides customers with paid access to a data lake for research purposes.

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

- The Argos Edge™ platform offers 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. The core threat intelligence capability is offered as 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.

- The platform also offers other capabilities, such as 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. It also provides supply chain intelligence, social media monitoring, and phishing detection.

- The key differentiator of the Argos Edge™ platform is a 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 one click.

Market Perspective:

- Regarding geographic presence, Cyberint has a strong presence in the Middle East and Africa, and the USA. From an industry perspective, the company has a presence across a wide variety of industry verticals, including financial services, retail and e-commerce, media and gaming, healthcare, 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.

Cybersixgill

URL: https://cybersixgill.com/

Company Introduction:

Founded in 2014, headquartered in Tel Aviv, Israel. Cybersixgill is a cybersecurity company known for its focus on threat intelligence solutions. Cybersixgill offers a range of products and services designed to provide organizations with enhanced visibility and proactive defense mechanisms against cyber threats.

Product Introduction:

Cybersixgill provides both threat intelligence product and service. Cybersixgill's threat intelligence products include, cyber threat intelligence, vulnerability exploit intelligence, attack surface management, and MSSP solutions.

Technology Perspective:

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

- Cybersixgill provides a comprehensive threat intelligence solution aimed at enhancing organizations' cybersecurity posture. Cybersixgill's solution offers real-time insights into emerging threats, including malware, phishing attacks, and data breaches. Cybersixgill enables organizations to proactively identify and mitigate potential risks By continuously monitoring underground sources and dark web forums.

- Cybersixgill offers threat intelligence with capabilities such as language agnostic, through this capability Cybersixgill collects information from valuable sources that are generally considered difficult to fetch. Another capability offered by Cybersixgill is access to OSINT data that includes a wide range of reports and research.

- Cybersixgill utilizes advanced AI and machine learning algorithms to index, correlate, analyze, tag, and filter the data. These processes aim to provide essential context and practical recommendations for remediation. Addition-

ally, the company provides threat actor profiles that include comprehensive details about the threat actor's history, language, areas of operation, tactics, techniques, procedures (TTPs), interests, peer connections, and interactions. Cybersixgill also leverages NLP and OCR algorithms that are designed to handle data in all languages and formats. They autonomously translate text and extract content from images.

- Cybersixgill differentiates its threat intelligence solution from other vendors by offering its Cybersixgill IQ, which has a generative AI capability to simplify complex threat data. It offers the ability to instantly generate finished reports and comparison tables or provide 24/7 assistance.

Market Perspective:

- From a geographical perspective, Cybersixgill has a significant presence in North America and the Middle East region. From an industry vertical perspective, Cybersixgill caters to the financial services, the energy sector, the healthcare sector, and the gaming sector.

- From a use case perspective, the threat intelligence solution supports various use cases including, phishing intelligence, incident prevention, detection and response, third-party intelligence, vulnerability intelligence, brand intelligence, ransomware and malware intelligence, attack surface intelligence, adversary intelligence, terror investigations, and law enforcement intelligence.

Cyware

URL: https://cyware.com/

Company Introduction:

Founded in 2016, headquartered in New Jersey. Cyware is a cybersecurity company that offers cybersecurity automation solutions. Their security product offerings focus on threat intelligence and security orchestration.

Product Introduction:

Cyware offers threat intelligence through its Intel Exchange threat intelligence platform. The platform leverages AI to automate the threat intelligence process including ingestion, enrichment, and prioritization of threat intelligence. Cyware offers multiple deployment options including cloud, on-premise, and air-gapped. Cyware offers three versions of its Intel Exchange platform, i.e., Intel Exchange, Intel Exchange Lite, and Intel Exchange Spoke.

Technology Perspective:

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

- Cyware's Intel Exchange platform enables Native integration with collaboration and orchestration tools allowing organizations to automate responses, handle incidents, and proactively share and manage threats across different departments or trusted networks.

- Cyware offers various capabilities through its Intel Exchange platform including, centralized threat dashboards that provide streamlined threat intelligence operations from start to finish with a centralized, single-window dashboard. comprehensive visibility and governance controls, allowing for direct, controlled, and efficient management of threat intel activities. Additionally, Cyware provides automated workflows that span across the entire threat intel lifecycle, also utilizing a custom rules engine to tailor workflows to specific requirements.

- Cyware also has an ATT&CK Navigator, that visualizes threat actor tactics and techniques by employing MITRE ATT&CK™ mapping, enabling the organizations to gain insights into how threat actors operate and evolve, enhancing their ability to detect and respond to cyber threats effectively.

- Cyware differentiates its threat intelligence platform from other vendors in the market by providing a confidence score engine. The engine uses the Intel Exchange confidence score algorithm that scores threat data based on varied parameters. The Custom Confidence Score Engine offers a comprehensive range of configurations, allowing users to fine-tune the scoring mechanism according to their specific requirements.

- Another differentiator offered by Cyware is ML-based analysis, which automatically gathers data from sources and disseminates analyzed information to other platforms. Also, Cyware's Intel Exchange platform offers a Threat Intel Crawler that utilizes a threat intel crawler, implemented as a browser extension, to scan, identify, and extract threat intelligence from web-based content using ML and NLP.

- Cyware's Intel Exchange platform also has a feature of geo tagging that automatically maps and analyzes geo-specific threat intelligence collected from various external sources, and identifies geographical trends. Another unique feature of the Intel Exchange platform is the CQL (Cyware Query Language) which can construct robust queries with advanced logic. This allows users to delve deeper into extensive threat intelligence datasets and extract specific threat data tailored to their requirements.

Market Perspective:

- From a geographical perspective, Cyware has a strong presence in the USA. From an industry vertical perspective, the company holds a strong customer base in enterprise, ISAC/ISAO, CERT, and MSSPs.

- From a use case perspective Cyware Intel Exchange platform supports, automated IoC lifecycle management, automated vulnerability prioritization, threat intel orchestration through the SOAR platform, regulatory threat intel ingestion, and bi-directional threat intel sharing.

EclecticIQ

URL: https://www.eclecticiq.com/

Company Introduction:

Founded in 2014, headquartered in Amsterdam, North Holland. EclecticIQ is a cybersecurity vendor providing threat intelligence solutions and services. The company offers intelligence software solutions designed to assist organizations in collecting, analyzing, and managing diverse sources of information. Their product lineup includes tools for threat intelligence, risk management, and incident response.

Product Introduction:

EclecticIQ offers an open and extensible cybersecurity platform that delivers threat intelligence automation and collaboration. The platform displays a significant feature i.e., intelligence at the core™, and has products, packages, ecosystem support, services, and academy. EclecticIQ positions its threat intelligence solution as a practical tool to support organizations in staying vigilant and responsive to the ever-changing landscape of cybersecurity challenges. EclecticIQ offers threat intelligence products that include EclecticIQ Intelligence Center and EclecticIQ Curated Feeds.

Technology Perspective:

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

- EclecticIQ's threat intelligence solution is a part of the company's offerings focused on cybersecurity. It provides a tool for organizations to gather and analyze data from different sources, helping them understand potential threats. The platform includes features such as real-time threat feeds, incident analysis, and collaboration tools.

- Eclectic IQ offers varied capabilities through EclecticIQ Intelligence Center which is a Threat Intelligence Platform that combines machine-driven data processing with human-led analysis. It includes features like a threat intelli-

gence manager, analyst workbench, and integration tools. The Intelligence Manager by EclecticIQ serves as a centralized hub for consolidating extensive internal and external threat data from various sources. This includes open sources, commercial suppliers, and industry partnerships, forming a collaborative and contextual intelligence source. The platform offers flexibility by disseminating intelligence as reports or machine-readable feeds, integrating seamlessly with third-party controls for improved detection and response. the platform provides cloud-like scalability and cost-effectiveness within trusted environments, ensuring adaptability to varying organizational needs.

- Another feature offered by EclecticIQ Intelligence Center is the analyst workbench, which provides Tools to analyze, produce, and collaborate on threat intelligence. These tools support deep threat investigations through advanced search queries, graphical link analysis, and compatibility with leading Cyber Threat Intelligence (CTI) frameworks and standards. The platform enables easy sharing of dynamic results within a collaborative workspace, facilitating team collaboration. Additionally, tasks can be assigned within the workspace to expedite investigations.

- EclecticIQ's Intelligence Center boasts seamless integration capabilities with a wide array of feeds, enrichers, sharing communities, and security tools. The platform comes with pre-built integration, supports integration with incident response solutions, and facilitates integration with sharing and collaboration solutions like MISP, ISACs, and other groups using STIX/TAXII 2.1 standards.

- EclecticIQ curated Feeds is another threat intelligence product offered by the company. EclecticIQ provides users with two distinct threat data feeds tailored for primary threats and optimized for use with the EclecticIQ Intelligence Center. The Open Sources Feed is included with the Intelligence Center, offering curated data from various open sources. Users have the option to enhance their threat intelligence capabilities by opting for the Commercial Sources Feed. the combination of these feeds aims to offer a comprehensive and effective threat intelligence solution for users of the EclecticIQ Intelligence Center.

- EclecticIQ also provides Threat Intelligence Reports, sourced from the Commercial Sources Feed, which provide actionable threat intelligence crafted by the EclecticIQ Threat Research team. The research comprises tactical,

strategic, and operational weekly digests, each uniquely connected to structured visualizations within the EclecticIQ Intelligence Center. By leveraging this threat intelligence, CTI, and SOC analysts can expedite their investigations and enhance the dissemination of intelligence, ultimately strengthening their overall cybersecurity efforts.

- The EclecticIQ platform with threat intelligence as core™ provides EclecticIQ packages, these packages include Threat Intelligence platform for CTI and Threat Intelligence Platform for SOC. EclecticIQ's Threat Intelligence Platform (TIP) for Cyber Threat Intelligence (CTI) targets central governments and large enterprises. The platform accelerates the CTI lifecycle, emphasizing secure collaboration and community sharing for faster response and early warning capabilities.

- The EclecticIQ Threat Intelligence Platform (TIP) for the Security Operations Center (SOC) enables enterprises and government agencies to transition from a reactive, alert-driven approach to a proactive, intelligence-led operation. This allows SOC teams to navigate the abundance of alerts and Indicators of Compromise (IOCs) by concentrating on understanding adversary tactics, techniques, and procedures (TTPs).

Market Perspective:

- From a geographical perspective, the company has a significant presence in the North America and European regions. From an industrial perspective, the company holds a strong presence in the financial services, government and defense manufacturing, supply chain, and technology and IT sectors.

- From a use case perspective, EclecticIQ threat intelligence solution supports threat hunting and prevention, incident response & and investigation, strategic security planning & risk management.

Flashpoint

URL: https://flashpoint.io/

Company Introduction:

Founded in 2010, headquartered in New York. Flashpoint is a cybersecurity company that focuses on threat data and intelligence. The company offers a range of products and services. Flashpoint offers an intelligence platform, named Flashpoint Ignite platform.

Product Introduction:

Flashpoint offers a threat intelligence solution through its Flashpoint Ignite platform. Some of the features offered by Flashpoint CTI are intuitive advanced search, finished intelligence reports, data-driven dashboards, self-service collaboration, vulnerability intelligence, and threat actor profile.

Technology Perspective:

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

- The Flashpoint Cyber Threat Intelligence (CTI) solution gathers intelligence from various corners of the web, including the deep, dark, and surface web, to offer insight into your specific threat environment.

- Flashpoint with its Cyber Threat Intelligence offers a range of capabilities that include, intuitive advanced search that facilitates efficient exploration of extensive data collections, encompassing text, images, videos, and completed intelligence. Additionally, another capability offered by Flashpoint is data-driven dashboards, that offer a holistic perspective of the assets, such as organizations and domains, with intelligence. This enables users to identify notable aspects and seamlessly delve into specifics to understand ongoing developments.

- Another capability offered by Flashpoint Cyber Threat Intelligence solution is the threat actor profiles, Develop thorough threat actor profiles containing

comprehensive information on their behavioral patterns, including aliases, frequented communities, and posting activities tracked over time.

- Flashpoint differentiates its threat intelligence solution from other vendors through its IGNITE AI, which uses natural language search that enables users to ask questions using natural language and receive answers from Flashpoint Intelligence Reports. It streamlines the search process by providing tailored responses to specific queries using data from multiple intelligence reports. Another differentiator offered is self-service collaboration feature through which Users can collaborate with expert analysts to handle inquiries and conduct research within closed illicit communities using the Request for Information (RFI) portal.

Market Perspective:

- From a geographical perspective, Flashpoint has a strong presence in the North American region. The company holds a strong customer base catering to financial services, retail, healthcare and pharmaceuticals, technology, public sector and national security sectors.

- From a use case perspective, Flashpoint's threat intelligence solution supports vulnerability management, insider threat, managed intelligence, physical security intelligence, and curated alerting.

Group-IB

URL: https://www.group-ib.com/

Company Introduction:

Founded in 2003 and headquartered in Singapore, Group-IB is a cybersecurity company that specializes in providing a wide range of services and solutions to help organizations protect themselves against cyber threats and digital fraud.

Product Introduction:

Group-IB offers a unified risk platform as well as products including threat intelligence, fraud protection, managed XDR, attack surface management, digital risk protection, and business email protection. Group-IB Threat Intelligence solution offers extensive insights into adversaries and aims to enhance the efficiency of all security components through strategic, operational, and tactical intelligence.

Technology Perspective:

Following is the analysis of Group-IB's capabilities in the global Digital Threat Intelligence Management market:

- Group IB's threat intelligence solution offers organizations a comprehensive view of cyber threats by drawing on unique data sources like incident response investigations, undercover networks, and malware analysis. This allows for in-depth insights into adversary tactics and motivations, potentially enabling proactive threat prioritization and improved detection across security tools.

- Group-IB's threat intelligence solution offers strong capabilities including a tailored threat landscape that enables the organizations to prioritize security measures based on informed insights into threat actors and their attack strategies targeting the organization. This ability includes identifying relevant risks to the organization, streamlining one-click access to critical information, and offering proactive strategy forecasting. The capability provides a concise summary of key threats over a defined period, ensuring a proactive and resilient defense against evolving threat trends.

- Group-IB's threat intelligence solution offers dark web monitoring, enabling organizations to detect illegal activity and stay informed about relevant conversations. It encompasses the identification of emerging attack strategies, the detection of insider threats, and the monitoring of evolving tactics and target shifts. It goes a step further by identifying compromised data being sold and conducting hacker profile analysis, including tracking new malware and its variations.

- Along with malware detection, Group-IB also provides malware and vulnerability insights, which enable the organization to review in-depth analysis of the weaknesses targeted by malware and threat actors from the dashboard to prioritize patching. The insights give information about the malware family overview, detailed configuration information, the latest vulnerability updates, and discussions of exploits on the dark web and social media.

- Group-IB's threat intelligence solution also offers geopolitical activity and attack attribution capability, This capability creates hunting rules or deploys real-time filters, which is paramount for honing in on primary threats. This involves leveraging a diverse array of attributes, including the victim's industry, region, and country. Additionally, fine-tuning focuses on threat actor attribution, the application of MITRE ATT&CK techniques, and scrutiny of the attack timeline. This comprehensive approach extends to offering insights into threat mitigation strategies and providing actionable recommendations.

- With Group-IB's threat intelligence solution, the organization gets a real-time stream of cyber-threat Indicators of Compromise (IOCs) – including file indicators, IP addresses, domains, URLs, and more. Also, organizations can access information about suspicious IPs and generic attacks.

- Group-IB threat intelligence solution's key differentiator is providing additional features, including Graph Analysis, which provides a streamlined approach to exploring the correlations among threat actors, their infrastructure, and tools, with detailed information accessible at the click of a button. This facilitates various security measures, including efficient threat hunting, Indicator of Compromise (IoC) enrichment, correlation of alerts, and effective mitigation of phishing and fraud incidents. The backend search capability further enhances the tool's versatility, allowing security professionals to delve deeper into interconnected elements for a comprehensive understanding of potential risks.

- Group-IB's threat intelligence solution offers malware detonation, which allows uploading files or sharing links through the Threat Intelligence interface. This initiates an in-depth behavioral analysis, culminating in a comprehensive report of the findings. Additionally, Group-IB experts are available for reverse engineering upon request, enhancing the platform's capacity to address sophisticated threats effectively.

- Another differentiating feature of Group-IB is its comprehensive range of sources, based on human intelligence, our investigations with law enforcement and incident response, malware intelligence (based on our own in-house detonation tool, which is also used in our XDR), ISP-level sensors, C2 access, 24/7 scanning of the entire IPv4, open sources and so on.

Market Perspective:

- Regarding geographical presence, Group-IB has a significant presence in EMEA, followed by North America and the Asia Pacific region. It also holds a strong position in the BFSI, Telecommunication, and govt and public sector industries, followed by e-commerce, healthcare, manufacturing, retail, transportation and media, food and beverages, entertainment, and gaming industry verticals.

- From a use case perspective, Group-IB’s primary use cases include lower security costs, ransomware trends, compromised credentials monitoring, nation-state actors monitoring, dark web monitoring, monitoring of partners breaches, and TI as a tool – use of detonation, graph, and other sections to process investigation/research.

Roadmap:

- As part of the future roadmap, Group IB is focusing on enhancing its technological capabilities which include, threat actor profiles export, renewed global search, threat intelligence browser plugin, raw data analyzer, jabber servers tracking, tools for threat hunting, sigma rules compatibility, and speed enhancement for breached database.

- Group-IB also plans to introduce a unified console for Threat Intelligence, Attack Surface Management, and Digital Risk Protection. The company is also

developing a Threat Intelligence as an Analyst tool that focuses on transforming threat intelligence from a data feed to a professional tool for internal cybersecurity teams. The company also plans to focus on AI-based analytics which includes systems designed to simplify user interaction with Threat Intelligence data, using chatbot models trained on our unique Threat Intelligence dataset.

- In the next coming years, Group-IB plans to expand across the geographies to the EMEA region and later in the US.

IBM

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

Company Introduction:

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 offers comprehensive, cutting-edge technologies, including artificial intelligence, cloud computing, and quantum computing, that enable organizations to transform and develop in the digital era.

Product Introduction:

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.

Technology Perspective:

Following is the analysis of IBM's capabilities in the global 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 facilitates efficient IT environment monitoring and protection. It utilizes open standards to provide machine-readable indicators that can seamlessly integrate 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. The API, offered as a complementary feature to the IBM X-Force platform, utilizes 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 helps reduce the attack response and mitigate damage.

- The IBM platform's key differentiator is IBM Early Warning Feeds. This feed provides early alerts regarding numerous new malicious domains identified daily through IBM's partnership with Quad9. This content can be accessed via the Advanced Threat Protection Feed and the X-Force Exchange Commercial API. 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.

Market Perspective:

- Regarding geographical presence, 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 and 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.

Intel 471

URL: https://intel471.com/

Company Introduction:

Founded in 2014, headquartered in Delaware, United States. Intel 471. Intel 471 provider of cybercrime intelligence, specializing in offering adversary and malware intelligence to intelligence, security, and fraud teams.

Product Introduction:

Intel471 provides cyber threat intelligence through a centralized platform, TITAN Cyber Threat Intelligence. TITAN serves as the centralized platform through which Intel 471 delivers curated Cyber Threat Intelligence (CTI) information to its customers. The platform provides access to dashboards and intelligence reports curated by the company's global team of analysts. The core capabilities of the platform include adversary intelligence, credential intelligence, malware intelligence, vulnerability intelligence, and marketplace intelligence.

Technology Perspective:

Following is the analysis of Intel 471's capabilities in the global Digital Threat Intelligence Management market:

- The TITAN Threat Intelligence platform is a SaaS platform, it provides human-driven, automation-enabled insights aimed at delivering a comprehensive view of threat actors and the potential threats they pose to organizations. Intel 471 offers a robust suite of cyber threat intelligence tools, featuring Finished Intelligence Products that provide strategic and tactical insights. The platform's Alerting function ensures timely notifications while Pivoting capabilities enable seamless navigation between reports, raw data, vulnerabilities, and entities.

- Additionally, it enables the users to conduct precise searches and filter results, minimizing noise and focusing on critical threats. It also provides API that facilitates integration with various intelligence and security platforms. The inclusion of Images, OCR, and Logos recognition enhances threat contextualization.

- Intel 471 offers a wide range of capabilities with its TITAN Cyber Threat Intelligence platform, including 471 Advisory Intelligence which offers proactive insights into the strategies employed by high-level cybercriminals. This includes details on target selection, utilized assets and tools, as well as associations and other supporting entities. It provides a comprehensive understanding of the methodologies adopted by top-tier cybercriminals to better inform and support organizational security measures.

- Another capability offered by Intel471 is the credential intelligence feature, which provides comprehensive coverage of the entire underground marketplace offering. It enables the users to monitor and address the risk associated with compromised credentials as they appear on the marketplace. Additionally, Intel471 provides vulnerability intelligence that delivers pertinent and timely information about the adversary landscape. It addresses a gap in existing vulnerability offerings that predominantly concentrate on known exploits from documented attacks and open-source data. This service aims to provide a comprehensive understanding of potential vulnerabilities, offering a proactive approach to cybersecurity that goes beyond the limitations of current offerings.

- Marketplace Intelligence offered by Intel471, is a tool used for threat analysis. It provides distinctive insights into the highly active and prolific underground marketplaces. The ‘marketplaces’ encompass underground websites designed for the illicit trade of goods and can be further categorized into markets and shops. The marketplace intelligence delivers assets including the TITAN platform and dashboards.

- Intel471 differentiates its threat intelligence platforms from other vendors through malware intelligence, which is also referred to as Malware Emulation and Tracking System (METS), which provides deep context to support various cybersecurity and intelligence use cases, enabling a timely and comprehensive understanding of evolving threats in the digital landscape.

Market Perspective:

- Intel 471 has a significant geographical presence in North America followed by Europe and Asia. From an industry perspective, the company caters to industries including, enterprises, government agencies, and other organizations.

- From a use case perspective, the Intel 471 threat intelligence platform supports vulnerability management, threat hunting, incident response, credential management, and threat actor tracking.

Kaspersky

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

Company Introduction:

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

Product Introduction:

Kaspersky's threat intelligence portfolio includes a threat intelligence platform titled 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.

Technology Perspective:

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

- Kaspersky's threat intelligence portfolio offers various solutions for organizations to assess their security and get recommendations for better defenses. The portfolio provides a detailed view of potential threats, helping in proactive mitigation strategies.

- Kaspersky's TI portfolio offers strong capabilities through its TI portal. The portfolio also provides actionable and trusted intelligence along 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 Threat data feeds provide contextual data that plays a crucial role in unveiling the broader perspective, enhancing the credibility and utility of the information. This ability facilitates quick decision-making and enables prompt actions to be taken.

- Kaspersky provides real-time Threat Intelligence (TI) feeds that seamlessly integrate with various security systems, including TI platforms, SIEM, SOAR, and XDR. These feeds provide security teams with timely information regarding suspicious or harmful IPs, initiating a triage process and facilitating decisions for further investigation. The extensive collection of data feeds caters to diverse requirements, offering threat information generated in real-time and accessible in formats like JSON, CSV, OpenIOC, STIX, Suricata, Sigma and Yara. Delivery occurs through HTTPS/TAXII, and connectors are provided for integration with SIEMs, TIPs, and 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 Threat dashboard feature that displays statistical data and highlights the best feeds. It also offers native integration of Kaspersky TI with Kaspersky SIEM, IRP, XDR , and MDR systems.

- Kaspersky threat intelligence portfolio offers a Threat Lookup feature that enables security teams to access a wealth of information on new and emerging threats, fostering global visibility into the ever-evolving landscape of cybersecurity. This, in turn, aids organizations in proactively securing their infrastructure and bolstering their defense mechanisms against potential cyber adversaries.

- Kaspersky provides Threat Intelligence Reporting for strategic planning: APT Intelligence Reporting, Crimeware Intelligence Reporting, and ICS Intelligence Reporting. They contain detailed descriptions of adversarial TTPs and customer-specific attack surfaces together with actionable recommendations, related IoCs, Yara, Sigma, and Suricata rules.

- Kaspersky Digital Footprint Intelligence is a digital risk protection service designed to assist customers in monitoring their digital assets and identifying potential threats originating from the surface, deep, and dark web. This enables

organizations to proactively safeguard their digital presence and mitigate risks associated with cyber threats lurking in the depths of the internet landscape.

- Kaspersky threat intelligence portfolio provides Threat Analysis - a set of malware analysis tools including Sandbox, Attribution and Similarity technologies available via Kaspersky Threat Intelligence Portal. Sandbox is a comprehensive tool that investigates sample file origin, gathers IoCs based on behavioral analysis, and detects undiscovered malicious objects. Attribution 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). Sandbox and Attribution technologies are available for on-prem deployment as well.

- Kaspersky distinguishes its Threat Intelligence (TI) solution from other vendors by offering multiple credible sources to generate reliable TI: Kaspersky Security Network (sophisticated cloud infrastructure that collects and analyzes anonymous cyber threat data from millions of voluntary participants worldwide), web crawlers, botnet tracking system, spam traps, sensors (such as honeypots sinkholes, and other methods of intercepting ITW attacks), passive DNS data, partners (cybersecurity vendors, LEAs and CERTs) and OSINT (news, social media, public reports, dark web etc.). All incoming data is dissected and interpreted by our in-house threat research teams (Anti-Malware Research, Threat Research, Global Research & Analysis Team, Global Emergency Response Team, Kaspersky SOC, and security assessment teams) speaking dozens of languages with threat research centers established in each region. The data is processed by numerous automated expert systems, transforming it into finished threat intelligence.

- Another 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.

- One more essential part of portfolio - Kaspersky Takedown Service that allows to quickly mitigate threats posed by malicious and phishing domains before any damage can be caused to a customer's brand and business. It enables to takedown fake social network accounts, apps in mobile marketplaces, phishing websites pretending to be associated with the customer's brand.

Market Perspective:

- From a geographical presence perspective, Kaspersky has a significant presence in EMEA, followed by APAC and 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.

- From a use case perspective, Kaspersky supports alerting & blocking, campaign uncovering through several global research and expert teams security telemetry enrichment, incidence response, threat hunting, brand protection, vulnerability monitoring, and attack surface monitoring.

Mandiant (Google)

URL: https://www.mandiant.com/

Company Introduction:

Founded in 2004 and headquartered in Reston, VA, Mandiant is a cybersecurity company providing products and services in cyber defense, threat intelligence, and incident response. The company offers a multi-vector XDR platform that includes attack surface management, security validation, digital threat monitoring, breach analytics, threat intelligence, and managed defense products.

Product Introduction:

Mandiant offers threat intelligence through its Mandiant Threat Intelligence product. In September 2022, Mandiant was acquired by Google to enhance its cybersecurity offering. Mandiant Threat Intelligence offers use-case-based threat intelligence subscriptions, which include a security operations and fusion subscriptions.

Technology Perspective:

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

- Mandiant Threat Intelligence helps security teams establish or modify their security strategy by improving comprehensive intelligence on pertinent malware, vulnerabilities, and adversaries targeting them. This intelligence includes insights into the tactics, techniques, and procedures employed in attacks.

- Mandiant offers various capabilities with its threat intelligence offering. These capabilities include cyber threat profile assessment that provides insights into the potential impact of these threats on the organization and its partners, both currently and in the future. Cyber threat profile serves as a tool for shaping an intelligence-led security strategy and addressing communication gaps between different departments.

- Mandiant Threat Intelligence enables the users to get threat insights from the existing workflows. Users can integrate Mandiant's browser plugin or API into any web page or security analytics tool, such as SIEMs, NTAs, and EDRs. This integration seamlessly facilitates the incorporation of the most recent threat insights, allowing users to gather more information about a vulnerability, indicator, malware, or threat actor without the need to leave the browser or disrupt their workflow. It also has a browser plugin or API that integrates threat intelligence seamlessly into existing workflows. It overlays threat intelligence directly in the user's browser.This functionality extends to various platforms, including social media sites and SaaS-based security consoles.

- Mandiant Threat Intelligence also offers prioritized patching through threat intelligence vulnerability, which enables security risk teams to evaluate, prioritize, and address discovered vulnerabilities on an enterprise scale. This ability is achieved through a unique scoring mechanism that takes into account factors such as the ease of exploitation, likelihood of the exploit, and perceived threat or impact.

- Mandiant threat intelligence also offers digital threat monitoring capability, which offers early visibility into external threat exposures by monitoring various online sources, including underground marketplaces, paste sites, blogs, forums, and malware repositories. This proactive approach aims to anticipate potential attacks and identify unknown data leaks and compromised credentials.

- The key differentiator of Mandiant’s threat intelligence offering is its use of Google’s Duet AI. This constant AI collaborator offers generative AI-powered assistance to help distill Mandiant's extensive threat intelligence into easily understandable summaries. This functionality allows users to grasp how adversaries might be targeting their organization and influencing the threat landscape. Additionally, Mandiant offers Threat Intelligence services, which provide a comprehensive set of offerings to assist in optimizing the capacity to consume, analyze, and apply threat intelligence. This includes expert assistance in building a sustainable intelligence-led organization and enhancing the analytical and threat-hunting capabilities of the team.

Market Perspective:

- From a geographical presence perspective, Mandiant has a significant presence in North America, followed by Europe and the APAC region. From an industry vertical perspective, Mandiant's primary verticals include technology, finance, healthcare, and government sectors.

- From a use case perspective, Mandiant Threat Intelligence offering's primary use cases include proactive threat preparation, security operations, threat hunting, and cyber threat profile development.

Microsoft

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

Company Introduction:

Founded in 1975 and headquartered in Redmond, 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.

Product Introduction:

The Microsoft Defender Threat Intelligence platform provides the user organization's security teams with the insights and tools they need to protect themselves from various types of threats. 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.

Microsoft provides the Defender Threat Intelligence solution in two versions: Defender Threat Intelligence (free) and Defender Threat Intelligence (Premium).

Technology Perspective:

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

- Microsoft Defender Threat Intelligence is a comprehensive threat intelligence platform. The platform supports security experts in evaluating and responding to internet-derived signals obtained through a widespread global network. 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 continuous threat intelligence capability. This capability 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 by allowing teams collaboration to investigate and analyze potential threats, leveraging the teams' collective expertise. 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 platform also protects internal resources by unveiling and blocking 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.

Market Perspective:

- 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's primary use cases include incident response, threat hunting, vulnerability management, and risk management.

Netcraft

URL: https://www.netcraft.com/

Company Introduction:

Founded in 1994 and headquartered in Salt Lake City, US, London, UK, and Melbourne, AU. Netcraft is an internet service and cybersecurity company that focuses on cybersecurity solutions for organizations around the globe. Netcraft solutions include phishing detection, cybercrime detection, threat intelligence, disruptions and takedowns, and transparency and reporting.

Product Introduction:

Netcraft provides threat intelligence through Netcraft's cybercrime detection and disruption platform. The platform utilizes automation, incorporating machine learning and AI in conjunction with a vast array of curated rules.

Technology Perspective:

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

- Netcraft offers threat intelligence solutions focused on cybercrime disruption and brand protection. Their platform leverages automation, machine learning, and human expertise to analyze vast amounts of data and identify potential threats like phishing sites and malware. This data is then transformed into actionable intelligence feeds that are licensed by browsers, security companies, and other internet infrastructure providers.

- Netcraft, through its threat intelligence offering, provides various capabilities, including detection and threat intelligence. Netcraft's detection and threat intelligence solutions process billions of data points from proprietary and open sources with human-written rules, pattern recognition, and artificial intelligence to enhance outcomes in detection, threat analysis, and remediation for its clients. This engine leverages advanced automation to enable rapid disruption shortly after detection, boasting a median takedown times that are considered a benchmark within the industry.

- Netcraft offers global threat feeds that encompass more than 100 cyber threats types, including phishing, malware, and other forms of cybercrimes targeting various institutions, regardless of whether they are customers or non-customers. These feeds are licensed by all major browsers and antivirus companies.

- Netcraft also offers threat analysis and deploys countermeasures on behalf of their customers, Netcraft ensuring prompt action to block malicious content across major browsers using its licensed threat feeds utilized by leading browsers and antivirus companies. This intervention ensures that threats are mitigated within minutes of detection.

- Netcraft differentiates its threat intelligence solution from others by utilizing AI and machine learning. Netcraft integrates AI and machine learning techniques, an expanding proprietary rule database, and insights from expert analysts into its platform. By combining these resources with end-to-end automation, Netcraft aims to establish itself as a benchmark for precise and rapid threat detection and mitigation.

Market Perspective:

- From a geographical perspective, Netcraft has significant presence in North America, followed by EMEA, APAC including Japan regions. From an industrial perspective, Netcraft has caters to various sectors, including Banking and financial services, government and public sector, telecommunication, healthcare and life sciences, retail, e-commerce, education, food and beverages, gaming and entertainment, and automotive industries.

- From a use case perspective, Netcraft's threat intelligence platform supports phishing detection and disruption, brand/citizen protection for governments, brand protection, domain and website takedown, cyber threat feeds, and social media takedowns.

Roadmap:

- Netcraft's roadmap focuses on building a single pane of glass for its users with UI/UX improvements and enhanced Deep and Dark web services. The company is also focusing on innovating new attack types to commercialize.

The company also focuses on expanding its position in the financial industry vertical with recent innovations to enable disruption of fraudulent financial transactions and takedown of previously undetectable threat sources used in direct message scams.

Outpost24

URL: https://outpost24.com/

Company Introduction:

Founded in 2001, headquartered in Karlskrona, Blekinge County. Outpost24 is a cybersecurity company providing solutions for organizations to protect their digital assets. Outpost24's product portfolio provides cyber threat intelligence, external attack surface management, risk-based vulnerability management, web application security testing, and active directory password security.

Product Introduction:

Outpost24 offers a modular-based digital threat intelligence management solution through its Threat Compass. The Threat Compass modules provide support through an in-house analyst team. Additionally, Outpost24 allows businesses to select the intelligence most pertinent to their operations. Some of the key features offered by Outpost24's Threat Compass include domain protection, threat context, threat explorer, actionable intelligence, and hacktivism module.

Technology Perspective:

Following is the analysis of Outpost24's capabilities in the global Digital Threat Intelligence Management market:

- Outpost24 through its Threat Compass offering automates the collection, analysis, correlation, and delivery of comprehensive threat data spanning various categories crucial to your business's security. This approach includes identifying threats such as botnets and command & control servers, pinpointing targeted malware variants, tracking compromised credentials and stolen credit cards, detecting rogue mobile apps, monitoring hacktivist activities, and uncovering phishing campaigns.

- Outpost24 offers a wide range of capabilities that include, Threat Context which provides real-time insights on threat actors, campaigns, malware, and more. By using historical data, Threat Context facilitates focused red teaming and strengthens cybersecurity measures.

- Another capability offered by Threat Compass is the Threat Explorer feature that provides essential global Threat Context information. The Threat Explorer conducts analyses using our Threat Intel-Driven Sandbox. This ensures that users get the insights necessary to mitigate risks effectively and safeguard their digital assets.

- Outpost24's Threat Compass also helps in retrieving leaked credential information, Outpost24 employs sinkholes, honeypots, crawlers, and sensors to constantly scour for stolen credentials. This proactive approach helps mitigate serious attack vectors and fraudulent activities and reduces response times.

- Outpost24 provides integration capabilities through plugins compatible with leading SIEMs, SOAR platforms, and TIPs, ensuring integration into existing security infrastructures. Additionally, support for STIX/TAXII formats.

- Outpost24 differentiates its threat intelligence offerings from other vendors, by offering a Hacktivism module, that monitors hacktivism activity across social networks, paste sites, IRC chats, and other platforms. This module aids in the identification and detection of zero-day vulnerabilities affecting both software and hardware.

Market Perspective:

- From a geographical perspective Outpost24 has a significant presence in the North America region, followed by Europe. From an industry vertical perspective, the company caters to various sectors including manufacturing, energy, utilities, transportation, and telecommunications.

- Outpost24's Threat Compass solution supports a wide range of use cases including, vulnerability management, incident response, threat hunting, and security awareness training.

Rapid7

URL: https://www.rapid7.com/

Company Introduction:

Founded in 2000 and headquartered in Boston, Massachusetts, Rapid7 offers a range of information security solutions and services through its Rapid7 Insights platform. These solutions and services include vulnerability management, incident detection, and response, as well as analytics and automation tools.

Rapid7 acquired IntSights in 2021 to improve its platform's threat intelligence capabilities, ensuring accurate detections across internal and external surfaces earlier, for quick response.

Product Introduction:

Rapid7 offers threat intelligence through its Threat Command solution, offered through the Insights platform. The solution is designed to provide organizations with insights into potential cybersecurity threats. The solution aggregates and analyzes vast amounts of data from various sources to deliver actionable intelligence.

Rapid7 Threat Command solution offers various capabilities, including digital risk protection, threat protection expertise, rapid remediation & takedown, advanced investigation and threat mapping, dark web protection, IOC Management, seamless automation, and an expansive threat library.

Technology Perspective:

Following is the analysis of Rapid7’s capabilities in the global Digital Threat Intelligence Management market:

- Rapid7's Threat Command solution tackles external threats by continuously monitoring the web for organization-specific threats. The solution analyzes millions of sources to deliver relevant, contextualized threat intelligence that prioritizes critical risks. The solution streamlines the threa detection process by automating IOC management and seamlessly connecting with the client’s

existing security tools for faster threat response and mitigation. This comprehensive solution aims to simplify threat intelligence gathering and empower security teams to proactively manage external threats, ultimately reducing risk and workload.

- The Rapid7 threat intelligence solution offers varied capabilities, including Digital Risk Protection. The Threat Command solution systematically scans the clear, deep, and dark web to spot potential dangers before they impact an organization. The solution provides straightforward alerts about threats affecting businesses. These alerts allow users to proactively investigate malware, tactics, techniques, and procedures (TTPs), phishing scams, and other threat actors. The solution also lets users keep an eye on dark web discussions for real-time updates.

- The Threat Command solution also offers advanced investigation and threat mapping capability by tracking the digital footprint using a dynamic asset mapping framework. This framework identifies new potential attack vectors and evaluates areas of exposure. The platform delivers customized insights by automatically correlating threat actor intelligence with the unique digital footprint.

- Rapid7 ThreatCommand solution also offers the dark web protection capability that safeguards clients against threats from the dark web by offering clear visibility of the threat landscape to counteract potential attacks. The solution also provides early warnings and automated intelligence on vulnerabilities across employees, networks, and customers. The solution's AI and machine learning technology ensures swift detection and alerts spanning the clear, deep, and dark web.

- The Rapid7 Threat Command Solution’s key differentiator is its ability to offer rapid remediation and takedown. The company has a dedicated expert team that accelerates the process, streamlining workflows with legal teams for quick removal of malicious campaigns. The Threat Command solution also monitors code and file-sharing sites for exploits and leaked credentials while keeping tabs on the larger online ecosystem for vulnerabilities across social platforms, app stores, and web hosting providers.

- The Threat Command solution also provides IOC management and enrichment through a single-pane-of-glass dashboard. This dashboard provides a

comprehensive view of the entire digital footprint of the user, encompassing web, social, and mobile apps. The solution enables automatic and continuous connection of indicators of compromise (IOCs) by offering real-time contextual visibility into organization-specific threats. The solution allows for prioritized and automated responses by syncing security events, vulnerabilities, and attacks to well-managed data.

- The Threat Command solution supports seamless automation by leveraging custom research, threat hunting, and external threat feeds. it provides a comprehensive understanding of the entire threat environment. The solution's active directory integration feature automatically detects new and existing credential leaks in real time, alleviating the manual burden of identification on SOCs and initiating timely credential resets.

Market Perspective:

- From a geographical presence perspective, Rapid7 has a significant presence in North America, Europe, and Asia-Pacific regions. From an industry vertical perspective, the primary verticals for Rapid7 include healthcare, manufacturing, technology, insurance, energy and utilities, finance, communications and media, education, services, real estate, retail, transportation, government, and hospitality.

Recorded Future

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

Company Introduction:

Founded in 2009 and headquartered in Somerville, MA, US, Recorded Future provides security and threat intelligence through an Intelligence platform. Recorded Future's product lineup includes tools for real-time threat intelligence, risk assessment, and situational awareness.

Product Introduction:

The Recorded Future Intelligence Platform includes different product modules, including 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. The threat intelligence module offers various capabilities, including a threat map, sandbox, advanced query builder, custom alerting, threat hunting packages, and integrations.

Technology Perspective:

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

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

- The Recorded Future Intelligence Platform, with its threat intelligence modules, offers various capabilities that include Recorded Future Links™, which offers solid, evidence-backed links between clues to enhance investigations and tracking 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 provide insights into potential threats and adversaries.

- The threat intelligence modules provide 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 platform also offers threat maps, which provide automated visuals showing threat actors and malware relevant to the organization, third parties, and the specific industry.

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

- The threat intelligence modules offer an advanced query builder, which serves as a pragmatic asset for refining search parameters and extracting pertinent data, contributing to a systematic and methodical analytical process. Users can conduct precise searches tailored to their specific needs, with the ability to save and share these searches for convenient access. Recorded Future threat intelligence module offers real-time, machine-readable intelligence that highlights the integration capabilities.

- 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 and turns 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.

- Another differentiator offered 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.

Market Perspective:

- 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/

Company Introduction:

Founded in 2007 and headquartered in Tampa, FL, US, ReliaQuest is the provider of a security operations platform titled GreyMatter. The company offers Threat Intelligence (TI) as part of its GreyMatter platform. The GreyMatter platform is built on an open XDR architecture.

Product Introduction:

The GreyMatter platform enables bi-directional integration across security tools, which helps the SecOps teams unify the detection and response process with singular visibility, reduced complexity, and managed risk across the security ecosystem.

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

Technology Perspective:

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

- ReliaQuest's 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 envi-

ronment. Additionally, GreyMatter provides actionable intelligence with track and drill-down threat advisories and weekly intelligence summaries.

- GreyMatter Threat Intelligence offers 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 ability 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's key differentiator is "Bring your Own" threat feeds that allow organizations to add commercially available threat feeds 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.

Market Perspective:

- From a geographical presence 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 vertical perspective, ReliaQuest serves clients across various industries, including healthcare, financial services, retail, hospitality, and technology, among others. ReliaQuest offers several use cases that enhance an organization's cybersecurity posture, including real-time threat detection, proactive threat hunting, malware analysis, and compliance monitoring.

SecurityScorecard

URL: https://securityscorecard.com/

Company Introduction:

Founded in 2013, headquartered in New York. SecurityScorecard is a cybersecurity vendor that provides cybersecurity ratings and risk assessment solutions to help organizations manage and mitigate their cybersecurity risks. The SecurityScorecard platform provides products for supply chain risk, threat landscape, security and risk operations, and cyber insurance.

Product Introduction:

SecurityScorecard platform offers threat intelligence through attack surface intelligence. Attack Surface Intelligence offers a capabilities including global sinkhole network, malware attribution system, and actionable insights.

Technology Perspective:

Following is the analysis of Security Scorecard's capabilities in the global Digital Threat Intelligence Management market:

- SecurityScorecard's Attack Surface Intelligence assists threat hunters in preventing future disruptions by providing global threat data sourced from both the clear and dark web. This data is consolidated within a single platform, to enhance precision and effectiveness in threat detection and response efforts.

- The capabilities offered by SecurityScorecard's Attack Surface Intelligence is the malware attribution system that processes and analyzes thousands of malware samples and indicators of compromise (IOCs) daily. The Attack Surface Intelligence also holds a global data set. The platform's search index relies on scanning a vast array of routable IP addresses every week, covering numerous ports across the globe.

- SecurityScorecard differentiates its offerings from other vendors in the market by offering a global sinkhole network that provides unparalleled insights into infections across a wide spectrum of malware families. This network of-

fers comprehensive coverage and depth, allowing SecurityScorecard to offer visibility into emerging threats and cyber risks.

- SecurityScorecard offers actionable insights aimed at preventing breaches by enabling businesses to identify threat actors likely to target their operations. By providing both strategic and tactical recommendations, the platform enables organizations to minimize exploitability across their attack surface.

Market Perspective:

- SecurityScorecard has a strong presence in the US. From an industry perspective, the company has a presence across a wide variety of industry verticals, including financial services, insurance, healthcare, government, retail & consumer, technology, and enterprise.

- From a use case perspective, SecurityScorecard supports enterprise cyber risk, third-party risk, executive-level reporting, cyber insurance, due diligence, service providers, and compliance.

ThreatBook

URL: https://www.threatbook.io/

Company Introduction:

Founded in 2015, headquartered in Beijing, China. ThreatBook is a cybersecurity vendor that focuses on providing cyber threat intelligence solutions. ThreatBook offers a platform - ThreatBook Security Cloud, which is a combination of cybersecurity Big Data and AI Platform along with SaaS products and services.

Product Introduction:

ThreatBook provides threat intelligence solutions through its ThreatBook Security Cloud. The ThreatBook Security Cloud focuses on security intelligence and has an intelligence extraction system. ThreatBook threat intelligence solution offers capabilities including threat discovery, actionable insights for detection and response, compromise detection, and security alert noise reduction.

Technology Perspective:

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

- ThreatBook offers a range of capabilities with its solution, including threat discovery which consolidates data from multiple sources, and provides a holistic view of the threat landscape, uncovering intricate connections between different threats. ThreatBook leverages a team of professional analysts and employs rigorous quality control within its proprietary intelligence production system.

- Another capability offered by ThreatBook includes actionable insights for detection and response. With this capability ThreatBook provides thorough investigations to mitigate threats which enables organizations to respond promptly to threats, isolate affected systems, or proactively mitigate risks, thereby minimizing the likelihood of severe repercussions.

- ThreatBook offers security alert noise reduction, which minimizes false alerts and uncovers security incidents by extracting domains or IP addresses from

logs collected by Security Operations Centers (SOCs) or Security Information and Event Management (SIEM) systems.

- ThreatBook differentiated its threat intelligence offering from others in the market by providing compromise detection, that detects threats targeting office terminals and servers within production networks or DMZ environments. It enables organizations to effectively safeguard their networks and infrastructure against various cyber threats, enhancing overall security posture and resilience.

- Another differentiator offered is contextual data, which consolidates data and information into clear verdicts, behavioral conclusions, and intruder profiles. It enables SOC teams to streamline their workflow, minimizing time spent on benign activities.

- ThreatBook also provides IP reputation identification, which identifies whether suspicious IPs present risks like scanning, vulnerability exploitation, or botnet involvement. It offers additional attributes such as gateway, IDC (Internet Data Center), CDN (Content Delivery Network), and more, tailored to suit specific business needs.

Market Perspective:

- From a geographical perspective, ThreatBook has a significant presence in the APAC region including China, Singapore, Japan, Thailand, Indonesia, etc. From an industry perspective, ThreatBook caters to the finance, energy, manufacturing, internet, healthcare, etc.

- From a use case perspective, ThreatBook's threat intelligence solution supports early threat detection, incident response optimization, vulnerability management, phishing detection, threat hunting, and compliance and risk management.

ThreatConnect

URL: https://threatconnect.com/

Company Introduction:

Founded in 2011, headquartered in Arlington,VA. ThreatConnect cybersecurity company focused on providing solutions to help organizations mitigate digital threats effectively. ThreatConnect has a ThreatConnect platform that offers tools for managing threat intelligence, orchestrating security operations, and enhancing defenses against cyberattacks.

Product Introduction:

ThreatConnect offers threat intelligence through its Threat Intelligence Operations platform. The ThreatConnect TI Ops platform is an AI-powered solution, that provides centralized and enriched threat intelligence data. It facilitates analysis, prioritization, and action against relevant threats through AI and ML capabilities, automation, and seamless interoperability with enterprise tools.

Technology Perspective:

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

- The ThreatConnect TI Ops platform supports analysts in predicting threats aimed at various industries and enterprises. It enables the implementation of intelligence requirements within the platform, offering insight into attackers' tactics, techniques, procedures, behaviors, and infrastructure.

- ThreatConnect through its TI Ops platform offers capabilities that include, threat graphs. The Threat Graph feature visualizes the connections within your threat intelligence, enabling users to investigate and enrich intelligence data while also initiating automated actions, all through an interactive user interface.

- Another capability offered by ThreatConnect is the ATT&CK Visualizer, it aids in comprehending the behaviors and methods employed by threat actors,

thereby uncovering potential weaknesses in technical controls, and enhancing overall defense strategies.

- ThreatConnect offers additional capabilities including reporting and dashboarding. The reporting and dashboarding capability aids in comprehending the behaviors and methods employed by threat actors, thereby uncovering potential weaknesses in technical controls and enhancing overall defense strategies. Additionally, ThreatConnect provides playbook and task automation, it streamlines processes and increases efficiency by utilizing the drag-and-drop automation feature for Tasks and Playbooks.

- ThreatConnect differentiates its offering from other vendors in the market through their CAL™ which is ThreatConnect's AI-powered global intelligence and analytics feature that offers real-time insights into threats. It includes optimized open-source feeds, as well as unique feeds like the Automated Threat Library and Report Cards for feed performance analytics.

- Another differentiator offered by ThreatConnect is the Intelligence Anywhere feature, which is a browser extension. It provides real-time scanning and identification of pertinent information from any web-based resource, it also seamlessly integrates with the ThreatConnect Platform. Leveraging CAL (Common Attack Language), Intelligence Anywhere identifies and highlights ATT&CK tactics and techniques, while also deconflicting threat actor aliases

Market Perspective:

- From a geographical perspective, ThreatConnect has a significant presence in North America, Europe, Asia-Pacific, and the Middle East region. From an industry perspective, ThreatConnect caters to the finance, healthcare, government, and technology sectors.

- From a use case perspective, ThreatConnect's threat intelligence solution supports threat detection and prevention, vulnerability prioritization, and automated phishing analysis and response.

Threater

URL: https://www.threater.com/

Company Introduction:

Founded in 2014 and headquartered in Tysons, VA, Threater 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 Threater platform includes TI, automation, and network enforcement into a single, simple-to-deploy, and managed solution.

Product Introduction:

The SaaS-based Threater 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. Threater provides its solution through Threater Collect, Threater Enforce, and Threater Marketplace. The Threater Collect acts as a free threat intelligence solution and Threater Enforce is offered as an upgrade of Threater Collect solution.

Technology Perspective:

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

- Threater Collect is a centralized SaaS solution to aggregate all the threat intelligence. Threater Collect provides users with cyber intelligence feeds and lists, access to open-source data, and intelligence to be fed to the firewall. Additionally, Threat Collect provides other capabilities that include, a centralized management for cyber intelligence, user-defined lists, feeds, and intelligence. It also provides the ability to integrate the threat lists and feeds with other security tools and technologies. Threat Collect enables the users to create their list and manage the organization's cyber intelligence. The users can integrate tools and technologies into the collect platform to have a real-time view of the threat landscape.

- Threater Evolve is an extended offering of Threat Collect. Threat Evolve implements and ensures the deployment of updates and real-time enforcement of data across the entire network, effectively preventing known malicious actors from gaining access. Threater Evolve gathers cyber intelligence feeds from various sources to inform enforcement decisions on both inbound and outbound traffic seamlessly.

Market Perspective:

- 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 & e-commerce, media & gaming, healthcare, and digital enterprises, and others.

ThreatQuotient

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

Company Introduction:

Founded in 2013 and headquartered in Ashburn, Virginia, US, 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, investigation, and response.

Product Introduction:

The ThreatQ platform works through a unique DataLinq engine, a Threat Library, dynamic scoring, Smart Collections, customizable data model, and the ThreatQ Marketplace. The platform offers additional modules, of ThreatQ TDR Orchestrator (for orchestration and automation), ThreatQ Data Exchange (for intelligence sharing), and ThreatQ Investigations (for collaborative investigations). The platform offers flexible deployment options, including cloud based, on-prem, virtual instance, and air-gapped.

Technology 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, investigation, and response.

- The ThreatQ platform's key differentiator is 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 detec-

tion and response. The engine aims to add value to existing data and systems that exist in the operational environment.

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

- The platform offers dynamic scoring as a differentiating feature. Dynamic scoring allows customers to define how data is scored within the platform based on the configuration and risk profile. This capability enables an organization to define the characteristics of what threat data is most important to them, and is applied through AI and ML algorithms for scoring/prioritization versus a global scoring mechanism.

- ThreatQ has a customizable data model that allows customers to update their system to support additional object types to meet their business requirements.

- ThreatQ offers a Smart Collections framework where 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 who need to edit/view them can do so.

- ThreatQ also provides ThreatQ Investigations. This cybersecurity situation room is designed for collaborative threat analysis, shared understanding, and coordinated response. ThreatQ Investigations embeds visualization and documentation in a shared environment to allow users to gain a greater understanding of the investigation and focus throughout the analysis process.

- Additionally, ThreatQ Data Exchange enables and manages inter and intra-organization intel collaboration. It uses TAXII to enable bi-directional sharing of all of the intelligence data within the ThreatQ platform and scales sharing

across many teams and organizations of all sizes. Another key capability of ThreatQ is the ThreatQ Marketplace, which includes over 400 integrations of intelligence feeds, security tools, enrichment services, sandboxes, and many more.

- The platform also has a module called ThreatQ TDR Orchestrator, to simplify orchestration and automation through a no-code / low-code approach. ThreatQ enables orchestration through data curation and extracts and simplifies much of the complexity of process-driven playbooks. Through its data-driven approach, the ThreatQ platform can ensure high-fidelity inputs before initiating a playbook execution, therefore reducing the total number of playbooks runs and ensuring relevance and priority of actions taken.

Market Perspective:

- Regarding geographical perspective, ThreatQuotient has a significant presence in North America and Europe, followed by the Middle East, Africa, Asia Pacific, and Latin America. Regarding industry verticals, ThreatQuotient's primary verticals include IT, government and public sectors, banking and financial services, energy and utilities, retail and e-commerce, healthcare and life sciences, education, and manufacturing.

- From a use case perspective, some of the top use cases for ThreatQ includes the aggregation, storage, and analysis of threat data, automation and integration of multiple cyber defense products, creation of bespoke threat intelligence, the curation and delivery of custom threat data as an MSSP or MDR provider, vulnerability prioritization, incident management and response.

Roadmap:

- ThreatQuotient continues to work on its vision for data-driven automation for Threat Intelligence as well as threat detection, investigation and response use cases. It is also adding a data retention policy feature that enables the customers to choose what types of data, from what sources, is retained for how long. The company is also focusing on innovation and leading in risk scoring and prioritization to include additional use cases within SecOps and the wider SOC, resulting in improved business outcomes for the end users.

Trellix

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

Company Introduction:

Founded in 2022 and headquartered in Milpitas, CA, US, Trellix offers products addressing cybersecurity solutions and services, including XDR, endpoint security, SecOps and analytics, data security, network security, threat intelligence, email security, and cloud security. The company provides an XDR platform equipped with advanced cyber threat intelligence.

Product Introduction:

Trellix offers multiple threat intelligence solutions, including Trellix Insights, Trellix ATLAS, Trellix Global Threat Intelligence, Trellix Private Global Threat Intelligence, Trellix Threat Intelligence Exchange, and Trellix Intelligence as a service. Trellix has partnered with Intel 471 to provide improved threat intelligence for Trellix Insights and Trellix ATLAS.

Technology Perspective:

Following is the analysis of Trellix's capabilities in the global Digital Threat Intelligence Management 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 Insights serves as the first line of defense for XDR. It employs a combination of human-machine collaboration to predict threats and suggests straightforward actions to prevent attacks and enhance security infrastructure. This tool monitors global threats, assesses and prioritizes potential risks, employs machine learning for threat analysis, and provides practical protection recommendations ahead of potential attacks.

- Trellix Insights has added a new capability, vulnerability intelligence, which is used for a Common Vulnerability Scoring System (CVSS) for accessing critical vulnerabilities with vulnerability intelligence enrichment.

- Trellix offers a data analysis tool known as Trellix Advanced Threat Landscape Analysis System (ATLAS). The tool collects and consolidates data from various Trellix sources and enriches it with essential details like industry sector and geolocation. Trellix ATLAS supports data enrichment and threat correlation, real-time threat intelligence and contextual threat intelligence, and vulnerability intelligence.

- Trellix offers a cloud-based reputation service titled Global Threat Intelligence (GTI), which is integrated into Trellix products. The service 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. An extension to the GTI service is the Trellix Private Global Threat Intelligence, 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 Threat Intelligence Exchange integrates an organization's local Threat Intelligence (TI) with global insights from sources like Trellix Global Threat Intelligence and external third-party platforms. This collective intelligence is then disseminated throughout the security ecosystem via the Trellix Data Exchange Layer (Trellix DXL). This shared intelligence facilitates a unified response from the organization's security solutions by effectively collaborating to counteract threats and bolster overall security measures. Trellix DXL serves as the conduit for security solutions to join the Threat Intelligence Exchange ecosystem, enabling them to block potential attacks proactively. The focus is on practical collaboration and information sharing to enhance the organization's security posture.

- Trellix Threat Intelligence Exchange (TIE) provides practical features, including customizable threat intelligence, allowing organizations to tailor comprehensive threat information for immediate responses to potential threats. This capability enables security teams within the organization to assemble, override, augment, and fine-tune threat intelligence according to the specific protection requirements for their environment.

- Trellix's key differentiator is 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 performed through Trellix Enterprise Security Manager. It investigates the IoCs identified by the TIE and enhances the security posture by accessing historical security information and creating an automated watch list for the same.

- Trellix also offers a new feature titled 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 provides custom intelligence reporting as well as analysis of domains and IP addresses.

Market Perspective:

- 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's primary use cases include threat detection, threat hunting, threat visibility, and malware and ransomware detection.

ZeroFox

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

Company Introduction:

Founded in 2013 and headquartered in Baltimore, MD. US, 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.

Product Introduction:

ZeroFox External Cybersecurity platform focuses on protection, intelligence, disruption, and response. The platform provides ZerFox intelligence that includes capabilities like intelligence search, dark web operations, physical security intelligence, intelligence feeds, finished intelligence reporting, and dedicated analysts. ZeroFox acquired Looking Glass Cyber Solutions in 2023 to expand its platform's attack surface intelligence capabilities.

Technology Perspective:

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

- The ZeroFox platform offers threat intelligence that allows organizations to collect and analyze extensive threat data. ZeroFox tailors its threat intelligence as per the specific security requirements of each organization. The platform also provides access to threat research from the dark web and delivers insights for organizations to respond effectively. The platform utilizes AI processing, deep learning algorithms, and black ops agents to sift through extensive datasets on the surface, deep, and dark web to provide pertinent, timely, and actionable intelligence.

- ZeroFox offers a dark web ops approach by curating relevant intelligence and monitoring threats important to specific organizations. The DarkOps capability

provides real-time underground intelligence, special investigation, preemptive intelligence, bad actor attribution, breach containment, and risk mitigation. It also provides identification of data and content exposure to ensure compromised intellectual property recovery, threat actor engagement, and information about malware infections.

- ZeroFox also offers an intelligence search capability that offers a searchable interface to access ZeroFox's extensive threat intelligence data lake, covering various aspects such as attacks, threat actor details, and indicators of compromise. The capability enables the organization to search across a massive database, gain direct access to incidents, and benefit from analyst-curated findings.

- ZeroFox also provides threat intelligence feeds capability. The 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 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's key differentiator is on-demand investigations. ZeroFox provides a team of experienced investigative specialists and expert analysts to conduct risk assessments and investigations and delivers finished intelligence reports. This capability supports third-party attack surface assessment, after-hours support, managed access to international data sources, deep-dive analysis for global threats, and foreign language interpretive skills.

- ZeroFox also provides 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.

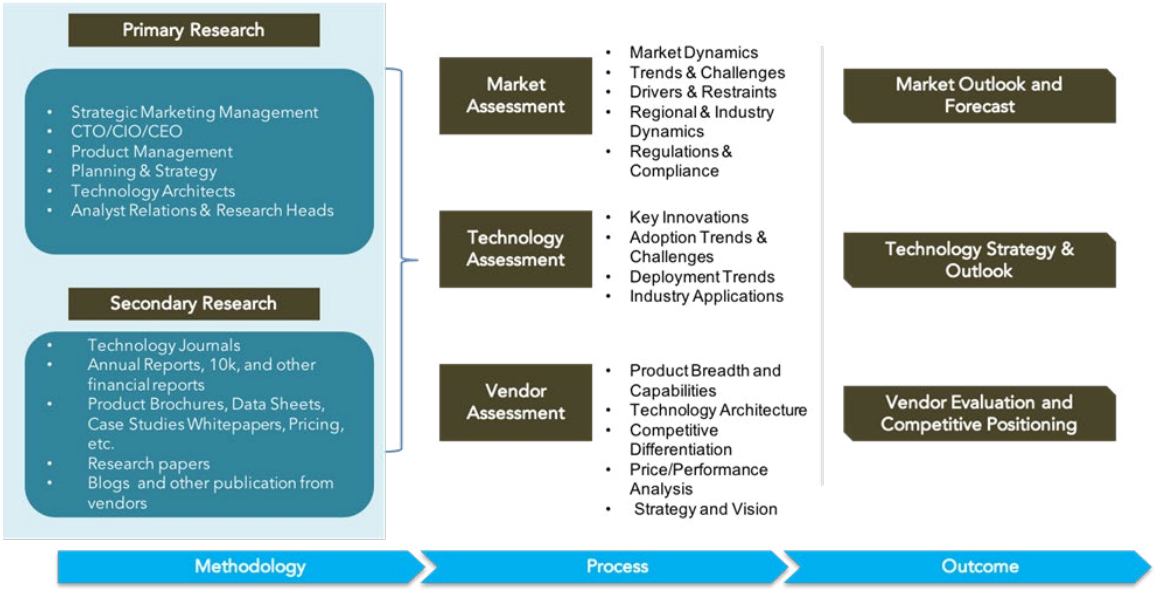
- ZeroFox also supports managed intelligence services and dedicated analysts. The company's managed intelligence services provide external threat experts to help organizations get insights about critical risks and offer effective responses. The dedicated analysts provide support to the client organization's security team and deliver intelligence tailored to the organization's security goals.

Market Perspective:

- From a geographical presence perspective, ZeroFox has a strong presence in the US, followed by the UK, Australia, and India. From an industry vertical perspective, the company's primary verticals include 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
- 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, 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 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