MARKET PERSPECTIVE

The Strategic, Operational, and Tactical Dimensions of Threat Intelligence: A Vendor Perspective

Monika Soltysik Christopher Kissel

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: The Strategic, Operational, and Tactical Dimensions of Threat Intelligence — A Vendor Perspective

This IDC Market Perspective explores the three intricacies of threat intelligence: strategic, operational, and tactical. It differentiates between these aspects of intelligence and highlights their unique capabilities and applications. By showcasing how participating vendors contribute, the document offers a distinctive view of how this intelligence is applied across various use cases, emphasizing their unique features and capabilities.

Key Takeaways

- The cyberthreat environment is rapidly evolving with sophisticated ransomware, nation-state cyberactivities, and the innovative use of GenAI by adversaries, underscoring the need for advanced threat intelligence.
- The strategic, operational, and tactical layers of threat intelligence are crucial for a comprehensive understanding and management of cyberthreats, each serving a distinct yet interconnected role.
- Regional regulations significantly influence the deployment and application of threat intelligence globally, highlighting the necessity for tailored approaches in different markets.
- There is a shift from traditional malware signature feeds to more complex needs like data science–driven intelligence and global adversarial tracking, demanding more sophisticated solutions from vendors.

Recommended Actions

- Ensure comprehensive integration of threat intelligence platforms with diverse technology stacks to facilitate a cohesive and efficient incident response and enhance overall security operation effectiveness.
- Develop artificial intelligence algorithms within threat intelligence systems that are transparent and easily understandable, fostering greater trust and clarity in decision-making processes.
- Actively collaborate with industry organizations to standardize threat intelligence practices and ensure compliance with international data privacy regulations.
- Innovate to create user-friendly tools and resources in threat intelligence, making them accessible and beneficial for both security professionals and nontechnical staff.

Source: IDC, 2023

December 2023, IDC #US51451823

NEW MARKET DEVELOPMENTS AND DYNAMICS

The need for effective global threat intelligence (TI) is growing as world events make the environment more complex and uncertain for businesses and consumers. Threat actors are developing, with new groups and threats appearing around the world. They are also finding new ways to use or carry out old tactics and methods. Ransomware is a big problem for many organizations globally, as these groups grow in size and complexity. This includes working together with other threat actors on online forums. While GenAI is the rage in cybersecurity, the adversary can use these tactics as well enabling adversary to devise tricks that manipulate individuals into giving away access to their devices or personal information as campaigns are becoming more customized toward the intended target. In addition, cyberattacks are increasingly being used for political, economic, and territorial goals by nations engaging in spying, warfare, and misinformation, as seen in activities in Ukraine, Taiwan, Israel, and other areas.

As organizations depend more on threat intelligence to spot and handle cyberthreats, the threat landscape keeps changing. To assist organizations in this complex situation, leading companies have identified different types of threat intelligence to help make better security decisions.

Introduction

In today's rapidly evolving digital landscape, where cyberthreats are an ever-present danger, understanding the multifaceted nature of threat intelligence becomes crucial. Neglecting its proper application can lead to significant risks and vulnerabilities for businesses, impacting their security posture and operational integrity. This document delves deep into the essence of threat intelligence, which is structured around three pivotal layers: strategic, operational, and tactical. Our exploration is enriched by insightful survey responses from leading threat intelligence vendors, offering a unique perspective on the complex interplay of these layers.

The objective in this IDC Market Perspective is not only to differentiate between these aspects of intelligence but also to highlight their unique capabilities and applications. This comprehensive document aims to provide a clear, engaging, and in-depth analysis of the intricacies of threat intelligence. By showcasing the contributions of participating vendors, we offer a distinctive view of how this intelligence is applied across various use cases with distinctive features and capabilities.

Harmonizing the Layers and Goals of Threat Intelligence

In the complex arena of cybersecurity, the essence of threat intelligence is uniquely encapsulated in three distinct yet interrelated layers: strategic, operational, and tactical. Each of these layers plays a pivotal role in achieving a set of critical goals that collectively shape a robust threat intelligence strategy.

This three-layered approach is important conceptually but realize that a threat intelligence vendor must be proficient in all three aspects. If you think about the history of threat intelligence, it could be roughly classified as malware signature feeds and reports about cyberattackers. This was great technology, but threat intelligence needs have changed because (unfortunately) the adversary is becoming faster and more lethal. As we describe the strategic, operational, and tactical aspects of threat intelligence, envision how data science, global adversarial tracking, and the charting of new tactics and novel threats are gathered and refined to empower security operations and how threat intelligence is used to improve security tools and tighten security posture assessment going forward.

Strategic Threat Intelligence for Real-Time Data Analysis and Decision-Making

Strategic threat intelligence, with its focus on long-term trends and motivations behind cyberthreats, is vital for enabling real-time data analysis. This aspect is crucial in a world where threats rapidly evolve, necessitating that threat intelligence solutions be capable of swift and agile analysis.

Operational Threat Intelligence Integrated into Security Operations

Operational threat intelligence centers on the practical application of intelligence in day-to-day security operations. This layer's seamless integration into security operations emerged as a key theme from our surveys. It plays a critical role in ensuring that intelligence is not only gathered but also effectively implemented in operational decisions, enhancing the responsiveness and efficacy of security measures.

Tactical Threat Intelligence and the Balance Between Automated and Human Analysis

Tactical threat intelligence, the most granular layer, focuses on the immediate, technical indicators of threats. This layer exemplifies the need for a balance between automated and human analysis. In an era where artificial intelligence (AI) and machine learning (ML) are prevalent, our discussions with vendors have highlighted various strategies to maintain this balance, ensuring that technology aids but does not replace the crucial human element in threat analysis.

By aligning these three layers of threat intelligence with their respective goals, we create a synergistic framework that is not only comprehensive but also highly effective in addressing the multifaceted nature of cyberthreats. This approach, informed by rich vendor insights, positions us to navigate the complexities of cybersecurity with a more nuanced and proactive strategy.

Threat Intelligence Vendors and Clientele Is Global

The largest global regional consumer of threat intelligence is the United States. IDC estimates roughly 65% of TI revenue that comes from United States-based business (see *How Global Threat Intelligence Vendors Address the Nuances of Regional Markets,* IDC #US49127923, February 2023). However, globally different regulatory standards shape how threat intelligence can go to market, take for example the German Privacy Act Bundesdatenschutzgesetz (BDSG) that sets strict guidelines on how data collection and data processing is enabled in Germany. The net effect is that data containing personally identifiable information (PII) does not travel outside of German borders. These vendors, operating outside of the United States, have to navigate different regulatory landscapes, including strict data protection laws like the BDSG in Germany. For instance:

- Cyberint and Cybersixgill, both based in Israel, would need to consider how their data collection and processing align with the stringent privacy regulations in the European Union (EU), including Germany. Their global operations imply a need to comply with various national laws regarding data privacy and cross-border data transfer.
- CYFIRMA, with operations in Singapore, the United States, Japan, India, and potentially catering to clients in Europe, would similarly need to ensure compliance with regional data protection laws.
- ESET, headquartered in Slovakia and operating globally, would have to be particularly mindful of EU regulations (like GDPR and BDSG) when handling data, especially PII, ensuring it adheres to the principles of data minimization and locality.

Evolution of Threat Intelligence

Cybersecurity is a constantly evolving field that requires organizations to stay ahead of the curve and anticipate the next move of their adversaries. One of the key tools that enables this proactive approach is threat intelligence. Threat intelligence has evolved significantly over the past decade, allowing organizations to proactively identify and mitigate cyberthreats. In addition to this, by leveraging threat intelligence data, they can better understand their risk profile and develop comprehensive security strategies that protect against malicious actors. Furthermore, through advanced analytics capabilities such as machine learning algorithms, threat intelligence solutions are able to quickly detect potential risks and provide real-time notifications about emerging threats so that companies can take appropriate action before an attack occurs. As a result of this increased visibility into the cyberlandscape, businesses are now able to more effectively manage their digital risk while simultaneously improving overall cybersecurity posture.

Breaking Down Vendors' Capabilities in Strategic, Operational, and Tactical Threat Intelligence

Strategic Intelligence

Strategic intelligence is nontechnical, risk-based intelligence used by high-level decision makers. Strategic threat intelligence is focused on identifying and assessing threats at a high level, understanding the motivations and capabilities of potential threat actors as well as the potential impact of a threat on the organization's overall goals and objectives. This type of intelligence is used by decision makers that are responsible for allocating resources and budgets and in protecting assets.

Key capabilities include insights into long-term trends and motivation of threat actors, executive reports and KPIs, industry-specific reports, and geopolitical trends.

Insights into Long-Term Trends and Motivations of Threat Actors

Common Themes and Execution

Vendors focus on aggregating data from diverse sources like open source intelligence (OSINT), commercial feeds, threat bulletins, underground forums, and the dark and deep web, along with technical indicators, to discern the long-term trends and motivations of threat actors. The use of dashboards and visual tools like Threat Graphs, MITRE ATT&CK Visualizers, and Threat Maps is common for tracking threat actors and trends; tactics, techniques, and procedures (TTPs); and indicators of compromise (IoCs). These tools aid in pattern recognition and decision-making, while predictive analytics and historical context provide a deeper understanding of the evolution of threat actors. This comprehensive approach combines rich data sets and advanced visualization for proactive cybersecurity strategies.

Vendor Examples

- Analyst1 aggregates tactical and strategic threat intelligence from various sources and extracts unique insights aligned with organizational-specific priority intelligence requirements (PIRs). The platform offers powerful visualizations to represent changes over time.
- Anomali provides threat bulletins that describe additional trends and motivations of threat actors, along with separate threat actor profiles.
- CrowdStrike provides insights into long-term trends and motivations of named adversaries across different threat landscapes. CrowdStrike's Falcon cloud-native platforms offer detailed adversary profiles, reports, MITRE ATT&CK mapping, and kill chain analysis.

- Cybersixgill analyzes data from deep and dark web, social media, and closed sources to provide contextual insight into cybercriminal discourse, activity, motivations, peer networks, and capabilities. The platform tracks evolving tactics, techniques, and procedures of threat actors over time.
- Flashpoint offers insights into long-term trends and threat actor motivations through data analysis, historical context, industry specialization, behavioral analysis, and predictive analytics. It provides Flashpoint Finished Intelligence (FINTEL) and Threat Actor Profiles.
- Fortra's PhishLabs leverages threat and vulnerability data sets from various sources, including third-party data sources, to investigate threat actors, campaigns, trends, and other items of interest.
- Intel 471 provides comprehensive intelligence into threat actors, their communication channels, malware, vulnerabilities, and TTPs. The TITAN platform focuses on delivering accurate linkages between threat actors, their motivations, and their tactics.
- Mandiant utilizes various sources for its threat intelligence, including internal data lakes, threat hunting activities, and open source intelligence. This broad spectrum of data sources allows Mandiant to cross reference and validate the long-term trends and motives observed in threat actors' activities.
- Recorded Future utilizes Intelligence Graph to index, organize, and analyze adversary and victim data from various sources. It offers threat maps, trend analysis, and insights into threat actor motivations through dedicated threat research.
- ThreatConnect utilizes ATT&CK Visualizer and Threat Graph features to visually display threat intelligence data, uncovering patterns and relationships. The combination allows correlation of data across multiple sources and generates threat bulletins.
- ThreatQuotient offers a unified perspective on threat actors and campaigns by aggregating and correlating data from multiple sources. ThreatQ provides dashboard capabilities to track threat actors, including trends, associated tactics, techniques, and indicators.
- ZeroFox monitors and analyzes data from a variety of sources, including the surface, deep, and dark web. The approach includes maintaining detailed profiles of threat actors and conducting in-depth analysis of their tactics, techniques, and procedures. It also maintains a collection of threat actor profiles sourced from databases like MITRE ATT&CK.

Insights into Global and Geopolitical Trends

Common Theme and Execution

Vendors integrate geopolitical trends into threat intelligence platforms (TIPs), acknowledging the connection between global political dynamics and cyberthreats. These platforms utilize a range of data sources like open source intelligence, deep and dark web, signals intelligence (SIGINT), and proprietary data to offer a comprehensive analysis of threats. Advanced analytics correlate cybersecurity incidents with geopolitical events to identify patterns and potential threats. The focus is both on detailed analysis of threat actors in relation to geopolitical shifts and on selective aspects relevant to cybersecurity. Customizable dashboards and reporting tools are tailored to specific geopolitical contexts, allowing for focused analysis on certain areas or sectors. Continuous updates and monitoring keep the intelligence up to date, reflecting the ever-evolving geopolitical landscape and its implications for cyberthreats.

Vendor Examples

- Analyst1 proprietary analytics engine, which automatically extracts and reconciles information about threat actors and builds complex relationships, offers a unique angle in threat

intelligence. The ability to track changes in relationships and tactics over time provides a dynamic view of the threat landscape influenced by geopolitical factors.

- CrowdStrike tracks over 115 nation-state adversaries leveraging technical data sources, including its own Falcon Platform with endpoints in over 180 countries. Its methodology includes processing millions of malware samples; collecting intelligence from deep and dark webs, criminal forums, and social media; and operating honeypots across the internet.
- Flashpoint dynamically escalates online activities into targeted attacks and vice versa. Its focus is on all-source collection, including OSINT, SIGINT, and D/DW, for understanding triggers and scenario analysis.
- Intel 471 aligns its reporting methodology with evaluation techniques used by U.S. government, law enforcement, and NATO partners. This approach, focusing on enriched evaluation and detailed reporting including malware intelligence, vulnerability intelligence, and breach alerts, enhances the speed and clarity of understanding and responding to threats.
- Mandiant operates in over 28 countries with a team of analyst researchers proficient in 33+ languages positioned to gather and interpret threat intelligence from various parts of the world, providing a global perspective.
- Recorded Future offers a dedicated analysis of geopolitical threats with a unique focus on the convergence of cyberthreats and geopolitical threats. Its use of ontology relationships to connect entities and uncover trends is distinctive, offering a complete risk picture at various levels, from country to city to facility specific.

Executive Reports and Key Metrics

Common Theme and Execution

The emphasis is on providing clear, concise, and actionable intelligence summaries that focus on the most relevant threats and trends. Key metrics often include threat actor tactics, impact assessments, and threat landscape trends. Reports are tailored and often customizable to specific audience needs, offering both high-level overviews and detailed analyses.

Vendor Examples

- Analyst1 enables the creation of visualizations through *a no-code* dashboarding interface, catering to both tactical monitoring and strategic analysis in its executive reporting.
- Anomali focuses on providing executive reports that include both a summary of current team activities and detailed information on threats specific to the customer's environment or industry.
- CrowdStrike delivers executive-level reports that highlight trends across various threat types and offers situational awareness of the global threat landscape, focusing on metrics like breakout time and adversary activity.
- Cybersixgill monitors and analyzes geopolitical trends impacting cybersecurity, using a comprehensive range of data sources for threat landscape assessment and detailed report generation.
- Fortra's PhishLabs tailors key metrics in its executive reports based on the report's focus, such as providing detailed insights into the phishing threat landscape.
- Flashpoint communicates trends in the evolving threat landscape and provides detailed impact assessments of threat intelligence findings, alongside sharing a strategic road map for threat intelligence.

- Mandiant offers a comprehensive view of cyberthreats designed to inform strategic decision including cyberthreat profiles and discovered assets of exposure.
- ThreatConnect utilizes its platform for centralized production, management, and sharing of reports, emphasizing key metrics like analyst effectiveness, MTTR/mean time to detect (MTTD), ROI, and bespoke customer metrics.
- ThreatQuotient offers robust capabilities for dashboard and report customization, enabling executive-level reports to be tailored for understanding threats and assessing potential risks within an organization's infrastructure.
- Recorded Future provides executive reports in categories such as threats for enterprises, specific threats, and intelligence maturity, employing advanced visualization and in-depth research reports for analysis.

Operational Threat Intelligence

Operational threat intelligence provides real-time, actionable insights into threats, risks, and TTPs by collecting and analyzing data from various sources, with the goal of reducing mean time to detect.

Key capabilities include real-time actionable insights, alerts and mechanism for alerting and incident response, speed of intelligence distribution to defense tools, handling of false positives, and threat feeds.

Real-Time Actionable Insights

Common Themes and Execution

Vendors focus on advanced technology, particularly AI and machine learning for processing and analyzing vast quantities of data to provide timely and accurate identification and scoring of cyberthreats such as malware, ransomware, and advanced persistent threat (APTs). Execution techniques include the integration of AI-driven platforms into existing security infrastructure, use of sophisticated algorithms, prioritizing threats based on severity and reliability, ensuring relevant and actionable intelligence. In addition, vendors commonly employ customizable dashboards for targeted monitoring and advanced data collection methods, including automated techniques for sourcing information from the surface, deep, and dark web. This comprehensive approach allows organizations to receive real-time alerts and updates, enabling them to respond quickly and effectively to emerging threats.

Vendor Examples

- Anomali uses an AI system named Macula to score data from over 100 sources, providing insights on the severity and type of threats.
- CrowdStrike stands out with its real-time threat feed, sourced from a static malware analysis platform processing millions of samples per day and real-time monitoring of the criminal underground through Falcon intelligence Recon.
- Cybersixgill emphasizes its asset-based alerting capabilities, continuously monitoring data from the deep, dark, and clear web to provide early warnings of threats targeting specific organizational assets.
- Mandiant monitors the open, deep, and dark web to provide real-time awareness of threat that includes information on targeting the company, VIPs, technical resources, and trusted relationships.
- ThreatQuotient combines internal data production with external source ingestion, offering manual and automatic scoring within its ThreatQ platform.

- Recorded Future provides real-time analysis of malicious infrastructure and targeted threat monitoring, using integrations with various security systems for comprehensive threat attribution.
- ZeroFox combines extensive real-time monitoring with advanced AI-driven analysis to rapidly identify and assess cyberthreats across the surface, deep, and dark web. Its team of analysts further enhances this process by validating and triaging alerts, ensuring that clients receive accurate and actionable insights.

Alerts and Mechanism for Incident Response

Common Themes and Execution

Alerts and mechanisms for incident response among threat intelligence vendors emphasize proactive, real-time alerting, and integration with existing security operations and incident response workflows, prioritizing timely and actionable alerts that are based on a comprehensive analysis of a wide range of data sources, including the deep and dark web, open source intelligence, and proprietary data. The focus is on delivering intelligence that is not only immediate but also contextual and relevant to specific threats and organizational needs.

Vendor Examples

- Anomali utilizes an AI system named Macula to score threat data. This system processes data from over 100 sources, providing real-time alerts that include details on the origin, severity, and type of threats such as malware, ransomware, and APTs. The scoring system aids in prioritizing alerts based on confidence levels.
- CrowdStrike offers a real-time threat feed created by processing millions of malware samples daily. Its Falcon platform provides insights into threats blocked at endpoints, while Falcon intelligence Recon monitors the criminal underground in real time. This multilayered approach ensures that alerts are timely, detailed, and relevant for effective incident response.
- Cybersixgill continuously monitors data from the deep, dark, and clear web. Its asset-based alerting capabilities focus on real-time monitoring of discovered organizational assets, providing early warnings of targeted threats. Alerts can be delivered via email or integrated with existing security systems for a streamlined response.
- Intel 471 delivers near-real-time alerts keyed to customer-specific watcher lists. Its approach includes intelligence on malware families, botnet configurations, and other indicators, enabling proactive security. The platform's integration with tools like VirusTotal and ReversingLabs augments its capabilities, providing a powerful extension for incident response.
- ThreatConnect uses customizable dashboards constructed from various data cards to monitor real-time information, leveraging its ThreatConnect Query Language (TQL). This approach allows for the creation of detailed and specific views on threats, facilitating efficient incident response based on the organization's unique requirements.
- ThreatQuotient combines internal data production with external source ingestion in its ThreatQ platform. It offers both manual and automatic scoring for aggregated and normalized information, which aids in surfacing relevant threats. Its platform also supports external sharing, native security orchestration, automation, and response (SOAR) capabilities, and an investigation workbench, providing a comprehensive toolset for incident response.
- Recorded Future provides real-time analysis of malicious infrastructure and threats both within and outside an organization's environment. The company's integration with SIEM, endpoint detection and response (EDR), and other systems, along with its Collective Insights feature,

allows for comprehensive threat attribution and monitoring, crucial for timely incident response.

Handling of False Positives

Common Themes and Execution

In handling false positives, threat intelligence vendors primarily focus on machine learning and automated processes for identifying and distinguishing threats, supplemented by expert human analysis. These systems are enhanced with scoring and indicator weighting to prioritize threats, while whitelisting and customization features enable users to manage known nonthreats effectively. In addition, strategies like data retention for reevaluation and community sharing provide a comprehensive approach, ensuring that threat intelligence remains accurate and adaptable to the evolving cyberthreat landscape.

Vendor Examples

- Analyst1 uses an intelligence verification workflow in its platform based on hands-on analyst experience.
- Anomali uses machine learning to check against a list of known indicators and retains data flagged as false positives for possible future reevaluation.
- CrowdStrike combines human analysis, machine learning, and validation through its Threat Graph, along with indicator deduplication and enrichment.
- Cybersixgill uses a mix of machine learning, human review, and threat intelligence sharing, along with customizable alert options.
- Flashpoint and Fortra's PhishLabs focus on alert curation and expert analyst review to reduce false positives.
- Intel 471 emphasizes multiple layers of review, including human intelligence expertise, to minimize false positives.
- ThreatConnect allows analysts to manually annotate false positives and uses community-reported false positive information to influence scoring mechanisms.
- ThreatQuotient implements an indicator scoring system, allows whitelisting of non-malicious indicators, and employs automatic expiration for stale intelligence.
- Recorded Future utilizes a multivariate model and a support team for addressing false positives, with options for clients to exclude any identified false positives.

Integrations

The overarching theme in the integration strategies of these cybersecurity vendors with other technology stacks revolves around two primary methods: integration through partnerships and the use of APIs. Many vendors establish strategic partnerships with other technology providers to create seamless, collaborative solutions that enhance overall security capabilities. This approach often leads to more deeply integrated systems, offering a unified security experience. Concurrently, the use of APIs is a prevalent method, allowing for flexible and customizable integration with a wide range of existing security tools and infrastructures. This dual approach — partnerships for comprehensive solutions and APIs for customization and flexibility — underscores the vendors' commitment to interoperability and the enhancement of the overall security ecosystem.

Planning and Execution of Specific Cybersecurity Operations

Common Theme and Execution

Vendors focus on proactive and reactive planning, integrating threat intelligence into cybersecurity operations, and using automated tools and platforms to enhance threat detection, analysis, and response capabilities.

Vendor Examples

- Anomali emphasizes proactive and reactive planning by integrating threat intelligence into customer environments, allowing for the anticipation and prevention of potential attacks.
- Analyst1 assists in planning by identifying relevant threat intelligence and deploying detection and mitigation content through automation.
- CrowdStrike supports tasks like detection, investigation, incident response, vulnerability management, threat alerting, expert malware analysis, domain takedowns, and security operations center (SOC) workflow automation.
- Cybersixgill features automated alerts, partnerships with SOAR and security automation tools, and generative AI capabilities for end-to-end threat protection, reducing response times through automated workflows and playbooks.
- Flashpoint offers intelligence support, program building, tabletop exercises, and retainer services.
- Fortra's PhishLabs consolidates intelligence across multiple solutions, providing insights into security functions, threat trends, and effective utilization by peer organizations.
- Mandiant provides several services and tools focused on actionable intelligence, continuous monitoring, and validation of security measures to aid in planning and executing effective cybersecurity strategies.
- ThreatConnect provides visual tools like ATT&CK Navigator and Threat Graph for cyberthreat intelligence (CTI) teams, alongside features for SOC Analysts, Threat Hunters, and Incident Responders such as Workflows and Low-Code Automation.
- ThreatQuotient offers the "Cyber Situation Room" with ThreatQ Investigations, enabling coordinated planning and response operations through interactive tools, timelines, and multiteam interfaces.
- Recorded Future provides services for threat identification, prioritization, operational planning, incident response, communication, training, awareness, improvement of preventative measures, and resource allocation.

Tactical Intelligence

Tactical intelligence is technical in nature and involves identifying simple indicators of compromise (IoCs) such as bad IP addresses, URLs, file hashes, and known malicious domain names. Tactical threat intelligence helps security teams understand the tactics, techniques, and procedures employed by threat actors, enabling them to develop effective countermeasures and response strategies:

Key capabilities include in-depth information about specific threats and attackers to support threat hunting, incident response, and security planning; understanding attacker tactics, techniques and methods and procedures, and developing threat models; network traffic analysis to help identify specific malware infections, track the movement of attackers within a network, and gather evidence of attacks; support of the planning and execution of specific cybersecurity operations; and identifying IoCs.

Examples of tactical threat intelligence in action include indicators of compromise that can be used to identify a security threat or attack that can include IP addresses, domain names, file hashes, and other artifacts associated with threats or attackers. Another aspect involves analyzing malware samples to understand their capabilities, behaviors, and potential impact on organizational systems. In addition, threat actor profiling is utilized to identify their motives, capabilities, and tactics.

Malware, Threat Actors, and Attack Methods Monitored by TIP/TISS Platforms

Vendor Examples

- Anomali monitors all types of malware and attack methods, focusing on understanding indicators of compromise and their associations with specific threat actors and their tactics, techniques, and procedures.
- Analyst1 tracks a wide array of malware, threat actors, and attack methods based on intelligence reports and human analysis inputs.
- CrowdStrike covers hundreds of malware families and over 220 adversaries, categorizing them by motivation. The company uses MITRE ATT&CK for categorizing attack methods and constantly updates its intelligence based on a wide range of sources, including its Falcon sensor endpoints.
- Cybersixgill monitors a broad spectrum of malware, threat actors, and TTPs, sourcing intelligence from clear, deep, and dark web sources. The company offers an extensive entity database with detailed information on various threat entities, including related TTPs, activity analysis, and related IoCs.
- Flashpoint focuses on the MITRE ATT&CK framework for monitoring threats.
- Intel 471 operates in underground forums, gathering intelligence in pre-attack stages. The company provides both automated and manual early warnings, offering insights into the planning stages of threat actors.
- Mandiant tracks and monitors, primarily through its Mandiant Advantage platform, a wide array of cyberthreats including over 3,000 threat actors and 3,600+ malware families.
- ThreatConnect provides comprehensive coverage of all types of indicators, fully supporting MITRE ATT&CK tactics, techniques, and subtechniques. The platform serves as an aggregation point for various threat intelligence sources.
- ThreatQuotient offers customer-controlled monitoring, where users can choose to monitor any combination of malware families, threat actors, and attack methods through objects within the Threat Library. This data can be sourced from the ThreatQ Marketplace or custom data used by the organization.
- Recorded Future monitors over 155,000 malware types, 10,000 threat actors, and various attack methods, integrating MITRE ATT&CK TTPs across multiple domains like enterprise, ICS, mobile, and cloud.
- ZeroFox collects malware that is sourced through community sandboxes and proprietary means. It conducts both static and dynamic analysis on malware samples, providing metadata and deeper insights for unique malware families.

Indicators of Compromise

Common Themes

A prevalent theme is the extensive coverage of basic IoCs, including IP addresses, URLs, domain names, file hashes, and email addresses. These indicators frequently extend to more specialized categories, highlighting the platforms' capabilities in distinguishing between general and specific threat

types, such as differentiating malware-associated IPs from generic ones. Another notable theme is the emphasis on advanced threat indicators, encompassing business email compromise (BEC), ransomware, credential phishing, and brand threat indicators. This includes a focus on details like malicious senders, attachments, and look-alike domains. In addition, there's a significant trend toward tracking sophisticated elements like command and control (C2) infrastructure, malicious social media handles, and various malicious file types.

Vendor Examples

- Anomali offers over 130 types of IoCs, including basic ones like IP, URL, domain, hash, and email, which further break down into more specific categories like malware IP versus generic IP.
- ThreatQuotient and ThreatConnect aggregate dozens of indicator types, including standard ones like IP addresses, URLs, file hashes, and ATT&CK IDs depending on the feed.
- Flashpoint focuses on malware-related IoCs.
- Fortra's PhishLabs provides a comprehensive array of indicators of compromise, including email threat indicators (such as Office 365 lures, business email compromise, ransomware, credential phishing, malicious senders, and look-alike domains), brand threat indicators, malicious files and IP addresses, command and control infrastructure, web mail accounts, and stolen credentials, among other elements.
- Intel 471 emphasizes malware intelligence with IoCs derived from its TRAP system, covering malware C2 infrastructure, botnet IPs, malware hashes, and URL/domain data.
- Analyst1 supports all atomic IoC types and offers dynamic signature-based detection content for various formats.
- Recorded Future provides both traditional IoCs (IPs, domains, URLs, and hashes) and TTPs, including behavioral hunting rules and analysis of malicious infrastructure protocols.
- CrowdStrike offers a real-time IoC feed including hashes, URLs, domains, IP addresses, and various other types, enriched with detailed information such as malware family and related actors.
- Cybersixgill includes a vast database of IoCs like file hashes, IP addresses, domains, and URLs accessible through its Darkfeed and entity database, with additional generative AI capabilities.

Vulnerability Assessment

Common Themes

Vendors conduct vulnerability assessments within their TIP/threat intelligence security service (TISS) that revolves around integrating and enriching vulnerability data, often in collaboration with other security tools and platforms.

Vendor Examples

- Anomali focuses on ingesting and enriching vulnerabilities, with capabilities to integrate with vulnerability management (VM) systems for data enrichment.
- ThreatQuotient conducts assessments through integration with VM partners like Tenable, Qualys, and Rapid7, adding context to vulnerability intelligence and correlating it with internal data for prioritization.

- ThreatConnect uses its platform to consume and analyze threat and vulnerability intelligence, integrating features for collaboration between CTI and vulnerability management teams. It also includes cyber-risk quantification for prioritization.
- Fortra's PhishLabs provides insight for threat intelligence offerings through its solutions in vulnerability management and offensive security, including Beyond Security, Digital Defense, Core Security, and Cobalt Strike.
- Intel 471 enhances data automation and enrichment through integrations with other TIPs, pairing well with its adversary, malware, credential, and vulnerability products.
- Analyst1 integrates with leading vulnerability management platforms like Tenable and Rapid7, correlating internal vulnerabilities with external threats for patch prioritization and automated incident generation.
- Recorded Future identifies external attack surfaces and vulnerabilities, including weak configurations, and monitors vulnerability scan results for life-cycle changes, assigning dynamic risk scores.
- CrowdStrike provides dynamic context on vulnerabilities, assessed using both human and machine analysis. The company focuses on exploit prioritization and confidence levels derived from various internal and external data sets.
- Cybersixgill offers a proprietary scoring system for CVEs, the DVE score, using machine learning to correlate vulnerability information with threat intelligence data, focusing on vulnerabilities actively targeted by threat actors.
- Mandiant Advantage Attack Surface Management (ASM) offers continuous monitoring for vulnerabilities and misconfiguration, while its Security Validate services allow organizations to test and validate their security posture against specific threats.

Correlation of Operational, Tactical, and Strategic Threat Intelligence

Common Themes

Vendors integrate and correlate operational, tactical, and strategic threat intelligence through a combination of advanced technologies, integration capabilities, and intelligence processing methods.

Vendor Examples

- Anomali uses machine learning (through Macula) to score and categorize indicators, focusing on new, tactical threats and moving older data to an inactive state. This approach emphasizes the importance of current, actionable intelligence.
- ThreatQuotient approach involves a robust ecosystem of integrations and an adaptive data engine (DataLinq) for managing key data steps including ingestion, normalization, correlation, prioritization, and translation. This shows the emphasis on handling diverse data sources and continuous updating of threat intelligence.
- ThreatConnect designed a platform built around the concept of associations for pivoting between different intelligence levels. This is complemented by visual analytics (Threat Graph), API integrations, and custom dashboards, indicating a focus on contextual understanding and flexibility in intelligence analysis.
- Fortra's PhishLabs and Intel 471 emphasize sourcing intelligence from a variety of security solutions and closed-source environments, highlighting the value of diverse intelligence sources for comprehensive operational, tactical, and strategic insights.

- Analyst1 uses bidirectional SIEM integrations for tactical correlation, allowing for automated indicator correlation and instant threat awareness. This points to the importance of seamless data flow between TIPs/TISS and other security systems.
- Recorded Future focuses on providing a consistent set of prioritized intelligence across an organization, derived from strategic priorities and operational context. This approach underlines the need for intelligence that is directly relevant to the organization's specific risk and operational framework.
- CrowdStrike utilizes real-time correlation and automation capabilities, integrating various types of intelligence and providing both machine-readable and human-readable formats. The company's approach shows an emphasis on real-time updates and accessibility of intelligence.
- Cybersixgill offers features for integrating operational, tactical, and strategic intelligence, with use-case specific dashboards and asset management modules for a comprehensive view of threats. This indicates a focus on holistic integration and the ability to pivot between different intelligence levels.

Vendor Profiles

While the representative sample vendor profiles in the Detailed Participant Profiles: Insights from the Intricacies of Threat Intelligence Questionnaire section are derived from vendors that participated in the three aspects of the Threat Intelligence Questionnaire, it would be remiss not to mention other key players such as ZeroFox, ReliaQuest, OpenText, and Cyberint – these vendors are mentioned in the Prominent Industry Players section.

Prominent Industry Players

ZeroFox

ZeroFox offers a comprehensive suite of threat intelligence security services through its agentless software-as-a-service (SaaS) platform, focusing on external data collection. Its integrated service portfolio includes domain monitoring, brand/social media monitoring, executive protection, adversary disruption/takedowns, physical security intelligence, intelligence search, and intelligence feeds. These services are complemented by additional capabilities such as OnWatch Expert Dedicated Analyst, OnDemand Investigations, and Dark Ops threat actor engagement services. The platform's sophisticated threat intelligence data lake and analytics engine enable proactive monitoring and strategic mitigation, ensuring comprehensive coverage against various cyberthreats. In April 2023, ZeroFox completed acquisition of LookingGlass to enhance to key areas: broadened attack surface management and vulnerability intelligence capabilities.

Mandiant

Mandiant, through its comprehensive Mandiant Advantage platform, delivers a broad spectrum of cloud-based cybersecurity solutions. The platform, designed as a multitenant SaaS offering, simplifies deployment, requiring just an internet connection and a browser. Key offerings include threat intelligence for actionable insights into cyberthreats, Alert Prioritization & Investigation to assist organizations in responding to critical threats efficiently, Attack Surface Management for continuous monitoring of digital assets, and Security Validation that facilitates automated testing against known threats. The company is known for its deep and comprehensive threat intelligence, powered by over 350 security researchers and analysts. This intelligence is derived from a multitude of sources, including internal data lakes, deep and dark web collections, threat hunting activities, and open source intelligence. Mandiant's capabilities include detailed threat actor profiling, web classification and

reputation scoring, file reputation analysis, dark web insights, and ransomware detection and mitigation. Mandiant's Digital Risk Protection solution focuses on the initial reconnaissance stage of the attack life cycle, providing customers with visibility into risk factors impacting their extended enterprise and supply chain. The company's offerings are not one size fits all; they provide tailored threat intelligence subscriptions ranging from a free limited offering to more comprehensive packages like Security Operations and Fusion subscriptions, catering to different segments of the security team. In September 2022, Mandiant was acquired by Google retaining its brand.

Cyberint

Cyberint, a key player in the threat intelligence security services market, offers robust cybersecurity solutions through its Argos Edge platform, a sophisticated cloud-based SaaS product. Its service portfolio extends beyond traditional cyberthreat monitoring to include specialized services like brand abuse, fraud alerts, access to in-depth dark web intelligence, and advanced analytics with the Forensic Canvas. A standout feature is its proactive threat alerting system, which efficiently processes over 1.1 million intelligence indicators each day, tailoring high-impact alerts for effective risk reduction. Key capabilities of Cyberint include comprehensive attack surface management, monitoring of exposed interfaces, and tracking of leaked credentials, which are critical for mitigating ransomware threats and initial infection vectors. The platform excels in sifting through extensive data sources, including deep and dark web forums, social media, and antimalware repositories, to provide actionable intelligence. Cyberint's approach of continuous asset discovery ensures relevant and accurate threat intelligence, essential for maintaining an up-to-date security posture. This focus on impactful intelligence, coupled with its advanced data processing and alerting mechanisms, positions Cyberint as a significant and innovative contributor in the rapidly evolving cybersecurity domain.

OpenText

OpenText Threat Intelligence offers a robust platform that enables organizations to proactively identify, assess, and mitigate potential risks. Its threat intelligence capabilities are derived from a combination of internal data sources, external feeds, and advanced analytics, enabling it to deliver actionable insights and timely alerts to its customers. OpenText Threat Intelligence advanced threat hunting capabilities allow organizations to stay one step ahead of cyberadversaries. Its platform offers real-time monitoring, threat actor profiling, and deep visibility into emerging threats. In addition, OpenText provides comprehensive reporting and analysis, empowering organizations to make informed decisions and strengthen their security posture. OpenText's threat intelligence solutions are scalable and customizable, catering to the unique needs and requirements of different organizations. With a strong emphasis on collaboration and integration, Open Text Threat Intelligence seamlessly integrates with existing security infrastructure, enabling organizations to enhance their overall security operations.

ReliaQuest

In 2022, ReliaQuest strengthened its offerings by acquiring Digital Shadows, a renowned provider of threat intelligence services. This strategic move enables ReliaQuest to incorporate Digital Shadows' expertise in monitoring digital risks and gathering threat intelligence into its existing portfolio. Digital Shadows is recognized for its advanced threat intelligence capabilities. Its platform provides organizations with critical visibility into their digital risk environment, helping them preemptively recognize potential threats. Utilizing sophisticated techniques like web-crawling and data mining, Digital Shadows collects intelligence from a variety of sources, including dark web, social media, and online forums. The integration of Digital Shadows' features into ReliaQuest's threat intelligence

platform significantly enhances its ability to offer a more comprehensive solution for monitoring and managing digital risks. This upgraded platform facilitates continuous monitoring to identify issues like data breaches and brand impersonation and in-depth insights into the dark web,

Detailed Participant Profiles: Insights from the Intricacies of Threat Intelligence Questionnaire

Analyst1

Analyst1 is a cybersecurity company founded in 2012, focusing on advanced threat intelligence. It provides a threat intelligence platform designed to help clients across various sectors convert intelligence into actionable insights for enhanced security efficacy. The platform is used extensively by government and commercial organizations for threat investigation, vulnerability management, and reducing response times. The TIP features automated data ingestion and analysis, assessing the effectiveness of security measures. Analyst1 has built a solid reputation and trust among its clients, including the U.S. government and global enterprises, evidenced by its strong customer loyalty and retention.

Strategic Threat Intelligence

The Analyst1 TIP provides a comprehensive overview of cybersecurity threats by systematically collecting and analyzing data from a wide range of sources. This includes the ongoing evolution of TTPs, emerging technical threats, and the changing preferences of threat actors. Central to the platform is a proprietary analytics engine that is calibrated to align with specific priority intelligence requirements (PIRs) of each organization, facilitating a more targeted approach to their unique security environments. This engine effectively tracks and analyzes threat actors, detailing their operational methods, the vulnerabilities they exploit, and the types of malware they use. In addition, Analyst1 includes a historical intelligence archive, which allows for the examination of past threat trends and contributes to forecasting future cybersecurity challenges, including those shaped by geopolitical factors. The platform also features a no-code dashboard interface, which aids in the efficient generation of executive reports and supports decision-making processes that are sensitive to industry-specific risks.

Operational Threat Intelligence

The platform delivers real-time insights on emerging threats by rapidly extracting technical metadata and IoCs from source intelligence, enabling detection engineering staff to build and maintain signature-based detection content. This content can be swiftly deployed to existing infrastructure through the Analyst1 platform, offering near-real-time detection and mitigation of threats. The platform integrates seamlessly with leading SIEM platforms, enhancing security analysis and threat correlation. The platform's "Auto Mitigations" feature enables custom deployment rules for defensive infrastructure like firewalls and IDS/IPS. Analyst1 also offers robust in-platform alerting and integrates with tools like SOAR and ITSM for effective incident response. It minimizes false positives through a specialized verification workflow. In addition, the platform allows users to "follow" updates on any object, and its user-friendly interface and no-code dashboarding enable swift action based on relevant intelligence. Analyst1 supports a broad range of threat feeds and APIs from top vendors like Mandiant, CrowdStrike, and IBM X-Force, as well as numerous OSINT sources, ensuring a comprehensive threat intelligence spectrum.

Tactical Threat Intelligence

Analyst1's tactical threat intelligence platform provides a dynamic approach to cybersecurity, tracking a diverse array of threats through a combination of source intelligence and human analysis. It has the ability to extract and monitor industry-specific vulnerabilities and threats, supported by customizable dashboards for targeted vigilance. The platform assists in cybersecurity operations by quickly identifying relevant threat intelligence and implementing proactive mitigation strategies through automated rules. Analyst1 supports nearly all atomic types of IoCs and allows for the creation and management of dynamic signature-based detection content. Its capabilities extend to malware and network traffic analysis, with tailored intelligence filtering and support for multiple file types, including packet captures. While Analyst1 does not conduct traditional vulnerability assessments, it integrates with platforms like Tenable and Rapid7 for correlating internal vulnerabilities with external threats, aiding in efficient patch prioritization and incident response.

Additional Platform Capabilities

Analyst1's platform offers additional capabilities that enhance its core offerings. It is highly customizable, allowing it to adapt to various organizational needs. The platform incorporates advanced analytics and machine learning to provide insights and automate data analysis. A user-friendly interface facilitates ease of use. Analyst1 is scalable, capable of handling large volumes of data and accommodating organizational growth. The platform aids organizations in meeting cybersecurity regulatory requirements. Regular updates ensure the platform stays current with evolving cyberthreats and user needs.

Anomali

Established in 2013, Anomali specializes in modernizing security operations through the integration of analytics, intelligence, automation, and AI. Its solutions aim to enhance threat detection, response, and manage cyberexposure. Central to Anomali's approach is the automation of processes within security operations centers, focusing on improving security efficacy and reducing operational costs. Serving a wide range of clients, including global business-to-business (B2B) enterprises, large public sector entities, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and service providers, Anomali plays a key role in safeguarding critical infrastructure and providing security solutions to top-tier companies worldwide.

Strategic Threat Intelligence

Anomali provides strategic threat intelligence by creating comprehensive threat bulletins and detailed actor profiles. This is achieved through analyzing a broad spectrum of data, including indicators of compromise and leveraging machine learning tools. The platform offers insights into emerging global threats through reports generated by Anomali's threat intelligence team and various open source and premium providers. Anomali's approach in considering geopolitical trends in cybersecurity is reflected in its specialized dashboards, which showcase observable data and source-to-destination information, aiding in a thorough assessment of the global threat landscape.

Operational Threat Intelligence

Anomali delivers real-time operational intelligence by ingesting data from over 100 sources, each scored by an AI tool named Macula. This scoring system rates items on a scale of 0–100, allowing for the identification of severity and type of threat. Its operational intelligence can be rapidly distributed to defensive tools like firewalls and IDS/IPS within seconds, courtesy of its Integrator offering. Anomali handles false positives through ML, maintaining a database of known indicators and flagging false

positives without deletion, in case of status change. Alerts and notifications are delivered via email, dashboard, and other systems as required.

Tactical Threat Intelligence

On the tactical front, Anomali provides over 130 types of IoCs and offers a detailed breakdown of these indicators, such as malware IPs versus generic IPs. The platform aids in malware and network traffic analysis by associating indicators with malware families and actors, enhancing understanding of the threat environment. In vulnerability assessments, Anomali enriches ingested vulnerabilities and integrates with vulnerability management systems for richer data correlation. In addition, it offers indicator expansion in ThreatStream for direct correlation of IoCs to actors, campaigns, or TTPs and supports tailored alerts for new TTPs using SIGMA rules within Match.

Additional Platform Capabilities

Anomali's platform stands out with its unique feature of aging out IoCs to focus on current threats, preventing legacy data from consuming unnecessary resources. Macula, its ML tool, plays a pivotal role in ensuring the quality and accuracy of data by scoring indicators, flagging false positives, and deduplicating indicators. The system is highly customizable, allowing users to modify indicators and create tailored dashboards. Anomali also features Copilot, a generative AI tool that can condense extensive threat bulletins into concise executive summaries, proving highly beneficial for both executives and analysts.

CrowdStrike

CrowdStrike offers a cloud-native cybersecurity platform focusing on protecting enterprise endpoints, cloud workloads, identities, and data. Its key offering, the Falcon platform, is designed to detect and respond to threats in real time. This platform leverages indicators of attack, threat intelligence, and telemetry from enterprise environments to facilitate accurate threat detection. CrowdStrike's technology is aimed at automating protection, enabling threat hunting, and managing vulnerabilities efficiently, all through a unified lightweight agent. The platform's capabilities are geared toward offering comprehensive threat intelligence and enhancing cybersecurity measures in enterprise environments.

Strategic Threat Intelligence

CrowdStrike provides a sophisticated approach to strategic threat intelligence, focusing on long-term trends, motivations, and capabilities of threat actors. The platform tracks over 220 named adversaries, including nation-state actors, ecrime groups, and hacktivists offering comprehensive profiles updated daily. Over thousands of malware families and hundreds of campaigns, associating malware profiles with adversaries, are tracked as part of the attribution process. These profiles, available within the Falcon platform's API, encompass an overview of each actor's motivations and targets, in-depth reports analyzing trends and tradecraft, and detailed insights into the MITRE ATT&CK matrix and kill chain. The platform's geopolitical analysis tracks over 115 nation-state adversaries and generates detailed reports on geopolitical trends and their impact on cybersecurity. The Threat Landscape dashboard from CrowdStrike allows users to filter and visualize key trends in cybersecurity threats, including global detections, actor activities, reports, and MITRE ATT&CK tactics. CrowdStrike's executive reporting is tailored to assist in strategic decision-making, offering weekly, monthly, quarterly, and annual reports that highlight significant trends across various threat landscapes.

Operational Threat Intelligence

CrowdStrike's operational threat intelligence is characterized by the company's real-time threat information and extensive integration capabilities. The company's scalable malware analysis platform processes millions of samples daily, providing timely indicators directly into its Falcon platform. Falcon Intelligence Recon monitors the criminal underground in real time, tracking restricted web pages, forums, and marketplaces. It identifies risks like data leaks and threats to personnel by surveying millions of sources across the deep and dark web and offers tools for users to create monitoring rules and receive alerts on potential threats. CrowdStrike's platform can integrate with various technology stacks, through its global partner ecosystem featuring over 1,900 solution providers and 420+ technical integrations. The company's Falcon platform APIs allow for custom integrations, and the Fusion Foundry offers tools for building custom integrations and visualizations. In addition, Falcon Fusion's no-code automation facilitates the seamless exchange of intelligence across an organization's technology stack, supported by 50+ turnkey intel integrations and 200+ partner-led integrations, enhancing the speed and efficiency of distributing operational intelligence. The handling of incident response and false positives is managed through sophisticated alerting mechanisms, with a strong emphasis on reducing false positives through comprehensive validation and verification processes.

Tactical Threat Intelligence

On the tactical front, CrowdStrike monitors a vast array of malware families, leveraging data from multiple sources, including millions of endpoints, malware analysis communities, incident response engagements, and partnerships. To support the planning and execution of cybersecurity operations, the platform provides automated contextualized threat information, vulnerability management, threat alerting, expert malware analysis, domain takedown and blocking, identity protection, and SOC workflow automation. Its real-time IoC feed is enriched with detailed information on each indicator, aiding in a more thorough understanding and response to threats. For malware analysis and network traffic analysis, CrowdStrike provides an integrated automated malware sandbox and expert-driven reverse engineering services. Its weekly SNORT and Suricata rule sets assist users in detecting malicious network activities. In vulnerability assessments, CrowdStrike combines human expertise and machine learning to provide a thorough understanding of vulnerabilities, their exploit status, and prioritization. Its approach is threat centric, focusing on vulnerabilities with the highest risk and potential impact. In addition, CrowdStrike offers unique features tailored for tactical threat intelligence, such as credential monitoring, domain abuse detection, data leakage detection, fraud detection, physical asset protection, and real-time raw intelligence access. Its alert system allows users to receive tailored notifications on new TTPs and emerging threats, ensuring that organizations are always one step ahead of potential cyberthreats.

Integrating and correlating intelligence across strategic, operational, and tactical dimensions, CrowdStrike offers unique features like unparalleled raw intelligence collection and actionable threat intelligence. The quality and accuracy of its data are ensured through rigorous validation processes, and it provides customized solutions like Falcon Intelligence Elite and Recon+ to meet specific organizational needs. Leveraging innovative technologies such as GenAI, CrowdStrike enhances the customer's ability to consume intelligence effectively, demonstrating its commitment to staying at the forefront of threat intelligence innovation.

Cybersixgill

Cybersixgill specializes in providing advanced threat intelligence delivered through a SaaS portal, reports, services, and a wide set of APIs and feeds. Its Cyber Threat Intelligence platform offers real-time insights into emerging threats by monitoring and analyzing data from the deep, dark, clear web and social messaging platforms, helping organizations preempt cyberattacks. Alongside, Cybersixgill provides an attack surface management solution to identify and monitor networked assets. Cybersixgill IQ, a generative AI solution offering instantaneous, offers easily understandable intelligence responses, catering to a range from threat analysts to C-suite executives. Cybersixgill's intelligence insights enable organizations to covertly search, monitor, and generate reports across tactical, operational, and strategic levels with a goal to empower informed decision-making and proactive risk mitigation.

Strategic Threat Intelligence

Cybersixgill's strategic threat intelligence capability is particularly effective in analyzing long-term trends and motivations of threat actors. By utilizing a comprehensive threat intelligence data lake, which archives historical data from as far back as the 1990s, the platform provides an in-depth, contextual understanding of cybercriminal behaviors and motivations. This includes insights into activities within underground forums, leak sites, and access broker marketplaces, giving a full picture of adversaries' operational cycles. Cybersixgill's strategic reporting also encompasses geo-specific and industry-specific threat landscape analyses, offering customized insights for various sectors. In addition, its generative AI solution, Cybersixgill IQ, enhances this strategic facet by generating high-level intelligence summaries and facilitating the production of on-demand intelligence reports, crucial for informed strategic planning and risk management.

Operational Threat Intelligence

Cybersixgill delivers real-time information on emerging and current threats through its Cyber Threat Intelligence platform. This continuous monitoring of varied data sources, including the deep, dark, and clear web, is crucial for early threat detection and vulnerability analysis. With the assistance of Cybersixgill's attack surface management, the platform's asset-based alerting system identifies and classifies an organization's networked assets, monitoring for threats in real-time. Integration with existing security infrastructure (e.g., SOAR, SIEM, and ticketing systems) enhances the platform's utility in threat detection and response. Cybersixgill's over 40 global partnerships, including with major security vendors, extend its operational intelligence reach, offering diverse and tailored integrations to enhance operational efficiency and foster innovative security solutions. Using Cybersixgill IQ, analyst can easily request operational summaries and briefs with actionable measures against threats and vulnerabilities.

Tactical Threat Intelligence

Cybersixgill's tactical threat intelligence focuses on real-time monitoring, extensive databases, API access, actionable alerts, and advanced analysis tools. Specializing in identifying and processing IoCs such as IP addresses, URLs, file hashes, and domain names, the platform sources this information from diverse web environments. Both the Investigative Portal and API provide access to the vast collection of data on IoCs, threat actors, and APTs. The API suite offers direct, programmatic access to this intelligence for integration with existing security systems or custom applications. Using Cybersixgill IQ, analyst can easily request detailed information of current IoCs and remediation measures against threats. Moreover, the platform's Dynamic Vulnerability Exploit (DVE) Intelligence

and compliance dashboards enable clients to prioritize vulnerabilities and compliance issues specific to their industry.

Additional Capabilities

Cybersixgill's threat intelligence offers sophisticated search functionalities within an extensive database that includes over 7 million detailed profiles of threat actors, encompassing APTs and state-sponsored entities. The platform's specialized dashboards streamline the prioritization of mitigation and remediation actions. Key features include automated alerts tailored to each organization's unique assets, a robust Vulnerability Exploit Intelligence module, and comprehensive malware analysis. Integration with the MITRE ATT&CK framework enhances understanding of adversary tactics and techniques. In addition, its multitenancy support and collaborative case management tools make it an adaptable solution for both individual organizations and managed security service providers, ensuring a broad applicability across different cybersecurity contexts.

Flashpoint

Flashpoint offers a software-as-a-service–based platform, serving a diverse client base of over 750 global entities, including major financial institutions, retailers, technology providers, healthcare organizations, and governments, with a strong presence in North America and expanding influence in EMEA and APAC. The Flashpoint Ignite platform delivers comprehensive data and intelligence from varied online sources and integrates threat information from proprietary and public sources like STIX/TAXII. Enhanced by the acquisitions of vulnerability database (VulnDB) and Echosec Systems, Flashpoint offers in-depth vulnerability intelligence and advanced open source intelligence collections for physical security intelligence.

Strategic Threat Intelligence

Flashpoint's strategic threat intelligence integrates deep and dark web data analysis with open source intelligence, supported by over a decade of historical data. The methodology includes behavioral analysis and predictive analytics using frameworks like MITRE ATT&CK to identify long-term trends and actor motivations. This results in Flashpoint Finished Intelligence and dynamic Threat Actor Profiles. The intelligence covers global threats, offering daily briefs, biweekly summaries, and in-depth reports, as well as ad hoc analyses and analyst knowledge pages. It also encompasses geopolitical trends, combining OSINT, signals intelligence, and deep/dark web data for comprehensive scenario analysis. Reports focus on threat landscape trends, impact assessments, and intelligence road maps.

Operational Threat Intelligence

Flashpoint provides operational threat intelligence with a focus on real-time, actionable insights. The platform updates continuously and is accessible via API, integrations, and a graphical user interface (GUI). It supports integration with leading SIEM, TIP, analysis, and digital risk solutions providers like Splunk, Qualys, ServiceNow, Anomali, and IBM QRadar. Intelligence is distributed to defensive tools in near real time. Flashpoint's alerting and incident response mechanism is multifaceted, involving keyword monitoring, saved searches, domain name tracking, and brand monitoring with alerts curated by human analysts for accuracy. The platform minimizes false positives and offers various alert types, including automated, curated, and customized options. Flashpoint also supports various threat feeds and APIs, like compromised credentials, vulnerability insights, and card fraud, providing a comprehensive view of potential threats.

Tactical Threat Intelligence

Flashpoint's tactical threat intelligence specializes in the identification of indicators of compromise, with a strong focus on the MITRE ATT&CK framework. It monitors various malware, threat actors, and attack methods, maintaining an extensive vulnerability database. This database features both CVE-assigned vulnerabilities and over 100,000 of non-CVE vulnerabilities, enabling clients to prioritize mitigation strategies effectively. These vulnerabilities are tagged with keywords including industry, providing more targeted information for specific sectors. An upcoming feature, the Premium Vulnerabilities module, aims to expand this database by adding vulnerabilities that do not have CVE assignments, along with more sophisticated alerting and filtering capabilities. The platform also facilitates malware and network traffic analysis by correlating IoCs with information about threat actors derived from open source and dark/deep web intelligence.

Additional Platform Capabilities

Flashpoint integrates strategic, operational, and tactical threat intelligence, primarily through FINTEL and supplemented by API integrations. It ensures data quality and accuracy through confidence assessments, validation engines, and veracity checks. Customized solutions are available for specific organizational needs. The Ignite AI feature facilitates conversational interaction with its intelligence database, enhancing user access to complex threat intelligence data.

Fortra

Fortra's PhishLabs, a cyberthreat intelligence company, became a part of Fortra following its acquisition in October 2021. Founded in 2008, PhishLabs specializes in providing Digital Risk Protection by offering threat intelligence and mitigation solutions. The company's role in Fortra's cybersecurity portfolio is to address a variety of cyberthreats, including brand impersonation, account takeovers, data leakage, social media threats, and the analysis of suspicious emails. PhishLabs utilizes a range of tools and techniques, such as proprietary kill switches, fast lanes, takedown networks, browser blocking, and API integrations, to effectively counteract these threats. Serving a global client base, PhishLabs has a notable track record in the cybersecurity domain, marked by a high success rate in the rapid removal of phishing sites and extensive experience in handling a significant number of phishing attacks and social media threats since its inception.

Strategic Threat Intelligence

Fortra's strategic threat intelligence synthesizes data from a diverse array of sources, including its suite of security products like Agari, Alert Logic, Digital Defense, PhishLabs, and Digital Guardian, along with various third-party sources. This data is integrated into Fortra Threat Brain, where the Threat Research team employs it to investigate threat actors, campaigns, and trends. Its approach in detailed analysis and tracking of threat actor groups is utilized through observations from its commercially deployed security products and extensive web, email, and social media threat data for identification, monitoring, and assessment. Fortra's strategic threat intelligence reports provide comprehensive insights into cybercrime threats such as Business Email Compromise, phishing campaigns, and fraud operations, encompassing details on activity groups, threat infrastructure, and trends in the threat landscape. These reports and insights are supported further by Fortra's customer success programs and intelligence reporting.

Operational Threat Intelligence

Fortra's operational threat intelligence, delivered through its Digital Risk Protection solution powered by the PhishLabs Platform, offers comprehensive visibility by collecting data from the surface, deep,

and dark web, social media sources, and various data feeds. The intelligence, enriched by experts, is available in near real time and integrates into enterprise security tools via robust APIs. The platform provides a web app for full visibility into alerts and incidents and automates mitigation of external threats. False positives are rare due to expert curation, and users can update incidents in the web app if needed. The platform's alerting and notification system is managed through the PhishLabs web application, which also provides configurable dashboards and reports for immediate action. API feeds include DRP incidents, malicious email indicators, IP addresses, domains, URLs, file hashes, and vulnerability data.

Tactical Threat Intelligence

Fortra's approach to tactical threat intelligence involves monitoring a broad spectrum of malware, threat actors, and attack methods. This is done across various security functions such as endpoint detection and response, managed detection and response (MDR), email security, and digital risk protection. Fortra utilizes vulnerability management and offensive security solutions to gain direct insights into vulnerabilities, adapting to evolving threats. Fortra Threat Brain plays a key role in integrating this intelligence, offering insights into security trends and industry-specific threats. Fortra provides detailed IoC's on email threats (sender details, IPs, and URLs), Office 365 lures, BEC, ransomware, and credential phishing and tracks brand threat indicators, malicious files, C2 infrastructure, malicious IPs, money mule accounts, and stolen credentials. Fortra's platforms, including Beyond Security, Digital Defense, Core Security, and Cobalt Strike, contribute to the company's tactical threat intelligence by offering insights into vulnerabilities and threats.

Additional Platform Capabilities

Fortra's platform uniquely combines a wide array of open source and proprietary data with advanced data science techniques, including machine learning and neural networks, to correlate and contextualize intelligence. Fortra Threat Brain stands out for its comprehensive data warehousing architecture and integration of data from globally deployed commercial security products. To ensure data fidelity, intelligence is curated by expert analysts both at the product level and within Fortra Threat Brain. Customization is a key aspect of Fortra's services, with DRP services tailored to specific customer threats and requirements.

Intel 471

Intel 471 is renowned as a provider of cyberthreat intelligence for top-tier enterprises and governments across the globe. The company was established in 2014 and experienced organic growth until 2021, when it received a strategic investment from Thoma Bravo, a leading private equity firm. Leadership at Intel 471 is marked by extensive experience in tracking sophisticated cybercriminals, engaging in tactical intelligence collection in military operations and a noteworthy background in federal law enforcement. Headquartered in Wilmington, Delaware, Intel 471 employs nearly 200 professionals with backgrounds in intelligence, law enforcement, military, and sector-specific cyberthreat intelligence actively operating across six continents. Intel 471 focuses on the following core intelligence domains: Malware Intelligence, Adversary Intelligence, Vulnerability Intelligence, Credential Intelligence, Marketplace Intelligence, and Attack Surface Protection. Customers leverage the insights garnered from these domains to solve real-world use cases, including third-party risk management, security operations, and fraud.

Strategic Threat Intelligence

Intel 471's SaaS-based platform, TITAN provides in-depth insights into cyberthreats and cyberattacker motivations by integrating diverse intelligence sources. This approach combines insights from the cyberunderground, including closed forums and various communication channels, with sophisticated malware intelligence, such as its patented Malware Emulation and Tracking System, which covers over 200 malware families. In addition, analysis and forecasts enhance its capability to analyze and track malware on a global scale. Deep, HUMINT-centric insights ensure a comprehensive linkage between the threat actors, their intentions, the malware they develop, and their evolving tactics and procedures. The company's focus on quality over quantity ensures mission-critical intelligence is delivered with precision. Intel 471 provides reports and other intelligence via the TITAN platform as described previously and also allows consumption of intelligence via programmatic interface. These include a variety of intelligence reports that cover high-level topics, those that analyze specific products and adversary TTP profiles aligned with the MITRE ATT&CK framework. These reports conform to ODNI's ICD 203 and the NATO Admiralty System to convey credibility and reliability assessment. Weekly Executive Intelligence reports are also provided to support comprehensive decision-making.

Operational Threat Intelligence

The TITAN platform offers real-time operational threat intelligence through various mechanisms. It delivers near-real-time alerts on emerging threats based on customer-subscribed keywords, aiding in proactive security measures. The platform integrates seamlessly with existing technology stacks through TITAN's RESTful API, enabling automatic and immediate intelligence distribution to defensive tools (e.g., TIPs, SIEMs, and SOARs). TITAN provides actionable intelligence and immediate alerts for incident response, with users able to set up Watchers for specific issues or queries. In addition, Intel 471's General Intelligence Requirement (GIR) category code classification system in TITAN enables customized alerting and monitoring, offering quick access to relevant intelligence for immediate action. Its extensive collection and dissemination coverage includes closed, online sources, which are rendered accessible by a skilled team of researchers. These researchers have native proficiency in the languages used by threat actors but also the vernacular and customs of the closed cyberunderground ecosystems they frequent. Researchers are able to deliver unique insights based on the years of skills and patience in gaining access to these exclusive areas and the relationships they foster there.

Tactical Threat Intelligence

Intel 471's tactical threat intelligence capabilities are focused on monitoring specific malware, threat actors, and attack methods, primarily operating in underground forums where preattack planning occurs. The platform is designed to provide early warnings, both automated and manual, aiding in prevention and mitigation. It continuously tracks the life cycle of disclosed vulnerabilities, assessing exploitation probabilities and compromised credentials, thus enabling early detection of threats specific to an industry. Intel 471 supports cybersecurity operations through responsible disclosure processes and sensitive intelligence handling. The company's patented Threat Research and Analysis Platform (TRAP) emulates over 204 malware families, providing actionable IoCs like malware C2 infrastructure and botnet IPs. Integration with platforms like MISP and Maltego aids in malware and network traffic analysis. Furthermore, its TITAN platform offers tailored alerts for new TTPs deployments, and its open API allows for customization to meet specific organizational needs.

Recorded Future

Recorded Future Intelligence Cloud Platform is a comprehensive solution comprising nine modules that offer a wide range of capabilities for gathering, processing, and disseminating threat intelligence. The platform's central component is the Intelligence Graph, which is a data model designed to enhance threat intelligence capabilities. It utilizes a vast amount of internet data collected over 10 years to provide valuable insights. By combining analytics and human expertise, the Intelligence Graph generates intelligence on both stable and dynamic aspects of the global landscape that aids in effectively countering attackers. In addition, it employs natural language processing (NLP) and machine learning to extract and score relevant information from various sources, enabling quick identification of critical insights. The platform also offers user-friendly visualizations, alerts, and integrations to support comprehensive threat management.

Strategic Threat Intelligence

Recorded Future's strategic threat intelligence focuses on long-term trends and motivations of threat actors by leveraging its Intelligence Graph within the Intelligence Cloud to analyze data from over a million sources. This analysis offers insights into the actions and intents of diverse threat actors, including nation-states and cybercriminals. The platform's threat actor threat map, updated daily, aligns with an organization's specific threat landscape and tracks priority threats to reveal historical and potential high-impact trends. Recorded Future's dedicated team of over 80 analysts, known as the Insikt Group, connects technical analysis with detailed research on threat actor behaviors. The platform's global scope encompasses data from the open web, dark web, and technical sources, ensuring comprehensive coverage of emerging threats. Recorded Future's executive reports focus on industry-specific threats, emerging trends, and intelligence maturity, providing key metrics such as top threat actors, malware trends, and industry-specific risks to aid in strategic decision-making.

Operational Threat Intelligence

Recorded Future enhances real-time, actionable insights by analyzing data from diverse sources. It offers over 100 integrations into top tools such as SIEMs, EDR, email gateway, third-party risk management, network, and cloud delivering operational intelligence to defensive tools, updated in near-real-time bases. Alerting is continuous, using various channels like email, mobile, and API, with incident response processes streamlined through automation, including link analysis and expanded hunts. A multivariate model is employed to minimize false positives, backed by a 24 x 7 support team for corrections. The platform provides customized alerts for a wide range of scenarios, including new vulnerabilities and emerging threats. Recorded Future delivers specific, actionable intelligence through tailored dashboards and threat maps, offering recommendations like hunting packages for enhanced threat hunting capabilities. It supports numerous threat feeds and APIs, covering diverse scenarios like Command and Control (C&C) servers, phishing URLs, and nation-state threat actors, available in various data formats.

Additional Capabilities

Recorded Future's platform excels in tracking domain and IP reputation, with over 2 billion analyzed domains and 215 million IPs, providing detailed risk scores and context. It integrates and correlates operational, tactical, and strategic threat intelligence to derive priority controls and proactive strategies. Unique features include a wide-ranging, AI-driven collection from numerous sources, delivering unbiased and real-time intelligence across the full attack surface. This approach ensures quality and accuracy, with source transparency and a sophisticated risk scoring model. The platform is tailored to each client, merging their internal telemetry with external threats and offering customization through

dashboards and managed services. Recorded Future has demonstrated success across all intelligence levels, as evidenced by customer case studies. Since April 2023, it incorporates generative AI to summarize and report intelligence, maintaining source transparency for effective SOC triage and incident response.

ThreatConnect

The ThreatConnect TI Ops Platform is an advanced threat intelligence platform enhanced with AI capabilities. It's designed to support cyberthreat intelligence teams by providing scalable and flexible solutions for managing cyberthreat intelligence. The platform collects and refines threat intelligence, allowing for effective analysis and prioritization. It incorporates AI and machine learning, automation, and compatibility with various enterprise tools to facilitate a more efficient response to cyberthreats. The platform aids cybersecurity teams in identifying, investigating, and responding to threats in a timely and accurate manner.

Strategic Threat Intelligence

ThreatConnect's strategic threat intelligence capabilities are centered around ATT&CK Visualizer and Threat Graph features, which aid in visually displaying threat intel data. This setup facilitates the easy uncovering of patterns and relationships, helping analysts quickly understand and respond to attacker behaviors across various tactics and techniques. ThreatConnect offers proprietary feeds through its analytics engine, CAL, which includes open source intelligence, data on newly registered domains, and algorithmic domain generation. The platform supports the creation of customizable reports and dashboards, enabling organizations to tailor intelligence to their specific needs. In tracking threat actor groups, ThreatConnect's Threat Library, based on the Diamond Model of Intrusion Analysis, employs the concept of Groups and atomic "Objects" such as adversaries, campaigns, and intrusion sets. The platform also tracks geopolitical trends impacting cybersecurity using data attributes like source and target countries and industry sectors. For executive reports, key metrics such as analyst effectiveness, MTTR/MTTD, ROI, and custom metrics are emphasized, aiding high-level decision-making.

Operational Threat Intelligence

On the operational front, ThreatConnect provides real-time information about current and emerging threats through customizable dashboards constructed using the ThreatConnect Query Language. The platform integrates with popular SIEM and security analytics tools, distributing operational intelligence to defensive tools in real time. Alerting and incident response are managed through customizable automation Playbooks and a centralized Notifications Center. For handling false positives, analysts can manually notate data objects in the platform, and community-reported false positives are also integrated into the intelligence. The platform offers a variety of alerts and notifications, customizable to specific organizational needs. ThreatConnect supports a wide range of threat feeds and APIs and provides extensive training programs and resources to help organizations respond to operational threats effectively.

Tactical Threat Intelligence

Tactically, ThreatConnect monitors a comprehensive range of specific malware, threat actors, and attack methods, supporting all MITRE ATT&CK tactics, techniques, and subtechniques. The platform can natively track vulnerabilities and ingest data from various sources for industry-specific analysis. For supporting cybersecurity operations, features like the ATT&CK Visualizer and Threat Graph are utilized, along with Workflows and Low-Code Automation, to facilitate analyses and response actions. The platform aggregates various types of indicators of compromise and integrates with leading

malware analysis sandboxes and network monitoring tools for enhanced malware and network traffic analysis. Vulnerability assessments are conducted with features that enable collaboration between CTI and Vulnerability Management teams, and the platform offers additional features specifically designed for tactical threat intelligence.

Additional Capabilities

ThreatConnect's platform offers additional tools and capabilities such as ThreatAssess and CAL to score and rate the severity of indicators related to domains and IP addresses, supplemented by automated data from sources such as VirusTotal and DomainTools. The platform integrates and correlates intelligence across operational, tactical, and strategic levels using an associations-based approach, which is visualized through a Threat Graph and accessible via an API. Unique features include intelligence requirements management, an ATT&CK Visualizer for analyzing threat actor behaviors, and built-in reporting functions. Quality and accuracy are ensured through the evaluation of intelligence feeds using the Feed Explorer and Scorecards, and the platform offers customization services to align with specific organizational needs.

ThreatQuotient

ThreatQuotient emphasizes the human element in cybersecurity, focusing on enhancing threat operations through its flagship platform, ThreatQ. This platform integrates artificial intelligence with threat intelligence, improving security operations by prioritizing, automating, and collaborating on threat detection and response. It offers comprehensive intelligence by merging data from various sources, ensuring a unified view of threat actors. Key features include customizable intelligence storage, industry-specific analysis, and capabilities for strategic threat prioritization. In addition, ThreatQ supports vital functions like incident response, threat hunting, and vulnerability management, empowering organizations to effectively navigate the cybersecurity landscape.

Strategic Threat Intelligence

ThreatQuotient's strategic threat intelligence, delivered via its ThreatQ platform, enables decision makers to gain a deep understanding of the cyberthreat landscape. Central to this is the DataLinq Engine, which aggregates and correlates intelligence from various sources like open source, commercial feeds, and both structured and unstructured data, leading to a unified view of threat actors and campaigns. Importantly, the platform's flexibility in storing and contextualizing intelligence, using attribute and tag models, allows for the application of industry-specific contexts, aiding in tailored analysis and strategic prioritization of threats. Users can leverage these capabilities to create Smart Collections in the Threat Library for custom dashboard development, focusing on specific industry risks or geopolitical trends. This feature, coupled with the platform's ability to develop custom algorithms for prioritizing threats, enhances the relevance of the intelligence to the specific industry, thus empowering organizations to make informed strategic decisions and efficiently navigate the intricacies of cybersecurity challenges in their respective sectors.

Operational Threat Intelligence

ThreatQ's operational threat intelligence platform offers a comprehensive approach to real-time threat intelligence, emphasizing rapid integration with existing security infrastructures. Its marketplace features 400 integrations that include data enrichment from threat intelligence providers, bidirectional data sharing with technology stacks, and automation use cases such as ticket generation, blocking at the Firewall, EDR, and other enforcement points. The platform's strength is its rapid dissemination of operational intelligence to defensive mechanisms. This, combined with its comprehensive incident

response capabilities and adaptable integration with various incident response tools, highlights its effectiveness in managing security events. ThreatQ manages false positives through advanced scoring mechanisms and features like an automatic expiration of stale intelligence and a white-list system. Its alerting and notification system is well supported by customizable dashboards and reporting tools, which aid in prioritizing and acting on threat intelligence. In addition, the platform supports diverse range of commercial and open source threat feeds and APIs.

Tactical Threat Intelligence

On a tactical level, ThreatQuotient's platform allows clients to choose specific malware, threat actors, and attack methods for monitoring, utilizing a comprehensive Threat Library that combines data from the ThreatQ Marketplace and custom organizational data. This enables effective tracking of industry-specific vulnerabilities by integrating various data sources, including external threat intelligence, internal vulnerability scans, and commercial and OSINT data. The platform offers an extensive array of indicators of compromise, from ASN to custom object types, ensuring a wide coverage in threat detection. For vulnerability assessments, ThreatQuotient integrates with VM tools like Tenable, Qualys, and Rapid 7, using scan outputs to provide deeper vulnerability context and correlate with asset records. The ThreatQ Investigations tool, a "Cyber Situation Room," enhances cybersecurity operations planning with features like interactive evidence boards and multiteam interfaces. Operationalizing tactical intelligence is core workflow for Threat Detection Engineering teams. In addition, ThreatQ enables the export and translation of a standardized set of indicators into formats compatible with various security tools, thereby enhancing interoperability and effectiveness in threat detection. This capability is further augmented by the ThreatQ TDR Orchestrator, which automates the deployment of these indicators, streamlining the process and ensuring timely responses to emerging threats.

Additional Platform Capabilities

The platform's Dynamic Scoring feature allows for customization, enabling users to tailor risk prioritization to their specific needs. The core of its efficiency lies in the ThreatQ DataLinq Engine, which handles key data processes such as ingestion, normalization, and correlation. Unique to ThreatQuotient are features like a customizable data model and the Smart Collections framework, which offer enhanced user control and streamline data management that includes data retention policies. For threat intelligence sharing needs within or between communities, the platform has an optional module, ThreatQ Data Exchange (TQX). ThreatQ Data Exchange allows the creation of bidirectional information sharing communities where all peers can use ThreatQ or, alternatively, standards-compliant platforms that support STIX/TAXII. The platform also prioritizes data accuracy, incorporating Dynamic Scoring and whitelisting to ensure high-quality intelligence.

ADVICE FOR SERVICES PROVIDERS

- Integrate threat intelligence with security orchestration and automation platforms: This integration enables automated incident response and threat mitigation, streamlining the security operations process and reducing response time.
- Provide transparent and explainable artificial intelligence algorithms: Enhancing user trust and understanding of threat detection and decision-making is crucial. By providing transparent and explainable AI algorithms in threat intelligence platforms, users can have more confidence in the accuracy and reliability of the system.

- Collaborate with industry bodies and organizations: Establishing standardized threat intelligence formats, taxonomies, and governance frameworks is essential for improving data interoperability and consistency. Collaboration with industry bodies and organizations can help create a unified approach to threat intelligence, benefiting the entire cybersecurity community.
- Ensure compliance with data privacy regulations: Adhering to data privacy regulations and compliance requirements is crucial for maintaining trust and protecting sensitive information. TIP and TISS providers should ensure that their threat intelligence collection, processing, and sharing practices align with these regulations.
- Develop tools for non-security professionals: Making threat intelligence more accessible and usable for non-security professionals within organizations can enhance overall security posture. TIP and TISS providers should focus on developing user-friendly tools and resources that enable non-security professionals to leverage threat intelligence effectively.
- Promote experimentation and innovation: Encouraging experimentation and innovation in threat intelligence usage can help uncover new insights and approaches to cybersecurity. TIP and TISS providers should foster an environment that promotes continuous learning and improvement in the field.
- Provide metrics and analytics: Demonstrating the tangible impact of threat intelligence on organizational security posture and risk reduction can help organizations understand the value of investing in threat intelligence. TIP and TISS providers should offer metrics and analytics that showcase the effectiveness of their solutions.
- Contribute to open source initiatives: Supporting open source threat intelligence initiatives can enhance collective cybersecurity knowledge and capabilities. TIP and TISS providers should actively contribute to open source projects, sharing their expertise and collaborating with the cybersecurity community.
- Try to explain how platforms affect outcomes: Cybersecurity software is tough to assess in one-to-one comparisons. However, threat intelligence is not meant to be "shelfware." Vendors should explain how their threat intelligence is used to detect ransomware, prevent phishing, ensure a strong cybersecurity posture, and guarantee compliance.

LEARN MORE

Related Research

- *Worldwide Threat Intelligence Forecast, 2023-2027: Is There Room for Individual Vendors to Make Money While Serving the Greater Good?* (IDC #US50210623, June 2023)
- *IDC Market Glance: Cloud-Native XDR and Tier 2 SOC Analytics, 2Q23* (IDC #US50578923, April 2023)
- *IDC Market Presentation: Worldwide Threat Intelligence Report: Observing the Adversary When They Retreat to the Dark Web and Behind Social Media* (IDC #US50480023, March 2023)
- *Worldwide Threat Intelligence Market Shares, 2022: Providing Insight on the Gathering Threats Outside the Network Perimeter* (IDC #US49128022, March 2023)
- *How Global Threat Intelligence Vendors Address the Nuances of Regional Markets* (IDC #US49127923, February 2023)
- *Worldwide Threat Intelligence Coverage Preview (TIP/TISS): Surfacing the Adversary Before They Disrupt You!* (IDC #US49931022, December 2022)

- *What Threat Intelligence Platforms and Threat Intelligence Security Services (TIP/TISS) Are Asked in a Request for Proposal (RFP)* (IDC #US49933622, December 2022)

Synopsis

This IDC Market Perspective explores the three intricacies of threat intelligence: strategic, operational, and tactical. It differentiates between these aspects of intelligence and highlights their unique capabilities and applications. By showcasing how participating vendors contribute, the document offers a distinctive view of how this intelligence is applied across various use cases, emphasizing their unique features and capabilities.

"Threat Intelligence gained momentum in the early 2000s as it became clear that traditional security measures were no longer sufficient against advanced cyberthreats," says Monika Soltysik, senior research analyst, Security and Trust team at IDC. "Today, it's a critical component integrated into broader security strategies, helping organizations not only respond to but also anticipate and adapt to the ever-changing cyberlandscape."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
***.idc.com