+357 96 030922
info@marketpublishers.com

Global AI-Based Cyber Threat Intelligence Market 2026 by Company, Regions, Type and Application, Forecast to 2032

https://marketpublishers.com/r/GBFA8086EA72EN.html
Date: November 2026
Pages: 123
Price: US$ 3,480.00 (Single User License)
ID: GBFA8086EA72EN

Abstracts

According to our (Global Info Research) latest study, the global AI-Based Cyber Threat Intelligence market size was valued at US$ 641 million in 2025 and is forecast to a readjusted size of US$ 957 million by 2032 with a CAGR of 6.0% during review period.

AI-Based Cyber Threat Intelligence refers to cybersecurity intelligence platforms, software, and managed intelligence services that apply artificial intelligence, machine learning, natural language processing, behavioral analytics, graph analytics, and automated correlation technologies to collect, enrich, classify, prioritize, and operationalize information related to cyber threats. The research scope focuses on solutions that transform large volumes of structured and unstructured security data—including malicious indicators, malware information, vulnerabilities, attack infrastructure, threat actor activities, dark web information, open-source intelligence, proprietary telemetry, and enterprise security signals—into actionable intelligence for security operations and risk decision-making. Depending on the intelligence objective, AI-Based Cyber Threat Intelligence can provide Strategic Threat Intelligence, Operational Threat Intelligence, Tactical Threat Intelligence, or Technical Threat Intelligence. Core functions typically include automated threat discovery, indicator enrichment, threat actor profiling, attack campaign correlation, risk prioritization, anomaly identification, contextual analysis, intelligence dissemination, and integration with SOC, SIEM, XDR, SOAR, vulnerability management, and incident response workflows. Major application sectors include banking and financial services, government and defense, IT and telecommunications, healthcare, manufacturing, energy and utilities, and retail and e-commerce.

+357 96 030922
info@marketpublishers.com

Key Findings

AI is shifting cyber threat intelligence from data aggregation toward automated contextualization prioritization and operational response

Operational and technical intelligence remain closely integrated with SOC detection investigation hunting and incident response workflows

Multi-source intelligence fusion is becoming increasingly important as organizations manage fragmented internal and external security signals

Banking government telecommunications energy and other critical sectors represent important application areas for AI-Based Cyber Threat Intelligence

Competition increasingly centers on proprietary telemetry AI analytics intelligence quality workflow integration and threat research capabilities

Market Trends

The AI-Based Cyber Threat Intelligence market is evolving from conventional indicator collection and feed aggregation toward continuously updated, context-aware intelligence that can be embedded directly into security operations. Machine learning is increasingly used to identify patterns across large-scale telemetry, while generative AI and agentic reasoning are being introduced to summarize threat activity, correlate fragmented evidence, support natural-language investigation, accelerate malware analysis, and recommend defensive actions. Another important trend is the transition from standalone threat intelligence portals toward intelligence embedded within broader SOC, SIEM, XDR, SOAR, exposure management, and incident response environments. This reduces the distance between identifying a threat and taking defensive action. At the same time, customers increasingly expect intelligence to be organization-specific rather than generic, emphasizing relevance to their assets, industries, geographic exposures, vulnerabilities, and attacker profiles. As attack timelines shorten and threat volumes expand, the long-term direction of the market is toward higher automation, stronger human-AI collaboration, richer proprietary telemetry, and intelligence that can directly trigger investigation, prioritization, detection engineering, hunting, and response workflows.

+357 96 030922
info@marketpublishers.com

Market Dynamics

Drivers

The expansion of attack surfaces, cloud environments, digital supply chains, remote access, connected devices, and AI-enabled business systems is increasing the volume and complexity of threat information that security teams must process. Traditional manual analysis is increasingly insufficient for correlating rapidly changing indicators, vulnerabilities, attacker infrastructure, malware behavior, and threat actor activity across multiple sources. AI-Based Cyber Threat Intelligence addresses this problem by automating data enrichment, clustering, correlation, prioritization, and contextual interpretation, enabling security teams to identify relevant threats more quickly. The continued development of SOC modernization, XDR adoption, automated incident response, vulnerability prioritization, and threat-informed defense also increases demand for machine-readable and operationally integrated intelligence. In highly regulated and critical sectors, requirements for proactive monitoring, cyber resilience, supply-chain security, and early warning further support adoption.

Restraints

Market development is constrained by data quality, integration complexity, implementation costs, and uneven organizational maturity. AI models depend heavily on the completeness, timeliness, provenance, and labeling quality of underlying intelligence, meaning poor-quality or duplicated data can generate irrelevant findings or misleading prioritization. Enterprises frequently operate heterogeneous security architectures containing multiple SIEM, endpoint, network, identity, cloud, and vulnerability management tools, making integration and normalization difficult. Smaller organizations may also lack dedicated threat intelligence analysts capable of translating sophisticated intelligence into operational decisions. In addition, high-value proprietary intelligence, extensive telemetry, experienced analyst teams, and continuously maintained detection infrastructure require substantial investment, which can raise subscription and service costs. Concerns regarding sensitive data handling, model transparency, false positives, and the reliability of AI-generated conclusions can also slow adoption in highly regulated environments.

Opportunities

The largest opportunities are emerging around intelligence automation, organization-

+357 96 030922
info@marketpublishers.com

specific risk context, dark web monitoring, digital risk protection, supply-chain intelligence, and AI-assisted SOC workflows. AI can increasingly map external threat activity against an organization's assets, software dependencies, vulnerabilities, identities, and business priorities, improving the relevance of intelligence and reducing analyst workload. Another opportunity lies in the convergence of threat intelligence with exposure management, attack surface management, vulnerability prioritization, fraud intelligence, brand protection, and third-party risk. This broadens the role of intelligence from a specialist security function into a more comprehensive enterprise risk input. Generative AI and agentic systems may further improve investigation efficiency by automating evidence collection, summarization, relationship mapping, query generation, and recommended next actions. Providers able to combine strong proprietary data assets with AI analytics and direct workflow integration are positioned to capture a larger share of security operations budgets.

Challenges

One of the central challenges is maintaining intelligence accuracy and explainability as AI becomes more deeply involved in threat analysis. Cyber adversaries deliberately create deception, rapidly change infrastructure, and increasingly use automation and AI themselves, which can reduce the useful life of indicators and complicate attribution. Generative AI also creates risks of unsupported conclusions or incorrect relationships if outputs are not grounded in validated intelligence. Providers must therefore balance automation with analyst verification and evidence traceability. Another challenge is interoperability: intelligence must be delivered in formats that can be consumed across different security architectures while preserving context and prioritization. Regulatory requirements governing data location, privacy, cross-border information sharing, and critical infrastructure can further complicate global deployments. As more cybersecurity vendors incorporate AI capabilities, the market also faces increasing difficulty in distinguishing substantive threat intelligence capabilities from generic AI-assisted security functions.

Value Chain Analysis

The upstream layer of the AI-Based Cyber Threat Intelligence value chain consists primarily of intelligence data and technical infrastructure. Major inputs include endpoint and network telemetry, cloud security signals, malware samples, vulnerability information, DNS and domain data, internet scanning, open-source intelligence, dark web information, attack infrastructure observations, incident response findings, identity

+357 96 030922
info@marketpublishers.com

signals, and proprietary security telemetry. Cloud computing resources, data storage, graph databases, AI models, threat knowledge bases, and cybersecurity research teams provide the underlying analytical infrastructure. Data coverage, freshness, uniqueness, provenance, and historical depth strongly influence the quality of the resulting intelligence, making proprietary telemetry and threat research capabilities important sources of differentiation.

The middle layer transforms raw data into usable intelligence through collection, normalization, deduplication, enrichment, correlation, machine learning, behavioral analytics, natural language processing, graph analysis, threat actor mapping, risk scoring, and analyst validation. Value is created by reducing noise and converting fragmented data into contextualized judgments that answer who is attacking, what assets may be affected, how attacks are conducted, and what actions should be prioritized. Downstream delivery occurs through threat intelligence platforms, APIs, feeds, dashboards, managed intelligence services, and integrations with SIEM, XDR, SOAR, SOC, incident response, vulnerability management, and exposure management systems. The highest-value solutions increasingly combine intelligence content with automated operational workflows, allowing threat information to influence detection, hunting, prioritization, investigation, and response rather than remaining a standalone information product.

Segment Insights

By intelligence level, the market is structured around Strategic Threat Intelligence, Operational Threat Intelligence, Tactical Threat Intelligence, and Technical Threat Intelligence. Strategic intelligence primarily supports management-level understanding of cyber risk, geopolitical exposure, sector-specific threats, and long-term adversary trends. Operational intelligence focuses more directly on active campaigns, threat actors, attack infrastructure, targeting patterns, and likely attacker objectives. Tactical intelligence analyzes adversary techniques, tactics, and procedures and is closely aligned with threat hunting, detection engineering, and defensive planning. Technical intelligence concentrates on highly granular indicators such as malicious domains, IP addresses, URLs, file hashes, malware signatures, and infrastructure relationships. In practice, leading AI-Based Cyber Threat Intelligence solutions increasingly combine these intelligence levels rather than treating them as independent products, allowing technical signals to be connected with operational context and strategic risk.

The strongest product evolution is occurring in operational and technical intelligence because these areas can be directly connected with automated security workflows. AI

+357 96 030922
info@marketpublishers.com

can process large indicator volumes, cluster infrastructure, identify relationships among malware samples, connect vulnerabilities with active exploitation, and prioritize alerts according to organizational exposure. Strategic intelligence remains more dependent on expert interpretation, but generative AI is improving the speed with which complex technical findings can be translated into executive-level assessments. This creates a layered product opportunity in which automated technical intelligence provides scale, operational intelligence provides attacker context, tactical intelligence supports defensive action, and strategic intelligence supports business and security decision-making.

Downstream Market Opportunities

Demand for AI-Based Cyber Threat Intelligence is particularly strong in industries that operate large digital infrastructures, process sensitive information, or face high consequences from cyber disruption. Banking and financial services require early detection of fraud infrastructure, credential theft, ransomware, phishing, and financially motivated threat groups; government and defense organizations emphasize adversary monitoring, strategic intelligence, and critical-system protection; telecommunications and IT providers require visibility across large-scale networks and customer environments. Healthcare, manufacturing, and energy organizations are also increasing investment as ransomware, supply-chain compromise, operational technology exposure, and connected-device risks become more significant. Retail and e-commerce organizations increasingly use intelligence to monitor credential abuse, payment-related threats, impersonation, malicious domains, and digital fraud. Across these sectors, the strongest opportunity lies in solutions that translate broad external threat information into organization-specific risk priorities and directly support operational security decisions.

Regional Insights

North America represents a highly developed market for AI-Based Cyber Threat Intelligence, supported by a large concentration of cybersecurity technology providers, extensive enterprise security spending, mature SOC operations, broad cloud adoption, and strong demand from financial services, technology, government, defense, healthcare, and critical infrastructure sectors. The region is characterized by rapid integration of threat intelligence with XDR, SIEM, exposure management, and AI-assisted security operations. Enterprises increasingly evaluate providers not only on the volume of intelligence feeds but also on proprietary telemetry, analytic depth,

+357 96 030922
info@marketpublishers.com

automation capabilities, and the ability to connect intelligence with defensive action.

Europe and Asia-Pacific represent important growth areas with different market characteristics. European demand is influenced by data protection, cyber resilience, critical infrastructure protection, and cross-border threat visibility, while customers often place greater emphasis on regulatory alignment and regional intelligence coverage. Asia-Pacific combines mature cybersecurity markets such as Japan with rapidly expanding digital infrastructure and security investment across China and other regional economies. China has developed a substantial domestic cybersecurity ecosystem covering threat intelligence platforms, security operations, cloud security, vulnerability intelligence, and large-scale threat monitoring. Regional competition is therefore increasingly shaped by local language intelligence, domestic telemetry, regulatory requirements, data localization, and the ability to analyze region-specific threat actors and attack infrastructure.

Competitive Landscape Analysis

The AI-Based Cyber Threat Intelligence market is characterized by competition among large cybersecurity platform vendors, specialized threat intelligence providers, digital risk intelligence companies, and regional cybersecurity vendors. The competitive advantage of a provider depends on several interconnected assets: breadth and uniqueness of telemetry, depth of historical intelligence, threat research expertise, AI and machine learning capabilities, threat actor and infrastructure knowledge, integration with enterprise security workflows, and the ability to convert intelligence into actionable decisions. Large cybersecurity platform providers can leverage endpoint, network, cloud, and security operations telemetry to embed intelligence directly into detection and response workflows, while specialized intelligence providers differentiate through broader external-source collection, dark web visibility, adversary research, intelligence analysis, and cross-platform integration. Chinese cybersecurity vendors have developed meaningful capabilities in local threat monitoring, malicious infrastructure analysis, vulnerability intelligence, and security operations, creating a regionally differentiated competitive environment. As AI becomes increasingly common across cybersecurity products, sustainable differentiation is shifting away from simply offering AI functionality toward the quality of proprietary intelligence data, analytical accuracy, evidence traceability, workflow automation, and the ability to deliver intelligence that is relevant to each customer's specific attack surface and risk profile.

+357 96 030922
info@marketpublishers.com

Report Scope

This report is a detailed and comprehensive analysis for global AI-Based Cyber Threat Intelligence market. Both quantitative and qualitative analyses are presented by company, by region & country, by Type and by Application. As the market is constantly changing, this report explores the competition, supply and demand trends, as well as key factors that contribute to its changing demands across many markets. Company profiles and product examples of selected competitors, along with market share estimates of some of the selected leaders for the year 2025, are provided.

Key Features:

Global AI-Based Cyber Threat Intelligence market size and forecasts, in consumption value ($ Million), 2021-2032

Global AI-Based Cyber Threat Intelligence market size and forecasts by region and country, in consumption value ($ Million), 2021-2032

Global AI-Based Cyber Threat Intelligence market size and forecasts, by Type and by Application, in consumption value ($ Million), 2021-2032

Global AI-Based Cyber Threat Intelligence market shares of main players, in revenue ($ Million), 2021-2026

The Primary Objectives in This Report Are:

To determine the size of the total market opportunity of global and key countries

To assess the growth potential for AI-Based Cyber Threat Intelligence

To forecast future growth in each product and end-use market

To assess competitive factors affecting the marketplace

This report profiles key players in the global AI-Based Cyber Threat Intelligence market

+357 96 030922
info@marketpublishers.com

based on the following parameters - company overview, revenue, gross margin, product portfolio, geographical presence, and key developments. Key companies covered as a part of this study include CrowdStrike Holdings, Inc., Recorded Future, Inc., Palo Alto Networks, Inc., Fortinet, Inc., Check Point Software Technologies Ltd., IBM Corporation, Anomali, Inc., ThreatConnect, Inc., Group-IB, Rapid7, Inc., etc.

This report also provides key insights about market drivers, restraints, opportunities, new product launches or approvals.

AI-Based Cyber Threat Intelligence market is split by Type and by Application. For the period 2021-2032, the growth among segments provides accurate calculations and forecasts for Consumption Value by Type and by Application. This analysis can help you expand your business by targeting qualified niche markets.

Market segmentation

Market segment by Type

Strategic Threat Intelligence

Operational Threat Intelligence

Tactical Threat Intelligence

Technical Threat Intelligence

Market segment by Source

Open-Source Intelligence-Based

Dark Web Intelligence-Based

Proprietary Telemetry-Based

Market segment by Number of Intelligence Sources

Single-Source Intelligence

+357 96 030922
info@marketpublishers.com

2–5 Source Intelligence

6–20 Source Intelligence

More than 20 Source Intelligence

Market segment by Application

Banking, Financial Services and Insurance

Government and Defense

IT and Telecommunications

Healthcare

Manufacturing

Energy and Utilities

Retail and E-Commerce

Market segment by players, this report covers

CrowdStrike Holdings, Inc.

Recorded Future, Inc.

Palo Alto Networks, Inc.

Fortinet, Inc.

Check Point Software Technologies Ltd.

IBM Corporation

+357 96 030922
info@marketpublishers.com

Anomali, Inc.

ThreatConnect, Inc.

Group-IB

Rapid7, Inc.

Flashpoint

ZeroFox Holdings, Inc.

Trend Micro Incorporated

QAX Technology Group Inc.

ThreatBook

360 Security Technology Inc.

NSFOCUS Technologies Group Co., Ltd.

DBAPPSecurity Co., Ltd.

Market segment by regions, regional analysis covers

North America (United States, Canada and Mexico)

Europe (Germany, France, UK, Russia, Italy and Rest of Europe)

Asia-Pacific (China, Japan, South Korea, India, Southeast Asia and Rest of Asia-Pacific)

South America (Brazil, Rest of South America)

Middle East & Africa (Turkey, Saudi Arabia, UAE, Rest of Middle East & Africa)

Chapter Outline

+357 96 030922
info@marketpublishers.com

Chapter 1, to describe AI-Based Cyber Threat Intelligence product scope, market overview, market estimation caveats and base year.

Chapter 2, to profile the top players of AI-Based Cyber Threat Intelligence, with revenue, gross margin, and global market share of AI-Based Cyber Threat Intelligence from 2021 to 2026.

Chapter 3, the AI-Based Cyber Threat Intelligence competitive situation, revenue, and global market share of top players are analyzed emphatically by landscape contrast.

Chapter 4 and 5, to segment the market size by Type and by Application, with consumption value and growth rate by Type, by Application, from 2021 to 2032.

Chapter 6, 7, 8, 9, and 10, to break the market size data at the country level, with revenue and market share for key countries in the world, from 2021 to 2026.and AI-Based Cyber Threat Intelligence market forecast, by regions, by Type and by Application, with consumption value, from 2027 to 2032.

Chapter 11, market dynamics, drivers, restraints, trends, Porters Five Forces analysis.

Chapter 12, the key raw materials and key suppliers, and industry chain of AI-Based Cyber Threat Intelligence.

Chapter 13, to describe AI-Based Cyber Threat Intelligence research findings and conclusion.

+357 96 030922
info@marketpublishers.com

Contents

1 MARKET OVERVIEW

1.1 Product Overview and Scope
1.2 Market Estimation Caveats and Base Year
1.3 Classification of AI-Based Cyber Threat Intelligence by Type
  1.3.1 Overview: Global AI-Based Cyber Threat Intelligence Market Size by Type: 2021 Versus 2025 Versus 2032
  1.3.2 Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type in 2025
  1.3.3 Strategic Threat Intelligence
  1.3.4 Operational Threat Intelligence
  1.3.5 Tactical Threat Intelligence
  1.3.6 Technical Threat Intelligence
1.4 Classification of AI-Based Cyber Threat Intelligence by Source
  1.4.1 Overview: Global AI-Based Cyber Threat Intelligence Market Size by Source: 2021 Versus 2025 Versus 2032
  1.4.2 Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Source in 2025
  1.4.3 Open-Source Intelligence-Based
  1.4.4 Dark Web Intelligence-Based
  1.4.5 Proprietary Telemetry-Based
1.5 Classification of AI-Based Cyber Threat Intelligence by Number of Intelligence Sources
  1.5.1 Overview: Global AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources: 2021 Versus 2025 Versus 2032
  1.5.2 Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Number of Intelligence Sources in 2025
  1.5.3 Single-Source Intelligence
  1.5.4 2–5 Source Intelligence
  1.5.5 6–20 Source Intelligence
  1.5.6 More than 20 Source Intelligence
1.6 Global AI-Based Cyber Threat Intelligence Market by Application
  1.6.1 Overview: Global AI-Based Cyber Threat Intelligence Market Size by Application: 2021 Versus 2025 Versus 2032
  1.6.2 Banking, Financial Services and Insurance
  1.6.3 Government and Defense
  1.6.4 IT and Telecommunications

+357 96 030922
info@marketpublishers.com

1.6.5 Healthcare
1.6.6 Manufacturing
1.6.7 Energy and Utilities
1.6.8 Retail and E-Commerce
1.7 Global AI-Based Cyber Threat Intelligence Market Size & Forecast
1.8 Global AI-Based Cyber Threat Intelligence Market Size and Forecast by Region
1.8.1 Global AI-Based Cyber Threat Intelligence Market Size by Region: 2021 VS 2025 VS 2032
1.8.2 Global AI-Based Cyber Threat Intelligence Market Size by Region, (2021-2032)
1.8.3 North America AI-Based Cyber Threat Intelligence Market Size and Prospect (2021-2032)
1.8.4 Europe AI-Based Cyber Threat Intelligence Market Size and Prospect (2021-2032)
1.8.5 Asia-Pacific AI-Based Cyber Threat Intelligence Market Size and Prospect (2021-2032)
1.8.6 South America AI-Based Cyber Threat Intelligence Market Size and Prospect (2021-2032)
1.8.7 Middle East & Africa AI-Based Cyber Threat Intelligence Market Size and Prospect (2021-2032)

2 COMPANY PROFILES

2.1 CrowdStrike Holdings, Inc.
2.1.1 CrowdStrike Holdings, Inc. Details
2.1.2 CrowdStrike Holdings, Inc. Major Business
2.1.3 CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.1.4 CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.1.5 CrowdStrike Holdings, Inc. Recent Developments and Future Plans
2.2 Recorded Future, Inc.
2.2.1 Recorded Future, Inc. Details
2.2.2 Recorded Future, Inc. Major Business
2.2.3 Recorded Future, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.2.4 Recorded Future, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.2.5 Recorded Future, Inc. Recent Developments and Future Plans
2.3 Palo Alto Networks, Inc.
2.3.1 Palo Alto Networks, Inc. Details

+357 96 030922
info@marketpublishers.com

2.3.2 Palo Alto Networks, Inc. Major Business
2.3.3 Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.3.4 Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.3.5 Palo Alto Networks, Inc. Recent Developments and Future Plans
2.4 Fortinet, Inc.
2.4.1 Fortinet, Inc. Details
2.4.2 Fortinet, Inc. Major Business
2.4.3 Fortinet, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.4.4 Fortinet, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.4.5 Fortinet, Inc. Recent Developments and Future Plans
2.5 Check Point Software Technologies Ltd.
2.5.1 Check Point Software Technologies Ltd. Details
2.5.2 Check Point Software Technologies Ltd. Major Business
2.5.3 Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
2.5.4 Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.5.5 Check Point Software Technologies Ltd. Recent Developments and Future Plans
2.6 IBM Corporation
2.6.1 IBM Corporation Details
2.6.2 IBM Corporation Major Business
2.6.3 IBM Corporation AI-Based Cyber Threat Intelligence Product and Solutions
2.6.4 IBM Corporation AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.6.5 IBM Corporation Recent Developments and Future Plans
2.7 Anomali, Inc.
2.7.1 Anomali, Inc. Details
2.7.2 Anomali, Inc. Major Business
2.7.3 Anomali, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.7.4 Anomali, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.7.5 Anomali, Inc. Recent Developments and Future Plans
2.8 ThreatConnect, Inc.
2.8.1 ThreatConnect, Inc. Details
2.8.2 ThreatConnect, Inc. Major Business
2.8.3 ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Product and Solutions

+357 96 030922
info@marketpublishers.com

2.8.4 ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.8.5 ThreatConnect, Inc. Recent Developments and Future Plans
2.9 Group-IB
2.9.1 Group-IB Details
2.9.2 Group-IB Major Business
2.9.3 Group-IB AI-Based Cyber Threat Intelligence Product and Solutions
2.9.4 Group-IB AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.9.5 Group-IB Recent Developments and Future Plans
2.10 Rapid7, Inc.
2.10.1 Rapid7, Inc. Details
2.10.2 Rapid7, Inc. Major Business
2.10.3 Rapid7, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.10.4 Rapid7, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.10.5 Rapid7, Inc. Recent Developments and Future Plans
2.11 Flashpoint
2.11.1 Flashpoint Details
2.11.2 Flashpoint Major Business
2.11.3 Flashpoint AI-Based Cyber Threat Intelligence Product and Solutions
2.11.4 Flashpoint AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.11.5 Flashpoint Recent Developments and Future Plans
2.12 ZeroFox Holdings, Inc.
2.12.1 ZeroFox Holdings, Inc. Details
2.12.2 ZeroFox Holdings, Inc. Major Business
2.12.3 ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.12.4 ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.12.5 ZeroFox Holdings, Inc. Recent Developments and Future Plans
2.13 Trend Micro Incorporated
2.13.1 Trend Micro Incorporated Details
2.13.2 Trend Micro Incorporated Major Business
2.13.3 Trend Micro Incorporated AI-Based Cyber Threat Intelligence Product and Solutions
2.13.4 Trend Micro Incorporated AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)

+357 96 030922
info@marketpublishers.com

2.13.5 Trend Micro Incorporated Recent Developments and Future Plans
2.14 QAX Technology Group Inc.
2.14.1 QAX Technology Group Inc. Details
2.14.2 QAX Technology Group Inc. Major Business
2.14.3 QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.14.4 QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.14.5 QAX Technology Group Inc. Recent Developments and Future Plans
2.15 ThreatBook
2.15.1 ThreatBook Details
2.15.2 ThreatBook Major Business
2.15.3 ThreatBook AI-Based Cyber Threat Intelligence Product and Solutions
2.15.4 ThreatBook AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.15.5 ThreatBook Recent Developments and Future Plans
2.16 360 Security Technology Inc.
2.16.1 360 Security Technology Inc. Details
2.16.2 360 Security Technology Inc. Major Business
2.16.3 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Product and Solutions
2.16.4 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.16.5 360 Security Technology Inc. Recent Developments and Future Plans
2.17 NSFOCUS Technologies Group Co., Ltd.
2.17.1 NSFOCUS Technologies Group Co., Ltd. Details
2.17.2 NSFOCUS Technologies Group Co., Ltd. Major Business
2.17.3 NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
2.17.4 NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
2.17.5 NSFOCUS Technologies Group Co., Ltd. Recent Developments and Future Plans
2.18 DBAPPSecurity Co., Ltd.
2.18.1 DBAPPSecurity Co., Ltd. Details
2.18.2 DBAPPSecurity Co., Ltd. Major Business
2.18.3 DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
2.18.4 DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross

+357 96 030922
info@marketpublishers.com

Margin and Market Share (2021-2026)
2.18.5 DBAPPSecurity Co., Ltd. Recent Developments and Future Plans

3 MARKET COMPETITION, BY PLAYERS

3.1 Global AI-Based Cyber Threat Intelligence Revenue and Share by Players (2021-2026)
3.2 Market Share Analysis (2025)
3.2.1 Market Share of AI-Based Cyber Threat Intelligence by Company Revenue
3.2.2 Top 3 AI-Based Cyber Threat Intelligence Players Market Share in 2025
3.2.3 Top 6 AI-Based Cyber Threat Intelligence Players Market Share in 2025
3.3 AI-Based Cyber Threat Intelligence Market: Overall Company Footprint Analysis
3.3.1 AI-Based Cyber Threat Intelligence Market: Region Footprint
3.3.2 AI-Based Cyber Threat Intelligence Market: Company Product Type Footprint
3.3.3 AI-Based Cyber Threat Intelligence Market: Company Product Application Footprint
3.4 New Market Entrants and Barriers to Market Entry
3.5 Mergers, Acquisition, Agreements, and Collaborations

4 MARKET SIZE SEGMENT BY TYPE

4.1 Global AI-Based Cyber Threat Intelligence Consumption Value and Market Share by Type (2021-2026)
4.2 Global AI-Based Cyber Threat Intelligence Market Forecast by Type (2027-2032)

5 MARKET SIZE SEGMENT BY APPLICATION

5.1 Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2026)
5.2 Global AI-Based Cyber Threat Intelligence Market Forecast by Application (2027-2032)

6 NORTH AMERICA

6.1 North America AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2032)
6.2 North America AI-Based Cyber Threat Intelligence Market Size by Application (2021-2032)
6.3 North America AI-Based Cyber Threat Intelligence Market Size by Country

+357 96 030922
info@marketpublishers.com

6.3.1 North America AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2032)
6.3.2 United States AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
6.3.3 Canada AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
6.3.4 Mexico AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)

7 EUROPE

7.1 Europe AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2032)
7.2 Europe AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2032)
7.3 Europe AI-Based Cyber Threat Intelligence Market Size by Country
7.3.1 Europe AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2032)
7.3.2 Germany AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
7.3.3 France AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
7.3.4 United Kingdom AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
7.3.5 Russia AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
7.3.6 Italy AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)

8 ASIA-PACIFIC

8.1 Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2032)
8.2 Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2032)
8.3 Asia-Pacific AI-Based Cyber Threat Intelligence Market Size by Region
8.3.1 Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Region (2021-2032)
8.3.2 China AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
8.3.3 Japan AI-Based Cyber Threat Intelligence Market Size and Forecast

+357 96 030922
info@marketpublishers.com

(2021-2032)
8.3.4 South Korea AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
8.3.5 India AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
8.3.6 Southeast Asia AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
8.3.7 Australia AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)

9 SOUTH AMERICA

9.1 South America AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2032)
9.2 South America AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2032)
9.3 South America AI-Based Cyber Threat Intelligence Market Size by Country
9.3.1 South America AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2032)
9.3.2 Brazil AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
9.3.3 Argentina AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)

10 MIDDLE EAST & AFRICA

10.1 Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2032)
10.2 Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2032)
10.3 Middle East & Africa AI-Based Cyber Threat Intelligence Market Size by Country
10.3.1 Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2032)
10.3.2 Turkey AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
10.3.3 Saudi Arabia AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)
10.3.4 UAE AI-Based Cyber Threat Intelligence Market Size and Forecast (2021-2032)

11 MARKET DYNAMICS

+357 96 030922
info@marketpublishers.com

11.1 AI-Based Cyber Threat Intelligence Market Drivers
11.2 AI-Based Cyber Threat Intelligence Market Restraints
11.3 AI-Based Cyber Threat Intelligence Trends Analysis
11.4 Porters Five Forces Analysis
  11.4.1 Threat of New Entrants
  11.4.2 Bargaining Power of Suppliers
  11.4.3 Bargaining Power of Buyers
  11.4.4 Threat of Substitutes
  11.4.5 Competitive Rivalry

12 INDUSTRY CHAIN ANALYSIS

12.1 AI-Based Cyber Threat Intelligence Industry Chain
12.2 AI-Based Cyber Threat Intelligence Upstream Analysis
12.3 AI-Based Cyber Threat Intelligence Midstream Analysis
12.4 AI-Based Cyber Threat Intelligence Downstream Analysis

13 RESEARCH FINDINGS AND CONCLUSION

14 APPENDIX

14.1 Methodology
14.2 Research Process and Data Source
14.3 Disclaimer

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

Table 1. Global AI-Based Cyber Threat Intelligence Consumption Value by Type, (USD Million), 2021 & 2025 & 2032
Table 2. Global AI-Based Cyber Threat Intelligence Consumption Value by Source, (USD Million), 2021 & 2025 & 2032
Table 3. Global AI-Based Cyber Threat Intelligence Consumption Value by Number of Intelligence Sources, (USD Million), 2021 & 2025 & 2032
Table 4. Global AI-Based Cyber Threat Intelligence Consumption Value by Application, (USD Million), 2021 & 2025 & 2032
Table 5. Global AI-Based Cyber Threat Intelligence Consumption Value by Region (2021-2026) & (USD Million)
Table 6. Global AI-Based Cyber Threat Intelligence Consumption Value by Region (2027-2032) & (USD Million)
Table 7. CrowdStrike Holdings, Inc. Company Information, Head Office, and Major Competitors
Table 8. CrowdStrike Holdings, Inc. Major Business
Table 9. CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 10. CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 11. CrowdStrike Holdings, Inc. Recent Developments and Future Plans
Table 12. Recorded Future, Inc. Company Information, Head Office, and Major Competitors
Table 13. Recorded Future, Inc. Major Business
Table 14. Recorded Future, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 15. Recorded Future, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 16. Recorded Future, Inc. Recent Developments and Future Plans
Table 17. Palo Alto Networks, Inc. Company Information, Head Office, and Major Competitors
Table 18. Palo Alto Networks, Inc. Major Business
Table 19. Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 20. Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)

+357 96 030922
info@marketpublishers.com

Table 21. Fortinet, Inc. Company Information, Head Office, and Major Competitors
Table 22. Fortinet, Inc. Major Business
Table 23. Fortinet, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 24. Fortinet, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 25. Fortinet, Inc. Recent Developments and Future Plans
Table 26. Check Point Software Technologies Ltd. Company Information, Head Office, and Major Competitors
Table 27. Check Point Software Technologies Ltd. Major Business
Table 28. Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
Table 29. Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 30. Check Point Software Technologies Ltd. Recent Developments and Future Plans
Table 31. IBM Corporation Company Information, Head Office, and Major Competitors
Table 32. IBM Corporation Major Business
Table 33. IBM Corporation AI-Based Cyber Threat Intelligence Product and Solutions
Table 34. IBM Corporation AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 35. IBM Corporation Recent Developments and Future Plans
Table 36. Anomali, Inc. Company Information, Head Office, and Major Competitors
Table 37. Anomali, Inc. Major Business
Table 38. Anomali, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 39. Anomali, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 40. Anomali, Inc. Recent Developments and Future Plans
Table 41. ThreatConnect, Inc. Company Information, Head Office, and Major Competitors
Table 42. ThreatConnect, Inc. Major Business
Table 43. ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 44. ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 45. ThreatConnect, Inc. Recent Developments and Future Plans
Table 46. Group-IB Company Information, Head Office, and Major Competitors
Table 47. Group-IB Major Business
Table 48. Group-IB AI-Based Cyber Threat Intelligence Product and Solutions
Table 49. Group-IB AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross

+357 96 030922
info@marketpublishers.com

Margin and Market Share (2021-2026)
Table 50. Group-IB Recent Developments and Future Plans
Table 51. Rapid7, Inc. Company Information, Head Office, and Major Competitors
Table 52. Rapid7, Inc. Major Business
Table 53. Rapid7, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 54. Rapid7, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 55. Rapid7, Inc. Recent Developments and Future Plans
Table 56. Flashpoint Company Information, Head Office, and Major Competitors
Table 57. Flashpoint Major Business
Table 58. Flashpoint AI-Based Cyber Threat Intelligence Product and Solutions
Table 59. Flashpoint AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 60. Flashpoint Recent Developments and Future Plans
Table 61. ZeroFox Holdings, Inc. Company Information, Head Office, and Major Competitors
Table 62. ZeroFox Holdings, Inc. Major Business
Table 63. ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 64. ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 65. ZeroFox Holdings, Inc. Recent Developments and Future Plans
Table 66. Trend Micro Incorporated Company Information, Head Office, and Major Competitors
Table 67. Trend Micro Incorporated Major Business
Table 68. Trend Micro Incorporated AI-Based Cyber Threat Intelligence Product and Solutions
Table 69. Trend Micro Incorporated AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 70. Trend Micro Incorporated Recent Developments and Future Plans
Table 71. QAX Technology Group Inc. Company Information, Head Office, and Major Competitors
Table 72. QAX Technology Group Inc. Major Business
Table 73. QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 74. QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 75. QAX Technology Group Inc. Recent Developments and Future Plans
Table 76. ThreatBook Company Information, Head Office, and Major Competitors

+357 96 030922
info@marketpublishers.com

Table 77. ThreatBook Major Business
Table 78. ThreatBook AI-Based Cyber Threat Intelligence Product and Solutions
Table 79. ThreatBook AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 80. ThreatBook Recent Developments and Future Plans
Table 81. 360 Security Technology Inc. Company Information, Head Office, and Major Competitors
Table 82. 360 Security Technology Inc. Major Business
Table 83. 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Product and Solutions
Table 84. 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 85. 360 Security Technology Inc. Recent Developments and Future Plans
Table 86. NSFOCUS Technologies Group Co., Ltd. Company Information, Head Office, and Major Competitors
Table 87. NSFOCUS Technologies Group Co., Ltd. Major Business
Table 88. NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
Table 89. NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 90. NSFOCUS Technologies Group Co., Ltd. Recent Developments and Future Plans
Table 91. DBAPPSecurity Co., Ltd. Company Information, Head Office, and Major Competitors
Table 92. DBAPPSecurity Co., Ltd. Major Business
Table 93. DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Product and Solutions
Table 94. DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Revenue (USD Million), Gross Margin and Market Share (2021-2026)
Table 95. DBAPPSecurity Co., Ltd. Recent Developments and Future Plans
Table 96. Global AI-Based Cyber Threat Intelligence Revenue (USD Million) by Players (2021-2026)
Table 97. Global AI-Based Cyber Threat Intelligence Revenue Share by Players (2021-2026)
Table 98. Breakdown of AI-Based Cyber Threat Intelligence by Company Type (Tier 1, Tier 2, and Tier 3)
Table 99. Market Position of Players in AI-Based Cyber Threat Intelligence, (Tier 1, Tier 2, and Tier 3), Based on Revenue in 2025
Table 100. Head Office of Key AI-Based Cyber Threat Intelligence Players

+357 96 030922
info@marketpublishers.com

Table 101. AI-Based Cyber Threat Intelligence Market: Company Product Type Footprint
Table 102. AI-Based Cyber Threat Intelligence Market: Company Product Application Footprint
Table 103. AI-Based Cyber Threat Intelligence New Market Entrants and Barriers to Market Entry
Table 104. AI-Based Cyber Threat Intelligence Mergers, Acquisition, Agreements, and Collaborations
Table 105. Global AI-Based Cyber Threat Intelligence Consumption Value (USD Million) by Type (2021-2026)
Table 106. Global AI-Based Cyber Threat Intelligence Consumption Value Share by Type (2021-2026)
Table 107. Global AI-Based Cyber Threat Intelligence Consumption Value Forecast by Type (2027-2032)
Table 108. Global AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026)
Table 109. Global AI-Based Cyber Threat Intelligence Consumption Value Forecast by Application (2027-2032)
Table 110. North America AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2026) & (USD Million)
Table 111. North America AI-Based Cyber Threat Intelligence Consumption Value by Type (2027-2032) & (USD Million)
Table 112. North America AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026) & (USD Million)
Table 113. North America AI-Based Cyber Threat Intelligence Consumption Value by Application (2027-2032) & (USD Million)
Table 114. North America AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2026) & (USD Million)
Table 115. North America AI-Based Cyber Threat Intelligence Consumption Value by Country (2027-2032) & (USD Million)
Table 116. Europe AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2026) & (USD Million)
Table 117. Europe AI-Based Cyber Threat Intelligence Consumption Value by Type (2027-2032) & (USD Million)
Table 118. Europe AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026) & (USD Million)
Table 119. Europe AI-Based Cyber Threat Intelligence Consumption Value by Application (2027-2032) & (USD Million)
Table 120. Europe AI-Based Cyber Threat Intelligence Consumption Value by Country

+357 96 030922
info@marketpublishers.com

(2021-2026) & (USD Million)
Table 121. Europe AI-Based Cyber Threat Intelligence Consumption Value by Country (2027-2032) & (USD Million)
Table 122. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2026) & (USD Million)
Table 123. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Type (2027-2032) & (USD Million)
Table 124. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026) & (USD Million)
Table 125. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Application (2027-2032) & (USD Million)
Table 126. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Region (2021-2026) & (USD Million)
Table 127. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value by Region (2027-2032) & (USD Million)
Table 128. South America AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2026) & (USD Million)
Table 129. South America AI-Based Cyber Threat Intelligence Consumption Value by Type (2027-2032) & (USD Million)
Table 130. South America AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026) & (USD Million)
Table 131. South America AI-Based Cyber Threat Intelligence Consumption Value by Application (2027-2032) & (USD Million)
Table 132. South America AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2026) & (USD Million)
Table 133. South America AI-Based Cyber Threat Intelligence Consumption Value by Country (2027-2032) & (USD Million)
Table 134. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Type (2021-2026) & (USD Million)
Table 135. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Type (2027-2032) & (USD Million)
Table 136. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Application (2021-2026) & (USD Million)
Table 137. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Application (2027-2032) & (USD Million)
Table 138. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Country (2021-2026) & (USD Million)
Table 139. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value by Country (2027-2032) & (USD Million)

+357 96 030922
info@marketpublishers.com

Table 140. Global Key Players of AI-Based Cyber Threat Intelligence Upstream (Raw Materials)
Table 141. Global AI-Based Cyber Threat Intelligence Typical Customers

+357 96 030922
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

Figure 1. AI-Based Cyber Threat Intelligence Picture
Figure 2. Global AI-Based Cyber Threat Intelligence Consumption Value by Type, (USD Million), 2021 & 2025 & 2032
Figure 3. Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type in 2025
Figure 4. Strategic Threat Intelligence
Figure 5. Operational Threat Intelligence
Figure 6. Tactical Threat Intelligence
Figure 7. Technical Threat Intelligence
Figure 8. Global AI-Based Cyber Threat Intelligence Consumption Value by Source, (USD Million), 2021 & 2025 & 2032
Figure 9. Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Source in 2025
Figure 10. Open-Source Intelligence-Based
Figure 11. Dark Web Intelligence-Based
Figure 12. Proprietary Telemetry-Based
Figure 13. Global AI-Based Cyber Threat Intelligence Consumption Value by Number of Intelligence Sources, (USD Million), 2021 & 2025 & 2032
Figure 14. Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Number of Intelligence Sources in 2025
Figure 15. Single-Source Intelligence
Figure 16. 2–5 Source Intelligence
Figure 17. 6–20 Source Intelligence
Figure 18. More than 20 Source Intelligence
Figure 19. Global AI-Based Cyber Threat Intelligence Consumption Value by Application, (USD Million), 2021 & 2025 & 2032
Figure 20. AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application in 2025
Figure 21. Banking, Financial Services and Insurance Picture
Figure 22. Government and Defense Picture
Figure 23. IT and Telecommunications Picture
Figure 24. Healthcare Picture
Figure 25. Manufacturing Picture
Figure 26. Energy and Utilities Picture
Figure 27. Retail and E-Commerce Picture

+357 96 030922
info@marketpublishers.com

Figure 28. Global AI-Based Cyber Threat Intelligence Consumption Value, (USD Million): 2021 & 2025 & 2032
Figure 29. Global AI-Based Cyber Threat Intelligence Consumption Value and Forecast (2021-2032) & (USD Million)
Figure 30. Global Market AI-Based Cyber Threat Intelligence Consumption Value (USD Million) Comparison by Region (2021 VS 2025 VS 2032)
Figure 31. Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Region (2021-2032)
Figure 32. Global AI-Based Cyber Threat Intelligence Consumption Value Market Share by Region in 2025
Figure 33. North America AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 34. Europe AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 35. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 36. South America AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 37. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 38. Company Three Recent Developments and Future Plans
Figure 39. Global AI-Based Cyber Threat Intelligence Revenue Share by Players in 2025
Figure 40. AI-Based Cyber Threat Intelligence Market Share by Company Type (Tier 1, Tier 2, and Tier 3) in 2025
Figure 41. Market Share of AI-Based Cyber Threat Intelligence by Player Revenue in 2025
Figure 42. Top 3 AI-Based Cyber Threat Intelligence Players Market Share in 2025
Figure 43. Top 6 AI-Based Cyber Threat Intelligence Players Market Share in 2025
Figure 44. Global AI-Based Cyber Threat Intelligence Consumption Value Share by Type (2021-2026)
Figure 45. Global AI-Based Cyber Threat Intelligence Market Share Forecast by Type (2027-2032)
Figure 46. Global AI-Based Cyber Threat Intelligence Consumption Value Share by Application (2021-2026)
Figure 47. Global AI-Based Cyber Threat Intelligence Market Share Forecast by Application (2027-2032)
Figure 48. North America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type (2021-2032)

+357 96 030922
info@marketpublishers.com

Figure 49. North America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2032)
Figure 50. North America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Country (2021-2032)
Figure 51. United States AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 52. Canada AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 53. Mexico AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 54. Europe AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type (2021-2032)
Figure 55. Europe AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2032)
Figure 56. Europe AI-Based Cyber Threat Intelligence Consumption Value Market Share by Country (2021-2032)
Figure 57. Germany AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 58. France AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 59. United Kingdom AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 60. Russia AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 61. Italy AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 62. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type (2021-2032)
Figure 63. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2032)
Figure 64. Asia-Pacific AI-Based Cyber Threat Intelligence Consumption Value Market Share by Region (2021-2032)
Figure 65. China AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 66. Japan AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 67. South Korea AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 68. India AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) &

+357 96 030922
info@marketpublishers.com

(USD Million)
Figure 69. Southeast Asia AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 70. Australia AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 71. South America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type (2021-2032)
Figure 72. South America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2032)
Figure 73. South America AI-Based Cyber Threat Intelligence Consumption Value Market Share by Country (2021-2032)
Figure 74. Brazil AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 75. Argentina AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 76. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value Market Share by Type (2021-2032)
Figure 77. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value Market Share by Application (2021-2032)
Figure 78. Middle East & Africa AI-Based Cyber Threat Intelligence Consumption Value Market Share by Country (2021-2032)
Figure 79. Turkey AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 80. Saudi Arabia AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 81. UAE AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 82. AI-Based Cyber Threat Intelligence Market Drivers
Figure 83. AI-Based Cyber Threat Intelligence Market Restraints
Figure 84. AI-Based Cyber Threat Intelligence Market Trends
Figure 85. Porters Five Forces Analysis
Figure 86. AI-Based Cyber Threat Intelligence Industrial Chain
Figure 87. Methodology
Figure 88. Research Process and Data Source

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Global AI-Based Cyber Threat Intelligence Market 2026 by Company, Regions, Type and Application, Forecast to 2032

Product link: https://marketpublishers.com/r/GBFA8086EA72EN.html

Price: US$ 3,480.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/GBFA8086EA72EN.html