+357 96 030922
info@marketpublishers.com

Global AI-Based Cyber Threat Intelligence Supply, Demand and Key Producers, 2026-2032

https://marketpublishers.com/r/G6FEBAEE339FEN.html
Date: November 2026
Pages: 142
Price: US$ 4,480.00 (Single User License)
ID: G6FEBAEE339FEN

Abstracts

The global AI-Based Cyber Threat Intelligence market size is expected to reach $ 957 million by 2032, rising at a market growth of 6.0% CAGR during the forecast period (2026-2032).

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.

Key Findings

+357 96 030922
info@marketpublishers.com

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.

Market Dynamics

Drivers

+357 96 030922
info@marketpublishers.com

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-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

+357 96 030922
info@marketpublishers.com

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 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

+357 96 030922
info@marketpublishers.com

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 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

+357 96 030922
info@marketpublishers.com

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, 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,

+357 96 030922
info@marketpublishers.com

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.

Report Scope

This report studies the global AI-Based Cyber Threat Intelligence demand, key companies, and key regions.

+357 96 030922
info@marketpublishers.com

This report is a detailed and comprehensive analysis of the world market for AI-Based Cyber Threat Intelligence, and provides market size (US$ million) and Year-over-Year (YoY) growth, considering 2025 as the base year. This report explores demand trends and competition, as well as details the characteristics of AI-Based Cyber Threat Intelligence that contribute to its increasing demand across many markets.

Highlights and key features of the study

Global AI-Based Cyber Threat Intelligence total market, 2021-2032, (USD Million)

Global AI-Based Cyber Threat Intelligence total market by region & country, CAGR, 2021-2032, (USD Million)

U.S. VS China: AI-Based Cyber Threat Intelligence total market, key domestic companies, and share, (USD Million)

Global AI-Based Cyber Threat Intelligence revenue by player, revenue and market share 2021-2026, (USD Million)

Global AI-Based Cyber Threat Intelligence total market by Type, CAGR, 2021-2032, (USD Million)

Global AI-Based Cyber Threat Intelligence total market by Application, CAGR, 2021-2032, (USD Million)

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

+357 96 030922
info@marketpublishers.com

Stakeholders would have ease in decision-making through various strategy matrices used in analyzing the world AI-Based Cyber Threat Intelligence market

Detailed Segmentation:

Each section contains quantitative market data including market by value (US$ Millions), by player, by regions, by Type, and by Application. Data is given for the years 2021-2032 by year with 2025 as the base year, 2026 as the estimate year, and 2027-2032 as the forecast year.

Global AI-Based Cyber Threat Intelligence Market, By Region:

United States

China

Europe

Japan

South Korea

ASEAN

India

Rest of World

Market Segmentation

Global AI-Based Cyber Threat Intelligence Market, Segmentation by Type:

Strategic Threat Intelligence

+357 96 030922
info@marketpublishers.com

Operational Threat Intelligence

Tactical Threat Intelligence

Technical Threat Intelligence

Global AI-Based Cyber Threat Intelligence Market, Segmentation by Source:

Open-Source Intelligence-Based

Dark Web Intelligence-Based

Proprietary Telemetry-Based

Global AI-Based Cyber Threat Intelligence Market, Segmentation by Number of Intelligence Sources:

Single-Source Intelligence

2–5 Source Intelligence

6–20 Source Intelligence

More than 20 Source Intelligence

Global AI-Based Cyber Threat Intelligence Market, Segmentation by Application:

Banking, Financial Services and Insurance

Government and Defense

IT and Telecommunications

+357 96 030922
info@marketpublishers.com

Healthcare

Manufacturing

Energy and Utilities

Retail and E-Commerce

Companies Profiled:

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.

Flashpoint

ZeroFox Holdings, Inc.

Trend Micro Incorporated

QAX Technology Group Inc.

+357 96 030922
info@marketpublishers.com

ThreatBook

360 Security Technology Inc.

NSFOCUS Technologies Group Co., Ltd.

DBAPPSecurity Co., Ltd.

Key Questions Answered

1. How big is the global AI-Based Cyber Threat Intelligence market?
2. What is the demand of the global AI-Based Cyber Threat Intelligence market?
3. What is the year over year growth of the global AI-Based Cyber Threat Intelligence market?
4. What is the total value of the global AI-Based Cyber Threat Intelligence market?
5. Who are the Major Players in the global AI-Based Cyber Threat Intelligence market?
6. What are the growth factors driving the market demand?

+357 96 030922
info@marketpublishers.com

Contents

1 SUPPLY SUMMARY

1.1 AI-Based Cyber Threat Intelligence Introduction
1.2 World AI-Based Cyber Threat Intelligence Market Size & Forecast (2021 & 2025 & 2032)
1.3 World AI-Based Cyber Threat Intelligence Total Market by Region (by Headquarter Location)
  1.3.1 World AI-Based Cyber Threat Intelligence Market Size by Region (2021-2032), (by Headquarter Location)
  1.3.2 United States Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.3 China Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.4 Europe Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.5 Japan Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.6 South Korea Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.7 ASEAN Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
  1.3.8 India Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032)
1.4 Market Drivers, Restraints and Trends
  1.4.1 AI-Based Cyber Threat Intelligence Market Drivers
  1.4.2 Factors Affecting Demand
  1.4.3 Major Market Trends

2 DEMAND SUMMARY

2.1 World AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.2 World AI-Based Cyber Threat Intelligence Consumption Value by Region
  2.2.1 World AI-Based Cyber Threat Intelligence Consumption Value by Region (2021-2026)
  2.2.2 World AI-Based Cyber Threat Intelligence Consumption Value Forecast by Region (2027-2032)
2.3 United States AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.4 China AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)

+357 96 030922
info@marketpublishers.com

2.5 Europe AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.6 Japan AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.7 South Korea AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.8 ASEAN AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)
2.9 India AI-Based Cyber Threat Intelligence Consumption Value (2021-2032)

3 WORLD AI-BASED CYBER THREAT INTELLIGENCE COMPANIES COMPETITIVE ANALYSIS

3.1 World AI-Based Cyber Threat Intelligence Revenue by Player (2021-2026)
3.2 Industry Rank and Concentration Rate (CR)
  3.2.1 Global AI-Based Cyber Threat Intelligence Industry Rank of Major Players
  3.2.2 Global Concentration Ratios (CR4) for AI-Based Cyber Threat Intelligence in 2025
  3.2.3 Global Concentration Ratios (CR8) for AI-Based Cyber Threat Intelligence in 2025
3.3 AI-Based Cyber Threat Intelligence Company Evaluation Quadrant
3.4 AI-Based Cyber Threat Intelligence Market: Overall Company Footprint Analysis
  3.4.1 AI-Based Cyber Threat Intelligence Market: Region Footprint
  3.4.2 AI-Based Cyber Threat Intelligence Market: Company Product Type Footprint
  3.4.3 AI-Based Cyber Threat Intelligence Market: Company Product Application Footprint
3.5 Competitive Environment
  3.5.1 Historical Structure of the Industry
  3.5.2 Barriers of Market Entry
  3.5.3 Factors of Competition
3.6 Mergers & Acquisitions Activity

4 UNITED STATES VS CHINA VS REST OF WORLD (BY HEADQUARTER LOCATION)

4.1 United States VS China: AI-Based Cyber Threat Intelligence Revenue Comparison (by Headquarter Location)
  4.1.1 United States VS China: AI-Based Cyber Threat Intelligence Revenue Comparison (2021 & 2025 & 2032) (by Headquarter Location)
  4.1.2 United States VS China: AI-Based Cyber Threat Intelligence Revenue Market Share Comparison (2021 & 2025 & 2032)
4.2 United States Based Companies VS China Based Companies: AI-Based Cyber Threat Intelligence Consumption Value Comparison

+357 96 030922
info@marketpublishers.com

4.2.1 United States VS China: AI-Based Cyber Threat Intelligence Consumption Value Comparison (2021 & 2025 & 2032)
4.2.2 United States VS China: AI-Based Cyber Threat Intelligence Consumption Value Market Share Comparison (2021 & 2025 & 2032)
4.3 United States Based AI-Based Cyber Threat Intelligence Companies and Market Share, 2021-2026
4.3.1 United States Based AI-Based Cyber Threat Intelligence Companies, Headquarters (States, Country)
4.3.2 United States Based Companies AI-Based Cyber Threat Intelligence Revenue, (2021-2026)
4.4 China Based Companies AI-Based Cyber Threat Intelligence Revenue and Market Share, 2021-2026
4.4.1 China Based AI-Based Cyber Threat Intelligence Companies, Company Headquarters (Province, Country)
4.4.2 China Based Companies AI-Based Cyber Threat Intelligence Revenue, (2021-2026)
4.5 Rest of World Based AI-Based Cyber Threat Intelligence Companies and Market Share, 2021-2026
4.5.1 Rest of World Based AI-Based Cyber Threat Intelligence Companies, Headquarters (Province, Country)
4.5.2 Rest of World Based Companies AI-Based Cyber Threat Intelligence Revenue (2021-2026)

5 MARKET ANALYSIS BY TYPE

5.1 World AI-Based Cyber Threat Intelligence Market Size Overview by Type: 2021 VS 2025 VS 2032
5.2 Segment Introduction by Type
5.2.1 Strategic Threat Intelligence
5.2.2 Operational Threat Intelligence
5.2.3 Tactical Threat Intelligence
5.2.4 Technical Threat Intelligence
5.3 Market Segment by Type
5.3.1 World AI-Based Cyber Threat Intelligence Market Size by Type (2021-2026)
5.3.2 World AI-Based Cyber Threat Intelligence Market Size by Type (2027-2032)
5.3.3 World AI-Based Cyber Threat Intelligence Market Size Market Share by Type (2027-2032)

6 MARKET ANALYSIS BY SOURCE

+357 96 030922
info@marketpublishers.com

6.1 World AI-Based Cyber Threat Intelligence Market Size Overview by Source: 2021 VS 2025 VS 2032
6.2 Segment Introduction by Source
  6.2.1 Open-Source Intelligence-Based
  6.2.2 Dark Web Intelligence-Based
  6.2.3 Proprietary Telemetry-Based
6.3 Market Segment by Source
  6.3.1 World AI-Based Cyber Threat Intelligence Market Size by Source (2021-2026)
  6.3.2 World AI-Based Cyber Threat Intelligence Market Size by Source (2027-2032)
  6.3.3 World AI-Based Cyber Threat Intelligence Market Size Market Share by Source (2027-2032)

7 MARKET ANALYSIS BY NUMBER OF INTELLIGENCE SOURCES

7.1 World AI-Based Cyber Threat Intelligence Market Size Overview by Number of Intelligence Sources: 2021 VS 2025 VS 2032
7.2 Segment Introduction by Number of Intelligence Sources
  7.2.1 Single-Source Intelligence
  7.2.2 2–5 Source Intelligence
  7.2.3 6–20 Source Intelligence
  7.2.4 More than 20 Source Intelligence
7.3 Market Segment by Number of Intelligence Sources
  7.3.1 World AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources (2021-2026)
  7.3.2 World AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources (2027-2032)
  7.3.3 World AI-Based Cyber Threat Intelligence Market Size Market Share by Number of Intelligence Sources (2027-2032)

8 MARKET ANALYSIS BY APPLICATION

8.1 World AI-Based Cyber Threat Intelligence Market Size Overview by Application: 2021 VS 2025 VS 2032
8.2 Segment Introduction by Application
  8.2.1 Banking, Financial Services and Insurance
  8.2.2 Government and Defense
  8.2.3 IT and Telecommunications
  8.2.4 Healthcare

+357 96 030922
info@marketpublishers.com

8.2.5 Manufacturing
8.2.6 Energy and Utilities
8.2.7 Retail and E-Commerce
8.3 Market Segment by Application
8.3.1 World AI-Based Cyber Threat Intelligence Market Size by Application (2021-2026)
8.3.2 World AI-Based Cyber Threat Intelligence Market Size by Application (2027-2032)
8.3.3 World AI-Based Cyber Threat Intelligence Market Size Market Share by Application (2021-2032)

9 COMPANY PROFILES

9.1 CrowdStrike Holdings, Inc.
9.1.1 CrowdStrike Holdings, Inc. Details
9.1.2 CrowdStrike Holdings, Inc. Major Business
9.1.3 CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.1.4 CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.1.5 CrowdStrike Holdings, Inc. Recent Developments/Updates
9.1.6 CrowdStrike Holdings, Inc. Competitive Strengths & Weaknesses
9.2 Recorded Future, Inc.
9.2.1 Recorded Future, Inc. Details
9.2.2 Recorded Future, Inc. Major Business
9.2.3 Recorded Future, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.2.4 Recorded Future, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.2.5 Recorded Future, Inc. Recent Developments/Updates
9.2.6 Recorded Future, Inc. Competitive Strengths & Weaknesses
9.3 Palo Alto Networks, Inc.
9.3.1 Palo Alto Networks, Inc. Details
9.3.2 Palo Alto Networks, Inc. Major Business
9.3.3 Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.3.4 Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.3.5 Palo Alto Networks, Inc. Recent Developments/Updates
9.3.6 Palo Alto Networks, Inc. Competitive Strengths & Weaknesses

+357 96 030922
info@marketpublishers.com

9.4 Fortinet, Inc.
9.4.1 Fortinet, Inc. Details
9.4.2 Fortinet, Inc. Major Business
9.4.3 Fortinet, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.4.4 Fortinet, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.4.5 Fortinet, Inc. Recent Developments/Updates
9.4.6 Fortinet, Inc. Competitive Strengths & Weaknesses
9.5 Check Point Software Technologies Ltd.
9.5.1 Check Point Software Technologies Ltd. Details
9.5.2 Check Point Software Technologies Ltd. Major Business
9.5.3 Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Product and Services
9.5.4 Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.5.5 Check Point Software Technologies Ltd. Recent Developments/Updates
9.5.6 Check Point Software Technologies Ltd. Competitive Strengths & Weaknesses
9.6 IBM Corporation
9.6.1 IBM Corporation Details
9.6.2 IBM Corporation Major Business
9.6.3 IBM Corporation AI-Based Cyber Threat Intelligence Product and Services
9.6.4 IBM Corporation AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.6.5 IBM Corporation Recent Developments/Updates
9.6.6 IBM Corporation Competitive Strengths & Weaknesses
9.7 Anomali, Inc.
9.7.1 Anomali, Inc. Details
9.7.2 Anomali, Inc. Major Business
9.7.3 Anomali, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.7.4 Anomali, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.7.5 Anomali, Inc. Recent Developments/Updates
9.7.6 Anomali, Inc. Competitive Strengths & Weaknesses
9.8 ThreatConnect, Inc.
9.8.1 ThreatConnect, Inc. Details
9.8.2 ThreatConnect, Inc. Major Business
9.8.3 ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.8.4 ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)

+357 96 030922
info@marketpublishers.com

9.8.5 ThreatConnect, Inc. Recent Developments/Updates
9.8.6 ThreatConnect, Inc. Competitive Strengths & Weaknesses
9.9 Group-IB
9.9.1 Group-IB Details
9.9.2 Group-IB Major Business
9.9.3 Group-IB AI-Based Cyber Threat Intelligence Product and Services
9.9.4 Group-IB AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.9.5 Group-IB Recent Developments/Updates
9.9.6 Group-IB Competitive Strengths & Weaknesses
9.10 Rapid7, Inc.
9.10.1 Rapid7, Inc. Details
9.10.2 Rapid7, Inc. Major Business
9.10.3 Rapid7, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.10.4 Rapid7, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.10.5 Rapid7, Inc. Recent Developments/Updates
9.10.6 Rapid7, Inc. Competitive Strengths & Weaknesses
9.11 Flashpoint
9.11.1 Flashpoint Details
9.11.2 Flashpoint Major Business
9.11.3 Flashpoint AI-Based Cyber Threat Intelligence Product and Services
9.11.4 Flashpoint AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.11.5 Flashpoint Recent Developments/Updates
9.11.6 Flashpoint Competitive Strengths & Weaknesses
9.12 ZeroFox Holdings, Inc.
9.12.1 ZeroFox Holdings, Inc. Details
9.12.2 ZeroFox Holdings, Inc. Major Business
9.12.3 ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Services
9.12.4 ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.12.5 ZeroFox Holdings, Inc. Recent Developments/Updates
9.12.6 ZeroFox Holdings, Inc. Competitive Strengths & Weaknesses
9.13 Trend Micro Incorporated
9.13.1 Trend Micro Incorporated Details
9.13.2 Trend Micro Incorporated Major Business
9.13.3 Trend Micro Incorporated AI-Based Cyber Threat Intelligence Product and

+357 96 030922
info@marketpublishers.com

Services
9.13.4 Trend Micro Incorporated AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.13.5 Trend Micro Incorporated Recent Developments/Updates
9.13.6 Trend Micro Incorporated Competitive Strengths & Weaknesses
9.14 QAX Technology Group Inc.
9.14.1 QAX Technology Group Inc. Details
9.14.2 QAX Technology Group Inc. Major Business
9.14.3 QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Product and Services
9.14.4 QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.14.5 QAX Technology Group Inc. Recent Developments/Updates
9.14.6 QAX Technology Group Inc. Competitive Strengths & Weaknesses
9.15 ThreatBook
9.15.1 ThreatBook Details
9.15.2 ThreatBook Major Business
9.15.3 ThreatBook AI-Based Cyber Threat Intelligence Product and Services
9.15.4 ThreatBook AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.15.5 ThreatBook Recent Developments/Updates
9.15.6 ThreatBook Competitive Strengths & Weaknesses
9.16 360 Security Technology Inc.
9.16.1 360 Security Technology Inc. Details
9.16.2 360 Security Technology Inc. Major Business
9.16.3 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Product and Services
9.16.4 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.16.5 360 Security Technology Inc. Recent Developments/Updates
9.16.6 360 Security Technology Inc. Competitive Strengths & Weaknesses
9.17 NSFOCUS Technologies Group Co., Ltd.
9.17.1 NSFOCUS Technologies Group Co., Ltd. Details
9.17.2 NSFOCUS Technologies Group Co., Ltd. Major Business
9.17.3 NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Product and Services
9.17.4 NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.17.5 NSFOCUS Technologies Group Co., Ltd. Recent Developments/Updates

+357 96 030922
info@marketpublishers.com

9.17.6 NSFOCUS Technologies Group Co., Ltd. Competitive Strengths & Weaknesses
9.18 DBAPPSecurity Co., Ltd.
9.18.1 DBAPPSecurity Co., Ltd. Details
9.18.2 DBAPPSecurity Co., Ltd. Major Business
9.18.3 DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Product and Services
9.18.4 DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026)
9.18.5 DBAPPSecurity Co., Ltd. Recent Developments/Updates
9.18.6 DBAPPSecurity Co., Ltd. Competitive Strengths & Weaknesses

10 INDUSTRY CHAIN ANALYSIS

10.1 AI-Based Cyber Threat Intelligence Industry Chain
10.2 AI-Based Cyber Threat Intelligence Upstream Analysis
10.3 AI-Based Cyber Threat Intelligence Midstream Analysis
10.4 AI-Based Cyber Threat Intelligence Downstream Analysis

11 RESEARCH FINDINGS AND CONCLUSION

12 APPENDIX

12.1 Methodology
12.2 Research Process and Data Source
12.3 Disclaimer

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

Table 1. World AI-Based Cyber Threat Intelligence Revenue by Region (2021, 2025 and 2032) & (USD Million), (by Headquarter Location)
Table 2. World AI-Based Cyber Threat Intelligence Revenue by Region (2021-2026) & (USD Million), (by Headquarter Location)
Table 3. World AI-Based Cyber Threat Intelligence Revenue by Region (2027-2032) & (USD Million), (by Headquarter Location)
Table 4. World AI-Based Cyber Threat Intelligence Revenue Market Share by Region (2021-2026), (by Headquarter Location)
Table 5. World AI-Based Cyber Threat Intelligence Revenue Market Share by Region (2027-2032), (by Headquarter Location)
Table 6. Major Market Trends
Table 7. World AI-Based Cyber Threat Intelligence Consumption Value Growth Rate Forecast by Region (2021 & 2025 & 2032) & (USD Million)
Table 8. World AI-Based Cyber Threat Intelligence Consumption Value by Region (2021-2026) & (USD Million)
Table 9. World AI-Based Cyber Threat Intelligence Consumption Value Forecast by Region (2027-2032) & (USD Million)
Table 10. World AI-Based Cyber Threat Intelligence Revenue by Player (2021-2026) & (USD Million)
Table 11. Revenue Market Share of Key AI-Based Cyber Threat Intelligence Players in 2025
Table 12. World AI-Based Cyber Threat Intelligence Industry Rank of Major Player, Based on Revenue in 2025
Table 13. Global AI-Based Cyber Threat Intelligence Company Evaluation Quadrant
Table 14. Head Office of Key AI-Based Cyber Threat Intelligence Players
Table 15. AI-Based Cyber Threat Intelligence Market: Company Product Type Footprint
Table 16. AI-Based Cyber Threat Intelligence Market: Company Product Application Footprint
Table 17. AI-Based Cyber Threat Intelligence Mergers & Acquisitions Activity
Table 18. United States VS China AI-Based Cyber Threat Intelligence Revenue Comparison, (2021 & 2025 & 2032) & (USD Million)
Table 19. United States VS China AI-Based Cyber Threat Intelligence Consumption Value Comparison, (2021 & 2025 & 2032) & (USD Million)
Table 20. United States Based AI-Based Cyber Threat Intelligence Companies, Headquarters (States, Country)

+357 96 030922
info@marketpublishers.com

Table 21. United States Based Companies AI-Based Cyber Threat Intelligence Revenue, (2021-2026) & (USD Million)
Table 22. United States Based Companies AI-Based Cyber Threat Intelligence Revenue Market Share (2021-2026)
Table 23. China Based AI-Based Cyber Threat Intelligence Companies, Headquarters (Province, Country)
Table 24. China Based Companies AI-Based Cyber Threat Intelligence Revenue, (2021-2026) & (USD Million)
Table 25. China Based Companies AI-Based Cyber Threat Intelligence Revenue Market Share (2021-2026)
Table 26. Rest of World Based AI-Based Cyber Threat Intelligence Companies, Headquarters (Province, Country)
Table 27. Rest of World Based Companies AI-Based Cyber Threat Intelligence Revenue (2021-2026) & (USD Million)
Table 28. Rest of World Based Companies AI-Based Cyber Threat Intelligence Revenue Market Share (2021-2026)
Table 29. World AI-Based Cyber Threat Intelligence Market Size by Type, (USD Million), 2021 & 2025 & 2032
Table 30. World AI-Based Cyber Threat Intelligence Market Size Value by Type (2021-2026) & (USD Million)
Table 31. World AI-Based Cyber Threat Intelligence Market Size by Type (2027-2032) & (USD Million)
Table 32. World AI-Based Cyber Threat Intelligence Market Size by Source, (USD Million), 2021 & 2025 & 2032
Table 33. World AI-Based Cyber Threat Intelligence Market Size Value by Source (2021-2026) & (USD Million)
Table 34. World AI-Based Cyber Threat Intelligence Market Size by Source (2027-2032) & (USD Million)
Table 35. World AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources, (USD Million), 2021 & 2025 & 2032
Table 36. World AI-Based Cyber Threat Intelligence Market Size Value by Number of Intelligence Sources (2021-2026) & (USD Million)
Table 37. World AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources (2027-2032) & (USD Million)
Table 38. World AI-Based Cyber Threat Intelligence Market Size by Application, (USD Million), 2021 & 2025 & 2032
Table 39. World AI-Based Cyber Threat Intelligence Market Size by Application (2021-2026) & (USD Million)
Table 40. World AI-Based Cyber Threat Intelligence Market Size by Application

+357 96 030922
info@marketpublishers.com

(2027-2032) & (USD Million)
Table 41. CrowdStrike Holdings, Inc. Basic Information, Manufacturing Base and Competitors
Table 42. CrowdStrike Holdings, Inc. Major Business
Table 43. CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 44. CrowdStrike Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 45. CrowdStrike Holdings, Inc. Recent Developments/Updates
Table 46. CrowdStrike Holdings, Inc. Competitive Strengths & Weaknesses
Table 47. Recorded Future, Inc. Basic Information, Manufacturing Base and Competitors
Table 48. Recorded Future, Inc. Major Business
Table 49. Recorded Future, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 50. Recorded Future, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 51. Recorded Future, Inc. Recent Developments/Updates
Table 52. Recorded Future, Inc. Competitive Strengths & Weaknesses
Table 53. Palo Alto Networks, Inc. Basic Information, Manufacturing Base and Competitors
Table 54. Palo Alto Networks, Inc. Major Business
Table 55. Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 56. Palo Alto Networks, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 57. Palo Alto Networks, Inc. Recent Developments/Updates
Table 58. Palo Alto Networks, Inc. Competitive Strengths & Weaknesses
Table 59. Fortinet, Inc. Basic Information, Manufacturing Base and Competitors
Table 60. Fortinet, Inc. Major Business
Table 61. Fortinet, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 62. Fortinet, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 63. Fortinet, Inc. Recent Developments/Updates
Table 64. Fortinet, Inc. Competitive Strengths & Weaknesses
Table 65. Check Point Software Technologies Ltd. Basic Information, Manufacturing Base and Competitors
Table 66. Check Point Software Technologies Ltd. Major Business
Table 67. Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence

+357 96 030922
info@marketpublishers.com

Product and Services
Table 68. Check Point Software Technologies Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 69. Check Point Software Technologies Ltd. Recent Developments/Updates
Table 70. Check Point Software Technologies Ltd. Competitive Strengths & Weaknesses
Table 71. IBM Corporation Basic Information, Manufacturing Base and Competitors
Table 72. IBM Corporation Major Business
Table 73. IBM Corporation AI-Based Cyber Threat Intelligence Product and Services
Table 74. IBM Corporation AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 75. IBM Corporation Recent Developments/Updates
Table 76. IBM Corporation Competitive Strengths & Weaknesses
Table 77. Anomali, Inc. Basic Information, Manufacturing Base and Competitors
Table 78. Anomali, Inc. Major Business
Table 79. Anomali, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 80. Anomali, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 81. Anomali, Inc. Recent Developments/Updates
Table 82. Anomali, Inc. Competitive Strengths & Weaknesses
Table 83. ThreatConnect, Inc. Basic Information, Manufacturing Base and Competitors
Table 84. ThreatConnect, Inc. Major Business
Table 85. ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 86. ThreatConnect, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 87. ThreatConnect, Inc. Recent Developments/Updates
Table 88. ThreatConnect, Inc. Competitive Strengths & Weaknesses
Table 89. Group-IB Basic Information, Manufacturing Base and Competitors
Table 90. Group-IB Major Business
Table 91. Group-IB AI-Based Cyber Threat Intelligence Product and Services
Table 92. Group-IB AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 93. Group-IB Recent Developments/Updates
Table 94. Group-IB Competitive Strengths & Weaknesses
Table 95. Rapid7, Inc. Basic Information, Manufacturing Base and Competitors
Table 96. Rapid7, Inc. Major Business
Table 97. Rapid7, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 98. Rapid7, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)

+357 96 030922
info@marketpublishers.com

Table 99. Rapid7, Inc. Recent Developments/Updates
Table 100. Rapid7, Inc. Competitive Strengths & Weaknesses
Table 101. Flashpoint Basic Information, Manufacturing Base and Competitors
Table 102. Flashpoint Major Business
Table 103. Flashpoint AI-Based Cyber Threat Intelligence Product and Services
Table 104. Flashpoint AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 105. Flashpoint Recent Developments/Updates
Table 106. Flashpoint Competitive Strengths & Weaknesses
Table 107. ZeroFox Holdings, Inc. Basic Information, Manufacturing Base and Competitors
Table 108. ZeroFox Holdings, Inc. Major Business
Table 109. ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 110. ZeroFox Holdings, Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 111. ZeroFox Holdings, Inc. Recent Developments/Updates
Table 112. ZeroFox Holdings, Inc. Competitive Strengths & Weaknesses
Table 113. Trend Micro Incorporated Basic Information, Manufacturing Base and Competitors
Table 114. Trend Micro Incorporated Major Business
Table 115. Trend Micro Incorporated AI-Based Cyber Threat Intelligence Product and Services
Table 116. Trend Micro Incorporated AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 117. Trend Micro Incorporated Recent Developments/Updates
Table 118. Trend Micro Incorporated Competitive Strengths & Weaknesses
Table 119. QAX Technology Group Inc. Basic Information, Manufacturing Base and Competitors
Table 120. QAX Technology Group Inc. Major Business
Table 121. QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 122. QAX Technology Group Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 123. QAX Technology Group Inc. Recent Developments/Updates
Table 124. QAX Technology Group Inc. Competitive Strengths & Weaknesses
Table 125. ThreatBook Basic Information, Manufacturing Base and Competitors
Table 126. ThreatBook Major Business
Table 127. ThreatBook AI-Based Cyber Threat Intelligence Product and Services

+357 96 030922
info@marketpublishers.com

Table 128. ThreatBook AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 129. ThreatBook Recent Developments/Updates
Table 130. ThreatBook Competitive Strengths & Weaknesses
Table 131. 360 Security Technology Inc. Basic Information, Manufacturing Base and Competitors
Table 132. 360 Security Technology Inc. Major Business
Table 133. 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Product and Services
Table 134. 360 Security Technology Inc. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 135. 360 Security Technology Inc. Recent Developments/Updates
Table 136. 360 Security Technology Inc. Competitive Strengths & Weaknesses
Table 137. NSFOCUS Technologies Group Co., Ltd. Basic Information, Manufacturing Base and Competitors
Table 138. NSFOCUS Technologies Group Co., Ltd. Major Business
Table 139. NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Product and Services
Table 140. NSFOCUS Technologies Group Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 141. NSFOCUS Technologies Group Co., Ltd. Recent Developments/Updates
Table 142. NSFOCUS Technologies Group Co., Ltd. Competitive Strengths & Weaknesses
Table 143. DBAPPSecurity Co., Ltd. Basic Information, Manufacturing Base and Competitors
Table 144. DBAPPSecurity Co., Ltd. Major Business
Table 145. DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Product and Services
Table 146. DBAPPSecurity Co., Ltd. AI-Based Cyber Threat Intelligence Revenue, Gross Margin and Market Share (2021-2026) & (USD Million)
Table 147. DBAPPSecurity Co., Ltd. Recent Developments/Updates
Table 148. DBAPPSecurity Co., Ltd. Competitive Strengths & Weaknesses
Table 149. Global Key Players of AI-Based Cyber Threat Intelligence Upstream (Raw Materials)
Table 150. 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. World AI-Based Cyber Threat Intelligence Total Revenue: 2021 & 2025 & 2032, (USD Million)
Figure 3. World AI-Based Cyber Threat Intelligence Total Revenue (2021-2032) & (USD Million)
Figure 4. World AI-Based Cyber Threat Intelligence Revenue by Region (2021, 2025 and 2032) & (USD Million), (by Headquarter Location)
Figure 5. World AI-Based Cyber Threat Intelligence Revenue Market Share by Region (2021-2032), (by Headquarter Location)
Figure 6. United States Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 7. China Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 8. Europe Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 9. Japan Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 10. South Korea Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 11. ASEAN Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 12. India Based Company AI-Based Cyber Threat Intelligence Revenue (2021-2032) & (USD Million)
Figure 13. AI-Based Cyber Threat Intelligence Market Drivers
Figure 14. Factors Affecting Demand
Figure 15. World AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 16. World AI-Based Cyber Threat Intelligence Consumption Value Market Share by Region (2021-2032)
Figure 17. United States AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 18. China AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 19. Europe AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)

+357 96 030922
info@marketpublishers.com

Figure 20. Japan AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 21. South Korea AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 22. ASEAN AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 23. India AI-Based Cyber Threat Intelligence Consumption Value (2021-2032) & (USD Million)
Figure 24. Producer Shipments of AI-Based Cyber Threat Intelligence by Player Revenue ($MM) and Market Share (%): 2025
Figure 25. Global Four-firm Concentration Ratios (CR4) for AI-Based Cyber Threat Intelligence Markets in 2025
Figure 26. Global Four-firm Concentration Ratios (CR8) for AI-Based Cyber Threat Intelligence Markets in 2025
Figure 27. United States VS China: AI-Based Cyber Threat Intelligence Revenue Market Share Comparison (2021 & 2025 & 2032)
Figure 28. United States VS China: AI-Based Cyber Threat Intelligence Consumption Value Market Share Comparison (2021 & 2025 & 2032)
Figure 29. World AI-Based Cyber Threat Intelligence Market Size by Type, (USD Million), 2021 & 2025 & 2032
Figure 30. World AI-Based Cyber Threat Intelligence Market Size Market Share by Type in 2025
Figure 31. Strategic Threat Intelligence
Figure 32. Operational Threat Intelligence
Figure 33. Tactical Threat Intelligence
Figure 34. Technical Threat Intelligence
Figure 35. World AI-Based Cyber Threat Intelligence Market Size Market Share by Type (2021-2032)
Figure 36. World AI-Based Cyber Threat Intelligence Market Size by Source, (USD Million), 2021 & 2025 & 2032
Figure 37. World AI-Based Cyber Threat Intelligence Market Size Market Share by Source in 2025
Figure 38. Open-Source Intelligence-Based
Figure 39. Dark Web Intelligence-Based
Figure 40. Proprietary Telemetry-Based
Figure 41. World AI-Based Cyber Threat Intelligence Market Size Market Share by Source (2021-2032)
Figure 42. World AI-Based Cyber Threat Intelligence Market Size by Number of Intelligence Sources, (USD Million), 2021 & 2025 & 2032

+357 96 030922
info@marketpublishers.com

Figure 43. World AI-Based Cyber Threat Intelligence Market Size Market Share by Number of Intelligence Sources in 2025
Figure 44. Single-Source Intelligence
Figure 45. 2–5 Source Intelligence
Figure 46. 6–20 Source Intelligence
Figure 47. More than 20 Source Intelligence
Figure 48. World AI-Based Cyber Threat Intelligence Market Size Market Share by Number of Intelligence Sources (2021-2032)
Figure 49. World AI-Based Cyber Threat Intelligence Market Size by Application, (USD Million), 2021 & 2025 & 2032
Figure 50. World AI-Based Cyber Threat Intelligence Market Size Market Share by Application in 2025
Figure 51. Banking, Financial Services and Insurance
Figure 52. Government and Defense
Figure 53. IT and Telecommunications
Figure 54. Healthcare
Figure 55. Manufacturing
Figure 56. Energy and Utilities
Figure 57. Retail and E-Commerce
Figure 58. World AI-Based Cyber Threat Intelligence Market Size Market Share by Application (2021-2032)
Figure 59. AI-Based Cyber Threat Intelligence Industrial Chain
Figure 60. Methodology
Figure 61. Research Process and Data Source

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Global AI-Based Cyber Threat Intelligence Supply, Demand and Key Producers, 2026-2032

Product link: https://marketpublishers.com/r/G6FEBAEE339FEN.html

Price: US$ 4,480.00 (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/G6FEBAEE339FEN.html