+357 96 030922
info@marketpublishers.com

Cyber Threat Intelligence Market Forecasts to 2032 – Global Analysis By Intelligence Type (Strategic Intelligence, Tactical Intelligence, Operational Intelligence and Technical Intelligence), Component, Deployment Mode, Application, End User and By Geography

https://marketpublishers.com/r/CD865285AF9FEN.html
Date: October 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: CD865285AF9FEN

Abstracts

According to Stratistics MRC, the Global Cyber Threat Intelligence Market is accounted for $7.3 billion in 2025 and is expected to reach $29.5 billion by 2032 growing at a CAGR of 22% during the forecast period. Cyber Threat Intelligence (CTI) refers to the collection, analysis, and interpretation of data about potential or existing threats targeting an organization's digital environment. It involves gathering insights from various sources to understand threat actors' motives, tactics, and techniques. CTI helps organizations anticipate cyberattacks, strengthen their defenses, and make informed security decisions. By transforming raw data into actionable intelligence, CTI supports proactive threat detection, incident response, and risk management, ultimately enhancing overall cybersecurity resilience and reducing the likelihood of successful attacks.

Market Dynamics:

Driver:

Regulatory & compliance pressure

Regulatory and compliance pressure is prompting organizations to adopt proactive threat intelligence platforms across sectors. Governments and industry bodies are

+357 96 030922
info@marketpublishers.com

mandating real-time monitoring, incident reporting, and data breach prevention. Integration with SIEM, SOAR, and endpoint protection tools is enhancing visibility and response capabilities. Vendors are aligning solutions with GDPR, HIPAA, and NIST frameworks to support audit readiness. The market is shifting toward compliance-driven intelligence ecosystems.

Restraint:

High cost of implementation and maintenance

High cost of implementation and maintenance is affecting adoption of advanced threat intelligence systems. Organizations face challenges in scaling infrastructure, training personnel, and integrating with legacy environments. Subscription fees, data feed costs, and customization requirements add to operational overhead. ROI is often delayed due to long onboarding cycles and complex configuration needs. These barriers are limiting market penetration in cost-sensitive segments.

Opportunity:

Digital transformation, cloud & IoT adoption

Enterprise modernization and hybrid work models are expanding demand for predictive and adaptive security frameworks. Organizations are investing in platforms that can correlate data across endpoints, networks, and cloud assets. Integration with AI and machine learning is improving threat detection and contextual analysis. Partnerships between cybersecurity vendors and cloud providers are accelerating solution deployment. This momentum is driving intelligence-led security across industries.

Threat:

Integration complexity & lack of standardization

Integration complexity and lack of standardization are slowing deployment of unified threat intelligence platforms. Organizations struggle to harmonize data formats, APIs, and alert protocols across tools and teams. Limited interoperability reduces visibility and increases response time during active threats. Vendors must address compatibility with legacy systems and emerging technologies simultaneously. These challenges are reshaping product design and partnership strategies.

+357 96 030922
info@marketpublishers.com

Covid-19 Impact:

The pandemic accelerated cyber risk exposure as remote work and cloud migration surged globally. Organizations faced increased phishing, ransomware, and insider threats during operational disruption. Cyber threat intelligence platforms became essential for monitoring distributed endpoints and cloud workloads. Investment in real-time analytics and automated response tools rose sharply during recovery. Regulatory scrutiny around data protection intensified across healthcare, finance, and government sectors. The crisis permanently elevated threat intelligence from tactical support to strategic necessity.

The strategic intelligence segment is expected to be the largest during the forecast period

The strategic intelligence segment is expected to account for the largest market share during the forecast period due to its role in informing long-term security planning and executive decision-making. This segment focuses on geopolitical risk, adversary profiling, and industry-specific threat trends. Enterprises are integrating strategic feeds into board-level dashboards and risk management frameworks. Vendors are offering tailored insights for sectors such as finance, energy, and defense. Demand for contextual intelligence and predictive modeling is rising across regulated industries. This segment anchors the intelligence layer of enterprise cybersecurity.

The managed services segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the managed services segment is predicted to witness the highest growth rate as organizations seek scalable, cost-effective threat intelligence capabilities. Providers offer 24/7 monitoring, incident response, and threat hunting without requiring in-house expertise. SMEs and large enterprises are outsourcing intelligence operations to reduce complexity and improve agility. Integration with MDR, MSSP, and SOC-as-a-Service models is expanding service scope. Demand for turnkey solutions is rising across healthcare, retail, and manufacturing. This segment is redefining how threat intelligence is delivered and consumed.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share due to its mature cybersecurity ecosystem, regulatory enforcement, and

+357 96 030922
info@marketpublishers.com

high digital exposure. The United States and Canada are scaling threat intelligence adoption across finance, healthcare, and government sectors. Investment in AI-driven platforms, threat sharing networks, and zero-trust architectures is driving innovation. Presence of leading cybersecurity vendors and research institutions is reinforcing market strength. Regulatory mandates such as CCPA and HIPAA are accelerating platform deployment.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR as digital infrastructure, cloud adoption, and cyber risk awareness expand. Countries like China, India, Japan, and Australia are investing in national cybersecurity frameworks and enterprise threat intelligence. Local vendors and global providers are launching region-specific platforms tailored to language, regulation, and threat landscape. Growth in e-commerce, fintech, and smart cities is increasing demand for real-time monitoring and predictive analytics. Government-backed initiatives and public-private partnerships are accelerating market maturity.

Key players in the market

Some of the key players in Cyber Threat Intelligence Market include Recorded Future, Mandiant, CrowdStrike Holdings, Inc., Palo Alto Networks, IBM Security, Cisco Talos Intelligence Group, Check Point Software Technologies, FireEye, Fortinet, Inc., Kaspersky Lab, Group-IB, EclecticIQ, ThreatConnect, Anomali and Intel 471.

Key Developments:

In September 2024, Recorded Future acquired by Mastercard announced for about $2.65 billion, citing the need to bolster payment-ecosystem security and fraud prevention with Recorded Future’s AI-driven threat intelligence. The deal, signaled Mastercard’s strategic push to embed advanced cyber intelligence into its global security stack and expand its threat detection capabilities.

In August 2024, Mandiant partnered with Rubrik to integrate its threat intelligence into Rubrik’s backup and recovery platform. This integration allows organizations to detect threats within backup data, enhancing visibility across potential attack surfaces. It also accelerates incident response and improves recovery during security incidents.

Intelligence Types Covered:

+357 96 030922
info@marketpublishers.com

- Strategic Intelligence
- Tactical Intelligence
- Operational Intelligence
- Technical Intelligence

Components Covered:

- Threat Intelligence Platforms
- Threat Feeds & Aggregators
- Threat Analysis Tools
- Managed Services
- Professional Services

Deployment Modes Covered:

- On-Premise
- Cloud-Based

Applications Covered:

- Security Information & Event Management (SIEM)
- Incident Response & Forensics
- Threat Hunting & Detection
- Vulnerability Management

+357 96 030922
info@marketpublishers.com

- Risk & Compliance Management
- Other Applications

End Users Covered:

- BFSI
- Government & Defense
- IT & Telecom
- Healthcare
- Energy & Utilities
- Retail & E-commerce
- Manufacturing
- Other End Users

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK

+357 96 030922
info@marketpublishers.com

- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

- Saudi Arabia

+357 96 030922
info@marketpublishers.com

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

+357 96 030922
info@marketpublishers.com

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

5 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY INTELLIGENCE TYPE

5.1 Introduction
5.2 Strategic Intelligence
5.3 Tactical Intelligence
5.4 Operational Intelligence
5.5 Technical Intelligence

6 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY COMPONENT

6.1 Introduction
6.2 Threat Intelligence Platforms
6.3 Threat Feeds & Aggregators
6.4 Threat Analysis Tools
6.5 Managed Services
6.6 Professional Services

7 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY DEPLOYMENT MODE

7.1 Introduction
7.2 On-Premise
7.3 Cloud-Based

8 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY APPLICATION

8.1 Introduction
8.2 Security Information & Event Management (SIEM)
8.3 Incident Response & Forensics
8.4 Threat Hunting & Detection
8.5 Vulnerability Management
8.6 Risk & Compliance Management
8.7 Other Applications

9 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY END USER

9.1 Introduction
9.2 BFSI
9.3 Government & Defense
9.4 IT & Telecom

+357 96 030922
info@marketpublishers.com

10 GLOBAL CYBER THREAT INTELLIGENCE MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cyber Threat Intelligence Market Forecasts to 2032 – Global Analysis By Intelligence Type (Strategic Intelligence, Tactical Intelligence, Operational Intelligence and Technical Intelligence), Component, Deployment Mode, Application, End User and By Geography

Product link: https://marketpublishers.com/r/CD865285AF9FEN.html

Price: US$ 4,150.00 (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/CD865285AF9FEN.html