Cybersecurity Certification Market by Certification Category (Cloud Security, Information Security, AI Certifications), Target User (Individual Professionals and Enterprises), Delivery Mode (Online and in-person) - Global Forecast to 2030

https://marketpublishers.com/r/CFD27F282F9CEN.html
Date: December 2024
Pages: 310
Price: US$ 4,950.00 (Single User License)
ID: CFD27F282F9CEN

Abstracts

The global CyberSecurity Certification market size is projected to grow from USD 3,987.6 million in 2024 to USD 8,033.5 million by 2030 at a Compound Annual Growth Rate (CAGR) of 12.4% during the forecast period.

The Government regulations in the form of the EU Cybersecurity Act, GDPR, and CMMC are forcing the demand for certification for greater compliance and security practice. The increase in cloud computing, IoT, and remote work exposed new vulnerabilities to organisations, making the demand for experts urgent. A global shortage of more than 3.5 million cybersecurity experts underscores the essential role of certification in addressing this gap. Emerging technologies in AI, ML, and blockchain complicates threats; therefore, specialized certifications are required. Sectors such as finance and healthcare require tailor-made certifications complying with compliance standards, driving the demand for cybersecurity certification services.

'By Offering Segment, the Certification Services will grow at a higher CAGR during the forecast period.'

The Certification Services segment is expected to grow at the highest CAGR driven by escalating cyber threats, workforce skill gaps, and regulatory demands. Organizations are focusing on certifications to secure sensitive data and systems, adhere to frameworks such as NIST, and regulations such as the GDPR, and address emerging technologies like IoT and AI. Industry-specific certifications address different considerations, thereby making it more attractive and increasing the sector's growth. As such, certification services are of paramount importance in market expansion since regulatory norms face continuous updates.

'By Certification Category Segment, the Information Security Certification segment accounts for the largest market size during the forecast period. '

The Information Security Certifications are facing high demand due to cyber threats, need for securing data, adhering to compliance, regulatory demands, and emerging technologies. Certifications ensure that security practices are being followed and there is adherence to a very significant framework like GDPR or HIPAA, thereby driving demand in the market. Organizations seek certifications to standardize cybersecurity practices and establish increased credibility and to meet industry-specific demands in cloud security and healthcare security. Reputable bodies such as ISC2 and ISACA help build the integrity of a certification, fuel individual career growth, and increase organizational credibility. Certification such as CISSP and CompTIA Security+ tend to improve employability, so becoming certified is important in addressing emergent security issues.

By Region, Asia Pacific will grow at the highest CAGR during the forecast period.

The Asia Pacific region is among the fastest-growing regions for the cybersecurity certification market, driven by rapid digital transformation, growing cyber threats, regulatory compliance, and increased investment in cybersecurity. With increasing internet and mobile usage and technologies such as IoT, cloud computing, and 5G, exposure to cyber risks is increasing; thus, strong security requires certifications. With a number of threat types in the region-state-sponsored attacks and sophisticated organized cybercrime-it is important to have an effective, trained, and certified workforce. A strict regulatory and government mandate drives certification demand to meet requirements for compliance and credibility. Moreover, national initiatives and investments in cybersecurity infrastructure further establish Asia Pacific as a strategic market for protecting digital assets.

Breakdown of primaries:

In-depth interviews were conducted with Chief Executive Officers (CEOs), marketing directors, other innovation and technology directors, and executives from various key organizations operating in the Cybersecurity Certification market.

By Company Type: Tier 1:40%, Tier 2: 35%, and Tier 3: 25%

By Designation: C Level Executives: 45%, Directors: 35% and Managers: 20%

By Region: North America: 35%, Asia pacific: 30%, Europe: 25%, Middle East and Asia: 5%, Latin America: 5%

SGS(Switzerland), DEKRA(Germany), Intertek(UK), Bureau Veritas(France), DNV GL(Norway), TUV SUD(Germany), UL Solutions(US), Eurofins Scientific (Luxembourg), TUV NORD(Germany), Element(UK), Keysight(US), BSI(UK), TUV Rheinland(Germany), EY Certifypoint(Netherlands), A-Lign(Florida), HITRUST(US), Schellman(US), Coalfire Certification(US), DQS(Germany), Control Case(US), ISC2(US), Infosec Train(India), EXIDA(US), ISASecure(US), ISACA(US), and CompTIA(US) are some of the key players in the Cybersecurity Certification market. The study includes an in-depth competitive analysis of these key players in the Cybersecurity Certification Market, with their company profiles, recent developments, and key market strategies.

Research Coverage

The report comprehensively segments the Cybersecurity Certification Market. It provides forecasts regarding its size across various dimensions, including By Offering(Platform & Tools, Certification Services), By Certification Category(Network Security Certifications, Cloud Security Certification, Information Security Certifications, Governance, Risk, And Compliance (GRC) Certifications, Artificial Intelligence (AI) Certifications, Application Security Certifications, Device & IoT Security Certification, Others, Operational Technology (OT) Security Certifications,), By Target User(Individual Professionals, Entreprises), By Delivery mode(Online and In-person), By Vertical(BFSI, Government & Defense, IT& ITeS, Telecommunication, Healthcare, Automotive, Other Verticals) and Region (North America, Europe, Middle East & Africa, Asia Pacific, and Latin America). Additionally, the study encompasses a thorough competitive analysis of key market players, offering insights into their company profiles, product and business offerings, recent developments, and key market strategies.

Key benefits of buying report

The report offers valuable insights to market leaders and new entrants by closely approximating the Cybersecurity Certification market's revenue figures and subsegments. Stakeholders can leverage this report to better understand the competitive landscape, enabling them to position their businesses more effectively and develop tailored go-to-market strategies. Additionally, stakeholders can grasp the market dynamics and stay informed about key drivers, restraints, challenges, and opportunities shaping the industry landscape.

The report provides insights on the following pointers:

Analysis of critical drivers (Rising cyber-attacks and data breaches are driving the demand for certified cybersecurity professionals, Increasing complexity of the regulatory landscape is driving enterprises to adopt cybersecurity certification services, Growing IoT adoption driving demand for specialized cybersecurity certifications), restraints (High certification costs, Need for certifications renewal,), opportunities (Rising demand for industry-specific certifications, Increased adoption of corporate training programs), and challenges (Rapid technological changes, Cybersecurity skill gaps).

Product Development/Innovation: Detailed insights on upcoming technologies, research development activities, new products, and service launches in the Cybersecurity Certification market.

Market Development: Comprehensive information about lucrative markets – the report analyses the Cybersecurity Certification market across varied regions.

Market Diversification: Exhaustive information about new products and services, untapped geographies, recent developments, and investments.

Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players SGS(Switzerland), DNV GL(Norway), Bureau Veritas(France), TUV SUD(Germany), UL LLC(US).

Contents

1 INTRODUCTION

1.1 STUDY OBJECTIVES
1.2 MARKET DEFINITION
  1.2.1 INCLUSIONS AND EXCLUSIONS
1.3 STUDY SCOPE
  1.3.1 MARKET SEGMENTATION
  1.3.2 YEARS CONSIDERED
1.4 CURRENCY CONSIDERED
1.5 STAKEHOLDERS

2 RESEARCH METHODOLOGY

2.1 RESEARCH DATA
  2.1.1 SECONDARY DATA
  2.1.2 PRIMARY DATA
    2.1.2.1 Breakup of primary profiles
    2.1.2.2 Key insights from industry experts
2.2 DATA TRIANGULATION
2.3 MARKET SIZE ESTIMATION
  2.3.1 TOP-DOWN APPROACH
  2.3.2 BOTTOM-UP APPROACH
2.4 MARKET FORECAST
2.5 ASSUMPTIONS
2.6 RESEARCH LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

4.1 ATTRACTIVE OPPORTUNITIES FOR KEY PLAYERS IN CYBERSECURITY CERTIFICATION MARKET
4.2 CYBERSECURITY CERTIFICATION MARKET, BY OFFERING
4.3 CYBERSECURITY CERTIFICATION MARKET, BY CERTIFICATION CATEGORY
4.4 CYBERSECURITY CERTIFICATION MARKET, BY TARGET USER
4.5 CYBERSECURITY CERTIFICATION MARKET, BY DELIVERY MODE
4.6 CYBERSECURITY CERTIFICATION MARKET, BY VERTICAL

4.7 MARKET INVESTMENT SCENARIO

5 MARKET OVERVIEW AND INDUSTRY TRENDS

5.1 INTRODUCTION
5.2 MARKET DYNAMICS
5.2.1 DRIVERS
5.2.1.1 Rising cyberattacks and data breaches driving demand for certified cybersecurity professionals
5.2.1.2 Increasing complexity of regulatory landscape
5.2.1.3 Growing IoT adoption
5.2.2 RESTRAINTS
5.2.2.1 High certification costs
5.2.2.2 Complex certification renewal process
5.2.3 OPPORTUNITIES
5.2.3.1 Rising demand for industry-specific certifications
5.2.3.2 Increased adoption of corporate training programs
5.2.4 CHALLENGES
5.2.4.1 Rapid technological changes
5.2.4.2 Shortages of skilled cybersecurity professionals
5.3 VALUE CHAIN ANALYSIS
5.3.1 PLANNING AND DESIGNING
5.3.2 CERTIFICATION BODIES AND ACCREDITATION ORGANIZATIONS
5.3.3 SYSTEM INTEGRATION
5.3.4 DISTRIBUTION
5.3.5 END USERS
5.4 ECOSYSTEM
5.5 IMPACT OF GENERATIVE AI ON CYBERSECURITY CERTIFICATION MARKET
5.5.1 GENERATIVE AI
5.5.2 TOP USE CASES AND MARKET POTENTIAL IN CYBERSECURITY CERTIFICATION MARKET
5.5.2.1 Key use cases
5.5.3 IMPACT OF GENERATIVE AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS
5.5.3.1 Cybersecurity training and education providers
5.5.3.2 Certification bodies and accreditation organizations
5.5.3.3 Government and regulatory bodies
5.5.3.4 Tech sectors (AI, cloud, IoT, blockchain)
5.5.3.5 Managed Security Service Providers (MSSPs)

5.6 PORTER'S FIVE FORCES ANALYSIS
5.6.1 THREAT OF NEW ENTRANTS
5.6.2 THREAT OF SUBSTITUTES
5.6.3 BARGAINING POWER OF SUPPLIERS
5.6.4 BARGAINING POWER OF BUYERS
5.6.5 INTENSITY OF COMPETITIVE RIVALRY
5.7 PRICING ANALYSIS
5.7.1 INDICATIVE PRICING ANALYSIS BY OFFERING
5.8 TECHNOLOGY ANALYSIS
5.8.1 KEY TECHNOLOGIES
5.8.1.1 Certification & Compliance Management Systems (CCMS)
5.8.1.2 Security testing platforms
5.8.1.3 Risk assessment tools
5.8.1.4 Learning Management Systems (LMS)
5.8.2 COMPLEMENTARY TECHNOLOGIES
5.8.2.1 Data encryption technologies
5.8.2.2 Endpoint protection
5.8.3 ADJACENT TECHNOLOGIES
5.8.3.1 Artificial Intelligence (AI) and Machine Learning (ML)
5.8.3.2 Blockchain
5.9 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS
5.10 PATENT ANALYSIS
5.10.1 CYBERSECURITY CERTIFICATION MARKET
5.11 REGULATORY LANDSCAPE
5.11.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS
5.11.2 KEY REGULATIONS
5.11.2.1 Payment Card Industry Data Security Standard (PCI–DSS)
5.11.2.2 Health Insurance Portability and Accountability Act (HIPAA)
5.11.2.3 Federal Information Security Management Act (FISMA)
5.11.2.4 Gramm-Leach-Bliley Act (GLBA)
5.11.2.5 Sarbanes-Oxley Act (SOX)
5.11.2.6 International Organization for Standardization (ISO) Standard 27001
5.11.2.7 European Union General Data Protection Regulation (EU GDPR)
5.11.2.8 California’s Privacy Rights Act (CPRA)
5.12 KEY STAKEHOLDERS & BUYING CRITERIA
5.12.1 KEY STAKEHOLDERS IN BUYING PROCESS
5.12.2 BUYING CRITERIA
5.13 KEY CONFERENCES & EVENTS IN 2025

5.14 INVESTMENT AND FUNDING SCENARIO
5.15 CASE STUDY ANALYSIS
5.15.1 CLEARDATA LEVERAGED BSI CERTIFICATIONS TO DRIVE BUSINESS GROWTH, GAIN COMPETITIVE EDGE, AND STRENGTHEN CLIENT TRUST
5.15.2 IDR STRENGTHENED DATA SECURITY AND GAINED COMPETITIVE EDGE WITH ISO 27001 CERTIFICATION POWERED BY A-LIGN
5.15.3 TRUEWORK CHOSE COALFIRE’S COMPLIANCE ESSENTIALS TO AUTOMATE AND STRENGTHEN ITS SECURITY AND TRUST PROGRAM

6 CYBERSECURITY CERTIFICATION MARKET, BY OFFERING

6.1 INTRODUCTION
6.1.1 OFFERINGS: CYBERSECURITY CERTIFICATION MARKET DRIVERS
6.2 PLATFORMS & TOOLS
6.2.1 NEED TO OPTIMIZE CYBERSECURITY CERTIFICATION PROCESS WITH PLATFORMS AND TOOLS TO DRIVE MARKET
6.3 CERTIFICATION SERVICES
6.3.1 NEED TO ENHANCE CYBERSECURITY THROUGH ORGANIZATIONAL AND INDIVIDUAL CERTIFICATION SERVICES TO PROPEL MARKET
6.3.2 GAP ANALYSIS & PRE-ASSESSMENT
6.3.3 VULNERABILITY ASSESSMENT & PENETRATION TESTING
6.3.4 AUDIT & EVALUATION SERVICES
6.3.5 TRAINING & WORKSHOPS
6.3.6 POST-CERTIFICATION SUPPORT
6.3.7 RECERTIFICATION

7 CYBERSECURITY CERTIFICATION MARKET, BY CERTIFICATION CATEGORY

7.1 INTRODUCTION
7.1.1 CERTIFICATION CATEGORIES: CYBERSECURITY CERTIFICATION MARKET DRIVERS
7.2 NETWORK SECURITY CERTIFICATIONS
7.2.1 NEED FOR ENHANCING SECURITY POSTURE WITH NETWORK CERTIFICATION TO DRIVE MARKET
7.2.2 ISO/IEC 15408
7.2.3 ISO/IEC 27033
7.2.4 FIPS 140
7.2.5 IEC 62443
7.2.6 OTHERS

7.3 CLOUD SECURITY CERTIFICATIONS
  7.3.1 NEED FOR ACHIEVING REGULATORY COMPLIANCE WITH CLOUD SECURITY STANDARDS TO FUEL MARKET GROWTH
  7.3.2 ISO/IEC 27017
  7.3.3 CSA STAR
  7.3.4 FEDRAMP
  7.3.5 CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)
  7.3.6 OTHERS
7.4 INFORMATION SECURITY CERTIFICATIONS/PRIVACY & DATA PROTECTION CERTIFICATIONS
  7.4.1 NEED FOR ADHERING TO REGULATORY COMPLIANCE WITH INFORMATION SECURITY CERTIFICATION TO ACCELERATE MARKET GROWTH
  7.4.2 SOC 2
  7.4.3 ISO/IEC 27001
  7.4.4 PCI DSS
  7.4.5 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)
  7.4.6 CERTIFIED INFORMATION PRIVACY PROFESSIONAL (CIPP)
  7.4.7 MIFARE
  7.4.8 GDPR
  7.4.9 EUROPRIVACY
  7.4.10 ENX VEHICLE CYBERSECURITY (ENX VCS)
  7.4.11 TISAX
  7.4.12 OTHERS
7.5 GOVERNANCE, RISK, AND COMPLIANCE (GRC) CERTIFICATIONS
  7.5.1 NEED FOR RISK MANAGEMENT AND COMPLIANCE FRAMEWORK IMPLEMENTATION TO BOLSTER MARKET GROWTH
  7.5.2 ISO 22301
  7.5.3 ISO/IEC 27005
  7.5.4 COBIT
  7.5.5 NIST CYBERSECURITY FRAMEWORK (CSF)
  7.5.6 OTHERS
7.6 ARTIFICIAL INTELLIGENCE (AI) CERTIFICATIONS
  7.6.1 NEED TO ENSURE PRIVACY AND SECURITY IN AI SYSTEMS TO BOOST MARKET GROWTH
  7.6.2 ISO/IEC 23894
  7.6.3 ISO/IEC 20546
  7.6.4 OTHERS
7.7 APPLICATION SECURITY CERTIFICATIONS
  7.7.1 APPLICATION SECURITY CERTIFICATIONS TO STRENGTHEN

APPLICATION SECURITY THROUGHOUT LIFE CYCLE
7.7.2 OWASP APPLICATION SECURITY VERIFICATION STANDARD (ASVS)
7.7.3 ISO/IEC 27034
7.7.4 OTHERS
7.8 DEVICE & IOT SECURITY CERTIFICATIONS
7.8.1 ADOPTION OF CLOUD-BASED SOLUTIONS BY SMALL AND MEDIUM-SIZED ENTERPRISES TO PROPEL MARKET
7.8.2 FIPS 140-3
7.8.3 COMMON CRITERIA
7.8.4 IEC 62443-4-2
7.8.5 ISO/IEC 20000
7.8.6 ISO/IEC 30141
7.8.7 IEC 62443-4-2
7.8.8 NIST 8228
7.8.9 OTHERS
7.9 OTHER CERTIFICATION CATEGORIES
7.9.1 BUSINESS CONTINUITY CERTIFICATIONS
7.9.1.1 ISO 22301
7.9.1.2 ISO/IEC 24762
7.9.2 OPERATIONAL TECHNOLOGY (OT) SECURITY CERTIFICATIONS
7.9.2.1 IEC 62351
7.9.2.2 NERC CIP

8 CYBERSECURITY CERTIFICATION MARKET, BY TARGET USER

8.1 INTRODUCTION
8.1.1 TARGET USERS: CYBERSECURITY CERTIFICATION MARKET DRIVERS
8.2 INDIVIDUAL PROFESSIONALS
8.2.1 NEED TO ADVANCE IN FIELD AND ORGANIZATIONS SEEKING QUALIFIED PERSONNEL TO FUEL MARKET GROWTH
8.3 ENTERPRISES
8.3.1 ENTERPRISES TO NEED CYBERSECURITY WITH ESSENTIAL CERTIFICATIONS FOR COMPLIANCE AND DATA PROTECTION

9 CYBERSECURITY CERTIFICATION MARKET, BY DELIVERY MODE

9.1 INTRODUCTION
9.1.1 DELIVERY MODES: CYBERSECURITY CERTIFICATION MARKET DRIVERS
9.2 ONLINE

9.2.1 NEED FOR ENHANCING FLEXIBILITY AND ACCESS THROUGH ONLINE CYBERSECURITY CERTIFICATIONS TO FUEL MARKET GROWTH
9.3 IN-PERSON
9.3.1 BOOSTING ENGAGEMENT AND HANDS-ON LEARNING WITH IN-PERSON CYBERSECURITY CERTIFICATIONS

10 CYBERSECURITY CERTIFICATION MARKET, BY VERTICAL

10.1 INTRODUCTION
10.1.1 VERTICALS: CYBERSECURITY CERTIFICATION MARKET DRIVERS
10.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)
10.2.1 CYBERSECURITY CERTIFICATIONS TO DRIVE SECURITY AND COMPLIANCE
10.3 GOVERNMENT & DEFENSE
10.3.1 NEED TO ENSURE NATIONAL SECURITY AND REGULATORY COMPLIANCE THROUGH CYBERSECURITY CERTIFICATIONS TO BOOST MARKET GROWTH
10.4 IT & ITES
10.4.1 NEED FOR ENHANCING SECURITY AND COMPLIANCE THROUGH CYBERSECURITY CERTIFICATIONS
10.5 TELECOMMUNICATIONS
10.5.1 FORTIFYING NETWORK SECURITY AND COMPLIANCE THROUGH CYBERSECURITY CERTIFICATION TO BOOST MARKET GROWTH
10.6 HEALTHCARE
10.6.1 NEED TO ENHANCE PATIENT DATA SECURITY AND COMPLIANCE THROUGH CYBERSECURITY CERTIFICATION TO FOSTER MARKET GROWTH
10.7 AUTOMOTIVE
10.7.1 NEED TO AUGMENT VEHICLE SECURITY AND TRUST THROUGH CYBERSECURITY CERTIFICATION TO BOLSTER MARKET GROWTH
10.8 OTHER VERTICALS

11 CYBERSECURITY CERTIFICATION MARKET, BY REGION

11.1 INTRODUCTION
11.2 NORTH AMERICA
11.2.1 NORTH AMERICA: MACROECONOMIC OUTLOOK
11.2.2 NORTH AMERICA: CYBERSECURITY CERTIFICATION MARKET DRIVERS
11.2.3 US
11.2.3.1 Rising cyber threats, regulatory demands, and shortage of skilled

professionals to drive market
11.2.4 CANADA
11.2.4.1 Increasing cyber threats, regulatory requirements, and emphasis on digital security among businesses to propel market
11.3 EUROPE
11.3.1 EUROPE: MACROECONOMIC OUTLOOK
11.3.2 EUROPE: CYBERSECURITY CERTIFICATION MARKET DRIVERS
11.3.3 UK
11.3.3.1 Rising cyber threats, evolving regulatory requirements, and increased demand for skilled professionals to fuel market growth
11.3.4 GERMANY
11.3.4.1 Sharp increase in cyberattacks and urgent need for skilled professionals to accelerate market growth
11.3.5 FRANCE
11.3.5.1 Rising cyber threats, regulatory compliance demands, and focus on digital security across industries to foster market growth
11.3.6 ITALY
11.3.6.1 Government’s commitment to bolstering national cybersecurity through initiatives led by Agence Nationale de la S?curit? des Syst?mes d'Information (ANSSI) to drive market
11.3.7 REST OF EUROPE
11.4 ASIA PACIFIC
11.4.1 ASIA PACIFIC: MACROECONOMIC OUTLOOK
11.4.2 ASIA PACIFIC: CYBERSECURITY CERTIFICATION MARKET DRIVERS
11.4.3 CHINA
11.4.3.1 Increased cyber threats, government policies, demand for skilled professionals, and increased cybersecurity awareness campaigns to boost market growth
11.4.4 JAPAN
11.4.4.1 Rising cyber threats and government initiatives to augment demand for cybersecurity certifications
11.4.5 INDIA
11.4.5.1 Growing cyber threats, digital transformation, and heightened awareness of cybersecurity's critical importance to enhance market growth
11.4.6 SINGAPORE
11.4.6.1 Increasing digitalization and adoption of emerging technologies to fuel demand for cybersecurity certifications
11.4.7 REST OF ASIA PACIFIC
11.5 MIDDLE EAST & AFRICA

11.5.1 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK
11.5.2 MIDDLE EAST & AFRICA: CYBERSECURITY CERTIFICATION MARKET DRIVERS
11.5.3 GCC COUNTRIES
11.5.3.1 Escalating cyber threats, regulatory requirements, and digital transformation digitalization to foster market growth
11.5.3.2 KSA
11.5.3.3 UAE
11.5.3.4 Rest of GCC countries
11.5.4 SOUTH AFRICA
11.5.4.1 Heightened awareness of cyber risks, government initiatives, and rising demand for certified professionals to boost market growth
11.5.5 REST OF MIDDLE EAST & AFRICA
11.6 LATIN AMERICA
11.6.1 LATIN AMERICA: MACROECONOMIC OUTLOOK
11.6.2 LATIN AMERICA: CYBERSECURITY CERTIFICATION MARKET DRIVERS
11.6.3 BRAZIL
11.6.3.1 Growing cyber threats, digital transformation, increased regulatory compliance needs, and focus on advanced technologies to propel market
11.6.4 MEXICO
11.6.4.1 Escalating cyber threats, accelerated digital transformation, and rising need for skilled professionals to propel market
11.6.5 REST OF LATIN AMERICA

12 COMPETITIVE LANDSCAPE

12.1 KEY PLAYER STRATEGIES/RIGHT TO WIN
12.2 REVENUE ANALYSIS
12.3 MARKET SHARE ANALYSIS
12.4 BRAND/PRODUCT COMPARISON
12.4.1 SGS
12.4.2 DNV GL
12.4.3 BUREAU VERITAS
12.4.4 UL SOLUTIONS
12.4.5 TUV SUD
12.5 COMPANY VALUATION AND FINANCIAL METRICS
12.5.1 COMPANY VALUATION
12.5.2 FINANCIAL METRICS USING EV/EBIDTA
12.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023

12.6.1 STARS
12.6.2 EMERGING LEADERS
12.6.3 PERVASIVE PLAYERS
12.6.4 PARTICIPANTS
12.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2023
12.6.5.1 Company footprint
12.6.5.2 Offering footprint
12.6.5.3 Vertical footprint
12.6.5.4 Regional footprint
12.7 COMPANY EVALUATION MATRIX: START-UPS/SMES, 2023
12.7.1 PROGRESSIVE COMPANIES
12.7.2 RESPONSIVE COMPANIES
12.7.3 DYNAMIC COMPANIES
12.7.4 STARTING BLOCKS
12.7.5 COMPETITIVE BENCHMARKING: START-UPS/SMES, 2023
12.7.5.1 Detailed list of key start-ups/SMEs
12.7.5.2 Competitive benchmarking of SMEs
12.8 COMPETITIVE SCENARIO
12.8.1 PRODUCT LAUNCHES AND ENHANCEMENTS
12.8.2 DEALS

13 COMPANY PROFILES

13.1 KEY PLAYERS
13.1.1 SGS
13.1.1.1 Business overview
13.1.1.2 Products/Solutions/Services offered
13.1.1.3 Recent developments
13.1.1.3.1 Product launches
13.1.1.3.2 Deals
13.1.1.4 MnM view
13.1.1.4.1 Right to win
13.1.1.4.2 Strategic choices
13.1.1.4.3 Weaknesses and competitive threats
13.1.2 BUREAU VERITAS
13.1.2.1 Business overview
13.1.2.2 Products/Solutions/Services offered
13.1.2.3 Recent developments
13.1.2.3.1 Deals

13.1.2.4 MnM view
13.1.2.4.1 Right to win
13.1.2.4.2 Strategic choices
13.1.2.4.3 Weaknesses and competitive threats
13.1.3 TUV SUD
13.1.3.1 Business overview
13.1.3.2 Products/Solutions/Services offered
13.1.3.3 Recent developments
13.1.3.3.1 Product launches & enhancements
13.1.3.3.2 Deals
13.1.3.4 MnM view
13.1.3.4.1 Right to win
13.1.3.4.2 Strategic choices
13.1.3.4.3 Weaknesses and competitive threats
13.1.4 DNV GL
13.1.4.1 Business overview
13.1.4.2 Products/Solutions/Services offered
13.1.4.3 Recent developments
13.1.4.3.1 Product launches
13.1.4.3.2 Deals
13.1.4.4 MnM view
13.1.4.4.1 Right to win
13.1.4.4.2 Strategic choices
13.1.4.4.3 Weaknesses and competitive threats
13.1.5 UL SOLUTIONS
13.1.5.1 Business overview
13.1.5.2 Products/Solutions/Services offered
13.1.5.3 Recent developments
13.1.5.3.1 Deals
13.1.5.4 MnM view
13.1.5.4.1 Right to win
13.1.5.4.2 Strategic choices
13.1.5.4.3 Weaknesses and competitive threats
13.1.6 DEKRA
13.1.6.1 Business overview
13.1.6.2 Products/Solutions/Services offered
13.1.6.3 Recent developments
13.1.6.3.1 Product launches
13.1.6.3.2 Deals

13.1.7 INTERTEK
13.1.7.1 Business overview
13.1.7.2 Products/Solutions/Services offered
13.1.7.3 Recent developments
13.1.7.3.1 Product launches
13.1.7.3.2 Deals
13.1.8 EUROFINS SCIENTIFIC
13.1.8.1 Business overview
13.1.8.2 Products/Solutions/Services offered
13.1.8.3 Recent developments
13.1.8.3.1 Product launches & enhancements
13.1.9 TUV NORD
13.1.9.1 Business overview
13.1.9.2 Products/Solutions/Services offered
13.1.9.3 Recent developments
13.1.9.3.1 Product launches & enhancements
13.1.10 ELEMENTS MATERIALS TECHNOLOGY
13.1.10.1 Business overview
13.1.10.2 Products/Solutions/Services offered
13.1.10.3 Recent developments
13.1.10.3.1 Product launches
13.2 OTHER PLAYERS
13.2.1 KEYSIGHT
13.2.2 BSI
13.2.3 TUV RHEINLAND
13.2.4 EY CERTIFYPOINT
13.2.5 A-LIGN
13.2.6 HITRUST
13.2.7 SCHELLAM
13.2.8 COALFIRE CERTIFICATION
13.2.9 DQS
13.2.10 CONTROL CASE
13.2.11 ISC2
13.2.12 INFOSEC TRAIN
13.2.13 EXIDA
13.2.14 ISASECURE
13.2.15 ISACA
13.2.16 COMPTIA

14 ADJACENT MARKETS

14.1 INTRODUCTION TO ADJACENT MARKETS
  14.1.1 LIMITATIONS
14.2 CYBERSECURITY MARKET
14.3 EGRC MARKET

15 APPENDIX

15.1 DISCUSSION GUIDE
15.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL
15.3 CUSTOMIZATION OPTIONS
15.4 RELATED REPORTS
15.5 AUTHOR DETAILS

I would like to order

Product name:	Cybersecurity Certification Market by Certification Category (Cloud Security, Information Security, AI Certifications), Target User (Individual Professionals and Enterprises), Delivery Mode (Online and in-person) - Global Forecast to 2030
Product link:	https://marketpublishers.com/r/CFD27F282F9CEN.html
Price:	US$ 4,950.00 (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/CFD27F282F9CEN.html