

SOC-as-a-Service (SOCaaS) Market by Service Type (Managed SIEM & Log Management, Vulnerability Scanning & Assessment, Threat Detection & Remediation), Security Type (Endpoint Security, Network Security, Cloud Security) - Global Forecast to 2030

<https://marketpublishers.com/r/SC59AEA7EED8EN.html>

Date: February 2025

Pages: 443

Price: US\$ 4,950.00 (Single User License)

ID: SC59AEA7EED8EN

Abstracts

The global SOCaaS market size is estimated to grow from USD 7.37 Billion in 2024 to USD 14.66 Billion by 2030 at a compound annual growth rate (CAGR) of 12.2% during the forecast period.

The growing demand for robust, scalable, and cost-effective solutions to address vulnerabilities, identify threats, and respond to crises is propelling the SOC as a Service (SOCaaS) industry. The increased digitization of enterprises, the proliferation of cloud-based platforms, and the increasing complexity of cyberattacks have all fueled demand for sophisticated SOCaaS solutions. Challenges such as high implementation costs, integration complexities, and a shortage of skilled cybersecurity professionals are being mitigated by tailored services, automated tools, and ongoing innovations in managed security solutions. A heightened focus on threat visibility, regulatory compliance, and real-time monitoring ensures that organizations can maintain secure, efficient, and resilient security operations in an increasingly complex cyber threat landscape.

By sector, private sector accounts for a larger market size during the forecast period

The private sector segment is expected to hold the largest market size in SOCaaS market during the forecast period. This is because of the increased adoption of digital transformation programs and the sophistication of cyber threats targeting private

organizations. Cyberattacks are particularly prevalent in industries such as BFSI, IT & ITeS, and telecoms, necessitating the provision of effective threat detection, response, and remediation services. Furthermore, the need to comply with regulatory standards, secure sensitive customer data, and preserve business continuity in the face of rising cyber dangers is driving private enterprises to spend extensively in SOCaaS solutions.

By region, Asia-Pacific accounts for the highest CAGR during the forecast period.

Major drivers in Asia-Pacific region in SOCaaS market are the rapid digital transformation across industries, increased adoption of cloud technologies, and a growing emphasis on cybersecurity in emerging economies such as India, China, and Southeast Asian countries. The rise in complex cyber threats, along with a dearth of in-house cybersecurity experience, is pushing firms to embrace SOCaaS solutions. Furthermore, favorable government policies and programs boosting cybersecurity awareness, as well as investments in smart city projects and digital infrastructure, are driving the region's strong market growth.

Breakdown of primaries

The study contains insights from various industry experts, from component suppliers to Tier 1 companies and OEMs. The break-up of the primaries is as follows:

By Company Type: Tier 1 – 35%, Tier 2 – 45%, and Tier 3 – 20%

By Designation: C-level Executives – 40% and Managerial & Other Levels – 60%

By Region: North America – 20%, Europe – 35%, Asia Pacific – 45%

Major vendors in the SOCaaS market include Thales (France), Airbus Cybersecurity (France), NTT (Japan), Lumen Technologies (US), Fortinet (US), Cloudflare (US), Check Point (US), Kaseya (US), Trustwave (US), Arctic Wolf Networks (US), Proficio (US), LRQA (UK), Inspirisys (India), Eventus Security (India), Cyber Security Hive (India), eSentire (Canada), Clearnetwork (US), CyberSecOp (US), Foresite Cybersecurity (US), Stratosphere Networks (US), eSec Forte (India), Cybersafe Solutions (US), 10xDS (India), CISO Global (US), Ace Cloud Hosting (US), plusserver (Germany), SafeAeon (US), SOCWISE (Hungary), inSOC (Enhanced.io) (UK), Wizard

Cyber (UK), Eventus Security (India), and Cyber Security Hive (India).

The study includes an in-depth competitive analysis of the key players in the supply chain security market, their company profiles, recent developments, and key market strategies.

Research Coverage

The report segments the SOCaaS market by service type, offering, security type, organization size, sector, vertical, and region.

It forecasts its size by Service type (Managed SIEM & Log Management, Vulnerability Scanning & Assessment, Threat Detection & Remediation, Incident Response, and GRC) Offering (Fully Managed and Co-managed), By Security type (Endpoint Security, Network Security, Cloud Security, and Application Security), By Organization Size (SMEs and Large Enterprises), By Sector (Public Sector and Private Sector), By Vertical (BFSI, Healthcare, Government, Manufacturing, Energy & Utilities, IT & ITeS, Telecommunications, Transportation & Logistics, and Other verticals), By Region (North America, Europe, Asia Pacific, Middle East and Africa, Latin America).

The study also includes an in-depth competitive analysis of the market's key players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

Key Benefits of Buying the Report

The report will help the market leaders/new entrants with information on the closest approximations of the revenue numbers for the SOCaaS market and the subsegments. This report will help stakeholders understand the competitive landscape and gain more insights to position their businesses better and plan suitable go-to-market strategies. The report also helps stakeholders understand the market pulse and provides information on key market drivers, restraints, challenges, and opportunities.

The report provides insights on the following pointers:

Analysis of key drivers, such as (Escalating complexity and frequency of cyberattacks, Shortage of cybersecurity talent and expertise, Rapid technological advancements and growing trends of BYOD, CYOD, and WFH, Simplifying complex threat response processes, Increasing prevalence of

customizable security solutions); Restraints (Integration complexity with compatibility and interoperability issues, Cost constraints); Opportunities (Rising adoption of cloud-based solutions among SMEs, Implementation of AI, ML, and blockchain technologies for cyber defense advancements, Expanding integration with extended detection and response (XDR) platforms) and Challenges (Data privacy and regulatory complexity, Limited customization and misalignment with business needs, Managing alert fatigue and false positives).

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

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

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

Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players including Thales (France), Airbus Cybersecurity (France), NTT (Japan), Lumen Technologies (US), Fortinet (US), Cloudflare (US), Check Point (US), Kaseya (US), Trustwave (US), Arctic Wolf Networks (US), Proficio (US), LRQA (UK), Inspirisys (India), Eventus Security (India), and Cyber Security Hive (India), among others, in the SOCaaS market strategies.

Contents

1 INTRODUCTION

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

2 RESEARCH METHODOLOGY

- 2.1 RESEARCH DATA
 - 2.1.1 SECONDARY DATA
 - 2.1.2 PRIMARY DATA
 - 2.1.2.1 Breakup of primaries
 - 2.1.2.2 Key industry insights
- 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 COMPANY EVALUATION QUADRANT METHODOLOGY
 - 2.5.1 FOR LARGE PLAYERS
 - 2.5.2 FOR STARTUPS
- 2.6 RESEARCH ASSUMPTIONS
- 2.7 RESEARCH LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

- 4.1 ATTRACTIVE GROWTH OPPORTUNITIES FOR PLAYERS IN SOC-AS-A-SERVICE MARKET
- 4.2 SOC-AS-A-SERVICE MARKET, BY SERVICE TYPE, 2024

- 4.3 SOC-AS-A-SERVICE MARKET, BY OFFERING, 2024
- 4.4 SOC-AS-A-SERVICE MARKET, BY ORGANIZATION SIZE, 2024
- 4.5 SOC-AS-A-SERVICE MARKET, BY SECURITY TYPE, 2024
- 4.6 SOC-AS-A-SERVICE MARKET, BY SECTOR, 2024
- 4.7 SOC-AS-A-SERVICE MARKET, BY VERTICAL, 2024
- 4.8 MARKET INVESTMENT SCENARIO

5 MARKET OVERVIEW AND INDUSTRY TRENDS

5.1 INTRODUCTION

5.2 MARKET DYNAMICS

5.2.1 DRIVERS

- 5.2.1.1 Escalating complexity and frequency of cyberattacks
- 5.2.1.2 Shortage of cybersecurity talent and expertise
- 5.2.1.3 Rapid technological advancements and growing trends of

BYOD, CYOD, and WFH

- 5.2.1.4 Demand for simplifying complex threat response processes
- 5.2.1.5 Increasing prevalence of customizable security solutions

5.2.2 RESTRAINTS

- 5.2.2.1 Integration complexity with compatibility and interoperability issues
- 5.2.2.2 Cost constraints

5.2.3 OPPORTUNITIES

- 5.2.3.1 Rising adoption of cloud-based solutions among SMEs
- 5.2.3.2 Implementation of AI, ML, and blockchain technologies for cyber defense

advancements

- 5.2.3.3 Expanding integration with extended detection and response (XDR) platforms

5.2.4 CHALLENGES

- 5.2.4.1 Data privacy and regulatory complexity
- 5.2.4.2 Limited customization and misalignment with business needs
- 5.2.4.3 Managing alert fatigue and false positives

5.3 CASE STUDY ANALYSIS

5.3.1 VERIZON HELPED FUJIFILM ENHANCE GLOBAL CYBERSECURITY WITH ADVANCED SOC SERVICES

5.3.2 FORTINET HELPED GRAND VIEW UNIVERSITY STRENGTHEN CYBERSECURITY WITH SOCAAS AND MDR SERVICES

5.3.3 INSPIRA ENHANCED CYBERSECURITY WITH MODERNIZED SOC POWERED BY IBM QRADAR

5.3.4 CHILLISOFT AND ADVANTAGE EMPOWERED FIJI NATIONAL

UNIVERSITY'S CYBERSECURITY WITH SOC-AS-A-SERVICE

5.3.5 CYBERSECOP HELPED MULTIPLE INDUSTRIES ENHANCE CYBER SECURITY WITH SOC-AS-A-SERVICE

5.4 HISTORICAL EVOLUTION

5.4.1 EARLY DAYS AND TRADITIONAL FOCUS

5.4.2 INTEGRATION OF COMPLIANCE AND TECHNOLOGY

5.4.3 GOLDEN PERIOD OF EVOLUTION

5.4.4 EMERGENCE OF MANAGED SECURITY SERVICES PROVIDERS (MSSPS)

5.4.5 RISE OF NEXT-GEN SOCS

5.4.6 THREAT INTELLIGENCE AND CLOUD SECURITY

5.4.7 POST-PANDEMIC CHALLENGES AND BEYOND

5.4.8 MODERN CYBER DEFENSE CENTERS

5.4.9 SERVICES OFFERED BY MODERN CYBER DEFENSE CENTERS

5.5 FRAMEWORK

5.5.1 BENEFITS OF SOC-AS-A-SERVICE

5.5.2 FEATURES OF SOC-AS-A-SERVICE MARKET FRAMEWORK

5.6 VALUE CHAIN ANALYSIS

5.6.1 ANALYZING OVERALL SECURITY ARCHITECTURE AND PLANNING STRATEGIES ACCORDINGLY

5.6.2 OFFERING

5.6.3 DISTRIBUTORS/RESELLERS/VARS

5.6.4 END-USER GROUPS

5.6.5 MONITORING OF ALL BUSINESS PROCESSES

5.6.6 INCIDENT RESPONSE

5.6.7 MEASURES FOR REMEDIATION

5.7 ECOSYSTEM ANALYSIS

5.8 PORTER'S FIVE FORCES ANALYSIS

5.8.1 THREAT OF NEW ENTRANTS

5.8.2 BARGAINING POWER OF SUPPLIERS

5.8.3 BARGAINING POWER OF BUYERS

5.8.4 THREAT OF SUBSTITUTES

5.8.5 INTENSITY OF COMPETITIVE RIVALRY

5.9 PRICING ANALYSIS

5.9.1 AVERAGE SELLING PRICE OF PRODUCTS, BY SECURITY TYPE

5.9.2 INDICATIVE PRICING ANALYSIS OF PRODUCTS, BY SERVICE

5.10 TECHNOLOGY ANALYSIS

5.10.1 KEY TECHNOLOGIES

5.10.1.1 SIEM

5.10.1.2 SOAR

- 5.10.1.3 Extended detection and response (XDR)
- 5.10.1.4 Threat intelligence platforms
- 5.10.1.5 Network traffic analysis
- 5.10.2 COMPLEMENTARY TECHNOLOGIES
 - 5.10.2.1 IAM
 - 5.10.2.2 Deception technology
 - 5.10.2.3 ZTNA
 - 5.10.2.4 SASE
- 5.10.3 ADJACENT TECHNOLOGIES
 - 5.10.3.1 Blockchain technology
 - 5.10.3.2 OT security
 - 5.10.3.3 Quantum-safe cryptography
- 5.11 PATENT ANALYSIS
 - 5.11.1 LIST OF MAJOR PATENTS
- 5.12 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS
- 5.13 BUSINESS MODEL
 - 5.13.1 CUSTOMERS
 - 5.13.2 PRODUCTS AND SERVICES
 - 5.13.3 PRICING
 - 5.13.4 DISTRIBUTION CHANNELS
 - 5.13.5 MARKETING & SALES
 - 5.13.6 PARTNERSHIPS
 - 5.13.7 OPERATIONS
 - 5.13.8 PROFITABILITY
- 5.14 REGULATORY LANDSCAPE
 - 5.14.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS
 - 5.14.1.1 Payment Card Industry Data Security Standard (PCI-DSS)
 - 5.14.1.2 General Data Protection Regulation (GDPR)
 - 5.14.1.3 Sarbanes-Oxley Act (SOX)
 - 5.14.1.4 California Consumer Privacy Act (CCPA)
 - 5.14.1.5 Gramm-Leach-Bliley Act of 1999 (GLBA)
 - 5.14.1.6 Health Insurance Portability and Accountability Act (HIPAA)
 - 5.14.1.7 International Organization for Standardization (ISO) Standard 27001
 - 5.14.1.8 Federal Information Security Management Act (FISMA)
 - 5.14.1.9 FFIEC Cybersecurity Assessment Tool
 - 5.14.1.10 NIST Cybersecurity Framework
 - 5.14.1.11 Information Technology Infrastructure Library (ITIL)
 - 5.14.1.12 CSA STAR

- 5.14.2 REGULATIONS, BY REGION
- 5.15 KEY STAKEHOLDERS AND BUYING CRITERIA
 - 5.15.1 KEY STAKEHOLDERS IN BUYING PROCESS
 - 5.15.2 BUYING CRITERIA
- 5.16 KEY CONFERENCES AND EVENTS, 2025
- 5.17 INVESTMENT AND FUNDING SCENARIO
- 5.18 TECHNOLOGY ROADMAP
- 5.19 IMPACT OF AI/GENERATIVE AI ON SOC-AS-A-SERVICE MARKET
 - 5.19.1 GENERATIVE AI
 - 5.19.2 TOP USE CASES AND MARKET POTENTIAL IN SOC-AS-A-SERVICE MARKET
 - 5.19.2.1 Key use cases
 - 5.19.3 IMPACT OF GENERATIVE AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS
 - 5.19.3.1 AI & ML
 - 5.19.3.2 Blockchain
 - 5.19.3.3 Extended detection and response (XDR)
 - 5.19.3.4 Cloud
 - 5.19.3.5 Endpoint detection and response (EDR)
 - 5.19.3.6 Security Information and Event Management (SIEM)

6 SOC-AS-A-SERVICE MARKET, BY THREAT TYPE

- 6.1 INTRODUCTION
 - 6.1.1 THREAT TYPE: SOC-AS-A-SERVICE MARKET DRIVERS
- 6.2 ADVANCED PERSISTENT THREATS
 - 6.2.1 PERSISTENT THREATS AND EVOLVING CYBERATTACK TO DRIVE MARKET
- 6.3 INSIDER THREATS
 - 6.3.1 RISING COMPLEXITY AND NEED FOR PROACTIVE DETECTION TO BOOST MARKET
- 6.4 DDOS ATTACKS
 - 6.4.1 RISING THREAT COMPLEXITY AND DEMAND FOR PROACTIVE MITIGATION TO DRIVE MARKET
- 6.5 MALWARE & RANSOMWARE
 - 6.5.1 INCREASING THREAT COMPLEXITY AND PROLIFERATION TO AUGMENT MARKET
- 6.6 PHISHING & SOCIAL ENGINEERING ATTACKS
 - 6.6.1 SOPHISTICATION OF ATTACKS AND HUMAN VULNERABILITY

TO PROPEL MARKET

6.7 OTHER THREAT TYPES

7 SOC-AS-A-SERVICE MARKET, BY SERVICE TYPE

7.1 INTRODUCTION

7.1.1 SERVICE TYPE: SOC-AS-A-SERVICE MARKET DRIVERS

7.2 MANAGED SIEM & LOG MANAGEMENT

7.2.1 NEED FOR PROACTIVE THREAT DETECTION AND REGULATORY COMPLIANCE TO PROPEL MARKET GROWTH

7.3 VULNERABILITY SCANNING & ASSESSMENT

7.3.1 DEMAND FOR PROACTIVE RISK MITIGATION AND COMPLIANCE ENABLEMENT TO DRIVE MARKET

7.4 THREAT DETECTION & REMEDIATION

7.4.1 DEMAND FOR ADVANCED AUTOMATION AND PROACTIVE SECURITY TO BOLSTER MARKET GROWTH

7.5 INCIDENT RESPONSE SERVICES

7.5.1 NEED FOR RAPID DETECTION AND PROACTIVE MITIGATION TO STRENGTHEN MARKET

7.6 GOVERNANCE, RISK, & COMPLIANCE

7.6.1 REQUIREMENT FOR ENHANCED COMPLIANCE AND PROACTIVE RISK MANAGEMENT TO FORTIFY MARKET

8 SOC-AS-A-SERVICE MARKET, BY OFFERING

8.1 INTRODUCTION

8.1.1 OFFERING: SOC-AS-A-SERVICE MARKET DRIVERS

8.2 FULLY MANAGED

8.2.1 RISING DEMAND FOR CONVENIENCE ALONG WITH COST AND TIME EFFICIENCY TO DRIVE MARKET

8.3 CO-MANAGED

8.3.1 NEED FOR ADDRESSING PRIVACY AND SCALABILITY CONCERNS TO DRIVE MARKET

9 SOC-AS-A-SERVICE MARKET, BY ORGANIZATION SIZE

9.1 INTRODUCTION

9.1.1 ORGANIZATION SIZE: SOC-AS-A-SERVICE MARKET DRIVERS

9.2 SMALL AND MEDIUM-SIZED ENTERPRISES

- 9.2.1 COST BENEFITS AND HIGH-SECURITY RISKS TO FACTOR IN FOR SMES
- 9.3 LARGE ENTERPRISES
 - 9.3.1 RAPID INCREASE IN BYOD/CYOD FOLLOWED BY RISE IN SECURITY ATTACKS TO DRIVE DEMAND

10 SOC-AS-A-SERVICE MARKET, BY SECURITY TYPE

10.1 INTRODUCTION

- 10.1.1 SECURITY TYPE: SOC-AS-A-SERVICE MARKET DRIVERS

10.2 NETWORK SECURITY

- 10.2.1 INCREASING USE OF CLOUD AND DIGITAL PLATFORMS AND RISE IN NETWORK ATTACKS TO DRIVE MARKET

10.3 CLOUD SECURITY

- 10.3.1 CONCERNS ABOUT SENSITIVE DATA STORAGE ON CLOUD TO DRIVE MARKET

10.4 ENDPOINT SECURITY

- 10.4.1 RISING NUMBER OF MOBILE DEVICES AND GROWTH IN BYOD/CYOD TREND TO DRIVE MARKET

10.5 APPLICATION SECURITY

- 10.5.1 GROWTH IN DIGITALIZATION AND BUSINESS-SENSITIVE APPLICATIONS TO DRIVE MARKET

11 SOC-AS-A-SERVICE MARKET, BY SECTOR

11.1 INTRODUCTION

- 11.1.1 SECTOR: SOC-AS-A-SERVICE MARKET DRIVERS

11.2 PUBLIC SECTOR

- 11.2.1 CRITICAL INFRASTRUCTURE MANAGEMENT AND STRINGENT REGULATIONS TO DRIVE MARKET

11.3 PRIVATE SECTOR

- 11.3.1 INCREASING CYBERATTACKS AND NEED TO PROTECT HUGE DATA TO DRIVE MARKET

12 SOC-AS-A-SERVICE MARKET, BY VERTICAL

12.1 INTRODUCTION

- 12.1.1 VERTICAL: SOC-AS-A-SERVICE MARKET DRIVERS

12.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)

- 12.2.1 GROWTH IN SENSITIVE FINANCIAL DATA AND CYBERATTACKS

TO FUEL MARKET

12.3 HEALTHCARE

12.3.1 CRITICAL NEED TO SAFEGUARD SENSITIVE PATIENT DATA AND ENSURE OPERATIONAL CONTINUITY TO STRENGTHEN MARKET

12.4 GOVERNMENT

12.4.1 NEED TO PROTECT CRITICAL INFRASTRUCTURE AND SENSITIVE DATA TO BOLSTER MARKET

12.5 MANUFACTURING

12.5.1 GROWING DEPENDENCE ON DIGITIZED OPERATIONS AND INTERCONNECTED SYSTEMS TO PROPEL MARKET

12.6 ENERGY & UTILITIES

12.6.1 INCREASING RELIANCE ON DIGITAL AND INTERCONNECTED SYSTEMS TO BOOST MARKET

12.7 IT & ITES

12.7.1 GROWING DEPENDENCE ON DIGITAL INFRASTRUCTURE AND TECHNOLOGY-DRIVEN OPERATIONS TO DRIVE MARKET

12.8 TELECOMMUNICATIONS

12.8.1 HEIGHTENED EXPOSURE OF CRITICAL INFRASTRUCTURE TO SOPHISTICATED CYBER THREATS TO DRIVE MARKET

12.9 TRANSPORTATION & LOGISTICS

12.9.1 INCREASING RELIANCE ON DIGITAL INFRASTRUCTURE AND GROWING CYBER THREATS TO SUPPLY CHAINS TO DRIVE MARKET

12.10 OTHERS

13 SOC-AS-A-SERVICE MARKET, BY REGION

13.1 INTRODUCTION

13.2 NORTH AMERICA

13.2.1 NORTH AMERICA: SOC-AS-A-SERVICE MARKET DRIVERS

13.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK

13.2.3 US

13.2.3.1 Government initiatives and public-private partnerships to drive market

13.2.4 CANADA

13.2.4.1 Escalating cyber threats, increasing reliance on digital infrastructures, and government initiatives to propel market

13.3 EUROPE

13.3.1 EUROPE: SOC-AS-A-SERVICE MARKET DRIVERS

13.3.2 EUROPE: MACROECONOMIC OUTLOOK

13.3.3 UK

13.3.3.1 Cost efficiency and expertise provided by managed SOC services to propel market

13.3.4 GERMANY

13.3.4.1 Advancements in cloud-native solutions and increased digitalization to boost market

13.3.5 FRANCE

13.3.5.1 Robust regulatory framework and increasing awareness of digital threats to bolster market

13.3.6 ITALY

13.3.6.1 Sustainability and digital innovation initiatives to strengthen market

13.3.7 SPAIN

13.3.7.1 Rising cyber threats, regulatory frameworks, and digitalization to fuel market

13.3.8 NETHERLANDS

13.3.8.1 Robust digital infrastructure, advanced cyber threats, and strategic investments to drive market

13.3.9 REST OF EUROPE

13.4 ASIA PACIFIC

13.4.1 ASIA PACIFIC: SOC-AS-A-SERVICE MARKET DRIVERS

13.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK

13.4.3 CHINA

13.4.3.1 Rapid technological advancement and widespread cloud adoption to drive market

13.4.4 JAPAN

13.4.4.1 Technological advancement and rising cybersecurity breaches to enhance market

13.4.5 INDIA

13.4.5.1 Rapid cloud adoption and technological advancement to drive market

13.4.6 SINGAPORE

13.4.6.1 Escalating cyber threats amid rapid cloud adoption to drive market

13.4.7 AUSTRALIA AND NEW ZEALAND

13.4.7.1 AI, automation, and managed SOC's to fortify market

13.4.8 REST OF ASIA PACIFIC

13.5 MIDDLE EAST & AFRICA

13.5.1 MIDDLE EAST & AFRICA: SOC-AS-A-SERVICE MARKET DRIVERS

13.5.2 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK

13.5.3 MIDDLE EAST

13.5.3.1 GCC

13.5.3.1.1 Increasing digitalization, rising cyber threats, and growing investments in cybersecurity infrastructure to fuel market

13.5.3.1.2 KSA

13.5.3.1.3 UAE

13.5.3.1.4 Qatar

13.5.3.1.5 Rest of GCC

13.5.3.2 Rest of Middle East

13.5.4 AFRICA

13.5.4.1 Widespread utilization of information and communication technology to boost market

13.6 LATIN AMERICA

13.6.1 LATIN AMERICA: SOC-AS-A-SERVICE MARKET DRIVERS

13.6.2 LATIN AMERICA: MACROECONOMIC OUTLOOK

13.6.3 BRAZIL

13.6.3.1 Rising cyberattacks and increasing adoption of cloud technologies to drive market

13.6.4 MEXICO

13.6.4.1 Increasing digital transformation across industries and urgent need to combat escalating cyber threats to drive market

13.6.5 REST OF LATIN AMERICA

14 COMPETITIVE LANDSCAPE

14.1 KEY PLAYER STRATEGIES/RIGHT TO WIN, 2020–2024

14.2 REVENUE ANALYSIS, 2020–2024

14.3 COMPANY VALUATION AND FINANCIAL METRICS

14.4 MARKET SHARE ANALYSIS, 2024

14.5 PRODUCT/BRAND COMPARISON

14.5.1 THALES

14.5.2 NTT DATA

14.5.3 LUMEN TECHNOLOGIES

14.5.4 FORTINET

14.5.5 CLOUDFLARE

14.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2024

14.6.1 STARS

14.6.2 EMERGING LEADERS

14.6.3 PERVASIVE PLAYERS

14.6.4 PARTICIPANTS

14.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2024

14.6.5.1 Company footprint

14.6.5.2 Region footprint

14.6.5.3 Service type footprint

14.6.5.4 Offering footprint

14.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2024

14.7.1 PROGRESSIVE COMPANIES

14.7.2 RESPONSIVE COMPANIES

14.7.3 DYNAMIC COMPANIES

14.7.4 STARTING BLOCKS

14.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2024

14.7.5.1 Detailed list of key startups/SMEs

14.7.5.2 Competitive benchmarking of key startups/SMEs

14.8 COMPETITIVE SCENARIO

14.8.1 PRODUCT LAUNCHES AND ENHANCEMENTS,
JANUARY 2021–DECEMBER 2024

14.8.2 DEALS, JANUARY 2021–DECEMBER 2024

15 COMPANY PROFILES

15.1 INTRODUCTION

15.2 KEY PLAYERS

15.2.1 THALES

15.2.1.1 Business overview

15.2.1.2 Products/Solutions/Services offered

15.2.1.3 Recent developments

15.2.1.3.1 Product launches and enhancements

15.2.1.3.2 Deals

15.2.1.4 MnM view

15.2.1.4.1 Right to win

15.2.1.4.2 Strategic choices

15.2.1.4.3 Weaknesses and competitive threats

15.2.2 AIRBUS CYBERSECURITY

15.2.2.1 Business overview

15.2.2.2 Products/Solutions/Services offered

15.2.2.3 Recent developments

15.2.2.3.1 Product launches and enhancements

15.2.2.3.2 Deals

15.2.2.4 MnM view

- 15.2.2.4.1 Right to win
- 15.2.2.4.2 Strategic choices
- 15.2.2.4.3 Weaknesses and competitive threats
- 15.2.3 NTT DATA
 - 15.2.3.1 Business overview
 - 15.2.3.2 Products/Solutions/Services offered
 - 15.2.3.3 Recent developments
 - 15.2.3.3.1 Product launches and enhancements
 - 15.2.3.3.2 Deals
 - 15.2.3.4 MnM view
 - 15.2.3.4.1 Right to win
 - 15.2.3.4.2 Strategic choices
 - 15.2.3.4.3 Weaknesses and competitive threats
- 15.2.4 LUMEN TECHNOLOGIES
 - 15.2.4.1 Business overview
 - 15.2.4.2 Products/Solutions/Services offered
 - 15.2.4.3 Recent developments
 - 15.2.4.3.1 Product launches and enhancements
 - 15.2.4.3.2 Deals
 - 15.2.4.4 MnM view
 - 15.2.4.4.1 Right to win
 - 15.2.4.4.2 Strategic choices
 - 15.2.4.4.3 Weaknesses and competitive threats
- 15.2.5 FORTINET
 - 15.2.5.1 Business overview
 - 15.2.5.2 Products/Solutions/Services offered
 - 15.2.5.3 Recent developments
 - 15.2.5.3.1 Product launches and enhancements
 - 15.2.5.3.2 Deals
 - 15.2.5.4 MnM view
 - 15.2.5.4.1 Right to win
 - 15.2.5.4.2 Strategic choices
 - 15.2.5.4.3 Weaknesses and competitive threats
- 15.2.6 VERIZON
 - 15.2.6.1 Business overview
 - 15.2.6.2 Products/Solutions/Services offered
 - 15.2.6.3 Recent developments
 - 15.2.6.3.1 Deals
- 15.2.7 CLOUDFLARE

- 15.2.7.1 Business overview
- 15.2.7.2 Products/Solutions/Services offered
- 15.2.7.3 Recent developments
 - 15.2.7.3.1 Product launches and enhancements
 - 15.2.7.3.2 Deals
- 15.2.8 CHECK POINT
 - 15.2.8.1 Business overview
 - 15.2.8.2 Products/Solutions/Services offered
 - 15.2.8.3 Recent developments
 - 15.2.8.3.1 Product launches and enhancements
 - 15.2.8.3.2 Deals
- 15.2.9 KASEYA
 - 15.2.9.1 Business overview
 - 15.2.9.2 Products/Solutions/Services offered
 - 15.2.9.3 Recent developments
 - 15.2.9.3.1 Product launches and enhancements
 - 15.2.9.3.2 Deals
- 15.2.10 TRUSTWAVE
 - 15.2.10.1 Business overview
 - 15.2.10.2 Products/Solutions/Services offered
 - 15.2.10.3 Recent developments
 - 15.2.10.3.1 Product launches and enhancements
 - 15.2.10.3.2 Deals
- 15.2.11 ARCTIC WOLF NETWORKS
 - 15.2.11.1 Business overview
 - 15.2.11.2 Products/Solutions/Services offered
 - 15.2.11.3 Recent developments
 - 15.2.11.3.1 Product launches and enhancements
 - 15.2.11.3.2 Deals
- 15.2.12 PROFICIO
 - 15.2.12.1 Business overview
 - 15.2.12.2 Products/Solutions/Services offered
 - 15.2.12.3 Recent developments
 - 15.2.12.3.1 Product launches and enhancements
 - 15.2.12.3.2 Deals
- 15.2.13 LRQA
 - 15.2.13.1 Business overview
 - 15.2.13.2 Products/Solutions/Services offered
- 15.2.14 INSPIRISYS

- 15.2.14.1 Business overview
- 15.2.14.2 Products/Solutions/Services offered
- 15.2.15 CONNECTWISE
 - 15.2.15.1 Business overview
 - 15.2.15.2 Products/Solutions/Services offered
 - 15.2.15.3 Recent developments
 - 15.2.15.3.1 Product enhancements and enhancements
 - 15.2.15.3.2 Deals
- 15.2.16 TECEZE
 - 15.2.16.1 Business overview
 - 15.2.16.2 Products/Solutions/Services offered
- 15.2.17 CLOUD4C
 - 15.2.17.1 Business overview
 - 15.2.17.2 Products/Solutions/Services offered
- 15.2.18 INFOPULSE
 - 15.2.18.1 Business overview
 - 15.2.18.2 Products/Solutions/Services offered
- 15.3 OTHER PLAYERS
 - 15.3.1 ESENTIRE
 - 15.3.2 CLEARNETWORK
 - 15.3.3 CYBERSECOP
 - 15.3.4 FORESITE CYBERSECURITY
 - 15.3.5 STATOSPHERE NETWORKS
 - 15.3.6 ESEC FORTE
 - 15.3.7 CYBERSAFE SOLUTIONS
 - 15.3.8 10XDS
 - 15.3.9 CISO GLOBAL
 - 15.3.10 ACE CLOUD HOSTING
 - 15.3.11 PLUSSERVER
 - 15.3.12 SAFEAEON
 - 15.3.13 SOCWISE
 - 15.3.14 INSOC (ENHANCED.IO)
 - 15.3.15 WIZARD CYBER
 - 15.3.16 EVENTUS SECURITY
 - 15.3.17 CYBER SECURITY HIVE
 - 15.3.18 SATTRIX INFORMATION SECURITY
 - 15.3.19 ALERT LOGIC
 - 15.3.20 SYSCOM GLOBAL SOLUTIONS
 - 15.3.21 SOURCEPASS

- 15.3.22 ONTINUE
- 15.3.23 AIUKEN CYBERSECURITY
- 15.3.24 DIGISOC

16 ADJACENT MARKETS

- 16.1 INTRODUCTION
- 16.2 LIMITATIONS
- 16.3 SOC-AS-A-SERVICE MARKET ECOSYSTEM AND ADJACENT MARKETS
- 16.4 MANAGED DETECTION AND RESPONSE (MDR) MARKET
 - 16.4.1 MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY SECURITY TYPE
 - 16.4.2 MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY DEPLOYMENT MODE
 - 16.4.3 MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY ORGANIZATION SIZE
 - 16.4.4 MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY VERTICAL
 - 16.4.5 MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY REGION
- 16.5 MANAGED SECURITY SERVICES (MSS) MARKET
 - 16.5.1 MANAGED SECURITY SERVICES (MSS) MARKET, BY SERVICE TYPE
 - 16.5.2 MANAGED SECURITY SERVICES (MSS) MARKET, BY TYPE
 - 16.5.3 MANAGED SECURITY SERVICES (MSS) MARKET, BY ORGANIZATION SIZE
 - 16.5.4 MANAGED SECURITY SERVICES (MSS) MARKET, BY SECURITY TYPE
 - 16.5.5 MANAGED SECURITY SERVICES (MSS) MARKET, BY VERTICAL
 - 16.5.6 MANAGED SECURITY SERVICES (MSS) MARKET, BY REGION
- 16.6 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET
 - 16.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY COMPONENT
 - 16.6.2 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY APPLICATION
 - 16.6.3 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY DEPLOYMENT MODE
 - 16.6.4 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY ORGANIZATION SIZE
 - 16.6.5 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY VERTICAL
 - 16.6.6 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MARKET, BY REGION

17 APPENDIX

17.1 DISCUSSION GUIDE

17.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

17.3 CUSTOMIZATION OPTIONS

17.4 RELATED REPORTS

17.5 AUTHOR DETAILS

I would like to order

Product name: SOC-as-a-Service (SOCaaS) Market by Service Type (Managed SIEM & Log Management, Vulnerability Scanning & Assessment, Threat Detection & Remediation), Security Type (Endpoint Security, Network Security, Cloud Security) - Global Forecast to 2030

Product link: <https://marketpublishers.com/r/SC59AEA7EED8EN.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/SC59AEA7EED8EN.html>