Security Operations Center Market Forecasts to 2030 – Global Analysis By Component (Solutions and Services), Service Type, Security Type, Deployment Mode, Organization Size, End User and By Geography

https://marketpublishers.com/r/SF70FB03A56DEN.html
Date: April 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: SF70FB03A56DEN

Abstracts

According to Stratistics MRC, the Global Security Operations Center Market is accounted for $47.68 billion in 2024 and is expected to reach $102.06 billion by 2030 growing at a CAGR of 13.5% during the forecast period. Security experts may monitor, identify, assess, and react to cybersecurity threats in real time in a centralised location called a Security Operations Centre (SOC). It protects an organization's networks, systems, and data by acting as the first line of defence against cyberattacks. A SOC works around-the-clock and uses cutting-edge technologies to find vulnerabilities, such as automation, threat intelligence, and Security Information and Event Management (SIEM). By proactively reducing security threats, guaranteeing business continuity, and protecting vital assets from cyber threats and unauthorised access, it improves incident response, compliance, and risk management.

Market Dynamics:

Driver:

AI & automation integration

Real-time analysis of enormous data volumes by automated algorithms reduces false positives and finds abnormalities. AI-driven analytics reduce cyber risks by improving incident prediction and speeding up cleanup. Cybersecurity defences are strengthened by machine learning models that are constantly adjusted to new threats. Routine procedures are streamlined by automation, freeing up security staff to concentrate on intricate threats. SOC capabilities are improved by this sophisticated connection, guaranteeing quicker and more proactive security management.

Restraint:

High initial investment

Establishing a SOC necessitates a large investment in innovative technology, infrastructure, and qualified staff. Due to their inability to allocate such cash, small and medium-sized businesses (SMEs) are less able to participate in the market. Furthermore, many organisations find it less affordable because to the complexity of maintaining and operating a SOC. Market growth is slowed by this expensive obstacle as many prospective clients choose to use outsourced or less complete security solutions. All things considered, the high initial prices limit market penetration and acceptance in a number of industries.

Opportunity:

Zero trust security adoption

Monitoring and implementing stringent access restrictions are critical functions of SOCs as organisations transition from perimeter-based defences to continuous verification. SOCs must combine automation, artificial intelligence, and sophisticated analytics to successfully manage Zero Trust settings due to the growing complexity of cyberthreats. Businesses are further encouraged to invest in SOC solutions for real-time security monitoring by compliance rules and data protection obligations. Because of the increased attack surfaces brought about by cloud adoption and remote work, SOC-driven Zero Trust frameworks are crucial for cybersecurity resilience. The market demand for security analytics platforms and managed SOC services is anticipated to increase as a result of this trend.

Threat:

Competition from AI-driven security solutions

AI-based solutions lessen the need for human analysts by providing automatic threat identification and quicker reaction times. Additionally, these solutions scale more effectively, which appeals to companies looking for quick and affordable security solutions. Traditional SOC models, which mostly rely on human procedures, find it difficult to keep up with the rapid advancements in AI. AI-driven solutions also give traditional SOCs a competitive edge by offering predictive capabilities that they do not. SOC providers are being forced to innovate or risk becoming obsolete due to the trend towards automation and artificial intelligence.

Covid-19 Impact

The COVID-19 pandemic significantly impacted the Security Operations Center (SOC) market, driving increased demand for cybersecurity solutions due to the rapid shift to remote work and rising cyber threats. Organizations accelerated digital transformation, increasing reliance on cloud-based SOC services. However, budget constraints and supply chain disruptions initially slowed investments. The pandemic also highlighted the need for AI-driven security automation to manage growing threats efficiently.

The cloud security segment is expected to be the largest during the forecast period

The cloud security segment is expected to account for the largest market share during the forecast period as organizations increasingly migrate to cloud environments. The demand for SOC solutions is increased by cloud-based infrastructures' requirement for ongoing monitoring and threat detection. Scalability and flexibility provided by cloud security services allow SOCs to more effectively handle a variety of security threats. SOCs may guarantee real-time protection across hybrid and multi-cloud platforms by including cutting-edge cloud security capabilities. SOCs are changing as a result of the increased dependence on cloud-based operations, which is also propelling innovation and acceptance in the security space.

The government & defense segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the government & defense segment is predicted to witness the highest growth rate, due to increasing cyber threats to national security. Strong cybersecurity measures are necessary because governments and defence agencies handle sensitive data, which increases demand for SOC solutions. This industry makes significant investments in cutting-edge security technologies to protect critical infrastructure and thwart cyberattacks, and the adoption of SOCs to guarantee data protection is pushed by rising government regulations and compliance standards.

Region with largest share:

+357 96 030922
info@marketpublishers.com

During the forecast period, the North America region is expected to hold the largest market share due to increasing cybersecurity threats and the need for advanced threat detection systems. The region's strong adoption of cloud computing and Internet of Things (IoT) technologies is driving demand for SOC services. Companies in North America are increasingly focusing on integrating AI and machine learning into their security operations to enhance incident response capabilities. Additionally, government regulations and rising concerns over data privacy are pushing businesses to invest in robust SOC solutions.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, owing to the increasing frequency of cyber threats and the rise of digital transformation initiatives. Governments and enterprises in countries like China, India, and Japan are investing heavily in advanced cybersecurity solutions. Furthermore, the region’s increasing reliance on remote working models is heightening the need for comprehensive security operations. As a result, managed security services and automation tools are expected to dominate the market, offering efficient and scalable solutions.

Key players in the market

Some of the key players profiled in the Security Operations Center Market include Palo Alto Networks, Fortinet, SentinelOne, Splunk, Secureworks, Symantec, Sogeti, IBM Security, Cisco Secure, Check Point Software Technologies, Trend Micro, FireEye, Rapid7, LogRhythm, AT&T Cybersecurity and CrowdStrike.

Key Developments:

In October 2024, Fortinet partnered with Bharti Airtel's enterprise arm to launch 'Airtel Secure Internet,' a managed cybersecurity solution. This service combines Airtel's internet connectivity with Fortinet's next-generation firewall (NGFW) and integrates with Airtel's Security Operations Centre (SOC) to provide comprehensive protection against cyber threats.

In May 2024, Fortinet introduced the industry's first Generative AI IoT Security Assistant. This tool leverages AI to enhance network and security operations, providing organizations with advanced natural language processing capabilities to improve threat detection and response times.

+357 96 030922
info@marketpublishers.com

In June 2023, Palo Alto Networks partnered with L&T Technology Services (LTTS) to offer security services in 5G and Operational Technology (OT) sectors. As a Managed Security Services Partner (MSSP), LTTS delivers a suite of security services, including 5G, OT, and IT/OT Converged SOC services, utilizing Palo Alto Networks' Zero Trust OT Security solution.

Components Covered:

- Solutions
- Services

Service Types Covered:

- Prevention Services
- Detection Services
- Incident Response Services
- Remediation Services
- Other Service Types

Security Types Covered:

- Network Security
- Cloud Security
- Endpoint Security
- Application Security
- Database Security

+357 96 030922
info@marketpublishers.com

Other Security Types

Deployment Modes Covered:

On-Premises

Cloud-Based

Hybrid

Organization Sizes Covered:

Small and Medium-Sized Enterprises (SMEs)

Large Enterprises

End Users Covered:

BFSI (Banking, Financial Services, and Insurance)

Government & Defense

Healthcare & Life Sciences

IT & Telecommunications

Retail & E-commerce

Manufacturing

Energy & Utilities

Education

Transportation & Logistics

Other End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

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

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 2022, 2023, 2024, 2026, and 2030
- 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
  - Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

+357 96 030922
info@marketpublishers.com

11 GLOBAL SECURITY OPERATIONS CENTER MARKET, BY GEOGRAPHY

+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.

I would like to order

Product name: Security Operations Center Market Forecasts to 2030 – Global Analysis By Component (Solutions and Services), Service Type, Security Type, Deployment Mode, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/SF70FB03A56DEN.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/SF70FB03A56DEN.html