Automated Breach And Attack Simulation Market is anticipated to surpass US$34.664 billion by 2029 at a CAGR of 33.40%

The automated breach and attack simulation market is anticipated to grow at a CAGR of 33.40% from US$4.611 billion in 2022 to US$34.664 billion by 2029.

NOIDA, UTTAR PARDESH, INDIA, May 29, 2024 /EINPresswire.com/ -- According to a new study published by Knowledge Sourcing Intelligence, the automated breach and attack simulation market is projected to grow at a CAGR of 33.40% between 2022 and 2029 to reach US$34.664 billion by 2029.

> The automated breach and attack simulation market is anticipated to grow at a CAGR of 33.40% from US$4.611 billion in 2022 to US$34.664 billion by 2029."
>
> *Knowledge Sourcing Intelligence*

Automated BAS(breach and attack simulation) is being used as a security testing technique and is very helpful for organizations to find out the vulnerabilities within their security setups. By imitating the attack paths, vectors, and storylines, BAS software is designed to assist enterprises by providing security measures to the system by safeguarding the data from various attacks. Automated Breach and Attack Simulation (BAS) is the software-driven strategic approach in offensive security that mimics cyberattacks to measure the capacity of security controls.

BAS is a sophisticated approach to computer security testing that reveals weaknesses in security mechanisms by imitating hacker tactics. Breach attack simulation tools, for instance, can evaluate both external and internal risky conditions, in addition, they are able to identify lateral movement and data exfiltration. Besides these, they may determine the organization's readiness to a cyber-attack by conducting simulated attacks to test existing rules and systems in place. If there is any weakness detected, BAS simulations will further propose the actions that need to be undertaken in the sequence that they need to be priority corrected.

The surge in cybersecurity threats is the primary driving force behind the automated breach and attack simulation market growth. For instance, according to IBM published article in 2024 it state that, there has been a 71% growth in cyberattacks that use stolen or hijacked credentials

advantages over the previous year. Also, statistics show that about 32% of cyber events resulted in data theft or leak, meaning that the attackers focus on stealing and selling data rather than on encryption for extortion. Similarly, the AI market share reaching the 50% milestone will serve as an impetus to the cybercriminal communities to prepare low-cost tools to attack AI technologies.

Breach and attack simulation help info security teams to discover and counter possible hackers or viruses cybers in advance. This makes it possible for security teams to confine their time and resources to assessing vulnerabilities and may not necessarily face the insidious problem of critical data breaches, loss of access or any other undesirable consequences.

Numerous product launches and collaborations are taking place in the market thereby, increasing the automated breach and attack simulation market growth.

• For instance, in August 2023: The AttackIQ newest product line which is revolutionizing cybersecurity testing "AttackIQ for Everyone" services offer many options that include on-demand testing and full-manage services. This enables an organization of any size to quickly know the security stance and vulnerabilities in the system without much investment in resources or knowledge.

Access sample report or view details: https://www.knowledge-sourcing.com/report/automated-breach-and-attack-simulation-market

The automated breach and attack simulation market, based on the solution is segmented into four categories namely breach & attack simulation platform, services, professional services, and managed security services. Breach & attack simulation platform is expected to account for the major share of the automated breach and attack simulation market growth. Breach & attack simulation platforms are the most desired option because of the self-service feature for proactive security testing that does not need external expertise.

The automated breach and attack simulation market, based on the deployment is segmented into two categories namely on-premises and cloud-based. Cloud-based is expected to account for the major share of the automated breach and attack simulation market growth. Cloud computing implementations are continuously evolving as marketing and media companies adopt scalable, affordable, and convenient cloud storage to permeate the media landscape and replace on-premises offerings.

The automated breach and attack simulation market, based on the application is segmented into four categories namely threat management, configuration management, patch management, and others. Threat management is expected to account for the major share of the automated breach and attack simulation market growth. The BAS (Breach and Attack Simulation) systems view Threat Management as one of the most vital aspects as they proactively identify deficiencies in a company's defense capability to withstand real-life attacks thus exceeding a mere attack

patching.

Based on geography, the automated breach and attack simulation market is expanding significantly in the North American region due to various factors. In countries like the United States, Canada, and Mexico there is a growing demand for automated breach and attack simulation in various industries, including IT and Telecommunication, banking, hospitals, and government offices. The demand is being driven by these nations is due to the rising cyber threats in the realm of attacks, tightening regulatory frameworks and increasing adoption of cloud-based technologies are the major drivers for the companies to integrate preventive security measures.

The research includes several key players from the automated breach and attack simulation market, such as Sophos, XM Cyber, Cymulate, AttackIQ, Skybox Security, and Aujas.

The market analytics report segments the automated breach and attack simulation market as follows:

- By Solution

  - Breach & Attack Simulation Platform
  - Services
  - Professional Services
  - Managed Security Services

- By Deployment

  - On-premises
  - Cloud-based

- By Application

  - Threat Management
  - Configuration Management
  - Patch Management
  - Others

- By Geography

  - North America

- United States
- Canada
- Mexico

o South America

- Brazil
- Argentina
- Others

o Europe

- United Kingdom
- Germany
- France
- Spain
- Others

o Middle East and Africa

- Saudi Arabia
- UAE
- Israel
- Others

o Asia Pacific

- Japan
- China
- India
- South Korea
- Indonesia
- Thailand
- Others

Companies Profiled:

- Sophos
- XM Cyber
- Cymulate
- AttackIQ
- Skybox Security
- Aujas

Explore More Reports:

• Network Security Market: https://www.knowledge-sourcing.com/report/network-security-market

• AI (Artificial Intelligence) In Simulation Market: https://www.knowledge-sourcing.com/report/ai-artificial-intelligence-in-simulation-market

• Simulation Software And Services Market: https://www.knowledge-sourcing.com/report/simulation-software-and-services-market

Ankit Mishra
Knowledge Sourcing Intelligence LLP
+1 850-250-1698
email us here
Visit us on social media:
Facebook
X
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/715428590

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2024 Newsmatics Inc. All Right Reserved.