Cyber Security For Industrial Automation Market Report 2023-2032 : Why You Should Invest In This Market ?

The growing role of cybersecurity in threat response and tech integration in industrial automation will drive market growth, with APAC leading by 2032.

Cyber Security For Industrial Automation Market Size

WILMINGTON, DE, UNITED STATES, March 3, 2025 /EINPresswire.com/ -- According to a new report published by Allied Market Research, the cyber security for industrial automation market size was valued at $9 billion in 2022, and is estimated to reach $20.5 billion by 2032, growing at a CAGR of 8.7% from 2023 to 2032. Cybersecurity for industrial automation implements a set of practices, tools, and technologies to protect the industrial systems, data, and network from cyber threats such as ransomware, malicious software's, emails, data breach, and others.

Industrial automation, which is quite popular across industries namely automotive, pharmaceutical, food & beverage, and others involves the use of control systems, sensors, and other devices for managing the industrial processes. Furthermore, the integration of digital technologies and advanced connectivity has led to increase in cyber threats and related vulnerabilities that can expose the crucial data. In such cases, cyber security for industrial automation plays a major role in protecting the critical infrastructure present in industrial units as well as preventing unauthorized access, data breaches, and cyber threats.

Download Sample Report (Get Full Insights in PDF - 320 Pages) at: https://www.alliedmarketresearch.com/request-sample/A289338

Cyber security in industrial automation implements set of measures such as network security, encryption, endpoint security, access control, regulatory compliance, physical security, and others to prevent cyber-attacks. For instance, in network security, the trained cyber security professionals implement firewalls, virtual private networks (VPNs), intrusion detection & prevention systems, and others to ensure network security. The cyber security for access control

restricts or manages access to critical systems and data via various authorization mechanisms, authentication, and role-based access control. In addition, the end-point security is quite popular in the automotive and food & beverage sectors as it helps in securing individual devices, programmable logic controllers, and other devices.

The adoption of cyber security in industrial automation faces notable restraints majorly owing to the challenges associated with acquiring the requisite skills and expertise. For instance, the existing workforce comprised of specialists and engineers with extensive experience & technical expertise faces difficulties in adapting to the demands of emerging technologies. Thus, to bridge this skills gap, several organizations have to rely on contract workers for integration advanced cyber security technologies in the industrial automation processes. Thus, organizations must invest in training programs to upskill their existing workforce which is an additional expense for the companies. These factors are anticipated to restrain the cyber security for industrial automation industry growth in the upcoming years.

Buy Now & Get Exclusive Report at: https://www.alliedmarketresearch.com/cyber-security-for-industrial-automation-market/purchase-options

The cyber security technologies that aim to enhance the production of industrial automation systems against cyber-attacks has been undergoing technological advancements which is anticipated to generate excellent opportunities for the market players in the upcoming years. For instance, the integration of artificial intelligence (AI), helps in process optimization and enhances employee safety. This is majorly owing to the real-time monitoring of network traffic and anomalies via cyber security solutions that helps in efficiently detecting cyber threats and responding to these threats in the real-time. In addition, quantum computing that have high processing power can be used in encryption methods to protect the sensitive data. These technologies are anticipated to have positive impact on the cyber security for industrial automation market forecast.

The cyber security for industrial automation market share is segmented on the basis of type, tools or technologies, security type, end use, and region. By type, it is classified into fixed automation system, programmable automation system, flexible automation system, and integrated automation system. By tools or technologies, it is classified into numerical control (NC) machine tools, programmable logic controllers (PLCs), computer numerical control (CNC) systems, and industrial sensors. By security type, it is classified into enterprise security, SCADA security (supervisory control and data acquisition), network security, device security, and physical security. By end use, the market is classified into automotive manufacturing, electronics & telecommunication, food & beverage processing, pharmaceuticals, and others. By region, the market is analyzed across North America, Europe, Asia-Pacific, and LAMEA.

The key players profiled in the cyber security for industrial automation market analysis report include IBM, ABB, Schneider Electric, Honeywell International Inc., Siemens AG, Microsoft Corporation, Rockwell Automation Inc., Palo Alto Networks, Cisco Systems, Inc., and Dell Inc.

If you have any special requirements, Request customization: https://www.alliedmarketresearch.com/request-for-customization/A289338

The report offers a comprehensive study on global cyber security for industrial automation market trends by thoroughly studying different aspects of the market including major segments, market statistics, market dynamics, regional market outlook, investment opportunities, and top players working towards the growth of the market. The report also highlights the present scenario and upcoming trends & developments that are contributing toward the growth of the market. Moreover, restraints and challenges that hold power to obstruct the market growth are also profiled in the report along with the Porter's five forces analysis of the market to elucidate factors such as competitive landscape, bargaining power of buyers and suppliers, threats of new players, and emergence of substitutes in the market.

Impact of COVID-19 On The Global Cyber Security For Industrial Automation Industry

1. The pandemic led to disruptions in global supply chains due to lockdowns, restrictions on international trade, and reduced manufacturing activities. These disruptions led to remote work culture that exposed several industries to cyber threats by compromising network security and leading to data breach.

2. Industrial automation staff became the target for phishing emails containing malicious links or attachments. The cybercriminals took advantage of uncertainty and fear due to pandemic owing to which it became easy for cyber criminals to launch the attacks.

3. As cyber security led to financial losses and budget constraints for the industrial or manufacturing companies due to closed operations, several industries were facing issues in updating and maintaining effective cyber security measures during the pandemic. These factors led to negative impact on the cyber security for industrial automation market during the pandemic.

For Purchase Enquiry: https://www.alliedmarketresearch.com/purchase-enquiry/A289338

About Us:

Allied Market Research (AMR) is a full-service market research and business-consulting wing of Allied Analytics LLP based in Portland, Oregon. Allied Market Research provides global enterprises as well as medium and small businesses with unmatched quality of "Market Research Reports" and "Business Intelligence Solutions." AMR has a targeted view to provide business insights and consulting to assist its clients in making strategic business decisions and achieving sustainable growth in their respective market domains.

Pawan Kumar, the CEO of Allied Market Research, is leading the organization toward providing

high-quality data and insights. We are in professional corporate relations with various companies. This helps us dig out market data that helps us generate accurate research data tables and confirm the utmost data procurement methodology includes deep presented in the reports published by us is extracted through primary interviews with top officials from leading online and offline research and discussion with knowledgeable professionals and analysts in the industry.

Contact:
David Correa
1209 Orange Street,
Corporation Trust Center,
Wilmington, New Castle,
Delaware 19801 USA.
Int'l: +1-503-894-6022
Toll Free: + 1-800-792-5285
UK: +44-845-528-1300
India (Pune): +91-20-66346060
Fax: +1-800-792-5285
help@alliedmarketresearch.com

David Correa
Allied Market Research
+ 1 800-792-5285
email us here
Visit us on social media:
Facebook
X
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/790545262

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.
© 1995-2025 Newsmatics Inc. All Right Reserved.