SIEMENS
Ingenuity for life

The importance of industrial security services

As industrial machines, equipment and systems grow more and more connected, manufacturers are more vulnerable than ever to cyberattacks. The same technologies and platforms that allow companies to drive unparalleled efficiency and quality also increase the risk of crippling cyber-attacks.

Malware, traditional cyber-attacks, phishing, and malicious insiders are all disturbingly common threats to manufacturers. Regardless of the variety, cyber-attacks are also enormously expensive. A recent study from Frost & Sullivan reported that on average, a large manufacturer loses $10.7 million in direct costs and $8.1 million in indirect costs from a single attack.

Cybersecurity has already been growing more important, but it is especially crucial with record numbers of employees working remotely. Combined with the steady advance of digitalization in industrial facilities, it is clear that manufacturers need a comprehensive, state-of-the-art solution to protect against cyber threats. Siemens Industrial Security Services answers this challenge, paving the way for a safe, seamless and secure digitalization journey.

A three step process to securing your industrial network

Protecting complex industrial OT systems from the evolving, myriad threats of cyber-attacks is not a simple process. There's no one-size-fits-all solution - every network will have unique vulnerabilities and characteristics that must be accounted for. Manufacturers must take great care to ensure that they are carefully reviewing their network and OT systems from top to bottom and rigorously safeguarding them against potential threats.

Siemens Industrial Security Services follows our end-to-end approach with a three-step process for ensuring your OT system is protected. The first step is a security assessment. For most manufacturers, cybersecurity is simply not their area of expertise - and compromise is not an option when it comes to protecting your network.

Our security service experts comb through your network for specific vulnerabilities and security risks with assessments aligned with IEC 62443 and ISO 27001 international standards. We also ensure the recommendations meet your policies, plant-specific network, and manufacturing processes. Altogether, this stage provides you with a clearly defined roadmap for safeguarding your network against cybersecurity threats.

Building a state-of-the-art security program

Once we have a comprehensive understanding of your network and any security gaps, we are able to get to work building a state-of-the-art security solution. We implement proven, cutting-edge security solutions that are adapted to fit seamlessly into an automation environment.

Our experts use tools from well-known and respected organizations in OT security and make sure they are properly implemented to protect your network against threats without interfering with daily processes. From cybersecurity training to automation firewalls and routine data hygiene, our team ensures your network has rock-solid protection against threats of all varieties.

Malware never sleeps - and neither should your cybersecurity

No organization on Earth is immune to cyber-attacks. One of the biggest challenges in cybersecurity is staying abreast of rapidly evolving cyber threats. Even the most advanced security systems require continual, routine updates to ensure protection against the latest malware and other threats.

Furthermore, the rapid technological advances and digitalization occurring in the manufacturing sector can easily create new vulnerabilities in otherwise secure networks. To keep your network safe, it is crucial to regularly reassess and update your cybersecurity platform - as well as monitor for new threats.

In the optimization phase, Siemens works with your organization to continuously adapt your security platform to stay ahead of new threats, technologies and regulations. Siemens offers end-to-end monitoring for proactive protection, vulnerability and patch management, and remote incident handling to quickly address any issues. Lastly, Siemens is able to monitor legacy equipment across different vendors, making it easy and flexible to keep your network secure.

One of the most impressive tools in our optimization portfolio is industrial anomaly detection. In short, this tool passively monitors industrial automation equipment for anomalies. By using this tool in combination with AI and machine learning, it can rapidly identify and flag suspicious behavior for further investigation. As the tool does not interact whatsoever with the automation, there is no risk of harming equipment or otherwise interfering with production.

Siemens - the trusted partner for industrial security solutions

Manufacturers are spoiled for choice when it comes to industrial security partners. But there's a reason why leading manufacturers have chosen Siemens for a process this important. Siemens brings a truly unique blend of proven expertise in not only industrial security, but also first-hand experience with digitalization and manufacturing at our own innovative facilities.

As a leader in next-generation automation technologies, there is no partner better suited to bring your facility to industry 4.0 while also protecting it against tomorrow's cyber threats. In an area where compromise is not an option, it's hard to imagine settling for anything less.

To find out how we can help your business, or to get in contact with us, please visit usa.siemens.com/digital-enterprise-services

Published by
Siemens Industry, Inc. 2020

Siemens Digital Industries
100 Technology Drive
Alpharetta, GA 30005
1-800-365-8766