Schneider Electric First in Industry - Higher Level Cybersecurity Certification for EcoStruxure™ IT DCIM Solutions

GURUGRAM, HARYANA, INDIA, October 29, 2024 /EINPresswire.com/ -- [Schneider Electric](#) First in Industry to obtain Higher Level Cybersecurity Certification for EcoStruxure™ IT DCIM Solutions

• IEC 62443-4-2 SL2 certification provides higher level of protection against cyberthreats for EcoStruxureTM IT Data Center Infrastructure Management (DCIM) solutions
• Independent certification process features rigorous testing and assessment
• Network Management Card 3 (NMC3) only network management card to obtain this level of encryption and robustness

Schneider Electric logo

Schneider Electric, the leader in digital transformation of energy management and automation, announced an industry first: its EcoStruxure IT Network Management Card 3 (NMC3) platform has obtained a new and higher level of cybersecurity certification, making it the first Data Center Infrastructure Management (DCIM) network card to achieve IEC 62443-4-2 Security Level 2 (SL2) designation from the International Electrotechnical Commission (IEC).

TÜV Rheinland, one of the world's largest and leading testing providers, has independently certified the NMC3 platform, ensuring vendor products designed for data centre and distributed IT environments meet a set of well-defined security requirements and undergo thorough testing and assessment.

This new and higher level of cybersecurity certification underscores Schneider Electric's

commitment to leading the industry in secure operations and better protects against cyberthreats. SL2 certification provides more stringent requirements and increased security resiliency than SL1, which was obtained last year.

In addition to the new standard, TÜV Rheinland has certified Schneider Electric and the cybersecurity processes used to develop our products, including the NMC3, as ISASecure® Secure Development Lifecycle Assurance (SDLA) compliant. The NMC3 is embedded in the majority of Schneider Electric's EcoStruxure IT DCIM products and provides a robust, remotely accessible management application over the network for critical power and cooling infrastructure.

"According to the 2024 Allianz Risk Barometer, cyber incidents are ranked as the number one business concern. At an average reported cost of more than $4 million an incident, we understand why cybersecurity tops the priority list for CIOs," said Kevin Brown, SVP for EcoStruxure IT, Data Center Business, Schneider Electric. "With the IEC 62443-4-2 SL2 and ISASecure® SDLA cybersecurity certifications, Schneider Electric is leading the industry with this dual certification helping to reduce risks to critical infrastructure."

Simplifying the process of installing firmware

Companies are challenged to keep up with firmware updates. Many enterprise customers manage their critical power and cooling infrastructure with their own in-house management tools, third-party network management tools, or building management systems. These systems don't know when the firmware at your connected endpoints – particularly in distributed and edge environments - requires an update.

The EcoStruxure IT Secure NMC System offers improved embedded firmware management thanks to a new dedicated tool. The Secure NMC System Tool transforms the cumbersome process of researching and installing the latest firmware on all devices, making the process up to 90% faster. Users no longer need to search for firmware on an ad hoc basis, check to see if that firmware is the latest one for your device, and read the release notes to understand what's included in the new version before they download it and update their device. Instead, the Secure NMC System Tool notifies customers that new firmware is available and directs them to install the new version.

The benefits of the Secure NMC System include:
1. Eliminate fear of becoming outdated: Simplifies firmware management, making it up to 90% faster and reducing risk.
2. Achieve consistent compliance: Customers have a systematic, standardized approach to cybersecurity updates for their critical power and cooling infrastructure.
3. Reduce exposure to potential attack: IEC 62443-4-2 SL2 and ISASecure® SDLA cybersecurity certifications combined with the Secure NMC System Tool ensures connected devices are protected with the latest security updates.

"EcoStruxure IT is providing customers with a powerful approach - the flexibility to manage their IT infrastructure as they choose and to do it simply while also managing their cybersecurity compliance because being secure doesn't mean it has to be difficult," Brown said. "We are the first in the industry providing this solution as we continue our commitment to enable resilient, secure, and sustainable IT infrastructure."

About Schneider Electric
Schneider's purpose is to create Impact by empowering all to make the most of our energy and resources, bridging progress and sustainability for all. At Schneider, we call this Life Is On.
Our mission is to be the trusted partner in Sustainability and Efficiency.

We are a global industrial technology leader bringing world-leading expertise in electrification, automation and digitization to smart industries, resilient infrastructure, future-proof data centers, intelligent buildings, and intuitive homes. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth for our customers.

We are a people company with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace diversity and inclusion in everything we do, guided by our meaningful purpose of a sustainable future for all.

www.se.com

Debolina Mukherjee
Schneider Electric
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/755778727