Publicado en Barcelona el 11/10/2024

Schneider Electric, se posiciona como la primera empresa del sector en obtener una certificación de ciberseguridad de máximo nivel para sus soluciones EcoStruxure™ IT DCIM

La certificación IEC 62443-4-2 SL2 proporciona un mayor nivel de protección contra las ciberamenazas para las soluciones EcoStruxureTM IT Data Center Infrastructure Management (DCIM). El proceso de certificación independiente incluye pruebas y evaluaciones rigurosas. Network Management Card 3 (NMC3) es la única tarjeta de gestión de red que obtiene este nivel de cifrado y solidez

Schneider Electric, líder en la transformación digital de la gestión de la energía y la automatización, ha anunciado hoy que su plataforma EcoStruxure IT Network Management Card 3 (NMC3) ha obtenido un nuevo y más alto nivel de certificación de ciberseguridad, lo que la convierte en la primera tarjeta de red de gestión de infraestructuras de centros de datos (DCIM) en lograr la designación IEC 62443-4-2 Security Level 2 (SL2) de la Comisión Electrotécnica Internacional (IEC).

TÜV Rheinland, uno de los mayores y principales proveedores de ensayos del mundo, ha certificado de forma independiente la plataforma NMC3, lo que garantiza que los productos de los proveedores diseñados para centros de datos y entornos informáticos distribuidos cumplen una serie de requisitos de seguridad definidos y se someten a pruebas y evaluaciones exhaustivas.

Este nuevo y más alto nivel de certificación de ciberseguridad subraya el compromiso de Schneider Electric por liderar la industria en operaciones seguras y ofrecer una mayor protección contra las ciberamenazas. La certificación SL2 proporciona requisitos más estrictos y una mayor resistencia de seguridad que la SL1, obtenida el año pasado.

Además de la nueva norma, TÜV Rheinland ha certificado a Schneider Electric y los procesos de ciberseguridad utilizados para desarrollar los productos, incluidos los NMC3, como conformes con ISASecure® Secure Development Lifecycle Assurance (SDLA).

El NMC3 está integrado en la mayoría de los productos EcoStruxure IT DCIM de Schneider Electric y proporciona una aplicación de gestión robusta y accesible de forma remota a través de la red para infraestructuras críticas de energía y refrigeración.

"Según el Barómetro de Riesgos 2024 de Allianz, los incidentes cibernéticos ocupan el primer lugar entre las preocupaciones de las empresas. Con un gasto medio declarado de más de 4 millones de dólares por incidente, entendemos por qué la ciberseguridad encabeza la lista de prioridades de los CIO", afirma Kevin Brown, SVP de EcoStruxure IT, Data Center Business, Schneider Electric. "Con las certificaciones de ciberseguridad IEC 62443-4-2 SL2 e ISASecure® SDLA, Schneider Electric lidera la

industria con esta doble certificación que ayuda a reducir los riesgos para las infraestructuras críticas".

Simplificación del proceso de instalación del firmware
Las empresas se enfrentan al reto de mantenerse al día con las actualizaciones de firmware. Muchos clientes gestionan sus infraestructuras críticas de alimentación y refrigeración con sus propias herramientas de gestión internas, herramientas de gestión de redes de terceros o sistemas de gestión de edificios. Estos sistemas no saben cuándo es necesario actualizar el firmware de los terminales conectados, sobre todo en entornos distribuidos y periféricos.

EcoStruxure IT Secure NMC System ofrece una gestión mejorada del firmware integrado gracias a una nueva herramienta específica. La herramienta Secure NMC System transforma el engorroso proceso de búsqueda e instalación del firmware más reciente en todos los dispositivos, haciendo que el proceso sea hasta un 90% más rápido. Los usuarios ya no necesitan buscar firmware ad hoc, comprobar si ese firmware es el más reciente para su dispositivo y leer las notas de la versión para entender qué incluye la nueva versión antes de descargarla y actualizar su dispositivo. En su lugar, Secure NMC System Tool notifica a los clientes que hay un nuevo firmware disponible y les indica que instalen la nueva versión.

Entre las ventajas del sistema Secure NMC se incluyen:

- Elimina el riesgo de quedarse obsoleto: Simplifica la gestión del firmware, haciéndola hasta un 90% más rápida y reduciendo el riesgo.
- Logra un cumplimiento coherente: Los clientes disponen de un enfoque sistemático y estandarizado para las actualizaciones de ciberseguridad de sus infraestructuras críticas de energía y refrigeración.
- Reduce la exposición a posibles ataques: Las certificaciones de ciberseguridad IEC 62443-4-2 SL2 e ISASecure® SDLA, combinadas con Secure NMC System Tool, garantizan que los dispositivos conectados estén protegidos con las últimas actualizaciones de seguridad.

"EcoStruxure IT está proporcionando a los clientes un enfoque innovador: la flexibilidad para gestionar la infraestructura de IT como ellos elijan y hacerlo de forma sencilla, a la vez que gestionan el cumplimiento de la ciberseguridad, porque la protección no tiene por qué ser difícil", afirma Brown. "Somos los primeros del sector en ofrecer esta solución mientras continuamos con nuestro compromiso de hacer posible una infraestructura de IT resistente, segura y sostenible".

Descubrir más información sobre EcoStruxure IT Secure NMC System aquí. La nueva certificación de ciberseguridad IEC 62443-4-2 SL2 se puede ver aquí. Se requiere una suscripción Secure NMC para acceder al firmware certificado IEC a través de Secure NMC System Tool.

Recursos relacionados:

Vídeo explicativo de 60 segundos - EcoStruxure IT™ Industry Leader in Cybersecurity?

Tackling the dual IT infrastructure priorities of visibility and cybersecurity with EcoStruxure IT's secure NMC system?

Schneider Electric's new product security certification makes cybersecurity validation easy

Datos de contacto:
Noelia Iglesias
Team Lewis
93 522 86 00

Nota de prensa publicada en: Barcelona

Categorías: Nacional Software Ciberseguridad Sostenibilidad Innovación Tecnológica Sector Energético