TÜV Rheinland announces launch of its Global Industrial Cybersecurity Center of Excellence in Kuala Lumpur, Malaysia

06/12/2018 | Cologne / Singapore / Kuala Lumpur

TÜV Rheinland announces the launch of its global Industrial Cybersecurity Centre of Excellence (CoE) based in Kuala Lumpur, Malaysia. The Centre of Excellence will address the cybersecurity needs of its industrial clients such as manufacturing companies, plant operators, energy and utility companies, transportation and transit system operators to secure their operational technology landscape. In a rapidly evolving digitalization of markets across all businesses there is a significant need and demand for deep Industrial Security skills and expertise that this Centre of Excellence will continue to develop worldwide.

Under the Global Centre of Excellence, the first Operational Technology (OT) Security Lab based in Kuala Lumpur, Malaysia will serve as the Regional Hub for showcasing industrial cybersecurity technology, knowledge and client consultations. The Operational Technology Security Lab will provide a safe controlled environment for clients to experience scenario -based simulations to test and demonstrate industrial systems vulnerabilities and cybersecurity threats.

“Combining our expertise in Industrial Services and Operational Technology Security in our Centre of Excellence, we are one of the few organizations developing deep capabilities and able to offer this level of cybersecurity expertise to our clients concerned about the safety and security of their operations.” explains Frank Luzsicza, Executive Vice President, at TÜV Rheinland.

The facility will have equipment to showcase industrial manufacturing processes generating real-time industrial data which will be integrated with technologies that detect threats and secure such industrial facilities. “The OT Security lab is a unique and significant step to serve the needs of our clients. Using a combination of training sessions, pilots, demonstrations, threat research and cyber-attack simulations the Operational Technology Security lab will help our clients stay ahead of industrial cyber threats” adds Urmez Daver, Global Head for Industrial Cybersecurity Centre of Excellence.

Cybersecurity in the world of Operational Technology and Industrial Control Systems

Organizations operating industrial facilities have a responsibility to monitor, detect and mitigate cybersecurity attacks in order to maintain the safety, integrity and availability of their plant which, if compromised, may have a severe and detrimental impact on society. Leading cybersecurity standards for industrial control systems emphasize that systems operators should have cybersecurity management solutions in place. TÜV Rheinland has over 100 years of experience in testing and certifying industrial systems and has worked across some of the most challenging industries. Its services portfolio includes end-to-end visibility, threat detection and

continuous vulnerability assessment and monitoring for OT and industrial cybersecurity risks.

Contact for media inquiries: Norman Hübner
Phone: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland is a global leader in independent inspection services, founded nearly 150 years ago. The group maintains a worldwide presence of more than 20,000 people; annual turnover is EUR 2 billion. The independent experts stand for quality and safety for people, technology and the environment in nearly all aspects of life. TÜV Rheinland inspects technical equipment, products and services, oversees projects, and helps to shape processes and information security for companies. Its experts train people in a wide range of careers and industries. To this end, TÜV Rheinland employs a global network of approved labs, testing and education centers. Since 2006, TÜV Rheinland has been a member of the United Nations Global Compact to promote sustainability and combat corruption.

Website: www.tuv.com