kaspersky BRING ON THE FUTURE

7 reasons to choose Kaspersky Industrial CyberSecurity Assessment

“Primum Non Nocere” – First, Do No Harm!

It’s our absolute guiding principle. As experienced industrial cybersecurity practitioners and automation engineers ourselves, we fully understand the risks associated with undertaking any form of security test inside an operational environment. Working closely with your engineers at every stage of the CSA (Cybersecurity Assessment), we keep any potential negative impact set firmly at zero.

We Get To Grips With Your System

We conduct a comprehensive technical review and evaluation of your ICS operations architecture and components. This involves a deep-dive analysis of operational processes – including the underlying network architecture, IT and OT team integration, vendor support, cybersecurity controls, monitoring and all your internal and external connections.

We Take A Holistic Approach To Risk Factors Assessment

Our primary objective is to disclose attack vectors specific to your industrial systems, networks and industrial processes; these vectors (from human factors to advanced exploitation of zero-day vulnerabilities) can potentially come from anywhere in your IT/OT domains and even field devices. So we analyze your industrial organization holistically, as a complex cyber-physical system.

We Do Our Homework

We at Kaspersky demonstrate our industrial cybersecurity expertise not just during the assessment project itself, but in the thoroughness of our preparation. This includes conducting preliminary vulnerability analyses of the industrial equipment – both software and hardware – being used. Since 2016 Kaspersky researchers have found and reported more than 200 ICS/IIoT vulnerabilities.

We Establish What’s “Normal” So We Can Spot The Abnormal

We can conduct a non-intrusive analysis of network data from traffic occurring within your ICS network, to create a visual map of device-to-device communications. Once a benchmark for “normal” communications patterns is established, anomalies begin to reveal themselves.

We Hang On In There

Post-project support is important to us. We don't leave our customers with unpatched vulnerabilities and fuzzy recommendations like "implement network segmentation". We do all that we can to raise your cybersecurity levels, even without deploying additional solutions – like finding workarounds to close vulnerabilities or putting pressure on IAVs to produce prompt updates.

We Believe Every Customer Is Unique

All our CSA projects are about understanding customer specifics, not just about running vulnerability scanners. Every customer and technological process is unique, so we have researchers with specific expertise in different industry sectors – Oil&Gas, Power grids, Manufacturing and so on. Our experts undertake manual vulnerability searches, our ICS Cyber Emergency Response Team prepares an analysis of your specific regional/industry threat landscape, and we keep in touch with your IAVs regarding the status of your equipment.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com
Cyber Threats News:
www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize