Cybersecurity collaboration program for industrial laboratories and research communities

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Cybersecurity collaboration program for industrial laboratories and research communities

The number of cyberthreats to industrial enterprises grows each year. This includes the emergence of new types of threats, mass infections and targeted attacks. The ubiquitous digitization of industrial processes and integration of industrial systems and networks with external networks are opening up new avenues for unsanctioned interference with equipment handling critical industrial processes. This intrusion can in turn lead to a disruption of those industrial processes, financial and reputational losses, and severe ecological, social and macroeconomic implications.

The growth in threats is forcing governments, industry-focused organizations and industrial enterprises to develop requirements for industrial cybersecurity processes. Industrial enterprises, however, are often unprepared for the current threat landscape and do not have effective technologies or qualified personnel to tackle the threats.

Research laboratories and testing facilities are being established under the aegis of various organizations to resolve these issues of industrial cybersecurity. To support their efforts, Kaspersky has launched a program for collaboration with industrial laboratories.

Partner profile

The collaboration program applies to various types of organizations, including educational institutions, research departments at industrial companies, security operations centers (SOC) linked to cybersecurity service providers, emergency response teams (CERT and CSIRT), and numerous other entities that have laboratories, conduct research and train specialists.

The prerequisites for collaboration are:

1. Availability of, or plans to create, testbeds consisting of physical or virtual components used for modeling industrial processes in various sectors such as natural resource extraction, transportation and refinement of oil and gas, the energy and chemical industries, metallurgy, machine building, manufacturing, water supply, etc.

2. Availability of educational programs/modules on industrial cybersecurity or plans for research such as attack impact analysis, analysis of the effectiveness of cybersecurity and protection monitoring systems, vulnerability analysis, security policies and standards development, as well as the creation of a set of commercial cybersecurity systems.

3. Availability of a team or dedicated experts responsible for the operation, maintenance, and development of a laboratory.

Proposed technologies and expertise

To conduct training and research at the laboratories that meet the prerequisites of the program, Kaspersky is offering special conditions for the use of its specialized, advanced tools and expertise on ICS cybersecurity, including:

The benefits:

- ✓Holistic Endpoint Protection
- ✓Low impact on protected device
- ✓Centralized management

1. **Kaspersky Industrial CyberSecurity (KICS) for Nodes** – a solution designed to protect engineering and operator workstations, human-machine interfaces (HMI), and ICS/SCADA servers. It enables whitelisting, file integrity monitoring, peripheral device control, and malware detection and blocking.

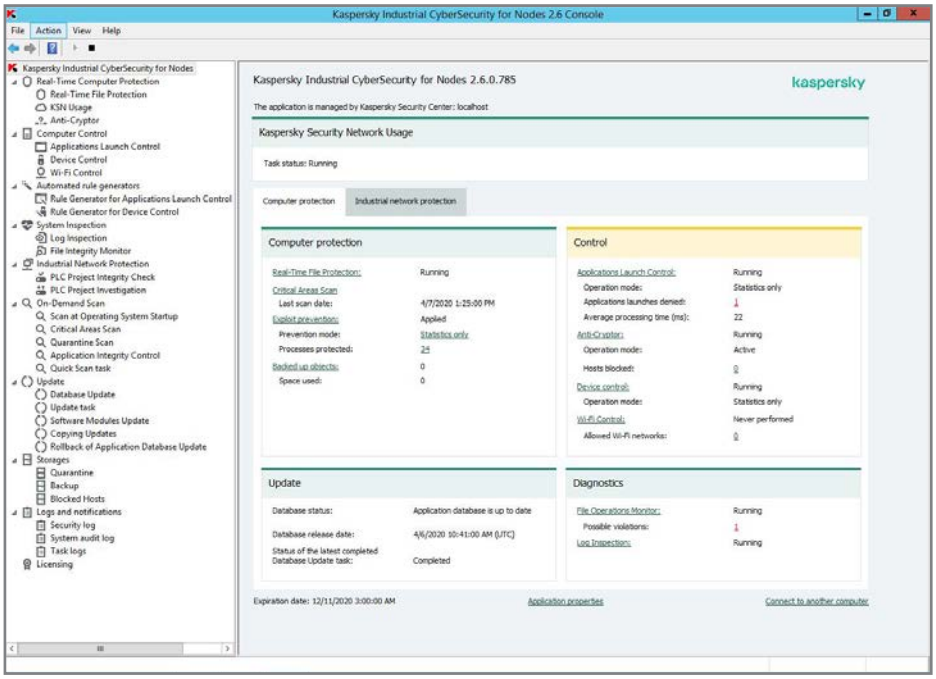

Image 1. KICS for Nodes interface

The benefits:

- ✓Asset inventory
- ✓Networks visualization
- ✓Early threat and anomaly detection
- ✓Process visibility and control
- ✓External integration

2. **Kaspersky Industrial CyberSecurity (KICS) for Networks** – a solution designed for passive devices and network communications inventory and visualization in an industrial network, as well as passive monitoring of attacks and anomalies in industrial network traffic, including inspection of industrial protocols (DPI) to control commands and technological process parameters.

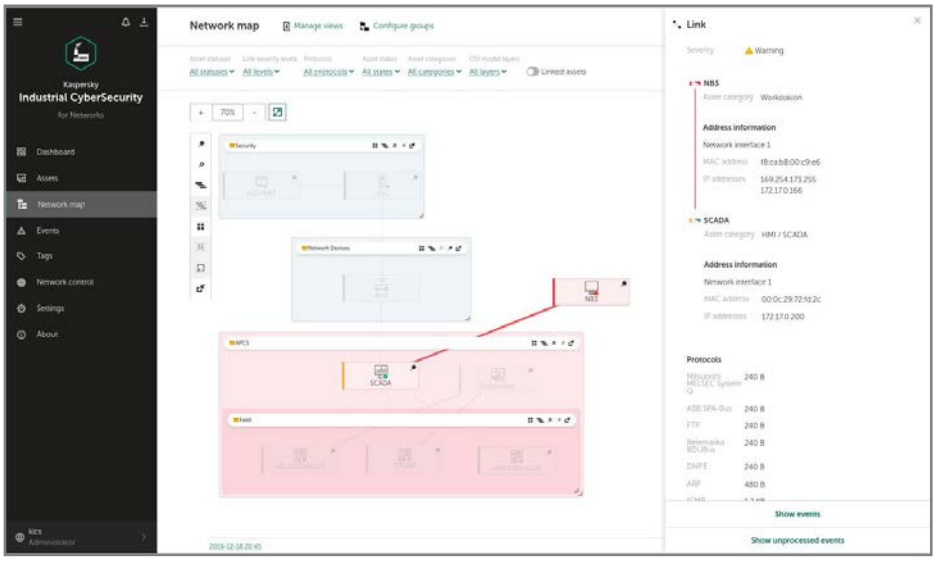

Image 2. KICS for Networks interface

The benefits:

- ✓ **Early process variables anomaly detection**
- ✓ **Process anomaly visualization and grouping**
- ✓ **Machine learning for process baselining**
- ✓ **Low human resources consumption**

3. **Machine Learning for Anomaly Detection (MLAD)** – a solution for detecting and interpreting anomalies in industrial telemetry at very early stages. The approach used can detect anomalies regardless of the underlying cause: cyberattack, human error or equipment failure. It automatically visualizes any process anomaly, connects machine-learning knowledge with expert knowledge and automatically groups similar anomalies. Expert recommendations for one anomaly can be used for a whole group of similar anomalies.

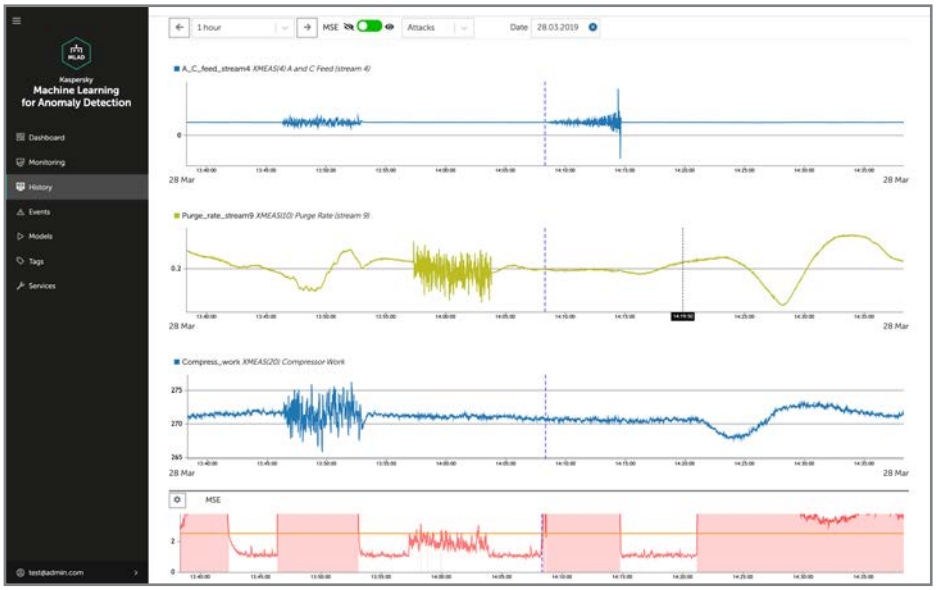

Image 3. Kaspersky MLAD interface

4. Consultative support from our experts on the creation of a laboratory environment, deployment and configuration of our tools, modeling of cyberattack scenarios, integration of solutions into SOC processes, and development of incident correlation rules.

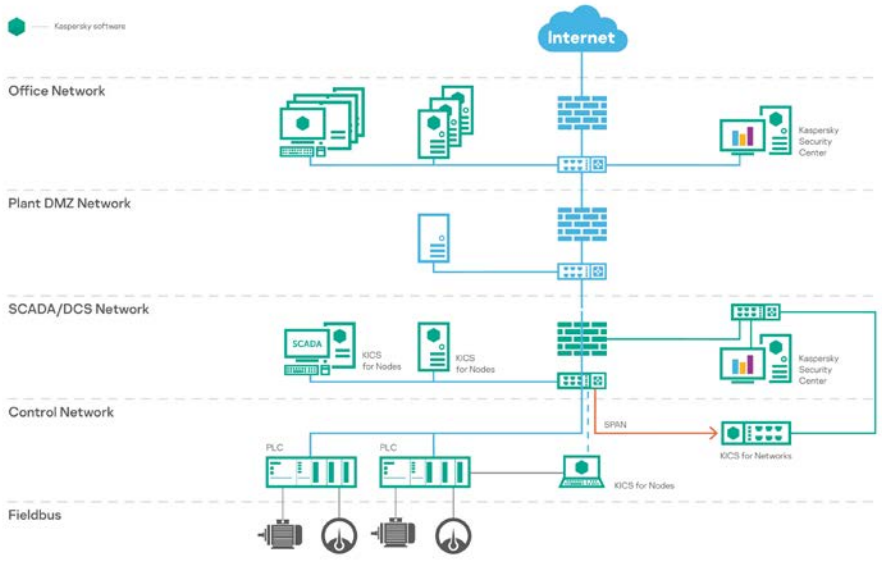

Image 4. Example of KICS component deployment for manufacturing

Our experience

Kaspersky already has experience of this kind of collaboration with a number of educational and research organizations, particularly in Russia (Gubkin Russian State University of Oil and Gas; Moscow Power Engineering Institute; Kazan State Power Engineering University; South Ural State University; and the Chuvash State University), Italy (smart polygeneration microgrid for the Savona Campus, University of Genoa) and Singapore (Security Showdown exercise 2017 and 2019 at the Singapore University of Technology and Design).

"The Chuvash State University is known for its scientific and research work in the field of power engineering, and most of the university graduates go on to work at the city's numerous electrical engineering enterprises. That's why our cooperation with Kaspersky, a company with such extensive experience in combating the most complex cyberthreats, is crucial for training highly qualified specialists whose activities will be inextricably linked with new technologies."

Andrey Alexandrov,
Rector of Chuvash State University

For example, the laboratory at the Chuvash State University hosts a Kaspersky research and development center for information security in the field of electric power. The center provides training for specialists and carries out scientific research into information security. This enables young specialists to access the most up-to-date information about cybersecurity methods that focus on the information infrastructure of critically important objects, particularly those involved in generating and distributing electricity.

In addition, we want to apply our own extensive experience of protecting real-world industrial facilities in various countries to this collaboration program. Some examples of our collaboration with industrial companies and industrial automation vendors are available here: public cases, certifications.

Our goals

By offering our technologies and expertise to industrial labs, we want to contribute to improving the knowledge and professional qualifications of industrial cybersecurity professionals, find ways to detect and block new attack vectors in various industrial segments, use the lessons learned to improve our own cybersecurity technologies, and take the opportunity to demonstrate our collaborative success to representatives of industrial enterprises, governments and the academic community.

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

All about ICS cybersecurity:
https://ics-cert.kaspersky.com

Cyber Threats News:
www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com

© 2020 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

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

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