kaspersky

Kaspersky Industrial CyberSecurity

Cybersecurity for Industrial Control Systems and critical industries

Oil & Gas

- Upstream
- Transportation
- Refinery
- Downstream

Energy

- Power Generation
- Power Distribution
- Smart Grids

Continuous Production

- Paper
- Construction materials

Chemistry

- Pharma
- Petrol-chemistry
- Chemistry

Metallurgy

- Steel production
- Aluminum

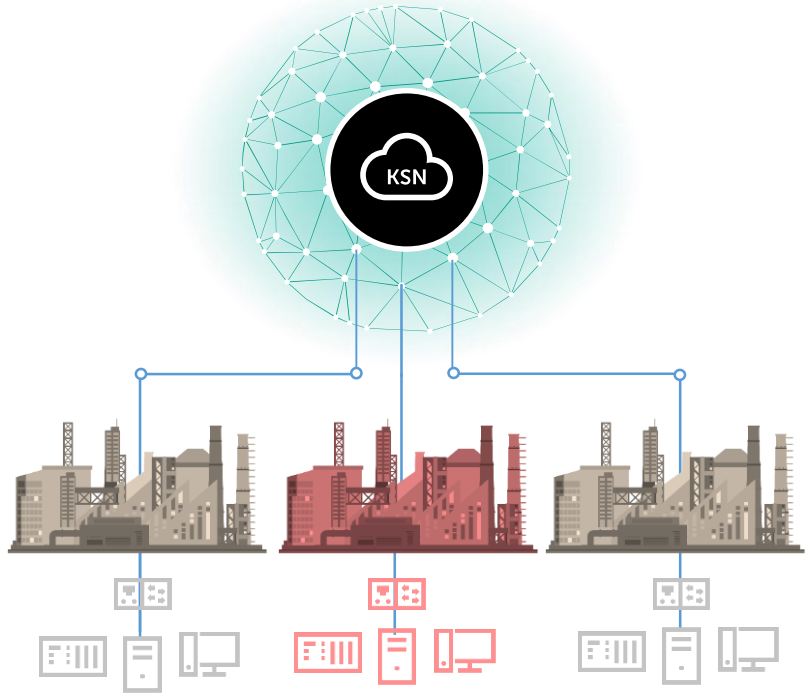
Industrial OT infrastructures now face modern cybersecurity threats

due to a growing connectivity to corporate networks

KASPERSKY LAB
ICS CERT

Monitors cybersecurity of

100 000 industrial nodes worldwide*



In 2018, almost every second (47.2%) ICS computer system had been infected by malware

180+ ICS / IIoT vulnerabilities found and reported since 2016

* According to Kaspersky Security Network

Typical “corporate” cybersecurity approaches don’t work for ICS

MISUSE OF A CORPORATE CYBERSECURITY SOLUTIONS:

High consumption of protected system’s resources lead to its failure

Proactive protection technologies often lead to false positives and failure

Specific industrial network protocols are easily hacked by undiscoverable by corporate IDS

TYPICAL SOLUTION

Fine tuning of corporate cybersecurity products to avoid negative impact on protected ICS

- Manual installation
- Creating lists of exclusions
- Disabling security components

TOO COMPLEX TO MAINTAIN

LEADS TO A SECURITY GAPS

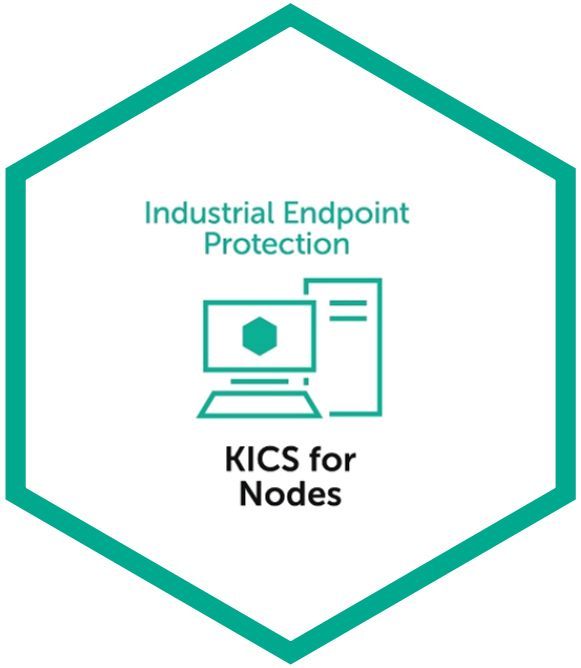
What does Kaspersky Industrial CyberSecurity offer?

KICS - is a holistic ICS Cybersecurity solution designed to:

- ✓ Provide hi-end level of cybersecurity for industrial nodes and networks out of the box
- ✓ Avoid false positives and harmful impact on protected ICS

Our holistic approach

KICS for Nodes: use cases and features



- ✓ SCADA/DCS Servers
- ✓ HMIs
- ✓ Workstations

PREVENT LAUNCH OF ANY UNWANTED APPLICATIONS

- Control which applications can start on each node
- Default Deny TEST & RULE environment
- Protects against Targeted attacks
- Protects against malevolent user activity

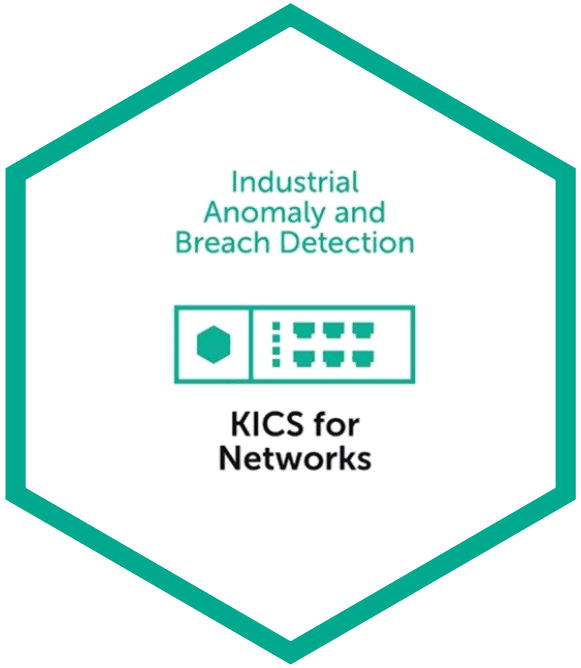
DETECT MALWARE WITHOUGHT NEGAITVE IMPACT ON THE ICS

- Multi-Process Anti-Malware Engine with the limitation on resource consumption
- Non-Intrusive architecture
- Anti-Cryptor
- OS Log Inspection

CONTROL INFORMATIONAL ENVIROMENT

- Device Control
- Wi-Fi connections control
- File Integrity Control

KICS for Networks: use cases and features



✓ Network equipment
✓ PLCs

DISCOVER ASSETS and MAINTAIN NETWORK INTEG

- Passive network devices and communications discovery
- Network map visualisation
- Communications whitelisting

MANAGE SECURITY EVENTS

- Display important events
- Correlate events into Incidents
- Manage event history

INTEGRATE ICS and CORP CYBERSECURITY

- Kaspersky Security Center
- Syslog Server
- SIEM

MONITOR TECHNOLOGY PROCESS

- Analyze the industrial process parameters
- Detect malicious modifications

MONITOR PLC COMMAND PROCESSING

- Configure system reaction to potentially dangerous PLC commands
- KICS for network alerts on: Authentication, start/stop PLC, read/write PLC, read/write PLC configuration, etc

Our Values

- Preventing the risks of technology process breakdown due to a malware actions on endpoints (WannaCry, ExPetr, StoneDrill)
- Early detection of APT and ability to react and prevent technology process breakdown
- Technical solution to monitor the actions of engineering staff an 3rd party advisories
- Cutting the costs on integration and maintenance of ICS Cybersecurity solutions
- Wide range of Services to boost up awareness and expertise in ICS Cybersecurity

kaspersky

Bring On The Future

kaspersky.com