

TERMS AND CONDITIONS

KASPERSKY ICS THREAT INTELLIGENCE REPORTING

WHEREAS, the Customer, being a legal entity named in the corresponding order ("Customer") wishes to use the Kaspersky Industrial Control System Threat Intelligence Reporting ("ICS Threat Intelligence Reporting" or "Product") of AO Kaspersky Lab ("Kaspersky") and Kaspersky wishes to provide the Product to the Customer;

NOW THEREFORE, in consideration of the mutual covenants and promises in these Terms and Conditions ("T&C") and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and by Customer purchasing access to the Product in accordance with the related ordering process and by clicking the appropriate button(s) if required by Kaspersky to confirm and accept this T&C (which to the maximum extent permitted under applicable law shall be deemed conclusive approval thereof), the parties agree as follows:

Kaspersky agrees to grant access to the Product in the manner and within the time period in accordance with this T&C, purchase order, placed by an authorized partner of Kaspersky ("Partner"), and/or and a separate agreement that may be entered into between Kaspersky and Customer. To the extent a separate agreement between Kaspersky or a Partner and Customer conflicts with any provisions of the T&C, such separate agreement shall prevail.

1. DESCRIPTION

Background

Kaspersky ICS Threat Intelligence Reporting provides Customer with heightened intelligence and awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in most popular industrial control systems and underlying technologies.

In addition to using the reports to identify, detect and mitigate risks posed by new attack techniques, tactics and procedures, recently discovered vulnerabilities and other important changes to the threat landscape, many organizations leverage the reports for private research purposes, to detect the reported threats, to further enhance their security strategy and to make informed decisions related to hardening their industrial infrastructure. Software and hardware vendors may also find this information useful for planning and designing changes that enhance the security of their products.

Kaspersky provides early notification reports on:

- ▶ new APT and attack campaigns targeting industrial organizations, as well as updates on active threats;
- ▶ significant changes to the threat landscape for industrial control systems, newly discovered important factors that affect the ICS security level and ICS exposure to various threats, including regional, country- and industry-specific information;
- ▶ vulnerabilities identified by Kaspersky in the most popular products used in industrial control systems, the industrial internet of things, and infrastructures in various industries across the globe.

Benefits

- ▶ **Exclusive access** to technical descriptions of the latest threats during ongoing investigations, before the relevant information is publicly released; technical description of publically

known vulnerabilities and vulnerabilities discovered by Kaspersky in industrial soft- and hardware, recommended mitigation measures

- ▶ **Quick start:** no additional infrastructure is required to start using the Product. Reports are delivered via the Portal (as defined below).
- ▶ **Technical support for investigations:** product subscription includes access to technical artifacts supporting investigations, such as indicators of compromise (“IoC”), as well as malware detection and classification rules if available.
- ▶ **Technical support for cybersecurity risk assessment:** product subscription includes access to technical artefacts supporting more precise vulnerability identification and assessment, such as intrusion detection rules.
- ▶ **Retrospective analysis:** access to all previously issued reports is provided during the subscription period.
- ▶ **Continuous malicious campaign monitoring:** access to actionable intelligence during the investigation (information on campaign distribution, IOCs, C&C infrastructure, etc.).
- ▶ **Early response to emerging threats:** information and tools provided in the reports make it possible to quickly respond to new threats and vulnerabilities, to block attacks via known vectors and to reduce the damage caused by advanced attacks.

The Product includes the following information¹:

- ▶ Executive summary
- ▶ For reports on threats:
 - Threat severity assessment
 - Threat description
 - Timeline
 - Distribution across regions, countries and industries
 - Recommendations on risk mitigation
 - Attack methods
 - Exploits used (if any)
 - Malware description(s)
 - C&C infrastructure and protocol descriptions
 - Victim analysis
 - Data exfiltration analysis
 - Attribution
- ▶ For reports on vulnerabilities:
 - Vulnerability severity assessment
 - Vulnerability description
 - Timeline
 - Distribution across regions, countries and industries
 - Recommendations on risk mitigation
 - Public availability of exploits
 - Signs of exploitation in real-world attacks
 - Methodology used to identify the vulnerability
 - Technical analysis of security issues that made exploiting the vulnerability possible

¹ The availability and relevance of information may vary

- Possible attack vectors (possibly in conjunction with other vulnerabilities and security flaws)
- Information on products / product versions affected
- Estimates of vulnerable product distribution across regions / countries / industries
- Recommended mitigation measures including Suricata/Snort rules and OVAL definitions
- For publically known vulnerabilities, validation of the initial vulnerability assessment provided by the vendor of the affected products.

► Conclusions

► Appendix

- Technical analysis, IOCs, C&C, hashes, and any other available information

Product Options

Product License (as defined below) may be purchased for 1, 2 or 3 years, and allows access to the complete ICS threat intelligence reporting database.

Available options are as follows: full access to database of reports including MRTI data, or limited option including access to executive summaries of the reports and reports MRTI.

The Product option prices shall be indicated in Kaspersky's price list in effect at the time of order placement, which the Customer declares to know and accept; the current price list shall supersede all previous lists.

In accordance with this T&C Kaspersky provides the option indicated in a license certificate furnished by Kaspersky after the relevant order is placed ("Certificate").

2. PROVISION

2.1. License. Kaspersky grants the Customer a non-exclusive, non-transferable limited license to access the Kaspersky threat intelligence reporting database and software allowing to get access to ICS Threat Intelligence Reporting or download reports in PDF format, IOC's in openIOC format solely for Customer's internal business purposes and Customer accepts this license ("License").

2.2. Access to Product. The Product is provided by means of granting access to a web-based portal ("Portal") or via restful API. Customer credentials and digital certificate for Portal access are delivered via encrypted email communication to the email address specified by Customer within five (5) working days from the date of the Certificate.

2.3. Term. The term of License equals the term of the relevant Product option indicated in the Certificate. This T&C shall commence on the effective date, which is the date of acceptance of this T&C by Customer.

2.4. Compensation. License fees and all applicable taxes payable are due within the period specified in an invoice provided to Customer by Kaspersky or a Partner.

2.5. Cooperation. Customer shall provide information as may be reasonably required by Kaspersky in order to permit Kaspersky to perform its obligations hereunder. Kaspersky will not be liable therefor if the required information is not provided to Kaspersky by the Customer or is inaccurate, and/or inadequate for provision of the Product.

2.6. Technical Support.

- ▶ Kaspersky shall provide Customer with Technical Support, which includes resolution of Customer problems related to the Product purchased and being utilized properly according to its intended use and in compliance with the documentation and technical specifications.
- ▶ Customer shall provide as much detailed information as possible to help Kaspersky Technical Support to achieve a resolution to the problem or to enable Kaspersky to correct any issues in the Product and/or further develop the Product as may be required by Kaspersky .

2.7. Warranties. EXCEPT FOR KASPERSKY OBLIGATIONS STATED HEREBY THE PRODUCT IS PROVIDED "AS IS" AND KASPESKY MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW. KASPERSKY AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. CUSTOMER ASSUMES ALL RESPONSIBILITY, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE PRODUCT TO ACHIEVE CUSTOMER INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE PRODUCT. WITHOUT LIMITING THE FOREGOING PROVISIONS, KASPERSKY MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE PRODUCT WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE PRODUCT WILL MEET ANY OR ALL OF CUSTOMER REQUIREMENTS WHETHER OR NOT DISCLOSED TO KASPERSKY .

2.8. Intellectual Property Ownership. Customer consents and agrees that the Product and the authorship, systems, ideas, methods of operation, documentation and other information contained in or relating to the Product are proprietary intellectual property and/or valuable trade secrets of Kaspersky or its Partners and that Kaspersky and its Partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patents of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This T&C does not grant the Customer any rights to the intellectual property, including any trademarks or service marks of Kaspersky and/or its Partners ("Trademarks"). Customer may use the Trademarks only insofar as to identify printed output produced by the Product in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give to the Customer any rights of ownership in that Trademark. Kaspersky and/or its Partners own and retain all right, title, and interest in and to the Product, including without limitation any error corrections, enhancements, updates or other modifications to the Product, whether made by Kaspersky or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Customer's possession, or use of the Product does not transfer to the Customer any title to the intellectual property in the Product, and Customer will not acquire any rights to the Product except as expressly set forth in this T&C. All copies of the Product made hereunder must contain the same proprietary notices that appear on and in the Product. Except as stated herein, this T&C does not grant the Customer any intellectual property rights in the Product and Customer acknowledges that the License, as defined herein, granted under this T&C only provides the Customer with a right of limited use under this T&C. Kaspersky reserves all rights not expressly granted to the Customer in this T&C. VIOLATION OF THE INTELLECTUAL PROPERTY RIGHTS TO THE PRODUCT SHALL RESULT IN CIVIL, ADMINISTRATIVE OR CRIMINAL LIABILITY IN ACCORDANCE WITH THE LAW.

2.9. Any pre-existing proprietary or Confidential Information of Kaspersky used to create the Product, or included into the results or deliverables of the Product provision, including but not

limited to software, appliances, methodologies, code, templates, tools, policies, records, working papers, know-how, data or other intellectual property, written or otherwise, shall remain Kaspersky exclusive property.

3. USE

3.1. Customer may use the Product to protect its own infrastructure and its own employees only upon acceptance of this T&C and as long as the License remains in effect.

3.2. Customer acknowledges that Kaspersky provides the same or similar Product to other customers and that nothing in the T&C shall be construed to prevent Kaspersky from carrying on such business. Customer acknowledges that Kaspersky may at its sole discretion develop, use, market, and distribute any components that are substantially similar to components of the Product with similar or other structure, content and organization. Notwithstanding the preceding sentence, Kaspersky agrees that it will not market or distribute any Product components that include confidential information of the Customer.

3.3. Customer may not distribute, transfer or resell the Product and/or its components. Providing the Product and/or its components to third parties regardless of whether they are provided on a commercial or free basis is strictly prohibited and considered as significant harm to Kaspersky. In the event that Customer violates the restrictions indicated herein Kaspersky shall be entitled to charge compensation which may include direct damages as well as loss of profit and any supplementary expenses which may be suffered by Kaspersky subject to such violation and Customer hereby agrees that payment of such compensation shall not be withheld.

3.4. Customer shall not emulate, clone, modify, decompile, or reverse engineer the Product or its components. Customer shall not sell, rent, lease or lend the Product or its components to any third party or use the Product to create own product or service used for detection, blocking or treating threats or any other purpose.

3.5. Customer may not remove or alter any copyright notices or other proprietary notices of the Product, related documentation or materials.

3.6. Due to the sensitive nature of some of the information contained in the reports, Kaspersky limits the Product to trusted government, public and private organizations. Restrictions on information reuse enforced.

3.7. All the information provided subject of the Product shall be properly marked according to the Traffic Light Protocol (TLP) (<https://www.us-cert.gov/tlp>), and Customer hereby agrees to honor the protocol.

For Product deliverables without a TLP but being part of the same publication, the TLP of the report is applicable to all the deliverables.

3.8. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL KASPERSKY BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER PRODUCTS, INFORMATION, SERVICE AND RELATED CONTENT THROUGH THE PRODUCT OR

OTHERWISE ARISING OUT OF THE USE OF THE PRODUCT, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS T&C, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF KASPERSKY, EVEN IF KASPERSKY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.9. If Customer violates any of its obligations hereunder or License limitations stipulated in this T&C or other legally binding document entered into between Kaspersky or a Partner and Customer, Kaspersky may revoke the License and terminate the Customer's access to the Portal.

3.10. Kaspersky reserves the right at any time to improve the Product and/or its components in its sole discretion.

3.11. Kaspersky reserves the right at any time to modify this T&C and to impose new or additional terms or conditions on the use of the Product. Such modifications will be effective immediately when incorporated into the T&C. Continued use of the Product by Customer will be deemed acceptance thereof.

3.12. No delay or omission by either party in exercising any right under this T&C shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of this T&C shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This T&C may also be amended or modified by a written instrument executed by both the Customer and Kaspersky or by Kaspersky only as stipulated in clause 3.11.

3.13. All disputes arising out of or in connection with this T&C, including any question regarding its existence, validity or termination, shall be referred to and finally settled under the Rules of Arbitration of the International Chamber of Commerce, which Rules are deemed to be incorporated by reference into this section. The number of arbitrators shall be three. The seat of arbitration shall be London, England. The procedural law of this place shall apply where the Rules are silent. The language to be used in the arbitration proceeding shall be English. The governing law of this T&C shall be the substantive law of England and Wales.

This T&C shall be binding upon, and inure to the benefit of, both parties and their respective successors and assigns.