kaspersky

Kaspersky Maintenance Service Agreement for Threat Intelligence

kaspersky

1. General terms and conditions

Herein is given a list of service requests, in relation to which Kaspersky will provide assistance to the owner of the Extended Technical Support Certificate of Maintenance Service Agreement (MSA) for the Kaspersky Threat Intelligence (TI) product line.

2. Definitions

"Company Account" shall mean web-based Kaspersky Technical Support request processing system

"Product(s)" shall mean subscription product(s) of Kaspersky Threat Intelligence products family, which the Customer has purchased, in accordance with the terms of a License Agreement between Kaspersky and the Customer, and for which the Customer has concluded a License Agreement.

"End User", **"User"**, **"Customer", (You / Your)** shall mean an organization, which has a functioning license to the Product that is supported in accordance with to this Program.

"Incident" shall mean any event reported by the Customer, which is not part of the standard operation of a Product and which causes, or may cause, an interruption to, or a reduction in, the quality of service provided by the Product.

"Local Time" shall mean the time zone of the Kaspersky Local Office

"Problem" shall mean an unknown underlying cause of one or more Incidents. It becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

"Known Error" shall mean a Problem that becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

"Product Error" shall mean undeclared behavior of the Product.

"Service Request" shall mean a request from a Customer for support, delivery, information, advice or documentation, which is not related to an incorrect functioning or non-functioning of the Product(s).

"Virus Outbreak" shall mean a Customer crisis situation, where a virus undetected by the Product(s) with the latest antivirus bases and executable modules is affecting technology process continuity and/or a large number of Customer's end- users. Virus Outbreak is a product-related Incident.

"Malware-related Incident / Virus Incident" shall mean not product-related Incident, requiring Kaspersky to provide recommendations on particular malware removal, and/or malware descriptions, and/or special malware removal tools.

"Incident Severity/Urgency" shall mean a measure of the business criticality of an incident or problem based on the business needs of the Customer.

"Response time" shall mean the elapsed time measured from the moment of any incident receipt until qualified answer to the initiator (via support system, email or phone).

"Update" shall mean Kaspersky-issued anti-virus databases with new virus signatures or modification of the Product's executable modules, which enhances its performance and/or expands its functionality.

"Upgrade" shall mean a Product update associated with assigning a new version number.

"Workaround" shall mean a procedure that may serve as a temporary solution to an incident.

"False Alarm", **"False Positive"** shall mean a situation when the Product erroneously detects a safe file as an infected one.

kaspersky

1. Description of MSA for TI support program

Service requests relating to product operations as well as acceptance of post- incident maintenance requests are implemented by the means of:

- Kaspersky Support web portal with acceptance of requests 24 hours a day, 365 days a year
- Priority telephone line during business hours.
- Email (only when having issues accessing Company Account), acceptance of requests 24 hours a day, 365 days a year
- Assigned Security Account Manager (SAM), 24 hours a day, 365 days a year.

Incident processing

Processing incidents via Company Account web portal

Web-based Kaspersky Technical Support request processing system is available at: https://companyaccount.kaspersky.com

By the means of this system, the Customer can take advantage of:

- access to personal account in order to create, update and monitor incidents;
- technical support and consulting in relation to incidents that may occur during Product installation, configuration and functioning;

Processing incidents by phone

Technical Support by phone is only available to the authorized contact persons of the Customer.

Response time

Kaspersky guarantees a 4 (four) hours response time. Phone call is required during out of business hours incl. weekends and holidays.

Requests from the customers, who owns the MSA for TI certificate, are assigned with higher priority compared to requests from other customers.

Incident resolution control

At any moment, an incident can be either on the Customer's side (i.e. Customer is taking actions that will promote/expedite the resolution of the issue by Kaspersky) or on Kaspersky side.

An incident is on the Customer's side when Kaspersky requests information from the Customer. When Customer provides the requested information to Kaspersky, the Incident is considered to be on the side of the latter. The period during which the incident may be on the Customer's side, is limited to 1 month. In case the Customer's response is overdue, the incident is closed by timeout.

Kaspersky is only responsible for the time during which the incident is on their side.

Dedicated Security Account Manager (SAM)

The Security Account Manager (SAM) is an employee of Kaspersky, which is assigned to a particular customer with the purpose of maintaining an integrated channel of communication. The SAM manages processing of all customer incidents. The responsibilities of the Security Account Manager are determined as follows:

- organizing communication for processing incidents by Kaspersky technical teams;

- notifying the Customer of the current status of incidents; providing quarterly reports;
- supervising the progress of tasks related to Customer requests and implementing timely escalations when processing requests;
- support of the Customer's IT department in relation to recommendations and instructions given by Kaspersky specialists for Kaspersky products;
- analytical working cooperation with the Customer in order to resolve current technical and operational incidents.
- communicating proactively with the Customer on a regular basis to maintain an open line of communication and ensure satisfactory operation of the Kaspersky TI products.
- informing Customer about new versions released by Kaspersky and discussing the conditions of additional services included into the MSA for TI program

The SAM is accessible during business working hours of local office by landline phone, by cellular phone and by email. If the SAM is unavailable (Outside of normal business hours including weekends), the Customer's requests are directed to the manager-on-duty on the MSA Technical Support line.

Business working hours may vary depending on the region; check your Kaspersky Maintenance Service Agreement certificate for details.

The Customer assigns contact persons (in accordance to Additional terms of support) for communication with Kaspersky, and shares with the latter his or her contact details (email, telephone number and others if available) for consistent and efficient collaboration in connection with incident resolution.

Quality management

The Customer may escalate unresolved incidents in case it is currently on the Kaspersky side.

Escalations concerning quality of technical support are accepted according to the following scheme:

Escalation level	1	2	3
	Security Account Manager	Head of support team, Kaspersky Regional office	Business Account Manager (Business Contact)

Scope of the service

The following services and actions are included into MSA for TI to ensure the maximum benefit from the service and to provide it with the highest quality.

CyberTrace Installation

The Customer may request the installation of the Kaspersky CyberTrace once a year.

During this service, the SAM will remotely guide the Customer through the installation of Kaspersky CyberTrace with the following conditions:

- Installation can be performed on a Windows or Linux operating system that meets CyberTrace's hardware and software requirements and can receive events from an event source determined by the Customer, such as a Customer's SIEM solution.
- Installation can be done according to the integration scheme of CyberTrace and the Customer's SIEM assuming it is supported (integration scheme is part of CyberTrace documentation).
- The Customer should ensure the availability of the infrastructure and possibility to install Kaspersky CyberTrace according to the integration scheme. For example, if Kaspersky CyberTrace and a SIEM solution are to be installed on separate computers, the Customer should check the available integration schemes for their SIEM solution to decide where to install Kaspersky CyberTrace.

SAM will also assist in the Post-installation configuration (Initial Setup Wizard) to complete the configuration.

kaspersky

Post-installation configuration may also include the following:

- Licensing configuration
- Feeds selection

SIEM (Log Source) Integration

Kaspersky will provide remote assistance of Kaspersky CyberTrace integration with Customer's event source. The service is limited up to 3 (three) log sources and consists of the following:

- assistance in configuring the event source (SIEM) to send events to Kaspersky CyberTrace and receive detection events from Kaspersky CyberTrace.
- installation of the specific Kaspersky applications and tools depending on the selected SIEM at customer's discretion.
- assistance in the modification of the regular expressions in Kaspersky CyberTrace to parse incoming events processed by normalizing rules and extract information to be checked in feeds and to be used in outgoing events.
- verification test (SIEM and\or non-SIEM solutions) to ensure whether Kaspersky CyberTrace is integrated correctly with the event target software.

Onboarding session and Value demonstration

Once a year Customer may request a remote onboarding session and ask to demonstrate the value of Kaspersky TI products. The session duration can be not long than 1 (one) working day and it can be provided to up to 10 people from Customer's employees.
During onboarding session, SAM reviews the Customer's Threat Intelligence Portal and CyberTrace utility, demonstrates best practices, and shows how to maximize the tools for research. The session may include the following areas:

Threat Intelligence Portal (TIP)	CyberTrace

• TIP Documentation.
• TIP (Research Tool) overview.
  ○ Home Statistics
  ▪ Worldwide
  ▪ Events list
  ○ APT Reporting
  ▪ Reports
  • YARA Rule
  • IOC
  ▪ Actor Profiles
  ▪ APT Associated IP addresses
  ○ Financial Reporting
  ○ Industry Controls (ICS) Reporting
  ○ Threat Lookup
  ▪ WHOIS Lookup
  ▪ WHOIS Hunting
  ○ Cloud Sandbox
  ○ Digital Footprint
  ○ Data Feeds
  ▪ Tools
  ▪ What the feeds look like
	• Data Feeds
	  ○ Tools
	  ○ What the feeds look like
	• CyberTrace Documentation
	• Dashboard
	  ○ Statistics overview
	  ○ Feed statistics
	  ○ Indicator statistics
	• Search
	  ○ Indicator
	  ○ Log file
	  ○ File
	• Settings
	  ○ Service
	  ○ Feeds
	  ○ Matching (Event sources)
	  ○ Event format
	  ○ Logging
	  ○ Users
	  ○ Licensing

Assessment & Health Check

Customer is entitled to request a service of Assessment and Health Check of his infrastructure and current setting of log-source. This service can be demanded once a year and not earlier than 90 (ninety) days from the particular

usage of Kaspersky TI products. The service is delivered remotely, the duration is no longer than 3 (three) days and includes the following:

- review of Customer's environment and log-sources.
- analysis if current feeds are sufficient/appropriate and aligned with the Customer's business objectives

The recommendations on how to configure the settings may be provided if it is needed.
In case the service can't be delivered remotely the separate Professional Services should be purchased additionally.

CyberTrace Tuning

Customer is entitled to ask for Kaspersky CyberTrace tuning service. It can be performed twice a year by demand of the Customer. During the tuning process, the SAM will:

- Perform tuning and configuration of regular expressions in CyberTrace where additional data from original event can be extracted and inserted to detection event – such as source/destination IP/port, username, hostname etc.)
- Guide modification of event formatting in CyberTrace.

Upgrades

The Customer has the possibility to upgrade Kaspersky TI products to the latest versions. The SAM will remotely guide the Customer through the upgrade process when new versions are released. Customer should ensure the availability of infrastructure necessary for upgrade including backup of current version and data.

Additional terms of support

The Customer can assign up to 4 (four) contact persons authorized to initiate requests to Kaspersky Technical Support. A list of authorized contact persons should be defined at time of support activation. To change a list of authorized contact persons the Customer should send a written request via Company Account.

The Customer can register an unlimited number of incidents.

The Customer should provide Kaspersky with all information necessary and specific software or hardware, which may be necessary for reproducing the condition under which the incident will re-occur and could be examined. This may be needed if Kaspersky does not have the necessary software or hardware available.

If the incident could not be reproduced, the Customer should grant to Kaspersky specialists supervised remote access to the malfunctioning system.

If the incident cannot be reproduced by either party, or the Customer did not grant access to the network environment where the incident could be reproduced, or if it is detected that the incident's cause lies beyond the Product, the incident cannot be classified within this Support Program.

Limitations of technical support program

MSA for TI support program does not include the following:

- Development of new product functionality at the request of a User
- Improvement of the performance and configuration of a User's device
- Disinfection of computers that are infected with malware (including mitigation of the effects of infection)
- Questions regarding third-party apps and/or operating systems
- Deployment and configuration of third-party SIEM systems and security controls
- Use of third-party patches for operating systems and applications to fix vulnerabilities
- Advice on configuring network security in general
- Liability to Kaspersky from correct or incorrect processing of recommendations
- Incidents already resolved for the Customer (i.e. incident that occurred on one installed copy of the Product after the same incident had been resolved for another copy of the Product);
- Troubleshooting of all issues similar or identical to already resolved issues (i.e. the incidents to which a previously produced solution can be applied without additional guidance from Kaspersky);

- Incidents caused by Customer's hardware malfunction;
- Incidents caused by software platform incompatibility (including, but not limited to beta software, new versions of service packs or additions, whose compatibility with the Product has not been confirmed by Kaspersky);
- Incidents caused by installing and running third-party applications (including, but not limited to the list of unsupported or incompatible applications published in the documentation);
- Incidents for which the Customer cannot provide accurate information, as reasonably requested by Kaspersky, in order to reproduce, investigate, and resolve the incident;
- Incidents which arise as a result of neglect or incorrect use of Kaspersky instructions, which, if properly used, would have obviously prevented the incident.

Some services that are not included in support program may be offered as individual paid services.

Technical support program shall not be implemented in case of the following incidents;

- troubleshooting of all issues similar or identical to already resolved issues (i.e. the incidents to which a previously produced solution can be applied without additional guidance from Kaspersky);
- incidents caused by Customer's hardware malfunction;
- incidents caused by software platform incompatibility (including, but not limited to beta software, new versions of service packs or additions, whose compatibility with the Product has not been confirmed by Kaspersky);
- incidents which arise on Product out of the Standard Support phase;
- incidents caused by installing and running third-party applications (including, but not limited to the list of unsupported or incompatible applications published in the documentation);
- incidents for which the Customer cannot provide accurate information, as reasonably requested by Kaspersky, in order to reproduce, investigate, and resolve the incident;

www.kaspersky.com/
www.securelist.com