Trellix (former FireEye) & Nozomi Services powered by IKARUS

Service Description

Version: 1.0

Date: 30.05.2023

Content

1.   General

Technical support is provided by the company IKARUS Security Software GmbH (IKARUS). This document describes the services that are included in the purchase price. Further services can be ordered optionally and are listed as examples in point 3.

The technicians employed by IKARUS are 3rd level technicians certified by the respective manufacturer. The service is available in German and English.

2.   Content of the Standard Service

IKARUS supports end customers during commissioning and during operational management of the respective Trellix/Nozomi solution to the extent described in 2.1.

In addition, IKARUS operates a Trellix data center environment hosted in Vienna, which is used by some of the offered services or Trellix products, or which requires access to the IKARUS data center for promised functions..

2.1   Installation Support (Onboarding, Setup)

Support requests can be sent to the email address mailto:managed.defense@ikarus.at . Questions will be answered either by phone or by email within IKARUS business hours (see www.ikarus.at) within 3 working days.

- Contacting the customer's point of contact for planning the installation.
- Explanation of the application including administration interface.
- Explanation and example: Basic instructions for rollout and commissioning.
- Explanation and recommendations for action for the configuration of the products.
- Training on how to use the products against cyber threats & potential infections.
- Explanation: Recommendations for action for device monitoring of the products.
- Initial configuration of the hardware that was ordered (software update, setting the basic configuration) and shipment to the customer.

2.2   Support during operational management

- Communication about new releases and their functions via a defined customer mail address.
- Delivery of replacement hardware in case of hardware defects within the warranty or purchased hardware maintenance. Service level: Best Effort, usually 48h on weekdays - depending on availability and access to the appliance, e.g. influence of customs delay.
- Correction of problems caused by central services from the IKARUS data center.

2.3   Requirements for the standard service

- Customer's participation in the planning and organization of IKARUS support services.
- The customer has made an appointment to provide the service.

- The necessary system requirements (hardware and software 3rd party) for the respective service have been checked by the customer and are fulfilled.

- Remote access to the user's computer is fully possible if necessary (an up to date Internet connection with sufficient bandwidth).

- At least one license was purchased by the customer.

- All necessary user account information and passwords are available.

- There is access to the IKARUS Service Account, which was previously stored by default in the customer's purchased system. This extended service access can be deactivated at the express request of the customer. This means that support and SLAs can only be fulfilled to a limited extent.

- IKARUS 3rd level technicians communicate exclusively with technical IT personnel of the customer. If Customer does not have its own technical IT personnel, Customer's main technical contact person shall be considered the main contact person for IKARUS.

2.4. Features not included in the standard service

- The complete commissioning (roll-out/onboarding) is the responsibility of the custome.

- All main functions and the most important configurations are shown or trained as an example. The creation or configuration of additional settings, such as the roll-out of additional clients or rules, the integration of further end devices or similar, are not included.

- On-site support at the customer. The service is provided via remote maintenance by appointment. On-site appointments will be made by IKARUS at its own discretion and only in exceptional cases.

- If viruses, malware, or similar threats are already present on Customer's hardware, even if they are detected only after activation of the purchased / tested IKARUS Services, cleaning of Customer's system from viruses and similar threats is not included in the price.

- Configuration/modification, etc. of third-party hardware or software.

- Creation of reports or statistics.

- Maintenance of Trellix and Nozomi hardware used at a customer site.

- Installation of spare parts for hardware used at a customer site.

- Patching, upgrading or updating software installed at the customer site.

3. Optional, fee-based additional services

If after four contact attempts by IKARUS (3 x by phone, then by email) and the expiration of a period of 10 working days, no customer reaction is received, IKARUS will send the standard installation descriptions. In this case, IKARUS reserves the right to provide further support services at a charge.

Additional, individual services can be put together and adapted to customer requirements. These include among others:

- Individual service number for end customers for direct telephone contact to IKARUS 3rd level support technicians.

- Extended support hours up to 24/7 service

- Takeover of responsibilities of the customer by IKARUS up to the complete outsourcing of all operational tasks of the Trellix and Nozomi products.

- Creation of reports, catalog of measures, best practices, dashboards, custom queries, enterprise search, configurations, integration of additional hardware/endpoints, network architecture support.

- Recommendations for 3rd party hardware/software purchases and integration support

- Maintenance of the hardware and software of the purchased appliances.

- Handling and purchase of Trellix Mandiant Services (Expertise on Demand) for all Trellix and Nozomi services used.

- Tuning of parameters for the installation
  (Data Acquisition Planning - positioning of hardware/software appliances (Network Security, Endpoint Security, E-Mail Security - On-Prem, Cloud, Trellix Cloud - Helix), 3rd Party Data Sources, Scoping Guide, network addresses, Mirror-Port/SPAN/TAP, access, maintenance access, support with triage catalogue (definition of network areas, responsibilities, contact persons))

- Support for software problems that arise in the course of the operation.

4.   Reaction times for dusruptions affecting the IKARUS data center

Error class 1	Critical error	Critical major service failure that causes the service to be completely interrupted.	95% of all reported faults are rectified within two hours during business hours..
Error class 2	Substantial error	Substantial loss of service that causes massive disruption or delay to the service.	85% of all reported faults are rectified within four hours during business hours.
Error class 3	Medium error	Standard service failure with no or insignificant impact on email scanning and forwarding	75% of all service failures are repaired within eight hours during business hours.
Error class 4	Minor error	Information requests related to the services.	65% of all reported incidents are resolved within eight hours during business hours.

5.   Maintenance

Any scheduled maintenance that results in an interruption of the services provided by IKARUS Data Center of more than 30 minutes will be communicated to the Customer by email at least 48 hours prior to the scheduled maintenance with the following information:

- Time of maintenance
- The expected duration of the interruption and
- Expected severity of the interruption.

To the extent possible, any scheduled maintenance that results in an interruption of service of more than 30 minutes will be carried out between 7:30 pm and 7:00 am.