IKARUS security software

IKARUS 24/7 incident.response
powered by Mandiant

Service Description

Version: 1.2

Date: 17 September 2021

Content

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

General

IKARUS offers a 24/7 incident response service with a 4-hour response time. This service gives customers guaranteed, fast and direct access to the incident response services of IKARUS in situations where a cyber security incident has either occurred or is reasonably suspected to have occurred within a company. IKARUS experts conduct a preliminary investigation and, if necessary, deploy a software for a more in-depth analysis. In a final step, provided this is necessary and desired by the customer, global Mandiant experts are requested.

In the event of a cyber security incident, IKARUS 24/7 incident.response guarantees immediate access to all necessary resources, both at IKARUS and its service partner Mandiant, which, normally, cannot be made available at short notice. Incidents are handled in accordance with a tried and tested three-phase model to ensure that customers receive quick and efficient support.

The 24/7 incident response (“IR”) service is provided by IKARUS Security Software GmbH (“IKARUS”). Subject to previous consultation between IKARUS and the customer, sub-tasks may be passed on to IKARUS’ global partner, Mandiant Corp. (2318 Mill Road Suite 500 Alexandria, VA 22314 United States). This document describes the services included in the purchase price, as well as additional offers and services.

Content of the standard service

Customers using this service may contact IKARUS at any time - 24/7 - if a cyber security incident occurs or is reasonably suspected to have occurred. The same applies, if the 24/7 IR service is purchased via a partner or reseller of IKARUS.

The customer will be charged for the number of hours actually worked. In this context, IKARUS offers a variety of packages with a different number of hours included. To prevent delays and ensure that customers are not forced to deal with purchasing additional hours under time pressure during an ongoing security incident, we recommend purchasing a larger number of hours already before an incident occurs. For more information, please contact the IKARUS sales team or an IKARUS partner.

IKARUS 24/7 incident.response guarantees each customer a maximum response time of 4 hours following the reporting of the incident. In these 4 hours, IKARUS’ three-phase model (as described below) is initiated.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

IKARUS' three-phase IR model

1st Phase: Preliminary investigation

After IKARUS has been contacted, a preliminary investigation based on the IKARUS Threat Intelligence Platform is initiated within 4 hours. The more meaningful information and data are made available, the more efficient the analysis conducted in consultation with the customer.

2nd Phase: Software deployment

In phase 2, IKARUS deploys a software to conduct a more in-depth analysis of the incident. The focus here is on monitoring, threat hunting and remediation, with detailed insights on the incident being gathered. Said insights will result in one of the following three recommendations being issued:

Action Point 1 (AP1):

The attack does not entail any further malicious events - IKARUS closes the case and deinstalls all of the technologies previously deployed by it. Duration of engagement - up to 1 week.

Action Point 2 (AP2):

IKARUS subjects the affected customer systems to a remediation process. Subsequently, IKARUS closes the case and deinstalls all of the technologies previously deployed by it. Duration of engagement - up to 1 week.

Action Point 3 (AP3):

The remediation process reaches an extent that cannot efficiently be covered by IKARUS' resources alone, hence, the additional support of Mandiant's global experts is required. After consultation with the customer, phase 3 is initiated.

3rd Phase: Engagement Mandiant

If IKARUS has classified the cyber security incident as AP3, the customer will receive an individual offer, based on its specific customer infrastructure, for involving additional global resources from Mandiant. During the entire phase 3, IKARUS remains the first point of contact for the customer. Duration of engagement - 1 to several weeks.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Customer onboarding

Immediately after purchasing the IKARUS 24/7 incident.response service for the first time, the customer may report cyber security incidents to IKARUS during its business hours, within the scope of an 8 to 5 SLA (Service Level Agreement). The 8 to 5 SLA is valid for 14 days following purchase. The business hours of IKARUS can be found on the company's website at https://www.IKARUSsecurity.com.

In the course of said 14 days, IKARUS adapts all relevant processes so as to be able to provide the customer with the 24/7 service purchased by it. This stage also includes a precautionary onboarding of the IR partner Mandiant in case it will have to take over a case within the scope of phase 3.

As from day 15 after purchase, the onboarding has been successfully completed and the customer can now enjoy the IKARUS IR service within the scope of a 24/7 SLA with a 4-hour response time.

Contact

After the purchase, the customer will receive a special telephone number from IKARUS to be able to contact IKARUS 24/7. Contacting IKARUS via e-mail is also possible 24/7.

Please consider that IKARUS/Mandiant technicians communicate exclusively with technical contact persons indicated by the customer upon purchase.

Optional, fee-based additional services

Within the scope of the three-phase model, additional costs may arise to the customer. For any additional costs, the customer will receive an individual offer from the IKARUS sales team or, where applicable, from an IKARUS partner. Before the provision of any fee-based additional services, the customer must approve the additional costs and/or purchase the relevant service. IKARUS guarantees full cost transparency.

Additional costs usually arise if more working hours must be spent on resolving an incident, or if additional expenses arise or extra costs are incurred due to additional software licenses being required. Customers may purchase working hours in the form of so-called "IKARUS get-direct" packages.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Optional: Hour packages – IKARUS get.direct

The standard service “IKARUS 24/7 incident.response powered by Mandiant” available at the base price does NOT include ANY working hours. It enables the customer to contact IKARUS security experts 24/7, to report cyber security incidents and to access resources reserved for the customer.

As soon as phase 1 (preliminary investigation) is initiated, IKARUS will start spending working hours on the case. Such working hours must be purchased in the form of hour packages which are either offered and invoiced in addition to the standard service or in a bundle with the standard service. If all working hours purchased are used up, the customer will receive an offer for a new hour package.

These so-called “IKARUS get.direct” packages are available in different sizes. IKARUS recommends purchasing the IKARUS 24/7 incident.response service along with an hour package to avoid losing time on administrative tasks during an actual cyber security incident.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Features not included in the standard service

- Working hours. The standard service does not include any working hours. Insofar as the customer did not purchase the standard service in a bundle with an included hour package, the customer needs to purchase an hour package (“IKARUS get.direct”) so that, if a cyber security incident occurs, IKARUS will be able to start phase 1 and subsequently initiate further phases.
- On-site support. The service is provided via remote maintenance after prior appointment. IKARUS will make on-site appointments at its own discretion and only in exceptional cases.
- Monitoring. The service does not include a proactive monitoring of the customer’s systems by IKARUS. The customer must report cyber security incidents to IKARUS by calling or sending an e-mail to the contacts indicated to it.
- System restoration. No restoration of customer systems is carried out (e.g. from backups).
- Configurations. No configuration/modification, etc. of third-party hardware or software is carried out.
- Spare parts. No spare parts for hardware used at a customer site will be installed.
- Maintenance. No software installed at the customer site will be patched, upgraded, or updated.
- Warranty. IKARUS and its partners cannot warrant that it will be possible to completely clean, rescue or restore infected customer systems.
- Liability. IKARUS and its partners shall not be liable to the customer for any kind of loss, damage or business interruption caused by a cyber attack or similar threats.
- Licenses. Within the scope of “IKARUS 24/7 incident.response powered by Mandiant”, the customer does not purchase any software. However, the software used by IKARUS may be offered to the customer for purchase by the IKARUS sales team or an IKARUS partner.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405

Conditions and requirements for the 24/7 IR standard service

- Customer's participation in the planning and organization of IKARUS support services.
- The customer forwarded its contact details to IKARUS.
- The customer reported a cyber security incident to IKARUS via e-mail or telephone. The contact details for doing so will be transmitted to the customer by IKARUS before or after purchasing the service.
- If necessary, remote access to the customer’s IT systems is fully possible (active internet connection with sufficient bandwidth).
- All necessary user accounts, information and passwords are available.
- The technicians employed by IKARUS are 3rd level technicians certified for, among other things, software solutions provided by IKARUS, FireEye and Nozomi. The service is available in German and English.
- IKARUS 3rd level technicians communicate exclusively with the customer’s technical IT personnel. If the customer does not have its own technical IT personnel, the customer's main technical contact person shall be considered the main contact person for IKARUS.
- Unless the customer agreement stipulates otherwise, the service is purchased for a period of 12 months after which it is automatically extended by further 12 months.
- The support hours included in the hour package (“IKARUS get.direct”) expire after 12 months. However, if the customer agreement is extended (automatically or manually) by further 12 months, the hours not used in the previous validity period can be carried forward to the next validity period. In this case, extending the agreement will incur merely the costs for the standard service.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com
Erste Bank Österreich | BIC GIBAATWWXXX | AT142011182122082100 | FN 64708i | Court of Jurisdiction: Vienna | VAT ID: ATU15191405