

# Trellix (ehemals FireEye) & Nozomi Services powered by IKARUS

---

## Servicebeschreibung

Version: 1.0

Datum: 30.05.2023

## Inhalt

---

1.	Allgemeines	3
2.	Leistungsinhalt des Standardservice	3
2.1	Installationsunterstützung (Onboarding, Setup)	3
2.2	Unterstützung während der Betriebsführung	3
2.3	Voraussetzungen für das Standardservice	4
2.4.	Im Standardservice nicht enthaltene Leistungen	4
3.	Optionale, kostenpflichtige Zusatzservices	5
4.	Reaktionszeiten für Störungen, die das IKARUS Rechenzentrum betreffen	6
5.	Wartung	6

## 1. Allgemeines

Der technische Support wird durch das Unternehmen IKARUS Security Software GmbH (IKARUS) durchgeführt. Dieses Dokument beschreibt die Serviceleistungen, die im Kaufpreis pauschal inbegriffen sind. Weitere Servicedienstleistungen können optional bestellt werden und sind im Punkt 3 exemplarisch angeführt.

Die von IKARUS eingesetzten Techniker sind vom jeweiligen Hersteller zertifizierte 3<sup>rd</sup> Level Techniker. Das Service ist in den Sprachen Deutsch und Englisch verfügbar.

## 2. Leistungsinhalt des Standardservice

IKARUS unterstützt Endkunden bei der Inbetriebnahme und während der Betriebsführung der jeweiligen Trellix /Nozomi Lösung im unter 2.1 beschriebenen Umfang.

Darüber hinaus betreibt IKARUS eine in Wien gehostete Trellix Rechenzentrumsumgebung, auf die manche der angebotenen Services bzw. Trellix Produkte zurückgreifen bzw. die zugesagten Funktionen einen Zugriff auf das IKARUS Rechenzentrum erfordern.

### 2.1 Installationsunterstützung (Onboarding, Setup)

Supportanfragen können über die E-Mail-Adresse [managed.defense@ikarus.at](mailto:managed.defense@ikarus.at) gestellt werden. Die Beantwortung der Fragen erfolgt entweder telefonisch oder per E-Mail innerhalb der IKARUS Geschäftszeiten (siehe [www.ikarus.at](http://www.ikarus.at)) innerhalb von 3 Werktagen.

- Kontaktaufnahme mit dem Ansprechpartner des Kunden zwecks Planung der Installation.
- Erklärung zur Applikation inkl. Administrationsoberfläche.
- Erklärung und Beispiel: Basis Anweisungen zum Rollout und der Inbetriebnahme.
- Erklärung und Handlungsempfehlungen zur Konfiguration der Produkte.
- Einschulung für die Handhabung der Produkte bei Cyber-Bedrohungen & potentiellen Infektionen.
- Erklärung: Handlungsempfehlungen zum Device Monitoring der Produkte.
- Erstkonfiguration der mitbestellten Hardware (Update der Software, Einstellen der Basiskonfiguration) und Versand an den Kunden.

### 2.2 Unterstützung während der Betriebsführung

- Kommunikation über neue Releases und deren Funktionen an eine definierte Kunden Mailadresse.
- Lieferung von Ersatzhardware bei Hardwaredefekten innerhalb der Gewährleistung bzw. mitgekaufter Hardwarewartung. Servicelevel: Best Effort, in der Regel 48h werktags – je nach Verfügbarkeit und Zugriffsmöglichkeit auf die Appliance, z.B. Einfluss von Zollverzögerung.
- Behebung von Problemen, die auf zentrale Services vom IKARUS Rechenzentrum zurückzuführen sind.

## 2.3 Voraussetzungen für das Standardservice

- Mitwirkung des Kunden bei der Planung und Organisation der IKARUS Support Leistungen.
- Der Kunde hat einen Termin zur Erbringung des Service vereinbart.
- Die notwendigen Systemvoraussetzungen (Hardware und Software 3<sup>rd</sup> Party) für das jeweilige Service wurden durch den Kunden überprüft und sind erfüllt.
- Der Fernzugriff auf den Computer des Benutzers ist im Bedarfsfall vollumfänglich möglich (aufrechte Internetverbindung mit ausreichender Bandbreite).
- Mindestens eine Lizenz wurde vom Kunden erworben.
- Alle notwendigen Benutzerkonten Informationen und Kennwörter sind verfügbar.
- Es besteht Zugriff auf den IKARUS Service Account, der vorab per Default im erworbenen System des Kunden hinterlegt wurde. Auf ausdrücklichen Wunsch des Kunden kann dieser erweiterte Servicezugriff deaktiviert werden. Dadurch sind der Support und die SLAs nur bedingt erfüllbar.
- IKARUS 3<sup>rd</sup> Level Techniker kommunizieren ausschließlich mit technischem IT-Personal des Kunden. Sollte der Kunde über kein eigenes technisches IT-Personal verfügen, so gilt der technische Hauptverantwortliche des Kunden als Hauptansprechpartner für IKARUS.

## 2.4. Im Standardservice nicht enthaltene Leistungen

- Die vollumfängliche Inbetriebnahme (roll-out/onboarding) obliegt der Verantwortung des Kunden.
- Alle Hauptfunktionen und die wichtigsten Konfigurationen werden als Beispiel einmal gezeigt bzw. geschult. Das Anlegen, bzw. Konfigurieren zusätzlicher Einstellungen wie z.B. das Ausrollen zusätzlicher Clients oder Regeln, das Einbinden weiterer Endgeräte oder ähnliches, sind nicht enthalten.
- Vor-Ort-Unterstützung beim Kunden. Das Service wird nach Terminvereinbarung via Fernwartung erbracht. Vor Ort Termine werden von IKARUS nach eigenem Ermessen und nur in Ausnahmefällen durchgeführt.
- Sollten bereits Viren, Malware oder ähnliche Bedrohungen auf der Hardware des Kunden vorzufinden sein, auch wenn diese erst nach der Aktivierung der gekauften/getesteten IKARUS Services erkannt werden, so ist die Bereinigung des Kundensystems vor Viren und ähnlichen Bedrohungen nicht im Preis inkludiert.
- Konfiguration/Änderung, etc. von Hard- oder Software von Drittanbietern.
- Erstellen von Reports oder Statistiken.
- Wartung von Trellix und Nozomi Hardware, die an einem Standort des Kunden eingesetzt wird.
- Einbau von Ersatzteilen für Hardware, die an einem Standort des Kunden eingesetzt wird.
- Patchen, Einspielen von Upgrades oder Updates von Software, die beim Kunden installiert ist.

### 3. Optionale, kostenpflichtige Zusatzservices

Wenn nach viermaligem Kontaktversuch durch IKARUS (3 x telefonisch, danach per E-Mail) und dem Ablauf einer Frist von 10 Werktagen keine Kundenreaktion erfolgt, werden von IKARUS die Standard-Installationsbeschreibungen übermittelt. IKARUS behält sich in diesem Fall vor, weitere Unterstützungsleistungen kostenpflichtig zu erbringen.

Es können zusätzliche, individuelle Leistungen zusammengestellt und auf die Kundenanforderungen angepasst werden. Diese beinhalten unter anderem:

- Eigene Servicrufnummer für Endkunden für direkten telefonischen Kontakt zu IKARUS 3<sup>rd</sup> Level Supporttechnikern.
- Erweiterte Supportzeiten bis hin zum 24/7 Service.
- Übernahme von Verantwortungen des Kunden durch IKARUS bis hin zum kompletten Outsourcing sämtlicher Betriebsaufgaben der Trellix und Nozomi Produkte.
- Erstellen von Reports, Maßnahmenkatalog, Best Practices, Dashboards, Custom Queries, Enterprise Search, Konfigurationen, Integration von weiterer Hardware/Endpoints, Netzwerkarchitektur Unterstützung.
- Empfehlungen für 3<sup>rd</sup> Party Hard-/Software Anschaffungen und Integrationsunterstützung
- Maintenance der Hard- und Software der mitgekauften Appliances.
- Abwicklung und Bezug von Trellix Mandiant Services (Expertise on Demand) für alle eingesetzten Trellix und Nozomi Services.
- Abstimmen von Parametern für die Installation (Data Acquisition Planning – Positionierung der Hardware/Software Appliances (Network Security, Endpoint Security, E-Mail Security – On-Prem, Cloud, Trellix Cloud - Helix), 3<sup>rd</sup> Party Data Sources, Scoping Guide, Netzwerkadressen, Mirror-Port/SPAN/TAP, Zutritte, Wartungszugang, Unterstützung bei Triage Katalog (Definition von Netzbereichen, Verantwortlichkeiten, Kontaktpersonen))
- Support bei Software Problemen, die sich im Laufe der Betriebsführung ergeben.

## 4. Reaktionszeiten für Störungen, die das IKARUS Rechenzentrum betreffen

Fehlerklasse 1	Kritischer Fehler	Kritischer größerer Dienstaussfall, durch den der Dienst vollständig unterbrochen wird.	95% aller gemeldeten Störungen werden innerhalb von zwei Stunden während der Geschäftszeiten behoben.
Fehlerklasse 2	Erheblicher Fehler	Wesentlicher Dienstaussfall, durch den der Dienst massiv unterbrochen wird oder es zu größeren Verzögerungen kommt.	85% aller gemeldeten Störungen werden innerhalb von vier Stunden während der Geschäftszeiten behoben.
Fehlerklasse 3	Mittelschwerer Fehler	Standard-Dienstaussfall mit keinem oder unerheblichem Einfluss auf E-Mail- Scanning und - Weiterleitung	75% aller Dienstaussfälle werden innerhalb von acht Stunden während der Geschäftszeiten behoben.
Fehlerklasse 4	Geringfügiger Fehler	Informationsanfragen im Zusammenhang mit den Diensten.	65% aller gemeldeten Störungen werden innerhalb von acht Stunden während der Geschäftszeiten behoben.

## 5. Wartung

Jede planmäßige Wartung, die zu einer Unterbrechung der vom IKARUS Rechenzentrum gelieferten Services von mehr als 30 Minuten führt, wird dem Kunden mindestens 48 Stunden vor der planmäßigen Wartung per E-Mail mit den folgenden Angaben mitgeteilt:

- Zeitpunkt der Wartung,
- voraussichtliche Zeitdauer der Unterbrechung und
- voraussichtlicher Schweregrad der Unterbrechung.

Soweit möglich wird jede planmäßige Wartung, die zu einer Unterbrechung des Service von mehr als 30 Minuten führt, zwischen 19:30 und 7:00 Uhr durchgeführt.