



IKARUS threat.intelligence.platform

## Cyber Threat Intelligence: Präzises Kontextwissen zu globalen und lokalen Cyberbedrohungen

Die **IKARUS threat.intelligence.platform (TIP)** bietet flexiblen Zugriff auf eine der umfassendsten und präzisesten Sammlungen von strukturierten und kontextualisierten Bedrohungsdaten, Hintergrundwissen und Methodik. Gewinnen Sie wertvolle Einblicke, um Ihre Abwehr zu stärken, Wissen, um Indicators of Compromise zu erkennen und zu verstehen, sowie Zeit, um Sicherheitsvorfälle effektiv zu beantworten.

Das Konzept der **IKARUS threat.intelligence.platform** ist weltweit einzigartig: Es beschreibt die Möglichkeit, Bedrohungsinformationen aller Art und aus den unterschiedlichsten Quellen und Formaten auf einer einzigen Plattform so zu verwalten, dass sie darin organisiert, gefiltert, gesucht, moderiert und in Verbindung gebracht werden können. Sie erhalten exklusiven Input für Ihre **Defense Technologien**, das **Incident Response Management**, das **Threat Hunting** und Ihre **Threat Landscape** und sind damit besser für Angriffe gewappnet als die meisten.

### Threat Intelligence ist weit mehr als Bedrohungsdaten

Viele Cyber-Security-Technologien enthalten spezifische Bedrohungsdaten, anhand derer die Lösungen gezielt reagieren. Diese Daten sind produktspezifisch angelegt und enthalten keinerlei Kontext.

Cyber Threat Intelligence ist evidenzbasiertes Wissen – einschließlich Kontext, Mechanismen, Indikatoren, Implikationen und umsetzbarer Ratschläge – über eine bestehende oder aufkommende Bedrohung oder Gefahr. Sie eignet sich als fundierte **Entscheidungsgrundlage** für die Reaktion auf potenzielle oder tatsächliche Incidents sowie für die **Identifikation und Bewertung** von Sicherheitsverletzungen, aber auch für das **Risikomanagement**, gezieltes **Threat Hunting** sowie die Erstellung von **strategischen Lagebildern**.

Bedrohungsinformationen alleine haben kaum Aussagekraft. Erst die Verknüpfung mit darüber hinausgehenden Informationen aus Bewertungen, Hashes und Algorithmen mit Hintergrundwissen zu Angreifergruppen, forensischen Untersuchungen, Rekonstruktionen bössartiger Infrastrukturen und Merkmalen zur Identifizierung von Akteuren, die weltweit von Cybersicherheitsforschern gesammelt werden, bringen wertvolle Einblicke und schärfen Ihr Wissen.

## Einzigartige Kombination aus Datenquellen und Datenqualität

In der IKARUS TIP sind sämtliche Daten in strategische, operationelle und taktische Informationen gegliedert und auf Knopfdruck abrufbar.

- Die **strategische Ebene** liefert ein Gesamtbild und Trendinformationen. Sie weist Informationen zu Branchen, Regionen, möglichen anderen Zielen, Motivationen oder Sponsoren der Angreifenden aus.
- Die **operationelle Ebene** bietet zusätzlichen Kontext rund um die Indikatoren (Tactics, Techniques and Procedures – TTPs), um Malware zu identifizieren oder einzelne Sicherheitsvorfälle bekannten Angriffstaktiken oder Angreifergruppen zuzuordnen.
- Die **taktische Ebene** ermöglicht es, einzelne Indicators of Compromise im technischen Kontext zu sehen: Anhand verknüpfter Daten zu Domains, IP-Adressen, Download-Links u.a. kann beispielsweise eine Absenderadresse mit einer Spear Phishing-Kampagne in Zusammenhang gebracht werden. Sie erfahren anhand einzelner Informationsschnipsel, ob Ihre SpamMail Teil einer generischen Malwarekampagne ist, Sie sich im Visier staatlicher Akteure befinden, gezielte Phishing-Aktionen auf Ihr Unternehmen gesetzt werden oder Angriffe auf Ihre Geschäftsgeheimnisse zu erwarten sind.

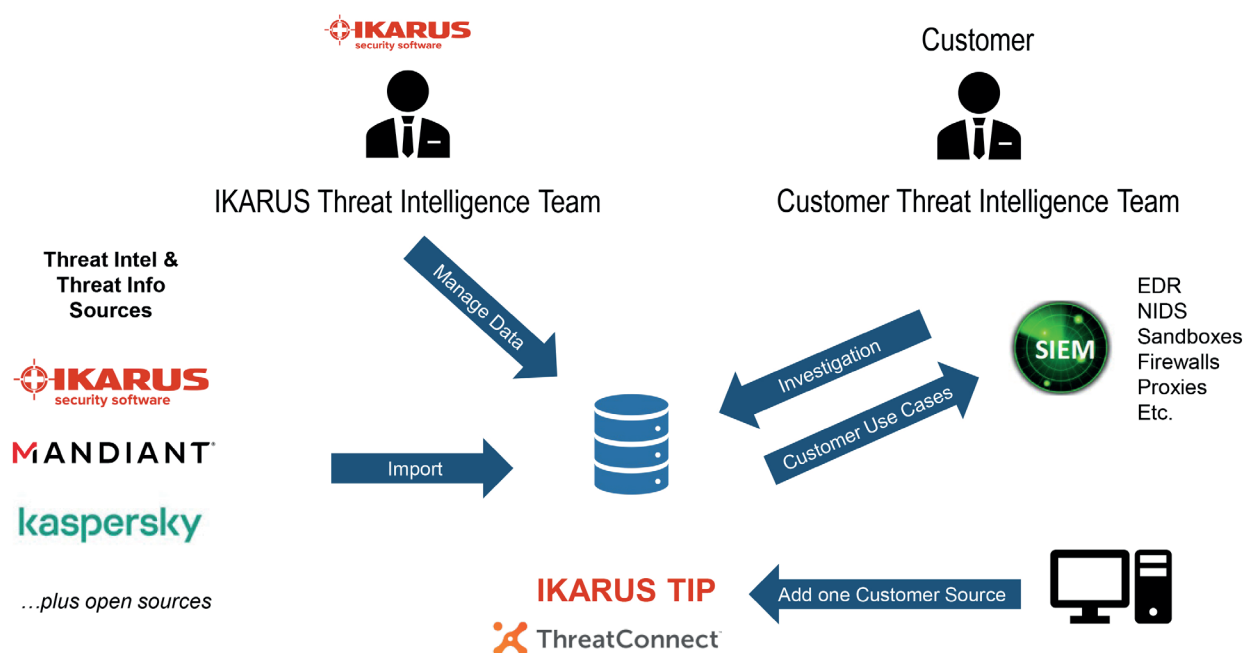
Die **IKARUS threat.intelligence.platform** ist in User Experience und Datenqualität weltweit einzigartig. Sie verbindet Open Sources und führende kommerzielle Quellen mit den lokalen Bedrohungsinformationen, welche durch IKARUS eigene Endpunkte gewonnen werden.

Die Datenquellen sind in **endpoint- und netzwerkbasierte Indikatoren, Schwachstelleninformationen, Angriffsmethoden und -techniken, Angreifergruppierungen und Attribuierungen, Kampagnen, Toolsets, Malware und Malware Familien, Reports und Signaturen** kategorisiert.

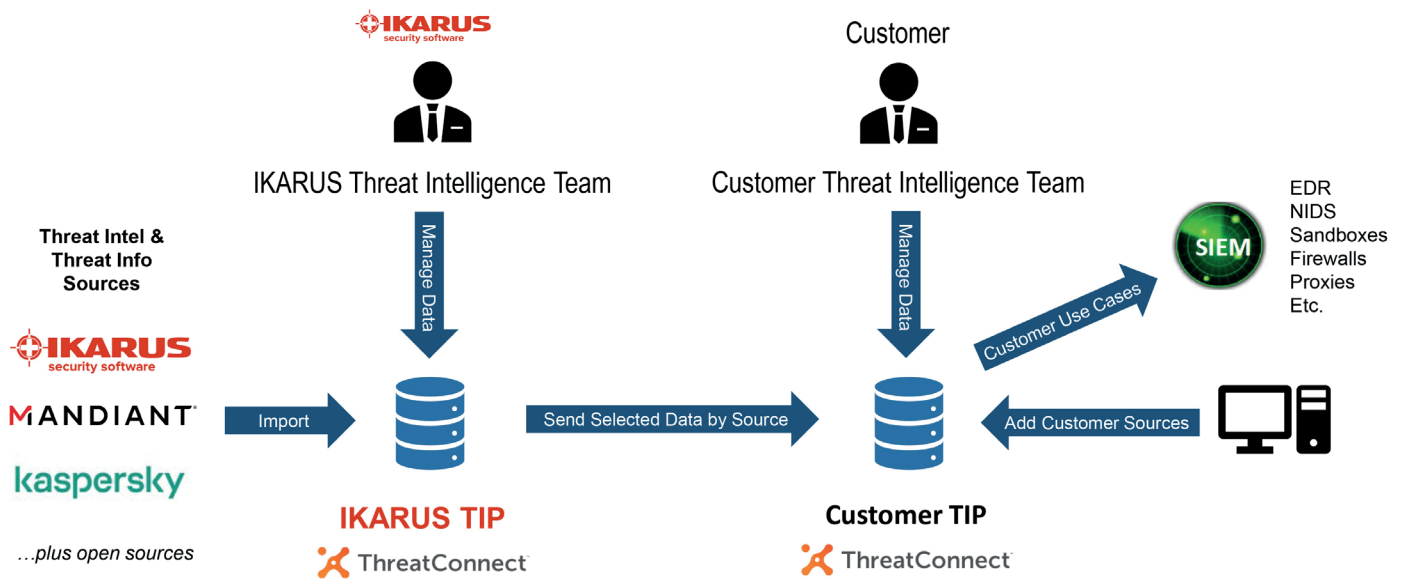
## Flexible Möglichkeiten der Systemintegration

Die Integration der Plattform kann via **Cloud, On-Premises** oder für **Air-Gapped-Systeme** erfolgen: Nutzen Sie Ihre Bedarf und Ihrer Infrastruktur entsprechend den direkten Zugriff auf die IKARUS TIP für gezielte Investigationen oder lassen Sie über Ihre eigene Instanz die Datenfeeds der IKARUS TIP in Ihr lokales SIEM, EDR, NIDS o.ä. einfließen. Auch die Integration in Air-Gapped Systeme wird unterstützt.

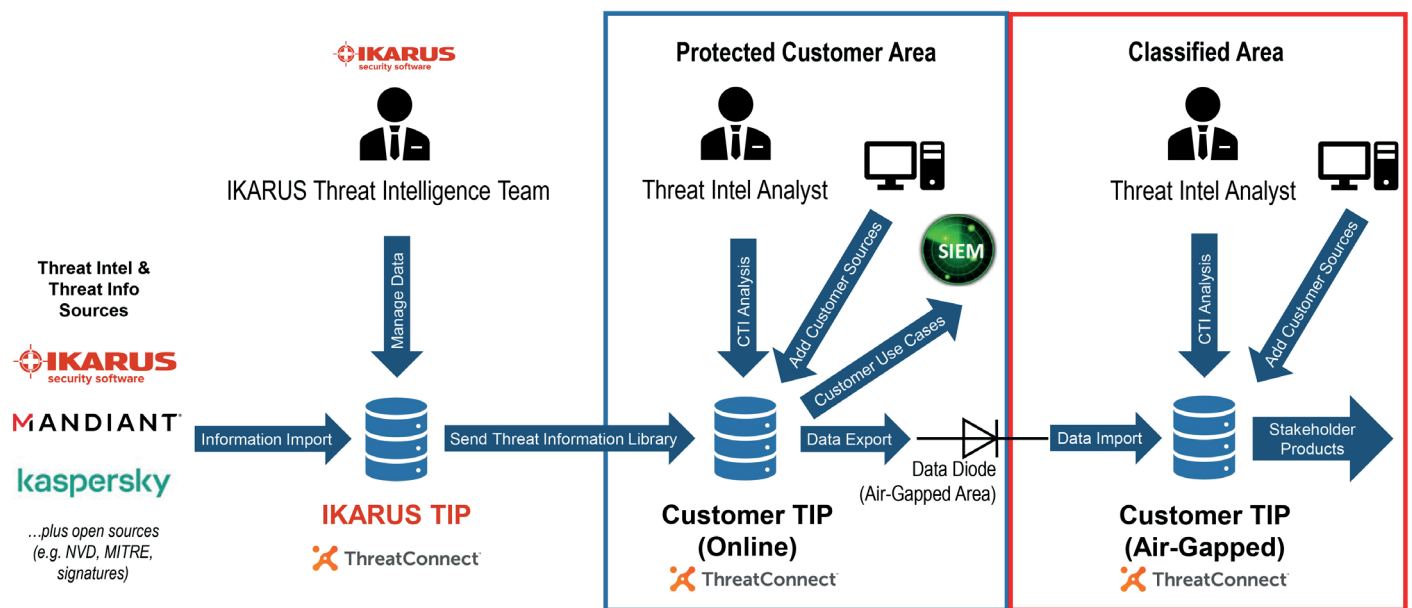
## IKARUS threat.intelligence.platform – Cloud-Integration



### IKARUS threat.intelligence.platform – On Premise-Integration



### IKARUS threat.intelligence.platform – Air-Gapped Environment



## Highlights

- ✓ Globale und lokale Datenquellen auf höchstem Niveau
- ✓ Strategische, operationelle und taktische Informationen
- ✓ Flexibler Datenzugriff / Systemintegration nach Bedarf
- ✓ Gezielte Investigation und Customer Use Cases
- ✓ Bereicherung bestehender Cyber Defense Technologien (EDR, NIDS, Sandboxes, Firewalls, Proxies etc.)

## Vorteile

- ✓ Gezielte Reaktion auf Cybersicherheitsvorfälle
- ✓ Attribuierte und aktuelle lokale und globale Bedrohungsinformation
- ✓ Wissen über aktuelle Angriffsmethoden und Vorfälle weltweit
- ✓ Erstellung von strategischen Lagebildern
- ✓ Optimiertes Risikomanagement und Cyberprävention

Wir beraten Sie gerne!

Kontaktieren Sie uns unter [sales@ikarus.at](mailto:sales@ikarus.at) oder Tel. +43 1 58995-500.

## Über IKARUS Security Software

Der österreichische Cyber-Security-Provider IKARUS Security Software macht seit 1986 Unternehmen, Privatkunden und Industrieumgebungen sicherer und resilienter gegen digitale Bedrohungen. Sowohl mit selbst entwickelten Services rund um die renommierte IKARUS Malware Scan Engine als auch mit ergänzenden Lösungen ausgewählter Technologiepartner schützt IKARUS IT-, OT und IoT-Netzwerke vor Cyber-Angriffen und Betriebsausfällen.

Zu den zufriedenen Kunden zählen lokale und internationale KMUs, öffentliche Einrichtungen, Industrieunternehmen, ISPs und Security-Hersteller.

**we provide security**

[www.IKARUSsecurity.com](http://www.IKARUSsecurity.com)

**IKARUS Sales Team** | [sales@ikarus.at](mailto:sales@ikarus.at) | +43 1 589 95-500  
**IKARUS Support Team** | [support@ikarus.at](mailto:support@ikarus.at) | +43 1 589 95-400