IKARUS security software

IKARUS threat.intelligence.platform

Cyber Threat Intelligence: Precise Contextual knowledge of global and local cyber threats

The **IKARUS threat.intelligence.platform (TIP)** provides flexible access to one of the most comprehensive and accurate collections of structured and contextualized threat data, background knowledge and methodology. Gain valuable insights to strengthen your defence, knowledge to identify and understand Indicators of Compromise, and time to respond effectively to security incidents.
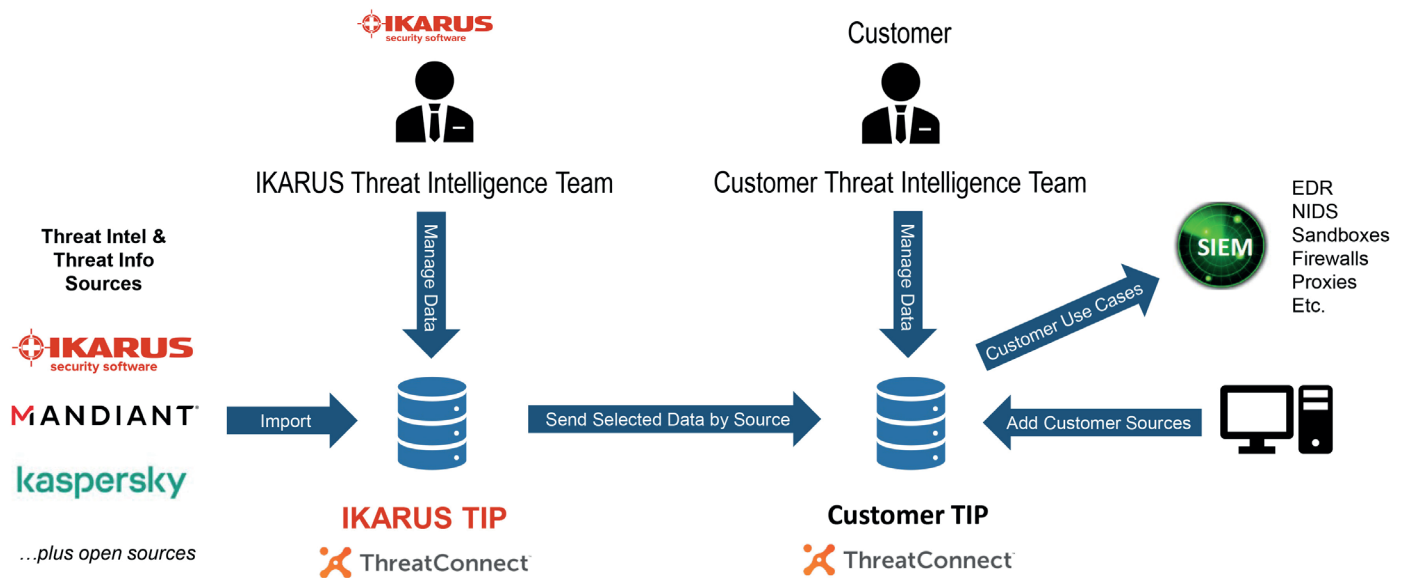
The concept of the **IKARUS threat.intelligence.platform** is unique in the world: it describes the ability to manage threat information of all kinds and from a wide variety of sources and formats on a single platform in such a way that it can be organized, filtered, searched, moderated and linked. Get exclusive input for your **Defense Technologies, Incident Response Management, Threat Hunting** and **Threat Landscape**, making you better equipped for attack than most.
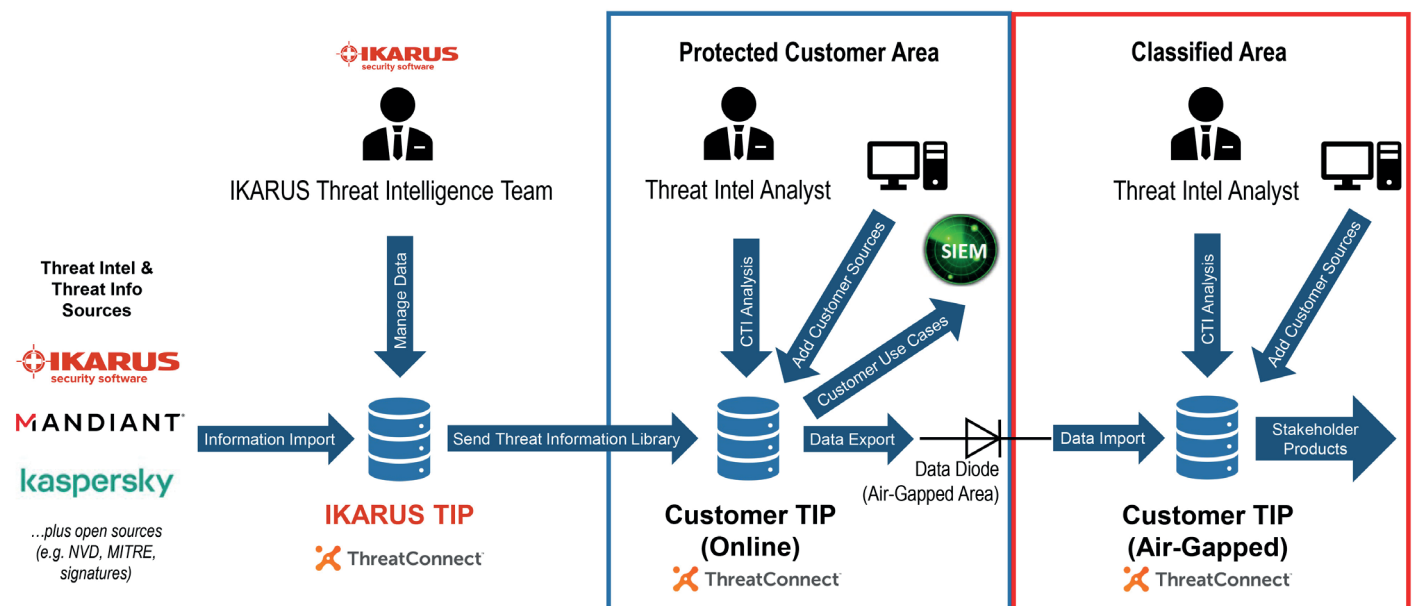
Threat Intelligence is much more than threat data

Many cyber security technologies contain specific threat data that allow solutions to respond in a targeted manner. This data is product-specific and does not contain any context. Cyber Threat Intelligence is evidence-based knowledge about an existing or emerging threat or menace, including context, mechanisms, indicators, implications, and actionable advice. It is suitable as an **informed decisionmaking basis** for responding to potential or actual incidents and **for identifying and evaluating** security breaches. It is also suitable for **risk management**, targeted threat hunting and creating **strategic situational pictures**.

Threat intelligence alone has little meaning. It is only by linking with additional information from assessments, hashes, and algorithms with background knowledge about attack groups, forensic investigations, and reconstructions of malicious infrastructures. It traits to identify actors collected by cyber security researchers worldwide so that you can gain valuable insights and sharpen your knowledge.

Unique combination of data sources and data quality

In the IKARUS TIP, all data is divided into **strategic, operational and tactical information** and can be accessed at the push of a button.

- The **strategic level** provides an overall picture and trend information. It provides information on industries, regions, possible other Targets, motivations or sponsors of the attackers

- The **operational level** provides additional context around the indicators (Tactics, Techniques and Procedures (TTPs) to identify malware or to assign individual security incidents to known attack tactics or attack groups.

- The **tactical level** makes it possible to see individual Indicators of Compromise in a technical context: Based on linked data on domains, IP addresses, download links, etc., a sender address can be connected to a Spear Phishing campaign. You can find out whether your spam mail is part of a generic malware campaign based on snippets of information, if State actors target you, targeted phishing actions are targeted at your company, or attacks on your business secrets are expected.

The **IKARUS threat.intelligence.platform** is unique regarding user experience and data quality. It combines open sources and leading commercial sources with local threat intelligence gathered through IKARUS' own endpoints.

The data sources are categorized into **endpoint-** and **network-based indicators, vulnerability information, attack methods** and **techniques, attacker groupings** and **attributions, campaigns, toolsets, malware and malware families, reports** and **signatures.**

Flexible options for system integration

The platform can be integrated via **cloud, on-premises** or **air-gapped systems**: Use direct access to the IKARUS TIP for targeted investigations according to your needs and infrastructure or let the data feeds of the IKARUS TIP flow into your local SIEM, EDR, NIDS or similar via your own instance. Integration into air-gapped systems is also supported.

IKARUS threat.intelligence.platform – Cloud-Integration

IKARUS threat.intelligence.platform – On Premise-Integration

IKARUS threat.intelligence.platform – Air-Gapped Environment

Highlights

✓ Global and local data sources at the highest level

✓ Strategic, operational and tactical information

✓ Flexible data access/system integration as required

✓ Targeted investigation and customer use cases

✓ Enrichment of existing cyber defence technologies (EDR, NIDS, sandboxes, firewalls, proxies etc.)

Advantages

✓ Targeted response to cyber security incidents

✓ Attributed and up-to-date local and global threat information

✓ Knowledge of current attack methods and incidents worldwide

✓ Creation of strategic situational awareness

✓ Optimized risk management and cyber prevention

We are happy to advise you!

Please contact us at sales@ikarus.at or phone +43 1 58995-500.

About IKARUS Security Software

The Austrian cyber security provider IKARUS Security Software has been making companies, private customers and industrial environments more secure and resilient against digital threats since 1986. IKARUS protects IT, OT and IoT networks against cyber attacks and operational failures with services developed in-house around the renowned IKARUS Malware Scan Engine as well as with complementary solutions from selected technology partners.

Satisfied customers include local and international SMEs, public institutions, industrial companies, ISPs and security manufacturers.

we provide security

www.IKARUSsecurity.com

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400