Case Study

IKARUS and ThreatConnect Deliver Next-Gen Threat Intelligence to Secure European Clients

Customer Profile

Organization Type	*Established*	*Headquarters*
MSSP	1986	VIENNA, AUSTRIA

Background

IKARUS Security Software is an Austrian company that has provided IT security solutions since 1986. The company is a leading provider of threat intelligence in Austria and Central Europe thanks to its unique technology and wide collection capabilities. In 2021, IKARUS decided to expand its security offerings to include a flexible yet impactful threat intelligence solution for customers. IKARUS partnered with ThreatConnect to build the new threat intelligence engine, streamlining threat intelligence collection and analysis for private and public sector organizations in Europe and beyond.

Challenges Faced

IKARUS is well-known in Europe for its antivirus solutions and offers customers a comprehensive suite of security products. After extensive research, IKARUS decided to partner with an existing threat intelligence platform to support its mission to be a one-stop cybersecurity shop for customers.

However, the IKARUS team quickly discovered the selected threat intelligence product did not meet promised expectations during testing. The team began to reconsider the feasibility of offering a high-quality threat intelligence solution. Disappointed, the IKARUS team initiated a second round of research for a potential partner.

How ThreatConnect Helped

During its next search, IKARUS found ThreatConnect's Threat Intelligence Platform (TI Ops). The team was impressed with ThreatConnect's extensive API integration capabilities, which would make it easy for its customers to plug the platform into their existing tech stacks. The main selling point, however, was that ThreatConnect's

TI Ops offering allowed for multiple deployment options, which helped IKARUS to meet diverse customer needs for on-prem, cloud, or hybrid services while complying with strict data residency requirements.

After a successful pilot, IKARUS and ThreatConnect deployed IKARUS threat.intelligence.platform (IKARUS TIP). IKARUS TIP is deployed using the ThreatConnect platform supplemented by IKARUS' own feeds, including local intel from its sensor network. The raw data is analyzed, organized, and formatted for easy machine and human consumption. IKARUS leverages ThreatConnect's multi-tenant capabilities to provide its customers in Austria and beyond with a powerful threat intelligence engine. Today, the two teams are collaborating to ensure IKARUS' customers receive high-quality, personalized service.

"When there are challenges, it's not an issue, nobody's playing blame games or pushing things toward each other. It's just: **We have this challenge, let's face that challenge together. Let's find a solution that everybody is happy with.**" says Amber Weinber, Team Lead, TIC & TDR at IKARUS.

A Powerful Threat Intelligence Platform for Improved Security Postures

Today, IKARUS' clients use the ThreatConnect-powered TIP to streamline threat intelligence and case management. For example, instead of logging into dozens of intel sources, analysts can reference all their data from a single platform. The TIP also includes automation in key areas that give teams more time for high-value analysis and collaboration. For example, the ThreatConnect platform's automated playbooks respond automatically to threats by enriching data, triggering alerts, and applying defensive actions.

> "That kind of diversity and breadth of functionality and capability—that's why we see such benefit in [ThreatConnect's TIP]. It's not a tool where we then have to change our clients' entire ecosystem to fit the tool. It's a tool that can integrate more or less seamlessly with the client's infrastructure. And that's a huge added value."
>
> - Amber Weinber, Team Lead, TIC & TDR, IKARUS

> "Once those playbooks have automated your risk scoring or your case generation… it tells you step-by-step what you need to do, why something is relevant, and who you need to inform. It takes so much room for human error out of the equation."
>
> - Amber Weinber, Team Lead, TIC & TDR at IKARUS.

About ThreatConnect:

ThreatConnect provides solutions to enable cyber defenders to continuously manage threat exposure and improve cyber resilience. Our threat and risk-informed defense products give defenders the advantage over adversaries with rich context, risk-based prioritization, and the ability to quickly and precisely act on emerging threats. Our products span threat, risk, and security operations, and come together in a single intelligence hub. More than 250 global enterprises rely on ThreatConnect every day to contextualize and prioritize emerging threats and automate defenses.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240