CUSTOMER STORY

Filigran

Intrinsec’s enhanced cybersecurity operations with OpenCTI

Explore the transformative journey of Intrinsec in optimizing their threat intelligence offering & practices through the strategic adoption of OpenCTI. Witness how this collaboration allowed us to match the vision of the company to deliver high level services and implement operational advancements.

KEY RESULT

-65%

Investigation Time reduced

+3M

Entries to expand knowledge base

-25%

Estimated reduction in IoCs Redundancy

About Intrinsec

For 30 years, Intrinsec has established itself as a reliable partner and a benchmark in protecting against diverse cyber threats. Leveraging extensive comprehension of cybersecurity challenges, Intrinsec actively fosters the protection of organizations and preserving their business by proactively meeting the cybersecurity requirements.

With a large cybersecurity coverage, Intrinsec is a leading pure-player with recognized expertise in consulting, cyber assessments and operational security services (anticipation, detection and response).

Cyber Threat Intelligence has been a strategic development matter for Intrinsec since 2015: the company now provides Digital Risks Protection services, Threat Intelligence services & External Attack Surface Management to its customers – as standalone services or as a part of a Fusion Center model.

All the knowledge generated from these activities & the threat Intelligence research activity also lead the company to release their very own intelligence on external threats through their brand new CTI Feeds.

Context

Intrinsec integrated OpenCTI into their SOC service offering. This service involved monitoring all attacks on their clients and data centralizing. For each type of Indicator of Compromise (IoC), detection alerts were configured to identify their presence in the SIEM. This threat sharing platform became a pivotal component in feeding various SIEMs across their client base.

Over time, Intrinsec observed **an important shift in customer expectations and requirements**. Initially, clients mainly focused on achieving the quickest possible threat detection. However, as their understanding and sophistication in cybersecurity grew, their demand evolved. They began seeking a more in-depth and nuanced comprehension of the nature of threats, signaling a maturation in their cybersecurity approach and awareness.

The challenges

As cybersecurity threats have evolved, so have the needs for threat intelligence and response. Intrinsec, always at the forefront of cybersecurity defense, has been quick to recognize and adapt to these changes. They identified several key areas within their threat intelligence operations that needed enhancement:

RESPONSIVENESS AND PERFORMANCE ISSUES

Confronted with the task of managing large data volumes, Intrinsec knew the importance of a solution capable of efficient data handling. Especially when dealing with large events populated with a significant number of Indicators of Compromise (IoCs) and reports. The goal was to ensure swift and effective responsiveness to a constantly changing threat landscape.

SIMPLIFICATION AMIDST COMPLEXITY

Managing a diverse range of technologies in a dynamic human resources environment presented its own set of challenges. Intrinsec aimed to streamline operational maintenance, with a focus on preserving and enhancing the specialized knowledge within their team. This drive for simplification was essential not only in bolstering operational effectiveness and agility but also in ensuring the platform's accessibility for new users and organizations lacking specialized resources for management and maintenance.

DEMAND FOR A COMPREHENSIVE INTELLIGENCE PLATFORM

Intrinsec's strategy included the integration of a robust platform that could not only consolidate a wide array of external threats, from IoCs to attacker groups, but also provide a unified and comprehensive view of the intelligence. Such a platform would be instrumental in delivering a more cohesive and complete understanding of the cybersecurity threats faced.

Why OpenCTI?

OpenCTI stood out as the ideal solution for Intrinsec's evolving needs due to its array of advanced features:

VISUALIZATION

A key advantage of OpenCTI is its **dynamic dashboards**, offering expansive views of the threat landscape. These dashboards make it possible to visualize a wide array of data, from STIX objects to the industries, geographies, and nationalities affected by threats, greatly aiding in report generation.

INTEROPERABILITY

OpenCTI's design allows for **seamless integration with third-party systems**. Examples are the the native "CTI Feeds" connector, which facilitates easy and efficient data exchange as well as the Splunk connector, that allows bi-directional integration with the central SIEM environment.

DESIGN

The platform's user interface is particularly noted for its **intuitiveness** and **user-friendliness**, enhancing the user experience and operational efficiency.

AUTOMATION

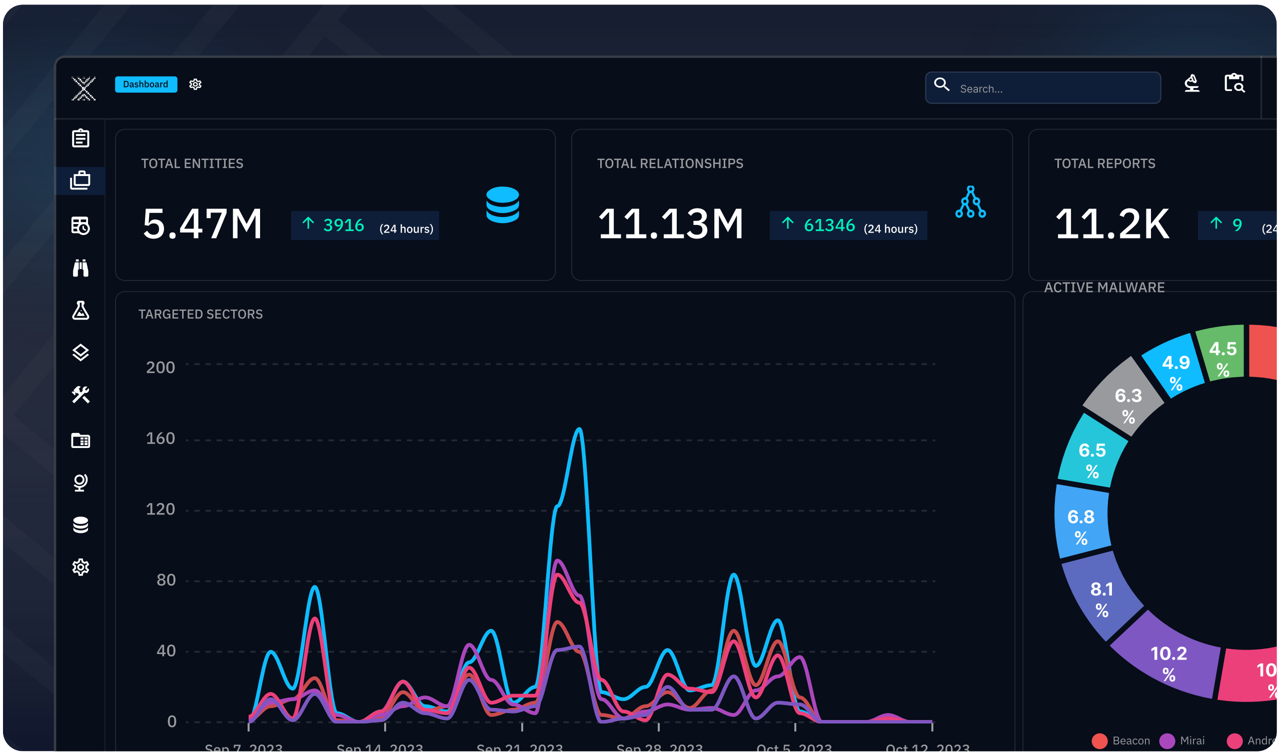
In OpenCTI, when IoCs or cases are integrated with related STIX objects, they automatically connect with other relevant elements. This level of **interconnectedness** offers a comprehensive and holistic view of the threat landscape, enhancing the overall **effectiveness of threat analysis and response**.

ADHERENCE TO THE STIX STANDARD

The systematic application of the STIX standard in OpenCTI streamlines data capitalization, making it more modular. This is evident in how OpenCTI **effectively manages relationships across various STIX objects**, including threat actors, campaigns, and IoCs.

INCIDENT RESPONSE IN CASE MANAGEMENT

The platform offers a comprehensive approach to managing incidents, allowing for in-depth analysis and effective response strategies. Additionally, OpenCTI's sophisticated correlation capabilities streamline complex threat analysis without necessitating additional scripting. This combination of features significantly **enhances the efficiency and efficacy of cybersecurity operations**, enabling teams to respond more swiftly and accurately.



TOTAL ENTITIES 5.47M ↑ 3916 (24 hours)

TOTAL RELATIONSHIPS 11.13M ↑ 61346 (24 hours)

TOTAL REPORTS 11.2K ↑ 9 (24

Adoption

SOC TEAM

Intrinsec's SOC (Security Operations Center) team has been significantly empowered by OpenCTI. The external threat knowledge base within OpenCTI, updated daily, provides their SOC analysts with a rich resource to speed-up the qualification process and enhance their investigation. This is particularly crucial when they encounter abnormal behaviors in the network, allowing for a more in-depth analysis.

CTI TEAM

Intrinsec's approach to Cyber Threat Intelligence (CTI) has been fundamentally shaped by the capabilities offered by OpenCTI. As the CTI team expanded, OpenCTI remained the tool of choice. The team has continuously refined their processes, customizing and adapting the platform to align with their evolving operational needs. This ongoing development of OpenCTI has cemented its role as an integral component of Intrinsec's CTI framework and lifecycle.

As a pioneer of the solution, Intrinsec was also able to promote OpenCTI to their customers wishing to benefit from a TIP for their own use. Their knowledge of both technological environment and variety of business functionalities has enabled them to offer high value-added support: best practices in architecture design, construction of specific business use cases, support in structuring of the cyber threat, etc.

Future outlook

Intrinsec's journey underscores a crucial imperative for organizations: the need to adapt and embrace tools that are not only responsive to current demands but are also capable of **anticipating and addressing future challenges**. In this context, OpenCTI has proven to be a significant asset for Intrinsec's teams, providing the versatility and comprehensive depth needed to navigate today's complex cyber landscape.

Looking ahead, Intrinsec has high expectations for the continued evolution of OpenCTI, particularly in terms of **new data streams and import connectors**. These developments are anticipated to significantly enhance Intrinsec's capability to efficiently deliver IOCs to their clients. This forward-thinking approach is aligned with Intrinsec's commitment to offering cutting-edge solutions and maintaining a proactive stance in cybersecurity defense.

Moreover, the need for correlations of different technical events (intrusion set, victimology, IOC, TTP, YARA rules, etc.) is a major challenge to make knowledge about cyber threats directly actionable (human & machine readable). Generative AI of reports and links between different events appears to be a growing need to structure and understand the threat landscape for different audiences (technical and strategic).

Key results

INVESTIGATION TIME REDUCED BY UP TO -65%

Intrinsec has realized a remarkable improvement in efficiency, with **investigation times reduced by half to two-thirds**. This significant reduction in time has led to **faster responses** and **more efficient analysis** in critical threat scenarios, enhancing their overall cybersecurity responsiveness.

KNOWLEDGE BASE EXPANDED TO OVER 3 MILLIONS ENTRIES

The substantial expansion of Intrinsec's knowledge base, **now exceeding 3 million entries**, underscores the vast scope of their intelligence repository. This growth significantly **strengthens their capabilities in threat intelligence and analysis**, equipping them with a richer resource for cybersecurity insights.

REDUCTION IN IOCS REDUNDANCY BY AN ESTIMATED 25%

The integration of OpenCTI has led to a significant reduction in feed redundancy, as **data aggregation and structuring are now centralized within a single platform**. This improvement allows for more effective comparison and detection of redundant information, enhancing the overall precision of their threat intelligence process.

ABOUT FILIGRAN

Filigran is a cybertech founded in 2022, providing open source cybersecurity solutions covering threat intelligence management, breach and attack simulation, and cyber risk management.

Filigran

contact@filigran.io | 𝕏

© Filigran 2024 All rights reserved.