FROST & SULLIVAN

CYCRAFT

REDUCING DIGITAL FORENSIC INVESTIGATION TIME WITH CYCRAFT'S CYCARRIER AIR PLATFORM

CyCraft's client was about to begin a critical acquisition. The CyCarrier AIR platform was able to shorten the pre-acquisition cybersecurity investigation from several months to just a few days, reducing investigation time by over 99%.

A Frost & Sullivan whitepaper commissioned by ITRI.

SUMMARY

CyCraft brings a comprehensive cybersecurity strategy to the table, building resilience through autonomous systems and human-AI collaboration powered by its flagship solution, the CyCarrier AIR platform.

The CyCarrier AIR platform automates SOC operations, forensics, detection and response operations for CyCraft's Fortune Global 500 and national government clients, performing managed detection and response (MDR), incident response (IR), threat hunting and accurate remediation. CyCarrier AIR collects endpoint evidence using the company's Xensor platform, conducts automated correlation and behavior analysis, and validates threats with its global threat intelligence platform, CyberTotal. Altogether, CyCraft's primary objective is to bring ROI-efficient cyber resilience solutions to the global stage.

CyCraft is one of the 21 vendors selected to join the second MITRE ATT&CK evaluation against APT 29, Cozy Bear. The CyCarrier AIR platform was designed specifically to defend against advanced persistent threats like Cozy Bear by leveraging ensemble machine learning techniques to classify sophisticated adversarial behavior according to the MITRE ATT&CK framework, enabling defenders to thoroughly understand malicious actions and generate a clear remediation plan in under 60 minutes from first alert.

CASE STUDY

The Client: One of the world's top four leading fabless semiconductor companies specializing in chipsets for wireless telecommunication and consumer technology, with over USD $7.7 billion in annual revenue and over 25 global branches.

Challenge:

In 2018, the Client was preparing for a strategic acquisition to expand its operations. As part of this endeavor, the Client began the process of conducting an exhaustive cybersecurity due-diligence investigation on the acquisition target in a bid to arm itself against the looming threat of supply chain attacks. In the acquisition and merger process, the Client inherited a large volume of legacy IT from the target company and had to formulate a strategy around incorporating it into their pre-existing systems. Before the merger, the Client would have had to first complete the task of doing a thorough pre-acquisition security investigation, which would have required the resources of their entire cybersecurity team as well as several months of diagnosing their existing IT systems to uncover all possible blind spots.

Solution:

The Client decided to bring in CyCraft's CyCarrier AIR platform security defense solution to perform security due diligence on the acquisition target. The primary intention of this service was to investigate and check the cybersecurity conditions of target company before proceeding with the complex, risk-heavy integration.

Results:

With the aid of CyCraft's CyCarrier AIR platform, the Client was able to shorten the pre-acquisition investigation from several months to just a few days, reducing investigation time by over 99%. The efficiencies gained included cost and man-hour reductions of over 95%, especially since the previously-planned team of technical experts was no longer required, and neither was the otherwise arduous and error-prone investigation process. CyCraft's CyCarrier AIR platform further helped smoothen the transition of integrating acquisition infrastructure into the Client's systems, allowing the process to successfully complete within a fraction of the originally estimated time. As testimony to this platform's proven benefits, the Client has continued using CyCraft's solution as a key inbuilt cybersecurity solution even after the successful completion of this acquisition.

BACKGROUND

CyCraft focuses on AI-driven next-gen cyber resilience.

Powered by deep learning, adversarial and reinforcement learning, the company's proprietary artificial intelligence engines enable customers and partners to rapidly perform intelligent security threat analysis on a scalable, user-friendly platform. In 2019, the company established the CyCraft AI Lab, creating a new artificial intelligence engine with a driverless model built on a framework of intelligent security and defense.

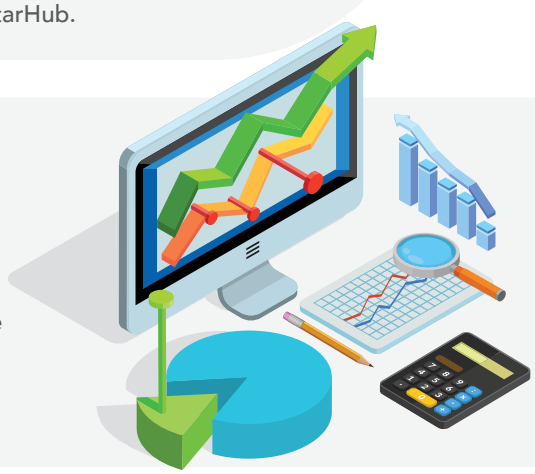
CyCraft ensures cyber resilience for sectors like government, finance, tech, semiconductor, and healthcare, with their next-gen AI-driven security operations: managed detection and response (MDR), threat hunting, cyber threat intelligence (CTI), and incidence response (IR).

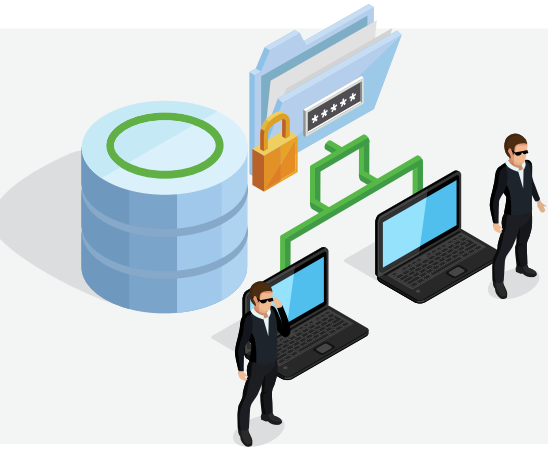
SCALE

With recurring revenue to the tune of over USD $7 million within its domestic base of Taiwan, CyCraft has also seen steady momentum with its growth in overseas markets. With a growing customer footprint in the APAC regions of Japan and Singapore, CyCraft also set up its first international office in Japan in 2019 and is also slated to establish a branch in Singapore soon. CyCraft's reach is enhanced by its partnership with Ensign InfoSecurity, a pure-play cybersecurity service firm that is a joint venture between Temasek Holdings and StarHub.

TYPE

CyCraft's top four target verticals are banking, financial services and insurance (BFSI), the public sector, and manufacturing, and telecommunications. Other compatible verticals are critical infrastructure providers: energy, water, and electricity vendors.





UNIQUE DOMAIN EXPERTISE

While CyCraft's competitors offer a partial view into their customers' cybersecurity environments, CyCraft offers an end-to-end forensic view and leverages that view into fully actionable response capabilities. Competing vendors still require humans to conduct effective investigation processes, which is where CyCraft asserts its market leadership: it's AI-led security process shortens investigation timelines from days to minutes – sometimes even seconds.

PRODUCT SUITE

01 XENSOR

(Next-generation MDR Endpoint Security System)

Combining machine learning with unique forensic telemetry technology, Xensor provides highly efficient automated threat triaging and remote endpoint access for incident investigation and threat hunting. Xensor integrates multidimensional threat intelligence including UEBA, program memory forensics, endpoint computer forensics, and network traffic analysis. The strategic combination of these features allows this platform to expediently respond to threats and reduce security costs.

02 CYCARRIER

(AI-driven Security Operations Center)

Although traditional MSSPs/SOCs can quickly generate alerts, dealing with false positives and the ensuing security investigations, especially root cause analysis, is inefficient, resource-draining, and slow. Multiplied by the dearth of cybersecurity talent - homegrown or hired - they struggle to keep pace with the rapid evolution of hackers.

With the CyCarrier platform, CyCraft has created an advanced AI-Driven Cybersecurity Situation Center. This is a hybrid solution that combines the company's patented AI analyst resources with teams of skilled security experts, providing continuous security analysis.

Using the full endpoint dataset as an integrated unit allows MSSP/SOC teams to execute remote forensics with cockpit-style visualizations and controls. This makes it easy and efficient to ascertain security threats within the enterprise, and to automatically analyze case situations within an innovative AI and evidence-based environment. The company's virtual agent houses contextual inference capabilities that can automatically generate malware association maps (file comparisons), program behavior association diagrams (call graphs), attack context charts (lateral movement) and intrusion case timing diagrams (storylines), to elevate MSSPs/SOCs to the next level.

03 CYBERTOTAL

(Global Threat Intelligence Platform)

Sharing threat intel and related security information has become an important early action mechanism to prevent and respond to attacks; however, traditional Cybersecurity Threat Intelligence (CTI) is dominated by exchanging static blacklists of IPs, domains, and MD5s, lacking higher-level attacker intelligence.

CyCraft's Cyber Intel team has extensively tracked various forms of intrusion, provided historical information on APT groups, and brought together various global threat intelligence information sources. The company channels these sources of high-quality threat intel into helping companies identify, verify and respond to threats immediately through AI automated correlation analysis and knowledge base optimization.

AWARDS AND RECOGNITION

Ministry of Science and Technology

"10 Most Innovative Taiwan Tech Startups of 2019"

MITRE ATT&CK 2019 Evaluations

"Selected to Join Round 2 of the MITRE ATT&CK Evaluations"

For more information, please visit https://www.cycraft.com/