DATA SHEET

CYCRAFT MDR

Fully managed endpoint detection and response (MDR) made F / A / S / T by the combined power of CyCraft experts and technology

CYCRAFT MANAGED DETECTION AND RESPONSE

CyCraft MDR is uniquely designed to detect malicious behavior and continuously monitor and manage the cyber situation of even large-scale enterprises with thousands of endpoints; however, unlike other services, we generate fully actionable reports, walk you through them step-by-step, rescan and confirm eradication of threats.

Through leveraging our frontline experience with both active and emerging threats, as well as their techniques, tactics, procedures, and behavior profiles, we've successfully assisted our customers in expanding visibility into their current cyber situation, preventing critical security incidents, conducting thorough digital forensic analyses, and accelerating maturity in long-term security solutions.

BE 100% SURE YOUR SOC IS EFFECTIVE AGAINST EMERGING THREATS

SOC teams operate in a highly painful and stressful environment. Pain points can slow down and harm effectiveness, potentially putting the entire organization at risk. Alleviating pain points is paramount for any organization. Mid-size and small organizations have more budget and resource constraints than large organizations do, leaving SOC teams lower on priority, less funded, and suffering from more pain.

The solution? Automated investigations. CyCraft MDR performs the heavy lifting and automates monitoring, threat triage, investigations, and response, providing SOC teams with an efficient, data-driven workflow without guesswork. CyCraft MDR is an affordable and effective solution regardless of the size of your environment.

OUR DELIVERABLES

Your clear, concise, and fully actionable reports cover everything you need to know to get back to business.

- Full storylines of any & all malicious activity
- True, system-wide root cause analysis
- Malicious domain, IP, URL analysis
- Alert triage automation and ranking
- Malware analysis
- Graphs of all affect nodes and executions
- A step-by-step plan for eradication
- Eradication confirmation
- Up-to-date Global Cyber Threat Intelligence
- MITRE ATT&CK mapping & more

F / A / S / T SECURITY F / A / S / T BENEFITS

Fast

Our thorough lightweight agent continuously detects, eradicates, and remediates issues, drastically reducing your MTTD and MTTR to prevent security incidents from evolving into business-altering events—all provided by the collaboration between our expert analysts, virtual forensic analyst AI, and our attacker-behavior modeling technology.

Accurate

We provide automated forensic analyses not just across multiple levels of contexts but also into the intricate relationships between each of those levels of context.

Simple

Receive regular in-depth reports on the current state of your entire network. Our CyCraft MDR Services Team is available to walk you through your fully-actionable reports step by step, explaining each step simply and clearly.

Thorough

We rescan and confirm eradication with cyber threat intel from multiple major proprietary sources and organizations across the globe, as well as the rigorous AI-driven vetting process of CyberTotal.

THE CYCRAFT DIFFERENCE

CyCraft MDR leverages patented AI-driven technology that provides real-time detection and response capable of detecting active and emerging threats.

▸Automated Investigations

CyCraft MDR automates forensic investigations, scanning every endpoint, process, file, or identity and access management (IAM) across your entire network. Moments after an initial high-severity alert triggers the automated investigation, CyCraft MDR delivers a full site-wide forensic analysis, performed by CyCraft AI and our team of experienced human security analysts.

▸Rapid Response

CyCraft MDR goes from detection to actionable report in under 20 minutes. Your auto-generated report not only links each step of the attack together but also includes the full context behind each step of the attack. Your actionable report informs you which processes to stop, which files to delete, which malware to remove, which user accounts were infected and need resetting, and which URLs, IP addresses, and domains to block.

▸Proactive Threat Hunting

CyberTotal, our global cyber threat intelligence platform, combined with CyCraft MDR's automated investigations means automated proactive threat hunting capabilities for your SOC. CyCraft MDR uniquely provides the visibility, contextual intelligence, and rapid response necessary to take your SOC on the offensive, reducing risk to your enterprise.

CYCRAFT MDR EXPERIENCE

"CyCraft has a deep understanding of information security and top-tier technology to prove it."
—INFORMATION TECHNOLOGY SERVICES

"CyCraft' s AI-driven managed detection and response, automated forensics, and security visualization showed us the key points and enterprise-wide root cause of all attacks, as well as greatly reduced our investigation time."
—TELECOMMUNICATION

ABOUT CYCRAFT SERVICES

CyCraft Services provides organizations worldwide with the innovative AI-driven technology necessary to stop cyber threats in the 2020s. CyCraft technology is uniquely designed to detect the latest trends in malicious behavior, automate investigations, and auto-triage alerts, allowing CyCraft customers to detect, track, contain, and eradicate threats in near real-time.

Learn more at www.cycraft.com/services/compromise-assessment or email us: engage@cycraft.com

YOUR THREATS COVERED

Spear Phishing

Socially-engineered attacks effectively target your staff. While typically emails and texts, this now includes voice/audio deepfakes, with video deepfakes now on the horizon.

Financial

Threat groups target not just your business' s financials but also your customers'. This includes payment card data theft and ransomware.

Ransomware

Attackers can copy, exfiltrate, and delete your sensitive data in seconds. Ransomware attacks are rapidly increasing in frequency, severity, and complexity.

Intellectual Property Theft

Sophisticated state-sponsored attacks are known to target trade secrets, proprietary product IP, and other sensitive information.

Supply Chain Attacks

Threat groups target less secure elements in your supply chain to infiltrate your environment and exfiltrate or destroy sensitive data.

Insider Threats

Insider threats can instantly bypass layers of security and are launched by people within your organization, former employees, contractors, partners, or business associates.