DATA SHEET

CYCRAFT

INCIDENT RESPONSE AND FAST FORENSIC SERVICES

Detect, contain, eradicate, and remediate from security incidents F / A / S / T
Fast / Accurate / Simple / Thorough

CYCRAFT INCIDENT RESPONSE

The CyCraft IR Services team has been at the frontlines of cybersecurity and cyber threat intelligence protecting government agencies, Global Fortune 500 firms, and critical infrastructure from the most sophisticated of cyberattacks.

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 multinational organizations in investigating critical security incidents, conducting thorough digital forensic analyses, and accelerating maturity in long-term security solutions.

In under 1 day after our scanner runs, you receive fully-actionable eradication and remediation reports, explained to you step-by-step by our CyCraft IR Services team. We rescan and confirm eradication with cyber threat intel from multiple major proprietary sources across the globe, as well as the rigorous AI-driven vetting process of CyberTotal.

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
- 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

YOUR KEY THREATS COVERED

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

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.

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.

Step 1
Deploy our IR forensic scanner to your endpoints.

Step 2
We receive the scanner data & our AI & experts analyze it.

Step 3
We generate a plan & execute it with you.

Step 4
Together we rescan & confirm eradication.

F / A / S / T SECURITY

FAST
Under 1 day after our scanner runs, you receive your actionable eradication plan with complete site-wide hacker tools and behavior analysis.

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

SIMPLE
Our CyCraft IR Services Team takes you through your fully-actionable eradication plan, 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.

CUSTOMER EXPERIENCE

"CyCraft's customer support provided excellent communication, incident reports, and response times, leaving us confident and at ease with our security situation."
— Telecommunications, Security Analyst

BRIDGING THE GAP

Is your network air-gapped or segmented? Not a problem. CyCraft IR & Fast Forensic Services can run investigations on-site and guarantees data privacy and zero data leakage. Your sensitive data never goes to the cloud.

	ON-PREM	NOT ON-PREM
IMMEDIATE RESPONSE	✓	✓
LICENSE POOL	✓	✓

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.

THOROUGH IR

CyCraft IR & Fast Forensic Services is the only IR service with the expertise and technology to leverage automated intelligent forensics to analyze security incidents across 7 levels of context to ensure your environment is thoroughly clean and back to healthy.

Level 7
Virtual Forensic Analyst Context: CyCraft leverages AI-behavioral automation of investigative methods to combine all of the below levels into a final analysis, gaining you a full understanding of your cybersecurity situation.

Level 6
Global Threat Intelligence Context: After thoroughly vetting global threat intel, CyCraft IR Services correlates it with behaviors and artifacts found at the lower levels.

Level 5
Org-Wide Context: Link together evidence found across the lower levels of context and examine them in the context of the entire organization.

Level 4
User Context: Examine user behaviors, successful logins & failed attempts.

Level 3
Isolated Artifact Context: a packet, an execution, a memory segment, or log file entry are among the many examples of isolated artifacts.

Level 2
Network Context: Examine the connections between systems in terms of the various protocols and behavioral purposes of the connections.

Level 1
Endpoint Context: Forensically scan the endpoint event logs, memory, startup files, processes, and more.

Suspect an incident? Engage with CyCraft at engage@cycraft.com or visit www.cycraft.com/services/incident-response