CYCRAFT

INCIDENT RESPONSE

DETECT, CONTAIN, ERADICATE SECURITY INCIDENTS F/A/S/T

Fast / Accurate / Simple / Thorough

WHAT IS CYCRAFT IR?

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 rapidly closing critical security incidents, by 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.

CYBER DEFENSE MATRIX

	Identify	Protect	Detect	Respond	Recover
Devices	■		■	■	
Applications	■		■	■	
Networks	■		■	■	
Data					
Users	■		■	■	

CRITICAL DELIVERABLES

CyCraft IR includes everything you need to understand and eradicate an APT-level security incident rapidly:

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

> *"The most impressive feature is FAST. An incident once occurred, and it took about half a day for CyCraft to inspect 4,000+ endpoints, saving us a lot of time and workforce costs on investigation."*
>
> Associate Executive VP,
> Security and Risk Management
> Banking, 30B+

READY FOR A DEMO?

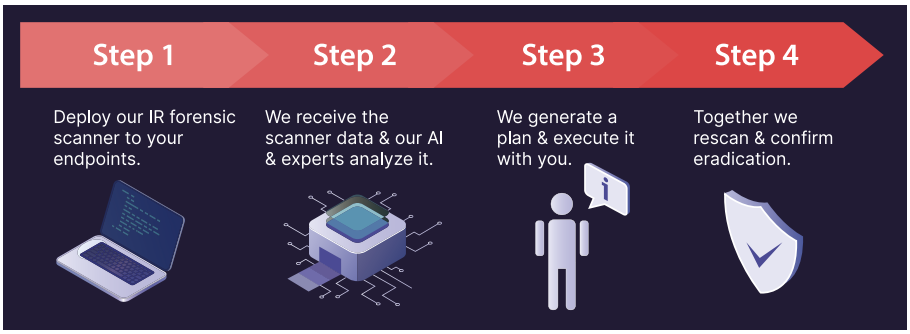
Visit **CyCraft.com**

About CyCraft

CyCraft 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.

engage@cycraft.com

HOW DOES IT WORK?



1. We provide automated forensic analysis not just across multiple levels of context (including isolated artifacts, network, memory/processes, system files, behavioral relationships, and global threat intelligence) but also analysis of the intricate relationships between each of those levels of context.
2. Our CyCraft IR Services Team takes you through your fully-actionable eradication plan, explaining each step simply and clearly.
3. We rescan and confirm eradication to see that the threat has been mitigated and to check if there have been other developments during the remediation process

EASE OF USE

- On-prem IR available through our partners
- Rapidly deploy across hybrid OS environments

WHAT SETS CYCRAFT APART?

Unlike other incident response services, CyCraft is battle-tested against the toughest APTs; provides enriched global threat intelligence on active and emerging threats; has been validated by the MITRE ATT&CK Evaluations; enhances your cybersecurity resilience through proprietary advancements in digital forensic artificial intelligence.

CYCRAFT MEETS GDPR & JAPAN PRIVACY LAWS

- We collect far less data than Windows
- We don't collect payment data, presentation files, messaging/email contents, or anything that would violate GDPR/Privacy laws
- In fact, we aid in GDPR/Privacy law compliance:
  - We stop attackers from stealing your data
  - We enable quicker reporting to meet compliance

CYCRAFT ADVANTAGE

CyCraft partners with your team to develop an impactful and thorough response, remediation, and eradication that takes into account all your operational needs as well as any existing investments and resources. We work with you to develop a uniquely customized action plan that balances both the business and security needs of your company.

WHY IT MATTERS

URGENT PAIN RESOLVED

Know What Happened
Understand the scope of the incident including all affected assets, attacker activities, timeline of events, with MITRE ATT&CK-mapping and CyberTotal threat intelligence analysis.

Know What to Do
Know what to block on the network, what to delete and quarantine file-wise, and which user accounts may have been abused.

FAST
Do the above as quickly, thoroughly, and accurately as possible.

BENEFITS TO CUSTOMERS + PARTNERS

Speed
By leveraging proprietary advances in automated forensics, CyCraft IR services give you the fastest opportunity to get back to a good state.

Reduced Impact from events coming from rapid handling of incidents and certainty as to what happened in incidents.

Site-Wide Understanding of events including root cause analysis and how the threat moved across the organization over time.

Talk to a Human
We have responsive and reactive human analyst support to immediately relieve any friction in the IR process.

Optionally opt for CyCraft Managed or Endpoint detection and response to see that this type of incident never happens again.