CYCRAFT

RISK INTELLIGENCE
GAIN VISIBILITY INTO UNKNOWN THREATS & DISRUPT ATTACKS BEFORE THEY DISRUPT YOU

WHAT IS RiskINT?

Risk no longer exists solely within your digital environment. Every day, adversaries on the dark web are buying and selling credentials and intelligence on potential targets. It's only a matter of time before your intel is leveraged against you. Risk Intelligence (RiskINT) provides granular visibility into your leaked accounts, passwords, and documents located on the dark web as well as phishing domains targeting your enterprise. Enhance your proactive defense capabilities and gain the time necessary to prepare an effective defense.

CYBER DEFENSE MATRIX

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

CRITICAL DELIVERABLES

	RiskINT Lite	RiskINT Pro	RiskINT Premium
Report Content	10 entries for leaked credentials and domains for sale on the deep and/or dark web	100% of entries + proactive phishing domain intelligence	100% of entries + phishing domains + leaked docs + pricing on leaked accounts + frequency of data being sold

Each RiskINT report has six sections:

> **Cumulative risk** over time interval scanned
> **Analyst notes:** Analyst insight into your external risk situation
> **Dark web risk:** Credentials sold on the dark web
> **Data exposure risk:** Sensitive documents that have been leaked
> **Credentials from third party:** Track credential leaks on third-party services
> **Phishing domain risk:** Recently registered domains that may be used to phish your org as rated by CyberTotal, CyCraft's threat intelligence platform

> *CyCraft's customer support provided excellent communication, reports, and response times, leaving us confident and at ease with our security situation.*

Telecommunications, Security Analyst

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.
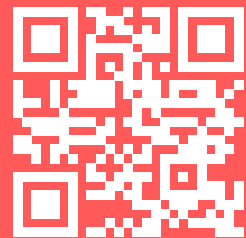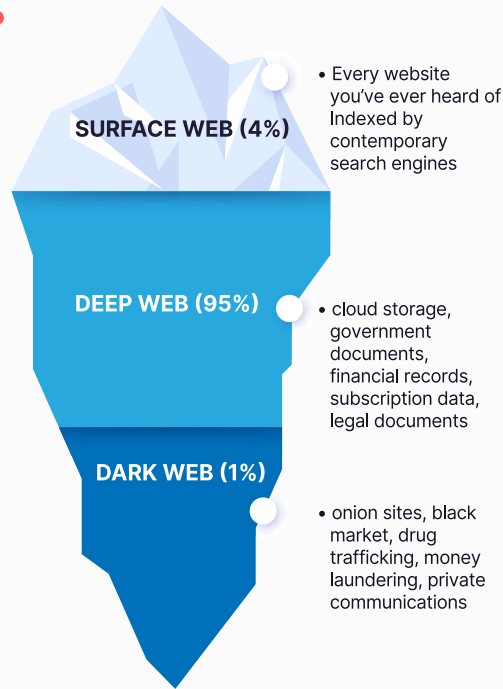
engage@cycraft.com

CYCRAFT

HOW DOES IT WORK?

CyCraft RiskINT reporting is generated by automated and manual collection and analyses of deep and dark web data as well as phishing domain discovery analysis combined with CyberTotal's threat intelligence for severity ranking.

You receive reports based on your subscription tier and then work with our analysts to understand and take action on the risks brought to light by RiskINT reporting.

SURFACE WEB (4%)
- Every website you've ever heard of Indexed by contemporary search engines

DEEP WEB (95%)
- cloud storage, government documents, financial records, subscription data, legal documents

DARK WEB (1%)
- onion sites, black market, drug trafficking, money laundering, private communications

EASE OF USE

> No installation, deployment, or maintenance necessary
> Automatically receive fully-featured deep/dark and phishing threat reporting
> See total cumulative threats over the time interval to get a quick, clear snapshot of your external threat risk

WHAT SETS CYCRAFT APART?

Unlike other threat intel vendors, instead of making you comb through the deep and dark web or through a threat intelligence platform and painstakingly assemble your external threat picture, RiskINT automates that process to give you immediate, clear, and easy to use results.

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

> **Gain direct visibility** into your leaked accounts, passwords, and documents located on the dark web so you can take action to mitigate those threat vectors

> **Discover** if your password policy has been leaked so you can maintain strong authentication and authorization in your organization

> **Acquire a fuller picture** of your entire attack surface by locating risky phishing domains targeting your enterprise

BENEFITS TO CUSTOMERS + PARTNERS

> **No more manual data collection** Automated reporting of salient discoveries that are ever-changing and hard to get on the deep and dark web

> **Available yearly, quarterly or monthly** depending on need

> **Uncover trends** and patterns in sensitive information attackers have on your org

> **Discover what attackers know about you**, and what industrial spies have access to so you can triage your business risk and take action

> **Prevent business email compromise** by proactively blocking high-risk phishing domains

> *Based on their up-to-date cyber threat intelligence, CyCraft is able to not only identify if and how the latest vulnerability impacts us but also check if the potential threat has been properly mitigated.*

Analyst
Transportation Services,
Aviation industry
(50M - 250M USD)