DeTCT® BY CYFIRMA

DeTCT®

Your business needs at be in peak performance 24x7. Do not let digital risk derail you. Take control of your cyber risk and thrive in the digital ecosystem. DeTCT is your essential digital risk discovery and protection platform working tirelessly to monitor hidden attack surfaces, vulnerable systems, leaked data, executive impersonation, brand infringement, and validating your patch and vulnerability processes so your cyber posture stays strong in the face of emerging threats.

DeTCT gives you full visibility to your digital footprint like no other.

DeTCT is the only fully automated, proactive monitoring service what works 24x7 to help you stay on top of rising cyber threats.

- Attack Surface Monitoring
- Impersonation and Infringement
- Data Breach Monitoring
- Social and Public Exposure Monitoring
- Third-Party Cyber Risk Monitoring

DeTCT gives you actionable insights so you can prioritize remedial actions.

Built to protect your brand and digital assets while enabling innovation.

- Every threat indicator comes with a risk score so you can assess its impact to your business
- Recommended remedial actions are provided to help you stem data leaks and breaches
- Dashboards with Risk and Hackability scores allow you to monitor progress over time

DeTCT is designed to help leaders mitigate the rising digital risk so they can focus on building a thriving business

CEO/CFO
How do I quantify the risks and gaps to my senior stakeholder/Board to get support for cyber initiatives? Is my business facing any threats? What do I need to focus and priortise on?

Business and Marketing Team
Is my brand under any risk of attack or being attacked? Any infringement or impersonation that could impact stakeholder' trust and erode my customers' loyalty?

IT Team
Do I have full view of my attack surface? What are my most critical vulnerabilities? Are my processes around patch and vulnerability management, and policy compliance effective? What do I need to do to enhance my security controls?

Attack Surface Monitoring

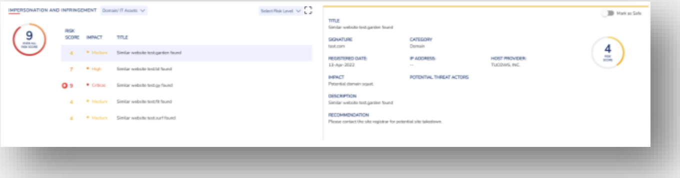
DeTCT monitors your attack surface so you would never be blindsided

- Domain/IP Vulnerability
- Certificate Weaknesses
- Configuration: DNS/SMTP/HTTP
- IP/Domain Reputation
- Open Ports
- Cloud Weakness

Impersonation and Infringement

DeTCT scans deep/dark/surface web and social media to look to signs of impersonation and infringement

- Domain/IP Assets
- Executive/People
- Product/Solution
- Social Handlers



Data Breach Monitoring

DeTCT brings to your attention to data which has been stolen and available for sale in underground marketplaces. This includes data which has been exfiltrated by ransomware groups.

- Emails/Identities/Credentials
- Leaks
- Dark Web
- Phishing
- Ransomware

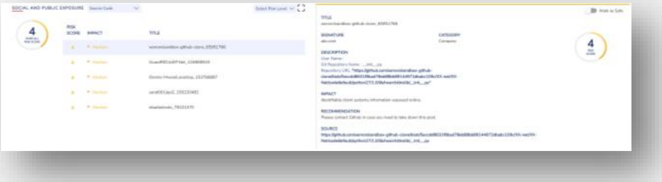
DATA BREACH AND WEB MONITORING

USER NAME	EMAIL	PASSWORD	NAME	PASSHASH	SOURCE	COMMENTS/NOTES	MARK AS SAFE
[illegible]	[illegible]	–	–	[illegible]	[illegible]	test	
[illegible]	[illegible]	–	[illegible]	[illegible]	[illegible]	test	
[illegible]	[illegible]	–	–	[illegible]	[illegible]	test	
[illegible]	[illegible]	••••••	–	–	Collections	test	
[illegible]	[illegible]	–	–	[illegible]	[illegible]	test	

Social and Public Exposures

With DeTCT, you would always know if your IP or confidential data has been exposed, including lookalike or malicious apps. You will also receive alerts on social sentiments that could present a threat to you or your business

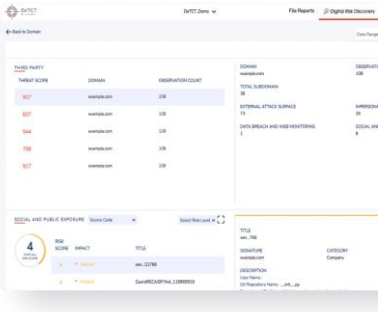
- Source Code
- Confidential Files
- PII/CII Dumps
- Malicious Mobile Apps
- Social Threat



Third-Party Risk Monitoring

DeTCT secures your digital ecosystem and gives you visibility to third-party cyber risk

- Discover weaknesses of your suppliers' digital assets
- Be alerted to their data leaks and exposures which could impact you
- Receive recommended remedial actions to help strengthen your suppliers' cyber posture
- Keep your company and people safe from cyberattacks



KEY FEATURE	DESCRIPTION	BENEFITS
ATTACK SURFACE DISCOVERY	▪ Proactively identify exposed external assets, shadow IT, and forgotten systems which can be exploited by cybercriminals. ▪ Build an effective and efficient attack surface management program with continuous monitoring capabilities.	▪ Regain control by having visibility to your external-facing assets and start looking at reducing your attack surface to protect the business ▪ Awareness of attack surfaces helps you identify a potential path of attack, and you can take steps to reduce and mitigate risk.
VULNERABILITIES EXPOSED	▪ Strengthen vulnerability management programs by continuous monitoring to identify weaknesses in your external assets. ▪ Understand how cybercriminals are looking at exploiting your vulnerabilities. ▪ Devise certificate management program by identifying weak, vulnerable certificates hosted on your external assets.	▪ Improve your vulnerability management program by knowing the risks and threats which need to be tackled urgently. ▪ Prioritize patch management program and remediation. ▪ Close security gaps quickly before further damage occurs.
DATA BREACH MONITORING	▪ Real-time detection of intellectual property, personal data or financial information which have been leaked. ▪ Background info, description and impact for each breach and exposure is provided.	▪ Know if and when your data has been leaked. ▪ Ensure employees, business partners and third-party contractors have not inadvertently shared sensitive information which could subject the company to cyberattacks and risks. ▪ Awareness of emails and credentials which have been compromised allows you to take action to protect your business from phishing and other social engineering attacks. ▪ Ensure your IP and trade secrets are not exposed. ▪ Ensure you are in compliance with regulatory policies. ▪ Avoid having to manage negative media in the event of a data breach or cyberattack.
DARK WEB EXPOSURE	▪ Gives you visibility into hacker conversations and suspected fraudulent activities from dark web. ▪ Uncover email ID and credentials, PII/CII data, and other sensitive information that on sale in underground forums and marketplaces.	▪ Be the first to know that your data has been exposed. ▪ Take swift actions such as closing specific network ports, resetting passwords and credentials to reduce the ramifications.
SOCIAL MEDIA AND PUBLIC EXPOSURE	▪ Continuous monitoring for spoof and lookalike domain and subdomains. ▪ DeTCT picks up newly registered domains as well as malicious domains. ▪ Uncover fake social media profiles of company and its executives (LinkedIn, Facebook and Twitter).	▪ Foil social engineering and phishing campaigns that masquerade as company executives or company profile. ▪ Sensitive data that has been leaked, either intentionally or accidentally, can be used by threat actors to launch an attack. Ability to detect these leaks allow you to take corrective actions and prevent a major attack.
IMPERSONATION AND INFRINGEMENT	▪ Identify cases of infringement, impersonation related to brand, product, solution, and people. ▪ These are threat indicators pointing to potential phishing campaigns.	▪ Reduce the risk of your brand, products and solutions being copied. ▪ Protect your brand integrity. Avert business disruptions from phishing and social engineering attacks that could erode stakeholder's trust and impact business viability. ▪ Protect your executives from being impersonated online and in social media platforms.
THIRD-PARTY RISK DISCOVERY AND MONITORING	▪ We help you monitor your 3rd party using their domains, no need for complex and intrusive implementations. ▪ Map out their digital risk profile and gain awareness on whether they have suffered any data leaks, vulnerabilities exposed, and more	▪ Secure your digital ecosystem and gain visibility to 3rd-party cyber risk. ▪ Discover weaknesses in your supplier's digital assets. ▪ Be aware of 3rd party's cyber risk posture and understand how it could impact you.
RISK AND HACKABIITY SCORES	▪ Get a quick view into your risk and hackability scores and understand how they trend over time. ▪ Risk rating is scored using the FAIR (Factor Analysis of Information Risk) framework and provided for each threat indicator or exposure.	▪ Gain insights into your risk posture so you can take actions to mitigate threats that could cause business disruption. ▪ Understand your overall digital risk status from an organization perspective.
RECOMMENDED REMEDIATION	▪ Recommended remedial actions are provided for each associated risk and exposure so teams can swing into action quickly.	▪ Triage quickly and decisively with clear and prioritized actions. ▪ Activate the right resources to close security gaps.

ABOUT CYFIRMA

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver predictive, personalized, contextual, outside-in, and multi-layered insights. We harness our cloud-based AI and ML-powered analytics platform to help organizations proactively identify potential threats at the planning stage of cyberattacks. Our unique approach of providing the hacker's view and deep insights into the external cyber landscape has helped clients prepare for upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices located across APAC, US and EU.

Official websites:
https://www.cyfirma.com/ https://www.cyfirma.jp/