DeTCT BY CYFIRMA

DATA SHEET

DeTCT™

DeTCT is a **digital risk** discovery and protection platform empowering businesses with real-time digital footprint discovery to reveal attack surfaces, vulnerable systems, data leaks, brand infringement and executive impersonation. DeTCT **proactively monitors** the dark web, surface web and social media platforms 24/7 so you can focus on growing your business.

From social engineering campaigns to ransomware and software supply chain attacks, there are now more pathways than ever for cybercriminals to get hold of your sensitive data such as intellectual property, customer and financial information and put your business at risk.

Do you have visibility to all your external facing IT assets?
Do you know if your systems and applications are vulnerable?
Are your software patches up to date?
Are you a target for phishing campaigns?
Has your data been leaked?
Is your brand under attack?
Is your sensitive information on public or social platforms?
Do you know the exact steps to take to remediate your vulnerabilities?

DeTCT will answer all the questions above. Designed to address the rising digital risk so you are always aware of your digital footprint, data leaks, breaches, and impersonation, DeTCT monitors your digital profile continuously and provide you real-time visibility to your risk posture.

Armed with full knowledge, you can confidently implement the right remedial actions to protect your business.

DeTCT is designed specifically to address the rising digital risk faced by the following leaders:

CEO/CFO
"What is my risk status? Is my business facing any threats? Am I complying with regulations and policies?"

Business and Marketing Team
"Is my brand under attack? Any infringement or impersonation that could impact stakeholders' trust?"

IT Team
"Do I have full view of my attack surface? What are my most critical vulnerabilities? What do I need to do to enhance my security controls?"

1

ATTACK SURFACE DISCOVERY

Identify 'doors' and 'windows' into the organization

Business Outcome: Real-time continuous monitoring to identify shadow IT or porous systems which can be accessed by cybercriminals. **Awareness of attack surface will allow you to conduct a realistic cost-benefit analysis of each asset and decide how to shrink your attack surface.**

2

VULNERABILITY INTELLIGENCE

Keys to 'doors' and 'windows' that are available for cyber criminals to exploit

Business Outcome: Vulnerabilities are mapped to assets and associated exploits and ranked based on criticality. **This allows the business to optimize resources to focus on the most important and urgent gaps.**

3

BRAND INTELLIGENCE

Know when your brand is under attack

Business Outcome: Understand who, why and how your brand is being targeted, get complete view of brand infringement. **Protect the brand and retain customer loyalty by ensuring it is not being tarnished by corporate espionage, insider threats or other malicious bad actors.**

4

DIGITAL RISK PROTECTION

Clarity on digital profile, data leaks, breaches, and impersonations

Business Outcome: Unveil digital footprints and cases of impersonation and data leaks. Get near real-time alert on your data leaked in the wild. **With this knowledge, you can plug the gap and avert any further reputation and financial damage.**

5

3RD PARTY RISK DISCOVERY AND MONITORING

Discover weaknesses in your supplier's digital assets.

Business Outcome: Map out their digital risk profile and gain awareness on whether they have suffered any data leaks, vulnerabilities exposed, and more. **Be aware of 3rd party's cyber risk posture and understand how it could impact you.**

© CYFIRMA 2022, ALL RIGHTS ARE RESERVED.

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.

© CYFIRMA 2022, ALL RIGHTS ARE RESERVED.

KNOW YOUR ATTACK SURFACE

Understand your digital footprint and external risk profile

Identify hacker-exposed client assets such as domain, sub-domain, IP address range, software versions, vulnerabilities, and more.

IMPERSONATION AND INFRINGEMENT

Identify all online entities that are masquerading your business digital profile, assets, products, brand based on the domain name provided.

DATA BREACH MONITORING

A holistic look into data breaches that can lead to exfiltration of critical data from your IT systems.

THRID-PARTY MONITORING

Secure your digital ecosystem and gain visibility to 3rd-party cyber risk. Discover weaknesses in your supplier's digital assets and understand how they could impact you.

SOCIAL AND PUBLIC EXPOSURE

Ability to identify look-alike domains, handlers, logo, public information exposure from surface web and social media.

DARK WEB EXPOSURE

Provides you visibility into hacker conversations and suspected fraudulent activities from dark web for any match of domain provided and ancillary info such as email ID, PII/CII data, and many more.

VULNERABILITIES EXPOSURE

Based on domain name provided, list flaws in asset design that could create potential security compromise.

Look out for these digital risks

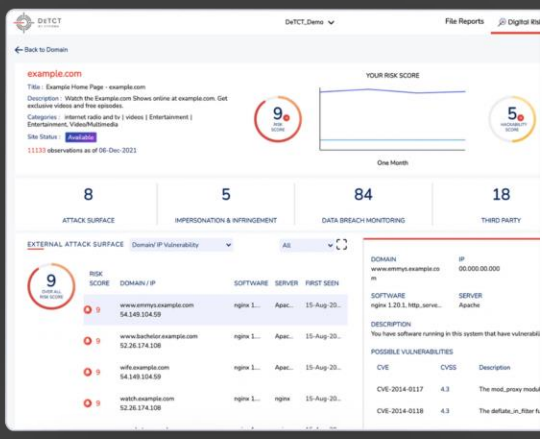
- Fake identities of your C-suite executives – these can be fake social media profiles, fake email IDs. These are signs of potential phishing campaigns where hackers would impersonate persons of authority to trick employees into clicking malicious emails.
- Look-alike domains and websites – created to deceive users into believing fake content or divulging personal/financial information.
- Your IP addresses, employee credentials, CII/PII are mentioned and thrown into hackers' forums, dark web, bin sites. This means hackers have found a way to breach your defences and have exfiltrated important data.

© CYFIRMA 2022, ALL RIGHTS ARE RESERVED.

DeTCT AUTOMATICALLY DISCOV
DIGITAL FOOTPRINT LIKE NO O

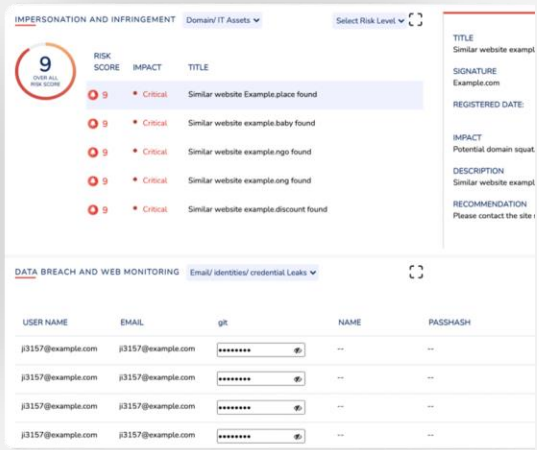
DeTCT is the only proactive service doi laims. It's fully automated,
d your 24/7 digital dete by eliminating blind spots

- tack surface
- Dark Web Exposure
- nd Inf
- Social & Public Exposure
- Vu



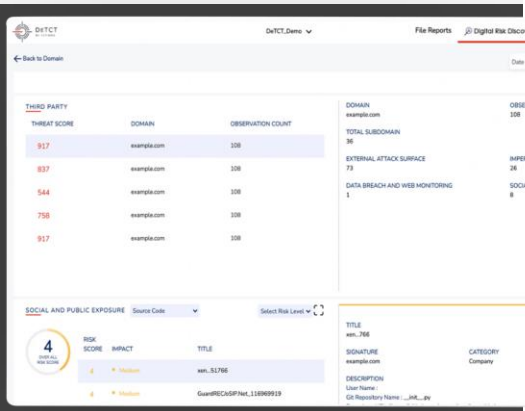
DeTCT PR MONITORS THE DARK WEB,
SURFACE AL MEDIA PLATFORMS 24/7

- Take remedial a s to stem data leaks and breaches
- Dashboards with quick Risk and Hackability scores, including trends to monitor progress over time
- Details of brand, domain, etc, impersonation with risk scores and impact analysis



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



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 in USA, Japan, Singapore, EU and India.

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

© CYFIRMA 2022, ALL RIGHTS ARE RESERVED.