Digital Risk Monitoring

Take control of your digital footprint

Your organization needs protection against cyber-crime 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 and brand infringement, 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 leading fully automated, proactive monitoring service what works 24x7 to help you stay on top of rising cyber threats.

- Attack Surface Monitoring
- Vulnerability Intelligence
- 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 at all levels of the organization mitigate the rising threat of digital risk so they can focus on building and supporting a thriving business

CEO/CFO

How do I quantify the digital exposure of my organization? What are the threats? What are the steps and investment needed to improve our risk posture. How do I ensure the Board is fully aware and engaged?

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 customer's affiliation and loyalty?

IT Team

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

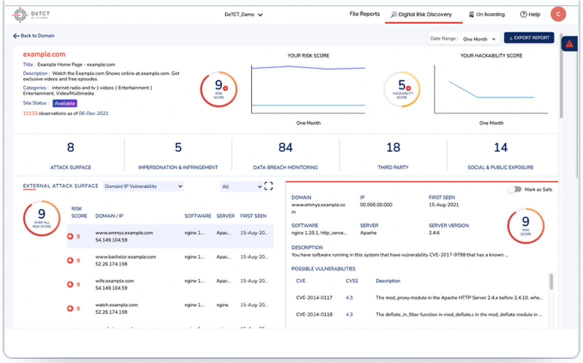
KEY FEATURE	DETAILS	BENEFITS
ATTACK SURFACE DISCOVERY	▪ Proactively identify exposed external assets, shadow IT, and forgotten systems which can be exploited by cybercriminals. ▪ Build an effective and efficient attack surface management program with continuous monitoring capabilities. ▪ Real time alerts on configuration weaknesses of your assets or certificates.	▪ Regain control and visibility in to your external-facing assets and start looking at reducing your attack surface weaknesses. ▪ Awareness of attack surfaces helps organizations identify a potential path of attack, so steps can be taken to reduce and mitigate risk.
VULNERABILITIES EXPOSED	▪ Strengthen vulnerability management programs by continuously monitoring weaknesses in your external assets. ▪ Understand how cybercriminals are looking at exploiting your vulnerabilities. ▪ Identify weak, vulnerable certificates hosted on your external assets.	▪ Improved vulnerability management program prioritizing the risks and threats which need to be mitigated urgently. ▪ Prioritized patch management program focusing on contextual exposure remediation. ▪ Close security gaps quickly before potential damage occurs.
DATA BREACH MONITORING	▪ Real-time detection of exposed intellectual property, personal data or financial information. ▪ Background information, description and impact for each breach and exposure.	▪ Know if and when your data has been leaked. ▪ Understand and action 3rd party supplier data exposure ▪ Proactively protect against email and credential leaks impacting users and business operations. ▪ Maintain compliance with regulatory policies in the event of a data breach. ▪ Proactively manage negative media in the event of a data breach.
DARK WEB EXPOSURE	▪ Provides visibility into hacker conversations and suspected criminal activities from deep/dark web. ▪ Understand if your stolen credentials or data has been sold or actively being sold in underground forums and marketplaces.	▪ Early warning notification that your data has been exposed. ▪ Actionable recommendations to mitigate the exposure such as resetting passwords and credentials.
SOCIAL MEDIA AND PUBLIC EXPOSURE	▪ Continuous monitoring for spoof and lookalike accounts - fake social media profiles of the organization or executive stakeholders (LinkedIn, Facebook and Twitter). ▪ Understand publicly accessible data and chatter about your organization.	▪ Stop social engineering and phishing campaigns that masquerade as company executives or company profile. ▪ Understand the public sources where you company is being discussed or information shared.
IMPERSONATION AND INFRINGEMENT	▪ Identify cases of infringement and impersonation related to brand, product, solution, and people. ▪ Identify potential targets for social engineering, phishing campaigns and typo-squatting. ▪ Understand threat actors behind the impersonation/infringement.	▪ Reduce the risk of your brand, products and solutions being copied. ▪ Protect your brand against phishing and social engineering attacks that could erode stakeholder's trust, affiliation and loyalty. ▪ Protect your executives from being impersonated online and in social media platforms.
THIRD-PARTY RISK DISCOVERY AND MONITORING	▪ Monitor 3rd party / partners using their domains and key information - no need for intrusive implementations. ▪ Understand the digital risk profile and gain awareness on whether they have suffered any data leaks, vulnerabilities exposed, etc.	▪ Reinforce your digital ecosystem by gaining visibility to 3rd party cyber risk. ▪ Discover weaknesses in your supplier's digital assets and understand how this can impact you. ▪ Refine/ influence procurement procedures / partner agreement process (vendor cyber hygiene score).
RISK AND HACKABIITY SCORES	▪ Snapshot view into your risk and hackability scores and monitor 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.	▪ Quantify your digital risk posture to drive conversations with stakeholders. ▪ Understand your overall digital risk status from an organization-wide perspective.
RECOMMENDED REMEDIATION	▪ Contextualized remedial actions provided for each associated risk and exposure to enable teams to action quickly.	▪ Triage risks quickly and decisively with clear and prioritized actions. ▪ Activate the right resources at the right time to close security gaps.

Actionable Insights

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



example.com
Title : Example Home Page - example.com
Description : Watch the Example.com Shows online at example.com. Get exclusive videos and free episodes.
Categories : internet radio and tv | videos | Entertainment | Entertainment, Video/Multimedia
Site Status : Available
11133 observations as of 06-Dec-2021

8	5	84	18	14
ATTACK SURFACE	IMPERSONATION & INFRINGEMENT	DATA BREACH MONITORING	THIRD PARTY	SOCIAL & PUBLIC EXPOSURE

EXTERNAL ATTACK SURFACE Domain/ IP Vulnerability All

RISK SCORE	DOMAIN / IP	SOFTWARE	SERVER	FIRST SEEN
9	www.emmys.example.com 54.149.104.59	nginx 1...	Apac...	15-Aug-20...
9	www.bachelor.example.com 52.26.174.108	nginx 1...	Apac...	15-Aug-20...
9	wife.example.com 54.149.104.59	nginx 1...	Apac...	15-Aug-20...
9	watch.example.com 52.26.174.108	nginx 1...	nginx	15-Aug-20...

Mark as Safe

DOMAIN
www.emmys.example.com

IP
00.000.00.000

FIRST SEEN
15-Aug-2021

SOFTWARE
nginx 1.20.1, http_serve...

SERVER
Apache

SERVER VERSION
2.4.6

DESCRIPTION
You have software running in this system that have vulnerability CVE-2017-9798 that has a known ...

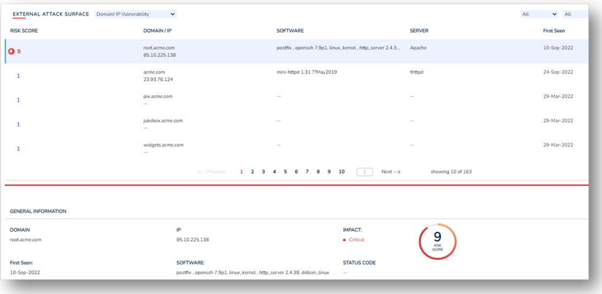
POSSIBLE VULNERABILITIES

CVE	CVSS	Description
CVE-2014-0117	4.3	The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, whe...
CVE-2014-0118	4.3	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in ...

Attack Surface Monitoring

Real-time continuous monitoring of your external attack surface to identify risks associated with patch vulnerability, misconfiguration and shadow IT that could be compromised by cybercriminals. Gain awareness so you can decide how to reduce your attack surface

- ❖ Domain Vulnerabilities
- ❖ Certificate Weaknesses
- ❖ Configuration Weaknesses (DNS/SMTP/HTTP)
- ❖ Open Ports
- ❖ IP/Domain Reputation
- ❖ Cloud Weaknesses



EXTERNAL ATTACK SURFACE Domain/ IP Vulnerability All All

RISK SCORE	DOMAIN / IP	SOFTWARE	SERVER	First Seen
9	root.acme.com 85.10.225.138	postfix , openssh 7.9p1, linux_kernel , http_server 2.4.3...	Apache	10-Sep-2022
1	acme.com 23.93.76.124	mini-httpd 1.31 ??May2019	thttpd	24-Sep-2022
1	pix.acme.com --	--	--	29-Mar-2022
1	jukebox.acme.com --	--	--	29-Mar-2022
1	widgets.acme.com --	--	--	29-Mar-2022

showing 10 of 163

GENERAL INFORMATION

DOMAIN
root.acme.com

IP
85.10.225.138

IMPACT:
● Critical

First Seen:
10-Sep-2022

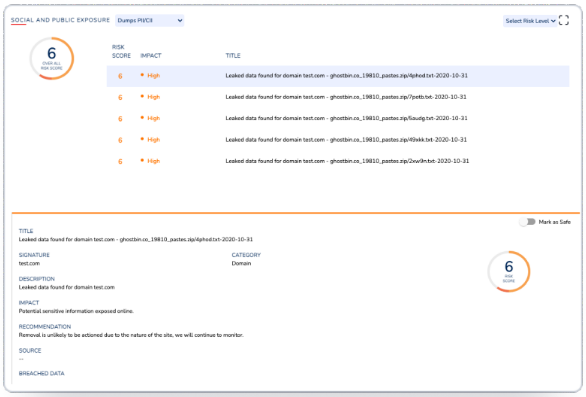
SOFTWARE:
postfix , openssh 7.9p1, linux_kernel , http_server 2.4.38, debian_linux

STATUS CODE
--

Social and Public Exposure

Sensitive data that has been leaked can be used by threat actors to plan and launch an attack. Detect these leaks, take corrective actions and prevent a successful attack

- ❖ Look alike social handlers
- ❖ Malicious Mobile Apps
- ❖ Negative Social Sentiments



SOCIAL AND PUBLIC EXPOSURE Dumps PII/CII Select Risk Level

RISK SCORE	IMPACT	TITLE
6	● High	Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/4phod.txt-2020-10-31
6	● High	Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/7potb.txt-2020-10-31
6	● High	Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/5audg.txt-2020-10-31
6	● High	Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/49xkk.txt-2020-10-31
6	● High	Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/2xw9n.txt-2020-10-31

Mark as Safe

TITLE
Leaked data found for domain test.com - ghostbin.co_19810_pastes.zip/4phod.txt-2020-10-31

SIGNATURE
test.com

CATEGORY
Domain

DESCRIPTION
Leaked data found for domain test.com

IMPACT
Potential sensitive information exposed online.

RECOMMENDATION
Removal is unlikely to be actioned due to the nature of the site, we will continue to monitor.

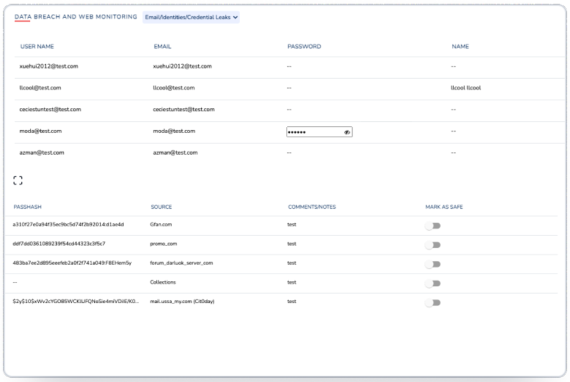
SOURCE
--

BREACHED DATA

Digital Risk Protection & Real-time Data Breach Monitoring

Pinpoint digital exposure and ensure your IP or trade secrets are not at risk. With real-time alerts on your data leaked in the wild, you can plug the gap and minimize impact to compliance, reputational and financial damage

- ❖ Emails, identities, credential leaks
- ❖ Intellectual Property leaks
- ❖ Personal data exposure
- ❖ Database exposure
- ❖ Financial Leaks and Carding



DATA BREACH AND WEB MONITORING Email/Identities/Credential Leaks

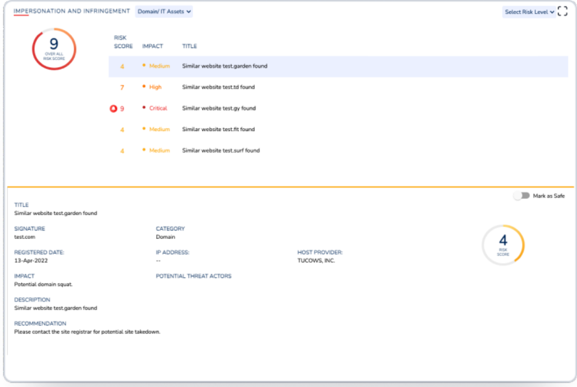
USER NAME	EMAIL	PASSWORD	NAME
xuehui2012@test.com	xuehui2012@test.com	--	--
llcool@test.com	llcool@test.com	--	llcool llcool
ceciestuntest@test.com	ceciestuntest@test.com	--	--
moda@test.com	moda@test.com	••••••	--
azman@test.com	azman@test.com	--	--

PASSHASH	SOURCE	COMMENTS/NOTES	MARK AS SAFE
a310f27e0a94f35ec9bc5d74f2b92014:d1ae4d	Gfan.com	test	
ddf7dd0361089239f54cd44323c3f5c7	promo_com	test	
483ba7ee2d895eeefeb2a0f2f741a049:F8EHem5y	forum_darluok_server_com	test	
--	Collections	test	
$2y$10$xWv2cYGOB5WCKlUFQNoSie4miVDiIE/K0...	mail.ussa_my.com (Cit0day)	test	

Impersonation & Infringement

Identify cases of Infringement, impersonation related to your brand, product, solution and people.

- ❖ Reduce the risk of your brand, products and solutions being copied or leveraged by threat actors
- ❖ Protect your brand integrity and reduce the impact to brand affiliation and customer loyalty
- ❖ Protect your executives from fake personas and deep fake manipulation



RISK SCORE	IMPACT	TITLE
4	• Medium	Similar website test.garden found
7	• High	Similar website test.td found
9	• Critical	Similar website test.gy found
4	• Medium	Similar website test.fit found
4	• Medium	Similar website test.surf found

TITLE
Similar website test.garden found

SIGNATURE
test.com

CATEGORY
Domain

REGISTERED DATE:
13-Apr-2022

IP ADDRESS:
--

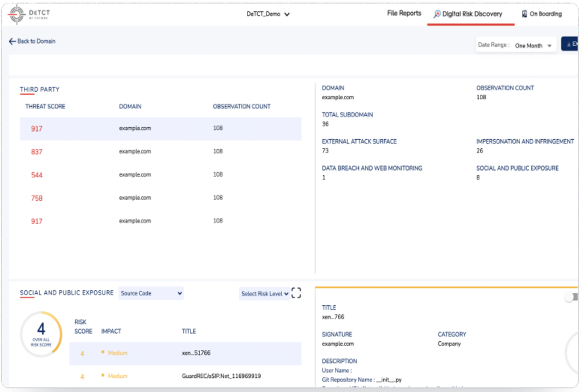
HOST PROVIDER:
TUCOWS, INC.

IMPACT
Potential domain squat.

POTENTIAL THREAT ACTORS

DESCRIPTION
Similar website test.garden found

RECOMMENDATION
Please contact the site registrar for potential site takedown.



THIRD PARTY

THREAT SCORE	DOMAIN	OBSERVATION COUNT
917	example.com	108
837	example.com	108
544	example.com	108
758	example.com	108
917	example.com	108

DOMAIN
example.com

OBSERVATION COUNT
108

TOTAL SUBDOMAIN
36

EXTERNAL ATTACK SURFACE
73

IMPERSONATION AND INFRINGEMENT
26

DATA BREACH AND WEB MONITORING
1

SOCIAL AND PUBLIC EXPOSURE
8

RISK SCORE	IMPACT	TITLE
4	• Medium	xen..51766
4	• Medium	GuardREC/oSIP.Net_116969919

TITLE
xen..766

SIGNATURE
example.com

CATEGORY
Company

DESCRIPTION
User Name :
Git Repository Name : __init__.py

Third-Party Risk Monitoring

Gain powerful insights in to your third-party's digital risk profile. Ensure these trusted partners have not inadvertently shared sensitive information or been compromised, which could subject your company to downstream cyberattacks and risks

- ❖ Discover weaknesses of your suppliers' digital assets
- ❖ Be alerted to any data leaks and exposures which could impact you
- ❖ Receive recommended remedial actions to help strengthen your suppliers' cyber posture

Thrive in Today's Digital World
Protect Your Business From Cyber-threats

Join the many businesses who are already using DeTCT to secure their digital assets.
Sign up today to start your free trial.
https://www.cyfirma.com/detct/

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, EMEA and the US.

CYFIRMA
DECODING THREATS

www.cyfirma.com