

External Threat Landscape Management

Predictive intelligence to stay ahead of cybercriminals

At CYFIRMA, we are redefining cyber-intelligence with the world's first external threat landscape management platform built to give defenders the view through their adversaries' lens so they can take actions before an attack occurs.

Security Strategies Need an Agile Approach

- ❖ Inward-looking security offerings, which fail to understand and correlate to the external threats
- ❖ Work in a reactive fashion & identify security gaps post-attack
- ❖ Events-focused security controls; lack of a holistic view of all the threats
- ❖ Creates pressure to take unplanned, immediate & costly remedial actions
- ❖ Massive tech spends on silo-offerings and unable to avert a data breach or attack
- ❖ Cybersecurity initiatives receive limited support at Executive and Board levels

Cybersecurity Challenges

- ❖ Not knowing if you are already being targeted by adversaries
- ❖ Rapid digitalization and changing technology landscape results in security tools are not optimized or configured to manage emerging threats
- ❖ Complex and time-consuming cybersecurity system configurations
- ❖ Limited knowledge of forgotten and shadow IT
- ❖ Drowning in cyber security data and starved of actionable insights that really matter
- ❖ Uptrend in cyber-crimes (like malware/ ransomware) with no contextual details on the nature of the attacks
- ❖ Nascent understanding of the new-age digital and brand risks (including 3rd party, supply chain)

The Solution - External Threat Landscape Management Platform

The solution lies in the ability to gain visibility into the external threat landscape, continuously monitor for emerging threats, harness predictive intelligence to proactively take actions to mitigate risks and avert an impending attack. DeCYFIR provide 6 threat views on a single pane of glass to uncover imminent attacks.

PREDICTIVE | PERSONALIZED | OUTSIDE-IN | CONTEXTUAL | MULTI-LAYERED



Attack Surface Discovery

Discover external-facing assets, process and technology weaknesses that can be exploited by hackers



Vulnerability Intelligence

Threat-led vulnerability enrichment based on changing external cyber environment. Reprioritization of identified vulnerabilities based on cybercriminals' interest, attribution and association to present a comprehensive threat story



Brand Intelligence

Monitor brand, product, solutions & service, executive infringement; and connect them with ongoing cybercrime campaigns



Digital Risk Discovery

Dark web, deep web, surface web and social media monitoring for data and identities leaks, confidential files, source code, sensitive information exposure, impersonation of domain, and much more



Situational Awareness

Understand cyber trends & threats specific to client's industry, technology & geos



Cyber- Intelligence

Predictive, personalized, contextual, outside-in and multi-layered cyber intelligence that address the who, why, what, when & how of a cyberattack. Equipped yourself with actionable and prioritized remediations



KEY FEATURE






DESCRIPTION



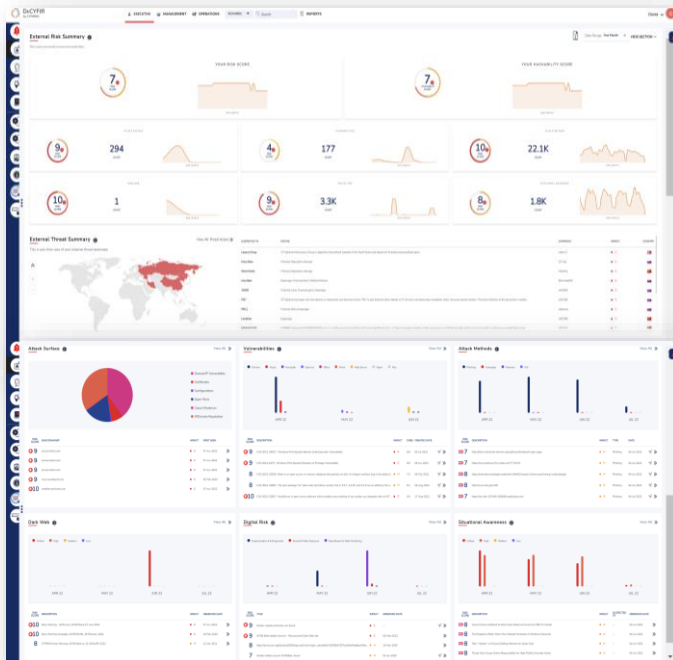
BENEFITS

PREDICTIVE	Predict impending cyber-attack targeting your organization and subsidiaries before cybercriminals can cause harm to your business.	Early warnings and alerts to help you quantify risk and prepare for impending cyberattacks.
PERSONALIZED	Insights are tailored to match the technology you are using, industry you are operating in and your geolocation.	Remove noise and reduce false positives to ensure the high impact alerts are actioned upon.
CONTEXTUAL	Comprehensive details of the external threat including adversary details, TTPs and related IoC. Insights include assessing if an IoC is malicious, its location details, what it is being used for e.g. C&C, the path and method of attack, malicious hosting site, affiliated cybercrime campaign, and more.	Give deep understanding of cyber threats so as to mount effective defence strategies. Help the business understand the evolving threat landscape, and its impact on them.
CYBER-INTELLIGENCE	Detailed insights into your external threat landscape - who are the cybercriminals interested in you, their motivation, what do they want from you, when can they attack and how are they going to attack, the tools and techniques they can use.	Comprehensive outside-in view to ensure cyber-defenders are not blind-sided and can take appropriate proactive action to align their cybersecurity strategy and capabilities.
ATTACK SURFACE DISCOVERY	Identify external assets and potential points of exploits such as shadow IT, forgotten IT, misconfigurations, leaky cloud buckets, vulnerable certificates.	Gain awareness of your external-facing assets which can be exploited by cybercriminals, and with this insight, identify ways to shrink your attack surface to reduce and mitigate risk.
VULNERABILITY INTELLIGENCE	Identify weakness into your software and external assets, understand how cybercriminals are looking at exploiting the identified vulnerabilities.	Optimize resources to focus on the most important and urgent gaps. Prioritise patch & vulnerability management programs and remediation.
BRAND INTELLIGENCE	Identify cases of infringement, impersonation related to brand, product, solution, and people.	Reduce the risk to your brand, products and solutions.
SITUATIONAL AWARENESS	Understand trends and new threats in your industry, technology stack you are using and geography where you are operating.	Provide insights which can guide important business decision including cyber investment.

		
KEY FEATURE	DESCRIPTION	BENEFITS
DIGITAL RISK PROTECTION	Proactively identify data leaks, breaches, executive impersonation, brand/product infringement, and more.	Reduce digital blind-spots and risk of cybercriminals hurting your brand and avert any further reputation and financial damage.
TAILORED DASHBOARD	3-Layered Dashboards <ul style="list-style-type: none"> Executive View is a risk-based approach meant for Executives to quickly understand external risk exposure and the probability of being hacked Management View is the guided approach on systematic remediation process Operational View presents you with technical details of findings and remediation 	<ul style="list-style-type: none"> Executive view – Help leaders allocate resources to be line with company strategy Management view – Guide security leaders on the path to take to manage remediation effectively Operations view – Focus on current indicators and specific actions needed
HEURISTIC SEARCH	Search capability helps you to search for threats, cyber-attacks, breaches, threat actors, malware, and phishing campaigns from a single platform.	Instantly address pressing indicators related to external threats.
RISK DOSSIER	Risk dossier showing correlation to IOCs, vulnerabilities, attack surface, digital risk, and more.	<ul style="list-style-type: none"> Enable you to quickly obtain holistic view of your threat landscape – e.g., how a vulnerability could be exploited via specific campaign, and the cybercriminals behind it. Understand impact on your assets and provide a comprehensive threat story.
ALERT CENTRE	Tailored alert center to understand what is the most important threats and risks to your organization.	Help you to quickly prioritize remedial actions.
TAKEDOWN SERVICES	We offer take down services for look-alike / scamming domain or websites, social media pages, removal of sensitive data on public forums and sites (conditional to site owner's action).	We manage the entire process end-to-end - drafting of legal documents, email and correspondence, and blacklisting.
INTEGRATION WITH SECURITY CONTROLS	You can integrate the insights using STIX and TAXII-compliant APIs into your security controls.	Enrich the data to strengthen cyber posture management.
INCIDENT ANALYTICS	Incident analytics using DeCYFIR' s intelligence hunting capability to provide complete contextual details.	Speed up incident response with incident analytics including analysis of external threat landscape.
THIRD-PARTY RISK DISCOVERY AND MONITORING	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Secure your digital ecosystem and gain visibility of 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

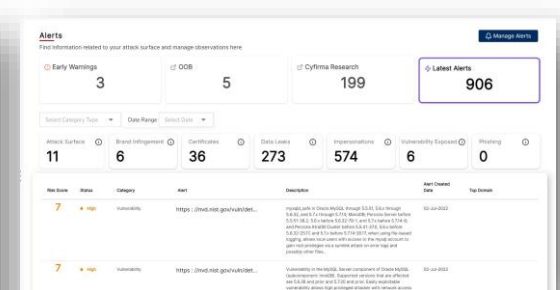
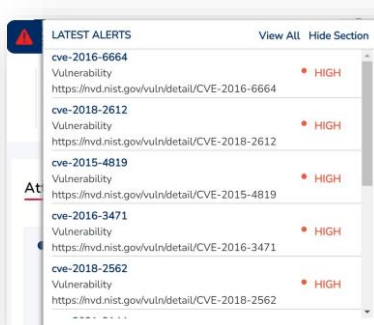
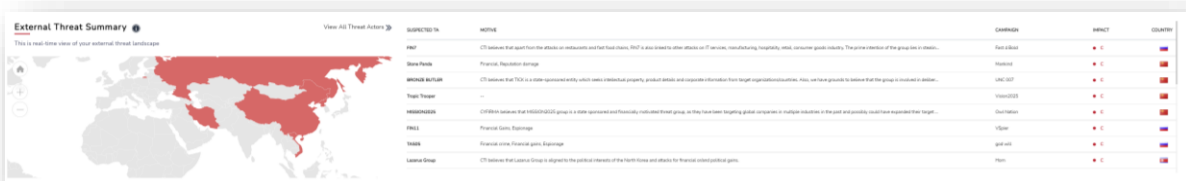
EXECUTIVE VIEW

DeCYFIR's dashboard is a decision tool for executive leadership helping them understand the shifting dynamics and accelerate critical decision-making.



Cyber Intelligence (Predictive, personalized, multi-layered, contextualised intelligence)

- Deep-analysis of a cyberattack campaign to answer WHO, WHY, WHAT, WHEN, HOW of a cyberattack campaign in the making
- Attribution and correlation between hackers, campaigns, motives, methods
- Keep the enemy at bay, receive early warning alerts to fend off cyberattacks to avoid disruption that could threaten business
- Dashboards for Executives to understand risk postures and trends with risk and hackability scores



MANAGEMENT VIEW

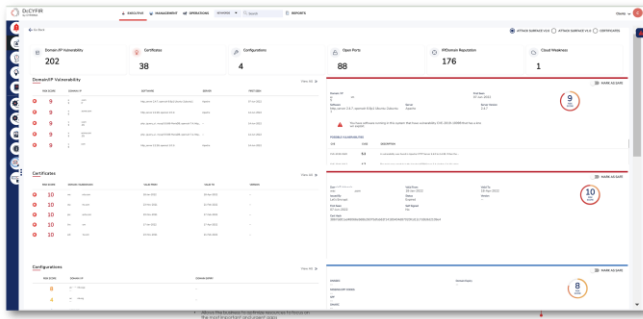
The best-practice systematic approach for security management that facilitates risk mitigation with step-by-step guidance. DeCYFIR methodically uncover attack surfaces, vulnerabilities, attack methods, digital risk exposures, dark web observations, and provide situational awareness.

Take swift actions to mitigate risk with step-by-step guidance

Systematically uncover:

- Attack surface
- Vulnerabilities
- Attack methods
- Digital risk exposures
- Dark web observations
- Situation awareness

1 IDENTIFY ATTACK SURFACE



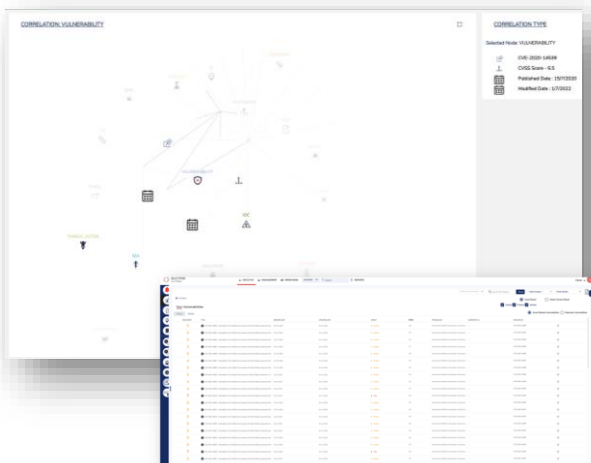
IDENTIFY ATTACKERS' POTENTIAL ENTRY POINTS

Attack Surface Discovery

(Identify doors and windows into the organization)

- Real-time and continuous monitoring to identify shadow IT or porous systems which can be accessed by cybercriminals
- Awareness of external-facing assets which can be exploited by cybercriminals such as domain, sub-domain, IP address range, software versions, vulnerabilities, and more, which are exposed to hackers
- Help client obtain a full view of attacker-exposed assets, consult methods and evaluate

2 DISCOVER VULNERABILITIES



SECURITY LEADERS BECOME PROACTIVE RISK ADVISORS RATHER THAN REACTIVE

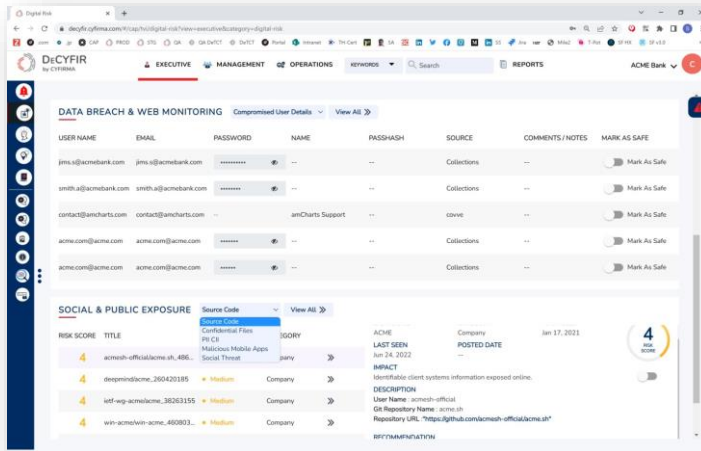
Vulnerability Intelligence

(Keys to doors and windows that are available for cybercriminals to exploit)

- Vulnerabilities are mapped to assets and associated exploits and ranked based on criticality
- Allows the business to optimize resources to focus on the most important and urgent gaps
- Help client see from cyber-attacker's point of view
- Understand weakness and potential points of compromise
- Vulnerability intelligence can be used to build threat models and security planning

3 DIGITAL RISK PROFILING

ENHANCE SECURITY TELEMETRY WITH DEEPER INSIGHTS INTO EXPOSURES AND POTENTIAL ATTACKS



USER NAME	EMAIL	PASSWORD	NAME	PASSHASH	SOURCE	COMMENTS / NOTES	MARK AS SAFE
jmsu@acmebank.com	jmsu@acmebank.com	*****	---	---	Collections	---	Mark As Safe
smith.a@acmebank.com	smith.a@acmebank.com	*****	---	---	Collections	---	Mark As Safe
contact@ancharts.com	contact@ancharts.com	---	ancharts Support	---	ovwe	---	Mark As Safe
acme.com@acme.com	acme.com@acme.com	*****	---	---	Collections	---	Mark As Safe
acme.com@acme.com	acme.com@acme.com	*****	---	---	Collections	---	Mark As Safe

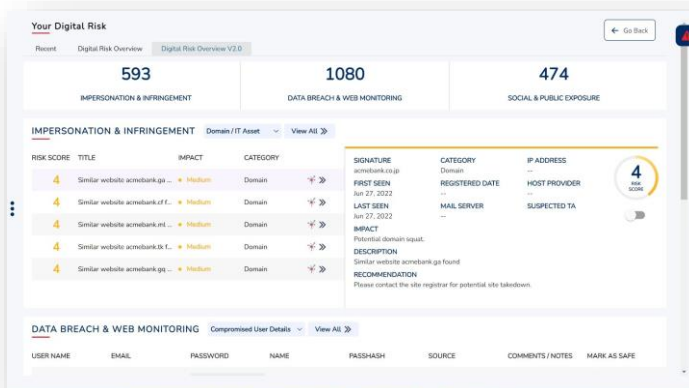
RISK SCORE	TITLE	SOURCE	ISORY	ACHIE	LAST SEEN	POSTED DATE	Jan 17, 2021
4	acme-official@acme.sh_486...	Confidential From	PI/CI	ISORY	Jun 24, 2022	---	4
4	deepmind@acme_260420135	Malicious Mobile Apps	Social Threat	Company	---	---	4
4	wtf-wp-acme@acme_38263155	Medium	Company	Company	---	---	4
4	win-acme@acme_460803...	Medium	Company	Company	---	---	4

Digital Risk Profiling (Clarity on digital profile)

- Unveil digital footprints and cases of impersonation to provide clarity on data leaks, breaches, and more across deep/dark/surface web and social media platforms
- Get near real-time alert on your data leaked in wild
- Enable clients to plug the gap and avert any further reputation and financial damage

4 BRAND INTELLIGENCE

AI ENGINES UNCOVER EVIDENCE INDICATING CYBER RISK AND ATTACKS TARGETING YOU



Your Digital Risk	
Recent	Digital Risk Overview V2.0
593	1080
IMPERSONATION & INFRINGEMENT	DATA BREACH & WEB MONITORING
474	SOCIAL & PUBLIC EXPOSURE

RISK SCORE	TITLE	IMPACT	CATEGORY	SIGNATURE	CATEGORY	IP ADDRESS
4	Similar website acmebank.ga...	Medium	Domain	acmebank.co.jp	Domain	---
4	Similar website acmebank.f...	Medium	Domain	---	REGISTERED DATE	HOST PROVIDER
4	Similar website acmebank.nl...	Medium	Domain	---	MAIL SERVER	SUSPECTED TA
4	Similar website acmebank.tk...	Medium	Domain	---	---	---
4	Similar website acmebank.ga...	Medium	Domain	---	---	---

Brand Intelligence (Know when your brand is under attack)

- Understand who, why and how your brand is being targeted, get complete view 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

5

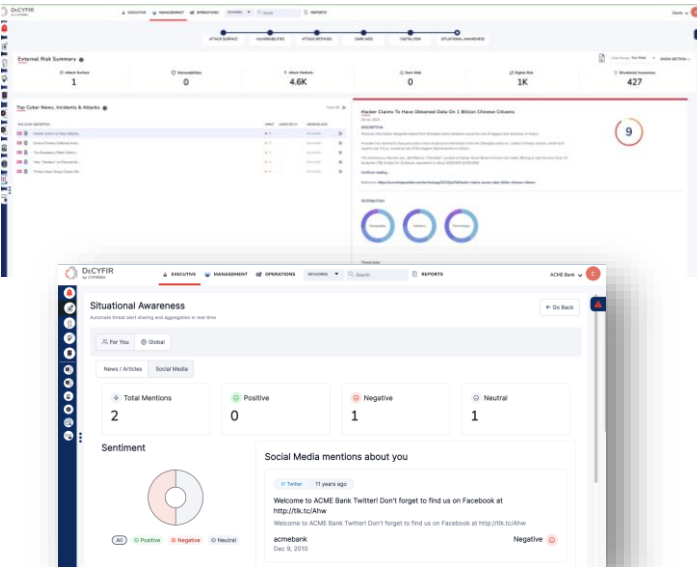
SITUATIONAL AWARENESS

ADAPT SECURITY ARCHITECTURE WITH DIGITAL RISK CONTEXT

Situational awareness

(Gain control of evolving threat landscape)

- Understand emerging threats, mitigations and potential attack scenarios
- Quick view of cyber attack incident and breach happening in your industry, technology you use and geography you operate from
- Provide insights which can guide important business decision including cyber investment
- Sentiment Analysis or opinion mining is key to understanding how your organization is viewed by external audience. Insights here can cast light on potential attacks from adversaries, hacktivist and others



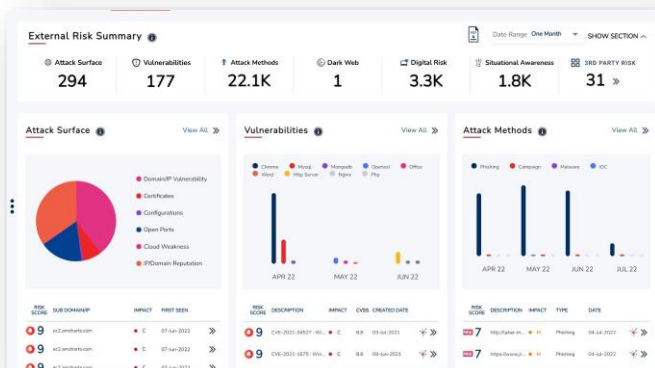
6

THIRD-PARTY RISK MONITORING

GAIN VISIBILITY TO YOUR SUPPLY CHAIN ECOSYSTEM AND UNDERSTAND HOW THEIR RISK IMPACTS YOU

Third-Party Risk Monitoring

- Provide customers with visibility of their third-party ecosystem e.g., suppliers, channels, partners
- Discover weaknesses of suppliers' digital assets
- Risk Scores are provided to help security teams prioritize resources and remedial actions



OPERATIONS VIEW

DeCYFIR allows operations team to see through the clutter and identify vulnerabilities that need immediate attention.



The **Hackability Score** quantifies the probability of client organization's digital profile and assets being hacked, considering recent malicious developments in client organization's external threat landscape.

The **Risk Score** signifies the level of risk applicable to client organization in the wake of recent developments in the external threat landscape.

Threat actors, their campaigns and impact to your organization

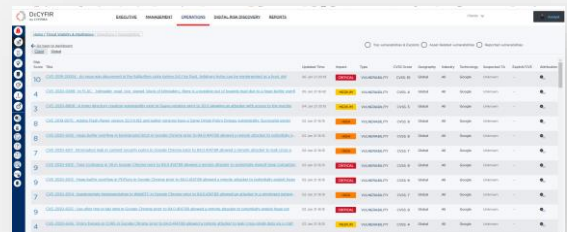
With over several hundred thousand software, middleware and hardware running in an enterprise, it is a complex job to keep the systems patched. DeCYFIR provides a full inventory of all your affected systems and respective vulnerabilities. Vulnerability management is prioritized on the basis of potential impact and ease of availability of exploits.

DeCYFIR uncovers **Digital Risk**, specifically, data leaks, breaches, brand infringement, impersonation, exposure in social/darkweb/etc.

Monitoring of exploit available for specific **vulnerabilities**, on surface web as well as dark web, allow security operations team to see through the clutter and identify the vulnerabilities which require immediate attention.

PRIORITIZED, RELEVANT AND TACTICAL MITIGATIONS FOR SOC TEAMS

- Operations Teams can optimize resources, increase efficiency and effectiveness
- Delivering actionable insights on vulnerabilities, IoCs, and hashes that are relevant to your industry, geography, and technology
- DeCYFIR validates an indicator and connects individual indicators with campaigns, threat actors, techniques



Extensive listing of relevant **Indicators of Compromise** - MD5, SHA, IP, DOMAIN, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL, etc.



DeCYFIR Delivers Immediate Benefits to Organizations

- ❖ 6-Pillar Unified View removes the need to use multiple tools
- ❖ Intelligence-hunting and threat-hunting are faster and more accurate
- ❖ Manage cybersecurity processes effortlessly, optimize vulnerability, certificate and CMDB management
- ❖ Identify unknown attack surfaces which you previously had no view so remedial actions can be taken
- ❖ A much more effective way of prioritizing risk by considering external factors – gain ability to respond to threats not just based on CVE
- ❖ Early warning to identify threats targeting you
- ❖ Mitigate Digital Risk by identifying data leak, impersonation and social profile hijack
- ❖ Access Risk Dossiers to connect threat actor, motive, campaign and method so as to accurately predict imminent cyberattacks
- ❖ CYFIRMA's platforms integrate with other tools to ensure workflows are managed seamlessly
- ❖ Gain visibility to third-party risk and be aware of how their weaknesses and vulnerabilities would impact your business

With DeCYFIR, organizations can turn the tide against cybercriminals with quality cyber-intelligence which will give them the view through the adversary's lens and take remedial actions to stop an attack in its track.



Cloud-native
SaaS Product



Subscription Based Revenue
Model



Different Plans Based On
Client Requirements



Simple Onboarding With
Minimal Intrusion

Ask for a demo today

<https://www.cyfirma.com/decyfir/>

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.

<https://www.cyfirma.com/>

