

DeCYFIR™

The cyber-ally for defenders to mitigate external threats and fend off cyberattacks

DeCYFIR is a SaaS-based external threat landscape management platform designed to defend your organization by uncovering your attack surfaces, building your digital risk profile, and using personalized cyber-intelligence to predict imminent attacks.

With DeCYFIR, clients receive a single pane of glass to their external threat landscape and know exactly the counter measures needed to close security gaps. They can deploy their cyber defenders and resources to where they are most needed and keep attackers at bay.

DeCYFIR is a non-intrusive cloud platform that provides quality cyber-intelligence that meet the following stringent criteria:

Predictive insights that give early warnings to clients on cybercriminals targeting them.

Personalized intel that is catered to client's industry, technology and geolocation.

Multi-layered intelligence that comprehensively covers strategic, management and operational layers.

Contextual insights that connect the dots between hacker, motive, campaign, and method.

Outside-in view provides insights into the external threat landscape so that client can see from the hacker's lens.

With DeCYFIR, clients are provided with a set of prioritized remediation to prevent a breach from occurring.

DeCYFIR is the unified external threat landscape management platform providing attack surface discovery, vulnerability intelligence, brand intelligence, digital risk protection, and situational awareness.



DeCYFIR™



KEY FEATURE



DESCRIPTION



BENEFITS

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 prepare against attacks
PERSONALIZED	Data points and insights are tailored to match the technology you are using, industry you are operating in and your geolocation.	Remove noise and reduce false positives
CONTEXTUAL	We present complete contextual details related to an indicator of compromise [what is it, background details, malicious / non malicious, location details, what it is being used for [C&C, hop to attack, malicious hosting site] affiliation cybercrime campaign, cybercriminals.	Gives deep understanding of cyber threats so as to mount effective defence strategies
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, tools, techniques they can use.	Comprehensive view to ensure cyber-defenders are not blindsided
ATTACK SURFACE DISCOVERY	Proactively identify exposed external assets, shadow IT, forgotten systems and more which can be exploited by cybercriminals.	Awareness of attack surfaces helps you identify a potential path of attack, and you can take steps to reduce and mitigate risk.
VULNERABILITY INTELLIGENCE	Identify weaknesses in your external assets, understand how cybercriminals are looking at exploiting identified vulnerabilities.	Helps prioritize patch 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	Reduce the risk to your brand, products and solutions

DeCYFIR™



KEY FEATURE

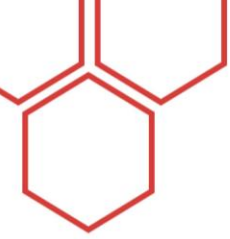


DESCRIPTION



BENEFITS

KEY FEATURE	DESCRIPTION	BENEFITS
DIGITAL RISK PROTECTION	Proactively identify data leaks, breaches, leaks, impersonation to	Reduce risk of cybercriminals hurting your brand or used against you for new cyberattacks
TAILORED DASHBOARD	<ul style="list-style-type: none"> Executive View is a risk-based approach meant for Executives to quickly understand external risk exposure and chances of being hacked Management View is the guided approach on systematic remediation process Operational View presents you with technical details of findings and remediation 	Caters across hierarchies and functions so everyone is on the same page
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 queries related to external threats
RISK DOSSIER	Risk dossier showing correlation to IOCs, vulnerabilities, attack surface, digital risk, and more	Enable you to quickly obtain holistic view on how a vulnerability could be exploited via specific campaign, and the cybercriminals behind it. Understand impact on your assets
ALERT CENTRE	Tailored alert center to understand what is the most important threats and risks to your organization	Helps you to quickly prioritize remedial actions
TAKEDOWN SERVICES	We offer takedown services with 3 RFI's a month under which we deliver intelligence-based research, deep dive reports on topics, incidents, evolving cyber trends identified by you	We help you mitigate the risk with concrete actions
INTEGRATION WITH SECURITY CONTROLS	You can integrate the insights using STIX and TAXII into your security controls	Incident response using DeCYFIR intelligence hunting capability provides complete contextual details
INCIDENT RESPONSE	Incident response using DeCYFIR intelligence hunting capability provides complete contextual details	Speed up incident response with complete external threat analysis
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 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.



EXECUTIVE VIEW

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



Understand Risk and Hackability Scores and Trends

Real-time view of External Threat Landscape



Critical threat indicators show up distinctly on dashboard to facilitate timely and accurate decision making

Deep insights attributing threat actor, motive, campaigns and impact

Provides Situational Awareness on what is happening globally and how these changes could be a threat to organization's digital profile. Understand the risks that could be coming your way as possible threats.



MANAGEMENT VIEW

The best-practice systematic approach for security management 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:

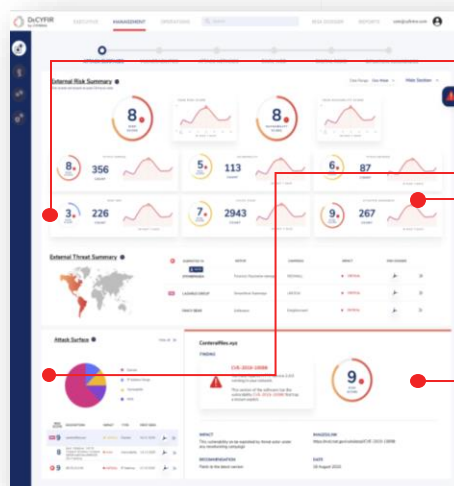
- Attack surface
- Vulnerabilities
- Attack methods
- Digital risk exposures
- Dark web observations
- Situation awareness

1 IDENTIFY ATTACK SURFACE

IDENTIFY ATTACKERS' POTENTIAL ENTRY POINTS

WHERE ARE THE DOORS AND WINDOWS TO GET IN

- Help client Identify assets 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 organizational risk
- Help clients establish an effective security strategy



Counts informs you of the latest exposures in last 7 days

Attack Surface provides doors & windows through which hackers can access your organization

Trends depict how you are faring in a particular time period for each category

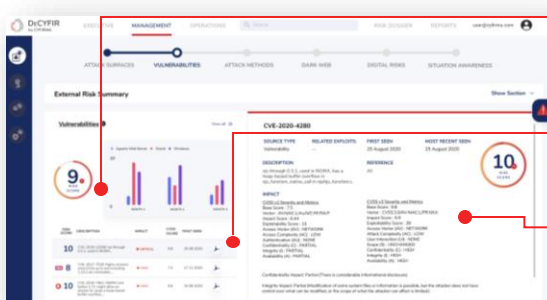
Detail View of an individual attack surface, tells you the severity and related attributes

2 DISCOVER VULNERABILITIES

SECURITY LEADERS BECOME PROACTIVE RISK ADVISORS RATHER THAN REACTIVE

KEYS TO 'DOORS' AND 'WINDOWS' CRIMINALS CAN EXPLOIT

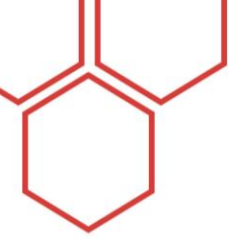
- Help client see from cyber-attacker's point of view
- Understand weakness and potential points of compromise
- Vulnerability intelligence can be used to build threat models and security planning



3 months trending helps manager to understand in which of their assets are more vulnerable

List of Critical vulnerabilities in the last 3 months that the organization should be looking out for

Details/attributes of the critical vulnerability

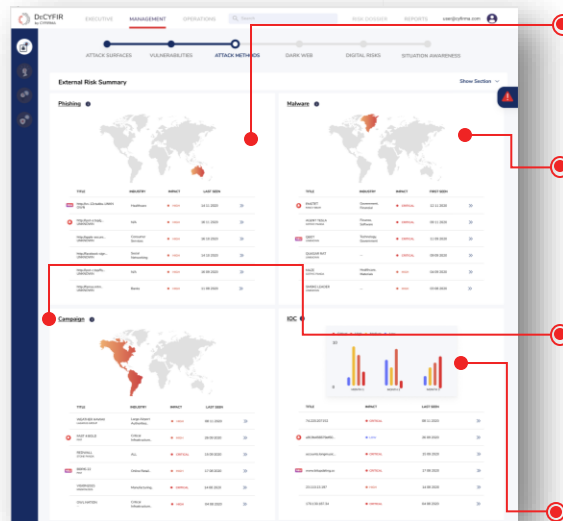


3 UNDERSTAND ATTACK METHODS

ENHANCE SECURITY TELEMTRY WITH DEEPER INSIGHTS INTO POTENTIAL ATTACKS

UNDERSTAND HOW HACKERS INTEND TO BREACH YOUR ORGANIZATION TO MOUNT AN EFFECTIVE RESPONSE

- Know the methods and tools deployed by adversaries
- Receive intelligence on campaign details at the early stage of planning



Latest **Phishing** attacks correlated to your organization

Important for Managers to view the Lists of most recently released Malwares by Hackers that can be hazardous to your organization,

Cyber attacks are often leveraged by threat actors as part of a coordinated **campaign** against your organization

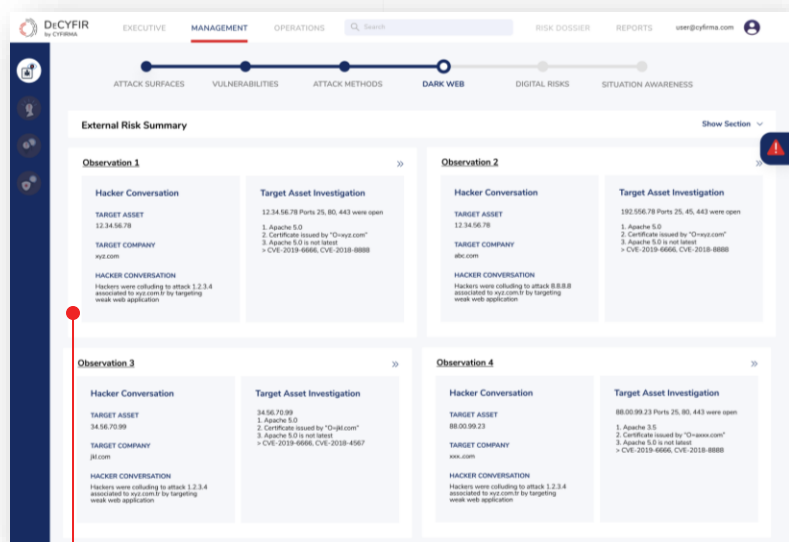
Extensive listing of relevant **Indicators of Compromise** - MD5, SHA, IP, DOMAIN, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL, etc.

4 DARK WEB OBSERVATIONS

AI ENGINES UNCOVER EVIDENCE INDICATING CYBER RISK AND ATTACKS TARGETING YOU

GO TO THE HACKER'S TRENCHES AND UNCOVER EVIDENCE OF POTENTIAL ATTACKS

- Stay ahead of cybercriminals by gaining insights to threat indicators
- Give yourself a head start with actionable cyber-intelligence
- Activate an effective defense strategy with timely intel



Threat Intel assets gathered from Deep/Dark Web and hackers forums, closed communities

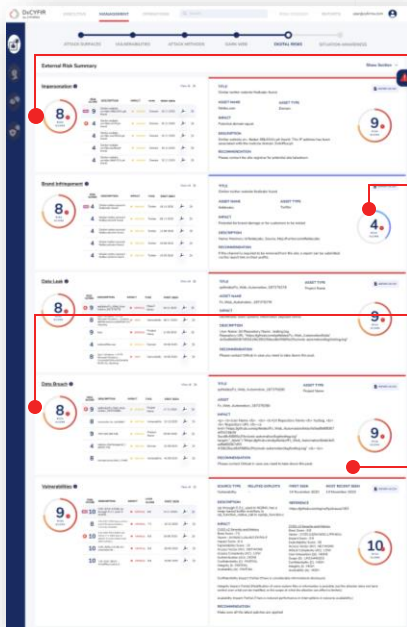


5 DIGITAL RISK PROFILE

ADAPT SECURITY ARCHITECTURE WITH DIGITAL RISK CONTEXT

TAKE BACK CONTROL OF YOUR DIGITAL LANDSCAPE

- Uncover brand/product infringement
- Expose executive impersonations
- Be the first to know when data leaks breaches, and impersonations have occurred
- Mount a defense strategy to prevent recurrence



All the online entities that are impersonating organization's digital profile and assets based on the domain name provided.

Digital profiles which have the potential to bring disrepute to your brand.

Know what data have been breached from your organization that hackers can potentially use to attack you. This can include files/usernames/passwords, etc.

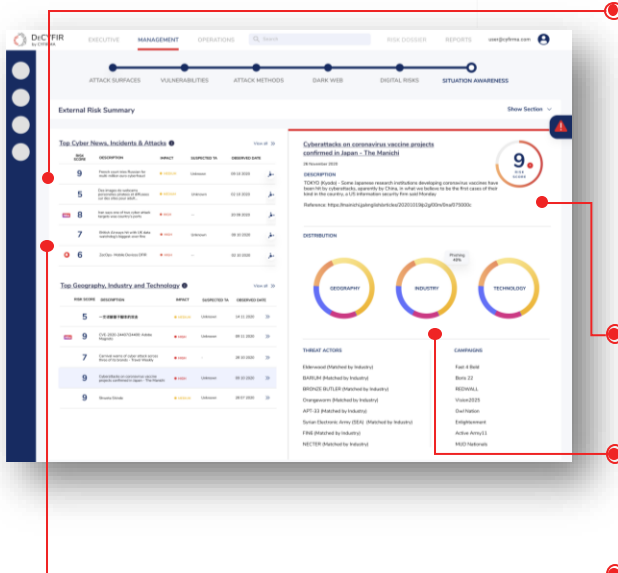
Hackers can exploit these vulnerabilities, attack vectors, bring disrepute to your organization, exfiltrate sensitive data, and more.

6 SITUATION AWARENESS

ACHIEVE HIGHER LEVELS OF EFFICIENCY, EFFECTIVENESS, AND ACCURACY IN DECISION-MAKING

GAIN CONTROL OF FAST CHANGING LANDSCAPE BY UNDERSTANDING EMERGING THREATS

- Arm yourself with relevant information to latest cyber-attacks in your industry, changes to cyber laws and other essentials
- Insights to guide strategic, management and tactical decision-making



Even in the best-funded, most mature organizations, there are information gaps in knowing what the current state is and what it should be. This is where situational awareness becomes a necessity to guide critical decision-making.

Arm your organization with the latest development in the cyber threat landscape and understand its impact to your business.

Risk scoring for specific insights to help prioritize resources to attend to risk and threats.

Graphical representation of types of threats and malware for quick update on threat landscape, view by geography, industry and technology lens.

Insights are curated just for the organization, relevant to the geography, industry and technology used.

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

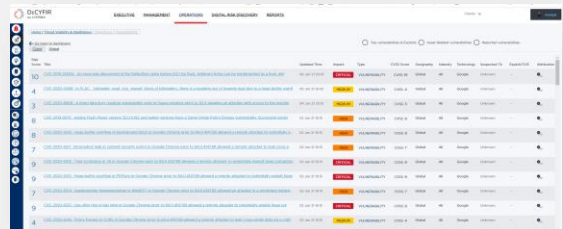
With over several hundred thousand software, middleware and hardware running in an enterprise, it is a complex job to keep the systems **patched**. DeCYFIR provides a full inventory of all your affected systems and respective vulnerabilities. Vulnerability management is prioritized on the basis of potential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

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.

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