DECYFIR®
BY CYFIRMA

DECYFIR®

Organizations are at a crossroad as they navigate the unchartered waters of a post-pandemic and volatile geopolitical landscape. Cybersecurity strategies which were previously designed to manage known threats using conventional security control tools need to be re-evaluated.

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 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

Brand Intelligence

Monitor brand, product & service, executive infringement and connect 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 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 the attacks. Equipped yourself with actionable and prioritized remediations

DECYFIR®
BY CYFIRMA

DECYFIR®

KEY FEATURE	DESCRIPTION	BENEFITS
PREDICTIVE	Predict impending cyber-attack targeting your organization and subsidiaries before cybercriminals can cause harm your business.	Early warnings and alerts to help you quantify risk and prepare for impending cyberattacks.
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 to ensure the high impact alerts are actioned upon.
CONTEXTUAL	Complete contextual details of the external threat including adversary details, TTPs and related IoCs (malicious / non-malicious, location details, what it is being used for C&C, the path 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, tools, techniques they can use.	Comprehensive outside-in view to ensure cyber-defenders are not blind-sided and can take appropriate proactive action to align cyber capabilities.
ATTACK SURFACE DISCOVERY	Identify external assets and potential points of exploits such as shadow IT, forgotten systems, misconfigurations, leaky buckets, vulnerable certificates.	Gain awareness of 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 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.

DECYFIR® BY CYFIRMA

DECYFIR®

KEY FEATURE	DESCRIPTION	BENEFITS
DIGITAL RISK PROTECTION	Proactively identify data leaks, breaches, brand/executive impersonation, 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 • 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	• 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.	• 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 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 RESPONSE	Incident response 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	▪ 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

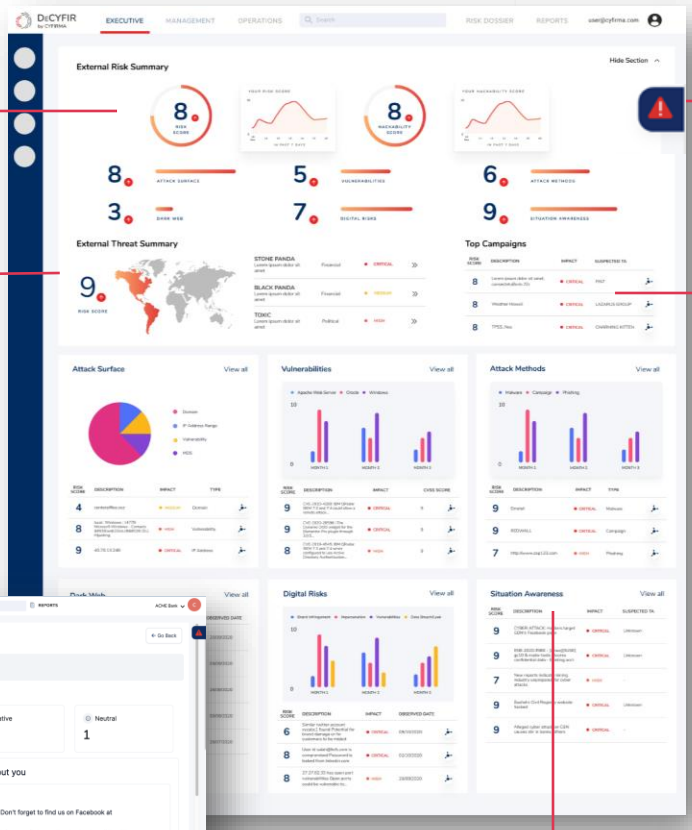
EXECUTIVE VIEW

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

- Executive dashboards to help leaders understand shifting dynamics and accelerate critical decision-making
- Risk and Hackability Scores for quick understanding of external cyber risk / threat posture
- Key indicators, trends, attributions and correlations
- Overview on cyber threats relevant to your organization

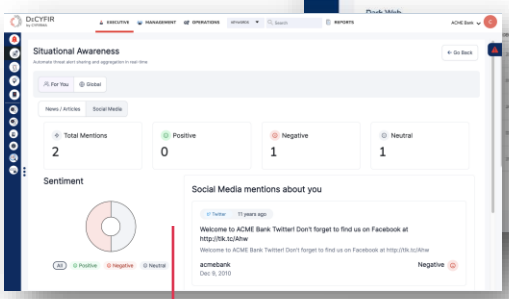
Understand **Risk and Hackability Scores** and Trends

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



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.

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:

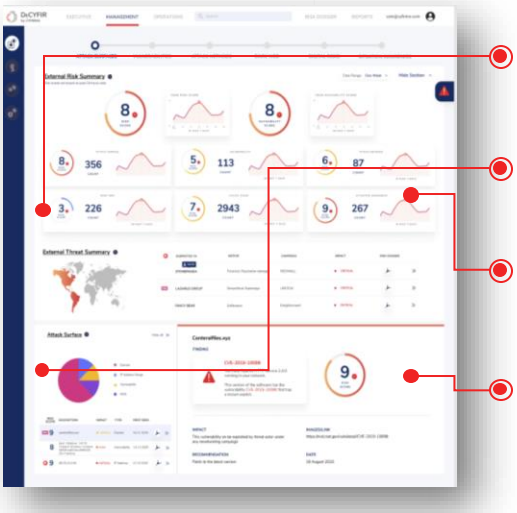
- Attack surface
- Vulnerabilities
- Attack methods
- Digital risk exposures
- Dark web observations
- Situation awareness

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

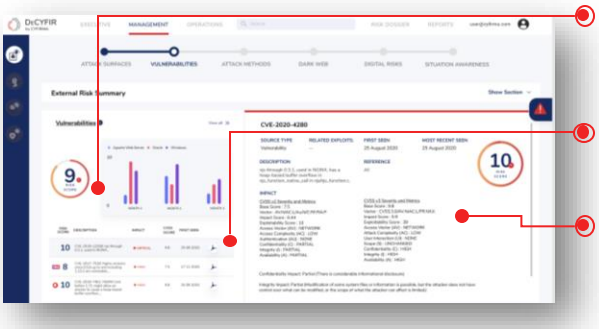
Detail View of an individual attack surface, tells you the severity and related attributes

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 which of their assets are more vulnerable

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

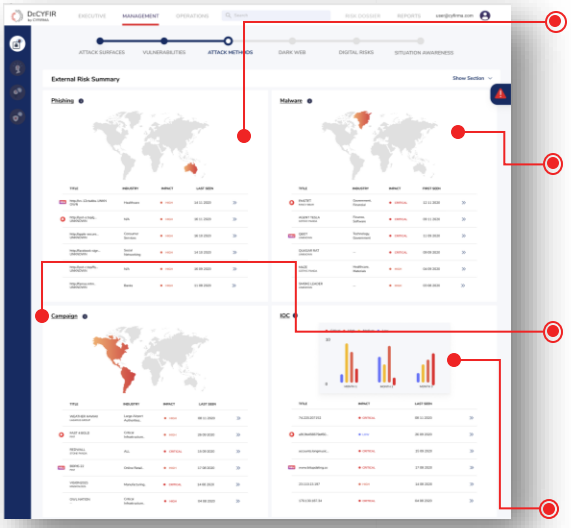
Details/attributes of the critical vulnerability

3 UNDERSTAND ATTACK METHODS

ENHANCE SECURITY TELEMETRY 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

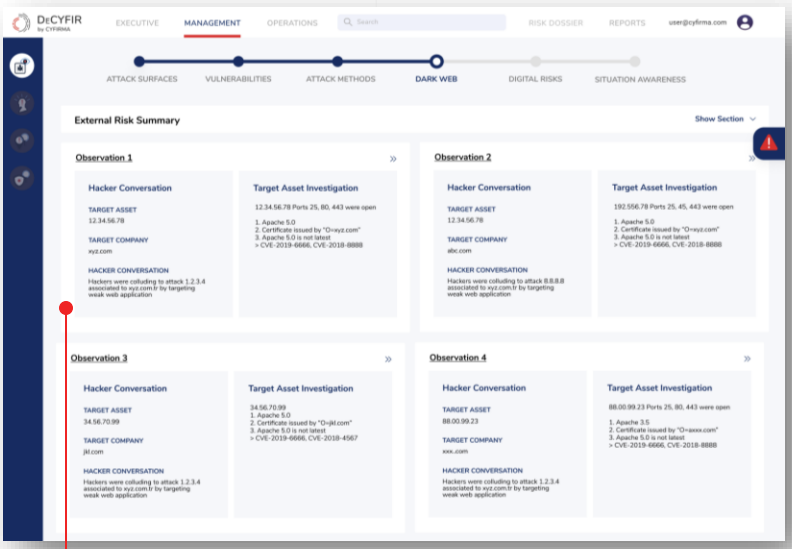
Extensive listing of relevant Indicators of Compromise - MD5, SHA, IP, DOMAIN, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL, etc.

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



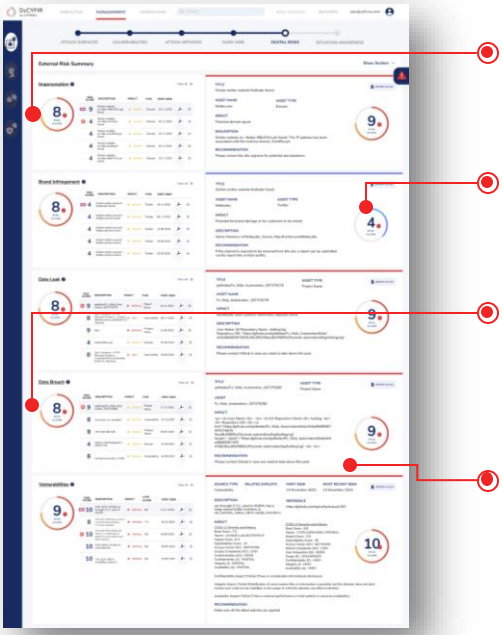
Threat Intel assets gathered from Deep/Dark Web and hackers forums, closed communities

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.

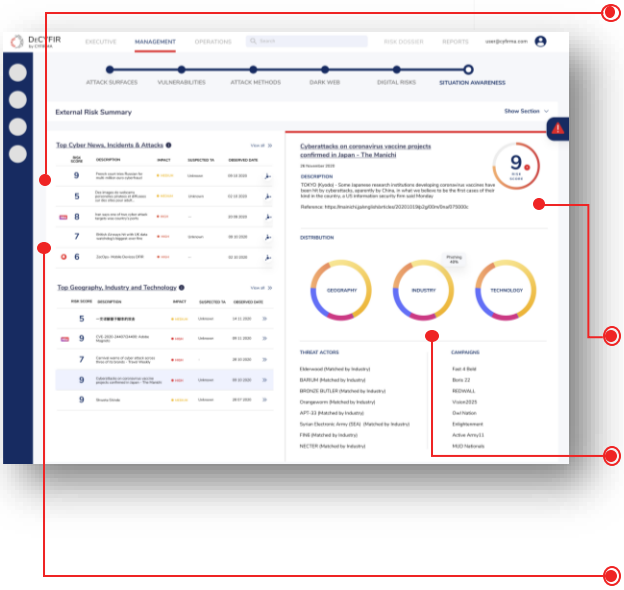
Hackers can exploit these vulnerabilities, attack vectors, bring disrepute to your organization, exfiltrate sensitive data, and more.

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

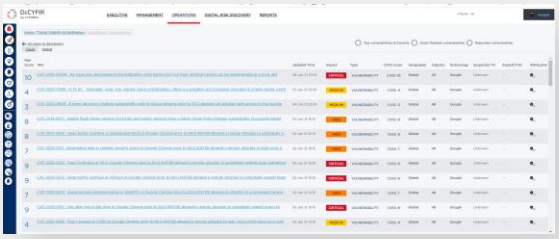
With over several hundred thousand software, middleware and hardware running in an enterprise, it is a complex job to keep the systems patched. DeCYFIR provides a full inventory of all your affected systems and respective vulnerabilities. Vulnerability management is prioritized on the basis of potential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

DECYFIR®
BY CYFIRMA

DECYFIR®

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 priorizing 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

To learn more, reach out to CONTACT@CYFIRMA.COM

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/

CYFIRMA
DECODING THREATS