DeCYFIR 4.0

Anticipate threats | Shape the Battlefield | Deny Attackers the Advantage

Preemptive Cybersecurity Starts Here

Cyber risk now unfolds at the speed of preparation, not response. Modern defense demands a shift from reactive containment to intelligence-led prevention, identifying and disrupting adversaries before impact.

DeCYFIR 4.0 is the world's first preemptive External Threat Landscape Management (ETLM) platform that unifies nine intelligence pillars to deliver continuous, adversary-centric visibility across the external attack surface. It moves security beyond detection into prediction, prevention, and deception, interrupting attacks during reconnaissance and weaponization. With DeCYFIR 4.0, cyber defenders will achieve the following:

Executive Clarity
Contextual intelligence supports informed risk and governance decisions.

Operational Efficiency
Threats prioritized by exploitability and relevance reduce noise and speed action.

Brand Protection: Continuous monitoring safeguards brands, executives, and intellectual property.

Proactive Threat Disruption
Early warning and deception capabilities interrupt adversary campaigns before exploitation begins.

Reduced Risk
Early visibility into exposed assets, vulnerabilities, and third-party risks lowers breach impact.

Sustained Resilience
Deception and targeted awareness strengthen continuity in hostile environments.

Pillar 1: Attack Surface Discovery & Intelligence

Maps and monitors the full IT/OT environment, revealing hidden risks and identifying critical attack paths.

Pillar 2: Vulnerability Intelligence & Threat Prioritization

Delivers real-time detection and risk-based prioritization of weaknesses by correlating active exploitation trends with adversary intent.

Pillar 3: Brand & Online Exposure Management

Safeguards the brand, key executives, and the broader digital footprint from impersonation, deepfakes, and fraud across the open, deep, and dark web.

Pillar 4: Digital Risk & Identity Protection

Rapidly uncovers leaked credentials, data breaches, exposed source code, and targeted phishing or ransomware campaigns before they cause harm.

Pillar 5: Third Party Risk Management

Continuously assesses vendors and supply-chain partners for vulnerabilities, breaches, and reputational risks.

Pillar 6: Situational Awareness & Emerging Threats

Provides a highly contextual, real-time view of emerging threats tailored to your industry, region, and technology stack.

Pillar 7: Predictive Threat Intelligence

Delivers early-warning insights on threat actors, campaigns, and attack timelines targeting the organization, well before incidents unfold.

Pillar 8: Threat Adaptive Awareness & Training

Turns employees into an active human-sensor layer through training programs built on real threat activity directed at your organization.

Pillar 9: Sector Tailored Deception Intelligence

Deploys customized, high-interaction decoys that attract adversaries and convert every interaction into precise, early-stage threat intelligence.

WHY CYFIRMA

360 Degree Threat View
Unified platform covering attack surface, vulnerabilities, brand, digital, and third-party risks in one view.

Smart Correlation
AI links actors, motives, and campaign automatically, reducing manual work and cost.

Global Deception Network
Real-time threat data from dark/deep web and channels with AI + human curation.

Asia-First Advantage
Unmatched visibility into Asia-Pacific threats driven by geopolitical and economic shifts.

Preemptive ETLM

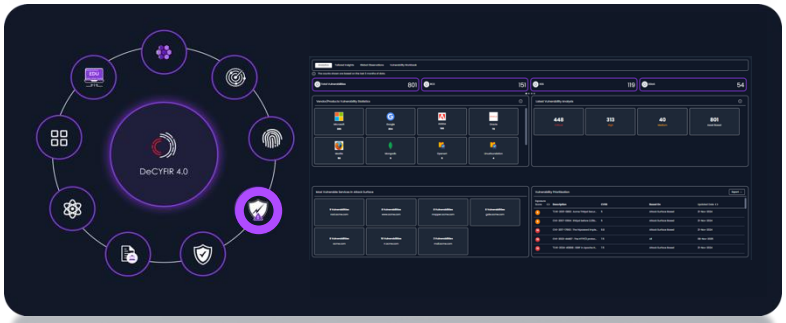
Security that acts before the attack begins

DeCYFIR defines Preemptive External Threat Landscape Management (ETLM), a security model focused on stopping attacks before they take shape. Powered by AI-native intelligence across nine integrated pillars, it interprets exposure and adversary intent from the attacker's perspective, predicts likely attack paths, and disrupts reconnaissance through early action and deception. Operating upstream of traditional detection and response, Preemptive ETLM reduces what becomes an incident and shifts cybersecurity from reactive defense to strategic control of the external threat landscape.

Pillar 1:

Attack Surface Discovery and Intelligence

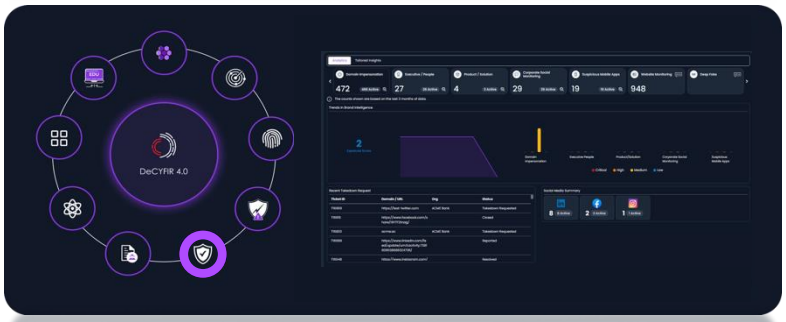
Provides the foundational visibility required for strategic risk reduction, ensuring no blind spot becomes an entry point for adversaries.



Pillar 2:

Vulnerability Intelligence and Threat Prioritization

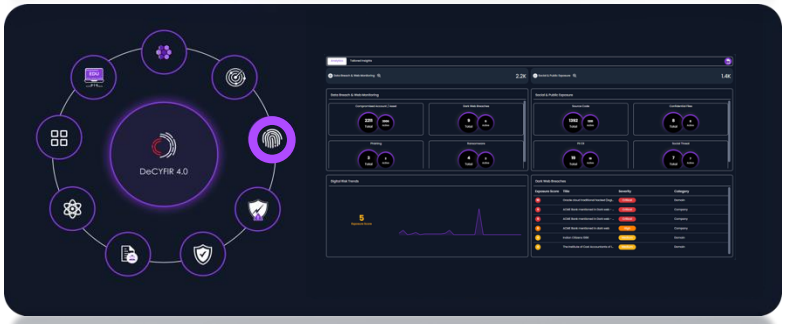
Places technical weaknesses into real-world context by aligning them with attacker behaviour, not theoretical scoring systems.



Pillar 3:

Brand and Online Exposure Management

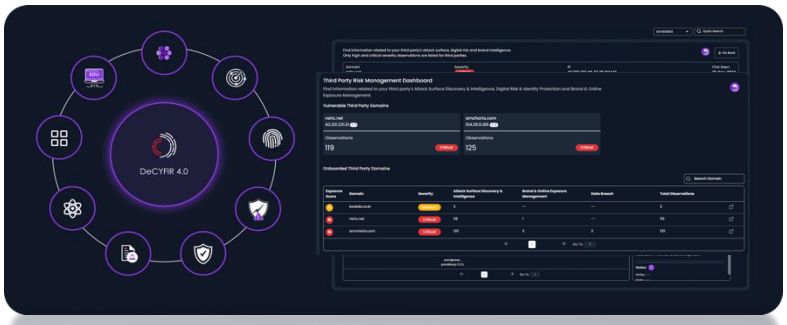
Safeguards corporate trust and executive reputation — often the first targets in campaigns designed to mislead customers or manipulate markets.



Pillar 4:

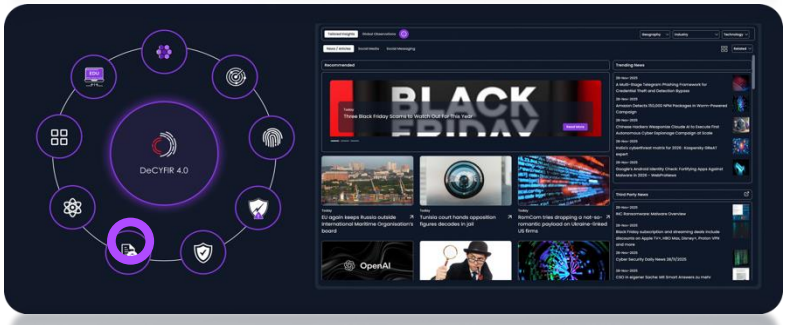
Digital Risk and Identity Protection

Bridges the gap between cyber hygiene and real-time incident prevention by intercepting sensitive data the moment it escapes controlled environments.



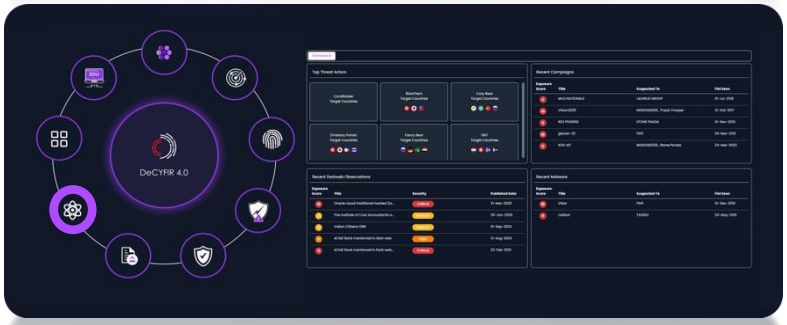
Pillar 5: Third Party Risk Management

Recognizes that modern breaches rarely start at the core; they begin at the edges, with unmanaged vendors, shared platforms, and inherited weaknesses.



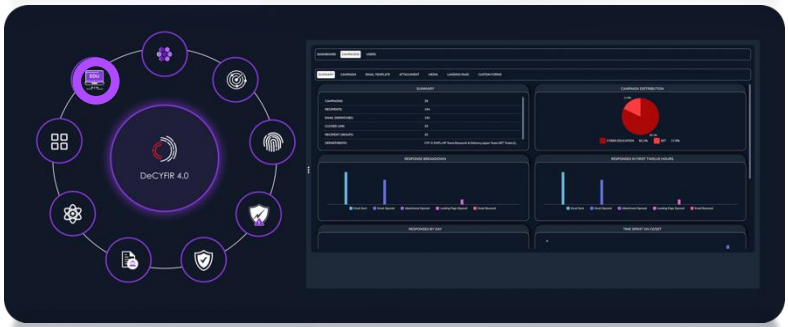
Pillar 6: Situational Awareness and Emerging Threats

Moves beyond generic threat reports, offering industry-specific insights that help leaders make informed, timely decisions.



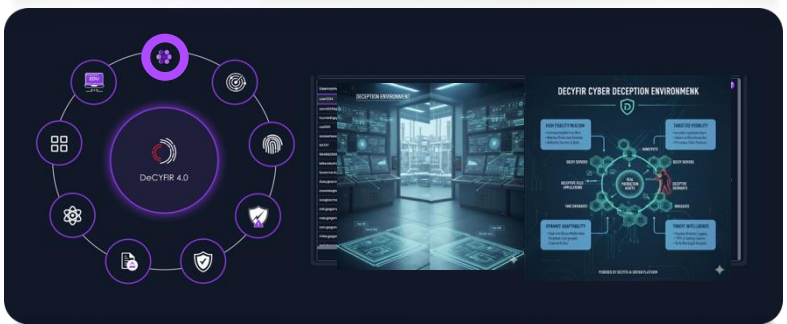
Pillar 7: Predictive Threat Intelligence

Shifts organizations from reactive firefighting to proactive posture management by forecasting hostile activity before it matures into an attack.



Pillar 8: Threat Adaptive Awareness and Training

Delivers real-time, intelligence-led cybersecurity awareness by automatically updating training content and phishing simulations based on live, active threats targeting your industry that mirror real attacker techniques.



Pillar 9: Sector Tailored Deception Intelligence

Flips attacker reconnaissance into actionable early-stage intelligence that strengthens defenses from the start.

Uncover what attackers see, plan, and execute before threats materialize.

01 AI to increase velocity of data collection
02 NLP to collect data and analyze for tone and textual
03 AI and ML models for correlation
04 Agentic AI analysis, reporting, dissemination and recommendations

DeCYFIR overcomes limitations of conventional threat intelligence

COMPLETE INTEGRATION
Siloed tools do not communicate with each other, leading to a fragmented view of threats and missing critical vulnerabilities. DeCYFIR's unified platform solves that once and for all.

INTELLIGENCE-LED PRIORITIZATION
Relying on CVE scores and traditional methods overlook the fact that attackers often exploit medium and low-severity vulnerabilities. Use intelligence-led approach for effective and accurate prioritization.

THREAT PERSONALIZATION
Lack of personalized risk assessment tailored to an organization's unique assets, brand presence, digital footprint, and third-party dependencies hinders effective risk management. DeCYFIR overcomes that with deep personalization capabilities.

ACCURATE REMEDIATION MAPPING
The siloed approach leads to a lack of contextual understanding of threats, making it difficult to respond effectively. Use DeCYFIR AI-powered and HUMINT expertise to help you close the gaps.

Eliminate Noise
The absence of personalized threat prioritization results in too much irrelevant data, obscuring genuine risks. Let DeCYFIR guide you out of the noise.

AMBIGUOUS RISK ASSESSMENT
To effectively quantify the likelihood and impact of attacks, let DeCYFIR give you intel that will sharpen your defence strategy.

Consider this:

- Do you have full visibility into your expanding external attack surface, including unknown assets and shadow IT already being targeted by adversaries?
- Can your team effectively prioritize vulnerabilities amid thousands of alerts, using intelligence tied to active threats targeting your industry?
- Is your brand protected against impersonation, phishing, and dark web activity that could damage reputation or enable fraud?
- Do you have real-time insight into supply chain risks introduced by third-party vendors and partners?
- Can your security operations proactively detect and mitigate digital identity risks, such as leaked credentials or executive exposure on the deep and dark web?
- Are you equipped to anticipate emerging threats from hacktivists, ransomware groups, or state-sponsored actors amid shifting global events?
- Does your threat intelligence deliver predictive, personalized warnings, beyond generic feeds, about campaigns being planned against your organization?
- Are employees equipped with adaptive, threat-aware training that evolves with the latest adversary tactics relevant to your business?

Reach out to Team CYFIRMA today.

About CYFIRMA

CYFIRMA is a global leader in preemptive external threat landscape management, enabling organizations to predict and prevent cyberattacks through its AI-powered intelligence platform. By integrating nine pillars of external threat management including Attack Surface Discovery, Vulnerability Intelligence, Brand & Digital Risk Management, Third-Party Risk, Situational Awareness, Predictive Threat Intelligence, Threat Adaptive Awareness, and Sector-Tailored Deception Intelligence, CYFIRMA shifts cybersecurity from reactive to predictive. The platform delivers early warnings, personalized insights, and actionable intelligence from a hacker's perspective, helping reduce cyber risk and costs through threat prioritization, contextual decision-making, improved visibility, and stronger operational resilience. CYFIRMA serves Fortune 500 companies and national agencies and is headquartered in Singapore with offices across APAC, the US, and EMEA.

CYFIRMA
DECODING THREATS