CYFIRMA
DECODING THREATS

DeCYFIR 3.0

External Threat Landscape Management

FIGHT AI WITH AI-POWERED ETLM

DeCYFIR 3.0是全球領先的外部威脅情報管理平台，旨在讓具有前瞻性思維的網路安全領導者掌握對手的視角，並制定有效的防禦策略來應對新興的威脅。DeCYFIR 3.0 開創了一種稱為外部威脅態勢管理（ETLM）的突破性方法，可協助您針對網路攻擊建立策略性的嚇阻。在ETLM 框架的指導下，DeCYFIR 3.0 為您提供清晰的可視性，幫助您克服網路戰的迷霧。

DeCYFIR 3.0 利用最新的人工智慧（AI）、自然語言處理（NLP）和大型語言模型（LLM），深入挖掘針對您的威脅，為您提供時間優勢來阻止攻擊並降低風險。

Unified Approach

Attack Surface Discovery

發現面對外部的資產，以及可能被 駭客利用的流程和技術弱點

Vulnerability Intelligence

根據不斷變化的外部網路環境，以威脅為導向，對漏洞進行豐富化的評估。根據網路犯罪分子的興趣、歸因和關聯性，優先處理已識別的漏洞，提供端到端的威脅可視性。

Brand Intelligence

監控品牌、產品、解決方案和服務、執行侵權行為；並將其與正在進行的網路犯罪活動聯繫起來

Digital Risk Discovery

暗網、深網、表面網路和社交媒體監控，以尋找資料和身份外洩、機密檔案、原始碼、敏感資訊曝露、域名冒充等情況

Situational Awareness

了解特定組織行業、科技生態系統和地緣政治影響下的網路趨勢和威脅。

Cyber- Intelligence

預測性、個人化、情境化、由外而內和多層次的資訊安全情報，探討了網路攻擊的主要問題，包括who, why, what, when 及 how。提供可行且優先的解決方案。

Third-Party Risk

發現供應商數位資產的弱點，並警告您可能受到資料外洩和暴露的影響。

ETLM BENEFITS

全方位監控跨足暗網、深網、明網和社群媒體，支援28種語言，確保不漏過任何威脅。

基於人工智慧的分析預測潛在攻擊，使得能夠在事件發生之前部署禦措施。

提供量身訂製的見解，滿足行業獨特的資訊安全需求，增強有針對性的保護策略。

透過我們的數位風險發現和保護機制，保護客戶敏感的至關重要資訊方面發揮關鍵作用。

可行的情報是我們服務的核心，提供快速應對和減輕網路威脅的策略建議，確保您的營運安全。

協助評估和管理與供應商和合作夥伴相關的風險，使您的企業不僅領先於威脅，而且遵守法規。

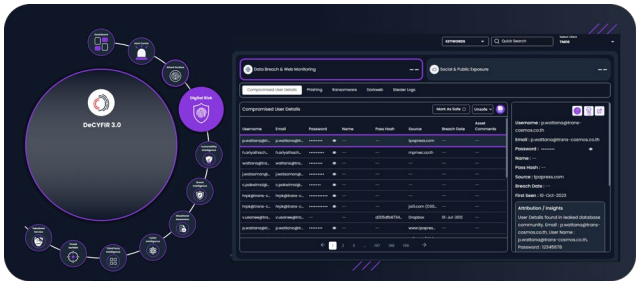
Fight AI with AI-powered ETLM

DeCYFIR將7個威脅視角呈現在單一管理平台上，將威脅和漏洞之間的點連接起來，顯示針對你的攻擊路徑。攻擊面、弱點、品牌、數位風險、情境感知、網路情報和第三方風險的洞察見解被收集、分析並呈現在單一畫面上，無縫指導補救措施，並在人員、流程和技術方面強化資安防護。

Attack Surface Intelligence

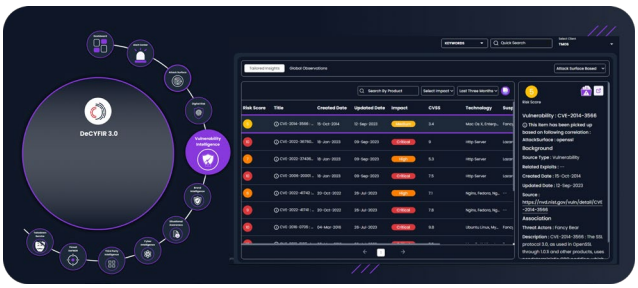
主動發現外部資產並找出可能被駭客利用的弱點。

Digital Risk Discovery



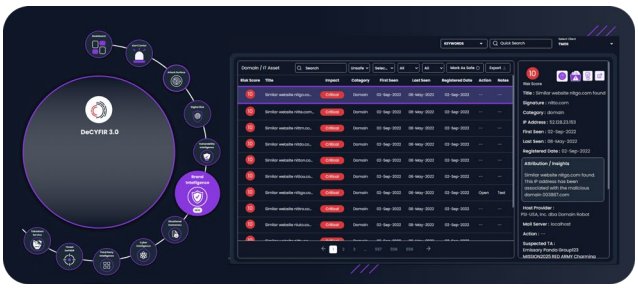
利用暗網、深網、表網和社群媒體管道的情報，主動偵測潛在的資料和身分外洩。

Vulnerability Intelligence



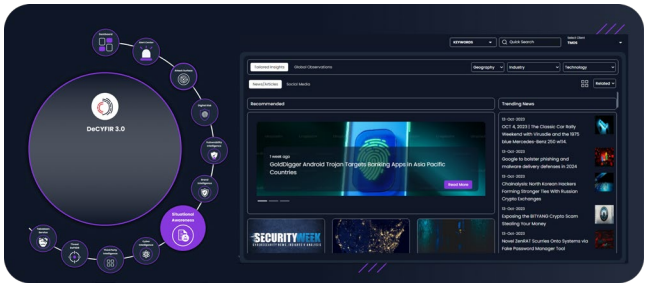
基於駭客的興趣、歸因和關聯進行威脅導向的漏洞監控，實現端到端 的威脅可視化。

Brand Intelligence



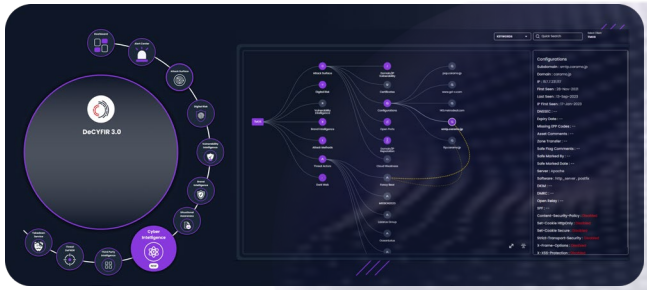
監控品牌、產品、解決方案、IP、關鍵基礎設施和高層管理者的侵權情況，無縫地將這些情況與正在進行的駭客攻擊和更廣泛的網路犯罪活動聯繫起來。

Situational Awareness



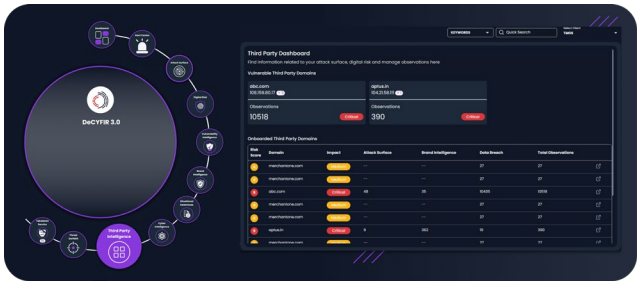
情報和洞察力，讓組織更深入地了解針對其特定行業、技術生態系統和地緣政治影響的網路趨勢和威脅。

Cyber- Intelligence



揭開連結威脅與公司網路安全狀態潛在影響的"golden thread (黃金線索) "

Third-Party Risk



以AI驅動的工具提供跨越不同領域的網路犯罪活動的全面視圖，並提供寶貴的情報，以強化網路安全防禦

Fight AI with AI-powered ETLM

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

01
Use AI to increase velocity of data collection

02
Use NLP to collect data and analyze for tone and textual

03
Use ML models for correlation

04
Use AI analyst for reporting, dissemination and recommendation engine

Cloud-native SaaS Product

Subscription-Based Model

Plans Based On Client Requirements

Simple, Agentless Onboarding

The Future is Now

請您回想:

- 你能否充份了解你組織的外部威脅？
- 你對於目前的威脅情報是否有信心，能夠有效保護你的關鍵基礎設施？
- 你的安全工具是否整合並無縫運作，以提供完整的數位足跡可視化？
- 地緣政治發展對你的網路風險有何影響？
- 你的數位化是否會給你的業務帶來網路風險？

See DeCYFIR 3.0 in action

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