ATHS

Presenting the ATHS AI Empowered Threat Hunting Solution

以最先進的多層次-多面向 EDR/NDR/XDR 威脅獵捕技術，保護您企業的安全。

The ATHS redefines threat detection and response capabilities by seamlessly integrating across network and endpoint environments, bolstered by its state-of-the-art Extended Detection and Response (XDR) technology.

- 先進的威脅獵捕行動
- 識別隱藏的威脅以預防缺口
- 威脅獵捕情資整合
- 多層次威脅風險分析圖

生態系整合

- 全面支援本地端和雲環境的網路偵測及回應(NDR)
- 先進的端點偵測及回應(EDR)能力
- 託管式偵測及回應(MDR)服務

ATHS Benefits

AI-Driven Detection	ATHS利用進階分析、深度學習與複雜行為分析來自動化威脅偵測，從資料點中辨別出事件，並有效精準指出網路上的攻擊與惡意交易的威脅及根因
Multilayer Threat Graph	多層次威脅圖是 ATHS 的智慧核心，利用 NDR 裝置所偵測到的安全事件、網路流量，以及端點主機日誌，提供應變人員即時的情境式威脅情資與有價值的可用資訊
Advanced Investigation	持續於網路環境與各主機間進行偵測，獲取其異常數據流、關聯性、意圖及營運衝擊等具有價值的可用資訊
Network Visibility	取得對所有網路活動的可視性，發掘先前未發現的隱藏惡意行為模式，並自動追蹤濫用特權憑證、橫向移動等攻擊者活動
Crystal-clear Insights	ATHS 以模擬攻擊者方式快速偵測威脅，並按優先順序即時處理回應，有效分辨實際攻擊與誤報
Unprecedented Productivity	整合化的自動調查及回應系統，使威脅獵捕團隊分析師生產力翻倍

Analysis of ATHS for Detection and Response

ATHS NDR

即時監控網路流量，警示異常情況，並阻斷惡意連接

ATHS EDR

結合日誌分析、規則引擎和行為分析，以識別端點設備上的惡意程式、漏洞和風險

ATHS Threat Hunting

利用人工智慧和大語言模型技術，將網路和主機的異常情況相關聯，主動跟踪、分析和識別威脅

AI-Driven Analysis

通過先進的分析、深度學習和複雜的行為分析，自動化威脅檢測，從數據中有效識別事件，精確定位網路上的威脅及攻擊和惡意交易

Seamless Streamline CPE and Device Management Cloud

Cybersecurity AI SaaS

AICAST Agent

NDR Device

- Network Threat Detection
- Real-time blocking
- Event Attestation
- AI-assisted traffic analysis

Threat Intelligence Center

- AI Analytics with LLM
- Deploying Threat Detection Mechanisms
- AIoT-focused Cyber Threat Intelligence

Device Management Service (DMS)

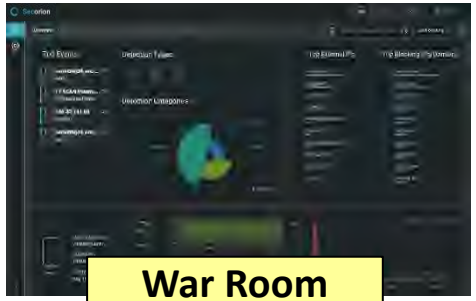
- Device Visibility and Monitoring
- Firmware Update (FOTA)
- Cloud Management and Control

Threat Hunting Engine

- Behavioral Analysis
- Potential Threat Discovery
- Attack Chain and Tactics Analysis
- Intelligence Integration

Threat Operation Center

- Real-time Intelligence
- Detection Status
- Threat Analysis
- Evidence Records
- Domain Asset Identification



War Room

- CPE-free, AI-powered AICAST Agent
- AI-driven cybersecurity SaaS solution
- Supported by a dedicated War Room App and SaaS
- Facilitating third-party operational support

NDR 網路偵測與情資 應用情境

系統自動定期發送威脅情資

將NDR設備進行連網，並 進行可視帳號權限設置，相關人員 可透過各類裝置，隨時就多台設備 監控下之場域安全狀況、設備所屬 環境安全狀況進行查閱。

NDR情資電子報給所設定 之收件閱覽者，報告內會對威脅項 目進行摘要說明並提供對應查閱連 結 ，顯示該 IP弱點掃描漏洞資料等。

NDR

MIS 人員

通報

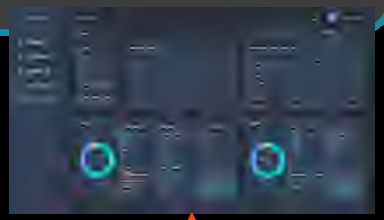
初步判斷

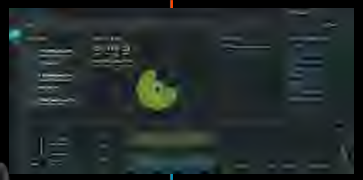
MIS 人員

MIS 主管

如有高風險事件發生...

監管人員可透過戰情室內找到該比高風險事件，並連結至事件 IP 的相關資訊 (外部IP) 漏洞風險 (內部IP) 且可查閱發生時序。





決策指示

CXO、CIO高階管理者

提升內部
改善自我缺失

風險事件排除、處理產生文件都確實歸檔保存，藉由區塊鏈進行存證紀錄，確保完整與安全性。

查閱存證紀錄

內部、外部 稽核單位/人員

偵測獵捕與威脅引擎 應用情境

對定義下範圍不間斷的偵測

定義抓捕規則
由內部資訊監控單位，對威脅類型、可能受影響的系統網路區域，依規範定義確認獵捕目標與範圍。

資料與情報彙總
搭配NDR蒐集而來 的數據和威脅，進行內外部 情報共享。

數據分析
針對蒐集到數據，以識別潛在異常行為、不尋常的活動以及可能發生攻擊特徵。如惡意流量、行為指紋入侵等等...

應變流程觸發
因應不同威脅事件，系統自動觸發對應應變流程，並通報關卡處理人，串聯應變相關人員...

制定對策
基於獵捕的結果，制定、裁定對策與應對措施，以減輕風險並防止攻擊進一步的擴散。

MIS 人員

MIS 人員

MIS 主管

顯示被攻擊的詳細內容

確認威脅存在

進階探索與驗證
驗證警報的真實性，分析系統的行為模式並追蹤攻擊活動跡象。

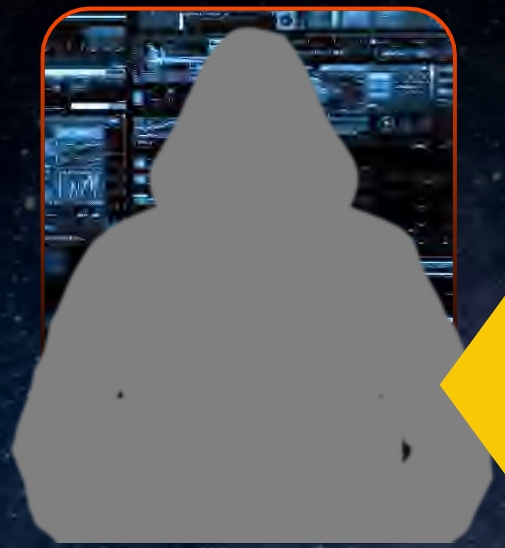
採取行動建議

拍板

CXO、CIO高階管理者

資安獵捕平台

雲端服務
Cloud service



高階
偵防
獵捕

網路勒索事件頻傳

造成作業癱瘓及鉅額損失，
更是供應鏈的信任問題。

台灣是勒索熱區

根據資安大廠Fortinet報告，
台灣每秒遭受1.5萬次攻擊，居亞太之冠。

被虎視眈眈的工控環境

數以百億的物聯網工控設備，
都存在被注入危險與潛伏威脅，

防火牆及防毒軟體已無力防禦

防毒軟體被動防止染毒檔案被開啟。
防火牆一味地限制流量及封鎖連線。

新一代網路檢測響應(NDR)方案
採用路由器與獵捕系統的一體設計，
軟體加硬體的堅強搭配，
提供最高安全係數的企業防護。

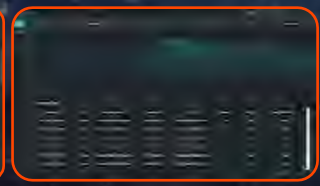
專為資安團隊設計

防駭

- 部署在網路最前沿
- 智能監控與回應

防勒索

- 即時比對全球情資網
- 追查攻擊行為軌跡



頂級Wifi路由器 | 高階戰情室 | 呈現入侵軌跡 | 自訂應對腳本

全球情資網 | AI風險辨識 | 威脅可視化 | 智能獵捕引擎

符合零信任機制 | 區塊鏈log存證 | 支持資安險

Advanced Endpoint Detection and Response (EDR)

入侵偵測

通過監控主機系統和網路活動，識別和警示可能的入侵事件、檢測惡意登入行為、惡意程式行為和其他可能的攻擊行為跟可疑的活動、有助於及早發現和應對潛在的安全威脅。

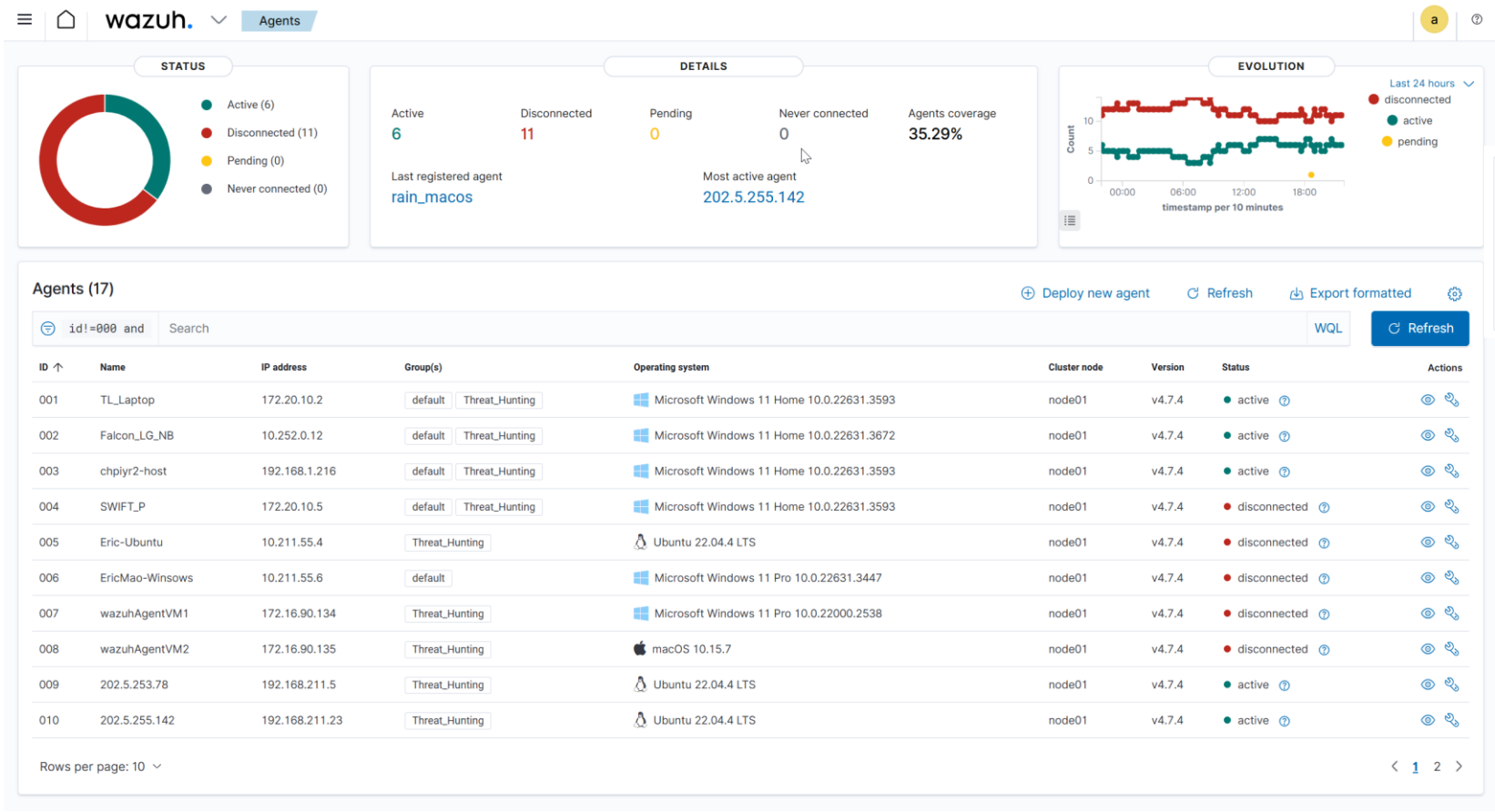
漏洞管理

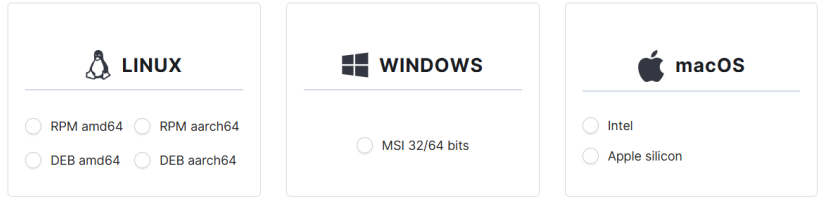
識別和評估主機系統中的漏洞，並整合漏洞資料庫，追蹤和管理系統中的弱點。

日誌分析

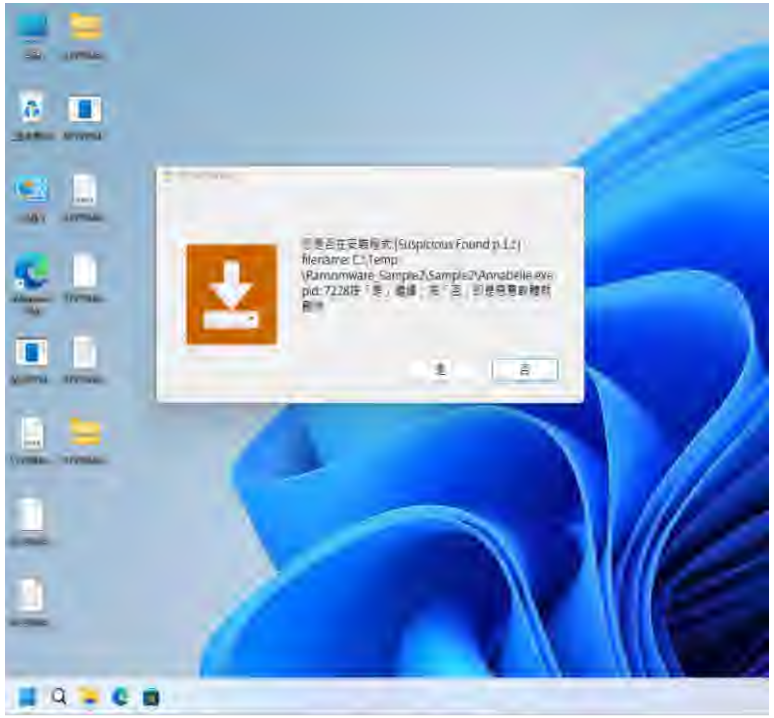
監控和分析主機系統和應用程式的日誌，識別異常行為與可能的威脅，並支援安全事件的調查和分析。

ATHS agent 支援多種作業系統環境 (Windows、Linux、MacOS)





RDS (Ransomware Detection Service)



RDS係針對需植入本機電腦，並自動執行的勒索病毒，所開發出的端點主動防禦勒索軟體。

- 能精準判斷出勒索病毒程式的名稱並將其自動刪除；更由 於操作簡單，過程幾乎全自動，所以使用者僅需具備電腦基本操作 能力即可正確操作此防禦軟體
- 可以配合其他防毒軟體一起運行達到雙重防禦功能
- 對新的勒索病毒也有一定的防護能力

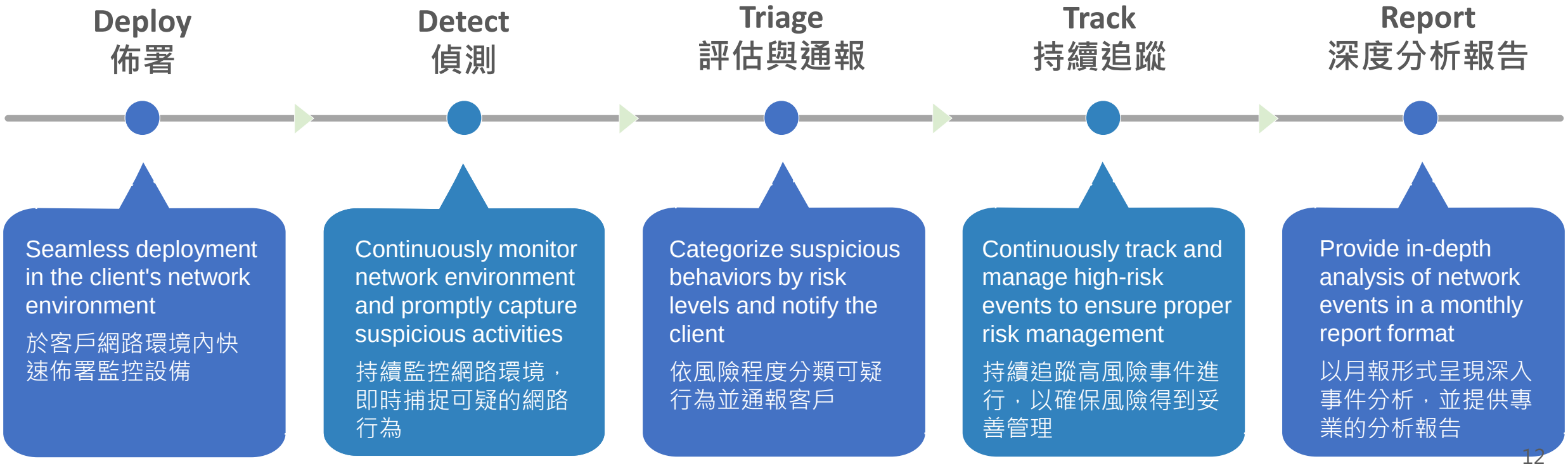
威脅獵捕服務說明

7X24資安監控

線上諮詢

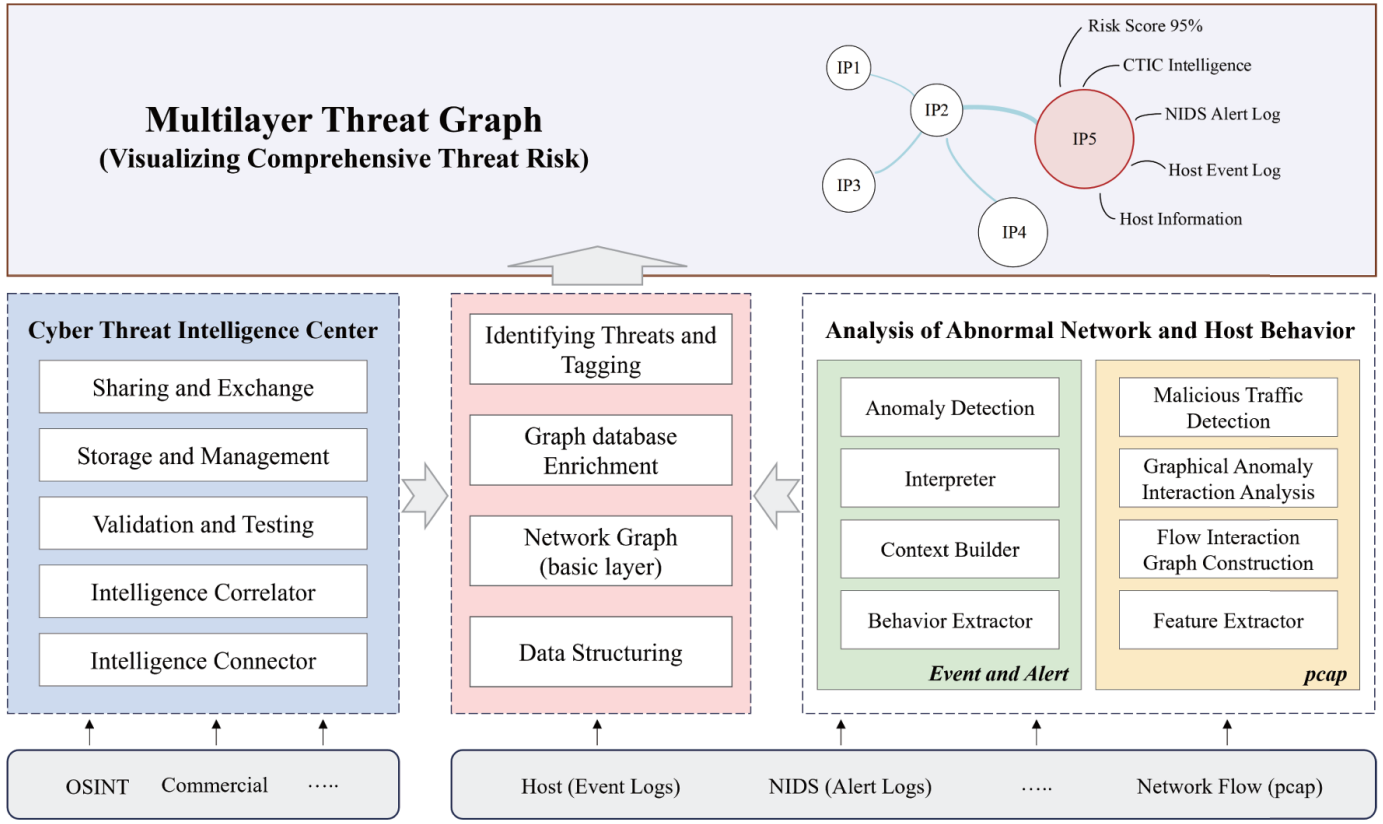
定期資安監控報告

資安專家團隊服務



Threat Hunting Platform

ATHS 提供一個強大的威脅獵捕平台，協助威脅獵捕人員即時偵測、分析並回應網路威脅。此外，它使用多層次威脅圖 (Multilayer Threat Graph) 將組織當前的網路威脅風險情況進行視覺化呈現



Multilayer Threat Graph

Capture: Preventing Breaches

利用客戶主機端點、網路流量和身份收集高保度的真安全遙測數據進行索引，以便快速有效的存取

Analyse: Identifying Threats

利用人工智慧、行為分析及專業威脅獵捕團隊的組合，即時辨識並阻止新興的進階威脅

Enrich: Contextual Data Injection

利用圖形資料庫將原始資料與威脅情資等外部來源相互結合，為資料注入上下文，使其不再單一，豐富其價值

Act: Rapid Response

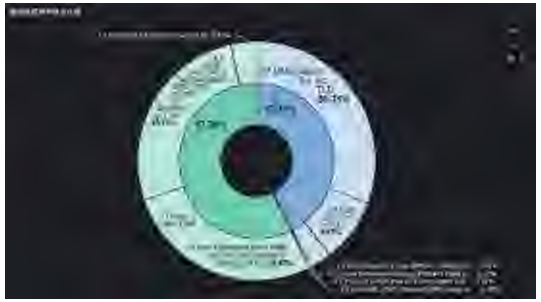
提供快速、無阻礙的資料存取，使事件應變人員和威脅獵捕團隊能夠快速偵測、回應並預防大規模的破壞

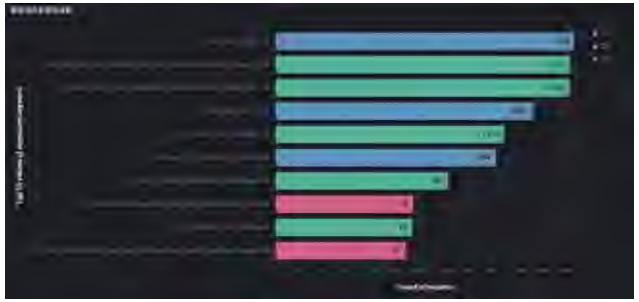
Threat Hunting Report

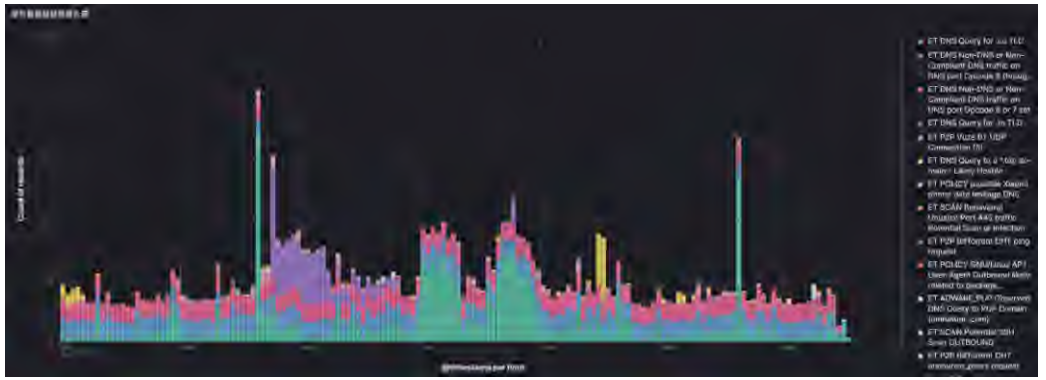
事件編號	20231206-001-AICTD	本週未觸發	
事件名稱	惡意軟體 Win32/PlugX 變種 CnC 活動		
事件類別	Malware		
風險程度	1		
觸發規則	ET MALWARE Win32/PlugX Variant CnC Activity		
事件描述	檢測到 Win32/PlugX 變種的 Command and Control (CnC) 活動，事件中的源IP是10.0.5.230，目的地IP是8.217.48.154。		
影響範圍	SCR IP	警報次數	觸發警報種類數
	10.0.5.230	0	
	DEST IP		
	8.217.48.154	0	
事件分析	在監控期間，源自 IP 地址 10.0.5.230 的網路流量顯示了 Win32/PlugX 變種的 Command and Control (CnC) 活動，指向目的地 IP 地址8.217.48.154。這種活動通常與惡意軟體相關，暗示著可能的安全漏洞。 客戶已確認 10.0.5.230 是一台網域控制站，主要用作檔案伺服器。為了解決這個問題，客戶已經建立了一台新的檔案伺服器，以取代先前展現可疑行為的舊伺服器。值得注意的是，新伺服器保留了舊伺服器的 IP 地址 10.0.5.230。然而，我們在後續的監控中發現，即使在新伺服器部署後，相同的異常行為仍然持續發生，源自同一個 IP 地址。 與客戶進一步溝通後，我們了解到雖然他們建立了新的檔案伺服器，但舊伺服器中的數據被直接轉移到了新伺服器上。這引發了一個重要的擔憂：如果舊伺服器上的數據已經被感染或受到污染，那麼這些惡意文件可能已經被無意中轉移到了新的檔案伺服器上。這樣的情況可能導致網路安全威脅持續存在，即使硬體設備已經更新。		
建議	對新檔案伺服器進行全面的惡意軟體掃描，以識別和清除任何可能的受感染或可疑文件。		

Security Monitoring Report

- NDR analysis
- EDR analysis
- Comprehensive Analysis
- Risk assessment
- Intelligence Report







The Value of Threat Hunting

Early Threat Detection

威脅獵捕能夠及早識別和追蹤潛在威脅，使組織在攻擊發生前採取適當行動。

Reduction of Damage

通過進行威脅獵捕，組織能夠迅速識別惡意活動和攻擊者戰術，從而減少攻擊造成的潛在損害。

Enhanced Overall Security

威脅獵捕通過解決漏洞、加強安全配置以及實施其他安全措施來提升整體安全性。這包括修補漏洞、消除安全漏洞、加強身份驗證和授權機制以及實施安全政策和標準。

Improved Threat Intelligence

威脅獵捕提供寶貴的威脅情報，幫助組織了解攻擊者的技術、技術和策略。這些威脅情報可用於改進安全防禦，並與其他組織共享，增強安全社群的集體防禦能力。