把重複的事自動化，一週工作 4 小時
- 將心力投資於副業

Wave Lo | Technical Consultant Director | AIShield Co.

2025/04

艾盾資科團隊成員經歷

AISHIELD

我們與其他顧問公司的差別
不是紙上談兵，我們懂如何落地實踐

我們與其他代理商的差別
不是只懂台灣，成員具備知名外商原廠經驗

我們與其他服務提供商的差別
不只是用產品，我們懂日誌解析與維運

AISHIELD

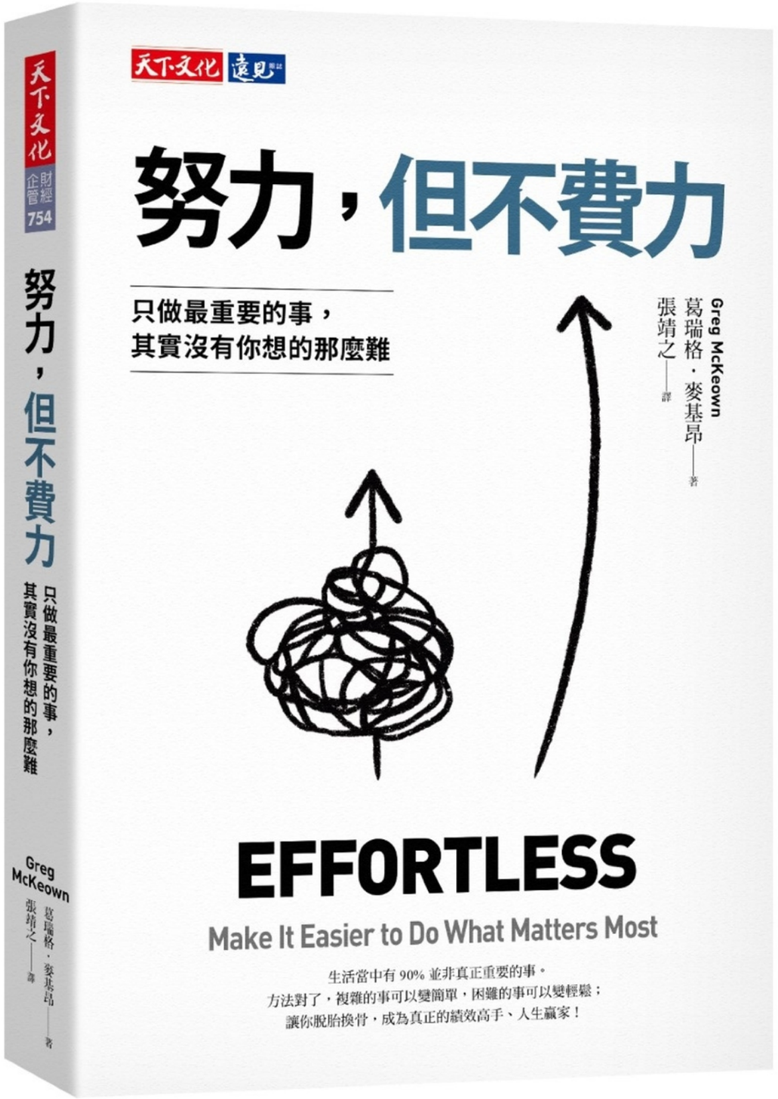
誰說做資安會過勞？

AISHIELD

在AI的時代，如果您感到過勞

那就是尚有改善空間

AISHIELD



生活當中有 90% 並非真正重要的事。

方法對了，複雜的事可以變簡單，困難的事可以變輕鬆；

讓你脫胎換骨，成為真正的績效高手、人生贏家！

只要有好的策略，化繁為簡，我們不必過勞，也能輕鬆做好更多重要的事。從此刻開始，讓我們以嶄新的姿態，迎向輕省的人生。

Source：https://www.books.com.tw/products/0010912262

打造全方位的業務營運發展、數位永續系統之資安磐石
- 用智慧取代勞力密集作業

AISHIELD

cynomi

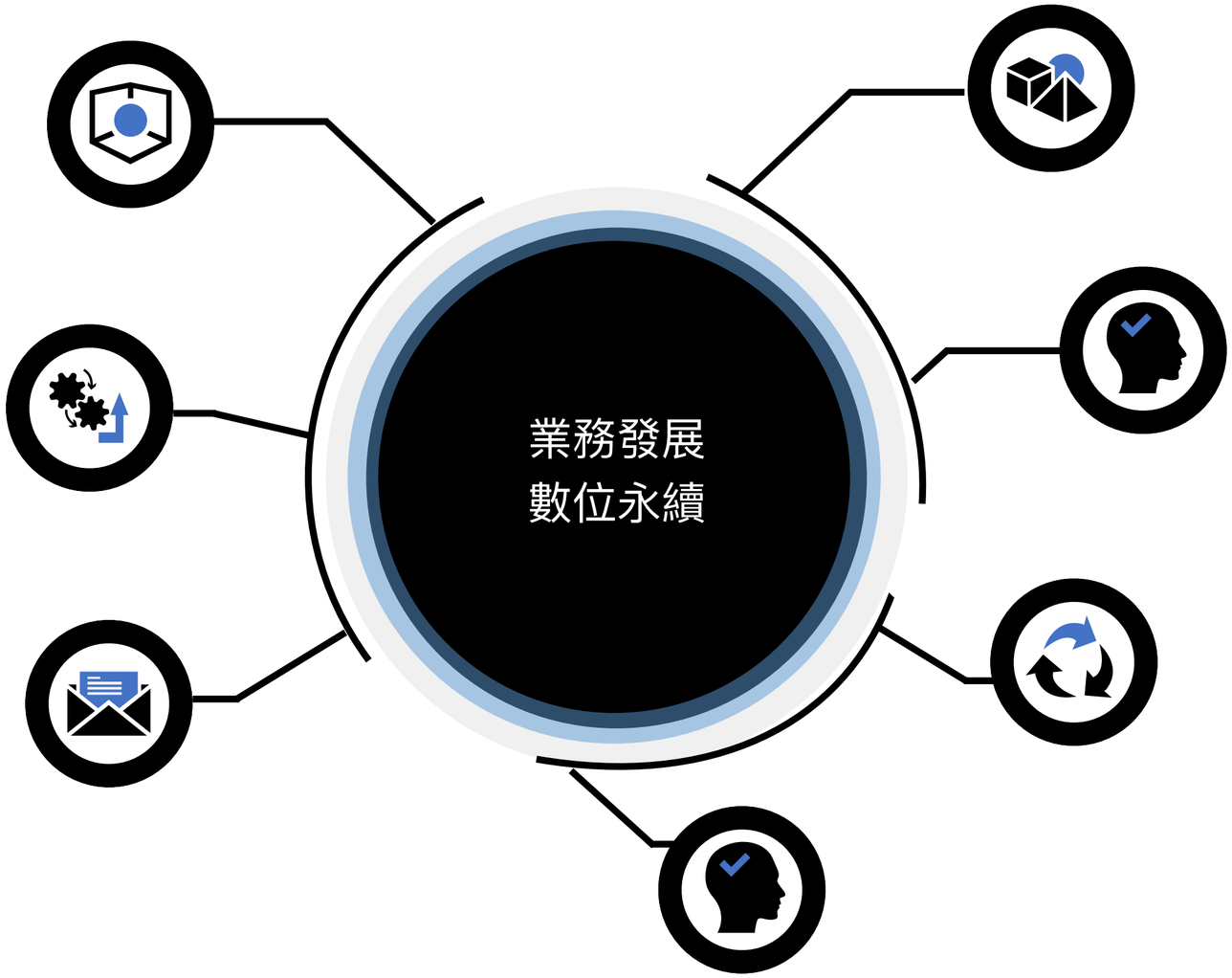
以 vCISO 虛擬資安長為企業發展
核心方針，擬定資安發展策略

WIZ

以再生能源之共享基礎建設，
加速數位系統與人工智慧發展

watchTowr

建立良好資訊系統衛生習慣
輔以 AI 科技建立首道防線



打造全方位的業務營運發展、數位永續系統之資安磐石
- 用智慧取代勞力密集作業

AISHIELD

cynomi

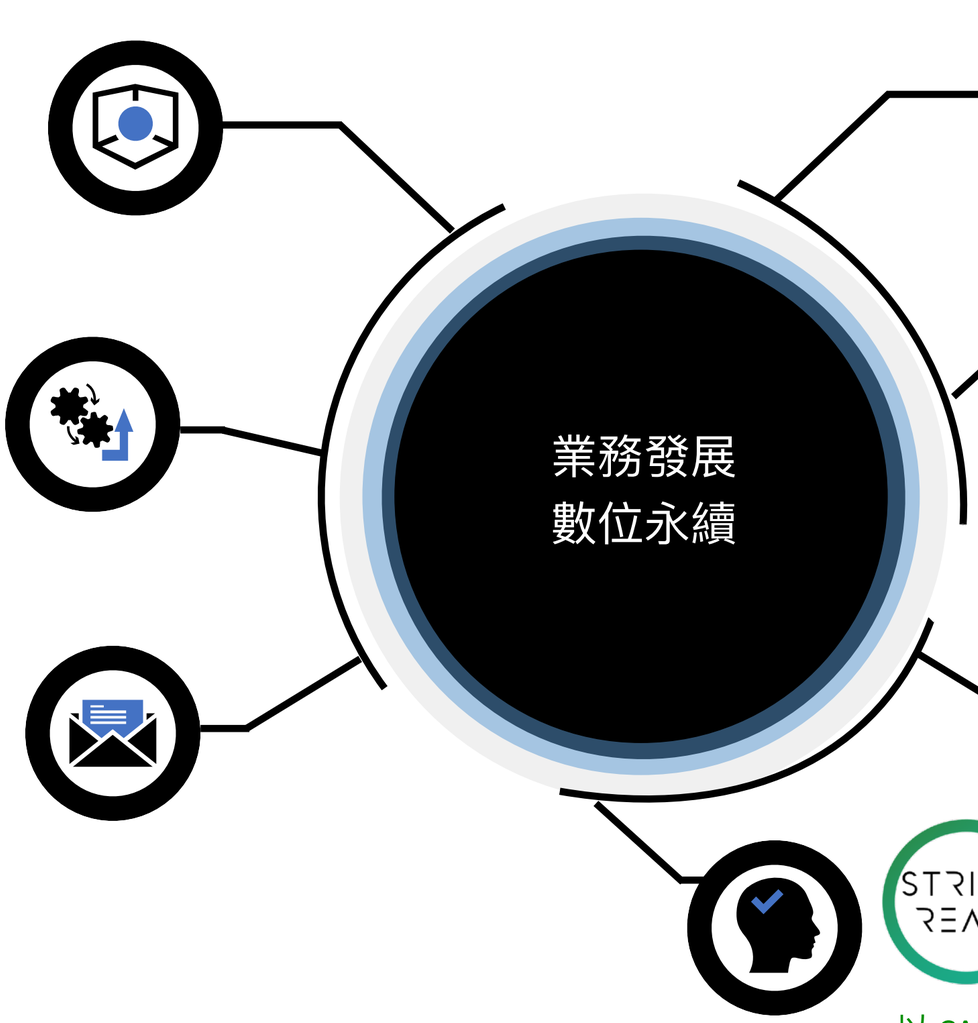
以 vCISO 虛擬資安長為企業發展
核心方針，擬定資安發展策略

WIZ

以再生能源之共享基礎建設，
加速數位系統與人工智慧發展

watchTowr

建立良好資訊系統衛生習慣
輔以 AI 科技建立首道防線



SEVCO SECURITY

減少穀倉營運現況，強化系統整合、
知識整合之共享決策平台

INTEZER

以 Agentic AI 建立數位永續風險控管
程序，成企業永續發展根基

<PRE™

以 ML、DL 建立資訊系統(IT) + 營運系統(OT) 等
智慧模型，打造數位永續供應鏈生態系

STRIKE READY

以 CARA AI 建構外部威脅資訊整合大平台，
系統設備共享數位產業知識


CYBERSECURITY REPORT
RISK ASSESSMENT
THREAT DETECTION
SECURITY METRICS
COMPLIANCE

Agentic AI SOC 資安風險管理戰情指揮中心

AISHIELD

(委外) SecOps Teams

資訊安全長

利害關係人之
外部參訪

永續治理報告

CIS Controls
NIST ISO 27001 Information Security Management
PCI DSS COMPLIANT AICPA SOC

20+ 合規性框架報告

雲端與容器化風險狀態

Open Issues
Current versus a month ago

0 Critical Issues	174 Medium Issues
0 High Issues	347 Low Issues

WIZ

組織曝險漏洞可被利用現狀

Continuous Assurance

16 Open findings

Critical
There are 4 Critical open findings.

4 Critical 11 High 1 Medium 8 Low 0 Informational

持續性外部密碼撞庫攻擊

Credential stuffing

18 Total attempts
- 0 Successful attempts
- 17 Unsuccessful attempts
- 1 Out - Of - Scope

EDR/IDP/SIEM/Cloud 告警調查結果

21,056 Ingested alerts	22,575 Monitored devices	2 min 34 sec Average investigation time
3.46% 729 Escalated	13.25% 2,790 Follow up recommended	83.29% 17,537 No action needed

INTEZER

資產與產品部署差異分析

Endpoint Security

1,522 of 2,198 Gaps 69.2%

SEVCO SECURITY

資產/帳號/環境威脅預測

Logs Ingested: 1,054,383

Asset Detections 6,668	Asset Predictions 2,227
User Detections 2,409	User Predictions 1,716
Network Detections 62,390	Environment Predictions 47

<PRE

EDR: Microsoft Defender for Endpoint · CORTEX XDR BY PALO ALTO NETWORKS · CROWDSTRIKE · SentinelOne

SIEM: Microsoft Sentinel · CORTEX XSIAM · splunk> SIEM · IBM Radar

CNAPP: WIZ

ASSET: zscaler · VMware vSphere · tenable · ivanti · RAPID7 · DUO · Qualys · Microsoft Intune · Red Hat · TREND MICRO · FORESCOUT · ManageEngine · CYBERARK · Meraki · jamf PRO · Active Directory · Nessus

WIZ
雲端安全可視化

INTEZER
駭侵監控自動化

STRIKE READY
情資處理標準化

SEVCO SECURITY
資產衛生正規化

watchTowr
漏洞曝險透明化

cynomi
合規制度一致化

<PRE
超前部署智慧化

Agentic AI SOC 資安風險管理戰情指揮中心架構

AISHIELD

已建產品資料收攏

- 端點防護
- 防火牆
- NAC
- NDR
- 弱掃軟體
- OT Data
- 郵件防護
- EDR
- IdP
- CNAPP

Agentic AI SOC

Asset Telemetry Data

SEVCO SECURITY

IT Management

200+ 外商產品整合

Intelligence Deploy

Remediation Actions

Raw Log

PRE™

Agentic AI SIEM Platform

(Parser-less SIEM)

STRIKE READY

CTI Manangement

400+ 外商產品整合

Alerts

Raw Alerts

WIZ Defend Alerts

INTEZER

EDR, IDP & Cloud Management

CS, S1, MDE MS XDR, PA, Extra ID, Okta, WIZ*

WIZ Fortune 100, 45% choose

cynomi

Cyber Security Governance Management (vCISO)

External Attack Surface Management

資安專家顧問

Monitor and Investigate

Alerts & Incidents

專家顧問解析

1. 威脅情資自動化部署 (SR)
2. 企業網域郵件密碼外洩偵測 (SR)
3. 釣魚郵件防護管理 (Intezer)
4. EDR 產品告警與即時記憶體分析 (Intezer)
5. 沙箱惡意程式解析 (Intezer)
6. 應用程式與腳本基因分析 (Intezer)
7. AD User Account 異常登入行為解析 (Intezer)
8. Cloud 公有雲平台異常行為分析 (Intezer)
9. 資產保護覆蓋率管理 (Sevco)
10. 端點授權採購管理 (Sevco)
11. 資產弱點與軟體安裝管理 (Sevco)
12. 資安治理與合規框架 (Cynomi)
13. 資安內外部曝險概況 (Cynomi)
14. 外部漏洞曝險管理 (WatchTowr)
15. 持續性密碼撞庫攻擊 (WatchTowr)
16. 資產/使用者/環境威脅預測 (PRE Security)
17. 雲端安全 All in One 平台 (WIZ)

跳脫同一種類產品從 A 品牌換 B 品牌的迷思
- 以 Agentic AI 將產品發揮到極致

AISHIELD

	1. 和平時期全面的治理活動	2. 事前與事中的防範	3. 事後的事件應變(IR)
Agentic AI 產品組合搭配	cynomi SEVCO SECURITY WIZ <PRE™	watchTowr INTEZER	SEVCO SECURITY INTEZER
應用場合	• 台灣市值 Top #20 執行資安年度計畫規劃 • 台灣市值 Top #20 執行全球資產衛生規劃 • 台灣市值 Top #100 的雲端安全重生計畫	研究機構 PHP CVE 2024-4577 重大漏洞協防成功案例	• 某大學遭 Flax Typhoon 攻擊的 IR 專案 • 某上市櫃公司遭 Crazy Hunter 攻擊 IR 專案*
實際使用	1. 作為現狀與業務目標之差異分析 2. 編列資安預算與擬定計畫執行方針 3. 持續追蹤修繕作業與新興科技規範訂定 4. 控制措施有效性之分析管理與改善措施 5. 重新定義雲端安全開發與維運管理方針 6. 環境參數演算恐遭受攻擊超前部署策略	1. 24 小時內通知客戶受 php 漏洞影響 2. 駭客於 48 小時內始進行攻擊活動 3. 艾盾早於該 MDR 廠商至少 2天前通知	1. 快速盤點 Shadow IT 讓 IR 團隊部署 EDR 2. 超過 20K+ EDR 端點解析後提供 IR 團隊使用 3. 提供惡意程式之基因檢測分析結果

以 Agentic AI 將事後左移至事前的自動化維運部署與預測，強化 ESG 永續治理、減少公關與財務危機

KEY Takeaway

AISHIELD

誰說做資安會過勞？

Agentic AI SOC 資安風險管理戰情指揮中心

只要你想得到，AI 都做得到！

用對策略，以 Agentic AI 把複雜的事變簡單、
把困難的事變輕鬆

公司過勞的絕對不會是資安從業人員，
資安人應省下工時以創造自己的副(興)業(趣)