SentinelOne

SentinelOne Vigilance

24×7 MDR 和 DFIR 服務

隨著新興威脅的數量以指數速度和範圍增長，全球組織正面臨著經驗豐富的網路安全專業人員短缺的挑戰，這一挑戰加劇了他們減輕風險的難度。隨著威脅形勢持續演變，安全運營中心和企業安全團隊正在轉向由自主網路安全支持的經驗豐富的威脅服務團隊，以加速其威脅調查和應對能力。

SentinelOne Vigilance 是一個全天候 24x7 的受管式檢測與回應（MDR）服務，旨在為我們的自主 Singularity™ 平台提供補充。

Vigilance Respond 讓安全團隊能夠將威脅調查和應對工作交給 SentinelOne 全球的網路安全專家團隊，讓您的團隊能夠專注於更具戰略性的事務。安全團隊還可以通過 Vigilance Respond Pro 將數位鑑識和事件應對 (DFIR) 服務添加到其標準 MDR 服務中。

事件處理速度平均只需 20 分鐘以下

Vigilance MDR 優異的事件處理速度源自於人工智慧自動化建立事件關聯，並由團隊一、二及三線工程師即時分工，優化事件處理速度。

想了解更詳細資訊？

管理平台：s1.ai/platform
Vigilance：s1.ai/vigilance

- **專業團隊**
  不進行外包
- **專業信任**
  深受全球各地大型組織信賴
- **實現價值**
  MDR 及 DFIR 服務
  降低 SOC 團隊負擔

Vigilance Respond

Vigilance Respond MDR 訂閱式服務可強化客戶資訊安全團隊架構，並降低資訊安全團隊工作量

+ 處理管理平台所有事件、不遺留未處理事件
+ 所有威脅事件都有專人分析、處理且加以記錄供管理者查閱
+ 重要與緊急事件通知，可確保使用者掌握站內資安情況

- 24 x 7 x 365 不間斷資安服務
- 威脅事件快速分流得以優先解決重要事件
- 降低告警數量 強化事件資訊
- 加速事件處理進程
- 簡潔的儀錶板
- 主動通知緊急事件
- 執行摘要與報告
- 定期致電關心客戶

Vigilance Respond Pro

Vigilance Respond Pro 在 Vigilance Respond 服務之上額外提供數位鑑識 (Digital Forensics，DF) 及威脅事件處理 (Incident Response，IR) 服務

+ 涵蓋所有 Vigilance MDR 服務及更多項目
+ 直接與鑑識專家溝通，討論事件處理方式、威脅阻斷及資安諮詢服務
+ 事件處理保留時數可用於惡意程式分析及 IR 威脅事件處理

- 2 倍速事件處理
- 威脅情資導向主動式威脅獵捕
- 年度 IR 事件處理服務保留時數
- 數位鑑識服務及惡意程式逆向工程
- IR Case 專責經理
- 事件處理、威脅關聯及清除
- 事件根因分析服務
- 事後檢驗顧問服務

Vigilance MDR 運作模式

威脅事件偵測
由 AI 系統快速將威脅事件自動分類分流，得以優先處理重要事件。

分析人員深入研究
分析師利用豐富的端點遙測、威脅情報及其他威脅詳細資訊以調查各個威脅。

威脅事件資訊解析
所有威脅事件皆進行註記且針對事件加以說明，可以確保管理者確實掌握環境內資安情況。

處置建議和後續動作
Vigilance 團隊即時完成威脅事件處置，並視情況需求主動通知管理者採取後續措施。

持續調整
建議並實施 SentinelOne 偵測引擎的例外。

	Respond	Respond Pro	服務內容
24×7 MDR	✓	✓	• 針對每個主控台威脅進行審核、採取行動與記錄 + 全面的應變能力 + 主動通知 • 新興威脅應對
Watchtower	⊕	⊕	• 針對攻擊者技術、全球 APT 活動和新興網路犯罪進行主動式活動威脅獵捕 • 在環境中偵測到威脅時發出威脅公告和警報
Watchtower Pro	⊕	⊕	• 每年兩次深入地威脅獵捕和入侵評估 • 無限制地存取訊號獵捕函式庫，以儲存自訂和預先建立的獵捕查詢
威脅調查	✓	✓	• 主控台指標和動態分析
DFIR 調查		✓	• RCA 感染向量、外洩確定、情報驅動獵捕、威脅情報豐富化和脈絡化、惡意軟體逆向、記憶體分析和程式碼擷取、惡意程式碼反混淆
IR 保留器		✓	• 隨依需求調查 • 預設保留時數（使用或遺失） • 調查 → 主動遏制 → 根除 → 報告 • 指派 IR 案例管理者 • 每次事件至少補充 4 小時
應變準備好審核		✓	• 動態季度報告以進行配置強化（代理程式健康度、原則和配置、強化建議） • 威脅 / 攻擊者趨勢

圖例：✓ 包含　⊕ 附加元件

Gartner Peer Insights™

“Vigilance Respond 很快就為我們的全球組織賦予很高的價值。”

IT 安全性和風險管理角色
服務業，50M-250M USD

“在可用性、偵測、預防能力、SLA 遵守方面提供優質服務。”

基礎設施和營運角色
媒體公司，500M - 1B USD

Vigilance 支援 FedRAMP Moderate 組織

Innovative. Trusted. Recognized.

Gartner
A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY™
Record Breaking ATT&CK Evaluation
+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights™
96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com
代理商 橙鎔科技 sales@ortech.com.tw
+ 886 2 8751 5663

© SentinelOne 2024