SentinelOne

WatchTower™

透過 24/7 即時威脅獵捕和調查加強 SecOps

隨著全球威脅情勢的複雜性和範圍演變，資訊安全團隊需要保護動態和分散的攻擊面，防範攻擊者不斷變化的動機和技術。

SentinelOne WatchTower 提供了安全團隊所需的專業知識和主動保護，通過檢測異常和實際操作的威脅活動，利用全球 SentinelOne 的監測資料，以及行為威脅狩獵、機器學習模型和一流的威脅情報。

不堪重負的資安團隊也可以透過 WatchTower Pro 進行更深入的探索，以發現和解決環境中獨有的隱藏威脅和安全風險，從而提供您放心的保障。WatchTower Pro 提供了深入的妥協評估，可增強團隊的靈活性，並通過攻擊面映射、暗網暴露審查和外部面向的漏洞風險審查來減輕風險。

由內部威脅情報驅動

當 SentinelOne 研究人員在野外追蹤新興攻擊者，WatchTower 會從專有、商業和開放來源以及暗網中提取情報且排定優先順序，以便在機器學習的輔助下，於環境中有目的地進行獵捕。

01

WatchTower

假設、情報驅動和行為威脅獵捕、分析和遏制

02

WatchTower Pro

WatchTower + 自訂威脅獵捕與入侵評估、進階獵捕的效益

95%

的 Gartner Peer Insights 評審推薦 SentinelOne Threat Services

Gartner Peer Insights™

WatchTower

WatchTower 讓網路安全團隊能夠透過 24/7 的行為威脅獵捕和脈絡分析將資安態勢最佳化，以識別異常和惡意活動、排定優先順序，並即時獵捕針對全球組織的可疑和惡意戰術、技術和程序 (TTP)。

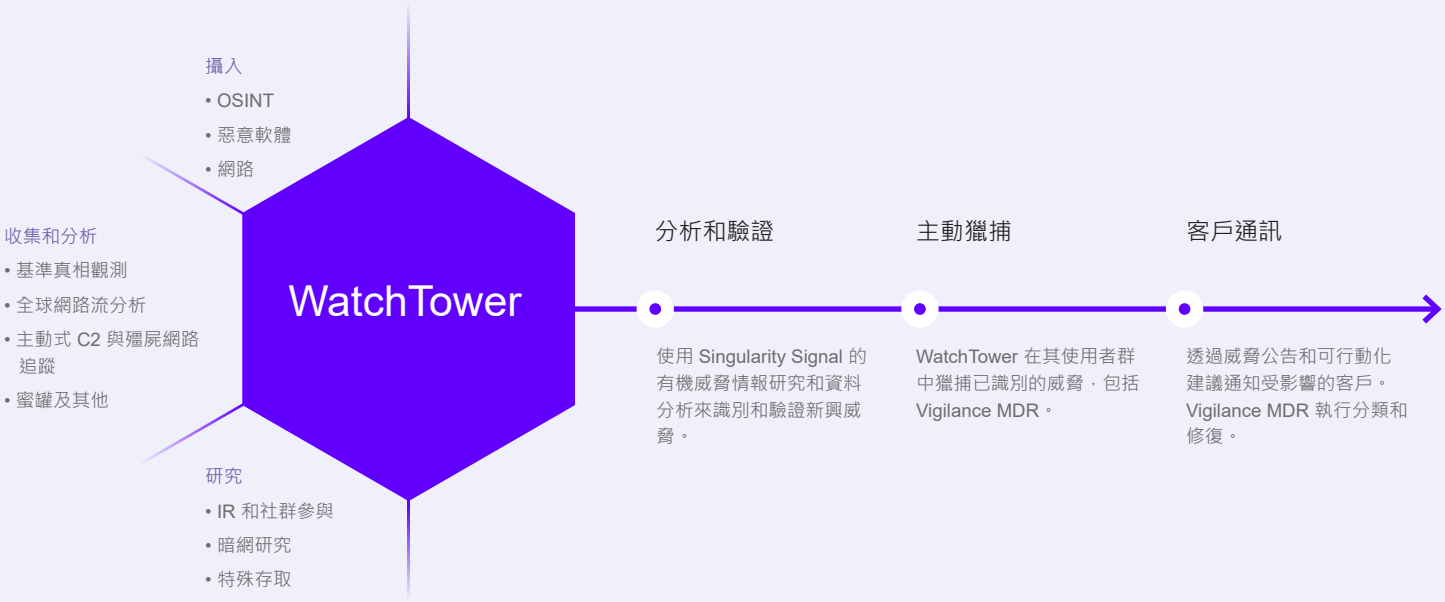
SentinelOne 的內部專家和研究人員提供假設驅動情境獵捕、實際威脅操作，以及針對新的惡意軟體、零時差漏洞、全球 APT 活動、新穎攻擊者技術和網路犯罪新興趨勢的強化偵測分析。

WatchTower 完美補足 SentinelOne 部署，提供 24/7 調查和脈絡分析，並以全球威脅情報專家團隊為後盾。WatchTower 會每月發佈獵捕摘要，其中包含我們團隊從上個月的獵捕活動中觀察到的全球威脅情勢之主要發現和趨勢。這些報告包含 SentinelOne 獨家情報及根據產業、部門、地區等提出的建議。

主要效益

+ 針對全球威脅進行實際威脅獵捕
+ 主動獵捕行為異常
+ 威脅情境模擬獵捕
+ 報告以策劃的威脅情報為輔助

WatchTower 方法



針對性

在組織內獵捕在野外發現的新興潛伏威脅。

有形

提取情報，直到最相關、可定址的詳細資訊。

可行動化

見解是為減少實際威脅而設計，而非僅為了覺察。

WatchTower Pro

WatchTower Pro 將 SentinelOne 的同類最佳威脅獵捕服務個人化，提供指定威脅獵手以進行自訂威脅獵捕，並對您的環境量身打造出全企業風險分析。WatchTower Pro 讓具有風險意識的組織能夠詳細評估攻擊面、整體風險態勢和內部資安實務 — 全都透過指定威脅獵手和專家支援團隊來提供。

使用 WatchTower Pro 的常見案例

- 入侵後（內部或產業內）
- 併購
- 新進或變動人員
- 組織安全性與風險評估

指定獵手將在深入獵捕後提供關於其所發現的自訂報告，並將在下一季進行驗證獵捕，以確認您的團隊已適當修復和解決先前偵測到的問題。他們的客製化建議是設計來用於及時填補資安缺口且建立組織韌性。Vigilance Respond 和 Vigilance Respond Pro 客戶也可以仰賴 MDR 分析師替他們執行修復和復原。

雖然 WatchTower Pro 由我們經驗豐富的團隊為您服務，但您可以隨時依照自己的條件進行獵捕且無限制地存取 WatchTower 獵捕函式庫中的威脅情報、獵捕查詢和 YARA 規則。函式庫依威脅行為者、活動、惡意軟體族系和 MITRE 戰術進行標記和排列，使獵捕變得簡單且易於存取，不需要全職情報團隊。

主要效益

+ 主動、客製化的保護，為您的環境量身打造威脅獵捕
+ 由指定威脅獵手提供個人化服務，且隨依需求提供針對性獵捕 / 威脅情報研究
+ 透過攻擊面映射和暗網暴露分析來減輕風險
+ 無限制地存取 WatchTower 威脅情報和獵捕查詢 / YARA 函式庫

透過 WatchTower Pro 深入地探索

WatchTower Pro 徹底且精準地捕捉您的資安態勢，包括外部和內部風險因素。指定獵手不僅會搜尋外部威脅的存在，也會搜尋使您暴露在風險中的內部實務和不當使用。

WatchTower Pro 流程

ONGOING
瞭解您受到的特殊影響
洞悉新興威脅對您的產業、部門、地理區域等影響

每年 2 次
深入地探索您的資安態勢
與指定獵手團隊協作，搜尋隱蔽威脅、入侵指標和高風險實務

每年 2 次
建立對防禦的信心
確認先前發現的問題是否仍然存在或已透過驗證獵捕而成功解決

	WatchTower	WatchTower Pro 包含 Watchtower
全球獵捕團隊 24×7 威脅獵捕專家團隊	✓	✓
新興威脅偵測 全球事件、供應鏈和零時差監控	✓	✓
以情報為基礎的獵捕 主動式活動追蹤和 TTP 獵捕	✓	✓
機器學習獵捕 以精準模型識別異常事件	✓	✓
行為獵捕 實際和內部威脅攻擊模式偵測	✓	✓
威脅情報報告 每月報告和快報	✓	✓
WatchTower 獵捕函式庫 獵捕查詢	✓	✓
高級獵捕支援 指定威脅獵手提供自訂獵捕和隨依需求情報	-	✓
入侵評估 客製化威脅獵捕程式開發、報告和緩解指引	-	✓
外部獵捕 攻擊面映射、暗網暴露、網域模擬和漏洞監控	-	✓

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATTACK Evaluation
+ 100% Protection. 100% Detection
+ Top 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