SentinelOne

# Purple AI

AI 資安分析師能夠更早偵測、更快應對並比攻擊領先一步

安全團隊面臨的威脅越來越複雜，而警報的數量也在不斷增加，遠超過團隊所能應付的範圍。這使得工作量巨大，難以進行主動威脅狩獵，並導致人員倦怠和警報遺漏。

**Purple AI** 是業界最先進的 AI 資安分析師，可將自然語言轉譯成結構化查詢、彙總事件紀錄和指標、透過建議的後續問題和自動產生的摘要電子郵件引導各級分析師完成複雜的調查，以及透過共用調查筆記本來擴充協作—確保快速偵測、調查和應變。

有別於充當主控台聊天機器人的其他解決方案，Purple AI 是一種力量倍增器，可協助分析師以更快、更好的方式進行調查：

+ 一鍵式威脅獵捕快速啟動：以最新的威脅情報為根據
+ 智慧建議後續查詢：繼續獵捕
+ 超快速查詢和可視性：在單一檢視中呈現原生和第三方資料
+ 共用調查筆記本：跨團隊協作
+ 直接回答 SentinelOne 支援問題：讓您不必搜尋線上文件

## 充分發揮資安團隊的潛力

### 簡化複雜性

透過智慧化方式結合常用工具，將威脅情報和脈絡見解合成為單一對話式使用者體驗，以簡化調查。

### 提升所有分析師的水準

找出隱藏風險、進行更深入的調查、更快速地應對—全都使用自然語言。根據自然語言提示透過 Power Query 轉譯來訓練分析師。

### 將獵捕從幾小時縮短成幾分鐘

利用正在申請專利的獵捕快速啟動、AI 驅動分析、自動摘要和建議查詢來加快 SecOps。透過在已儲存且可共用的筆記本中無縫協作進行調查，以節省時間。

### 保護資料

利用專為資料保護和隱私而設計的解決方案。Purple AI 從未受過客戶資料訓練並設有最高等級的保護措施。

## Purple AI 差異

**+80%**

早期採用者表示威脅獵捕和調查速度加快

### 以單一主控台、平台和資料湖確保速度和可視性

透過單一控制台、單一平台和業界最高效能的資料湖加快運作且更清楚地綜觀全局。Purple AI 是唯一理解 OCSF 紀錄的 AI 分析師，因此您可在單一正規化檢視中立即查詢原生及合作夥伴資料。

### 威脅獵捕快速啟動和引導式調查

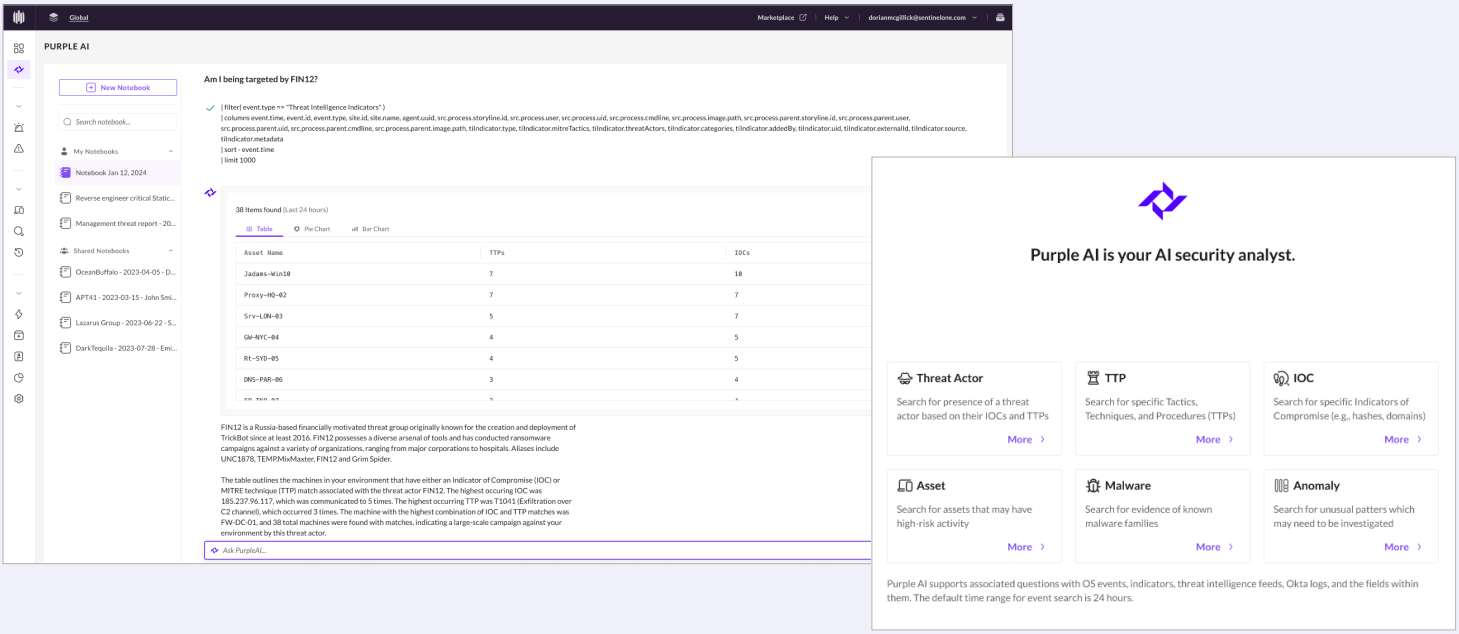
正在申請專利的獵捕快速啟動函式庫可協助所有分析師縮短 MTTD 且主動找出風險。利用智慧化、根據脈絡建議的後續查詢以自然語言繼續調查。

### 加快全面協作

自動產生可供團隊共用的威脅摘要、報告和通訊，並透過在已儲存、共用且可編輯的筆記本中協作以減少不必要的往返。

### 開放且可靠的 AI

AI 不應該是黑盒子。
透過 Purple AI，您可以輕鬆地檢視查詢轉譯以進行驗證和分析師訓練。Purple AI 也經過精心設計，具備防止不當使用和幻覺(AI hallucination)的保護措施。




# 主要特色

- 將自然語言轉譯為結構化的 PowerQueries，以搜尋隱藏風險。透過自然語言完整檢視查詢和彙總結果，以取得可信的成果。
- 超快速查詢和更高的可視性。Purple AI 以 Singularity Data Lake 為基礎，是唯一支援 Open CyberSecurity Schema Framework (OCSF) 的 GenAI 分析師，在單一正規化檢視中提供原生和第三方資料。
- 正在申請專利的威脅獵捕快速啟動讓分析師能夠使用基於領先的威脅情報以預先填入查詢，只要按一下，即可主動獵捕威脅。
- 使用建議的上下文跟進查詢，以進行更深入的調查。
- 利用 AI 驅動的威脅分析和摘要更快地呈現可行動化見解。
- 回顧自動儲存的私人調查筆記本或在共用筆記本中促進跨團隊獵捕協作。

## 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 · 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · 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

sales@sentinelone.com
+ 1 855 868 3733