FIREEYE™

集成式資安架構綜合安全

網絡威脅繼續擴散，組織用來保護自己的工具庫也不斷增加。與其添加更多工具，不如通過集成SIEM，業務流程和語境威脅情報集中資安操作。

當今的資安監控：工具太多，語境太少

當出現新的威脅時，許多組織會購買更多的專用工具。

結果是工具太多了.....

80

平均使用的安全工具數量由美國公司[1]

這些工具會產生太多警報...

10,000

普通公司每天收到的安全警報數量[2]

而且安全團隊沒有足夠的時間來確定哪些警報很重要...

20 分鐘

對單個警報進行分類所需的時間[3]

結果，不良分子可以訪問網路絡並將其隱藏幾個月。

78 天

組織發現違規的平均時間[4]

當團隊分心更長的時間時...

30 天

組織對違規做出響應所需的平均時間[4]

攻擊者針對三個主要媒介

通常的初步入侵步驟是通過電子郵件...

EMAIL

91%

最初的入侵以電子郵件開始[5]

然後，攻擊者通過網絡傳輸被盜的數據或資產，這通常被視為最後一道防線。

NETWORK

ENDPOINT

最終，攻擊者達到了目標；位於端點上的敏感數據...

您需要將工具和數據集中化與對電子郵件，端點和網路的可見性結合起來，以清楚地了解攻擊者的目標和應對方式。

借助集成式資安架構，您可以獲得:[6]

提升可視性

300+

集成產品，大幅減少橫軸點並加快響應速度

更快的響應時間

20x

加快手動任務的速度，例如驗證警報和分類

提高效率

86%

減少分析師在無回應活動上花費的時間

更高的價值

5–7

獨立產品功能集成到一個平台中

- 安全編排，自動化和響應 (SOAR)
- 安全事件響應平台 (SIRP)
- 威脅情報平台 (TIP)
- 威脅與漏洞管理 (TVM)
- 情報驅動的安全運營中心 (ISOC)
- 安全信息和事件管理 (SIEM)
- 用戶和行為分析 (UBA)

當投資回報率不僅僅是資產負債表上的時候[6]

在日常的，容易出錯的過程上花費更少的時間

在集成安全平台之前/之後花費在核心SOC活動上的平均時間

	BEFORE	AFTER
充實和驗證	39%	5%
票務和報告	35%	10%
通知和升級	7%	5%

花更多時間在關鍵威脅識別和響應活動上

	BEFORE	AFTER
響應	10%	44%
狩獵	4%	34%

要了解有關 FireEye Helix, 的更多信息，請訪問： **www.FireEye.com/solutions/helix_tw.html**

1 Security Intelligence (January 28, 2019). Break Through Cybersecurity Complexity With New Rules, Not More Tools.
2 CSO (May 3, 2017). False positives still cause threat alert fatigue.
3 FireEye (March 2018). M-Trends 2018.
4 FireEye (March 2019). M-Trends 2019.
5 PhishMe (2016). Enterprise Phishing Susceptibility and Resiliency Report.
6 Internal FireEye performance measurement results.

FIREEYE™