FIREEYE™

產品型錄

教育服務

訓練負責網路資安的員工，以守護企業

重點

- 講師主導、線上和電子學習課程
- 高熟練度的講師具布廣泛、前線產業以及政府經驗
- 依據真實世界調查而非理論式案例的課程與練習
- 在以最新攻擊者工具、攻擊手法和程序（TTPs）模擬環境下的實際案例
- 課程全球通用，配合當地的顧問
- 一致的教育與練習方法

「我們觀察到的所有趨勢可歸納出一個結論：比起以往，各個層面專注在資安狀態都顯得更加重要（人員、程序及技術）。」

- Mandiant M-Trends 報告

持續的專業教育為資安團隊提供了他們所需的最新技能和知識，以應對他們每天所面對的日新月益的威脅。

FireEye 教育服務能強化您資安團隊的作業技能，並提升他們防止、偵測和回應網路攻擊的能力。課程汲取 FireEye 的全效能，其中包括 FireEye 產品知識、進階網路威脅情報和來自 FireEye 公司 Mandiant 所提供的資安事件前線回應的專業知識。

我們的教育服務遵循自然進展，幫助組織開發，並使他們的作業準備狀態達到成熟階段。我們特地從 FireEye 產品的基礎技術訓練轉為更寬的網路資安訓練，從 Mandiant 課程轉為實際操作的練習，團隊會在模擬環境中回應網路事件。

FireEye 產品與技術教育

FireEye 產品教育課程教授學生如何使用與管理 FireEye 產品、如何回應並偵察警報，以及如何使用 FireEye 技術成功地防衛最新網路資安威脅。每項課程將講座與實際操作結合在一個無後果的沙箱環境中，讓學生有機會使用真正的惡意軟體，但沒有現實世界的風險。我們的課程由專業講師教授，他們也是熟練的網路資安老手。

除了全系列的產品部署和管理課程，也備有分析師課程，包含警報分析與鑑識，以及使用 FireEye 產品進行的獵捕與調查。也有教授系統經理如何使用與管理 FireEye 裝置的疑難排解課程。

表 1 FireEye 產品與技術教育課程提供

講師主導的訓練 (Instructor-Led Training, ILT)

核心資安平台課程
- 網路威脅防禦 (NX 系列) 部署
- 電子郵件威脅防禦 (EX 系列) 部署
- 內容威脅防禦 (FX 系列) 部署
- 中央管理 (CM 系列) 部署
- 鑑識分析 (AX 系列) 部署
- 警報分析
- 鑑識基礎
- FireEye 疑難排解

端點威脅防禦課程
- 端點威脅防禦 (HX 系列) 部署
- 端點威脅防禦 (HX 系列) 全面調查
- FireEye HX 疑難排解

網路鑑識課程
- 網路鑑識 (PX 系列) 使用與管理
- 網路鑑識 (PX 系列) 使用與調查分析 (IA 系列)

FireEye Helix 和威脅分析課程
- 威脅分析平台 (Threat Analytics Platform, TAP) 部署
- FireEye Helix

Mandiant 情報回應 (Mandiant Intelligent Response, MIR) 課程
- 企業資安事件回應 (Enterprise Incident Response, EIR) 與 MIR
- 進階 MIR

自我學習的線上課程

核心資安平台課程
- FireEye 平台概觀
- 網路威脅防禦 (NX 系列) 部署
- 電子郵件威脅防禦 (EX 系列) 部署
- 內容威脅防禦 (FX 系列) 部署
- 中央管理 (CM 系列) 部署
- 鑑識分析 (AX 系列) 部署
- 電子郵件威脅防禦 - 雲端版 (Email Threat Prevention, ETP)

端點威脅防禦課程
- 端點威脅防禦 (HX 系列) 部署

網路鑑識課程
- 網路鑑識 (PX 系列) 部署

惡意軟體鑑識與分析
- 惡意軟體鑑識介紹
- 惡意軟體二進位分析介紹

來自 Mandiant 的網路資安教育

Mandiant 網路資安教育課程將 Mandiant 豐富的第一線經驗攝入此課堂中。擁有超過 14 年站在第一線的網路資安與網路威脅情報經驗、回應過許多全球最複雜的入侵事件，Madiant 對於現有和新興的威脅發動者以及他們快速變動的工具、攻擊手法和程序，皆有深入的了解。

因爲這項專業技能，Mandiant 網路資安教育課程將實用、實際的資安架構直接帶入課堂。學生獲得有關攻擊者 TTPs、惡意軟體威脅發動者用來發動攻擊的工具，以及偵測和回應那些攻擊有效方法的第一手知識。

課程講師也是每日處於本領域的從業人員，他們回應攻擊、分析新惡意軟體範例或與企業網路執行紅隊演練合作。這些課程透過講師主導的講座和實際操作實驗室所支持的討論相結合的方式，提供最佳的學習體驗，所有內容皆由最新網路威脅情報提供。

表 2 網路資安教育課程提供

資安事件回應與鑑識	惡意軟體分析	網路資安與情報
• 企業的事件回應	• 惡意軟體分析基本課程	• 針對高階主管的網路犯罪介紹
• 網路流量分析	• 惡意軟體分析速成課	• 屬性介紹
• UNIX/Linux 調查	• 惡意軟體分析專家課	• 無線網路資安
• Windows 調查	• 逆向工程的 MacOS 惡意軟體分析	• 創意紅隊演練
• 路由器後門程式分析	• 自訂惡意軟體分析	• 針對資安專業人員的 Linux 介紹
• PLCs 數位鑑識與資安事件回應		

ThreatSpace

ThreatSpace 是一項技術驅動的服務，讓您的組織可以評估並開發其資安團隊的技術能力、流程和程序，以在不帶後果的環境下，回應真實世界的威脅。在 ThreatSpace 評估期間，團隊調查在使用模擬典型 IT 基礎架構（如網路區段、工作站、伺服器和應用程式）的虛擬化環境中的模擬攻擊案例。

作為流程的一部分，Mandiant 資安事件回應專家會幫助評估您團隊的技術能力、流程與程序。他們也會提供即時回饋與輔導，以協助提升您資安團隊對網路攻擊回應的能力。

要知道更多關於 FireEye，請參閱：**www.FireEye.com**

FireEye Taiwan | 台灣火眼有限公司
| 10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE |
taiwan@FireEye.com

關於 FireEye, Inc.

FireEye 是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴展的延伸，FireEye 提供單一平台，將創新的資安技術、國家級別的威脅情報和世界知名的Mandiant® 諮詢融合在一起。藉由此方法，FireEye 為努力準備、預防和應對網路攻擊的組織，消除資安機制的複雜性和重擔。