



M2M API 的 API 安全

對於保護機器與機器間 (M2M) API 和內部流量需與保護遭受外部攻擊同樣重要，但常常都被忽視。獨特的 Noname Security 從內到外提供您全面的保護。

完整的 API 防護就是：從內到外

Noname Security 即時保護 API，並幫助在被不當利用之前偵測到弱點和錯誤設定。Noname API 安全平台與您現有的 API 閘道器、負載平衡設備和 WAF 配合使用，透過無中斷的 out of band 整合提供深度可視化和安全性。

全面了解機器對機器的 API

- 找出所有已知和未知的 M2M API。
- 辨識哪些 M2M API 負責敏感資料傳遞或透過合作夥伴揭露公司資產。
- 追蹤資料流以更好地了解上下文中的錯誤設定和潛在漏洞。
- 找出威脅您組織安全的 Internet 相關或錯誤導流的 M2M API。

驗證是否符合最佳實務和法規要求

- 確認是否根據最佳實務部署身份驗證。
- 確認為所有合作夥伴/M2M API 正確設置授權和資料安全政策。
- 積極測試 API 以最小化攻擊面並確保安全政策符合法規要求。

即時保護流量

- 偵測憑證填充攻擊和竊取。
- 辨識 M2M API 的所有異常或異常行為。
- 自動阻擋威脅行動者和每一次針對您的 API 抓取/開採漏洞的嘗試。



API 安全狀態

使用資料分類盤點每個 API，包括舊有 API 和影子 API。

識別原始碼、網路設定和安全政策中的錯誤設定和漏洞



偵測與應變

使用基於行為的模型來進行 API 威脅偵測的。

自動化和半自動阻擋和修復威脅。



安全的 API 程式碼

持續測試 API 以在 API 風險出現之前辨識出它們。

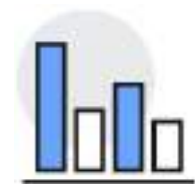
自動化且動態測試開發並整合到 CI/CD pipeline 中

Noname 如何實現 API 安全



找出所有 API、資料和 Metadata

查找並盤點各種 API，包括 HTTP、RESTful、GraphQL、SOAP、XML-RPC 和 gRPC。找出不受 API 閘道器管理的舊有 API 和惡意 API，並對 API 資料和 metadata 進行分類。



偵測 API 威脅並分析 API 行為

使用基於 AI 的自動化偵測來辨識最常見的 API 弱點，包括資料外洩、資料篡改、設定錯誤、違反資料政策、可疑行為偵測和攻擊偵測。



攻擊防護與修復 API 漏洞

即時防護攻擊、修復錯誤配置、自動更新防火牆規則、Webhook 到您的 WAF 以增加新安全政策來對可疑行為阻擋，並與現有工作流程（問題處理和 SIEM 平台）整合。



在部署至線上前積極測試 API

大多數應用程式在部署到線上之前都經過測試。但 API 並未被相同謹慎對待。作為軟體開發生命週期的一部分，更積極的測試 API，並在正式部署至線上前找出問題是首要任務。



www.nonamesecurity.com

info@nonamesecurity.com

+1 (415) 993-7371



關於 Noname Security

Noname Security 是唯一一家對 API 安全採取全面且主動做法的公司。Noname 與 20% 的財星全球 500 大企業合作，涵蓋整個 API 安全範圍的三大支柱——狀態管理、Runtime 安全與 API SDLC 安全。

Noname Security 是一家私人控股公司，總部位於美國加州帕羅奧圖，並在以色列特拉維夫和尼德蘭阿姆斯特丹設有辦事處