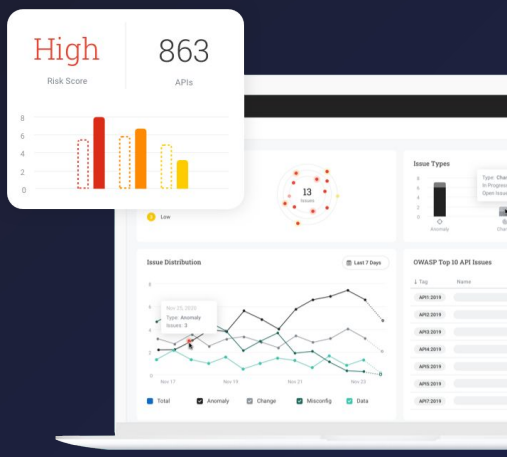
noname

產品簡介

API 安全測試

使用 Noname API 安全平台加快創新速度、降低成本並加速增長，這是唯一包含整個開發生命週期自動化 API 安全測試的完整 API 安全平台。



測試和保護您的 API。絕不妥協。

Noname API 安全平台在從開發到測試環境和正式環境，每一步都對您的 API 進行自動且全面的測試，使您的安全團隊能夠跟上應用程式開發人員的需求並達到戰略業務目標。透過在單一平台中進行 API 狀態管理、運行實時安全和主動測試，Noname Security 超越了許多獨立的解決方案和個別分開的流程，同時借助涵蓋正式和非正式環境的安全資料來確保 API 通過廣泛的弱點掃描測試。

快速且安全地進行創新

- 透過快速地開發和部署安全的 API 優先產品和服務來搶佔市場先機。
- 透過在 API 開發生命週期的每一步進行相關且詳盡的測試，減少技術債和漏洞修復帶來的拖累。
- 根據實際部署結果輕鬆建立準確的文檔，包括 Swagger 文件。

降低風險

- 透過在 API 部署至正式環境之前和之後對其進行靜態和動態分析來阻止漏洞。
- 與既有的工作流程工具和問題處理系統整合以進行快速修復。
- 減少攻擊面並改善您的整體 API 安全狀況。
- 將開發延遲的風險和成本降至最低。

降低成本

- 透過在部署至正式環境前找到和解決問題，將修復成本降低 10 到 100 倍。
- 與現有的持續整合/持續部署 (CI/CD) 系統整合，以增加目前的投資價值並降低 FTE 開發成本。
- 避免與資料洩露相關的法規罰款。
- 減少多餘的第三方安全測試工作並專注於目前該專注的重點。

協調開發人員和安全團隊

- 透過將自動化安全與您現有的 CI/CD pipeline 和流程整合來達到營運一致化。
- 將安全團隊定位為真正的業務合作夥伴和增長推動者。
- 促進提高員工留任率和士氣的 “shift left” 文化。
- 優化軟體開發和部署策略。

Noname Security 在 API 安全測試中處於領導地位

在程式碼部署至正式環境之前以及隨著您的環境與業界最全面的 API 安全平台一起發展，透過消除漏洞來主動保護 API。

嚴格且全面的測試

- 自動運行 100 多項測試以保護 API 遭受攻擊，包含 OWASP API Top 10。
- 透過動態更新從各種來源導入 API 。
- 與 API 狀態管理和運行時保護相結合，可立即偵測出漏洞。
- 在測試期間使用來自運行時的真實記錄的流量，以確保真實世界的準確性。
- 根據需求在開發環境、測試環境和正式環境中進行測試。
- 輔助滲透測試和其他安全服務

強大的靈活性

- 與現有的 CI/CD pipeline流程和工具（例如 Postman 和 Jenkins）以及問題處理和工作流系統整合。
- 輕鬆建立測試套件以符合業務目標或是團隊結構等。
- 根據組織的需求客製化調整行為測試和嚴重性測試，包含安排以期望的時間間隔自動運行測試。
- 使用基於群組的授權參數資料簡化測試，因此只有符合的團隊才能存取 API 進行測試。
- 根據應用程式、業務單元、功能能力或任何其他特徵自動或手動對 API 進行群組分類。

Noname API 安全平台

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

API 運行安全

使用基於行為的模型來進行 API 威脅檢測的。

自動化和半自動阻擋和修復威脅。

安全的 API SDLC

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

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 。

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371