IONIX

# Attack Surface Management
# 攻擊面管理 - 揭露真實攻擊面中的威脅

EASM 外部攻擊面管理已成為網路安全標準，是現代網路安全的核心組成之一。IONIX 是外部攻擊面管理的先驅，可提供您暴露在互聯網中資產的可見性、風險評估和主動保護，消除數位供應鏈風險，保護您的外部攻擊面。
EASM 是一個新興的產品，Gartner 將 EASM 定義為 “為發現企業面向外部的資產和系統可能存在的漏洞而部署的流程、技術和專業服務” ，並將 EASM 定位為 CTEM 持續威脅暴露管理（Continuous Threat Exposure Management）主要框架。

## 什麼是外部攻擊面？

其實您的攻擊面不僅包括您的組織與您的第三方供應商，您的客戶和員工在與公司連線存取的每一項資產都是構成外部攻擊面的一部份。所以，這些資產可能是您的組織所有，或是由第三方供應商擁有和營運，或者是您的 N 級供應鏈中的某個供應商，這些都可能構成組織的外部攻擊面。
簡而言之，外部攻擊面管理即是對攻擊媒介的持續發現、監控、評估、優先排序和修補。

## EASM 提供五種主要功能：

- 監控 - 持續掃描外部各種環境（如雲端服務和面向外部的本地基礎設施）、分散式生態系統（如物聯網基礎設施）
- 資產發現 - 發現未知的外部資產和系統，並將其對應到組織
- 分析 - 評估和分析資產屬性，以確定資產是有風險的、易受攻擊的，還是行為異常的
- 優先排序 - 優先考慮風險和漏洞等級，排定優先順序提供警告
- 補救 - 提供緩解首要威脅的行動計畫，以及補救工作流程或與事件系統、事件回應工具、SOAR 解決方案等系統的相互整合

EASM 應成為廣泛漏洞和威脅管理工作的一部分，以強化發現、管理內外部資產及其潛在的漏洞。
EASM 工具最常用於發現未知的面向外部資產和網路，並識別基於基礎設施的漏洞。EASM 還可以協助支援一些功能，如漏洞評估和雲端安全狀態管理（CSPM），以確定漏洞和配置錯誤的優先順序並進行補救。

## 第三方 Dependency 削弱您的網路安全防禦

一個網頁通常有數十個（或是數百個）從第三方主機提取的資源依賴項。例如：

**HTML 或 JavaScript Dependency**

Dependency 產生一個龐大的攻擊面，其中最普遍的連接是由 HTML 或 JavaScript 所產生的。這些連結可以在 HTML 圖像置入標籤、腳本標籤、CSS 和其他從第三方供應商和網站中取得資訊的標籤中找到。IONIX 可提供 Dependency 的查找和完整攻擊面的可見性。

**轉址(Redirect)**

轉址可建立使用者對網站的信任感，但需要對其進行監控和管理。IONIX 的攻擊面可見性能在單一中控台上自動顯示線上狀態中的所有轉址，不必讓資安團隊手動搜尋網站上每個頁面和每個轉址。

## 外部攻擊面可見性：第三方連接之外

在許多情況下，資源的相互依賴形成一條長鏈，而這龐大的攻擊面中的每個連接資產都可能是潛在的漏洞。透過控制單個第三方資產，攻擊者可以利用該資產的直接或間接連接來瞄準所有客戶。由於這種存取來自第三方供應商或合作夥伴，因此攻擊者可以避開組織複雜的防火牆、日誌、病毒掃描程式或其他檢測工具。如 Magecart 攻擊或是雲端資產盜用，都是第三方 JavaScript 的錯誤雲端配置所造成的漏洞，但這些可能都只是遭利用資產的冰山一角。因為近 50% 的網路攻擊是從組織的數位供應鏈發起的，IONIX 讓資安團隊能透過攻擊面可見性、持續的漏洞評估和主動保護來保護其攻擊面的每個組件。

IONIX 威脅暴露雷達（Threat Exposure）使資安和 IT 團隊可以輕鬆辨識組織的真實攻擊面及數位供應鏈中的關鍵暴露並採取行動。


### 不間斷的攻擊面管理
自動調整覆蓋範圍以適應變化並監控風險。

### 減少攻擊面
有系統地降低關鍵風險並淘汰未使用或被忽視的資產。

### 子公司風險控管
透過自動歸因集中監督並實現在地化的攻擊面管理。

### 弱點管理
透過攻擊面發現、評估和優先排序的自動化來強化既有資安計畫。

### 數位供應鏈安全
保護組織免於數位供應鏈威脅。

### M&A 併購相關風險
管理併購過程中，從評估到整合所有階段的網路風險。

### 雲端營運安全
獲取跨公有雲平台的可見性並管理風險暴露。

### 攻擊面驗證
使用自動化測試來驗證風險暴露的情況，並確認零時差威脅的可利用性（exploitability）。

• **攻擊面發現**

**發現您真正的攻擊面**

完整了解組織在數位供應鏈所有暴露的資產和有風險的連結。


• **網路風險評估**

**跨資產和連接的風險暴露**

動態監控整個數位資產和連接的風險。


• **風險優先順序**

**優先考慮最重要的事情**

根據事件影響範圍（blast radius）、可利用性和威脅情資，聚焦在當前最需要解決的問題。


• **主動威脅預防**

**更快、更多的威脅修復**

透過跨團隊明確的行動項目與工作流程整合加速風險處理，並藉由 IONIX Active Protection 實現自動風險緩解。