Panorays

供應鏈風險平台管理

側翼攻擊知多少?
供應鏈的管理為當今重要議題！

企業如何了解與管理眾多上下游供應鏈廠商？以確保供應鏈廠商不至於成為資安防護的破口！

這類供應鏈攻擊事件一再發生…

- 高科技製造業的生產機台因供應廠商的因素而遭到勒索軟體 WannaCry 變種惡意程式攻擊，最後導致數十億元的重大損失！
- 熱門的網路分析平台供應商被駭客入侵並植入惡意的JavaScript，藉此攻擊目標企業加密貨幣交易平台！
- 駭客集團Magecart透過第三方服務供應商的安全漏洞而入侵受害網站，利用惡意程式獲取消費者所輸入的個資後，再於暗網中銷售，或以這些信用卡資料進行消費！
- 知名的DevOps服務供應商開發作業流程中的工具和平台被攻擊並危害到目標企業！

許多惡意攻擊的目標由主要攻擊對象改為其供應鏈廠商來下手，也就是看準了較不重視資安防護的供應鏈上下游廠商的弱點，利用這類側翼入侵的攻擊手法來突破主要攻擊對象的資安防護。

Panorays提供單一的自動化平台，分析供應商網路安全狀態及評估政策相關風險，協助主要廠商管理其供應鏈。

> “Panorays 所提供的7*24持續監測和供應商自我評估是我最喜歡的服務”
>
> Johnny Jonathan | 資訊網路安全全球總監 SAPIENS

- 縮短審核供應商的時間
- 問卷調查過程自動化
- 可即時偵測供應商資安狀態與接收告警訊息
- 提供合規性驗證並持續更新條款
- SaaS服務，無須額外安裝任何程式

HOW IT WORKS

Outside-in
模擬駭客的入侵方式，透過Panorays檢測公司及供應商完整的數位足跡顯示第三方業者的網路漏洞

Inside-out
透過Panorays制定及管理自評表的平台，提供符合GDPR、PCI和NYDFS等的法規，也同時支援公司內部制定的政策來稽核供應商

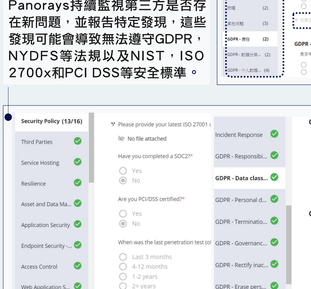
Context-Based Rating
評估標的參考了與供應商間的業務和技術關係，針對不同供應商制定不同的權重比例

BIG DATA

Actionable Insights
Panorays檢測受影響的數位資產並提供詳細的說明，易於資安團隊進行修復

※以上資訊彙整成相關聯的大數據進而評估其資安風險

Panorays讓您輕鬆管理您所有的供應商以確保企業資安防護



1.全方位能見度，將駭客的觀點與內部策略相結合
Panorays利用Outside-in與Inside-out的機制，模擬駭客的攻擊手法，以及供應商應遵循的資安政策，提供客戶資安等級的評分與建議，進而達到內外兼具全盤觀測的防護效果。

2.更有效率的使用線上調查表，縮短人工處理流程
Panorays自動定制的調查表包含與每個供應商業務相關的問題，可直接在網站上跟踪問題進度並隨法規更新調查表內容。

3.提供線上即時作業平台，改善雙方資訊不對等
可在同一平台上和供應商討論或檢視評估表，縮短回應時間與產出相關報表。

4.遵守及制定相關政策規定
Panorays持續監視第三方是否存在新問題，並報告特定發現，這些發現可能會導致無法遵守GDPR，NYDFS等法規以及NIST，ISO 2700x和PCI DSS等安全標準。

借助Panorays平台，公司可以加快其供應商安全評估流程及遵守GDPR、PCI和NYDFS等相關法規；Panorays能讓公司同仁輕鬆查看、管理其供應商、供應商的夥伴及其它業務夥伴的資安態勢，且Panorays為SaaS平台，無須安裝任何軟體；Panorays為目前業界唯一一個整合資安態勢與評估表的平台。