SecurityScorecard

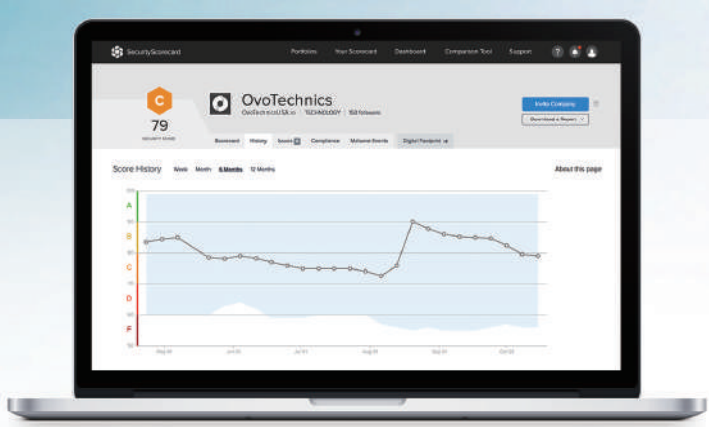
SecurityScorecard網路資安風險管理系統：智能預測與分析數據的力量

採取積極主動的態度來阻止資安違規事件

SecurityScorecard不只是一種資安風險係數的評估平台。通過10個評估關鍵資安風險因素計算出的字母等級來表示風險的級別，風險的級別揭示了組織資安狀況及其供應商資安風險狀況。通過成孰的數據收集技術與數百萬個專有和開放性資源數據，以及運用高階機器學習演算法可以確定組織的資安風險等級，這將可以預測組織成為資料外洩事件受害者的可能性。事實上，資安等級低於B級的組織遭受網路攻擊的可能性是5.4倍。

10個主要風險項目：

- Cubit Score
- 網路資安風險
- 端點資安風險
- 駭客訊息交流中心
- DNS資安風險
- 惡意程式IP連線訊息
- 帳密訊息洩漏風險
- 補丁修補週期
- 應用程式資安風險
- 社交平台風險分析



即時獲得整個供應鏈資安生態系統的風險可見性

當某個供應商或委外廠商出現漏洞時，這些資安問題將會環環相扣，因此造成了供應鏈資安生態系統的風險。

企業利用SecurityScorecard平台不僅可以持續監視自己的網路健康，還可以持續關注其供應鏈資安生態系統中的每個第三方可帶來的風險。這樣可以識別和確定哪些是高風險的供應商，以便進行評估或協同修復，從而為組織提供更簡化且高效率的供應商風險管理流程。

在攻擊者可利用漏洞發動攻擊之前修補資安漏洞

SecurityScorecard網路資安風險管理平台數量化了第三方的資訊安全意識以及資安風險係數的波動，例如:過舊的軟體版本或瀏覽器以及平均漏洞補丁修復的週期。

SecurityScorecard能精準的顯示風險問題的嚴重性，也可以透視問題的細節並允許組織更深入地了解特定的事件。SecurityScorecard協作工作流程使組織和供應商能夠協同工作，更有效率的修復所有已發現的資安風險和合規性的問題。

了解更多有關SecurityScorecard資安風險管理平台的數據科學信息：

- Threat Market威脅市場
- Threat Reconnaissance威脅偵察
- The Data Engine數據引擎
- The Intelligence Behind the Score 統計分數背後的科技智能

瞭解更多Securityscorecard資訊，請聯繫產品顧問: Mark Chang
E-mail: mchang@securityscorecard.io 電話: +886 928 362 938