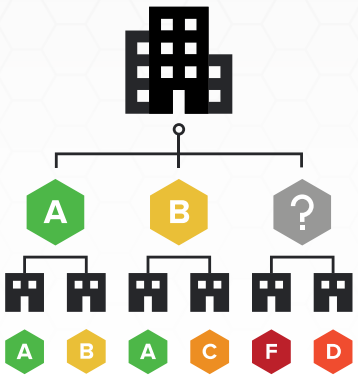
SecurityScorecard

啟動第三方風險管理

若要避免網路安全入侵(通常可以追溯到供應鏈漏洞),您所能做的最重要事情,就是開始使用第三方風險管理 (TPRM) 方案。

製定一套可行的方案來評估第三方和供應商的風險,可立即產生重大影響。SecurityScorecard 提供強大的自動化解決方案,能讓資安團隊無需增加預算和人員編制,即可管理不斷增長的第三方生態系統。



第三方風險管理 (TPRM) 方案能夠針對第三方及他們的數位環境,為貴公司提供識別、監控及管理其中網路安全風險的相關功能。

- 供應商
- 服務供應商
- 一級、下游和相關的廠商
- 雲端供應商
- 承包商
- 物聯網裝置
- 併購標的

簡化 TPRM 生命週期的重要階段:

01 供應商上線

- 建立整個企業範圍的流程,以引入新的潛在供應商 (例如在採購期間)
- 立即評級供應商的安全性,以判斷他們是否為永續型合作夥伴,並相應地排列出修補措施的優先順序。

02 供應商評估

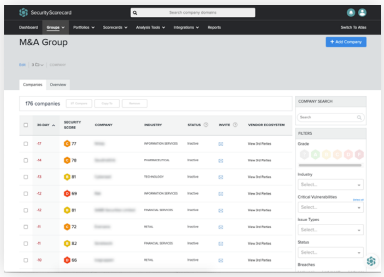
- 將由外而內的評級資料與由內而外的調查問卷資料進行比對,以 360 度全方位檢視風險所在。
- 細分大型供應商的數位足跡,以深入了解與您資料安全相關的確切資產和下屬機構。

03 供應商問題管理

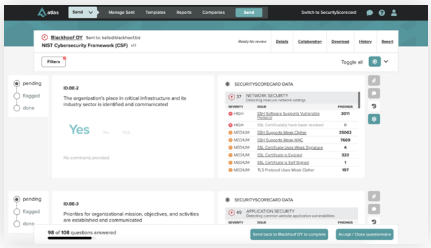
- 透過您首選的通訊管道來觸發警示並自動產生修補計畫,以快速識別及解決問題。
- 邀請供應商檢視他們的計分卡,並交回自訂改善計畫以提高他們的評級。

04 供應商調查問卷

- 大規模傳送、管理、完成及審查調查問卷。
- 使用機器學習驅動技術,將所儲存的證據內容自動填入問卷中並驗證回覆答案,可以將供應商評估週期縮短 83%。



使用 Groups 了解整個產品組合中的任務關鍵總體風險,並對高風險的供應商執行大量動作



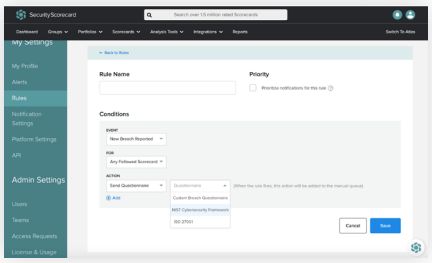
Atlas 能讓您將 SecurityScorecard 評級與 Atlas 中的各個問題進行比對，以即時驗證問卷回覆。

05 持續監控

- 持續掃描攻擊面，以快速識別第三方數位環境中的風險
- 在您的生態系統中搜尋 CVE，搶先在漏洞被威脅執行者利用之前及早發現並修補漏洞。

06 可行的商業情報

- 快速提取董事會級報告，其中顯示隨著時間變化在策略安全性和合規性方面的表現，以便您掌握進度、督促各方執行安全計畫。
- 善用來自可信賴的威脅情報合作夥伴和行業標準 SIEM 與 VRM 平台的整合訊號



使用規則產生器來觸發關鍵工作流程，以便在計分卡發生重要變化時（例如回報發生違規事件）自動執行指定動作。

為什麼選擇 SecurityScorecard？

- ✓ 完整可見度：每天掃描全球 IP 空間，以發現及管理影子 IT 和未修補的 CVE，並依照需求評級任何實體。
- ✓ 可行的安全情報：獲得的不僅僅是分數，SecurityScorecard 還會提供網路風險的情境脈絡和歸因。
- ✓ 持續監控填補了在固定時間點進行評估的可視化差距，因此您永遠都能掌握任何供應商的安全狀況。
- ✓ 大規模執行 TPRM：使用整合工具來進行協作和工作流程自動化，有助於團隊在不增加員工人數的情況下，仍能快速解決資安問題、規劃修補措施、監控更多公司。
- ✓ 一個平台：業界唯一完全整合的資安評級與供應商評估解決方案。
- ✓ 自訂報告功能可讓資安團隊和高階主管團隊深入了解對業務影響最大的風險領域。
- ✓ 強大的自動化工具：消除機械化任務，使得風險管理員能夠專注於執行更高價值的風險緩解策略。

關於 SecurityScorecard

SecurityScorecard 有助於資安專業人士協作，以透明的方式解決任務關鍵型網路安全問題。

SecurityScorecard 平台能為任何組織及它的生態系統提供持續、非侵入性的網路風險監控功能。

準備好開始了嗎？

立即預約產品示範：
https://securityscorecard.com/request-a-demo

> “SecurityScorecard 讓我和我的團隊能將供應商風險管理計畫的許多功能予以自動化和進一步擴展，並在面臨不斷增加的威脅環境時，持續監控環境內部和第三方的資安狀況。”

- Kal Dhisna
Virgin Pulse 資訊安全長