網路與系統安全 供應鏈攻擊事件 期中報告

事件：SolarWinds 攻擊事件

簡介： 2020 年 12 月美國資安大廠 Fireeye，揭露 SolarWinds Orion 網管監控軟體被植入含有惡意程式，卻擁有公司數位簽章，並發布此次事件的 DLL 檔，公開駭客入侵手法與管道，稱為「Sunburst 旭日攻擊」。不久後 GuidePoint、微軟及多家資安業者皆指出跟該產品相關的第二波「Supernova 超新星攻擊」，不同於 Sunburst 攻擊手法，採用 Webshell 方式進行入侵。隨後官方陸續公布事件入侵時間序，發現早在 2019 年可能就開始受到入侵，導致超過 18,000 個企業客戶受到感染，整個影響過程透過信任圈一路擴大，被認定為是一次重大的「供應鏈攻擊」。

事件學習：建議可從點、線、面進行通盤改善與處理：

1. 點：
   - 注意資安情資(NIST NVD、國家資通安全會報 N-ISAC)，受影響的軟體應盡速從官網下載更新。

2.線：
   - 對外公開的軟體檔案應確保完整性，要有獨立的確信安全檢查機制。
   - 伺服器不應上網，不應允許主動連線外部 TCP 80 及 443 埠。
   - 定期針對伺服器及設備進行資安健診。

3.面：
   - 發展領域資安規範：針對不同得供應鏈活動或委外專案特性，應訂出合適的安全規範，強化供應鏈上下游的資安。
   - 透過 SSRM 模型訂出雙方責任：讓多元而複雜專案活動或資訊作業委外，透過這框架客製化每項作業的資安基準，讓服務的企業(甲方)及供應商(乙方)明瞭雙方角色與責任，共同承擔應負事項。
   - 資安確信稽核：可透過自評或公正第三方進行供應鏈及委外廠商的確信稽核，找出問題並持續改善。

資料參考：https://www2.deloitte.com/tw/tc/pages/audit/articles/solarWinds-information-security-responsibility.html