資訊安全性管理 - 合作夥伴資訊套件

版本歷史紀錄

- 1.0 版 – 第一期

目錄

執行摘要

近年來，針對 IoT 裝置發動的網路攻擊猛烈密集，世界有目共睹。

在目前的網路安全性環境下，智慧型 IoT 系統的製造商需要有效增強其產品的內建保護機制。

SolarEdge 致力為其全系列智慧型變流器、全球的資料與通訊路基礎設施，以及資料中心提升網路安全性。

我們全方位的安全性架構不僅可保護太陽能光電 (PV) 基礎設施的傳輸中資料，也不需要額外的流量保護架構，例如 VPN。

SolarEdge 還會定期進行第三方網路風險評估與滲透測試，識別潛在的安全性缺口，以及改善網路安全性整備程度。

盡力讓所有的數位資產遵循網路安全性的最佳做法，並以符合 ISO27001 與 GDPR 等所有相關產業法規為目標。

免責聲明

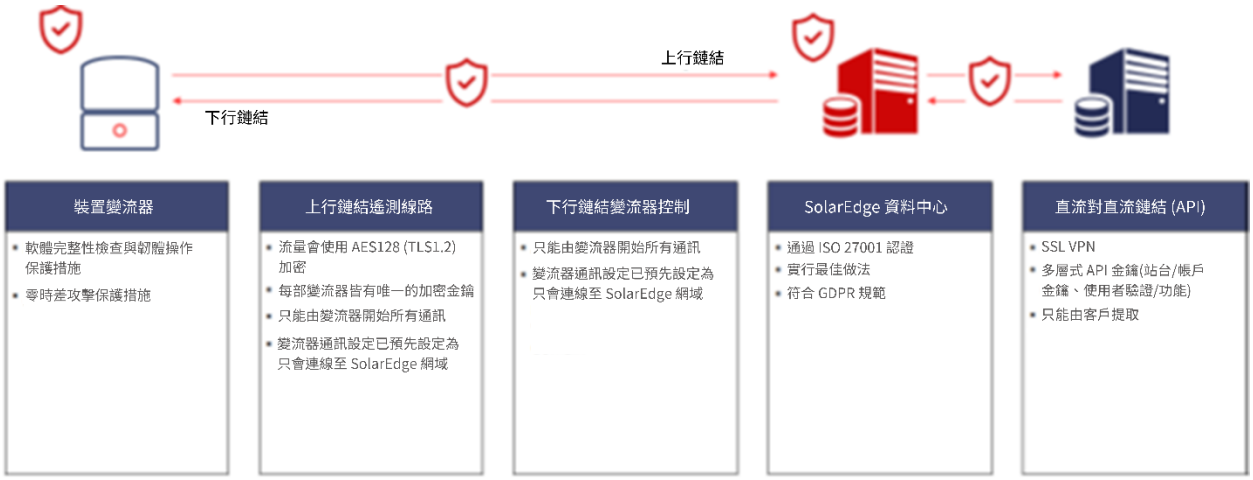
簡介

一般

本文件旨在向 SolarEdge 的目前和潛在客戶與合作夥伴，介紹 SolarEdge 軟體與硬體產品採用的資訊安全性架構、機制及控制功能。

SolarEdge 的太陽能光電控制與監控解決方案包括通訊與資訊系統，為客戶提供遠端電站、變流器及模組等級的監控功能。這些系統所面臨的威脅會危及系統與其不同元件所儲存、處理或傳輸資訊的機密性、完整性及可用性。SolarEdge 已設法持續防範這些威脅，包括蓄意攻擊、中斷服務、環境事件、人為/機器錯誤及結構性事故。

下圖概述 SolarEdge 的系統元件與相關聯的安全性措施。



全方位的多層安全性

SolarEdge 已實作多層解決方案，全面防範嘗試未經授權存取 SolarEdge 系統的情況。此解決方案可從遠端防範對單一裝置的可擴展攻擊與未經授權的存取。其設計旨在保護解決方案的每一個元件、連線、系統功能及儲存的資料。

解決方案範圍

審視下列安全性措施：

- 端點安全性
- 端點 (變流器) 與資料中心之間的通訊
- 伺服器安全性 (硬體與軟體)
- 安全主機服務設施
- 備份與業務連續性計畫 (BCP)
- 組織程序與流程

方法

進行定期安全性審查期間，SolarEdge 聘僱第三方網路安全性風險評估與滲透測試公司來審視 SolarEdge 的安全性機制。根據 NIST 800-171 與 OWASP 國際標準為執行資訊安全性指定的方法，定期評估 SolarEdge 的資訊安全性系統與通訊系統。

摘要

下列文件為第三方審查摘要。此公正的全面性分析顯示並未發現任何嚴重或重大問題。由此判定，SolarEdge 已為了持續改進安全性建立全方位流程。SolarEdge 的解決方案產品以資訊安全性與客戶隱私權為重。

安全性策略

SolarEdge 保留可隨時變更其安全性策略的權利。

端點 (智慧型變流器) 安全性

SolarEdge 變流器具備多層安全性 (包括內建與第三方機制)，其設計目的在限縮隨機與鎖定目標的網路攻擊面。

裝置存取控制

- 強化存取機制 - 停用所有未使用的變流器界面 (服務/連接埠)。只有指定的受保護連接埠才開放通訊、允許存取預先決定的安全服務。
- 僅限核准的使用者/服務帳戶存在。根據預設，我們會移除不必要的帳戶，以限縮未使用與不安全使用者/服務帳戶的攻擊面。
- 端點不支援 UPnP 提供的自動探索與連線功能，而必須手動進行配對，藉此避免建立未經授權與未知的連線。
- 根據 ZigBee 通訊協定與其安全性要求 (IEEE 802.15.4)，為多種不同的裝置提供短程無線通訊，強制須在變流器附近才能開始存取和建立連線。
- 變流器可作為 SolarEdge 周邊裝置的 Wi-Fi 路由器。變流器的 Wi-Fi 存取點不會發佈其 SSID (來源)，並只會在實際存取變流器時短時間開啟。隨意進行 Wi-Fi 掃描，並不會揭露變流器的存取點。

裝置驗證安全性

驗證機制可以驗證和識別使用者、流程或裝置，通常會當成允許存取資訊系統資源的必要條件。

SolarEdge 會在發電期間為每部變流器產生唯一的加密金鑰。因此：

- 設計上，每部變流器都能向控制與監控伺服器驗證其唯一身分。
- 金鑰交換流程可以限縮加密攻擊媒介。

防範遭受惡意程式碼攻擊

惡意程式碼是指意在執行未經授權動作的軟體或韌體程式碼，將會對資訊或作業系統的安全、機密性、完整性及可用性造成不利影響。惡意程式碼會以病毒、蠕蟲、特洛伊木馬程式，或其他會感染主機的程式碼實體形式出現。還有間諜軟體與某些形式的廣告軟體，也屬於惡意程式碼。

SolarEdge 韌體設計為使用下列機制，防範本機與遠端的惡意程式碼攻擊：

- 變流器韌體程式碼使用祕密金鑰加密，旨在確保韌體更新可靠，也未包含後門程式或未核准的程式碼。
- 安全開發生命週期 (SDLC) 的各個不同階段均內嵌安全性設計，以防範不同類型的程式碼弱點。
- 執行遠端無線 (OTA) 軟體升級時，SolarEdge 會保護傳輸通道並提供韌體驗證功能。由控制與監控平台 (管理伺服器) 管理該流程，以確保升級迅速又統一。
- 2020 年第 1 季，SolarEdge 與 Karamba Security 合作，在其智慧型變流器上整合先進的 IoT 反惡意程式碼代理程式，提供下列安全性強化功能：
  - Karamba Security 機制可以保護 IoT 防範零時差攻擊 (以程式碼中的未知安全性瑕疵為目標)，以及提供即時防護功能。
  - 還有額外的驗證層會在檢查程式碼合法後，才允許其更新。
  - 稱為控制流程完整性 (CFI) 的進階安全性階層，可讓變流器程式碼在生產線與現場防範惡意的操作嘗試。
  - 解決方案會持續監控安全性事件，並向 SolarEdge 安全性團隊 發出警示 (警示通知幾乎能即時傳輸至資訊安全監控中心)。

裝置資料保護 (隱私權)

- 硬體設計不具備錄音與錄影功能，也無法儲存如姓名或地址等的任何個人資訊。

變流器基準設定 (安全性設計)

變流器與功率優化器採用的基準設定，就是日後裝置韌體組建、版本或變更及其設定的基礎。基準設定包括端點硬體組建、出廠安裝的軟體、本機或遠端軟體升級，以及可控制功能的參數。端點設定可反映目前的現場設定。

SolarEdge 變流器與功率優化器均有定義的基準設定，其記載於各自的產品工程管理系統之中。如有變更，則會在經過正式審查後，於設計與製造流程期間更新。

發佈和套用修補程式

修補程式是由程式碼組成的軟體更新，可以插入 (或修補) 可執行程式的程式碼。一般來說，修補程式會部署至現有軟體程式之中。修補程式可進行下列任一項：

- 修正軟體錯誤 / 解決軟體穩定性問題
- 解決新出現的安全性弱點
- 升級韌體

SolarEdge 持續監控其產品的網路威脅，並據以提供安全性修補程式。修補程式均受到控制並會定期監控。

變流器遠端支援活動

須提供技術支援，才能解決各種不同的產品故障、服務中斷情況或其他問題。技術支援小組的人員都是經過認證的支援工程師，以及合格的支援合作夥伴。

由於支援活動在作業與安全性方面的敏感度，因此會記錄每項活動，同時存取重要支援活動也會受到限制和全面監控。

通訊安全性 (變流器與 SolarEdge 伺服器之間)

通訊加密

組織使用加密通訊鏈結，以增強機密性與完整性。不過，使用加密通訊鏈結會影響組織適當監控通訊流量，以發現惡意程式碼的能力。

SolarEdge 控制與監控解決方案會在使用乙太網路、Wi-Fi 或行動網路數據機時，使用進階加密標準 128 位元 AES 位元加密方式，為變流器與伺服器之間的通訊強制加密。

SolarEdge 的安全性方法假定裝置的使用者會提供防護措施，防止未經授權的人員實際存取硬體或滲透 LAN。

- 使用增強式驗證 (802.1x) 與加密演算法 (WPA2-PSK 搭配使用 128 位元 AES 金鑰) 的最佳安全性相關做法，實作 Wi-Fi LAN 與 WAN 通訊。
- SolarEdge 變流器只能在加密的 TCP 模式 (SSL over TCP) 下通訊。

非對稱式通訊

若是啟用變流器與資料中心伺服器之間的網路或網際網路通訊，會使系統遭到入侵。

開啟接收通道，則會遭到查詢裝置以尋找開啟連接埠和搜尋服務弱點的網路攻擊媒介利用。

為了減輕此風險，SolarEdge 變流器設計為單向通訊機制，*只有*在變流器開始與伺服器連線時，才會收到來自伺服器的訊息，提取新命令和傳輸新資料。

設計的解決方案可讓變流器匿蹤，不受潛在駭客侵擾，還可有效將其轉譯，以在掃描攻擊下隱身。

SolarEdge 資料中心安全性

SolarEdge 資料中心聚焦於智慧型變流器資料。

網頁式 SolarEdge 監控入口網站提供增強的太陽能光電效能監控功能，並透過模組、串列和系統等級的即時故障偵測和警示傳播功能，確保能產率。

SolarEdge 的控制與監控平台不會處理任何信用卡付款。

下列各節說明用來保護 SolarEdge 資料中心的措施：

強化伺服器

強化是實作標準安全設定的流程，提供公認、標準化及確立的基準來為特定資訊技術平台/產品規定安全配置設定，以及根據作業需求來設定這些資訊系統元件的指示。

SolarEdge 根據廠商指示與最佳產業做法，實作完整的強化流程，以改善伺服器的安全性態勢與作業效能。

使用利用 3DES/SHA256 加密演算法和需要使用雙重要素驗證的專用 SSL VPN，即可為了管理目的來存取伺服器。

基礎設施架構

SolarEdge 資料中心使用負載平衡器、防火牆及伺服器叢集。為了確保業務連續性，使用能利用重複、多餘伺服器的叢集拓撲，以滿足所需容量和強制實行資訊安全性標準。使用領先的防毒軟體與反惡意程式碼應用程式，部署防火牆與伺服器。資料中心以專用的網際網路存取鏈結，使用多家第 1 層供應商提供的備份。

資料庫安全性

根據產業最佳做法來維護 SolarEdge 資料庫。SolarEdge 還會根據如 NIST 800-123 等的國際標準，定期強化資料庫。

- 資料庫架設在根據 ISO 27001 指引來管理的安全設施中。
- 從網路觀點來看，資料庫位於受防火牆保護的個別網路中。只對特定應用程式開放資料庫流量 (區隔)。
- 強制定期資料備份，以及在發生必須還原為先前狀態的事件時，執行復原測試。
- 採用邏輯方式區隔客戶資料，強制實行嚴格的存取控制 (只向客戶揭露他們自己的資料)。

流量

SolarEdge 納入下列方法來保護流量：

- 透過網頁瀏覽太陽能光電監控平台時，使用 SSL 加密，搭配最新的加密最佳做法 (不再使用易受攻擊的 TLS 版本)。
- 使用者與安裝商應用程式使用 SSL 傳送所有往返伺服器的流量。
- 專用 VPN 可讓不同的資料中心之間安全地進行通訊。所有流量均經過加密。

修補和更新伺服器

如先前所述，SolarEdge 須管理全方位修補流程。由於其作業敏感度高，SolarEdge 會透過受控流程來更新其伺服器，該流程包括：

- 只在受控的 IT 環境下完成測試，識別有無任何作業差距或技術問題之後，才會部署更新。

監控伺服器

持續監控程式可促進不斷覺察威脅、弱點及資訊安全性現況，以支援組織風險管理決策。

SolarEdge 使用許多不同的技術解決方案與最佳做法，實作和持續調整其伺服器監控策略：

- 建立要監控的組織定義指標
- 根據上一項，使用技術工具持續進行效能監控
- 依照組織的監控策略，持續進行安全性控制評估

先進的主機服務設施

SolarEdge 在歐洲數處的專用主機服務設施儲存其資料，負責這些設施營運的全球主機服務供應商，在五大洲經營超過 140 處資料中心。

站台符合下列標準：

- ISO 9001:2008 品質管理系統標準 - 世界領先的品質管理標準，提供結構清晰的系統化方法，以維護和改善客戶體驗。
- ISO / IEC 27001:2005 與 27001:2013 資訊安全性管理系統標準 - 最獲廣泛接受的認證，用於支援資訊與實體安全性及業務連續性。ISO 27001 可確保：
  - 商業的風險與威脅均經過評估且受到控制。
  - 一致地強制執行實體安全性流程，例如限制/具名存取。
  - 定期在每個站台進行稽核，包括測試安全性以及規劃和監控 CCTV。
- NIST 800-53/FISMA 是由國家標準暨技術研究院 (NIST) 發佈，其為聯邦機構使用標準的建立者與推廣者，此標準可用於實施「聯邦訊息安全管理法」(FISMA)，以及管理設計來保護資訊和提升資訊安全性的其他程式。各機構必須在 NIST 指引與標準發佈後的一年內符合其規範。這些標準未納入國土安全問題。

備份與業務連續性計畫 (BCP)

備份週期

組織採用資訊備份機制來防止資料遺失，此機制也是推動任何業務連續性計畫 (BCP) 的重要一環。

SolarEdge 為其系統的設定與資料實作全方位的備份週期。備份可在發生有限資料遺失或資料中心故障時，用來快速地全面復原。備份複本不僅位於多個站台，而且每個站台都有數份複本。

除了歐洲資料中心的複本之外，還在 AWS 上與以色列儲存備份資料的複本。每季都會進行備份測試，以確保發生災害時能夠全面復原。

還原測試

進行定期記錄的還原測試，以驗證備份流程的完整功能，以及識別現有差距與故障情況。

SolarEdge 根據預先定義的計畫執行這些測試，全面驗證備份流程的功能。在這些測試中，SolarEdge 還原選取的資訊系統功能時，使用的是備份資訊樣本。

備份保護 (現場或異地)

SolarEdge 對其現場與異地備份主機服務站台，強制實行嚴格的實體與環境控制，以充分保證其備份可用。

備用站台 (災害復原規劃)

業務連續性計畫 (BCP) 是指開發預先安排與程序的流程，讓組織能夠回應服務中斷情況，使關鍵商業功能得以在規劃的服務中斷程度或必要變更下持續運作。簡言之，BCP 就是主動採取行動，制定策略性方法，盡可能預防災害發生，以及處理災後事務，讓影響層面侷限在企業可承受的範圍內。

災害復原規劃 (DRP)，其為 BCP 的主要環節，指的是 BCP 的技術層面，預先規劃和做好必要準備以將損失減至最低，並確保關鍵商業功能可在災害發生時持續運作。

SolarEdge 堅守對客戶的承諾，在歐洲設置專用的作業災害復原解決方案。

組織程序與流程

SolarEdge 的內部安全性程序與流程，目的在確保各項元件都符合相同的高標準，整個端對端流程也沒有弱點。

管理使用者帳戶

資訊系統帳戶類型包括個人、共用、群組、系統、來賓/匿名、緊急、開發人員/製造商/廠商、臨時及服務。組織資訊系統可以實作上述所列的一些帳戶管理要求。識別資訊系統的授權使用者以及載明的存取權限，也應反映出其他組織安全性程序中詳載的要求。

SolarEdge 採用自動商業智慧平台，支援管理資訊系統帳戶，包括監控帳戶使用情況的系統，以確保可接受其使用方式，以及防止發生惡意活動。

定期審視使用者權利，並隨各項新功能予以調整。

SDLC (安全開發生命週期)

SolarEdge 的硬體與軟體開發流程使用陣列開發方法。實行安全的軟體開發程序，包括定期弱點測試。發行任何次要或主要版本時，都會對所有權限相關的程式碼執行全自動化測試。

權限分派

組織使用「最低權限」，確保資訊系統使用者與流程不會以高於必要的權限進行操作來完成所需的組織任務/商業功能，藉此增強系統的安全性與資訊隱私權。

職能分工

職能分工可解決潛在濫用授權權限的問題，以及降低非共謀惡意活動的風險。

SolarEdge 在任務與資訊系統支援功能之間，以及不同的個人和/或角色間，實作職能分工。

驗證使用者與權限

SolarEdge 對使用者帳戶與權限實作定期存取審查，協助確保獲授權的個人能存取必要系統，而未獲授權的員工 (或歹徒) 則否。

與第三方的管理 SLA

服務等級協定 (SLA) 文件描述客戶期望供應商提供的服務等級、展示用以衡量服務的指標，以及未達到議定的等級時的救濟權或處分 (若有的話)。

SolarEdge 已與 IT 供應商簽訂合約與定義的 SLA，確保全年無休地全天候回應裝置或基礎設施相關問題。

錯誤回報獎勵

SolarEdge 依照常見做法，向回報網路安全性弱點的網路專家提供獎勵。所提供的獎勵會根據其風險高低、影響層面、利用難易度、報告品質及其他考量，由公司斟酌決定。

如需進一步詳細資料，請參閱 https://www.solaredge.com/cyber-security-policy

記錄

記錄，就是組織系統與網路內所發生事件的記錄。

SolarEdge 結合以時間為基礎的最佳資料庫系統，將所有監控平台基礎設施與網路記錄編製成以時間為基礎的索引，整合以時間為基礎的儀表板，允許 SolarEdge 搜尋過去與現在的記錄，以及調查過去與現在的事件。

滲透測試

SolarEdge 定期聘僱第三方公司，為其監控平台、API 及行動裝置應用程式進行滲透測試。以商業邏輯為重，使用手動與自動工具實作滲透測試，揭露可能造成嚴重商業衝擊的弱點。所得的任何測試結果都會根據其關鍵程度加以處理。

此外，SolarEdge 還利用自動網頁應用程式掃描工具，偵測其應用程式內的弱點。

事件回應

SolarEdge 安全性團隊利用進階 IR (事件回應) 工具，偵測其伺服器是否有任何可疑的缺口，並發出警示以立即進行處理。根據最佳做法，使用那些工具調查任何潛在的缺口和減輕風險。

供應商關係 – 供應鏈安全性

所有 SolarEdge 供應商在成為核准的廠商，獲得 SolarEdge ERP 系統存取權之前，都要接受法律審查。在潛在廠商獲核准成為合法供應商之前，審查會為其建立最低安全性基準，再對其套用風險參數。

GDPR – 一般資料保護規定

SolarEdge 的服務遍及世界各地，並持續活躍於歐洲市場。

SolarEdge 不儲存高度敏感的詳細資料，但仍以符合 GDPR 等隱私權法規的方式，悉心處理所有資料。

SolarEdge 完全符合 GDPR 的規範要求，包括：

- 處理合法、公正且透明
- 用途、資料及儲存限制
- 資料主體權利
- 同意
- 個人資料外洩
- 隱私權設計 - 技術控制
- 資料保護影響評估
- 資料保護員
- 覺察與訓練

附錄 A Qualys SSLabs 報告

若要產生和檢視該報告，請造訪以下網站：

https://www.ssllabs.com/ssltest/analyze.html?d=monitoring.solaredge.com