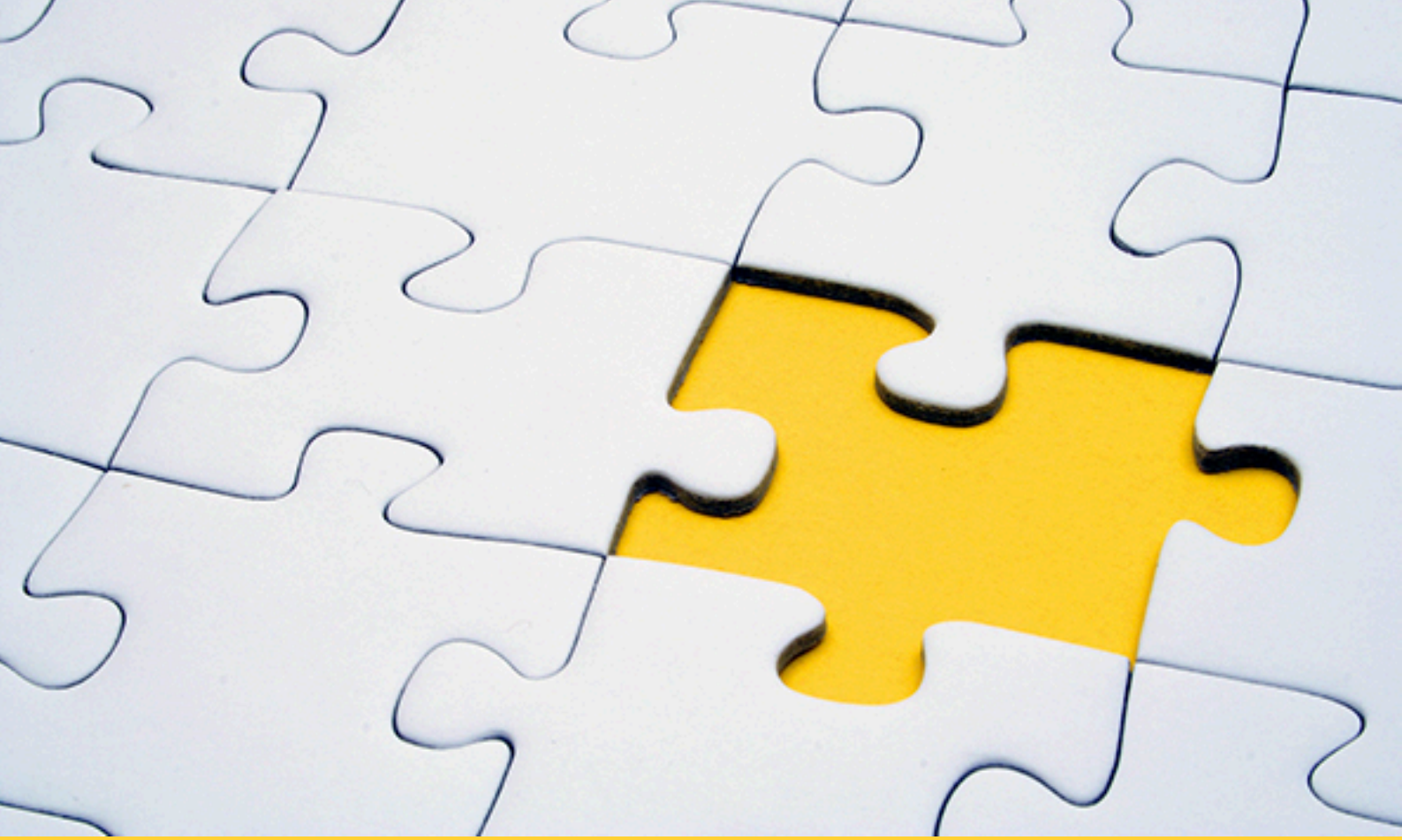

永續發展目標SGDs

力悅攜手高科技製造產業邁向科技永續，資安新疆界

Cyberview
力悅資訊

聯合國2015年永續發展目標(Sustainable Development Goals, SDGs)兼顧「經濟成長」、「社會進步」與「環境保護」三大面向，引領全球邁向永續。

隨著SDGs發展**力悅資訊**多年來積極協力高科技製造產業邁向**科技永續的路上，打造資訊安全新疆界**。

聯合國永續發展目標 SDGs 17個目標。素材來源：聯合國永續發展目標 SDGs

今多數人都擁有智能手機手錶、智能電視汽車等智能產品，高科技製造產業通過利用產品所產生大量數據，將其轉化為數據價值提升服務。

隨著近年發生各種網路攻擊威脅和未知漏洞，面臨資安與供應鏈安全的議題，2021年SEMICON Taiwan國際半導體展－資安趨勢高峰論壇，產業龍頭台積電宣布成立國際半導體產業協會(SEMI)臺灣資安委員會，積極推動晶圓廠設備資安標準，提升高科技製造產業供應鏈安全的實踐和網路安全意識。

力悅資訊協助高科技製造產業和供應商夥伴，以高規的資安防護通過首由台灣主導之『半導體產線設備資安標準規範』規範。

註：案號SEMI 6506C目前美國審核中，預計於2022年1月通過。

Cyberview
力悅資訊

註：本表內容參考草案 https://ams.semi.org/ebusiness/DownloadFiles/6506.pdf。

SEMI 6506 國際標準計劃 (草案) Requirment			解決方案 Solution
8.Computer Operation System Secuiry 電腦作業系統安全			
8.2	Long-term support for OS 長期支持作業系統	E<6506>.<BB>-RQ-00001-00	協力經銷夥伴提供顧問服務
8.3	Alternative countermeasures to address end of extended support 解決EOS的替代方案	E<6506>.<BB>-RQ-00002-00 晶圓廠設備作業系統EOS，供應商應有替代方案來減輕漏洞，應提供防火牆、安全閘道或替代安全設備。	Bitdefender -擴展偵測和響應 (XDR) Votiro -安全檔案閘道 (Secure File Gateway)
8.4	Full documentation with respect to availability of alternative proposal 提供完整文件說明替代方案的可用性	E<6506>.<BB>-RQ-00003-0 供應商應提供文件說明替代方案之可用性影響和操作程序。	協力經銷夥伴提供顧問服務
9. Network Security Requirement 網路安全要求			
9.2	Documentation and the control mechanism about equipment configuration management 設備配置管理的文檔和控制機制	E<6506>.<BB>-RQ-00004-00 E<6506>.<BB>-RQ-00005-00 (1)設備供應商對系統及其網絡應通過安全控管，包括已安裝軟件、服務、網路、Port和USB的安全策略 (2)設備供應商應提供強化管理的機制，例如啟用安全策略的配置和管理	Bitdefender -設備控制 (Device Control) -應用程式防火牆 (Firewall Application) -風險管理分析 (Risk Management)
9.3	The required policy of identification and authentication management on Fab equipment 晶圓廠設備識別和認證管理所需的政策	E<6506>.<BB>-RQ-00006-00 對於晶圓廠設備訪問控制，用戶認證和授權機制應實施以驗證用戶身份並執行最小權限原則	CyberArk -特權帳號存取管理 (PAM) -員工存取安全管理 (Workforce Identity)
9.4	Vulnerability scans before shipment to minimize system vulnerabilities 設備出貨前應進行漏洞掃描，減少系統漏洞	E<6506>.<BB>-RQ-00007-00 設備供應商應提供漏洞掃描報告證明沒有嚴重的高風險問題。漏洞掃描應遵循公認的安全建議。	協力經銷夥伴提供顧問服務

SEMI 6506 國際標準計劃 (草案) Requirment			解決方案 Solution
10.Endpoint Protection Requirement 端點防護要求			
10.2	Virus-Free Evidence 無病毒證明	E<6506>.<BB>-RQ-00008-00 設備供應商應在出貨時需提供無惡意軟件的證明。包括掃描時間、軟件、範圍和版本等資訊，掃描方法基於普遍接受的安全建議。	Bitdefenter -防止惡意軟件 (Anit Malware)
10.3	Certified endpoint protection 經認證的端點防護	E<6506>.<BB>-RQ-00009-00 設備應具備普遍接受的反惡意軟件解決方案，或用於端點保護的應用程序白名單控制。	Bitdefenter -端點偵測與回應 (EDR) -應用程序控制 (Application Control) -白名單 (Whitelist)
11.Security Monitor 安全監控			
11.2	Audit logs integrity 完整的稽核紀錄	E<6506>.<BB>-RQ-00010-00 設備應具有保存和導出與安全相關的稽核日誌的能力。 審核日誌至少包括同步時間軸、來源設備、應用程序/作業名稱、使用者帳號、事件。	CyberArk -特權帳號存取管理 (PAM) --- Bitdefenter -擴展偵測和響應 (XDR)
11.3	Audit logs protection 受保護的稽核紀錄	E<6506>.<BB>-RQ-00011-00 應提供保護機制以防止稽核日誌被篡改或刪除。	CyberArk Digital Vault 高度安全的數據金庫保護特權帳戶憑據、訪問控制政策、憑據管理策略和稽核紀錄。符合並利用 FIPS 140-2 加密算法來保護 Digital Vault 及其數據。通過資訊技術安全評估共同準則 EAL和聯邦資訊處理標準FIPS140-2 認證。 --- Bitdefender GravityZone 自我保護機制無法被用戶禁用或更改，每年依據 AICPA SSAE-16 SOC 2 的安全、保密和可用性原則進行審核，符合 SOC2 Type2 標準，證明能有效的保護稽核日誌防止篡改或刪除。

[撰文者：力悅資訊 李曉蕾]
更多方案內容，請參閱以下官方資訊：
力悅資訊官方網站 http://www.cyberview.com.tw/
力悅資安頻道 https://www.youtube.com/channel/UCFpYkj6GaEnGoTNslRf9oUg
力悅資訊粉絲專頁 https://www.facebook.com/Cyberview2005/