

影像監控系統資安標準-網路攝影機

資策會 資安所 技術經理

台灣資通產業標準協會 網路與資訊安全技術工作委員會 組長

高傳凱 博士



「經濟部工業局廣告」

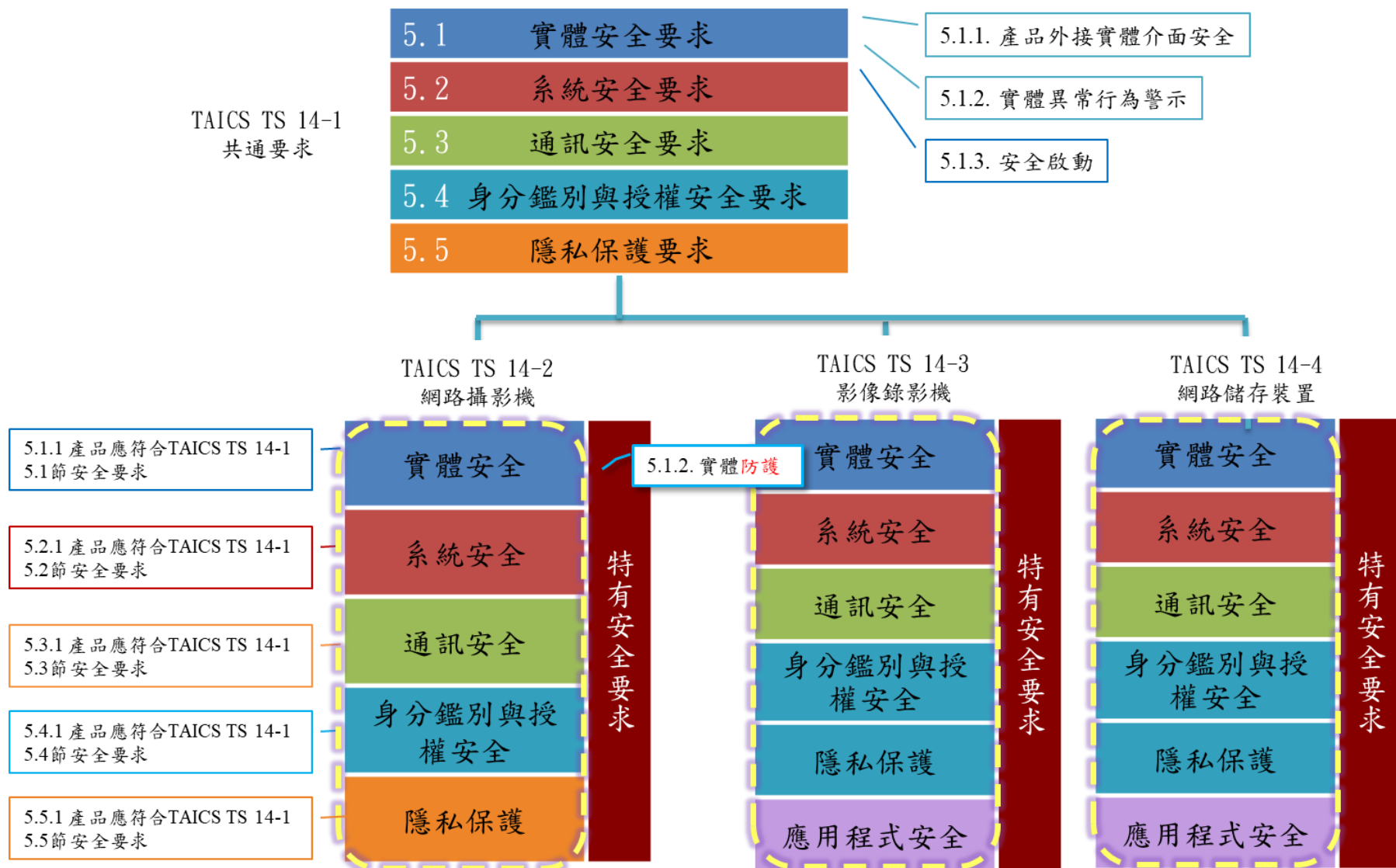
主辦單位



執行單位



影像監控系統系列資安標準框架



共通要求框架

安全面向	安全要求分項	認證	加密	完整性	資安漏洞	記錄功能
實體安全	5.1.1. 實體埠之安全管控			●		
	5.1.2. 實體異常行為警示					●
	5.1.3. 實體防護			●		
	5.1.4. 安全啟動	●		●		
系統安全	5.2.1. 作業系統與網路服務安全				●	
	5.2.2. 網路服務連接埠安全				●	
	5.2.3. 更新安全	●	●	●		
	5.2.4. 敏感性資料儲存安全		●			
	5.2.5. 網頁管理介面安全				●	
	5.2.6. 操控程式之應用程式介面安全	●				
	5.2.7. 系統日誌檔與警示					●
通訊安全	5.3.1. 敏感性資料傳輸安全	●	●	●		
	5.3.2. 通訊介面的安全設置		●		●	
	5.3.3. 通訊協定安全				●	
身分鑑別與授權	5.4.1. 鑑別機制安全	●				
	5.4.2. 通行碼鑑別機制	●				
	5.4.3. 權限控管	●				
隱私保護	5.5.1. 隱私資料的存取保護	●				●
	5.5.2. 隱私資料的傳輸保護	●	●	●		

實體安全要求

影像監控系統資安標準-共通要求

- 5.1.1 實體埠之安全管控
 - 5.1.1.1 產品僅提供使用者有限權限之設計，即預設不應透過實體埠存取產品作業系統之除錯模式。(1級)
 - ~~● 5.1.1.2 電路板上除錯測試用之連接器須移除。(2級)<=V2.0變動~~
- 5.1.2 實體異常行為警示
 - 5.1.2.1 產品須具有實體埠插拔操作記錄功能。(2級)
 - 5.1.2.2 產品須具備相關警示機制於實體操作發生斷訊時。(2級)
- 5.1.3 實體防護
 - 5.1.3.1 產品外部不應有徒手即可還原預設通行碼的設計。(1級)
 - ~~● 5.1.3.2 晶片上不應存在晶片編號，且電路板上不應存在除錯測試用之功能編號。(3級)<=V2.0變動~~
- 5.1.4 安全啟動
 - 5.1.4.1 產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。(3級)

影像監控系統資安標準-網路攝影機V2.0

● 新增之要求

- ◆ 5.1.1.2 卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。

系統安全要求

影像監控系統資安標準-共通要求

- 5.2.1 作業系統與網路服務安全
 - 5.2.1.1 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統CVSS嚴重性等級評比為重大。(1級)
 - 5.2.1.2 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統CVSS嚴重性等級評比為高。(3級)
- 5.2.2 網路服務連接埠安全
 - 5.2.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商須於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。(1級)

影像監控系統資安標準-共通要求

● 5.2.3 更新安全

● 5.2.3.1 韌體須具備更新機制。(1級)

(a) 產品若支援離線手動更新，則更新檔案須加密保護以確保機密性，且須採用FIPS 140-2 [10] 所核可之加密演算法；**抑或是**須於產品之身分鑑別因子、加解密用之金鑰（不含非對稱加解密用之公鑰）及敏感性資料，不應出現於韌體之程式碼與安裝檔內其他檔案中。

(b) 產品若支援線上更新，其**更新路徑須通過安全通道**，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能（Forward Secrecy），其中於身分鑑別過程須驗證憑證合法性，以及有效性(如:發證單位、有效期限、格式錯誤及憑證簽章等)。<=V2.0變動

● 5.2.3.2 產品必須具備**驗證韌體之正確性及完整性的功能**。(1級)

● 5.2.3.3 產品必須具備**備援更新功能**，即發生更新失敗時，系統能回復正常運作。(1級)

影像監控系統資安標準-共通要求

- 5.2.4 敏感性資料儲存安全
 - 5.2.4.1 產品所儲存之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不應明文儲存，而保護資料的加密方式須採用**FIPS 140-2**所核可之加密演算法。(1級)
 - 5.2.4.2 產品所儲存的敏感性資料，須被授權的個體始可存取。(1級)
 - 5.2.4.3 敏感性資料須存放於產品的**安全區域**(Security Domain)，從正常作業環境中隔離。(3級)
- 5.2.5 網頁管理介面安全
 - 5.2.5.1 產品之網頁管理介面不應存在OWASP web top 10 [11]之**Injection**及**Cross-Site Scripting (XSS)**攻擊。(1級)

影像監控系統資安標準-共通要求V0.9

● 新增之要求

- ◆ 產品須提出金鑰管理程序，以確保金鑰管理的品質。

影像監控系統資安標準-共通要求

- 5.2.6 操控程式之應用程式介面(ONVIF API)安全
- 5.2.6.1 應用程式介面，其鑑別機制安全依5.4.1.1(a)及5.4.1.1(b)之要求。(1級)
- 5.2.6.2 應用程式介面，其通行碼鑑別安全依5.4.2該要求項之相關要求。(1級)
- 5.2.6.3 應用程式介面，其權限管控依5.4.3該要求項之相關要求。(1級)

• 影像監控系統資安標準-共通要求V2.0
5.2.6 操控程式之應用程式介面(ONVIF API)安全

影像監控系統資安標準-共通要求

- 5.2.7 系統日誌檔與警示
- 5.2.7.1 須具備安全事件記錄與顯示功能，確實記錄使用者的存取行為，得以查核未授權或異常的登入操作。其內容須包括完整時間戳記、使用者身分及操作行為等，供後續查閱之用。(1級)
- 5.2.7.2 產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的存取。(1級)
- 5.2.7.3 須要求產品之日誌檔留存時間，且符合NIST SP 800-92 [12]中high impact systems的日誌資料維護長度。(1級)
- 5.2.7.4 產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。(2級)

通訊安全要求

影像監控系統資安標準-共通要求

● 5.3.1 敏感性資料傳輸安全

- 5.3.1.1 敏感性資料之網路傳輸預設須通過**安全通道**，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能（Forward Secrecy），其中於身分鑑別過程須驗證憑證合法性，以及有效性(如:發證單位、有效期限、格式錯誤及憑證簽章等)。(1級)<=V2.0變動

- 5.3.1.2 安全通道所使用之加密演算法須支援**AES-256同等或以上加密強度**的演算法。(3級)

0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0x14 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=ChaCha20(256) Mac=AEAD
0xCC,0x13 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=ChaCha20(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256

影像監控系統資安標準-共通要求

- 5.3.2 通訊介面的安全設置
- 5.3.2.1 產品須提供使用者得自行開/關「網路裝置資訊探詢」功能，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。(1級) => V2.0變動
- 5.3.2.2 產品須提供使用者得自行開/關「Wi-Fi保護設置(WPS)」之WPS PIN功能，而其預設值須為關閉狀態。(1級)
- 5.3.2.3 無線網路傳輸的安全機制預設須採用「Wi-Fi保護存取2(WPA2)」。(1級) => V2.0變動
- 5.3.2.4 預設不應透過網路連線存取產品作業系統之除錯模式。(1級)
- 5.3.3 通訊協定安全
- 5.3.3.1 產品之關鍵通訊協定(見附錄C)，不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。(2級)

影像監控系統資安標準-共通要求V2.0

● 新增之要求

- ◆ 5.3.2.3無線網路傳輸的安全機制預設須採用「Wi-Fi保護設置 v2 同等或以上之版本。」

影像監控系統資安標準-網路攝影機V2.0

● 新增之要求

- ◆ 5.3.2.2 產品所提供之自行開/關「網路裝置資訊探詢」功能，預設須為關閉，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。

身分鑑別與授權機制安全要求

影像監控系統資安標準-共通要求

- 5.4.1 鑑別機制安全
- 5.4.1.1 存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制。(1級)
- 5.4.1.2 鑑別錯誤訊息不應顯露出合法使用者名稱。(1級)
- 5.4.1.5 產品之鑑別機制須採用多因子鑑別。(3級)
- 5.4.1.6 相連之影像監控產品須支援雙向認證，確保相連裝置之可信度。(3級)

影像監控系統資安標準-共通要求V2.0

● 新增之要求

- ◆ 5.4.1.3 產品應具備上傳憑證之功能，以增加憑證鑑別機制之可信度。
- ◆ 5.4.1.4 產品每一次還原出廠設定時，憑證之金鑰(包括SSH及TLS)都須改變，確保每台產品金鑰之唯一性，及降低金鑰外洩可能引發之資安風險。

影像監控系統資安標準-共通要求

- 5.4.2 通行碼鑑別安全
 - 5.4.2.1 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則CCE-33789-9、通行碼必須符合複雜性需求原則CCE-33777-4、及強制執行通行碼歷程記錄原則CCE-35219-5。(1級)
 - 5.4.2.2 廠商所生產之裝置，其預設通行碼都須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。(1級)
 - 5.4.2.3 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即：(1級)
 - (a) 最高五次嘗試登入失敗即鎖定帳戶。
 - (b) 帳戶鎖定期間至少一分鐘以上，始可自動解除。
 - (c) 帳戶鎖定計數器至少一分鐘以上的時間間隔，始可將失敗的登入嘗試計數器重設為零次。

影像監控系統資安標準-共通要求

- 5.4.3 權限管控
- 5.4.3.1 產品須將使用者角色切割成數個使用者環境，例如：
：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。
(1級)
- 5.4.3.2 產品之授權行為，須存在閒置時限供使用者設定，
假如遠端連線逾時、遺失或結束，須要求新的鑑別(1級)

隱私保護要求

影像監控系統資安標準-共通要求

- 5.5.1 隱私資料的存取保護
 - 5.5.1.1 產品所儲存的隱私資料，須被授權的個體始可存取。
。(1級)
 - 5.5.1.2 使用者對其儲存的隱私資料擁有刪除之權限和功能。
。(1級)
 - 5.5.1.3 每次發生新的存取事件時，產品必須主動發出警示。
。(1級)
- 5.5.2 隱私資料的傳輸保護
 - 5.5.2.1 隱私資料傳輸機密性依「5.3.1敏感性資料傳輸安全」該節之要求。

影像監控系統資安標準-網路攝影機V2.0

● 新增之要求

- ◆ 5.5.1.2 產品應支援隱私遮罩，避免正常作業引發之隱私外洩風險。
 -

網路攝影機v1.0與v2.0的差異 (3)

● 附錄A 安全通道應使用之密碼套件:

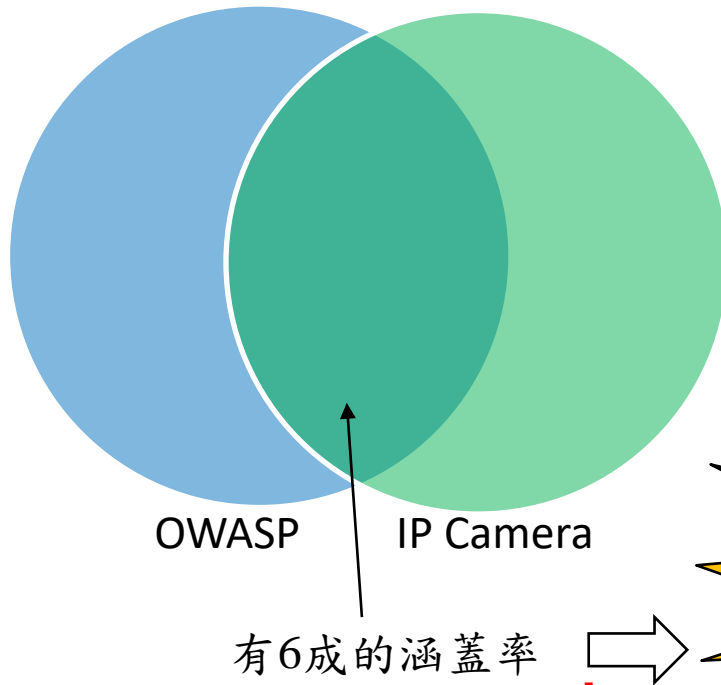
● TLSv1.2

- ◆ TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
- ◆ TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
- ◆ TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- ◆ TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- ◆ TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
- ◆ TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
- ◆ TLS_ECDHE_ECDSA_WITH_AES256_SHA384
- ◆ TLS_ECDHE_RSA_WITH_AES256_SHA384
- ◆ TLS_ECDHE_ECDSA_WITH_AES128_SHA256
- ◆ TLS_ECDHE_RSA_WITH_AES128_SHA256

● TLSv1.3

- ◆ TLS_AES_128_GCM_SHA256
- ◆ TLS_AES_256_GCM_SHA384
- ◆ TLS_CHACHA20_POLY1305_SHA256
- ◆ TLS_AES_128_CCM_SHA256
- ◆ TLS_AES_128_CCM_8_SHA256

OWASP IoT Top 10涵蓋率



有6成的涵蓋率

For Example: (未包含的OWASP資安要求)

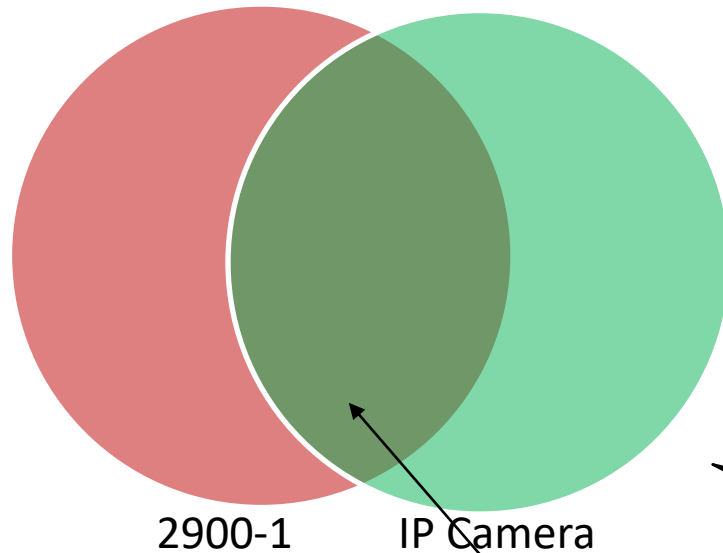
1. Ensuring the update server is secure.
2. the use of external ports such as USB to determine if data can be maliciously accessed on the device without disassembling the device.

8成9涵蓋率

去除掉IP CAM標準適用範圍外的要求

- I5: Privacy Concern (Privacy Notification)
- I6: Insecure Cloud Interface
- I7: Insecure Mobile Interface

ANSI/CAN/UL 2900-1 涵蓋率



For Example: (未包含的ANSI/CAN/UL 2900-1 資安要求)

1. Binary code and Byte code analysis.

7成2涵蓋率

去除掉IP CAM標準適用範圍外的要求

- 12. Vendor Product Risk Management Process

網路攝影機

資安認證推動時程



