

智慧巴士資通訊系統系列 資安產業標準檢測實務

技術服務處 資安認證組 副理
楊彩彤 Ann Yang
June 05, 2020

Leading Brand in Cybersecurity Compliance Solutions

www.onwardsecurity.com

CONTENT

01

About Onward Security

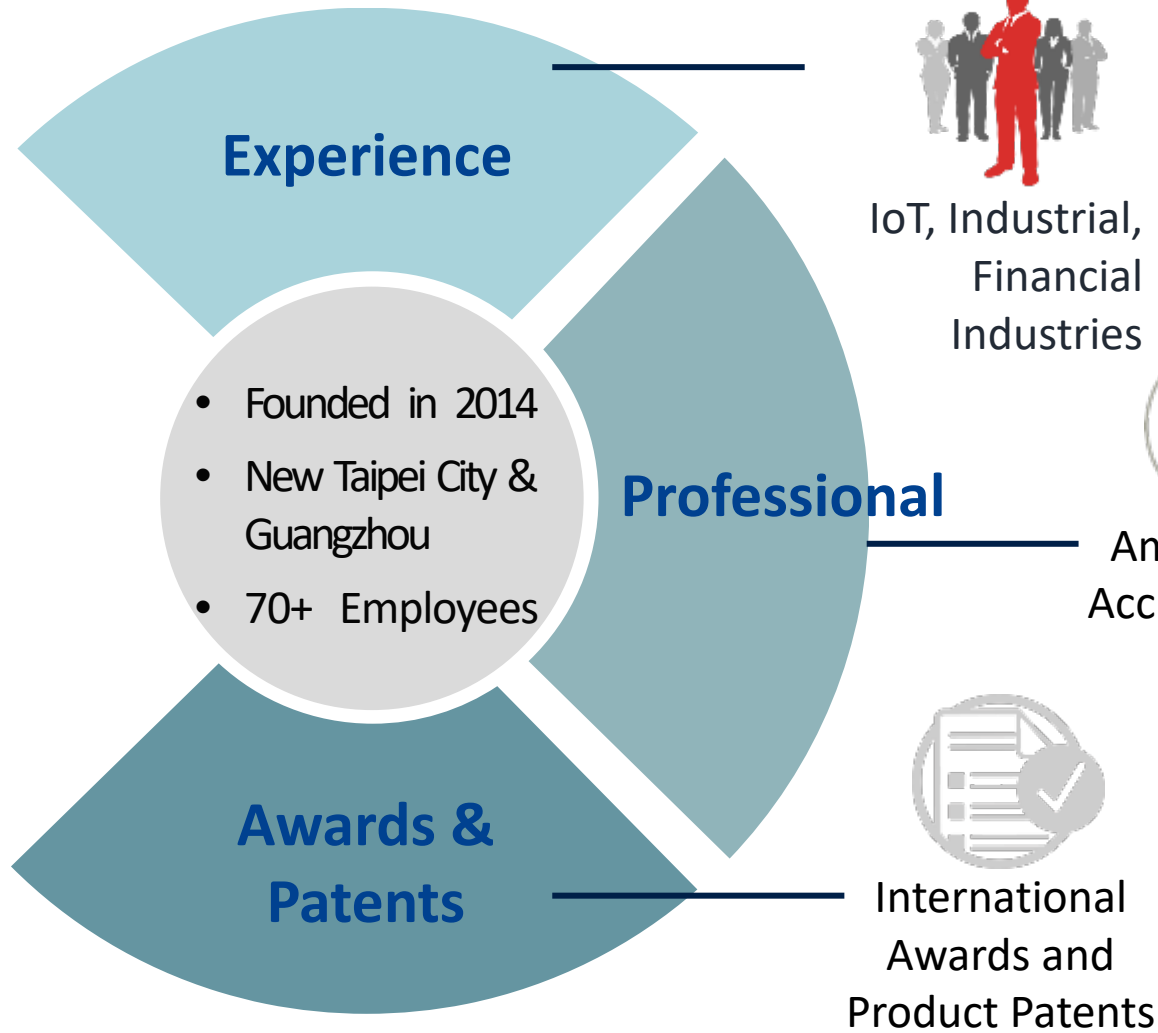
02

智慧巴士檢測實務分享

About Onward Security

01

Cybersecurity Assessment Solutions for Connected Devices



Amazon AVS
Accredited Lab



amazon alexa



International
Awards and
Product Patents



Security Services
Company of
the Year



Best Cybersecurity
Company - ASIA
Gold Winner



Enterprise Security- Top 10
Enterprise Security Startups in APAC

Company Milestone

2014 - 2016

- Equipped with 2G/3G smart grid and automobile CANbus testing capability
- Acquired the APP accreditation from MOEA
- Acquired the ISO/IEC 17025 accreditation from TAF

- Acquired NCC mobile phone security testing laboratory certification
- Processed smart grid security assessment capability
- Entered IIoT/IACS market with security assessment service and product

2017

2018

- Released Security Vulnerability Study at International Conference: DerbyCon/ CODEBLUE
- Equipped with Bluetooth/BLE Security Assessment Capability
- Obtained ISO 27001 ISMS Certification

- Acquired IPCAM and security testing lab certification of smart bus
- Established IQ Lab - international certificate lab

2019

2020

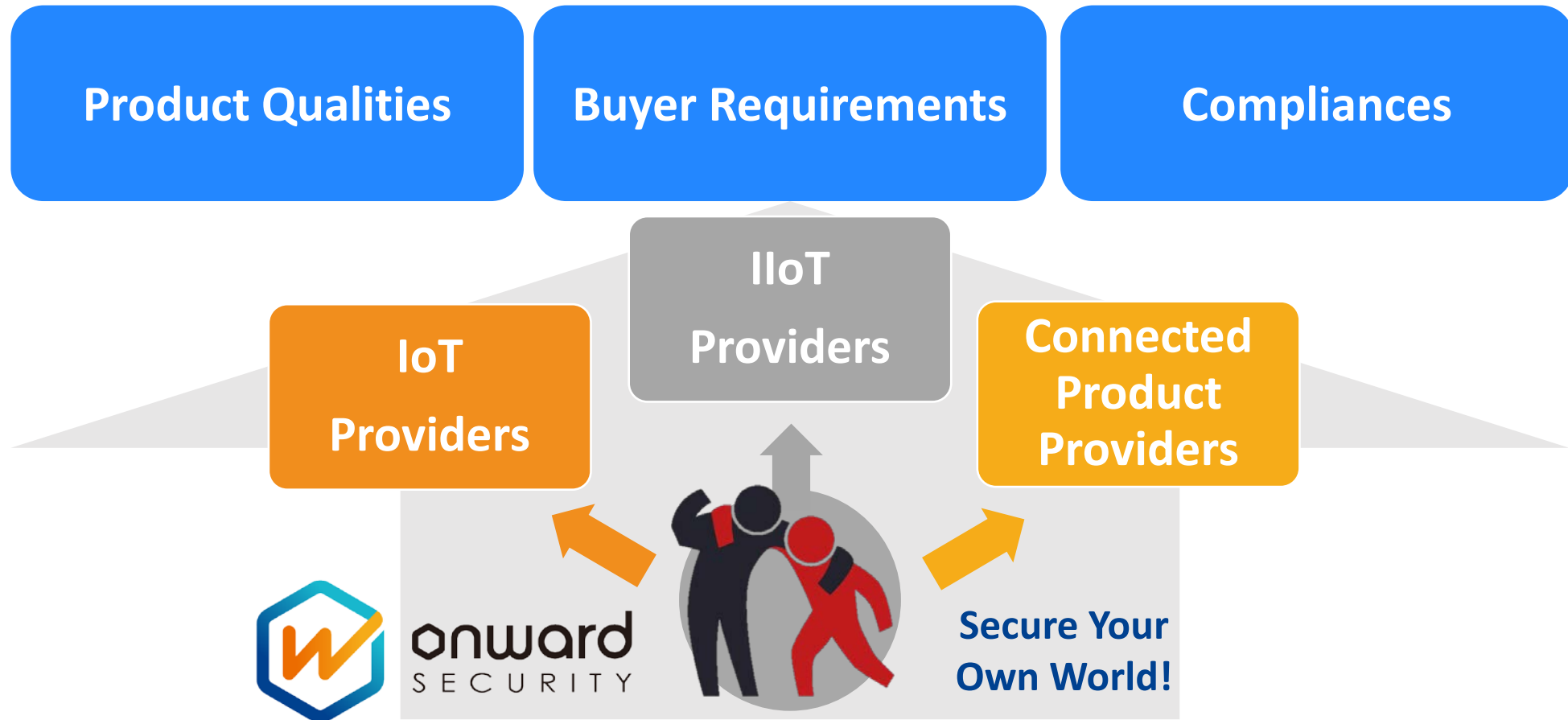
- The only authorized third-party lab in Taiwan for device testing and security assessment for Alexa built-In products



amazon alexa



Enabling Customers to Meet Product Security and Compliance Needs



Core Business and Solutions



Compliance
Services



Assessment
Services



Security
Products

SIMPLE

One-stop services
for cybersecurity
compliance

SECURE

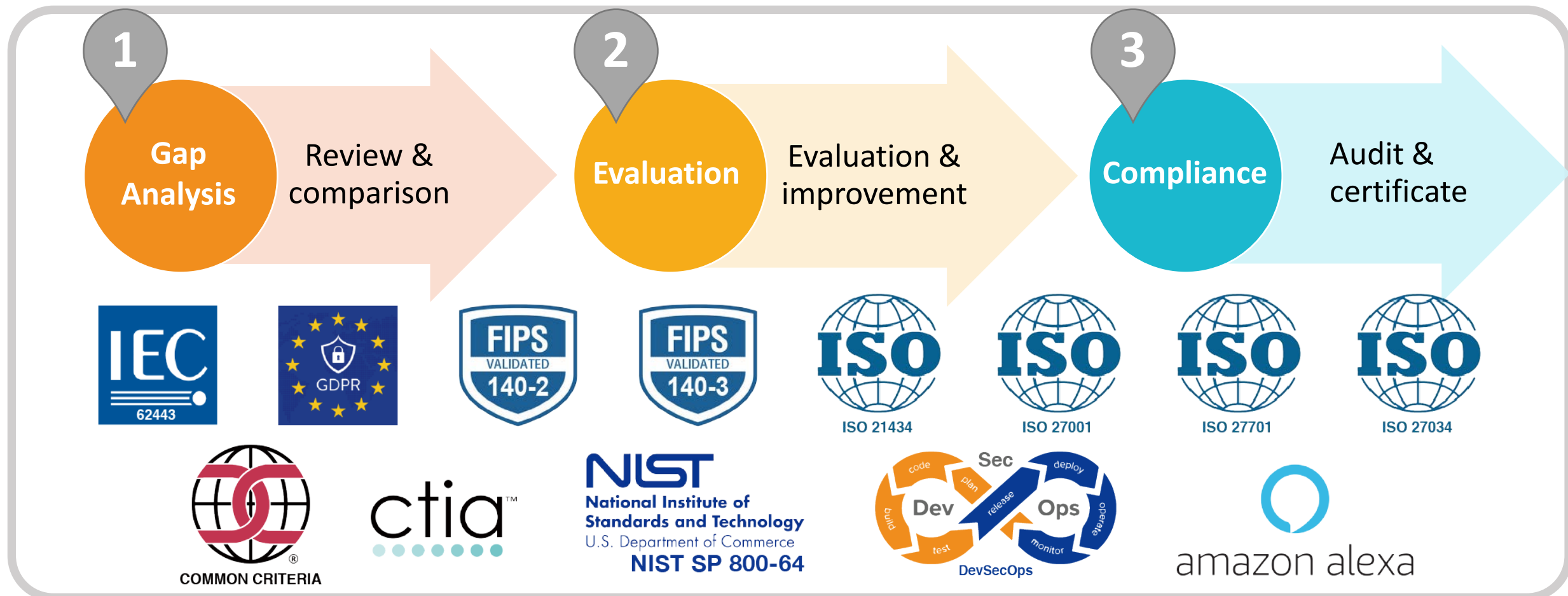
Supported by our
professional team
and keeping up to
date

SAVE

Save USD\$400,000+
cost of cybersecurity
assessment every
year

Compliance Services - Secure-by-Design Implementation

We make compliance easy



Assessment Services - Product Security Assessment and Certification



Fulfill most cybersecurity requirement you need

Our reports accepted by
10+ global buyers and governments and
150+ test items and keeping up to date

Assessment

IoT Products
IIoT Products
Automotive Products
Radio Frequency
(RF, Wireless, Cellular)



Certification

AVS (Amazon Alexa)
Embedded Systems (ISO 17025)
IP Cameras (ISO 17025)
Intelligent Bus (ISO 17025)
Mobile App (ISO 17025)
Smartphone (ISO 17025)

Security Products - Automated Product Security Assessment Platform



The mitigation of product vulnerability in a cost-effective manner

Threat sources



International Org.



Malware



Security Team

SecFlow
HERCULES

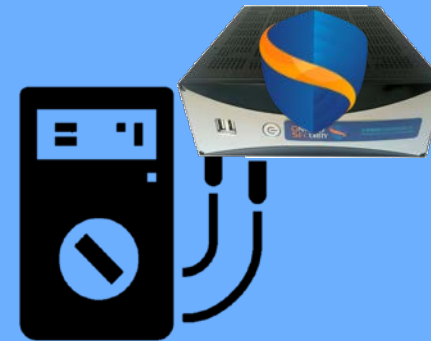
Let you know the
vulnerabilities



PM/RD/Security
Team

SecDevice
HERCULES

Help you find the
vulnerabilities



RD/QA/Security
Team

Secure
Products



智慧巴士檢測實務分享

02

一般要求 5.1.2.1 - 網路服務最小化測試

- 資安標準：非必要服務所需的網路埠須預設為關閉。
- 問題：廠商列出的連接埠與實驗室掃描結果不符。
- 建議：廠商進產品作業系統檢查對外開啟的連接埠，逐一確認該連接埠用途。

```
ann@kali:~$ sudo netstat -atnup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:8000             0.0.0.0:*               LISTEN      65563/python
tcp6       0      0 :::80                   :::*                   LISTEN      65554/apache2
udp        0      0 10.1.1.14:68            10.1.1.1:67            ESTABLISHED 53754/NetworkManage
udp        0      0 0.0.0.0:69              0.0.0.0:*               24813/inetutils-ine
udp        0      0 0.0.0.0:514             0.0.0.0:*               1023/syslog-ng
```

```
ann@kali:~$ sudo nmap -sS -Pn 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-27 22:36 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
8000/tcp  open  http-alt

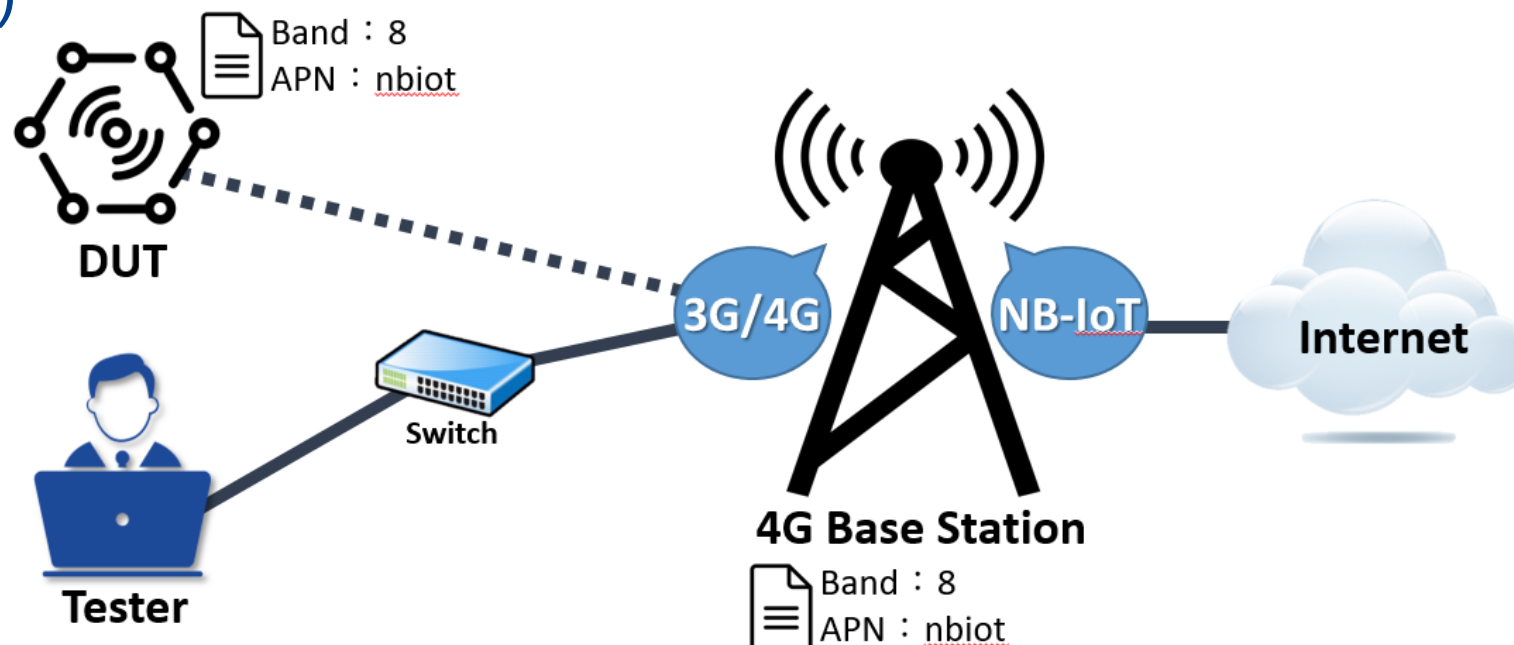
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```



一般要求 5.2.2.1(a) - 安全敏感性資料之傳輸保護測試

Level 1

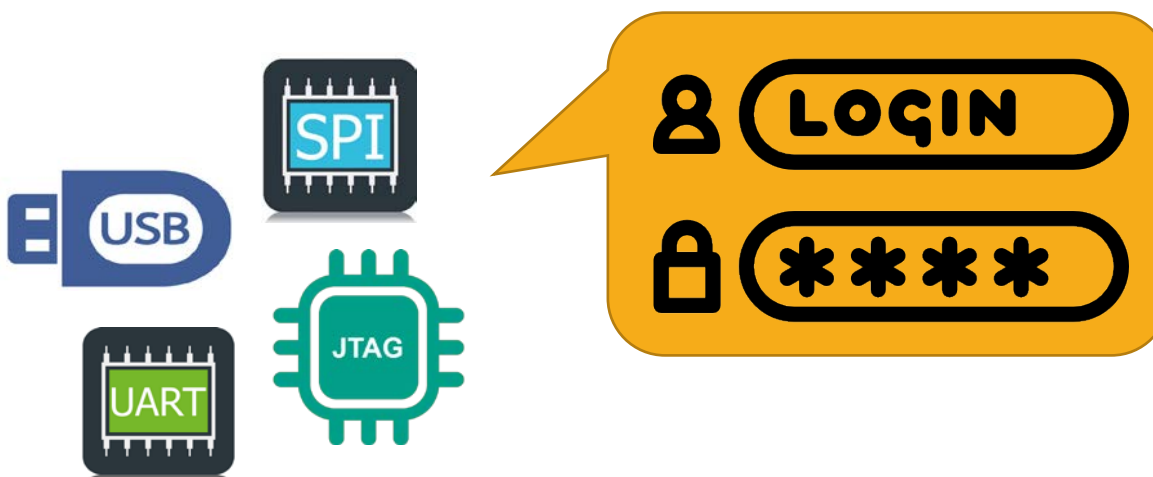
- 資安標準：傳輸安全敏感性資料須加密，加密方式須採用FIPS PUB 140-2 Annex A所核可之加密演算法。
- 問題：產品無法連線至實驗室4G基站。
- 建議：廠商提供4G/NB-IoT設定資訊(如APN、使用頻段等)；或調整成依照SIM卡設定(報告註明測試用韌體)。



車載機 5.3.2.1 - 產品實體連接介面安全管控測試

Level 1

- 資安標準：產品之實體連接介面(例如: UART、JTAG、USB)預設須關閉，或須經過身分鑑別方可被存取。
- 問題：產品維護需要使用UART介面。
- 建議：加上帳號密碼保護，且密碼要求須符合一般要求 5.4.2.1與5.4.2.2。



!@Wrq1245 ✓

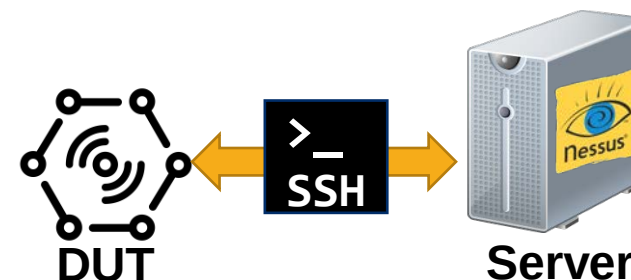
password ✗

test1234 ✗

123456789 ✗

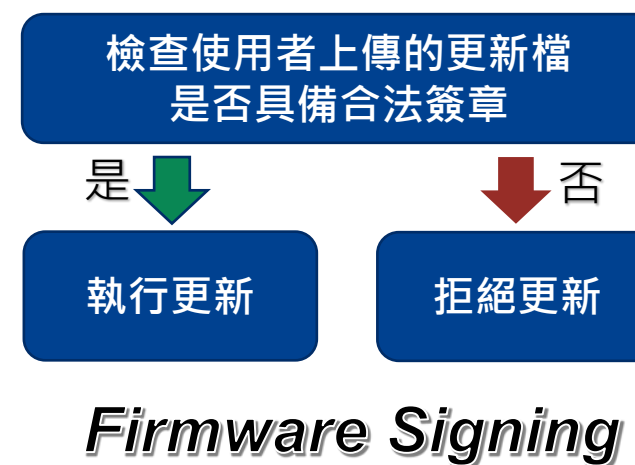
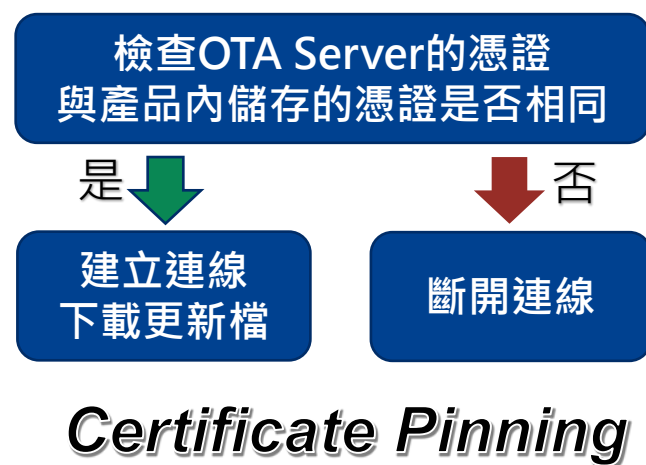
一般要求5.1.1.1 - 測試作業系統與網路服務是否存在CVSS v3評分為7.0分以上之常見資安弱點與漏洞

- 資安標準：作業系統與網路服務不應存在美國國家弱點資料庫所公開的常見弱點與漏洞資料，及通用漏洞評分系統CVSS v3評分為高資安風險之漏洞。
- 問題：產品本身不提供遠端介面存取進入作業系統方法。
- 建議：增加遠端介面(SSH服務)並提供root權限(報告註明測試用韌體)。



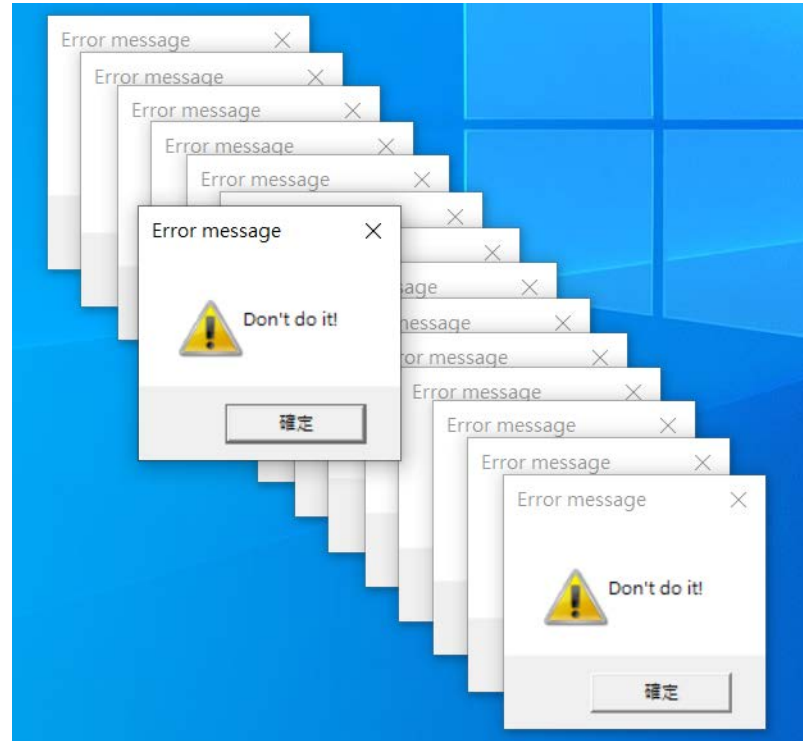
一般要求5.1.3.5 - 更新檔之合法性測試

- 資安標準：更新須驗證更新檔的合法性，該合法性驗證功能須採用FIPS PUB 140-2 Annex A所核可之簽章演算法。
- 問題：更新檔的合法性??甚麼是簽章??
- 建議：針對具備線上更新的產品，需實作憑證綁定(Certificate Pinning)；具備離線更新的產品，需實作驗證更新檔簽章機制(Firmware Signing)。



其他

- 問題：程式非廠商自行撰寫，無法修復/修改。
- 建議：如該功能為非必要，直接移除該功能(?)。



圖片來源：<https://www.mobile01.com/topicdetail.php?f=569&t=5241990>, <https://3c.ltn.com.tw/news/30149>, <https://www.zhifure.com/snzfj/66489.html>



THANK YOU

Leading Brand in Cybersecurity Compliance Solutions

© 2020 Onward Security Corp. All rights reserved. Tel: +886-2-8911-5035

