CMMC 2.0 標準

彙整與了解

王佑任 10/27

為什麼需要 CMMC

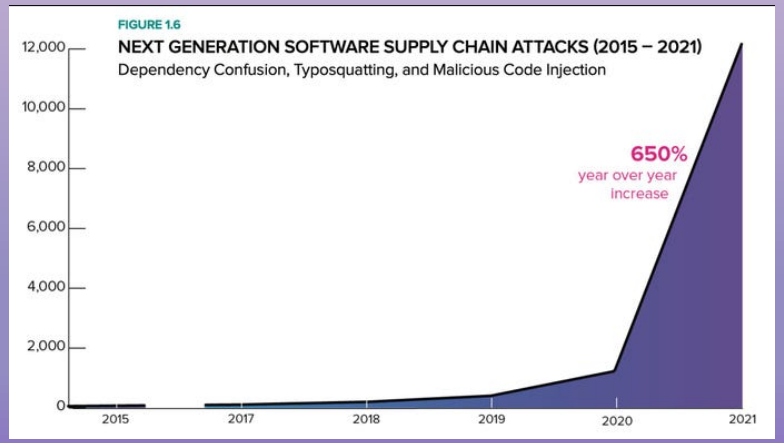
1. 惡意網路活動

盜竊美國工業部門的智慧財產權與敏感資料，進而威脅經濟安全和國家安全，每年對經濟造成上千億美元的損失。

2. 國防供應鏈遭受攻擊

攻擊者以國防工業基地(DIB)和美國國防部(DOD)的供應鏈為目標，削弱美國的技術優勢與創新，增加國家安全風險

近年軟體供應鏈攻擊事件高度增長



Source: sonatype 2021 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

CMMC 認證的主要目的

評估美國國防部承包商的網路安全能力，確保承包商遵循最佳實務做法，保護敏感資訊

CMMC 要保護哪些敏感資料

1

Federal Contract Information (FCI)

FCI is information provided by or generated for the Government under contract not intended for public release.

FCI 是合約相關資訊，由政府提供或廠商提供給政府，這些資訊並不適合被公開釋出。

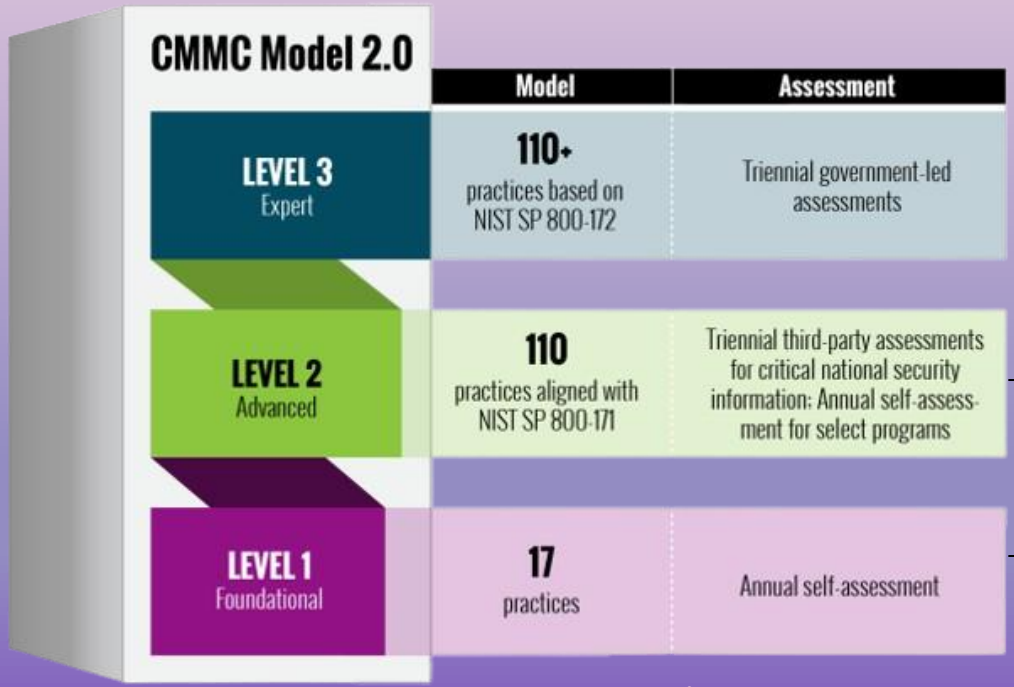
2

Controlled Unclassified Information (CUI)

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies,

CUI 是不具分類保密等級，但依據法令或政府政策，仍須受管控的資訊。

CMMC Model 2.0



CMMC 2.0 Level Overview

將包含 **NIST SP 800-172** 中規定的安全需求的一個子集

適用對象為對於 **CUI** 資訊的防護需要有最高優先等級者

評估方式: 由政府官員評估，評估準則正在制定中

包含 **NIST SP 800-171** 中規定的 **CUI** 安全需求

評估方式:

1. 涉及處理**CUI**資訊部分，每三年需進行一次第三方機構**(C3PAO)**評估
2. 不涉及處理國防安全之**CUI**資訊部分，採用年度自我評鑑

著重於保護 **FCI**, 包含 **FAR** 條款中規定的基本防護要求

評估方式: 年度自我評鑑，不須透過第三方評估機構

CMMC 2.0 改版差異

2021年美國國防部宣布將 **CMMC 1.0** 修訂為 **2.0** 版，
目的為簡化 **CMMC** 標準，減少合作承包商遵守標準的障礙，
提高整體合作夥伴執行的便利性。

1. 原先 CMMC 1.0 Model 的認證等級由 第一級 ~ 第五級 **精簡** 為 第一級 ~ 第三級

2. 將 CMMC 2.0 實踐作法對應至廣泛接受的 **NIST** 網路安全框架，並移除所有 CMMC 1.0 特有的實踐作法

3. CMMC 1.0 要求所有承包商進行第三方評估，而CMMC 2.0 則**放寬**了Level 1 級別，可進行**自評估**

CMMC 2.0 與 我國資安治理成熟度比較

	CMMC 2.0	資安治理成熟度架構
成熟度等級	Level 1 - Foundational Level 2 - Advanced Level 3 - Expert	Level 0 - 未成熟型 Level 1 - 基礎型 Level 2 - 管理型 Level 3 - 制度化型 Level 4 - 可預測型 Level 5 - 創新型
模型組成	14 大控制領域	3 大面向，11 個流程構面
控制項目	110+ 個控制項目	41 個檢核項目

參考資料

1. https://dodcio.defense.gov/CMMC/Documentation/
2. https://www.r3-it.com/blog/cmmc-1-0-cmmc-2-0-whats-changed
3. https://www.thecoresolution.com/understanding-the-difference-between-fci-and-cui
4. https://ingsafe.tw/cmmc
5. https://www.ithome.com.tw/news/154532
6. https://cybersecurenews.com.tw/policy-007/
7. https://cyber.ithome.com.tw/2023/session-page/2102