我們與弱點管理的距離

加入 CNA Program 以及
處理 PSIRT 弱點事件的實戰經驗

Robert Lai, EJ Feng

May 15, 2024

Key Takeaways

1

PSIRT

我們發展 PSIRT 面對的挑戰和解方

2

CNA

我們對於加入 CNA 的看法，以及加入後的觀點

3

SDL

從回應弱點到預防弱點

MOXA

Who We Are

Robert Lai

Lead Cybersecurity Engineer

Moxa 資安技術經理

主導 Moxa PSIRT 發展的品質與技術窗口

導入安全產品開發流程（IEC 62443 Part 4）

建立跨組織合作的資安政策與程序

EJ Feng

Senior Cybersecurity Engineer

Moxa 資深資安工程師

負責 Moxa PSIRT 與 CNA 弱點處理流程

協助 Moxa 成為台灣第 8 個 CVE 編號管理者
(CVE Numbering Authority, CNA)

MOXA

PSIRT

我們發展 PSIRT 面對的挑戰和解方

MOXA

資安發展里程碑

2018 2019 2020 2021 2022 2023 2024 2025

Cyber Security Response Team

Moxa Product Cybersecurity Response Team (Moxa PSIRT)

Moxa Secure Development Life-Cycle Procedure V1.1/2.0 certified by IECEE

Moxa Secure Development Life-Cycle Procedure V2.0 certified by ISCI

CVE Numbering Authority (CNA)

從回應資安事件轉換到滿足市場需求

V1.0: CSRT (Cyber Security Response Team)

Reason for establishment

Cybersecurity issue raised from ICS-CERT, NIST or other IT vulnerability

Development Strategy

Quick response to market once any cybersecurity issue raised

Achievement

Build 4 step process: Awareness, Investigation, Action, Response

Challenge

Risk assessment and vulnerability reproduction

V2.0: PSIRT (Product Security Incident Response Team)

Reason for establishment

Establishing a scalable and **market-expected** vulnerability response process.

Development Strategy

As a feedback loop for the **SDL process**.
Experts guide the team in addressing vulnerabilities from both a reactive and proactive perspective.

Achievement

Respond to vulnerability reports from the client side.
Management policies and processes for reinforcing vulnerability reproduction to vulnerability remediation verification.

Challenge

Vulnerability management of **third-party components**.

MOXA

基於標準發展的弱點管理政策

IEC 62443 Part 4-1 Practice 6 Defect Management			
Reviewing security-related issues	Assessing security-related issues	Addressing security-related issues	Disclosing security-related issues

FIRST PSIRT Services Framework v1.1			
Vulnerability Discovery	Vulnerability Triage	Vulnerability Remediation	Vulnerability Disclosure

ISO/IEC 30111 Vulnerability Handling Process			
Verification	Remediation development	Release	Post-release

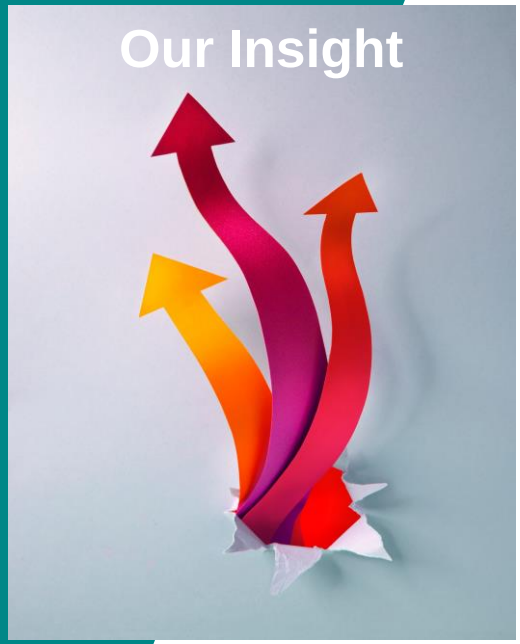
Product Security Incident Response Team 的日常

Awareness

Active Management

Vulnerability Fixes

Security Advisory



最大的挑戰

一邊開車，一邊修車

面對挑戰的解方

對齊使命和願景，課題分離

發展策略

先解決大家的痛點、再處理自己的議題

MOXA

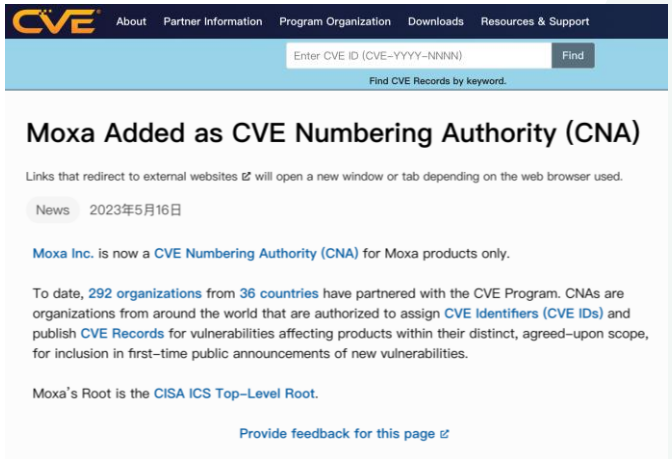
CNA

我們對於加入 CNA 的看法，
以及加入後的觀點

MOXA

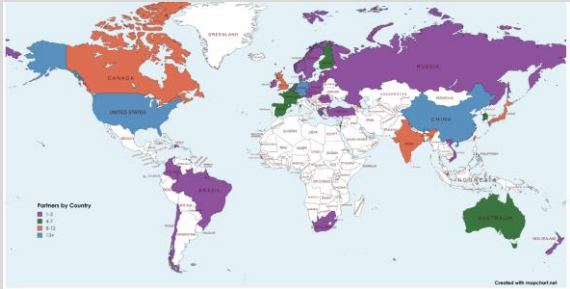
CNAs – PSIRT 團隊的全球肯定

- **Moxa PSIRT 於 2023 年 5 月正式成為台灣第 8 個 CNA，歸屬於美國 CISA (Root CNA) 管理下的 CNAs。**



Source: https://www.cve.org/Media/News/item/news/2023/05/16/Moxa-Added-as-CNA

Currently, there are only 367 organizations worldwide recognized as CNAs, with the majority in the USA (192), followed by China (22) and Germany (15). Taiwan currently has 9 CNAs.



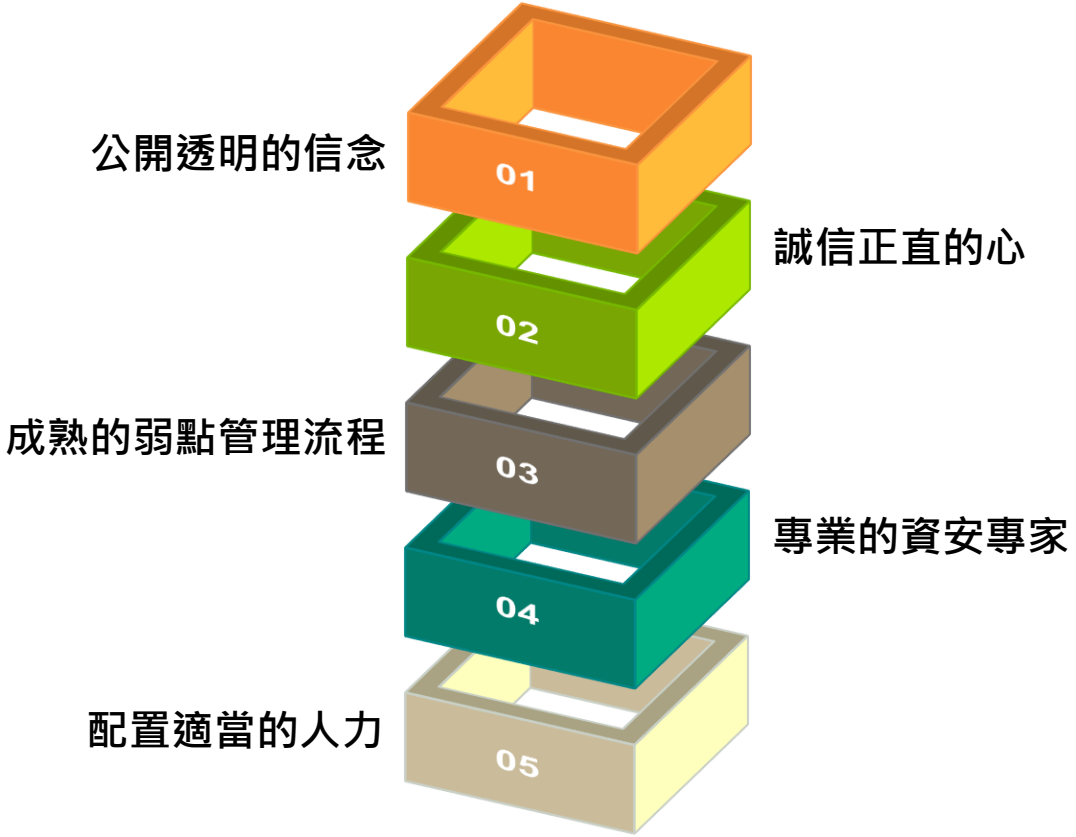
Australia: 5	Dominican Republic: 1	Latvia: 1	Slovak Republic: 2
Austria: 3	Estonia: 1	Lithuania: 1	South Africa: 1
Belgium: 2	Finland: 4	Netherlands: 6	South Korea: 7
Brazil: 2	France: 6	New Zealand: 2	Spain: 5
Canada: 8	Germany: 15	No country affiliation: 1	Sweden: 4
Chile: 1	Greece: 1	Norway: 2	Switzerland: 8
China: 22	India: 8	Poland: 1	Taiwan: 9
Colombia: 1	Ireland: 1	Romania: 1	Türkiye: 3
Czech Republic: 2	Israel: 9	Russia: 2	UK: 11
Denmark: 2	Japan: 12	Singapore: 2	USA: 192
			Vietnam: 1

https://www.cve.org/ProgramOrganization/CNAs

跨出舒適圈的第一步

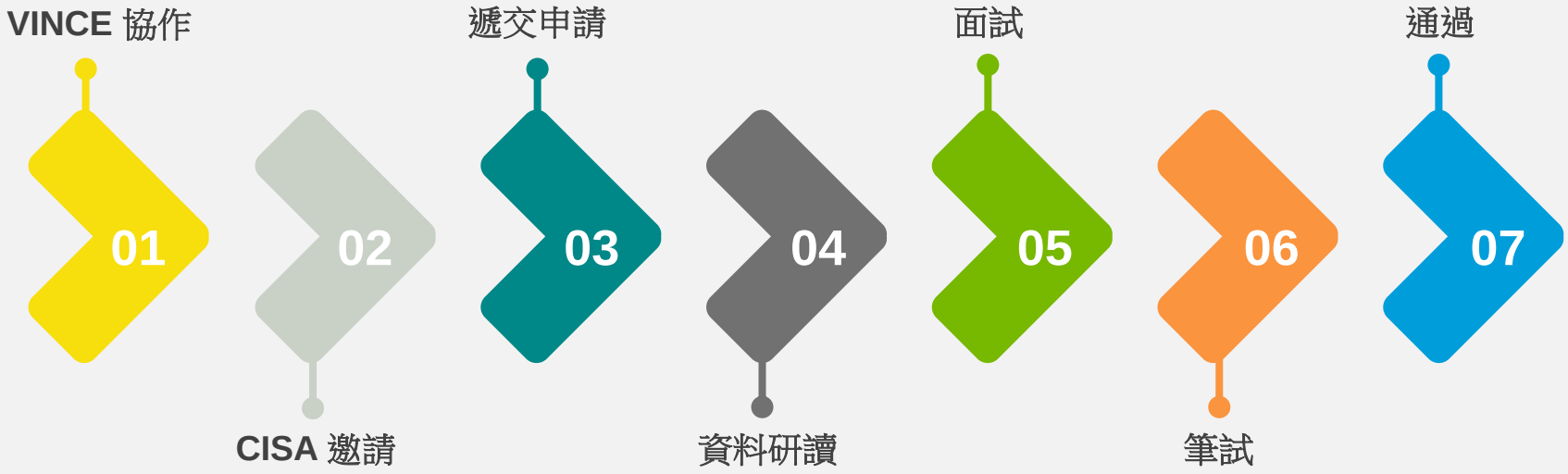
我們想加入 CNA 的原因

成為 CNA 之前要準備好的 5 件事



CNA 申請的過程，不會很久

我們加入 CNA 的過程



(以 Root CNA 是 CISA 為例)

MOXA

CVE® Numbering Authority (CNA) Operational Rules

Version 4.0

Effective August 8, 2024

Approved by CVE Board on May 8, 2024

責任

一定要遵守 CNA Rules

Source: https://www.cve.org/ResourcesSupport/AllResources/CNARules

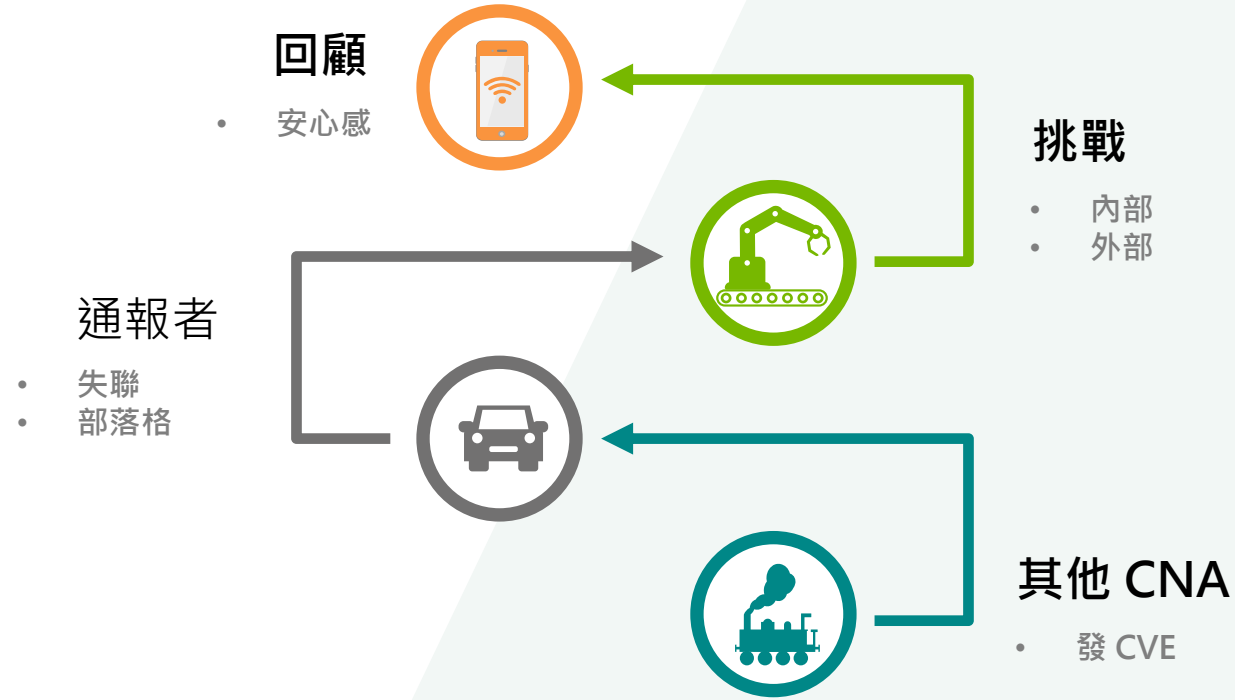
成為 CNA 之後

實現 CVE 自由？

權利	義務
• 在自己負責的範圍發 CVE • 別的 CNA 不可侵犯你的領域 • 自行管理 CVE 資料 • 參加 CNA 活動	• 不可以吃案 (誠信正直) • 弱點揭露 (公開透明) • 更及時的回應 • 積極與通報者溝通

MOXA

成為 CNA 之後 有趣的小故事分享



MOXA

SDL

從回應弱點到預防弱點

MOXA

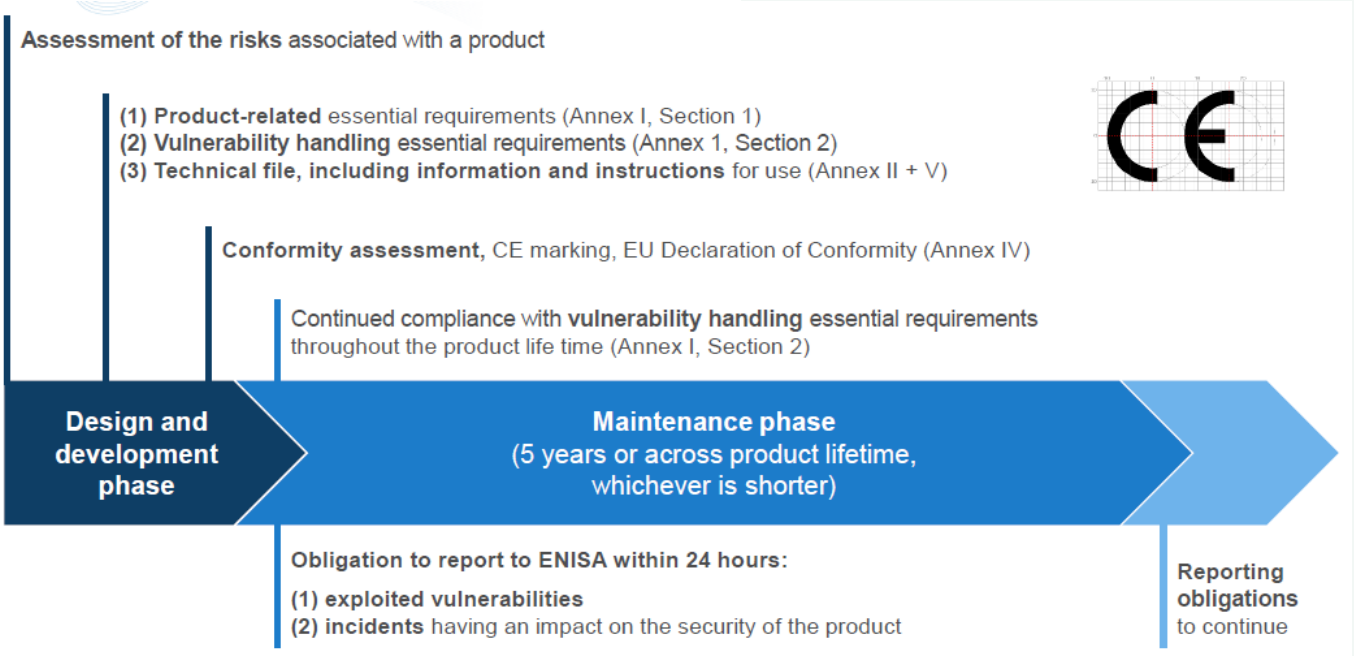
從被動回應到主動預防

SDL Process

Reason for establishment	**More and more demands are coming from the external.**
Development strategy	**Treating the evidentiary activities as short-term goals, learning from implementation.**
Achievement	**Certified products and processes**
Challenge	**Legacy products**

The Upcoming Challenges

Cyber Resilience Act and other regulations



Source: 01Policy-0 - DG CNECT - Cyber Resilience Act and NIS2.pdf (europa.eu)

MOXA

Review Key Takeaways

1

PSIRT

在策略規劃的節奏下，陪伴團隊（包含 PSIRT）成熟

2

CNA

成熟的弱點管理心態

3

SDL

取得小規模的勝利，再擴大戰果

MOXA

Thank You

MOXA®

Reliable Networks ▲ Sincere Service