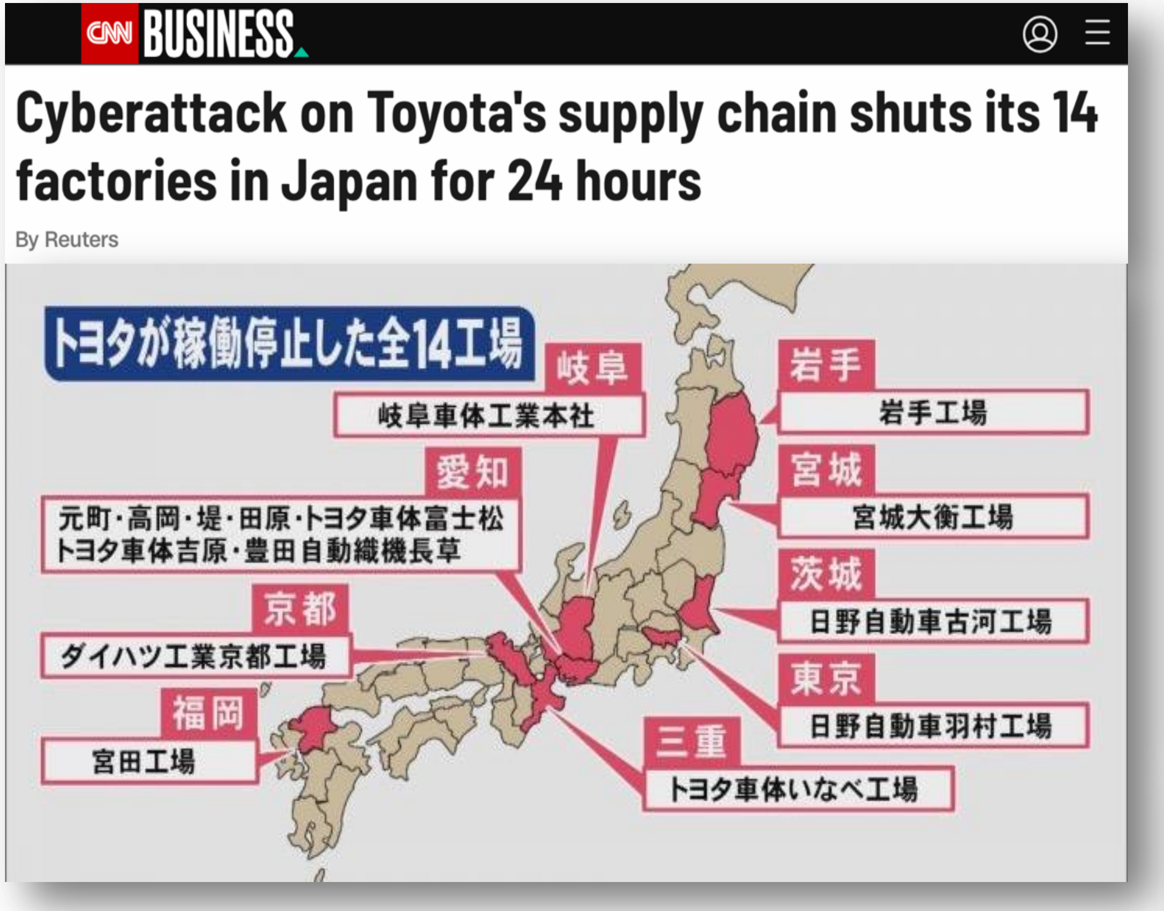
在智慧車安全道上，給您抵擋駭客攻擊的智慧之道 ，談最新車用資安技術和產品對策

Chelsea Chen
資深業務經理

駭客事件與趨勢

今日所見及不久的將來

複雜且充滿漏洞及風險的汽車供應鏈



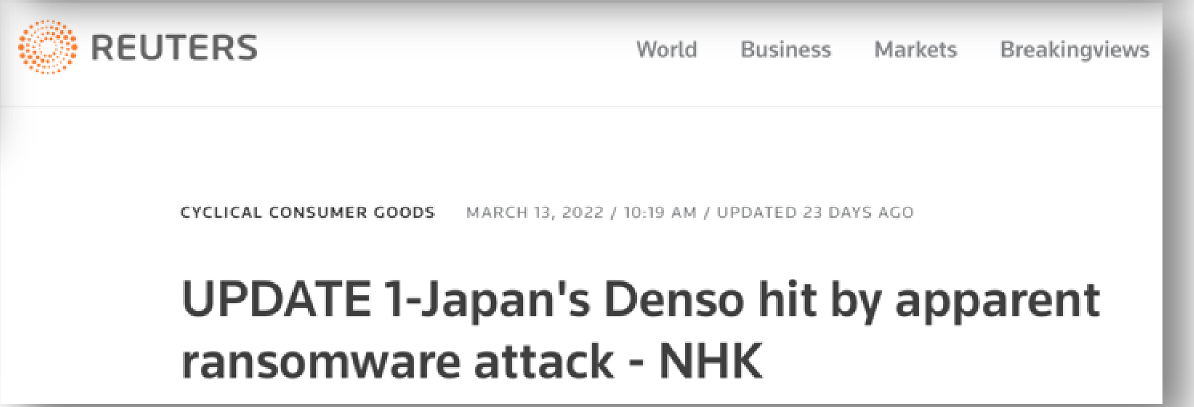
CNN BUSINESS

Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours

By Reuters

SolarWinds 18,000 Customers installed Malicious Bacdoor; U.S. Govt Issues Code Red!

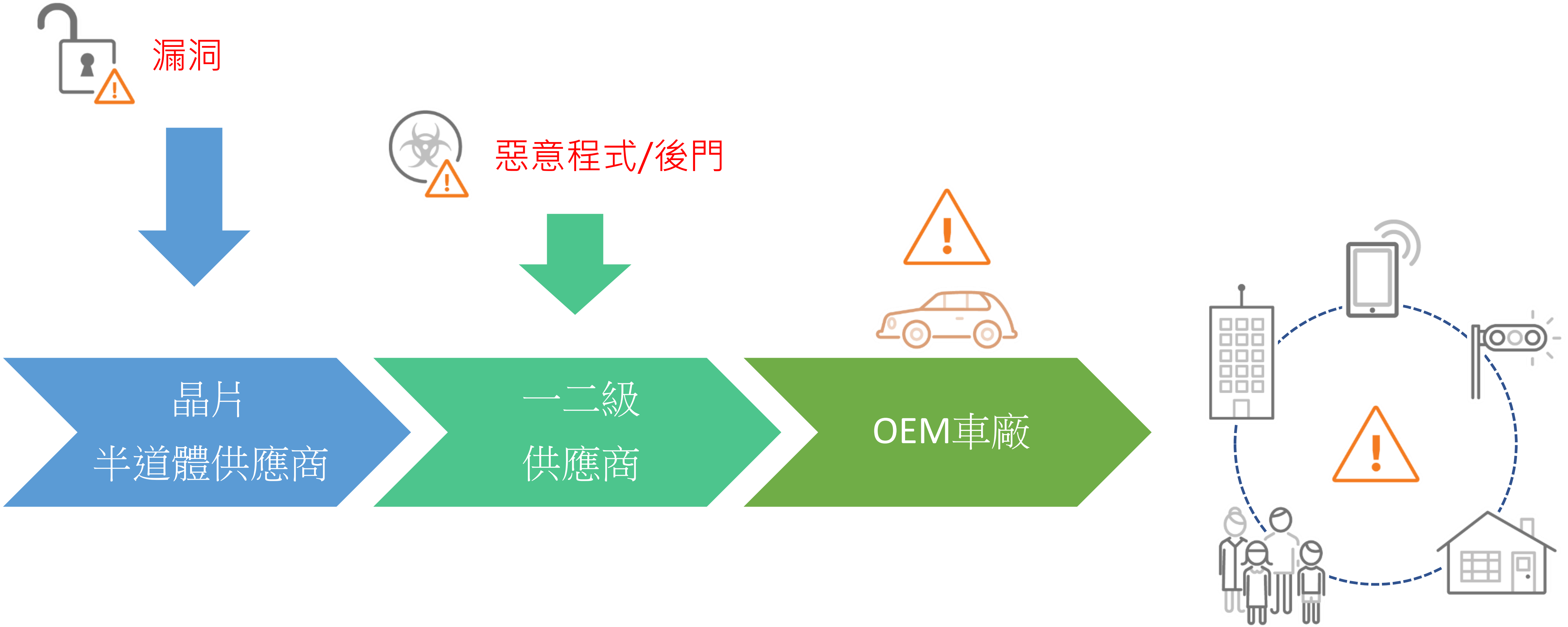
#DailyCybesecurityNews



CYCLICAL CONSUMER GOODS MARCH 13, 2022 / 10:19 AM / UPDATED 23 DAYS AGO

UPDATE 1-Japan's Denso hit by apparent ransomware attack - NHK

供應商本身的風險影響最終消費者



漏洞

惡意程式/後門

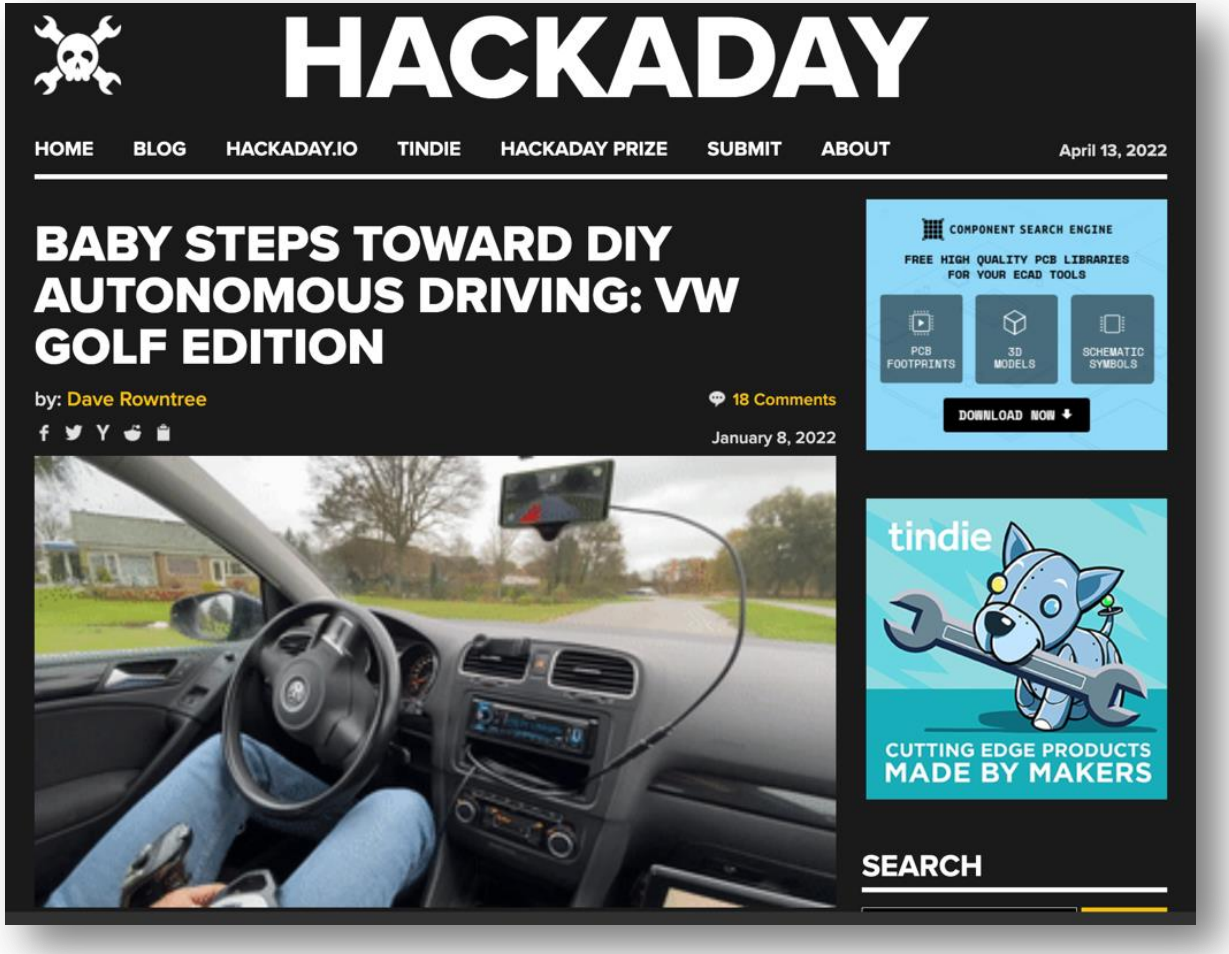
晶片
半道體供應商

一二級
供應商

OEM車廠

- 傳統網路犯罪已擴及車用產業，連網車讓駭客更容易攻擊
- 車用供應鍊成為駭客眼中的目標

駭入車輛的進入門檻已下降



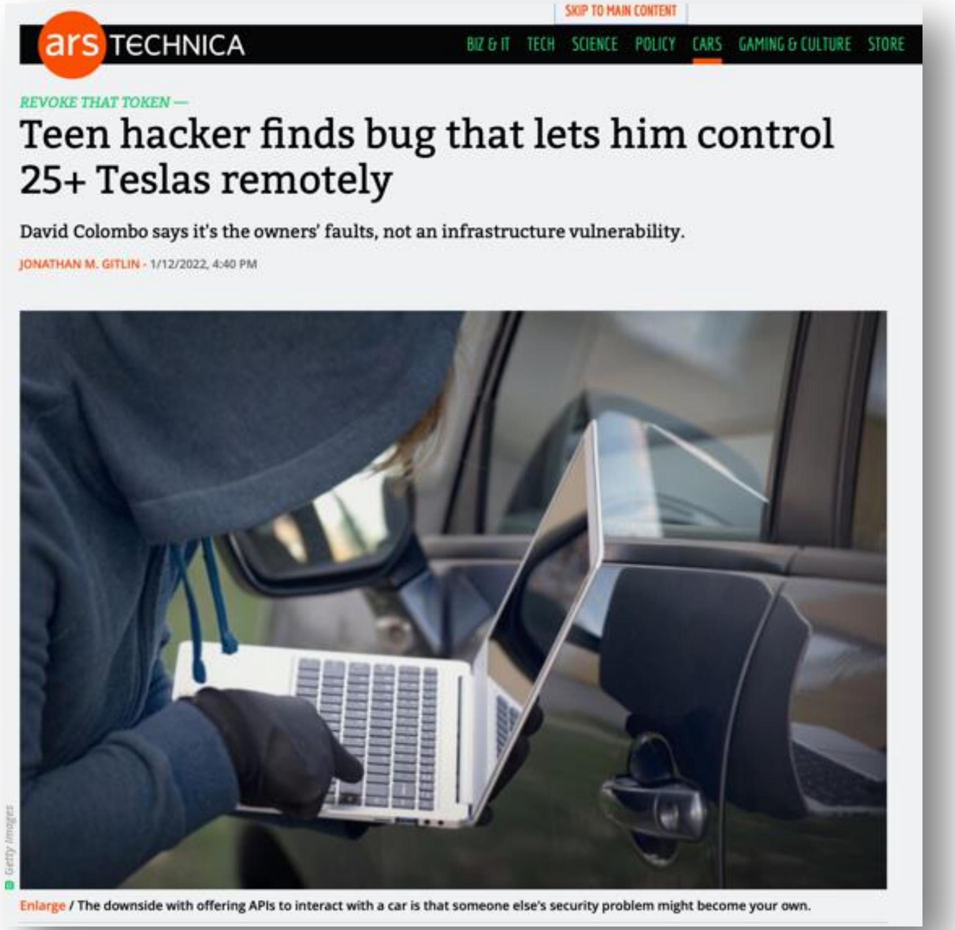
April 13, 2022

BABY STEPS TOWARD DIY AUTONOMOUS DRIVING: VW GOLF EDITION

by: Dave Rowntree

18 Comments

January 8, 2022



REVOKE THAT TOKEN —

Teen hacker finds bug that lets him control 25+ Teslas remotely

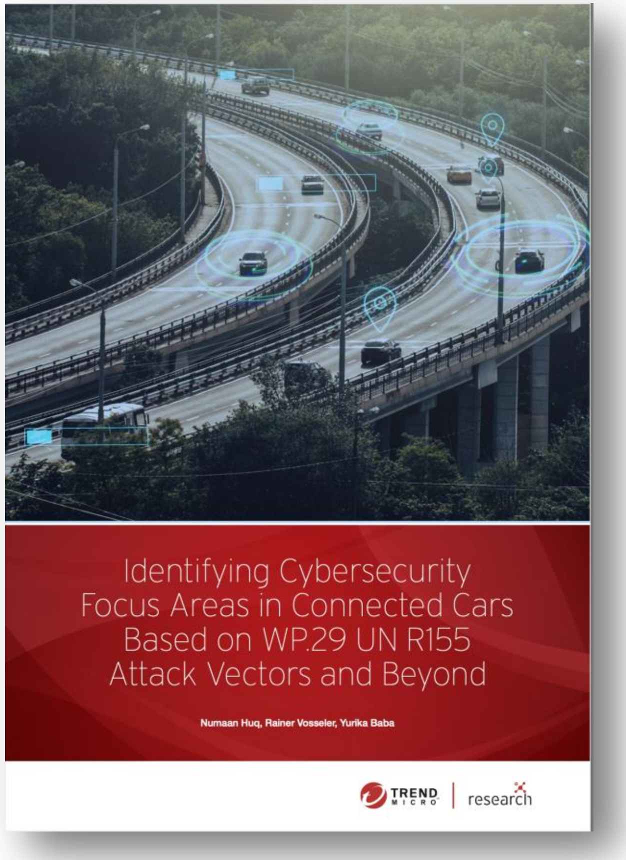
David Colombo says it's the owners' faults, not an infrastructure vulnerability.

JONATHAN M. GITLIN - 1/12/2022, 4:40 PM

Enlarge / The downside with offering APIs to interact with a car is that someone else's security problem might become your own.

- 聯網車帶來更多的便利性，卻也為” 路上跑的電腦” 帶來更多風險
- 即使普通人也能透過網路上的資訊/查詢如何破解車輛
- 車輛若能被輕易駭入，將對品牌形象 造成衝擊

CASE (聯網、自駕、共享、電動車)資安風險



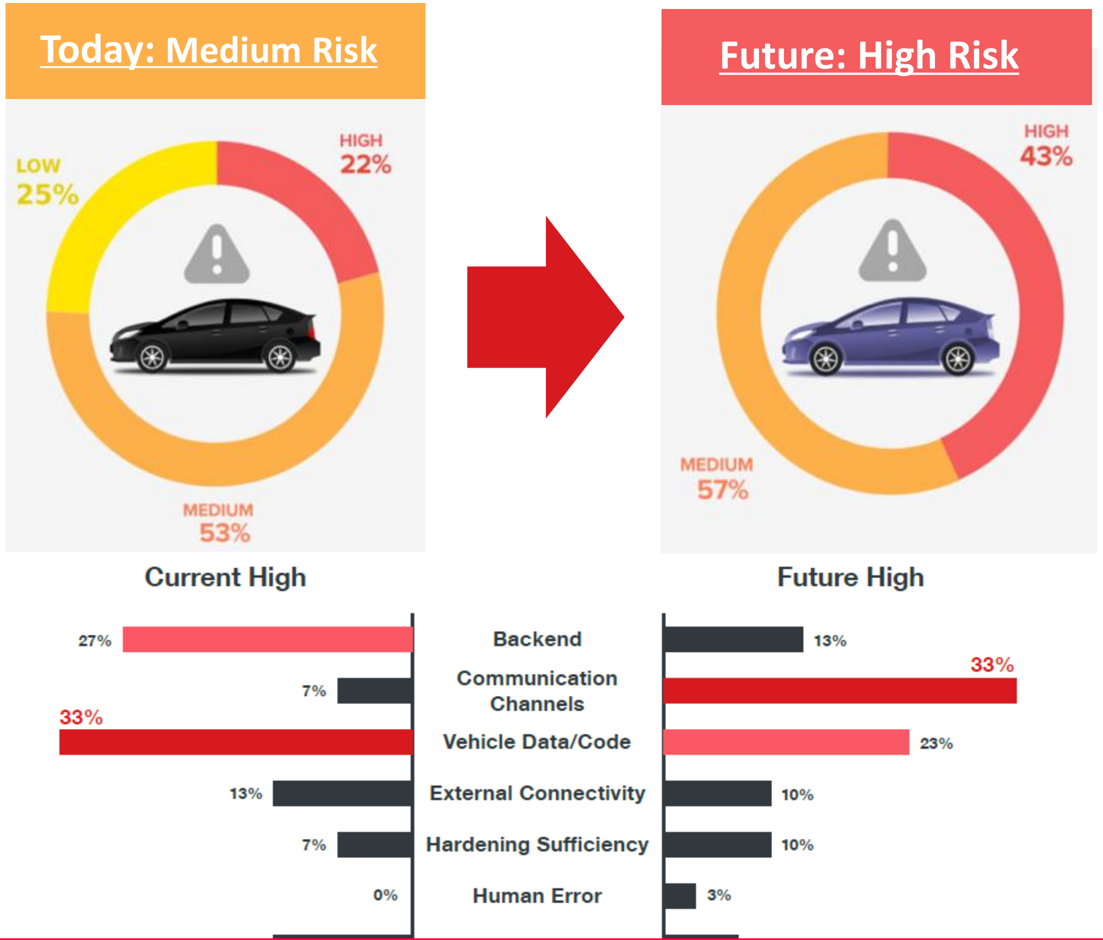
Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN R155 Attack Vectors and Beyond

Numaan Huq, Rainer Vosseler, Yurika Baba

TREND MICRO | research

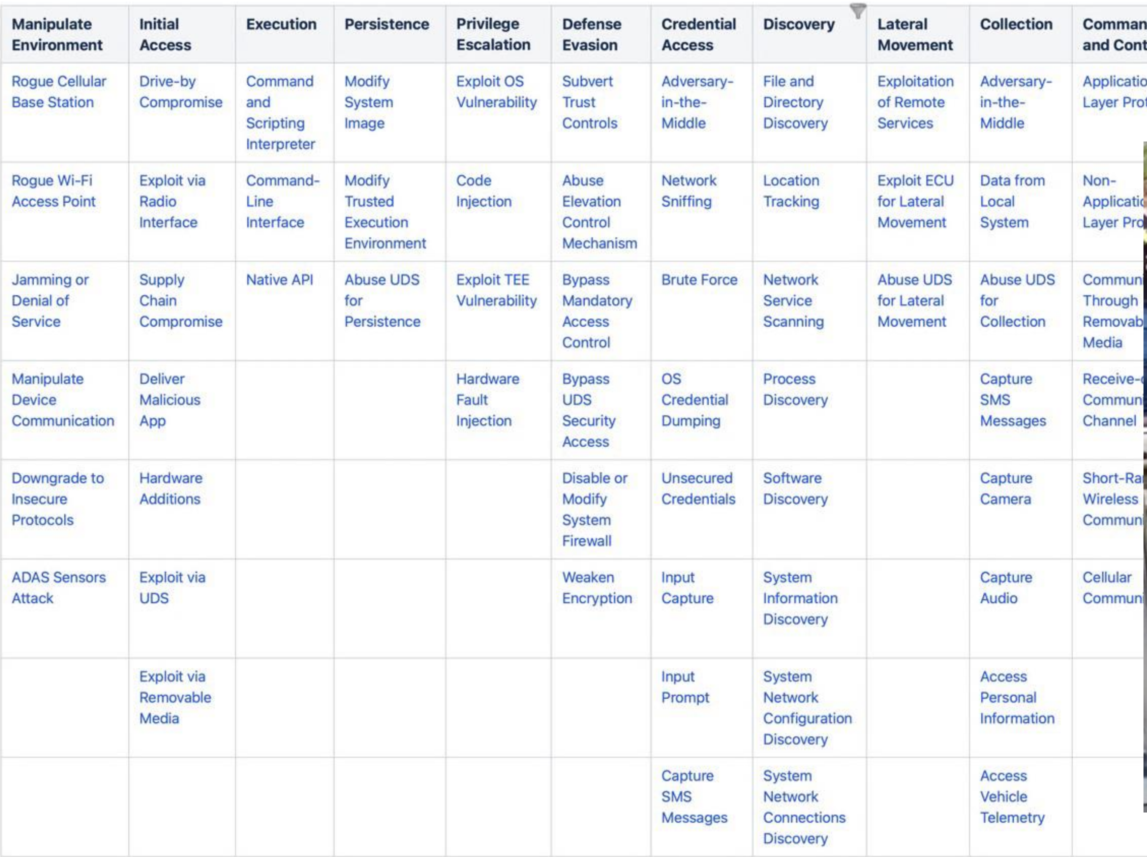
UN R155 附件 5

列出了 69 個攻擊途徑或風險



- 聯網車的風險與日俱增
- 車輛數據/代碼和通信是最需要注意的 2 個問題

VicOne車用威脅資料庫



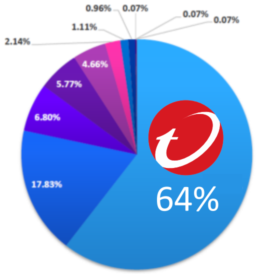
Manipulate Environment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Affect Vehicle Function	Impact
Rogue Cellular Base Station	Drive-by Compromise	Command and Scripting Interpreter	Modify System Image	Exploit OS Vulnerability	Subvert Trust Controls	Adversary-in-the-Middle	File and Directory Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Exfiltration Over C2 Channel	Unintended Vehicle Control Message	Loss of Availability
Rogue Wi-Fi Access Point	Exploit via Radio Interface	Command-Line Interface	Modify Trusted Execution Environment	Code Injection	Abuse Elevation Control Mechanism	Network Sniffing	Location Tracking	Exploit ECU for Lateral Movement	Data from Local System	Non-Applicati Layer Pro			
Jamming or Denial of Service	Supply Chain Compromise	Native API	Abuse UDS for Persistence	Exploit TEE Vulnerability	Bypass Mandatory Access Control	Brute Force	Network Service Scanning	Abuse UDS for Lateral Movement	Abuse UDS for Collection	Commun Through Removab Media			
Manipulate Device Communication	Deliver Malicious App			Hardware Fault Injection	Bypass UDS Security Access	OS Credential Dumping	Process Discovery		Capture SMS Messages	Receive-c Commun Channel			
Downgrade to Insecure Protocols	Hardware Additions				Disable or Modify System Firewall	Unsecured Credentials	Software Discovery		Capture Camera	Short-Ra Wireless Commun			
ADAS Sensors Attack	Exploit via UDS				Weaken Encryption	Input Capture	System Information Discovery		Capture Audio	Cellular Commun			
	Exploit via Removable Media					Input Prompt	System Network Configuration Discovery		Access Personal Information				
						Capture SMS Messages	System Network Connections Discovery		Access Vehicle Telemetry				

Automotive MITRE ATT&CK® 框架

VicOne 比同業提前 1~2 個月提供修補方案

ZERO DAY INITIATIVE

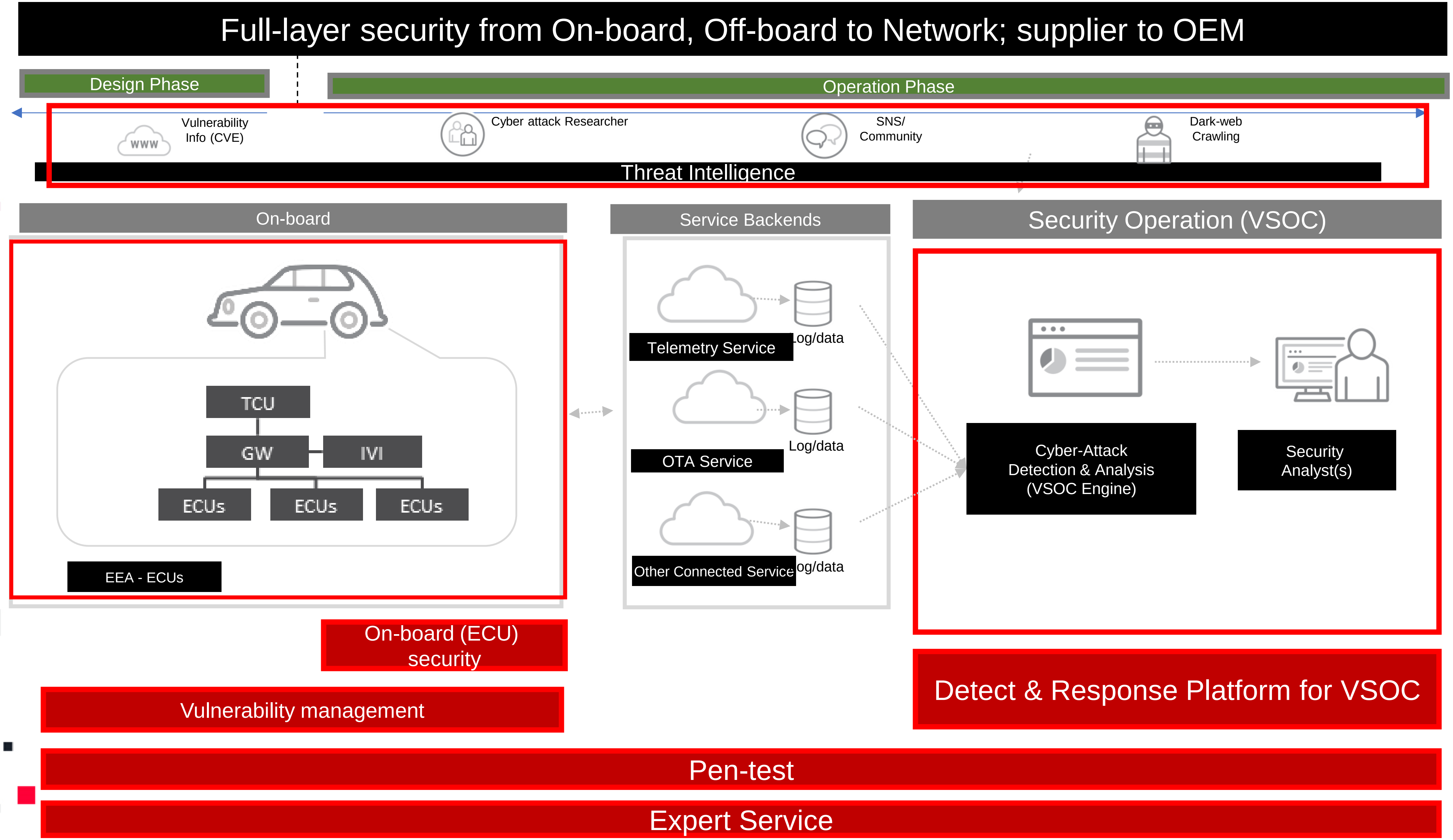
- Founded in 2005, market leader in the public disclosure market for past 13 years.
- Highest for disclosed vulnerabilities across all severity levels
- Powered by over 10,000 independent researchers
- Contributing research from many different areas including Automotive



VicOne
車用資安解決方案

VicOne車用資安解決方案適用範圍

🟥 : VicOne solution/ service



Full-layer security from On-board, Off-board to Network; supplier to OEM

Design Phase

Operation Phase

Vulnerability Info (CVE)

Cyber attack Researcher

SNS/ Community

Dark-web Crawling

Threat Intelligence

On-board

TCU

GW

IVI

ECUs

ECUs

ECUs

EEA - ECUs

Service Backends

Telemetry Service

Log/data

OTA Service

Log/data

Other Connected Service

og/data

Security Operation (VSOC)

Cyber-Attack Detection & Analysis (VSOC Engine)

Security Analyst(s)

On-board (ECU) security

Vulnerability management

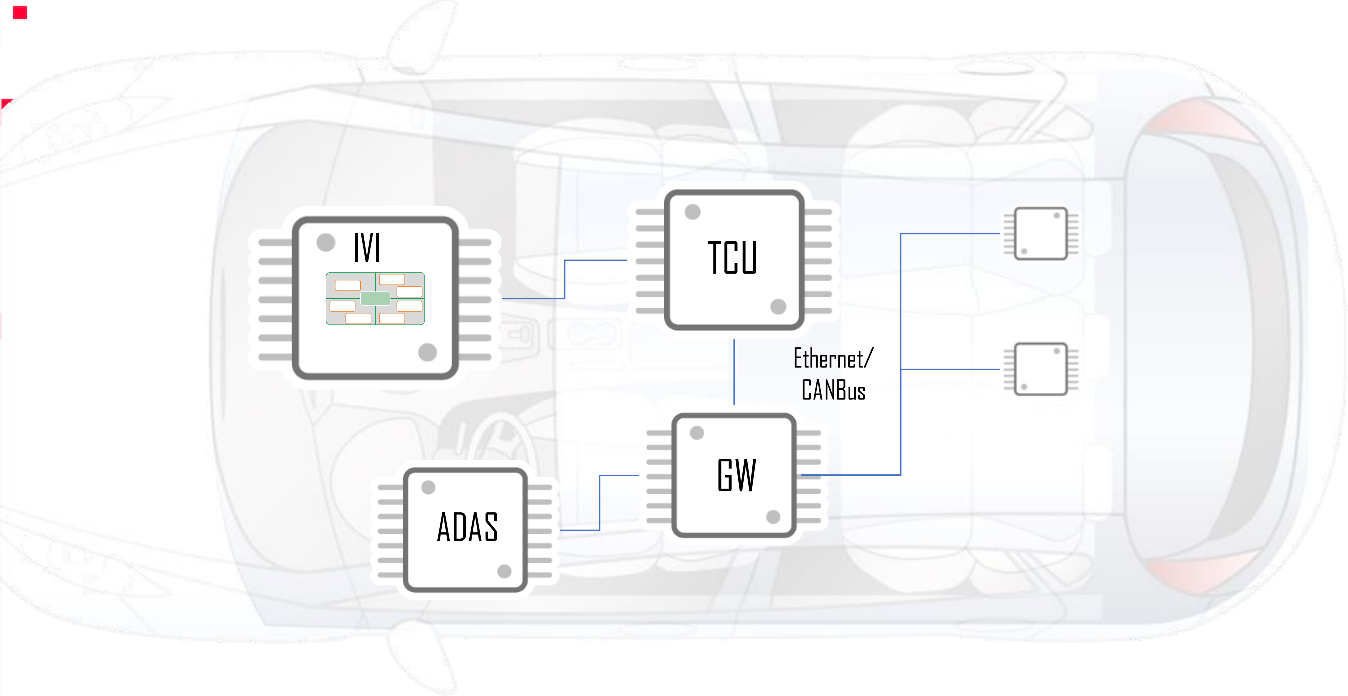
Detect & Response Platform for VSOC

Pen-test

Expert Service

xCarbon

適用於不同汽車EEA並針對各種ECU用途設計，整合零摩擦的車用入侵偵測防護系統



安全性和效能的平衡

考慮EEA 以整合ECU，將電子控制單元 (ECU) 效能影響降至最低。

模組化設計和可配置性

與 AUTOSAR 兼容；支援足夠的功能和配置，以滿足不同類型的車輛和服務級別。

掌握威脅趨勢

及時部署虛擬補丁(virtual patch)或入侵預防系統(IPS)規則，以防止和攔截漏洞攻擊。

xCarbon全面偵測及防護力

應用程式白名單

- 使用基於規則的應用程式控制，確保授權應用程式的完整性

系統漏洞防護

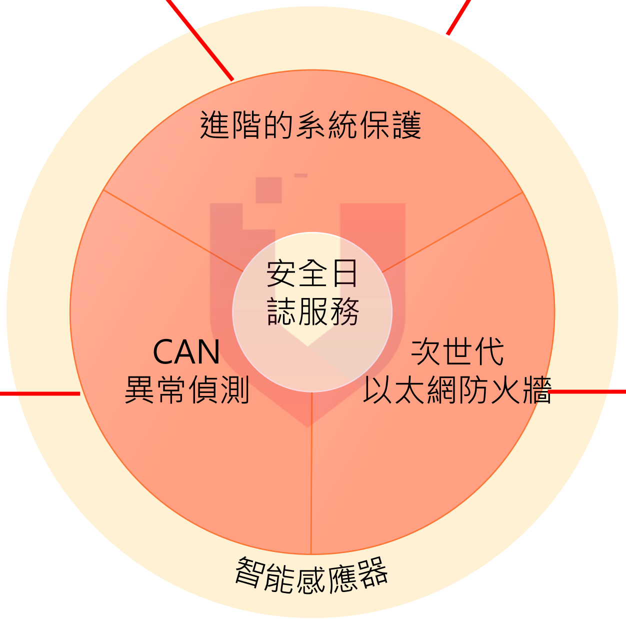
- 分析系統的異常活動，以防止漏洞被利用和權限提升

- **收集系統活動和關鍵事件**以進行分析和數據取證的自動化流程。
- 從系統日誌、進程日誌、網絡日誌等中提取數據，逐步分析和過濾威脅。

即時辨識出正常行為和異常行為以偵測出惡意的訊息如下

- 未知的CAN ID
- 頻率異常
- 內容異常
- CAN ID 序列異常

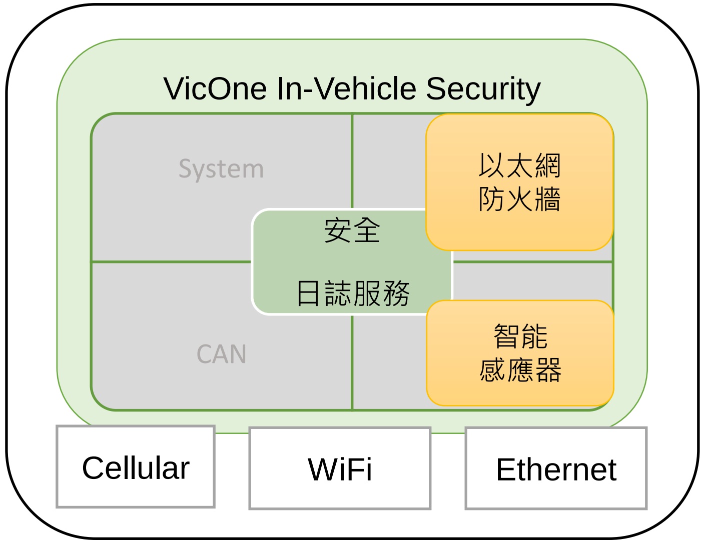
- **以太網入侵檢測**
  - 基於簽名的入侵檢測，使用深度數據包技術(DPI)檢測及識別可疑事件
- **虛擬補丁**
  - 使用預定義的簽名防止已知漏洞的攻擊
- **網頁/ IP 的過濾**
  - 檢測到惡意域名和 IP 地址的連接



適用於不同ECU的保護功能

TCU

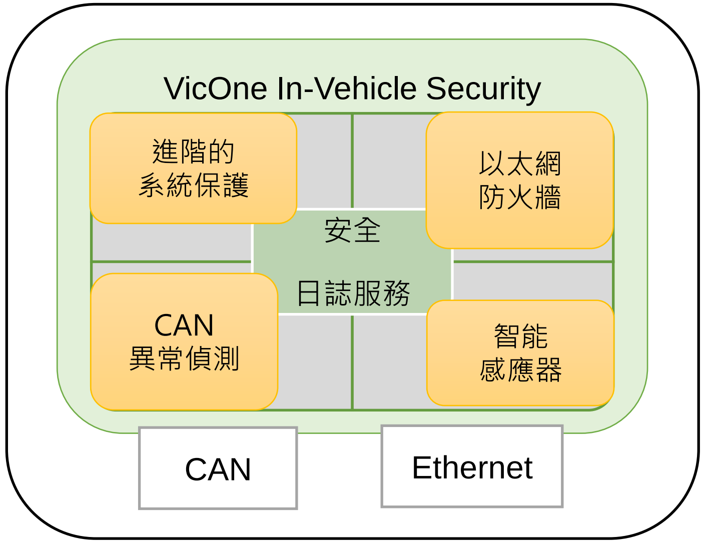
- Rich connectivity interfaces
- Limited HW resources and computing power



- Ethernet solution to mitigate the intrusions from connectivity interfaces
- Enable Sensor solution to leverage cloud engine for threat detection

GW

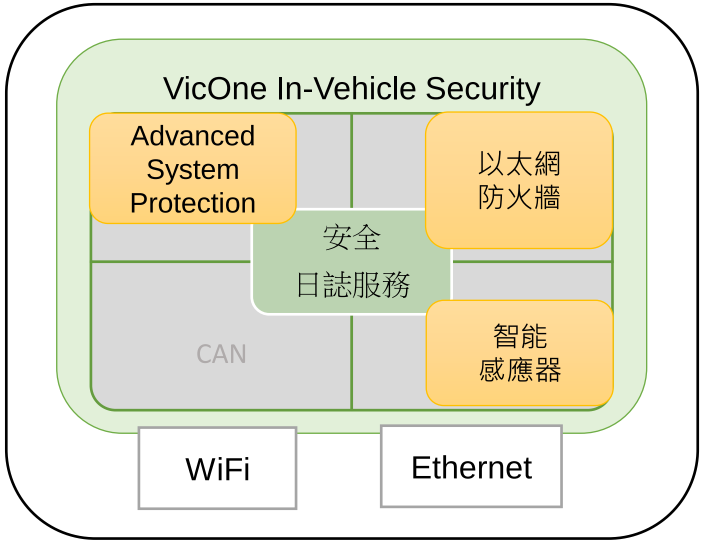
- Connects to Internet and in-vehicle network
- Running business-critical applications, ex: OTA



- Enable CAN and Ethernet solutions for network interfaces
- Enable System protection for critical apps
- Sensor solution for advanced cloud detection

IVI

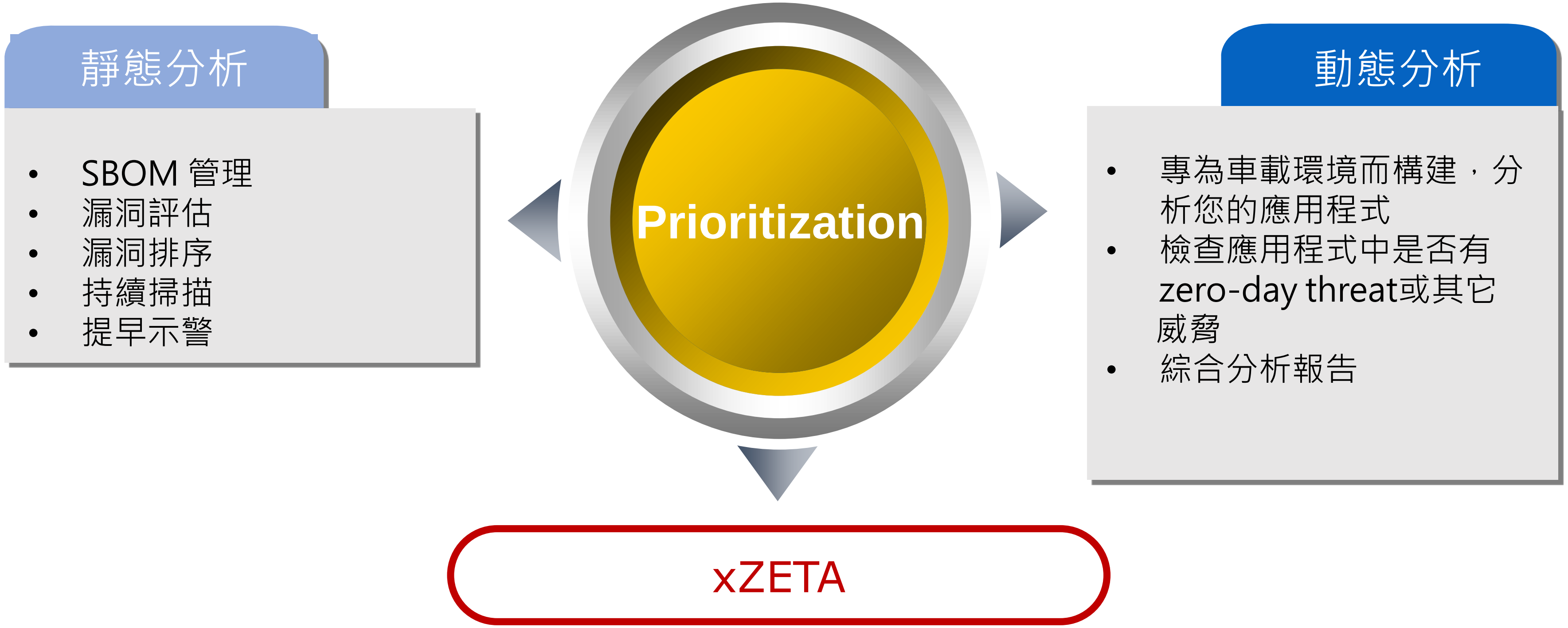
- Multiple connectivity interfaces
- Running various 3rd party applications, ex: Streaming, browser



- Ethernet solutions for connectivity interfaces
- Enable System solution to mitigate the risks of 3rd party apps
- Sensor solution for advanced cloud detection

xZETA

針對已知或不明的漏洞、潛在惡意軟體與後門風險的多層次安全保護



靜態分析

- SBOM 管理
- 漏洞評估
- 漏洞排序
- 持續掃描
- 提早示警

Prioritization

動態分析

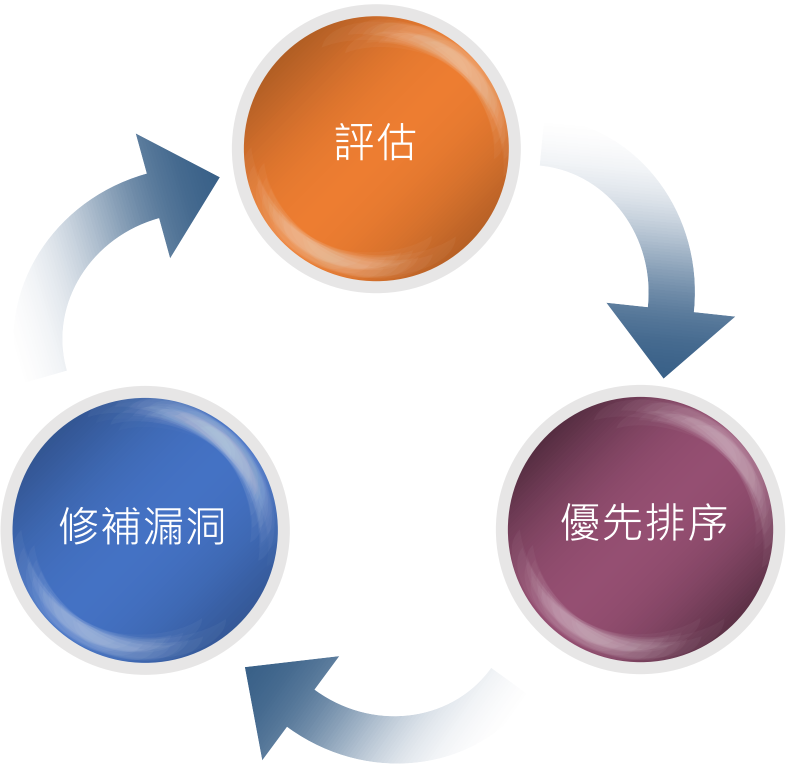
- 專為車載環境而構建，分析您的應用程式
- 檢查應用程式中是否有zero-day threat或其它威脅
- 綜合分析報告

xZETA

xZETA 漏洞掃描

xZETA漏洞掃描三步驟

評估	支援車載ECU Firmware
優先排序	考慮各別ECU系統環境及ZDI/VicOne資安專家建議，提供VicOne漏洞評分vulnerability impact rating (VIR)
修補漏洞	資安專家提供漏洞修補建議

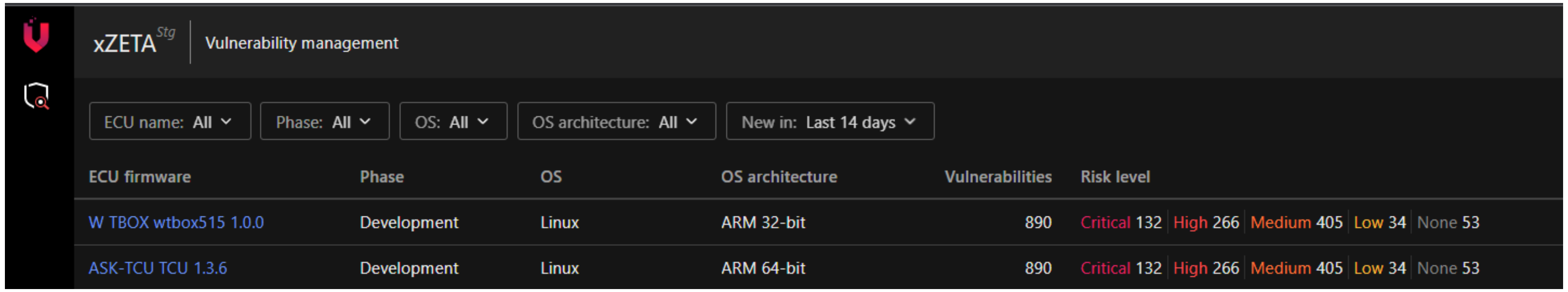


Vulnerabilities Sources

JVN | NVD CVE | ZDI | ICS-CERT | Mitre CWE | CNA Advisories | Project Zero | Bug Reports | Social Media

TREND MICRO Largest vulnerability discovery community

xZETA



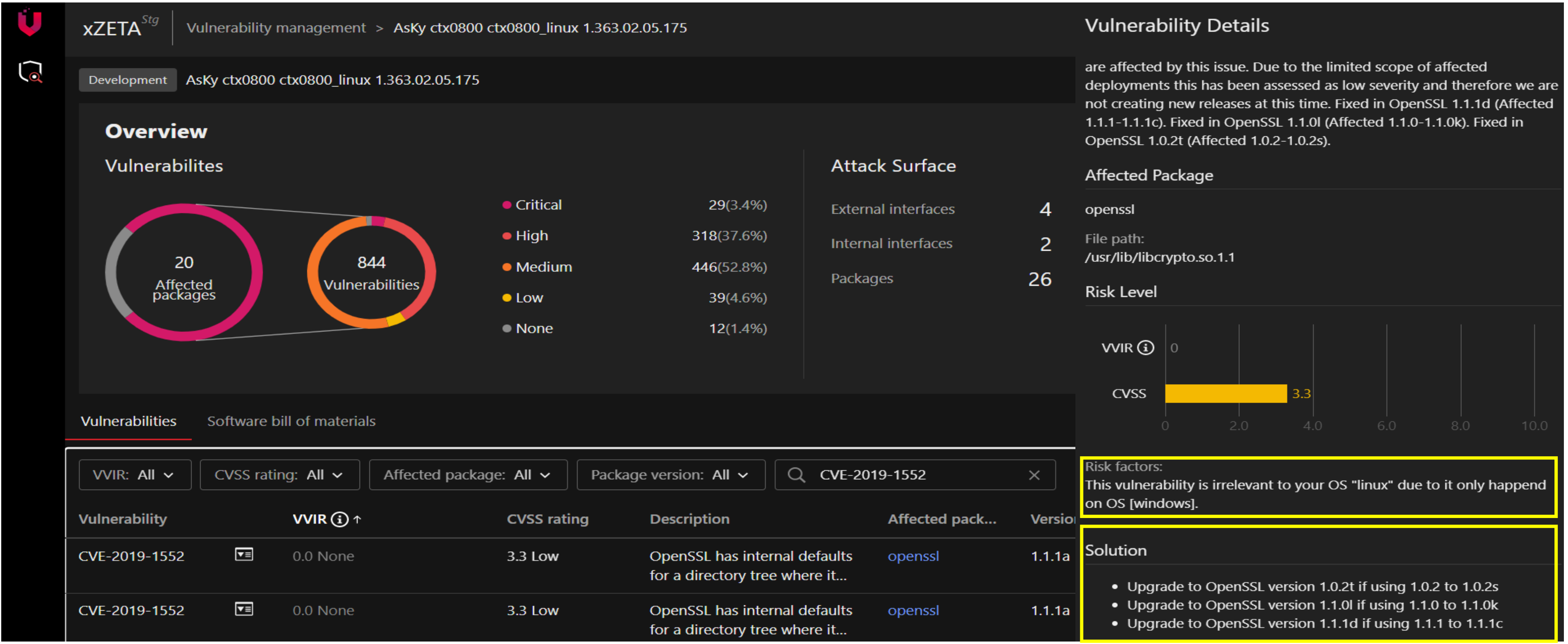
xZETA Stg | Vulnerability management

ECU name: All ⌄ | Phase: All ⌄ | OS: All ⌄ | OS architecture: All ⌄ | New in: Last 14 days ⌄

ECU firmware	Phase	OS	OS architecture	Vulnerabilities	Risk level
W TBOX wtbox515 1.0.0	Development	Linux	ARM 32-bit	890	Critical 132 | High 266 | Medium 405 | Low 34 | None 53
ASK-TCU TCU 1.3.6	Development	Linux	ARM 64-bit	890	Critical 132 | High 266 | Medium 405 | Low 34 | None 53

評估

優先排序
修補漏洞



xZETA Stg | Vulnerability management > AsKy ctx0800 ctx0800_linux 1.363.02.05.175

Development AsKy ctx0800 ctx0800_linux 1.363.02.05.175

Overview

Vulnerabilites

● Critical	29(3.4%)
● High	318(37.6%)
● Medium	446(52.8%)
● Low	39(4.6%)
● None	12(1.4%)

Attack Surface

External interfaces	4
Internal interfaces	2
Packages	26

Vulnerabilities | Software bill of materials

VVIR: All ⌄ | CVSS rating: All ⌄ | Affected package: All ⌄ | Package version: All ⌄ | CVE-2019-1552 ✕

Vulnerability		VVIR ⓘ ↑	CVSS rating	Description	Affected pack...	Versio
CVE-2019-1552		0.0 None	3.3 Low	OpenSSL has internal defaults for a directory tree where it...	openssl	1.1.1a
CVE-2019-1552		0.0 None	3.3 Low	OpenSSL has internal defaults for a directory tree where it...	openssl	1.1.1a

Vulnerability Details

are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

Affected Package

openssl

File path:
/usr/lib/libcrypto.so.1.1

Risk Level

Risk factors:
This vulnerability is irrelevant to your OS "linux" due to it only happend on OS [windows].

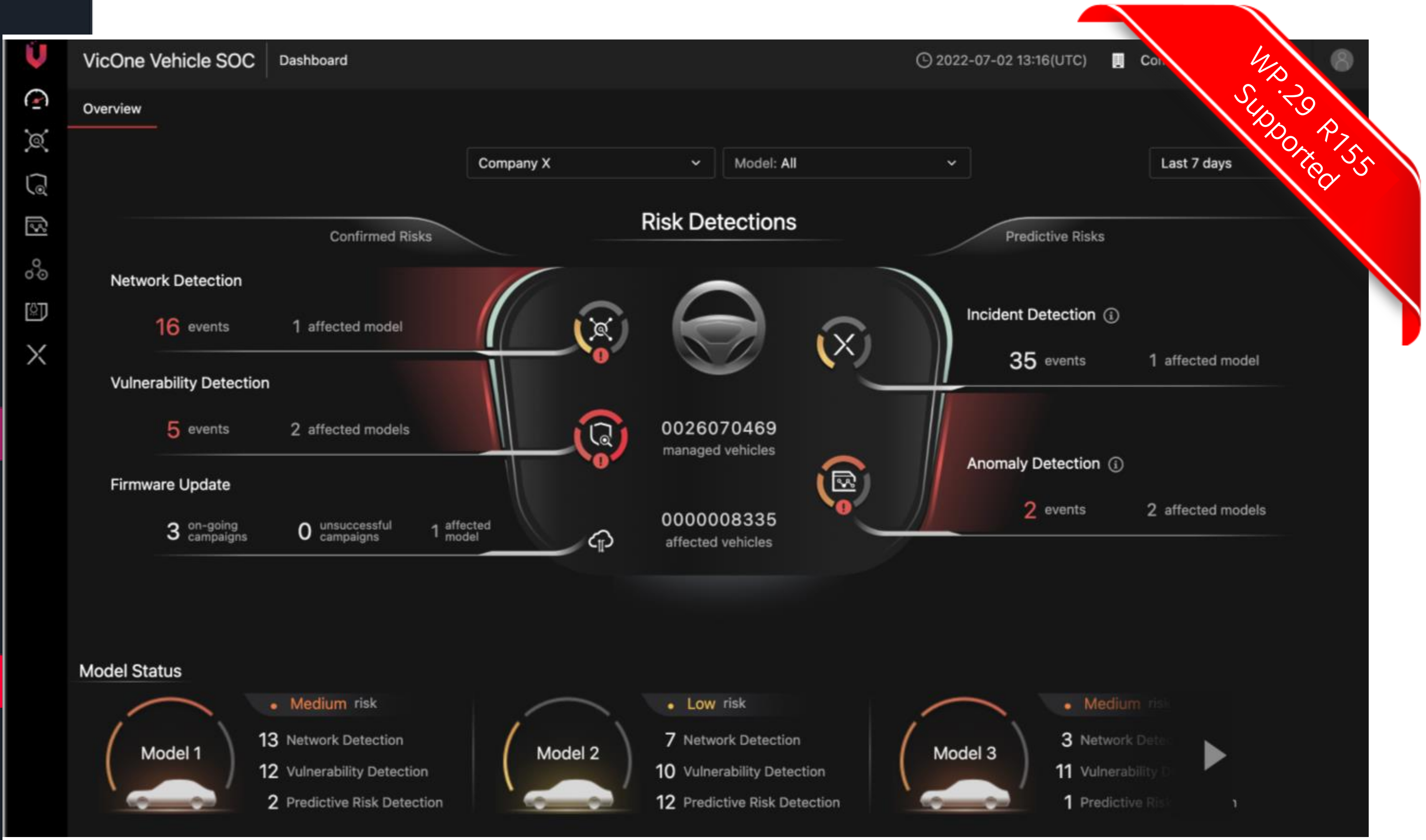
Solution

- Upgrade to OpenSSL version 1.0.2t if using 1.0.2 to 1.0.2s
- Upgrade to OpenSSL version 1.1.0l if using 1.1.0 to 1.1.0k
- Upgrade to OpenSSL version 1.1.1d if using 1.1.1 to 1.1.1c

VVIR- VicOne Vulnerability Impact Rating

xNexus

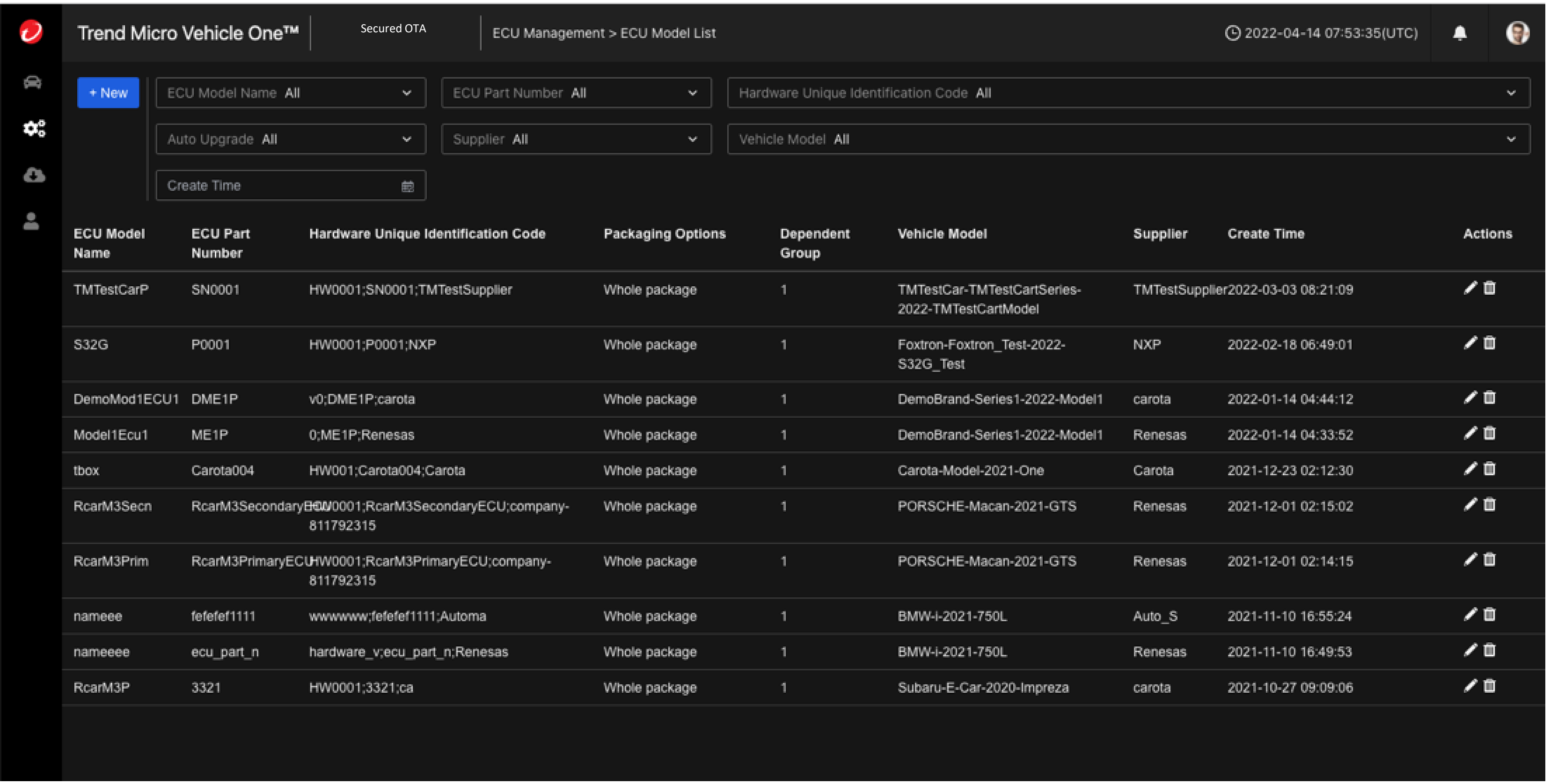
擁有偵測及回應能力的汽車專用資訊安全監控中心(VSOC)



- 支持 UN R155 的合規性。
- 彈性支援不同來源的數據
- 點、線、面，多層式可視性
- 業界認可的車用解決方案

xSUMO

資安強化的韌體更新系統(OTA)



ECU Model Name All

ECU Part Number All

Hardware Unique Identification Code All

Auto Upgrade All

Supplier All

Vehicle Model All

Create Time

ECU Model Name	ECU Part Number	Hardware Unique Identification Code	Packaging Options	Dependent Group	Vehicle Model	Supplier	Create Time	Actions
TMTestCarP	SN0001	HW0001;SN0001;TMTestSupplier	Whole package	1	TMTestCar-TMTestCartSeries-2022-TMTestCartModel	TMTestSupplier	2022-03-03 08:21:09	✎ 🗑
S32G	P0001	HW0001;P0001;NXP	Whole package	1	Foxtron-Foxtron_Test-2022-S32G_Test	NXP	2022-02-18 06:49:01	✎ 🗑
DemoMod1ECU1	DME1P	v0;DME1P;carota	Whole package	1	DemoBrand-Series1-2022-Model1	carota	2022-01-14 04:44:12	✎ 🗑
Model1Ecu1	ME1P	0;ME1P;Renesas	Whole package	1	DemoBrand-Series1-2022-Model1	Renesas	2022-01-14 04:33:52	✎ 🗑
tbox	Carota004	HW001;Carota004;Carota	Whole package	1	Carota-Model-2021-One	Carota	2021-12-23 02:12:30	✎ 🗑
RcarM3Secn	RcarM3SecondaryECU	HW0001;RcarM3SecondaryECU;company-811792315	Whole package	1	PORSCHE-Macan-2021-GTS	Renesas	2021-12-01 02:15:02	✎ 🗑
RcarM3Prim	RcarM3PrimaryECU	HW0001;RcarM3PrimaryECU;company-811792315	Whole package	1	PORSCHE-Macan-2021-GTS	Renesas	2021-12-01 02:14:15	✎ 🗑
nameee	fefefef1111	wwwwww;fefefef1111;Automa	Whole package	1	BMW-i-2021-750L	Auto_S	2021-11-10 16:55:24	✎ 🗑
nameeee	ecu_part_n	hardware_v;ecu_part_n;Renesas	Whole package	1	BMW-i-2021-750L	Renesas	2021-11-10 16:49:53	✎ 🗑
RcarM3P	3321	HW0001;3321;ca	Whole package	1	Subaru-E-Car-2020-Impreza	carota	2021-10-27 09:09:06	✎ 🗑

相容於OTA法規需求

支援 Uptane 及 UNECE WP.29 R156

彈性化設計

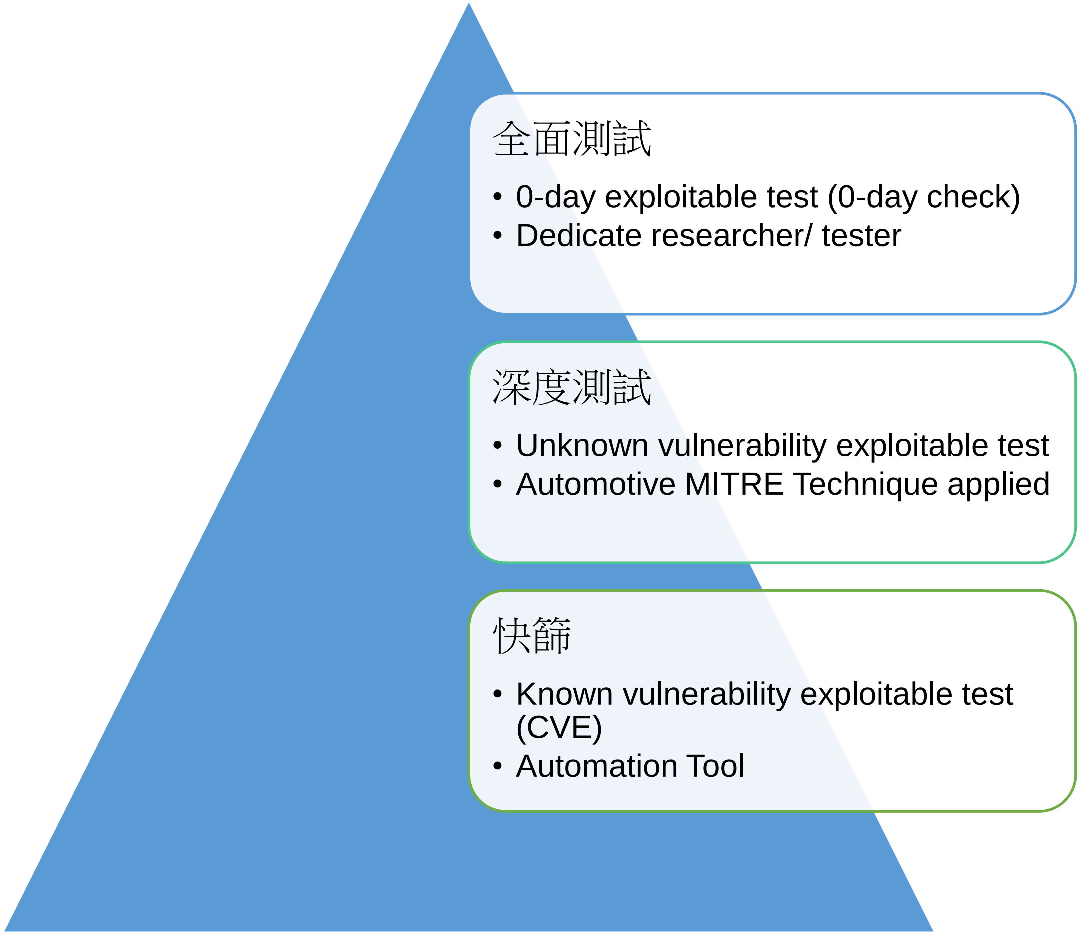
支援各式ECU及EEA架構，降低整合所需的花費

與VSOC的無縫接軌

OTA事件回報，整合於VSOC平台，確保每個動作都是安全無虞。

xScope

車用等級**滲透測試**提供您不同級別的選擇以滿足您的需求



全面測試

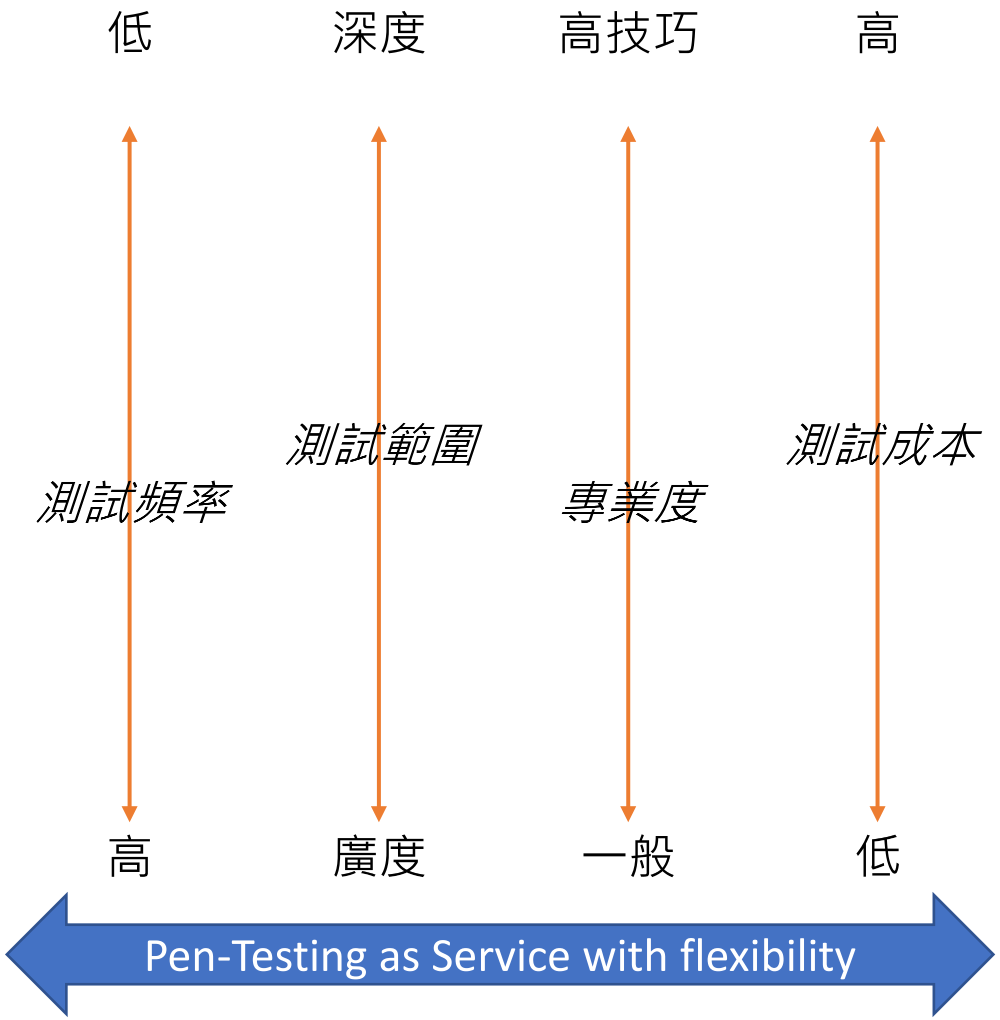
- 0-day exploitable test (0-day check)
- Dedicate researcher/ tester

深度測試

- Unknown vulnerability exploitable test
- Automotive MITRE Technique applied

快篩

- Known vulnerability exploitable test (CVE)
- Automation Tool



低 — *測試頻率* — 高

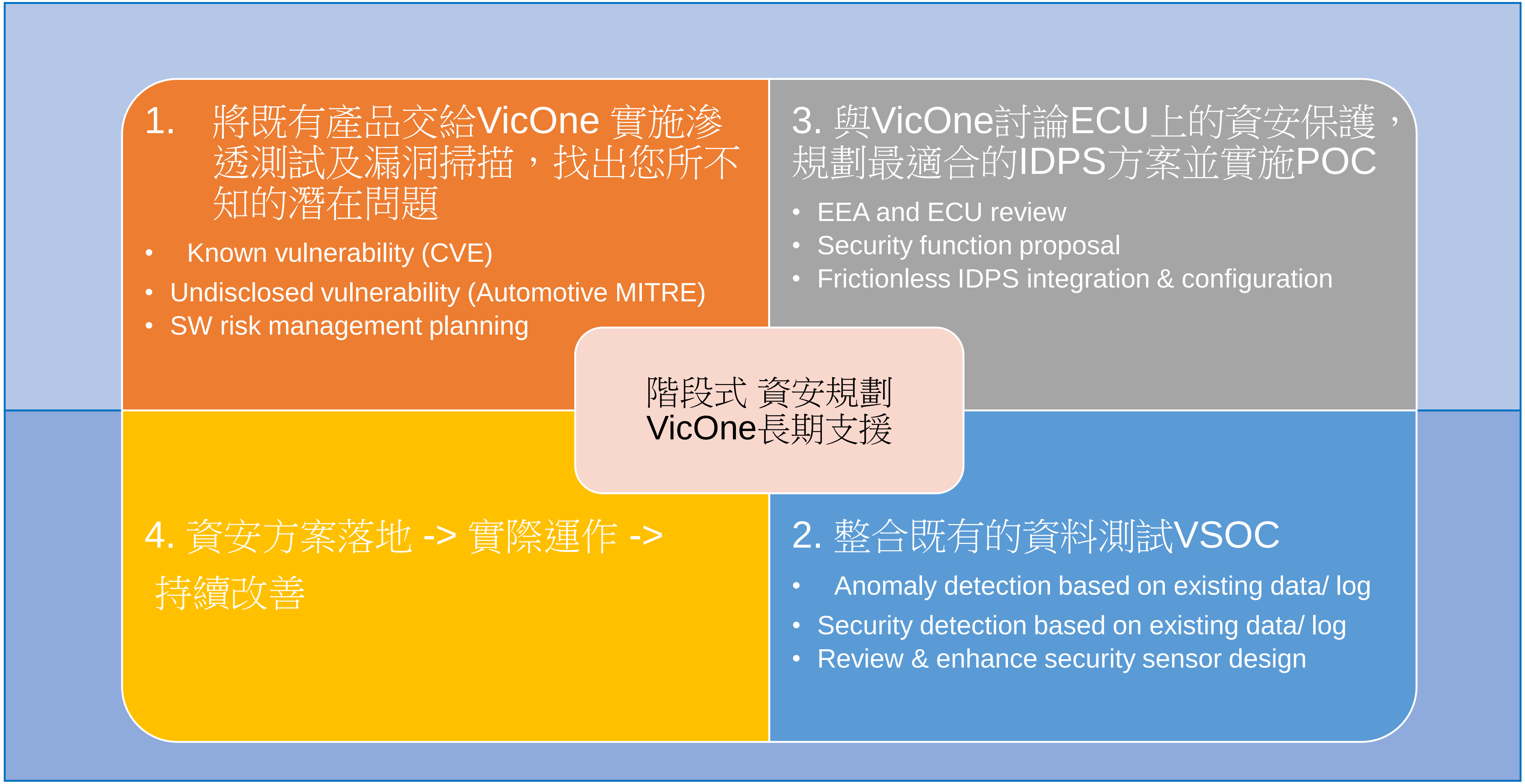
深度 — *測試範圍* — 廣度

高技巧 — *專業度* — 一般

高 — *測試成本* — 低

Pen-Testing as Service with flexibility

如何跨出車用資安第一步



1. 將既有產品交給VicOne 實施滲透測試及漏洞掃描，找出您所不知的潛在問題

- Known vulnerability (CVE)
- Undisclosed vulnerability (Automotive MITRE)
- SW risk management planning

3. 與VicOne討論ECU上的資安保護，規劃最適合的IDPS方案並實施POC

- EEA and ECU review
- Security function proposal
- Frictionless IDPS integration & configuration

階段式 資安規劃
VicOne長期支援

4. 資安方案落地 -> 實際運作 ->
持續改善

2. 整合既有的資料測試VSOC

- Anomaly detection based on existing data/ log
- Security detection based on existing data/ log
- Review & enhance security sensor design

THANK YOU!

chelsea_chen@vicone.com

VicOne

Driving Automotive Cybersecurity Forward